LCOS 10.90

Referenzhandbuch

04/2025

LANCOM SYSTEMS

Inhalt

1 LCOS....26
2 Konfiguration....27
2.1 Mittel und Wege für die Konfiguration....27
2.2 Software zur Konfiguration....27
2.2.1 LANconfig....28
2.2.2 WEBconfig....28
2.2.3 LANCOM Management Cloud (LMC)....41
2.2.4 Terminalprogramm....47
2.2.5 SNMP Management-Programm....77
2.3 LANCOM Layer 2 Management Protokoll (LL2M)....78
2.3.1 Einleitung....78
2.3.2 Konfiguration des LL2M-Servers....78
2.3.3 Befehle für den LL2M-Client....78
2.4 Speichern und Laden von Gerätekonfiguration und Skriptdateien....80
2.4.1 Konfigurationsverwaltung über WEBconfig und Konsole....81
2.4.2 Skriptverwaltung über WEBconfig und Konsole....82
2.4.3 Konfigurationsverwaltung über LANconfig....83
2.5 Alternative Boot-Konfiguration....84
2.5.1 Einleitung....84
2.5.2 Verwenden der Boot-Konfigurationen....85
2.5.3 Speichern und Hochladen der Boot-Konfigurationen....86
2.5.4 Löschen der Boot-Konfigurationen....87
2.5.5 Verwendung von Zertifikaten....87
2.6 FirmSafe....88
2.6.1 Einleitung....88
2.6.2 Konfiguration....88
2.6.3 Aktive Firmware über Konsolenbefehl umschalten....89
2.6.4 Asymmetrisches FirmSafe....89
2.7 Firmware über einen Client ins Gerät laden....89
2.7.1 Firmware-Upload über LANconfig....90
2.7.2 Firmware-Upload über WEBconfig....90
2.7.3 Firmware-Upload über Terminalprogramm....90
2.7.4 Firmware-Upload über Outband mit Rücksetzen der Konfiguration....91
2.8 LANCOM Auto Updater....92
2.8.1 Konfiguration des Auto Updaters....93
2.9 Dateien über TFTP, HTTP(S) oder SCP direkt in das/aus dem Gerät laden....95
2.9.1 Datei laden über einen TFTP-Client....95
2.9.2 Datei laden über einen SCP-Client....97
2.9.3 Datei-Download von einem TFTP- oder HTTP(S)-Server....99
2.10 Automatisches Laden von Firmware oder Konfiguration über USB....106

2.10.1 Automatisches Laden von Loader- und / oder Firmware-Dateien....106
2.10.2 Automatisches Laden von Konfigurations- und / oder Skript-Dateien....106
2.10.3 Konfiguration des automatischen Ladens via USB....107
2.11 Geräte-Reset durchführen....108
2.11.1 Konfiguration des Reset-Knopfes....108
2.12 Rechteverwaltung für verschiedene Administratoren....109
2.12.1 Die Rechte für die Administratoren....109
2.12.2 Konfigurieren des SNMP-Lesezugriffs....112
2.13 Geräteinterne SSH- / SSL-Schlüssel....113
2.13.1 Automatische Erzeugung gerätespezifischer SSH- / SSL-Schlüssel....113
2.13.2 Individuelle SSH-Schlüssel manuell erzeugen....114
2.14 SSH-Authentifizierung mit Hilfe eines Public-Keys....115
2.14.1 Ablauf der Zertifikatsprüfung beim SSH-Zugang....116
2.14.2 SSH-Schlüsselpaar erzeugen mit PuTTY....116
2.14.3 Syntax und Benutzer öffentlicher Schlüssel anpassen....118
2.14.4 Gerät für die Public-Key-Authentifizierung einrichten....118
2.14.5 Public-Key-Authentifizierung mit PuTTY....120
2.14.6 Public-Key-Authentifizierung mit LANconfig....121
2.15 SSH- und Telnet-Client im LCOS....122
2.15.1 Einleitung....122
2.15.2 Syntax des SSH-Clients....122
2.15.3 Syntax des Telnet-Clients....123
2.15.4 Öffentliche Schlüssel für die Authentifizierung....124
2.15.5 Schlüssel für den SSH-Client im LCOS erzeugen....125
2.15.6 Prioritäten für die SSH-Authentifizierung....126
2.15.7 Berechtigung zur Nutzung des SSH- / Telnet-Clients....126
2.16 Dateiimport auf der Konsole per Copy&Paste....126
2.17 Basic HTTP Fileserver für externe Speichermedien....129
2.17.1 Einleitung....129
2.17.2 Vorbereitung des USB-Speichermediums....129
2.17.3 Einhängepunkt des USB-Mediums im LCOS ermitteln....130
2.17.4 Zugriff auf die Dateien eines USB-Mediums....130
2.17.5 Regeln für den Verzeichniszugriff....130
2.17.6 Unterstützte Inhaltstypen....130
2.18 Rollout-Assistent....131
2.18.1 Default-Rollout-Assistent....131
2.18.2 Benutzerdefinierter Rollout-Assistent....132
2.18.3 Aktivierung des Rollout-Assistenten im WEBconfig....148
2.18.4 Konfiguration mit LANconfig....149
2.18.5 LSR-Informationen über DHCP-Server erhalten (Zero-Touch-Rollout)....150
2.19 TCP-Port-Tunnel....154
2.19.1 TCP- / HTTP-Tunnel konfigurieren....154
2.19.2 TCP- / HTTP-Tunnel per WEBconfig erzeugen....154
2.19.3 TCP- / HTTP-Tunnel per CLI erzeugen....156

2.19.4 TCP- / HTTP-Tunnel vorzeitig löschen....156
2.20 Die LANCOM High Availability Clustering Option....156
2.20.1 Konfigurations-Synchronisation einrichten....157
2.20.2 1-Klick WLC High Availability Clustering-Assistent....161
2.21 CPE WAN Management Protokoll (CWMP)....164
2.21.1 CWMP mit LANconfig einrichten....165
2.21.2 Gerätekonfiguration über CWMP....168
2.22 LANCOM Battery Pack....169
2.22.1 Konfiguration mit LANconfig....169
2.23 Benannte Loopback-Adressen einrichten....171
2.24 Konfigurationsmöglichkeit für IPv4/IPv6-Auflösung bei DNS-Auflösungen....172
2.25 Management-Ports für den Gerätezugriff anpassen....172
2.26 Ändern der SIM-Karten-PIN....173
3 LANtools....174
3.1 LANconfig – Geräte konfigurieren....174
3.1.1 LANconfig starten....175
3.1.2 Arbeiten mit LANconfig....177
3.1.3 Die Menüstruktur in LANconfig....209
3.1.4 Die Symbole der Symbolleiste....243
3.1.5 Das Kontextmenü in LANconfig....243
3.1.6 LANconfig Tastaturbefehle....243
3.1.7 LANconfig Kommandozeilen-Parameter....244
3.1.8 Anwendungskonzepte für LANconfig....246
3.1.9 Koppeln von Geräten mit der LANCOM Management Cloud....247
3.2 LANmonitor – Geräte im LAN überwachen....250
3.2.1 LANmonitor starten....251
3.2.2 QuickFinder im LANmonitor....251
3.2.3 Anzeige-Funktionen im LANmonitor....252
3.2.4 Die Menüstruktur im LANmonitor....252
3.2.5 Die Symbolleiste im LANmonitor....271
3.2.6 Das Kontextmenü im LANmonitor....272
3.2.7 LANmonitor Tastaturbefehle....272
3.2.8 Anwendungskonzepte für LANmonitor....272
3.3 WLANmonitor – WLAN-Geräte überwachen....276
3.3.1 WLANmonitor starten....278
3.3.2 QuickFinder im WLANmonitor....278
3.3.3 Rogue-Detection-Funktion....278
3.3.4 Die Menüstruktur im WLANmonitor....281
3.3.5 Die Symbolleiste im WLANmonitor....290
3.3.6 Das Kontextmenü im WLANmonitor....291
3.3.7 WLANmonitor Tastaturbefehle....291
3.3.8 Anwendungskonzepte für den WLANmonitor....291
3.4 LANtracer – Tracen mit LANconfig und LANmonitor....292
3.4.1 LANtracer starten....293

3.4.2 Arbeiten mit LANtracer....293
3.4.3 Die Menüstruktur im LANtracer....302
3.4.4 Die Symbolleiste im LANtracer....306
3.4.5 Das Kontextmenü in LANtracer....307
3.4.6 LANtracer Tastaturbefehle....307
4 Diagnose....308
4.1 Trace-Ausgaben....308
4.1.1 So starten Sie einen Trace....308
4.1.2 Übersicht der Schlüssel....308
4.1.3 Übersicht der Parameter im trace-Befehl....308
4.1.4 Kombinationsbefehle....313
4.1.5 Filter für Traces....313
4.1.6 Beispiele für die Traces....313
4.1.7 Traces aufzeichnen....314
4.1.8 Tracen auf ein angeschlossenes USB-Laufwerk....314
4.2 Tracen mit dem LANmonitor....315
4.3 Datenpakete aufzeichnen und analysieren....315
4.3.1 Capture-Daten via Paket-Capturing erstellen....316
4.3.2 Capture-Daten via LCOSCAP erstellen....317
4.3.3 Capture Daten via RPCap erstellen....318
4.3.4 Capture-Daten auf ein USB-Laufwerk ausgeben....322
4.4 Das SYSLOG-Modul....323
4.4.1 Aufbau der SYSLOG-Nachrichten....324
4.4.2 SYSLOG konfigurieren....325
4.4.3 Bedeutung von SYSLOG-Meldungen....332
4.5 Übersicht der Parameter im ping-Befehl....335
4.6 Monitor-Modus am Switch....338
4.7 Kabel-Test....338
4.8 Mittelwert der CPU-Lastanzeige....339
4.8.1 Einleitung....339
4.8.2 Konfiguration....339
4.9 Versand von Anhängen mit dem mailto-Kommando....340
4.10 Erweiterung der Sysinfo....341
4.10.1 Ausgabe zusätzlicher Ports im SYSINFO an der Konsole....342
4.10.2 Ausgabe des Konfigurations-Datums....342
4.10.3 Ausgabe des Konfigurations-Hashs....343
4.10.4 Ausgabe der Konfigurations-Version....343
4.11 Bandbreiten-Messung mit iPerf....344
4.11.1 iPerf mit LANconfig einrichten....345
4.11.2 Temporärer iPerf-Server und -Client....346
4.11.3 iPerf-Ergebnisse mit LANmonitor auswerten....346
4.12 SLA-Monitoring....347
4.12.1 Konfiguration von SLA-Monitoring über LANconfig....347
4.12.2 Anzeigen der SLA-Monitoring Ergebnisse in LANmonitor....349

4.13 Layer-7-Anwendungserkennung....350
4.13.1 IPv4- / IPv6-Traffic-Accounting....353
5 Sicherheit....355
5.1 Schutz für die Konfiguration....355
5.1.1 Passwortschutz....355
5.1.2 Weitere Administratoren mit eingeschränkten Rechten....357
5.1.3 Die Login-Sperre....357
5.1.4 Einschränkung der Zugriffsrechte auf die Konfiguration....358
5.1.5 Management-Protokolle....359
5.1.6 Abschalten von Ethernet-Schnittstellen....361
5.2 Standortverifikation über GPS....362
5.2.1 GPS-Standortverifikation....362
5.2.2 Konfiguration der Standortverifikation....362
5.3 Speicherung von Passwort-Formularfeldern im Browser verhindern....364
5.4 Die Sicherheits-Checkliste....364
6 Routing und WAN-Verbindungen....368
6.1 Allgemeines über WAN-Verbindungen....368
6.1.1 Brücken für Standard-Protokolle....368
6.1.2 Was passiert bei einer Anfrage aus dem LAN?....368
6.2 IP-Routing....369
6.2.1 Informationen zum Routingverhalten....369
6.2.2 Routing-Optionen....376
6.2.3 Präfix-Listen....378
6.2.4 Die Routing-Tabelle....379
6.2.5 Policy-based Routing....385
6.2.6 Dynamisches Routing mit IP-RIP....387
6.2.7 WAN-RIP....391
6.2.8 SYN/ACK-Speedup....393
6.3 Advanced Routing and Forwarding (ARF)....393
6.3.1 Einleitung....393
6.3.2 Definition von Netzwerken und Zuordnung von Interfaces....396
6.3.3 Zuweisung von logischen Interfaces zu Bridge-Gruppen....397
6.3.4 Protokolle filtern....398
6.3.5 Schnittstellen-Tags für Gegenstellen....402
6.3.6 Ermittlung des Routing-Tags für lokale Routen....403
6.3.7 Routing-Tags für DNS-Weiterleitung....403
6.3.8 Virtuelle Router....406
6.4 Die Konfiguration von Gegenstellen....407
6.4.1 Gegenstellenliste....408
6.4.2 Layer-Liste....413
6.5 Generic Routing Encapsulation (GRE)....415
6.5.1 Grundlagen zum Generic Routing Encapsulation Protokoll (GRE)....415
6.5.2 Ethernet-over-GRE (EoGRE)....417
6.6 IP-Masquerading....419

6.6.1 Einfaches Masquerading....419
6.6.2 Port-Forwarding (Inverses Masquerading)....421
6.7 Demilitarisierte Zone (DMZ)....423
6.7.1 Zuordnung der Netzwerkzonen zur DMZ....423
6.7.2 Adressprüfung bei DMZ- und Intranet-Interfaces....423
6.7.3 Unmaskierter Internet-Zugang für Server in der DMZ....424
6.8 Multi-PPPoE....425
6.8.1 Anwendungsbeispiel: Home-Office mit privatem Internetzugang....425
6.8.2 Konfiguration....425
6.9 Load-Balancing....426
6.9.1 DSL-Port-Mapping....427
6.9.2 Dynamisches Load-Balancing....429
6.9.3 Statisches Load-Balancing....434
6.9.4 Indirekte Bündelung für LAN-LAN-Kopplungen über PPTP....435
6.9.5 Konfiguration des Load-Balancing....435
6.10 SD-WAN Dynamic Path Selection....440
6.10.1 Konfiguration der Dynamic Path Selection....441
6.10.2 Show Kommandos....448
6.10.3 Beispielkonfigurationen....448
6.11 N:N-Mapping....450
6.11.1 Anwendungsbeispiele....451
6.11.2 Konfiguration....453
6.12 Verbindungsaufbau mit PPP....455
6.12.1 Das Protokoll....455
6.12.2 Alles o.k.? Leitungsüberprüfung mit LCP....456
6.12.3 Zuweisung von IP-Adressen über PPP....457
6.12.4 Einstellungen in der PPP-Liste....458
6.12.5 Die Bedeutung der DEFAULT-Gegenstelle....461
6.12.6 RADIUS-Authentifizierung von PPP-Verbindungen....461
6.12.7 32 zusätzliche Gateways für PPTP-Verbindungen....461
6.13 DSL-Verbindungsaufbau mit PPTP....463
6.13.1 Konfiguration von PPTP....463
6.14 Dauerverbindung für Flatrates – Keep-alive....464
6.14.1 Konfiguration des Keep-alive-Verfahrens....464
6.15 Datenvolumen auf der WAN-Schnittstelle....464
6.15.1 Konfiguration von Datenvolumen-Budgets....465
6.15.2 Budget-Auswertung....467
6.16 Manuelle Definition der MTU....468
6.16.1 Konfiguration....468
6.16.2 Statistik....469
6.17 Das Rapid-Spanning-Tree-Protokoll....469
6.17.1 Classic und Rapid Spanning Tree....469
6.17.2 Verbesserungen durch Rapid Spanning Tree....470
6.17.3 Konfiguration des Spanning-Tree-Protokolls....470

6.17.4 Statusmeldungen über das Spanning-Tree-Protokoll....472
6.18 Die Aktions-Tabelle....474
6.18.1 Einleitung....474
6.18.2 Aktionen für Dynamic DNS....474
6.18.3 Weitere Beispiele für Aktionen....477
6.18.4 Konfiguration....479
6.19 Verwendung der seriellen Schnittstelle im LAN....483
6.19.1 Einleitung....483
6.19.2 Betriebsarten....483
6.19.3 Konfiguration der seriellen Schnittstellen....484
6.19.4 Konfiguration des COM-Port-Servers....484
6.19.5 Konfiguration der WAN-Geräte....489
6.19.6 Status-Informationen über die seriellen Verbindungen....489
6.19.7 COM-Port-Adapter....492
6.20 IGMP- / MLD-Snooping....492
6.20.1 Einleitung....492
6.20.2 Ablauf des IGMP- / MLD-Snooping....494
6.20.3 IGMP- / MLD-Snooping über mehrere Bridges hinweg....494
6.20.4 Konfiguration....496
6.20.5 IGMP- / MLD-Status....501
6.21 Konfiguration des WWAN-Zugriffs....503
6.22 Umschalten zwischen Mobilfunk-Profilen oder SIM-Karten....509
6.23 BGPv4....509
6.23.1 Border Gateway Protokoll Version 4 (BGPv4)....509
6.23.2 Algorithmus für die Auswahl des besten Pfades....534
6.23.3 Tutorial: Einrichtung von BGPv4 unter LANconfig....535
6.23.4 Tutorial: Präferenz von Präfixen einrichten....540
6.23.5 Tutorial: Community-Attribut setzen....542
6.23.6 Tutorial: Empfangene Präfixe filtern....544
6.24 OSPF....546
6.24.1 OSPF mit LANconfig konfigurieren....547
6.24.2 Show-Commands über CLI....558
6.25 Bidirectional Forwarding Detection (BFD)....559
6.25.1 Profile....559
6.25.2 Key-Chains....561
6.25.3 Show-Kommandos über CLI....561
6.26 BGP RPKI-RTR....561
6.26.1 RPKI konfigurieren....562
6.26.2 Show-Kommandos über CLI....563
6.27 Locator / ID Separation Protocol (LISP)....564
6.27.1 Konfiguration....565
6.27.2 LISP-Tutorial....571
6.28 Route-Monitor....575
6.28.1 Route-Monitor mit LANconfig konfigurieren....575

6.29 DSLoL für WLAN-Router....576
7 IPv6....577
7.1 IPv6-Grundlagen....577
7.1.1 Warum IP-Adressen nach dem Standard IPv6?....577
7.1.2 Aufbau einer IP-Adresse nach IPv6-Standard....577
7.1.3 Migrationsstufen....578
7.2 Grundeinstellungen....578
7.2.1 LAN-Schnittstellen....579
7.2.2 WAN-Profile....581
7.2.3 RAS-Vorlagen....583
7.2.4 IPv6-Adressen....585
7.2.5 IPv6-Parameter....586
7.2.6 Loopback-Adressen....587
7.2.7 Einrichtung eines IPv6-Internetzugangs....587
7.3 Router-Advertisement....596
7.3.1 Schnittstellen-Optionen....597
7.3.2 Präfix-Liste....598
7.3.3 Präfix-Pools....599
7.3.4 DNS-Optionen....600
7.3.5 Routen-Optionen....601
7.3.6 PREF64-Optionen....601
7.3.7 Router-Advertisement-Snooping....602
7.4 DHCPv6....603
7.4.1 DHCPv6-Server....604
7.4.2 DHCPv6-Client....611
7.4.3 DHCPv6-Relay-Agent....614
7.4.4 Lightweight-DHCPv6-Relay-Agent (LDRA)....615
7.5 IPv6-Firewall....617
7.5.1 Funktion....617
7.5.2 Konfiguration....617
7.5.3 IPv6-Firewall-Log-Tabelle....633
7.6 IPv6-Tunneltechnologien....634
7.6.1 6to4-Tunnel....634
7.6.2 6in4-Tunnel....635
7.6.3 6rd-Tunnel....636
7.6.4 Dual-Stack Lite (DS-Lite)....636
7.6.5 464XLAT....637
7.6.6 Tunnel einrichten....638
8 Firewall....648
8.1 Gefährdungsanalyse....648
8.1.1 Die Gefahren....648
8.1.2 Die Wege der Täter....648
8.1.3 Die Methoden....649
8.1.4 Die Opfer....649

8.2 Was ist eine Firewall?....650
8.2.1 Die Aufgaben einer Firewall....650
8.2.2 Unterschiedliche Typen von Firewalls....651
8.3 Die Firewall im Gerät....654
8.3.1 So prüft die Firewall im Gerät die Datenpakete....655
8.3.2 Besondere Protokolle....657
8.3.3 Allgemeine Einstellungen der Firewall....658
8.3.4 Die Parameter der Firewall-Regeln....664
8.3.5 Die Alarmierungsfunktionen der Firewall....668
8.3.6 Strategien für die Einstellung der Firewall....671
8.3.7 Tipps zur Einstellung der Firewall....673
8.4 Konfiguration der Firewall mit LANconfig....674
8.4.1 Definition der Firewall-Objekte....675
8.4.2 Definition der Firewall-Regeln....677
8.5 Konfiguration der Firewall-Regeln über die Konsole....679
8.5.1 Regel-Tabelle....679
8.5.2 Objekttabelle....680
8.5.3 Aktionstabelle....680
8.6 Firewall-Diagnose....680
8.6.1 Die Firewall-Tabelle....681
8.7 Grenzen der Firewall....686
8.8 Abwehr von Einbruchsversuchen: Intrusion Detection....686
8.8.1 Beispiele für Einbruchsversuche....686
8.8.2 Konfiguration des IDS....687
8.9 Schutz vor „Denial-of-Service“-Angriffen....687
8.9.1 Erhöhter DoS-Schwellenwert für Zentralgeräte....688
8.9.2 Beispiele für Denial-of-Service-Angriffe....689
8.9.3 Konfiguration der DoS-Abwehr....690
8.9.4 Konfiguration von ping-Blocking und Stealth-Modus....691
8.10 WAN Policy-Based NAT....691
8.10.1 Konfiguration eines Policy-basierten NATs mit Firewall-Regeln....692
9 Quality-of-Service....696
9.1 Wozu QoS?....696
9.2 Welche Datenpakete bevorzugen?....696
9.2.1 Was ist DiffServ?....697
9.2.2 Garantierte Mindestbandbreiten....697
9.2.3 Limitierte Maximalbandbreiten....698
9.3 Das Warteschlangenkonzept....699
9.3.1 Sendeseitige Warteschlangen....699
9.3.2 Empfangsseitige Warteschlangen....700
9.4 Reduzierung der Paketlänge....701
9.5 QoS-Parameter für Voice-over-IP-Anwendungen....702
9.6 QoS in Sende- oder Empfangsrichtung....706
9.7 QoS-Konfiguration....707

9.7.1 ToS- und DiffServ-Felder auswerten....707
9.7.2 Minimal- und Maximalbandbreiten definieren....709
9.7.3 Übertragungsraten für Schnittstellen festlegen....710
9.7.4 Sende- und Empfangsrichtung....714
9.7.5 Reduzierung der Paketlänge....714
9.8 Quality-of-Service (QoS) mit 8 Queues....715
9.8.1 Queues....716
9.8.2 Queue-Listen....718
9.8.3 Schnittstellen....719
9.8.4 Paketstau-Aktion....719
9.8.5 Beispiel 1: Konfiguration eines QoS-Konzepts mit vier Klassen....720
9.8.6 Beispiel 2: Konfiguration eines QoS-Konzepts am VDSL-Anschluss mit zwei QoS-Klassen....723
9.8.7 Queue-Nutzung in der Firewall....725
9.9 QoS für WLANs nach IEEE 802.11e (WMM/WME)....728
10 Multicast Routing....730
10.1 Allgemeine Multicast Show-Kommandos....731
10.2 Allgemeine Einstellungen....731
10.2.1 IPv4-Filter-Listen....731
10.2.2 IPv6-Filter-Listen....732
10.3 IGMP (Internet Group Management Protocol)....733
10.3.1 IGMP-Parameter....733
10.3.2 SSM-Bereich....734
10.3.3 IGMP-Proxy....734
10.3.4 Statisches IPv4-Multicast Routing....735
10.3.5 SSM-Quell-IP-Liste....736
10.3.6 Tutorial: IGMP-Proxy einrichten....737
10.4 MLD (Multicast Listener Discovery)....738
10.4.1 MLD-Parameter....738
10.4.2 SSM-Bereich....739
10.4.3 MLD-Proxy....740
10.4.4 Statisches IPv6-Multicast Routing....740
10.4.5 SSM-Quell-IP-Liste....741
10.5 PIM (Protocol Independent Multicast)....742
10.5.1 Schnittstellen....744
10.5.2 IPv4-RP-Liste....745
10.5.3 IPv4-SSM-Liste....746
10.5.4 IPv4-SSM-Mapping....746
10.5.5 IPv6-RP-Liste....747
10.5.6 IPv6-SSM-Liste....748
10.5.7 IPv6-SSM-Mapping....748
10.6 Weitere Multicast-Protokolle....749
10.6.1 Bonjour-Proxy....749
11 Virtual Private Networks – VPN....754

11.1 Welchen Nutzen bietet VPN?....754
11.1.1 Herkömmliche Netzwerkstruktur....754
11.1.2 Vernetzung über Internet....755
11.1.3 Private IP-Adressen im Internet?....755
11.1.4 Sicherheit des Datenverkehrs im Internet?....756
11.2 Das VPN-Modul im Überblick....757
11.2.1 VPN-Anwendungsbeispiel....757
11.2.2 Funktionen des VPN-Moduls....758
11.3 VPN-Verbindungen im Detail....758
11.3.1 LAN-LAN-Kopplung....759
11.3.2 Einwahlzugänge (Remote Access Service)....759
11.4 Was ist LANCOM Dynamic VPN?....760
11.4.1 Ein Blick auf die IP-Adressierung....760
11.4.2 So funktioniert LANCOM Dynamic VPN....761
11.5 Konfiguration von VPN-Verbindungen....762
11.5.1 VPN-Tunnel: Verbindungen zwischen den VPN-Gateways....763
11.5.2 VPN-Verbindungen einrichten mit den Setup-Assistenten....763
11.5.3 1-Click-VPN für Netzwerke (Site-to-Site)....764
11.5.4 1-Click-VPN für LANCOM Advanced VPN Client....766
11.5.5 VPN-Regeln einsehen....767
11.5.6 Manuelles Einrichten der VPN-Verbindungen....767
11.5.7 IKE Config Mode....768
11.5.8 Diagnose der VPN-Verbindungen....769
11.6 Einsatz von digitalen Zertifikaten....770
11.6.1 Grundlagen....770
11.6.2 Vorteile von Zertifikaten....773
11.6.3 Aufbau von Zertifikaten....774
11.6.4 Sicherheit....775
11.6.5 Zertifikate beim VPN-Verbindungsaufbau....776
11.6.6 Zertifikate von Zertifikatsdiensteanbietern....777
11.6.7 Aufbau einer eigenen CA....777
11.6.8 Anfordern eines Zertifikates mit der Stand-alone Windows CA....778
11.6.9 Zertifikat in eine PKCS#12-Datei exportieren....779
11.6.10 Zertifikate mit OpenSSL erstellen....782
11.6.11 Zertifikate in das Gerät laden....784
11.6.12 Zertifikate sichern und hochladen mit LANconfig....785
11.6.13 Erweiterte Zertifkats-Unterstützung....786
11.6.14 VPN-Verbindungen auf Zertifikatsunterstützung einstellen....788
11.6.15 Zertifikatsbasierte VPN-Verbindungen mit dem Setup-Assistenten erstellen....791
11.6.16 LANCOM Advanced VPN Client auf Zertifikatsverbindungen einstellen....794
11.6.17 Vereinfachte Einwahl mit Zertifikaten....796
11.6.18 Vereinfachte Netzwerkanbindung mit Zertifikaten – Proadaptives VPN....797
11.6.19 Anfrage von Zertifikaten mittels CERTREQ....797

11.6.20 Certificate Revocation List – CRL....798
11.6.21 Wildcard Matching von Zertifikaten....799
11.6.22 Diagnose der VPN-Zertifikatsverbindungen....800
11.6.23 OCSP Client zur Zertifikatsüberprüfung....800
11.7 Mehrstufige Zertifikate für SSL/TLS....801
11.7.1 Einleitung....801
11.7.2 SSL / TLS mit mehrstufigen Zertifikaten....802
11.7.3 VPN mit mehrstufigen Zertifikaten....802
11.8 Zertifikatsenrollment über SCEP....802
11.8.1 SCEP-Server und SCEP-Client....803
11.8.2 Der Ablauf einer Zertifikatsverteilung....803
11.8.3 Konfiguration von SCEP....804
11.8.4 Verwendung digitaler Zertifikate (Smart Certificate)....810
11.9 NAT Traversal (NAT-T)....823
11.10 Extended Authentication Protocol (XAUTH)....825
11.10.1 Einleitung....825
11.10.2 XAUTH in der Firmware....825
11.10.3 Konfiguration von XAUTH....826
11.10.4 XAUTH mit externem RADIUS-Server....827
11.11 Backup über alternative VPN-Verbindung....828
11.11.1 Einleitung....828
11.11.2 Backup-fähige Netzstruktur....830
11.11.3 Konfiguration des VPN-Backups....832
11.12 Automatischer Konfigurationsabgleich (Config-Sync) mit der LANCOM VPN High Availability Clustering XL Option....834
11.13 IPSec over HTTPS....835
11.13.1 Einleitung....835
11.13.2 Konfiguration der IPSec over HTTPS-Technologie....835
11.13.3 Statusanzeigen der IPSec-over-HTTPS-Technologie....837
11.14 MPPE für PPTP-Tunnel....837
11.15 Layer 2 Tunneling Protocol (L2TP)....838
11.15.1 Konfiguration der L2TP-Tunnel....839
11.15.2 Authentifizierung über RADIUS....843
11.15.3 Betrieb als L2TP Access Concentrator (LAC)....845
11.15.4 Betrieb als L2TP Network Server (LNS) mit Authentifizierung über RADIUS....847
11.15.5 Betrieb als L2TP Network Server (LNS) für RAS-Clients....849
11.15.6 Konfiguration eines WLAN-Szenarios mit zentraler Auskopplung der Nutzdaten....851
11.16 VPN-Verbindungen: hohe Verfügbarkeit mit „Lastenausgleich“....854
11.16.1 Mehrere VPN-Gateway-Adressen....854
11.16.2 Gruppierung und Priorisierung von alternativen Gateways....855
11.17 Wie funktioniert VPN?....860
11.17.1 IPSec – Die Basis für VPN....860

11.17.2 Alternativen zu IPSec....861
11.18 Die Standards hinter IPSec....862
11.18.1 Module von IPSec und ihre Aufgaben....862
11.18.2 Security Associations – nummerierte Tunnel....862
11.18.3 Verschlüsselung der Pakete – das ESP-Protokoll....862
11.18.4 Management der Schlüssel – IKE....863
11.18.5 Replay-Detection....864
11.19 IKEv2....864
11.19.1 IKEv2 mit LANconfig konfigurieren....865
11.19.2 Zwei-Faktor-Authentifizierung im VPN....909
11.19.3 RADIUS-Unterstützung für IKEv2....912
11.19.4 Tutorial: Einrichtung von IKEv2 unter LANconfig....919
11.19.5 Tutorial: Einrichtung einer zertifikatsbasierten IKEv2-VPN-Verbindung (RSA)....923
11.19.6 Tutorial: Einrichtung einer zertifikatsbasierten IKEv2-VPN-Verbindung (Digital Signature)....930
11.19.7 Tutorial – EAP-Client gegen einen EAP-Server....937
11.20 Anwendungskonzepte für LANconfig....939
11.20.1 1-Click-VPN für Netzwerke (Site-to-Site)....939
11.20.2 1-Click-VPN für Advanced VPN Client....940
12 Virtuelle LANs (VLANs)....941
12.1 Was ist ein Virtuelles LAN?....941
12.2 So funktioniert ein VLAN....941
12.2.1 Frame-Tagging....942
12.2.2 Umsetzung in den Schnittstellen des LANs....943
12.2.3 Anwendungsbeispiele....943
12.3 Konfiguration von VLANs....945
12.3.1 Allgemeine Einstellungen....946
12.3.2 Die Netzwerktabelle....948
12.3.3 Die Porttabelle....948
12.4 Konfigurierbare VLAN-IDs....949
12.4.1 VLAN-IDs für WLAN-Clients....949
12.4.2 VLAN-IDs für DSL-Interfaces....950
12.4.3 VLAN-IDs für DSLoL-Interfaces....951
12.5 VLAN-Tags auf Layer 2/3 im Ethernet....951
12.5.1 Einleitung....951
12.5.2 Konfiguration des VLAN-Taggings auf Layer 2 / 3....952
13 Wireless LAN – WLAN....953
13.1 Einleitung....953
13.2 Anwendungsszenarien....953
13.2.1 Infrastruktur-Modus....954
13.2.2 Hotspot oder Gastzugang....954
13.2.3 Managed-Modus....955
13.2.4 WLAN-Bridge (Point-to-Point)....955

13.2.5 WLAN-Bridge im Relais-Betrieb....956
13.2.6 WLAN-Bridge zum AP – managed und unmanaged gemischt....956
13.2.7 Wireless Distribution System (Point-to-Multipoint)....957
13.2.8 Client-Modus....957
13.2.9 Client-Modus bei bewegten Objekten im Industriebereich....958
13.3 WLAN-Standards....958
13.4 WLAN-Sicherheit....959
13.4.1 Grundbegriffe....959
13.4.2 WPA3 (Wi-Fi Protected Access 3)....960
13.4.3 IEEE 802.11i / WPA2....962
13.4.4 TKIP und WPA....966
13.4.5 WEP....967
13.4.6 LANCOM Enhanced Passphrase Security (LEPS)....967
13.4.7 Background WLAN Scanning....971
13.4.8 Umgebungsscan zu einer konfigurierbaren Zeit starten....972
13.4.9 Erkennung von Replay-Attacken....973
13.4.10 WLAN Protected Management Frames (PMF)....973
13.5 LANCOM Active Radio Control (ARC)....976
13.5.1 Adaptive RF Optimization....978
13.5.2 Airtime Fairness....980
13.5.3 WLAN Band Steering....982
13.5.4 Client Management....983
13.5.5 Adaptive Noise Immunity zur Abschwächung von Interferenzen im WLAN....987
13.5.6 Spectral Scan....988
13.6 Dynamic Frequency Selection (DFS)....993
13.6.1 DFS-Konfiguration....995
13.7 APSD – Automatic Power Save Delivery....996
13.7.1 Einleitung....996
13.7.2 Konfiguration....997
13.7.3 Statistik....997
13.8 WLAN-Routing (Isolierter Modus)....997
13.9 Übernahme der User-Priorität von IEEE 802.11e in VLAN-Tags....998
13.10 Aufbau von Punkt-zu-Punkt-Verbindungen....999
13.10.1 Konfiguration der Punkt-zu-Punkt-Verbindungen....999
13.10.2 Einrichten von Punkt-zu-Punkt-Verbindungen mit dem LANmonitor....999
13.10.3 Geometrische Auslegung von Outdoor-Funknetz-Strecken....1001
13.10.4 Ausrichten der Antennen für den P2P-Betrieb....1003
13.10.5 Vermessung von Funkstrecken....1005
13.10.6 Punkt-zu-Punkt-Betriebsart aktivieren....1005
13.10.7 Konfiguration von P2P-Verbindungen....1006
13.10.8 LEPS-MAC für P2P-Verbindungen....1008
13.10.9 Access Points im Relais-Betrieb....1009
13.11 BFWA – mehr Sendeleistung für mehr Reichweite....1009

13.12 Adaptive Transmission Power....1010
13.13 Opportunistic Key Caching (OKC)....1010
13.13.1 Verschlüsseltes OKC über IAPP....1011
13.14 Fast Roaming....1012
13.14.1 Fast Roaming über IAPP....1013
13.15 Bandbreitenbegrenzung im WLAN....1013
13.15.1 Einstellung als Access Point....1014
13.15.2 Einstellung als Client....1014
13.15.3 Bandbreitenbeschränkung der LAN-Schnittstellen....1015
13.16 Automatische Anpassung der Übertragungsrate für Multicast- und Broadcast-Sendungen....1016
13.17 LANCOM "Wireless Quality Indicators" (WQI)....1016
13.18 Konfiguration der WLAN-Parameter....1017
13.18.1 Allgemeine WLAN-Einstellungen....1017
13.18.2 Die physikalischen WLAN-Schnittstellen....1018
13.18.3 Die logischen WLAN-Schnittstellen....1029
13.18.4 Punkt-zu-Punkt....1045
13.18.5 Die Punkt-zu-Punkt-Partner....1046
13.18.6 Experten-WLAN-Einstellugnen....1047
13.18.7 Konfigurierbare Datenraten je WLAN-Modul....1053
13.18.8 RTLS (Real-Time Location System)....1055
13.18.9 IEEE 802.11k-Roaming-Ziele....1057
13.18.10 WLAN-Data-Trace....1058
13.18.11 Client Management....1060
13.18.12 WLAN-Sicherheit....1064
13.18.13 Auswahl der im WLAN zulässigen Stationen....1072
13.18.14 Verschlüsselungs-Einstellungen....1078
13.18.15 IEEE 802.1X / EAP....1081
13.18.16 IEEE 802.11u und Hotspot 2.0....1085
13.18.17 Statischer WLAN-Controller....1103
13.18.18 AutoWDS....1105
13.18.19 Erweiterte WLAN-Parameter....1105
13.18.20 Location Based Services (LBS)....1108
13.19 Konfiguration des Client-Modus....1113
13.19.1 Client-Modus mit LANconfig aktivieren....1114
13.19.2 Client-Einstellungen....1114
13.19.3 Radio-Einstellungen....1115
13.19.4 SSID des verfügbaren Netzwerks einstellen....1116
13.19.5 Verschlüsselungseinstellungen....1116
13.19.6 PMK-Caching im WLAN-Client-Modus....1117
13.19.7 Prä-Authentifizierung im WLAN-Client-Modus....1118
13.19.8 Mehrere WLAN-Profile im Client-Modus....1118
13.19.9 Roaming....1119
14 WLAN-Management....1122

14.1 Ausgangslage....1122
14.2 Technische Konzepte....1122
14.2.1 WLC-Funktionen im LANCOM vRouter....1122
14.2.2 Der CAPWAP-Standard....1123
14.2.3 Die Smart-Controller-Technologie....1123
14.2.4 Kommunikation zwischen Access Point und WLAN-Controller....1125
14.2.5 Zero-Touch-Management....1127
14.2.6 Split-Management....1127
14.2.7 Schutz vor unberechtigtem CAPWAP-Zugriff aus dem WAN....1127
14.3 Grundkonfiguration der WLAN-Controller-Funktion....1128
14.3.1 Zeitinformation für den WLAN-Controller einstellen....1128
14.3.2 Beispiel einer Default-Konfiguration....1128
14.3.3 Zuweisung der Default-Konfiguration zu den neuen Access Points....1132
14.3.4 Konfiguration der Access Points....1133
14.4 Konfiguration....1134
14.4.1 Allgemeine Einstellungen....1134
14.4.2 Profile....1134
14.4.3 Access Point Konfiguration....1153
14.4.4 IP-abhängige Autokonfiguration und Tagging von APs....1190
14.5 Access Point Verwaltung....1192
14.5.1 Neue Access Points manuell in die WLAN-Struktur aufnehmen....1192
14.5.2 Access Points manuell aus der WLAN-Struktur entfernen....1195
14.5.3 Access Point deaktivieren oder dauerhaft aus der WLAN-Struktur entfernen....1195
14.6 AutoWDS – Kabellose Integration von APs über P2P-Verbindungen....1196
14.6.1 Hinweise zur Nutzung von AutoWDS....1198
14.6.2 Funktionsweise....1200
14.6.3 Einrichtung mittels vorkonfigurierter Integration....1207
14.6.4 Vorkonfigurierte Integration durch Pairing beschleunigen....1209
14.6.5 Einrichtung mittels Express-Integration....1209
14.6.6 Umschalten von Express- zu vorkonfigurierter Integration....1211
14.6.7 Manuelles Topologie-Mangement....1211
14.6.8 Redundante Strecken mittels RSTP....1214
14.7 Zentrales Firmware- und Skript-Management....1215
14.7.1 Allgemeine Einstellungen für das Firmware-Management....1216
14.8 RADIUS....1219
14.8.1 Prüfung der WLAN-Clients über RADIUS (MAC-Filter)....1220
14.8.2 Externer RADIUS-Server....1221
14.8.3 Dynamische VLAN-Zuweisung....1223
14.8.4 RADIUS-Accounting im WLAN-Controller für logische WLANs aktivieren....1224
14.9 Anzeigen und Aktionen im LANmonitor....1226
14.10 Funkfeldoptimierung....1227
14.10.1 Gruppenbezogene Funkfeldoptimierung....1228
14.11 Client Steering über den WLC....1230

14.11.1 Konfiguration....1231
14.12 Kanallastanzeige im WLC-Betrieb....1234
14.13 Sicherung der Zertifikate....1234
14.13.1 Backup der Zertifikate anlegen....1234
14.13.2 Zertifikats-Backup in das Gerät einspielen....1235
14.13.3 Sichern und Wiederherstellen weiterer Dateien der SCEP-CA....1236
14.13.4 One Click Backup der SCEP-CA....1237
14.13.5 Backup und Einspielen der Zertifikate über LANconfig....1238
14.14 Backuplösungen....1239
14.14.1 WLC-Cluster....1239
14.14.2 Backup mit redundanten WLAN-Controllern....1243
14.14.3 Backup mit primären und sekundären WLAN-Controllern....1245
14.14.4 Primäre und sekundäre Controller....1245
14.14.5 Automatische Suche nach alternativen WLCs....1246
14.14.6 One Click Backup der SCEP-CA....1246
14.15 Automatischer Konfigurationsabgleich (Config-Sync) mit der LANCOM WLC High Availability Clustering XL Option....1247
14.15.1 Spezielles LANconfig-Icon für Cluster-Geräte oder mit Config-Sync....1248
14.15.2 Spezielles LANmonitor-Icon für Cluster-Geräte oder mit Config-Sync....1250
15 Public Spot....1251
15.1 Einführung....1251
15.1.1 Was ist ein "Public Spot"?....1251
15.1.2 Anwendungsszenarien....1252
15.1.3 Das Public Spot-Modul im Überblick....1259
15.2 Einrichtung und Betrieb....1262
15.2.1 Grundkonfiguration....1262
15.2.2 Sicherheitseinstellungen....1287
15.2.3 Erweiterte Funktionen und Einstellungen....1288
15.2.4 Alternative Anmeldeformen....1311
15.2.5 Geräteeigene und individuelle Voucher- und Authentifizierungsseiten (Templates)....1346
15.2.6 Public Spot-Clients anzeigen....1368
15.2.7 Public Spot-Benutzern Werbung einblenden....1369
15.3 Zugriff auf den Public Spot....1370
15.3.1 Voraussetzungen für die Anmeldung....1370
15.3.2 Anmelden am Public Spot....1371
15.3.3 Informationen zur Sitzung....1372
15.3.4 Abmelden vom Public Spot....1372
15.3.5 Rat und Hilfe....1372
15.4 Tutorials zur Einrichtung und Verwendung des Public Spots....1374
15.4.1 Virtualisierung und Gastzugang über WLAN Controller mit VLAN....1374
15.4.2 Virtualisierung und Gastzugang über WLAN Controller ohne VLAN....1384
15.4.3 Einrichtung eines sicheren Hotspots mit Enhanced Open....1398
15.4.4 Einrichtung eines externen RADIUS-Servers für die Benutzerverwaltung..1399

15.4.5 Interner und externer RADIUS-Server kombiniert....1401
15.4.6 Prüfung von WLAN-Clients über RADIUS (MAC-Filter)....1405
15.4.7 Einrichtung eines externen SYSLOG-Servers....1406
15.5 XML-Interface....1407
15.5.1 Funktion....1408
15.5.2 Einrichtung des XML-Interfaces....1409
15.5.3 Analyse des XML-Interfaces mit cURL....1411
15.5.4 Befehle....1411
15.6 Anhang....1418
15.6.1 Allgemein übermittelte RADIUS-Attribute....1418
15.6.2 Durch WISPr übermittelte RADIUS-Attribute....1423
16 Voice over IP – VoIP....1424
16.1 Einleitung....1424
16.2 VoIP-Implementation im LANCOM VoIP Router....1425
16.2.1 Anwendungsbeispiele....1425
16.2.2 Die zentrale Position der LANCOM VoIP Router....1428
16.3 Die Gesprächsvermittlung: Call-Routing....1430
16.3.1 SIP-Proxy und SIP-Gateway....1431
16.3.2 Die Anmeldung von Benutzern am SIP-Proxy....1431
16.3.3 Rufnummernumsetzung an Netz-Übergängen....1434
16.3.4 Der Call-Manager....1434
16.3.5 Telefonieren mit dem LANCOM VoIP Router....1435
16.3.6 Halten, Makeln, Verbinden....1437
16.3.7 Übertragung von DTMF-Tönen....1438
16.4 Konfiguration der VoIP-Parameter....1440
16.4.1 Allgemeine Einstellungen....1440
16.4.2 Konfiguration der Leitungen....1441
16.4.3 Konfiguration der Benutzer....1461
16.5 Konfiguration des Call-Managers....1473
16.5.1 Ablauf des Call-Routings....1473
16.5.2 Behandlung der Calling Party ID....1474
16.5.3 Die Parameter der Call-Routing-Tabelle....1476
16.5.4 Parallelruf im ISDN signalisieren....1481
16.5.5 Erweiterte Einstellungen....1482
16.6 Telefoniefunktionen für LANCOM VoIP Router (PBX-Funktionen)....1484
16.6.1 Anrufweiterschaltung (Verbinden und Rufumleitung)....1484
16.6.2 Spontane Anrufsteuerung durch den Benutzer....1488
16.6.3 Feste Anrufweiterschaltung konfigurieren....1490
16.6.4 Rufumleitung (Call Deflection / Partial Rerouting) am SIP-Trunk (SIP 302)....1491
16.6.5 Faxen über T.38 – Fax over IP (FoIP)....1492
16.6.6 Gruppenrufe mit Ruf-Verteilung....1493
16.6.7 Mehrfachanmeldung (Multi-Login)....1494
16.7 VoIP-Media-Proxy – Optimierte Verwaltung von SIP-Verbindungen....1495

16.8 SIP-ID als Stammnummer bei Trunk-Leitungen....1497
16.9 Vermittlung beim SIP-Provider....1497
16.10 SIP Application Layer Gateway (SIP-ALG)....1499
16.10.1 Eigenschaften....1499
16.10.2 Konfiguration....1499
16.11 SIP-Anmeldung über WAN eingrenzen bzw. unterbinden....1500
16.12 Zertifikate für verschlüsselte Telefonie....1500
16.13 Behandlung kanonischer Rufnummern....1502
16.14 Verarbeitung der Ziel-Domänen....1502
16.14.1 Anmeldung an übergeordneten Vermittlungsstellen....1503
16.14.2 Vermittlung von internen Rufen....1503
16.15 Konfiguration der ISDN-Schnittstellen....1503
16.15.1 Punkt-zu-Mehrpunkt und Punkt-zu-Punkt-Anschlüsse....1503
16.15.2 Busterminierung....1504
16.15.3 Protokoll-Einstellung....1504
16.15.4 Taktung der ISDN-Anschlüsse....1505
16.16 Konfigurationsbeispiele....1506
16.16.1 VoIP-Telefonie im Stand-alone-Einsatz....1506
16.16.2 VoIP-Telefonie als Ergänzung zur übergeordneten ISDN-TK-Anlage....1511
16.16.3 Anbindung an übergeordnete SIP-TK-Anlage....1518
16.16.4 VoIP-Kopplung von Standorten ohne SIP-TK-Anlage....1522
16.16.5 SIP-Trunking....1527
16.16.6 Sperren von abgehenden Rufen zu Sonderrufnummern....1528
16.16.7 Verwerfen von eingehenden Rufen....1529
16.16.8 Rufe ohne übermittelte Rufnummer verwerfen....1530
16.16.9 Rufe ohne übermittelte Rufnummer umleiten....1531
16.17 Diagnose der VoIP-Verbindungen....1531
16.17.1 SIP Traces....1531
16.17.2 Diagnose der Verbindungen mit dem LANmonitor....1531
16.18 VoSIP-Unterstützung im Voice Call Manager....1533
16.19 Auto-Provisionierung LANCOM DECT 510 IP....1534
16.19.1 DECT-Basisstation und -Mobilteile mit LANconfig konfigurieren....1535
17 Backup-Lösungen....1537
17.1 Hochverfügbarkeit von Netzwerken....1537
17.1.1 Wie wird die Störung einer Netzwerkverbindung erkannt?....1537
17.1.2 Hochverfügbarkeit der Leitungen – die Backup-Verbindung....1542
17.1.3 Hochverfügbarkeit der Gateways – redundante Gateways mit VPN Load-Balancing....1543
17.1.4 Hochverfügbarkeit des Internetzugangs – Multi-PPPoE....1543
17.1.5 Anwendungsbeispiele....1544
17.2 Backup-Lösungen und Load-Balancing mit VRRP....1546
17.2.1 Einleitung....1546
17.2.2 Das Virtual Router Redundancy Protocol....1547
17.2.3 Anwendungsszenarien....1552

17.2.4 Zusammenspiel mit internen Diensten....1554
17.2.5 VRRP im WAN....1558
17.2.6 Interaktion mit dem WAN-Backup-Modul....1558
17.2.7 Steuerung des WAN/WAN-Backup durch das VRRP....1559
17.2.8 Konfiguration von VRRPv3....1559
17.2.9 Statusinformationen....1564
17.3 Schnittstellen-Bündelung mit LACP....1565
17.3.1 Konfiguration der LACP-Schnittstellen....1565
17.4 Unterstützung von vRouter-Redundanz in Amazon AWS....1567
17.4.1 Konfiguration....1567
17.4.2 Kommandos....1568
17.4.3 IAM-Rolle konfigurieren in AWS....1569
18 RADIUS....1570
18.1 Funktionsweise von RADIUS....1571
18.2 Über RADIUS in die LCOS-Verwaltungsoberfläche einloggen....1572
18.3 RADIUS als Authenticator bzw. Network Access Server (NAS)....1573
18.3.1 Allgemeine Einstellungen....1573
18.3.2 Einwahl über PPP und RADIUS....1574
18.3.3 Einwahl über WLAN und RADIUS....1576
18.3.4 Einwahl über einen Public Spot und RADIUS....1577
18.3.5 Einwahl über 802.1X und RADIUS....1580
18.3.6 Zusätzliche Source-Ports für Access-Requests....1583
18.4 RADIUS-Server....1583
18.4.1 RADIUS-Dienst....1584
18.4.2 RADIUS- / RADSEC-Clients....1585
18.4.3 Benutzer-Datenbank....1587
18.4.4 Weiterleitung....1594
18.4.5 EAP-Authentifizierung....1598
18.4.6 Benutzerdefinierte Attribute....1600
18.4.7 Optionen....1601
18.5 RADIUS-Attribute....1601
18.5.1 RADIUS-Attribute konfigurierbar....1604
18.5.2 Erweiterung der RADIUS-Attribute für IPv6-RAS-Dienste....1605
18.6 Dynamic Peer Discovery....1606
18.7 Dynamische Autorisierung durch RADIUS CoA (Change of Authorization)....1607
18.7.1 Dynamische Autorisierung mit LANconfig konfigurieren....1608
18.8 RADSEC....1609
18.8.1 Konfiguration von RADSEC für den Client....1610
18.8.2 Zertifikate für RADSEC....1610
19 IoT – Das Internet der Dinge (Internet of Things – IoT)....1611
19.1 Wireless ePaper....1611
19.1.1 Einstellungen für Wireless ePaper....1613
19.2 iBeacon....1615
19.3 BLE-Scanner und -Beacon....1616

19.3.1 Einstellungen für BLE....1617
19.3.2 Monitoring....1619
20 Weitere Dienste....1620
20.1 Automatische IP-Adressverwaltung mit DHCP....1620
20.1.1 Einleitung....1620
20.1.2 Konfiguration der DHCPv4-Parameter mit LANconfig....1622
20.1.3 Konfiguration der DHCP-Clients....1634
20.1.4 DHCP-Client-Option Classless Static Route....1634
20.1.5 DHCP-Relay-Server....1634
20.1.6 Anzeige von Statusinformationen des DHCP-Servers....1635
20.1.7 DHCP-Cluster....1636
20.1.8 Alternative DHCP-Server zur Weiterleitung....1637
20.1.9 DHCP-Snooping und DHCP-Option 82....1637
20.1.10 Zuweisung von IP-Adressen basierend auf DHCP-Option 82....1639
20.1.11 Parameter der LANCOM Management Cloud durch den DHCP-Server ausliefern....1640
20.2 Domain-Name-Service (DNS)....1641
20.2.1 Was macht ein DNS-Server?....1641
20.2.2 DNS-Forwarding....1641
20.2.3 So stellen Sie den DNS-Server ein....1643
20.2.4 Protokollierung von DNS-Anfragen über SYSLOG....1644
20.2.5 URL-Blocking....1646
20.2.6 DNS-Filter für DNS-Datentunnel....1647
20.2.7 Dynamic DNS....1647
20.3 Accounting....1649
20.3.1 Arbeitsweise....1650
20.3.2 Ein- bzw. Ausschalten des Accountings im laufenden Betrieb....1651
20.3.3 Zählung des Datenverkehrs....1651
20.3.4 Konfiguration des Accounting....1651
20.4 Gebührenmanagement....1652
20.4.1 Verbindungs-Begrenzung für DSL und Kabelmodem....1653
20.4.2 Einstellungen im Gebührenmodul....1654
20.5 Zeit-Server für das lokale Netz....1654
20.5.1 Konfiguration des Zeit-Servers unter LANconfig....1654
20.5.2 Konfiguration der NTP-Clients....1657
20.5.3 Beziehen der Gerätezeit über GPS....1659
20.6 Scheduled Events....1659
20.6.1 Zeitautomatik für LCOS-Befehle....1659
20.6.2 CRON-Jobs mit Zeitverzögerung....1660
20.6.3 Konfiguration der Zeitautomatik....1660
20.7 PPPoE-Server....1662
20.7.1 Einleitung....1662
20.7.2 PPPoE ist nur auf einem Netzwerksegment einsetzbar....1662
20.7.3 Anwendungsbeispiel....1662

20.7.4 Konfiguration....1664
20.7.5 PPPoE-Snooping....1665
20.8 Simple Network Management Protocol (SNMP)....1666
20.8.1 SNMPv3-Grundlagen....1667
20.8.2 SNMP konfigurieren....1668
20.9 Netflow / IPFIX....1678
20.9.1 NetFlow / IPFIX konfigurieren....1679
20.10 Betrieb von Druckern am USB-Anschluss des Gerätes....1681
20.10.1 Konfiguration des Printservers im Gerät....1682
20.10.2 Konfiguration der Drucker auf dem Rechner....1683
20.11 LANCOM Content Filter....1687
20.11.1 Einleitung....1687
20.11.2 Voraussetzungen für die Benutzung des LANCOM Content Filters....1689
20.11.3 Schnellstart....1689
20.11.4 Die Standardeinstellungen im LANCOM Content Filter....1690
20.11.5 Allgemeine Einstellungen....1691
20.11.6 Einstellungen für das Blockieren....1693
20.11.7 Override-Einstellungen....1697
20.11.8 Profile des LANCOM Content Filters....1699
20.11.9 Optionen des LANCOM Content Filters....1704
20.11.10 Zusätzliche Einstellungen für den LANCOM Content Filter....1706
20.12 BPjM-Modul....1709
20.12.1 Einsatzempfehlungen....1710
20.12.2 Menüaktion zum Löschen der BPjM-Signaturdefinition....1711
20.13 TACACS+....1711
20.13.1 Einleitung....1711
20.13.2 Konfiguration der TACACS+-Parameter....1712
20.13.3 Konfiguration der TACACS+-Server....1715
20.13.4 Anmelden am TACACS+-Server....1716
20.13.5 Rechtezuweisung unter TACACS+....1718
20.13.6 Autorisierung von Funktionen....1718
20.13.7 TACACS+-Umgehung....1720
20.14 LLDP....1721
20.14.1 Funktionsweise....1721
20.14.2 Aufbau der LLDP-Nachrichten....1722
20.14.3 Unterstützte Betriebssysteme....1723
20.15 SMS-Empfang und -Versand....1724
20.15.1 Empfang von SMS-Nachrichten....1724
20.15.2 Basiskonfiguration des SMS-Moduls....1724
20.15.3 SMS-Nachrichten mit LANmonitor verwalten....1725
20.15.4 SMS-Nachrichten mit LANmonitor versenden....1726
20.15.5 URL-Platzhalter für den SMS-Versand....1727
20.15.6 Zeichensatz für den SMS-Versand....1727
20.15.7 Aktionen auf eingehende SMS ausführen....1728

20.16 Geräte-LEDs bootpersistent ausschalten....1729
20.17 802.1X-Authenticator für Ethernet-Ports....1730
20.18 xDSL-Schnittstelle....1732
20.18.1 ADSL- / VDSL-Modem-Betrieb (Brigde-Mode)....1732
20.18.2 Allgemeine xDSL-Einstellungen....1734
20.19 GPON-Unterstützung....1735
20.20 ACME-Client....1736
20.20.1 ACME-Client konfigurieren....1737
20.21 Operations, Administration und Management (OAM)....1738
20.21.1 Ethernet Link OAM (IEEE 802.3ah)....1739
20.21.2 Connectivity Fault Management (IEEE 802.1ag / ITU-T Y.1731)....1741
20.22 Alive-Test....1745
21 Anhang....1748
21.1 Die CRON-Syntax....1748

Copyright

© 2025 LANCOM Systems GmbH, Würselen (Germany). Alle Rechte vorbehalten.

Alle Angaben in dieser Dokumentation sind nach sorgfältiger Prüfung zusammengestellt worden, gelten jedoch nicht als Zusicherung von Produkteigenschaften. LANCOM Systems haftet ausschließlich in dem Umfang, der in den Verkaufs- und Lieferbedingungen festgelegt ist.

Weitergabe und Vervielfältigung der zu diesem Produkt gehörenden Dokumentation und Software und die Verwendung ihres Inhalts sind nur mit schriftlicher Erlaubnis von LANCOM Systems gestattet. Änderungen, die dem technischen Fortschritt dienen, bleiben vorbehalten.

Windows® und Microsoft® sind eingetragene Marken von Microsoft, Corp.

LANCOM, LANCOM Systems, LCOS, LANcommunity, LANCOM Service LANcare, LANCOM Active Radio Control und AirLancer sind eingetragene Marken. Alle anderen verwendeten Namen und Bezeichnungen können Marken oder eingetragene Marken ihrer jeweiligen Eigentümer sein. Dieses Dokument enthält zukunftsbezogene Aussagen zu Produkten und Produkteigenschaften. LANCOM Systems behält sich vor, diese jederzeit ohne Angaben von Gründen zu ändern. Keine Gewähr für technische Ungenauigkeiten und / oder Auslassungen.

Das Produkt enthält separate Komponenten, die als sogenannte Open Source Software eigenen Lizenzen, insbesondere der General Public License (GPL), unterliegen. Die Lizenzinformationen zur Geräte-Firmware (LCOS) finden Sie auf der WEBconfig des Geräts unter dem Menüpunkt „Extras > Lizenzinformationen“. Sofern die jeweilige Lizenz dies verlangt, werden Quelldateien zu den betroffenen Software-Komponenten auf Anfrage über einen Download-Server bereitgestellt.

Produkte von LANCOM Systems enthalten Software, die vom „OpenSSL Project“ für die Verwendung im „OpenSSL Toolkit“ entwickelt wurde (*www.openssl.org*).

Produkte von LANCOM Systems enthalten kryptographische Software, die von Eric Young (*eay@cryptsoft.com*) geschrieben wurde.

Produkte von LANCOM Systems enthalten Software, die von der NetBSD Foundation, Inc. und ihren Mitarbeitern entwickelt wurde.

Produkte von LANCOM Systems enthalten das LZMA SDK, das von Igor Pavlov entwickelt wurde.

LANCOM Systems GmbH

A Rohde & Schwarz Company

Adenauerstr. 20/B2

52146 Würselen

Deutschland

www.lancom-systems.de

1 LCOS

Das LANCOM Operating System (LCOS) ist die speziell für LANCOM Router / SD-WAN Gateways und WLAN-Controller entwickelte Firmware und bildet das Herzstück der zuverlässigen und sicheren Netzwerkinfrastrukturen von LANCOM Systems. Als proprietäres Betriebssystem wird LCOS kontinuierlich weiterentwickelt und regelmäßig mit neuen Funktionen und Verbesserungen aktualisiert.

LCOS steht für höchste Sicherheitsstandards, die durch eine umfassende Qualitätssicherung und unabhängige Zertifizierungen untermauert werden. Das Siegel „IT-Security Made in Germany" (ITSMG) bestätigt die garantierte Backdoor-Freiheit und unterstreicht die vertrauenswürdige Entwicklung und Pflege des Systems. Durchgängige Prüfungen und kontinuierliche Updates stellen höchste Sicherheitsstandards sicher.

Durch eine zukunftssichere Hardware-Dimensionierung sind LANCOM Produkte auf eine langfristige Nutzung ausgelegt. Regelmäßige Software-Updates – einschließlich Security Patches, Feature Updates und Major Releases – gewährleisten, dass auch ältere Geräte über viele Jahre hinweg mit stabiler und sicherer Firmware betrieben werden können.

LCOS verkörpert die LANCOM Grundwerte:

- **Sicherheit**

  Jede LCOS-Version wird mit höchster Sorgfalt entwickelt und getestet. Zusätzlich wird LCOS wird regelmäßig Sicherheitstest und externen Prüfungen unterzogen. Backdoor-Freiheit und die Einhaltung strenger IT-Sicherheitsstandards sind garantiert.

- **Zuverlässigkeit**

  Durch kontinuierliche Weiterentwicklung und regelmäßige Updates bietet LCOS über den gesamten Produktlebenszyklus hinweg ein Höchstmaß an Stabilität und Verfügbarkeit.

- **Zukunftsfähigkeit**

  Im Einklang mit den LANCOM Lifecycle-Richtlinien unterstützt LCOS langfristig den sicheren Betrieb und die Weiterentwicklung von Netzwerkinfrastrukturen durch kontinuierliche Funktions- und Sicherheitsupdates.

Mit LCOS erhalten Unternehmen eine bewährte, leistungsfähige und vertrauenswürdige Grundlage für professionelle Netzwerklösungen – entwickelt und gepflegt in Deutschland.

2 Konfiguration

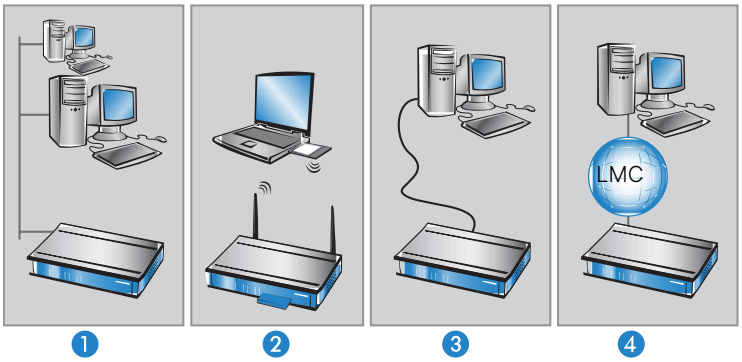
In diesem Kapitel erhalten Sie einen Überblick, mit welchen Mitteln und über welche Wege Sie auf das Gerät zugreifen können, um Einstellungen vorzunehmen. Sie finden Beschreibungen zu folgenden Themen:

- Konfigurationstools
- Kontroll- und Diagnosefunktionen von Gerät und Software
- Sicherung und Wiederherstellung kompletter Konfigurationen
- Installation neuer Firmware im Gerät

2.1 Mittel und Wege für die Konfiguration

Das Gerät unterstützt verschiedene Mittel (sprich Software) und Wege (in Form von Kommunikationszugängen) für die Konfiguration. Je nach verfügbaren Anschlüssen lässt sich das Gerät auf verschiedenen Zugangswegen erreichen:

- über das angeschlossene Netzwerk (sowohl [W]LAN als auch [W]WAN; auch „Inband" genannt) [1, 2];
- über die serielle Konfigurationsschnittstelle (Config-Schnittstelle; auch „Outband" genannt) [3];
- über die LANCOM Management Cloud (LMC) (Lizenz erforderlich) [4].



Was unterscheidet diese Wege?

Die oben gelisteten Zugangswege unterscheiden sich einerseits in ihrer möglichen Verfügbarkeit und andererseits in ihren Anforderungen an zusätzliche Hard- und Software:

- Die Inband-Konfiguration benötigt neben dem ohnehin vorhandenen Rechner im LAN, WAN oder WLAN nur noch eine geeignete Software, beispielsweise LANconfig oder einen Webbrowser für die Konfiguration über WEBconfig oder LMC (vgl. *Software zur Konfiguration* auf Seite 27). Die Inband-Konfiguration ist jedoch z. B. nicht mehr möglich, wenn das übertragende Netzwerk gestört ist.
- Die Outband-Konfiguration ist durch den separaten Übertragungsweg immer verfügbar. Sie benötigt zusätzlich zur Konfigurationssoftware noch einen Rechner mit serieller Schnittstelle.

2.2 Software zur Konfiguration

Die Situationen, in denen konfiguriert wird, unterscheiden sich ebenso wie die persönlichen Ansprüche und Vorlieben der Ausführenden. Das Gerät verfügt daher über ein breites Angebot von Konfigurationsmöglichkeiten:

- **LANconfig** – menügeführt, übersichtlich und einfach lassen sich nahezu alle Parameter eines Gerätes einstellen. LANconfig benötigt einen Konfigurationsrechner mit einem aktuellem Windows-Betriebssystem. Weitere Informationen finden Sie im Kapitel *LANconfig – Geräte konfigurieren* auf Seite 174.
- **WEBconfig** – diese Software ist fest in das LCOS eines Gerätes eingebaut. WEBconfig ist dadurch betriebssystemunabhängig; auf dem Konfigurationsrechner wird nur ein Webbrowser vorausgesetzt. Weitere Informationen finden Sie im Kapitel *WEBconfig* auf Seite 28.
- **LANCOM Management Cloud** – ist das Cloud-basierte Management-System, das ihre gesamte Netzwerkarchitektur im WAN, LAN, WLAN und SECURITY intelligent organisiert, optimiert und steuert.Weitere Informationen finden Sie im Kapitel *LANCOM Management Cloud (LMC)* auf Seite 41.
- **Terminalprogramm** – alternativ zu LANconfig können Sie auch Terminalprogramme (wie z. B. HyperTerminal oder PuTTY) verwenden, um ein Gerät über die Konsole zu konfigurieren. Je nach Funktionsumfang des Programms kann die Kommunikation dabei wahlweise über die serielle Schnittstelle oder innerhalb eines IP-Netzwerks erfolgen. Innerhalb von IP-Netzwerken stehen Ihnen die Protokolle Telnet, SSH oder das Dateiübertragungs-Protokoll TFTP zur Auswahl.
- **SNMP Management-Programm** – alternativ zu LANconfig können Sie auch geräteunabhängige Programme zum Management von IP-Netzwerken verwenden, die auf dem SNMP-Protokoll basieren.

Die folgende Tabelle zeigt, über welchen Weg Sie mit den jeweiligen Mitteln auf die Konfiguration zugreifen können:

Tabelle 1: Übersicht der Konfigurationsmittel in Abhängigkeit der Konfigurationswege

Verwendete Software	[W]LAN, [W]WAN (Inband)	Config-Schnittstelle (Outband)
LANconfig	Ja	Ja
WEBconfig	Ja	Nein
LANCOM Management Cloud	Ja	Nein
Serial-Client	Nein	Ja
Telnet-Client	Ja	Nein
SSH-Client	Ja	Nein
TFTP-Client	Ja	Nein
SNMP Management-Programm	Ja	Nein

Bitte beachten Sie, dass alle Verfahren auf dieselben Konfigurationsdaten zugreifen. Wenn Sie beispielsweise in LANconfig Einstellungen ändern, hat dies auch direkte Auswirkungen auf die Werte unter WEBconfig und Telnet.

2.2.1 LANconfig

Informationen zur Konfiguration der Geräte mit LANconfig finden Sie separat im LANtools-Kapitel *LANconfig – Geräte konfigurieren* auf Seite 174.

2.2.2 WEBconfig

Mit WEBconfig stellen Ihnen die Geräte eine grafische Benutzeroberfläche bereit, die direkt in das LCOS integriert ist. Dadurch kann die Konfiguration der Geräte aus der Ferne und / oder unabhängig vom verwendeten Betriebssystem Ihres Rechners erfolgen. Sie benötigen lediglich einen Webbrowser, um auf WEBconfig zuzugreifen.

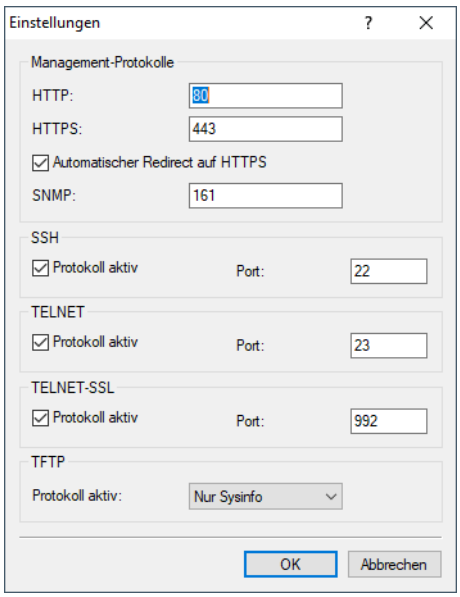
2.2.2.1 Zugang zum Gerät mit WEBconfig

Für die Konfiguration mit WEBconfig müssen Sie wissen, wie sich das Gerät ansprechen lässt. Das Verhalten der Geräte sowie ihre Erreichbarkeit zur Konfiguration über einen Webbrowser hängen davon ab, ob im LAN schon DHCP-Server und DNS-Server aktiv sind, und ob diese beiden Serverprozesse die Zuordnung von IP-Adressen zu symbolischen Namen im LAN untereinander austauschen. Der Zugriff mit WEBconfig erfolgt entweder über die IP-Adresse des Gerätes, über

den Namen des Gerätes (sofern bereits zugewiesen) bzw. sogar über einen beliebigen Namen, falls das Gerät noch nicht konfiguriert wurde.

Der Browser macht aus der IP-Adresse bzw. dem Namen eine unverschlüsselte Verbindungsanfrage an das LANCOM Gerät. Dieses schaltet dann automatisch auf eine verschlüsselte HTTPS-Verbindung um. Dadurch werden sensitive Daten wie z. B. das Passwort beim Login oder die Konfiguration durch die verschlüsselte Verbindung geschützt.

Falls die Funktion nicht aktiviert ist, dann können Sie die Funktion unter **Management** > **Admin** > **Management-Protokolle** > **Einstellungen** > **Automatischer Redirect auf HTTPS** einschalten.



Nach dem Einschalten prüfen unkonfigurierte Geräte zunächst, ob im LAN schon ein DHCP-Server aktiv ist. Je nach Situation kann das Gerät dann den eigenen DHCP-Server einschalten oder alternativ den DHCP-Client-Modus aktivieren. In dieser zweiten Betriebsart kann das Gerät selbst eine IP-Adresse von einem im LAN schon vorhandenen DHCP-Server beziehen.

Wenn Sie ein WLAN-Gerät von einem WLAN-Controller zentral verwalten lassen, schaltet das WLAN-Gerät beim Zuweisen der WLAN-Konfiguration ebenfalls den DHCP-Server vom Auto-Modus in den Client-Modus um.

2.2.2.2 Netz ohne DHCP-Server

In einem Netz ohne DHCP-Server schalten unkonfigurierte Geräte nach dem Starten den eigenen DHCP-Serverdienst ein und weisen den anderen Rechnern im LAN die IP-Adressen sowie Informationen über Gateways etc. zu, sofern diese auf den automatischen Bezug der IP-Adressen eingestellt sind (Auto-DHCP). In dieser Konstellation kann das Gerät von jedem Rechner mit aktivierter Auto-DHCP-Funktion mit einem Webbrowser unter der IP-Adresse **172.23.56.254** erreicht werden.

Im werksseitigen Auslieferungszustand mit aktiviertem DHCP-Server leitet das Gerät alle eingehenden DNS-Anfragen an den internen Webserver weiter. Dadurch können unkonfigurierte Geräte einfach durch Eingabe eines beliebigen Namens in die Adresszeile eines Webbrowsers angesprochen und in Betrieb genommen werden.



Falls der Konfigurations-Rechner seine IP-Adresse nicht vom DHCP-Server bezieht, ermitteln Sie die aktuelle IP-Adresse des Rechners (mit **Start** > **Ausführen** > **cmd** und dem Befehl **ipconfig** an der Eingabeaufforderung unter Windows 7 oder höher bzw. dem Befehl **ifconfig** in der Konsole unter Linux). In diesem Fall erreichen Sie das Gerät unter der Adresse **x.x.x.254** (die "x" stehen für die ersten drei Blöcke in der IP-Adresse des Konfigurationsrechners).

2.2.2.3 Netz mit DHCP-Server

Ist im LAN ein DHCP-Server zur Zuweisung der IP-Adressen aktiv, schaltet ein unkonfiguriertes Gerät seinen eigenen DHCP-Server aus, wechselt in den DHCP-Client-Modus und bezieht eine IP-Adresse vom DHCP-Server aus dem LAN. Diese IP-Adresse ist aber zunächst nicht bekannt; die Erreichbarkeit des Gerätes hängt von der Namensauflösung ab:

- Ist im LAN auch ein DNS-Server zur Auflösung der Namen vorhanden und tauscht dieser die Zuordnung von IP-Adressen zu den Namen mit dem DHCP-Server aus, kann das Gerät durch Eingabe der MAC-Adresse (z. B. `00a057xxxxxx`) erreicht werden.

  Die MAC-Adresse finden Sie auf einem Aufkleber auf der Geräteunterseite.

- Ist im LAN kein DNS-Server vorhanden oder ist dieser nicht mit dem DHCP-Server gekoppelt, kann das Gerät nicht über den Namen erreicht werden. In diesem Fall haben Sie folgende Optionen, um die IP-Adresse des Gerätes zu ermitteln:
  - Sie nutzen von einem anderen erreichbaren Gerät aus die WEBconfig-Funktion **Andere Geräte suchen / anzeigen**, oder alternativ die LANconfig-Funktion **Geräte suchen**.
  - Sie machen die per DHCP an das Gerät zugewiesene IP-Adresse über geeignete Tools ausfindig und versuchen, das Gerät mit dieser IP-Adresse direkt zu erreichen.
  - Sie schließen einen Rechner mit Terminalprogramm über die serielle Konfigurationsschnittstelle an das Gerät an.

2.2.2.4 Anmeldung am Gerät

Rufen Sie WEBconfig über die vom DHCP-Server vergebene IP-Adresse bzw. den vom DNS-Server vergebenen Namen auf. Wenn Sie beim Zugriff auf das Gerät zur Eingabe von Benutzername und Passwort aufgefordert werden, tragen Sie Ihre persönlichen Werte in die entsprechenden Felder der Eingabemaske ein. Achten Sie dabei auf Groß- und Kleinschreibung.

Falls Sie nur den allgemeinen Konfigurationszugang („root“) verwenden, tragen Sie nur das entsprechende **Passwort** ein. Das **Login**-Feld für den Benutzernamen ist in diesem Fall bereits vorbesetzt.

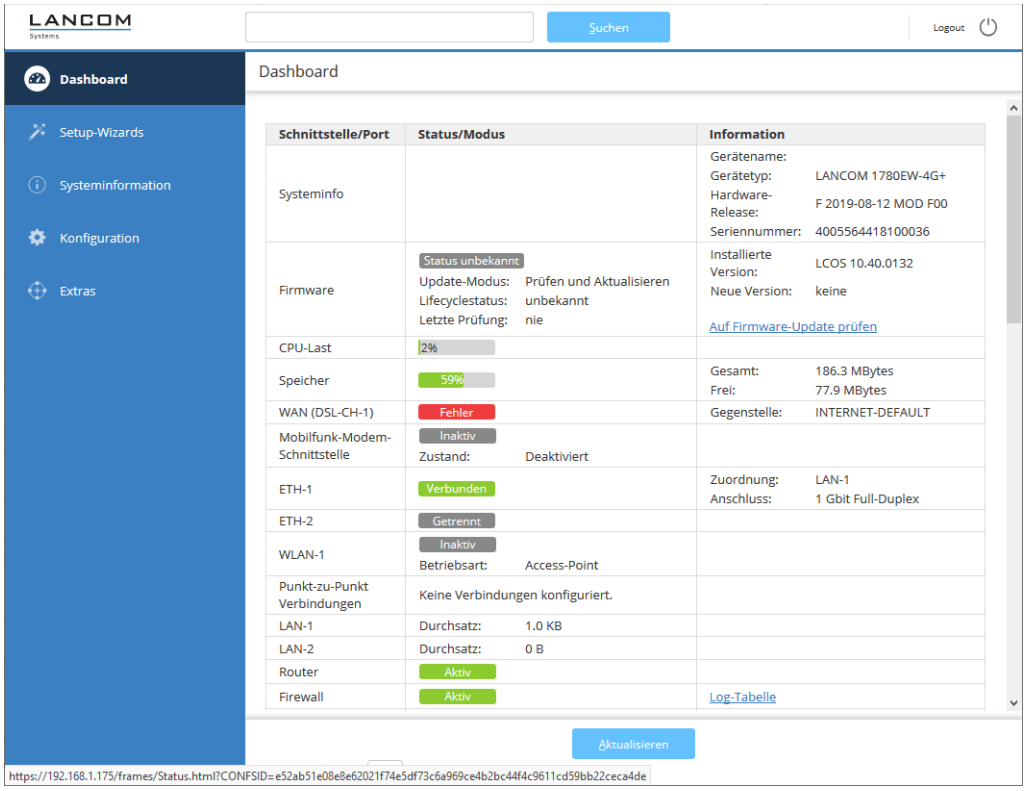
Für maximale Sicherheit sollten Sie stets die neueste Version Ihres Browsers verwenden. Überprüfen Sie dabei auch, ob Sie sich noch im aktuellen Entwicklungszweig befinden, da manche Browser automatische Updates nur in bestimmten Versionsbereichen durchführen oder Updates nicht mehr anzeigen, wenn die Unterstützung für bestimmte Betriebssysteme ausgelaufen ist. In diesem Fall empfiehlt sich dringend der Wechsel auf einen alternativen Webbrowser.

2.2.2.5 Suchen

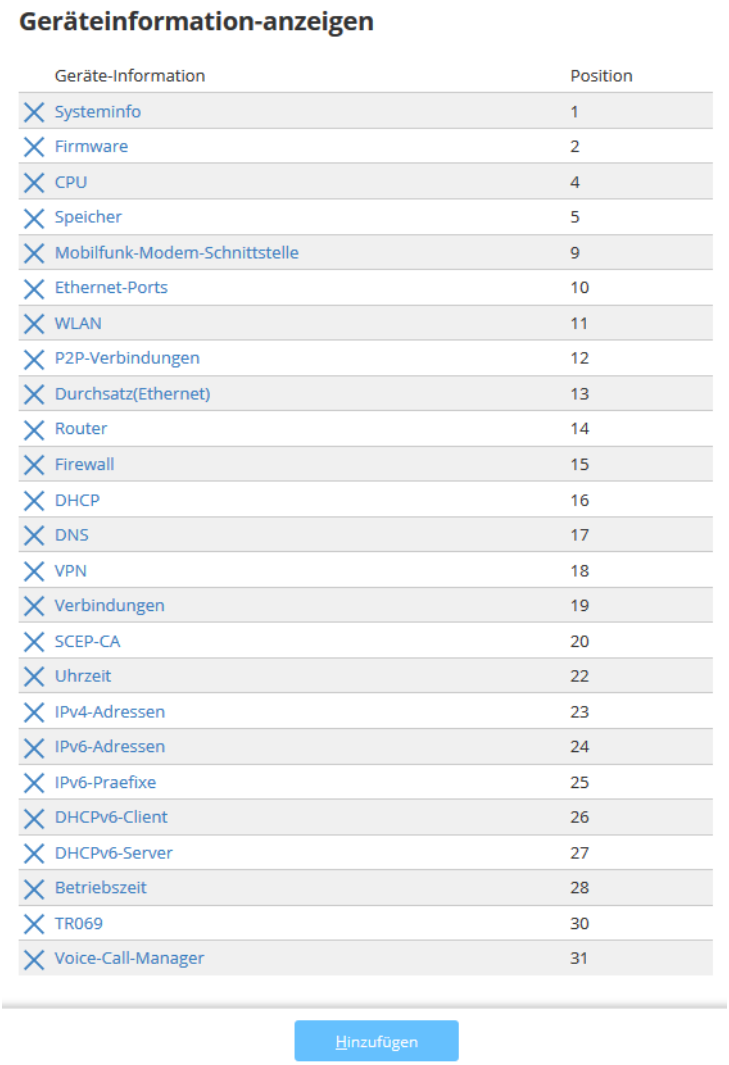
Mit der Suchfunktion im oberen Bereich durchsuchen Sie den kompletten Menübaum nach dem von Ihnen eingegebenen Wort. Falls Sie also zu einem bestimmten Status- oder Konfigurationsparameter den Namen kennen, aber nicht wissen, über welches Menü dieser Eintrag zu erreichen ist, können Sie die gewünschte Stelle auf diese Weise schnell auffinden.

2.2.2.6 Dashboard

Hier finden Sie umfangreiche Informationen über den aktuellen Betriebszustand des Gerätes. Dazu gehört z. B. die visuelle Darstellung der Schnittstellen mit Angabe der darauf aktiven Netzwerke. Über entsprechende Links können relevante weitere Statistiken aufgerufen werden (z. B. DHCP-Tabelle). Bei wesentlichen Mängeln in der Konfiguration (z. B. ungültige Zeiteinstellung) wird ein direkter Link zu den entsprechenden Konfigurationsparametern angeboten.

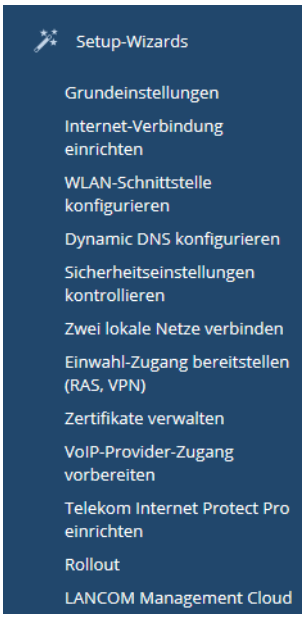


Den Umfang der auf dieser Seite angezeigten Informationen definieren Sie unter **Extras** > **LCOS-Menübaum** > **Setup** > **HTTP** > **Geräteinformation-anzeigen**. Dabei legen Sie über eine Indexnummer auch die Reihenfolge der Anzeige fest.



2.2.2.7 Setup-Wizards

Mit den Setup-Wizards haben Sie die Möglichkeit, schnell und komfortabel häufige Einstellungen für ein Gerät vorzunehmen. Wählen Sie dazu den gewünschten Assistenten aus und geben Sie auf den folgenden Seiten die benötigten Daten ein. Die einzelnen Einrichtungsschritte sind mit denen von LANconfig identisch.



Das Gerät speichert die getätigten Einstellungen erst dann, wenn Sie die Eingaben auf der letzten Seite eines Assistenten bestätigen. Die Verfügbarkeit einzelner Assistenten variiert zwischen einzelnen Gerätetypen (Access Point, WLAN-Controller, usw.).

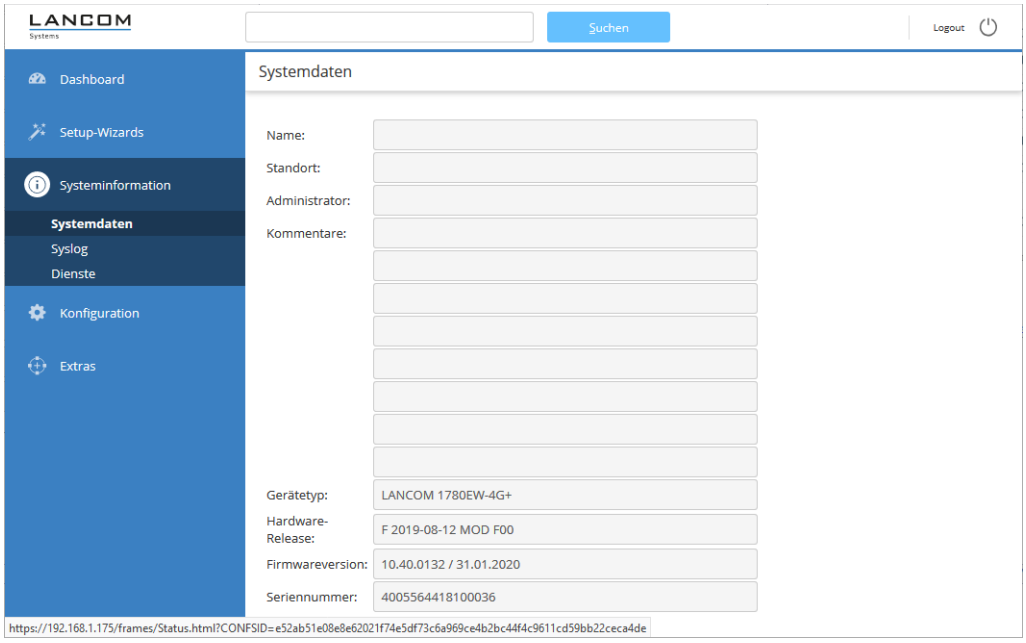
Auf Geräten mit VPN-Funktion lassen sich VPN-Client-Einwahlzugänge wie Advanced-VPN-Client auch über WEBconfig anlegen. Die 1-Click-VPN-Konfiguration ist in WEBconfig durch die Beschränkungen des Browserzugriffs nicht verfügbar.

2.2.2.8 Systeminformation

Ihr Gerät zeigt Ihnen im Menübereich **Systeminformation** die wichtigsten Daten zur Soft- und Hardware Ihres Gerätes, die Syslog-Tabelle sowie den Diensten an.

Systemdaten

Unter **Systeminformation** > **Systemdaten** finden Sie allgemeine Informationen über das Gerät, den Standort, die Firmware-Version, die Seriennummer etc.



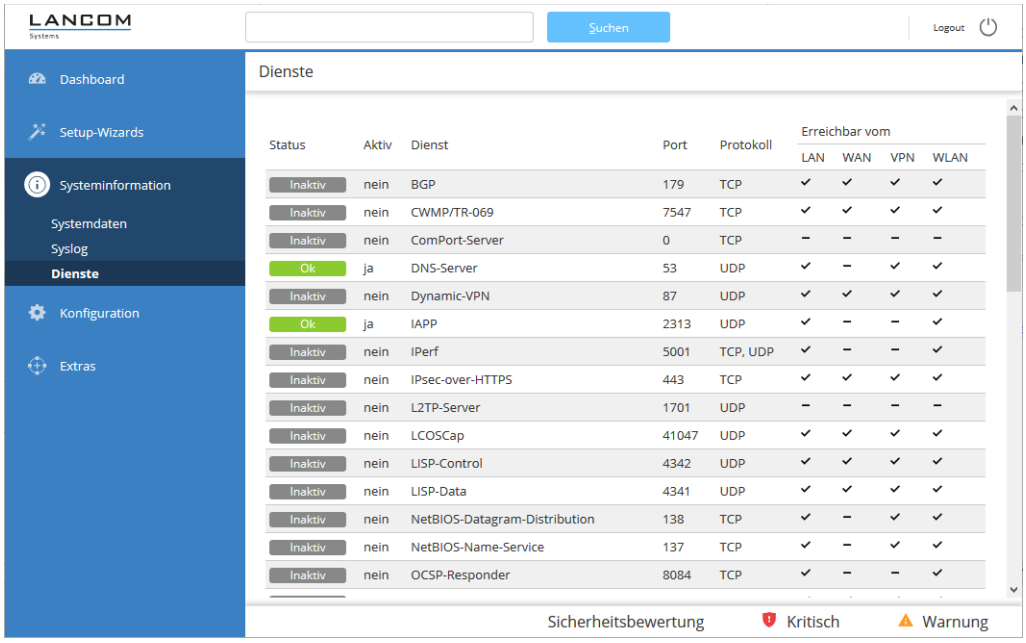
Syslog

Das Gerät legt Syslog-Informationen im Arbeitsspeicher ab (siehe dazu *Das SYSLOG-Modul* auf Seite 323).

Zeitstempel beginnend mit '1900-…' weisen auf eine nicht oder nicht korrekt gesetzte Uhrzeit hin.

Dienste

Hier erhalten Sie einen Überblick über die internen LCOS-Dienste, deren Ports und Protokolle, ob sie aktiv sind und auf welchem Weg sie erreichbar sind.



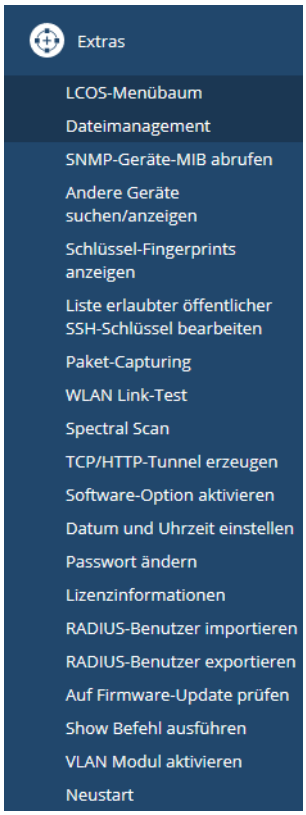
2.2.2.9 Konfiguration

Der Menübereich **Konfiguration** bietet dieselben Konfigurationsparameter in der gleichen Struktur an wie LANconfig.



2.2.2.10 Extras

Im Menübereich **Extras** finden Sie einige Funktionen, welche die Konfiguration der Geräte erleichtern; je nach Gerät aber auch einige Sonderfunktionen und spezielle Analysemodule bereitstellen, die sich keinem der bisherigen Menüpunkte sinnvoll zuordnen lassen.



Der Funktionsumfang dieses Menübereiches variiert je nach Gerätetyp.

LCOS-Menübaum

Der Bereich **LCOS-Menübaum** bietet die Konfigurations- und Statusparameter in der gleichen Struktur an wie auf der Kommandozeile des Gerätes. Die einzelnen Zweige des Menübaums gliedern sich in Menüpunkte, Tabellen, Parameter und Aktionen. Tabellen gruppieren Sätze von Parametern; Menüpunkte gruppieren Tabellen, einzelne Parameter und Aktionen.

Darüber hinaus verfügt der Menübaum über ein kontextsensitives Hilfesystem: Mit einem Klick auf das Fragezeichen neben einem Eintrag können Sie für jeden Menüpunkt, jede Tabelle und jeden Parameter eine eigene Hilfeseite aufrufen. Weitere Informationen zu den einzelnen Einträgen finden Sie außerdem in der Menüreferenz.

Status

Im **Status**-Menü speichert das Gerät alle Statuswerte. Statuswerte (gespeichert in den dazugehörigen Statusparametern) sind reine Informationswerte, die sich nur auslesen und nicht verändern lassen.

Ein Teil der Statuswerte wird direkt oder indirekt durch die im Setup-Menü gesetzten Parameter beeinflusst und hält nur in bestimmten Einstellungsszenarien tatsächlich auch Werte vor. Die DHCP-Tabelle z. B. zeigt nur dann Werte, wenn der geräteinterne DHCP-Server aktiviert und auch im Einsatz ist. Ein anderer Teil ist nicht durch Setup-Parameter beeinflussbar, wie z. B. die Hardware-Informationen. Einige Menüpunkte beinhalten außerdem Aktionen bzw. Analysefunktionen, die Sie manuell ausführen müssen, bevor das Gerät Ihnen Ergebnisse dazu anzeigt.

Setup

Im **Setup**-Menü speichert das Gerät alle einstellbaren Parameter. Setup-Parameter stellen die Konfigurationsbasis eines Gerätes dar; alle Einstellungen, die Sie in LANconfig oder WEBconfig vornehmen, werden letztendlich in den Parametern des Setup-Menüs gespeichert.

Da für den ordnungsgemäßen Betrieb und die Funktionsweise zahlreiche Parameter erforderlich sind, die jedoch nicht alle einer stetigen Änderung bedürfen (z. B. durch Normen und Standards festgelegte Unter- und Obergrenzen), finden Sie in diesem Menü auch Parameter vor, für die es im LANconfig keine Einstellungsmöglichkeit gibt. Normalerweise müssen diese Parameter nicht verändert werden; in einigen Fällen kann es jedoch sinnvoll oder erforderlich sein, bestimmte Vorgabewerte den eigenen individuellen Bedürfnissen entsprechend anzupassen.

Diese „Experteneinstellungen" erfordern in vielen Fällen ein fundiertes Hintergrundwissen über die Funktionsweise und Zusammenhänge der einzelnen Module des LCOS sowie der technischen Standards. Nicht selten müssen Parameter auch an mehreren Stellen im Setup-Menü verändert werden, um eine bestimmte Konfiguration zu erreichen. Nehmen Sie Einstellungen im Setup-Menü deshalb nur dann vor, wenn die Dokumentation oder der Support Sie explizit dazu auffordert oder Sie mit den technischen Standards und Normen hinter einer Funktion vertraut sind!

Firmware

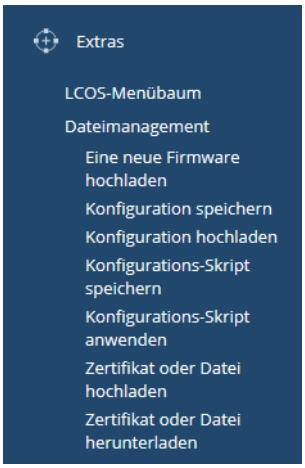
Im **Firmware**-Menü rufen Sie Informationen zur aktuellen Firmware-Version ab, konfigurieren Firmsafe und schalten ggf. auf eine andere Firmware um (lesen Sie dazu auch *FirmSafe* auf Seite 88), und laden bei Bedarf eine neue Firmware in das Gerät. Alternativ können Sie auch das *Dateimanagement* verwenden, um eine andere Firmware ins Gerät zu laden.

Sonstiges

Über dieses Menü können Sie manuell die Verbindung zu einer Gegenstelle aufbauen oder beenden, das Gerät neu starten sowie (an der Konsole) eine neue Firmware hochladen.

Dateimanagement

Im Menübereich **Dateimanagement** finden Sie alle Aktionen, mit denen Sie Dateien (wie z. B. Konfigurationsdateien und -skripte; aber auch Zertifikate, Templates und Logos) aus dem Gerät herunter oder in das Gerät hochladen. Darüber hinaus können Sie hierüber auch eine andere Firmware in das Gerät einspielen.



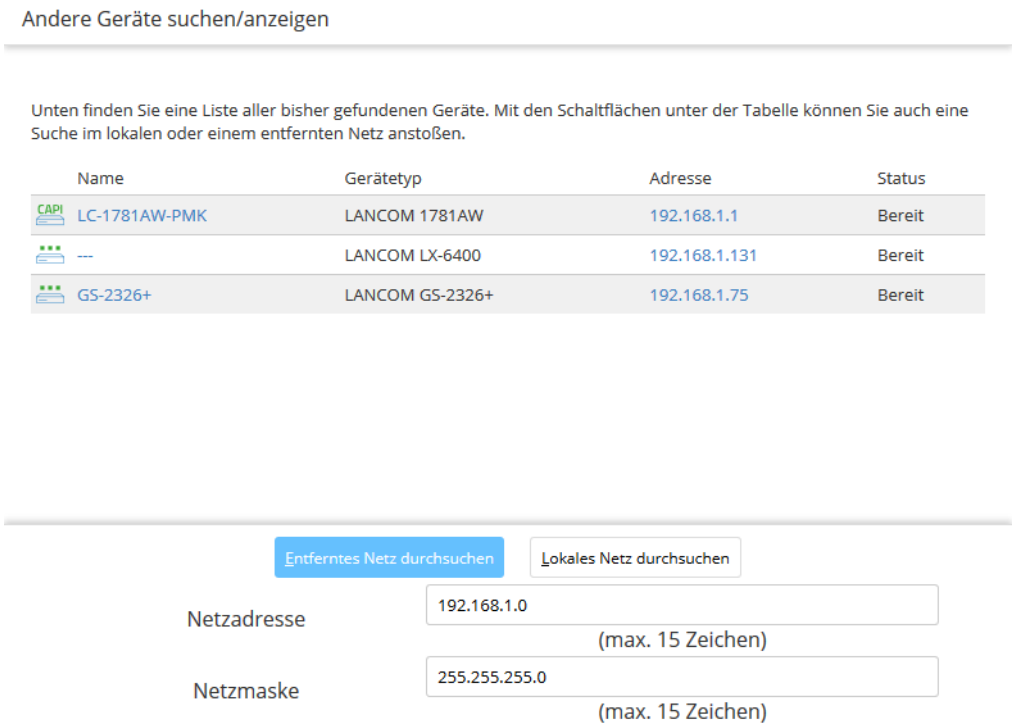
In das Gerät hochgeladene Zertifikate oder Dateien können Sie anschließend im Status-Menü unter **Dateisystem** einsehen.

SNMP-Geräte-MIB abrufen

Über diesen Menüpunkt laden Sie die gerätespezifische *.mib-Datei (Management Information Base) herunter, welche benötigt wird, um das Gerät in einer alternativen SNMP Management-Software zu überwachen und zu verwalten. Weitere Informationen dazu finden Sie unter *SNMP Management-Programm* auf Seite 77.

Andere Geräte suchen / anzeigen

Mit der Funktion zum Suchen und Anzeigen können Sie andere Geräte in Ihrem Netzwerk suchen und über einen entsprechenden Link direkt auf die Konfigurationsseite der gefundenen Geräte wechseln. Diese Funktion ähnelt somit der Funktion **Geräte suchen** in LANconfig.



Schlüssel-Fingerprints anzeigen

Diese Seite zeigt Ihnen eine Übersicht der Fingerprints aller im Gerät vorhandenen Kryptographie-Schlüssel an. Mehr dazu erfahren Sie unter *Geräteinterne SSH- / SSL-Schlüssel* auf Seite 113.

Erlaubte öffentliche SSH Schlüssel

Diese Seite zeigt Ihnen eine Übersicht der vom Gerät akzeptierten öffentlichen Schlüssel (SSH Public-Keys), anhand derer eine Public-Key-Authentifizierung möglich ist. WEBconfig gibt die Übersicht als Textfeld aus, wodurch Sie – als Alternative zum Datei-Upload im Bereich *Dateimanagement* – jederzeit weitere Schlüssel hinzufügen und / oder bestehende bearbeiten können.

Mehr zu dem Thema und zur Schlüssel-Syntax finden Sie im Abschnitt *Syntax und Benutzer öffentlicher Schlüssel anpassen* auf Seite 118.

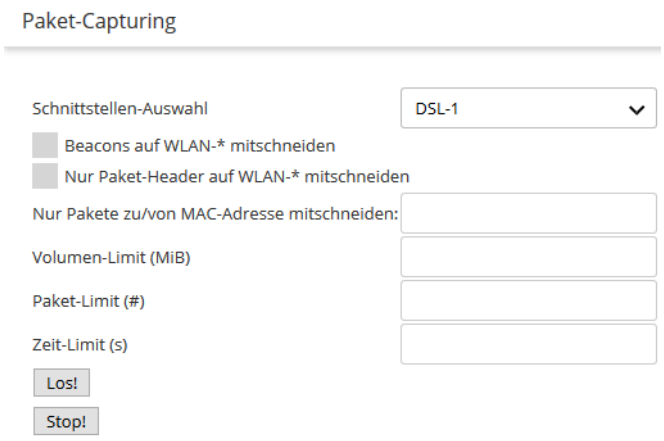
Neue Schlüssel tragen Sie in eine eigene Zeile ein; Zeilenumbrüche im Schlüssel-String selbst sind nicht erlaubt.

Paket-Capturing

Um Datenpakete zwecks Analyse von Störungen oder Problemen aufzuzeichnen, besteht die Möglichkeit, über ein Kommandozeilen-Tool den Befehl `lcoscap` auszuführen. Dieser Befehl aktiviert die Aufzeichnung der Pakete und schreibt die Ergebnisse in eine Datei, die Sie mit einem Tool wie z. B. „Wireshark" öffnen und analysieren können.

LCOS bietet Ihnen eine zusätzliche, deutlich komfortablere Methode: Wählen Sie in WEBconfig unter **Extras** > **LCOS-Menübaum** > **Setup** > **WLAN** > **Paket-Capture** > **WLAN-Capture-Format** ein Datenformat aus, in dem das Gerät Datenpakete ausgewählter Schnittstellen aufzeichnet und in eine Ergebnisdatei speichert.

Nach dem Festlegen der Parameter starten Sie unter **Extras** > **Paket-Capturing** mit einem Klick auf **Los!** das Paket-Capturing. Die erzeugte Datei können Sie anschließend z. B. mit „Wireshark" öffnen.



Diese Methode bietet Ihnen mehrere Vorteile:

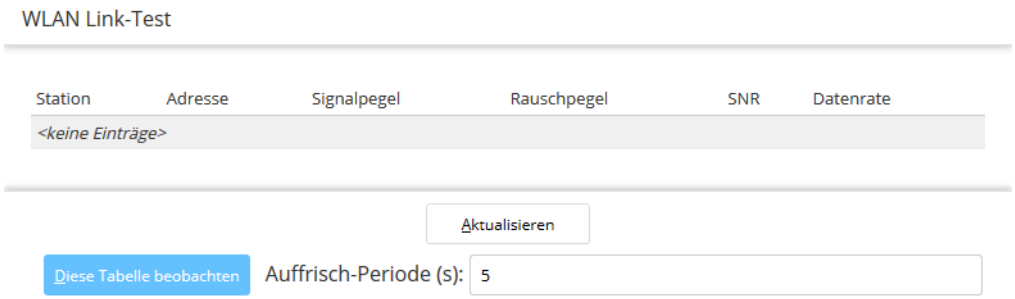
- Sie sind auf keine spezielle Software angewiesen, da Sie Webconfig auf beliebigen Web-Browsern ausführen können.
- Die Eingabe von Kommandozeilenbefehlen entfällt. Stattdessen stehen Ihnen komfortable Menü-Elemente zur Verfügung.
- Wenn Sie Webconfig über HTTPS betreiben, ist die Vertraulichkeit und Sicherheit des aufgezeichneten Datenverkehrs gewährleistet.

Das Paket-Capturing funktioniert sowohl mit IPv4- als auch mit IPv6-Verbindungen.

WLAN Link-Test

Dieser Menüpunkt ist nur auf Geräten mit WLAN-Modul verfügbar.

Diese Seite zeigt die Ergebnisse des WLAN Link-Tests an. Der WLAN Link-Test prüft die Verbindung zu verbundenen WLAN Clients.



Spectral Scan

Dieser Menüpunkt ist nur auf ausgewählten Geräten verfügbar.

Öffnet die Konfigurationsseite für Spectral Scan. Mehr über diese Funktion erfahren Sie unter *Spectral Scan* auf Seite 988.

TCP/HTTP-Tunnel erzeugen

Öffnet die Konfigurationsseite für das HTTP-Tunneling via TCP/IP. Mehr über diese Funktion erfahren Sie unter *TCP-Port-Tunnel* auf Seite 154.

Firmware in verwalteten Access Point laden

Dieser Menüpunkt ist nur auf WLAN-Controllern (WLCs) verfügbar.

Auf dieser Seite haben Sie die Möglichkeit, per Fernzugriff die Firmware auf einem vom WLC verwalteten Access Point manuell zu aktualisieren. Dies kann z. B. sinnvoll sein, um auf ausgewählten Access Points den Produktiveinsatz einer Firmware vorab zu testen. Wählen Sie dazu einen Access Point anhand seiner MAC-Adresse aus und wählen Sie die entsptechende Firmware-Datei. Klicken Sie anschließend auf **Starte Upload**, um die Firmware in den Access Point zu laden.

Beachten Sie, dass dieser Vorgang die Firmwareverwaltung in der Access Point-Tabelle für den ausgewählten Access Point deaktiviert. Dies verhindert, dass der WLC ggf. automatisch eine andere Firmware einspielt. Die Firmware-Verwaltung lässt sich im Setup-Menü unter **WLAN-Management** > **AP-Konfiguration** > **Verwalte-Firmware** jederzeit wieder aktivieren.

Damit der Access Point die geladene Firmware auch verwendet, müssen Sie anschließend einen Neustart des Gerätes durchführen. Durch Aktivieren der Einstellung **AP nach Aktualisierung der Firmware neustarten** veranlassen Sie einen automatischen Neustart, sobald der Firmware-Upload abgeschlossen ist.

Software-Option aktivieren

Sofern für Ihr Gerät zusätzliche Software-Optionen verfügbar sind, haben Sie nach Erwerb des dazugehörigen Aktivierungs- bzw. Registrierungsschlüssels auf dieser Seite die Möglichkeit, die dazugehörige(n) Option(en) freizuschalten.

Registrierungsschlüssel sind stets gerätespezifisch und lassen sich nicht auf andere Geräte übertragen. Heben Sie einen Schlüssel nach erfolgreicher Eingabe dennoch gut auf, um bei Bedarf (z. B. nach einer Reparatur) eine Option erneut freizuschalten.

Datum und Uhrzeit einstellen

Auf dieser Seite stellen Sie manuell das aktuelle Datum und die Uhrzeit ein. Alternativ können Sie auch einen Zeitserver verwenden, um die Uhrzeit zukünftig automatisch aktuell zu halten. Mehr dazu finden Sie unter *Zeit-Server für das lokale Netz* auf Seite 1654.

Das explizite Setzen von Datum und Uhrzeit ist für die korrekte Funktionsweise einiger Module (z. B. das Syslog- oder das Public Spot-Modul) unabdingbar!

Passwort ändern

Über diese Seite ändern Sie das Passwort für Ihren Benutzer-Account.

Neustart

Über diese Seite veranlassen Sie nach einem Klick auf die dazugehörige Schaltfläche einen Neustart des Gerätes. Dieser Befehl ist identisch mit dem unter **Extras** > **LCOS-Menübaum** > **Sonstiges** > **Kaltstart**.

2.2.2.11 Abmelden vom Gerät

Mit einem Klick auf den Menüpunkt **Logout** beenden Sie Ihre aktuelle WEBconfig-Sitzung und kehren zur Anmeldemaske des Gerätes zurück.

2.2.3 LANCOM Management Cloud (LMC)

Sie haben die Möglichkeit, eine Verbindung über die öffentliche LANCOM Management Cloud (public LMC) oder über eine privat gehostete Management Cloud (private Cloud) herzustellen.

2.2.3.1 Grundlagen der LANCOM Management Cloud

Die LANCOM Management Cloud (LMC) verwaltet beliebig große Netzwerke „software-defined“. Die LMC übernimmt die Konfiguration sämtlicher Netzwerkkomponenten und minimiert so den Kontrollaufwand und aufwändige Konfigurationen.

Weitere Informationen zur LANCOM Management Cloud finden Sie unter *www.lancom-systems.de/cloud*.

Wenn Sie die LANCOM Management Cloud für die Konfiguration und zur Überwachung Ihres Gerätes verwenden möchten, ist es erforderlich, das Gerät mit der LMC zu koppeln.

2.2.3.2 Koppeln von Geräten mit der LANCOM Management Cloud

In diesem Kapitel werden unterschiedliche Vorgehensweisen für das Koppeln von LANCOM Geräten mit der LMC beschrieben. Hierzu wird zwischen Cloud-ready-Geräten und Bestandsgeräten unterschieden.

Cloud-ready-Geräte sind LANCOM Geräte mit einer bereits vom Hersteller ausgelieferten LCOS-Version 10.0 oder höher (LANCOM Switches: Switch OS 3.30 oder höher) und besitzen eine PIN zur Kopplung mit der LMC. Die PIN finden Sie auf dem Beileger des jeweiligen Produktes.

Bestandsgeräte sind LANCOM Geräte, die von einer älteren LCOS-Version auf eine Version 10.0 (LANCOM Switches: Switch OS 3.30) oder höher aktualisiert wurden und mit dieser für die Verwaltung durch die LMC vorbereitet sind.

Besitzen Sie ein Cloud-Ready-Gerät, ist kein Pairing erforderlich. Fügen Sie in diesem Fall Ihr Gerät unter Angabe von Seriennummer und PIN Ihrem Konto in der LANCOM Management Cloud hinzu. Alternativ können Sie auch für Cloud-Ready-Geräte ein Pairing durchführen.

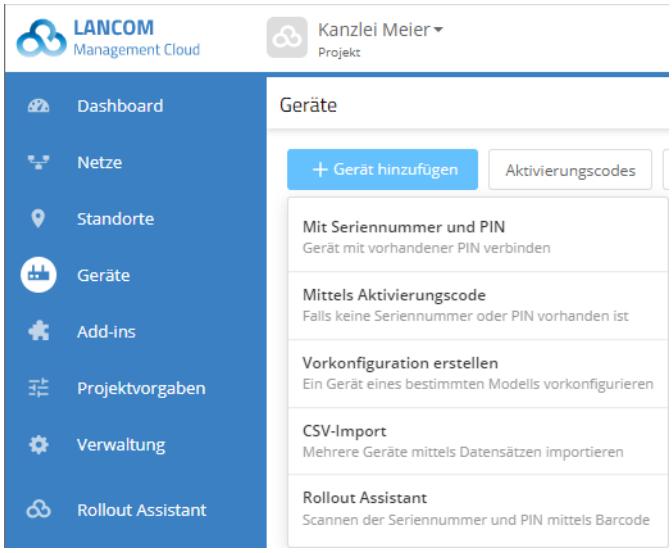
Im folgenden werden einige Pairing-Möglichkeiten beschrieben.

Aufnahme in die LMC über Seriennummer und Cloud PIN

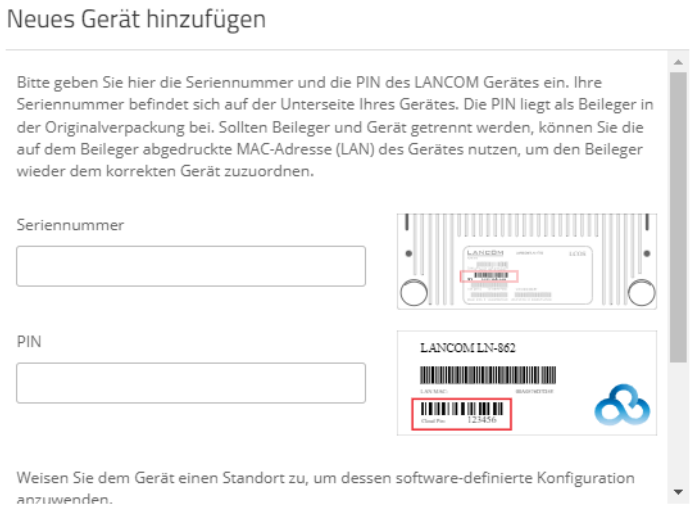
Sie können Ihr neues Gerät einfach einem Projekt in der LANCOM Management Cloud (Public) hinzufügen. Hierzu benötigen Sie die Seriennummer des Gerätes und die zugehörige Cloud PIN. Die Seriennummer finden Sie auf der Unterseite des Gerätes oder in LANconfig oder WEBconfig. Die Cloud PIN finden Sie auf dem Cloud-ready-Beileger, der dem Gerät beiliegt.



1. Öffnen Sie die Ansicht **Geräte** in der LANCOM Management Cloud und betätigen die Schaltfläche **Neues Gerät hinzufügen** und wählen anschließend die gewünschte Methode, hier **Mit Seriennummer und PIN**.



2. Im folgenden Fenster geben Sie die Seriennummer und die Cloud PIN des Gerätes an. Anschließend bestätigen Sie die Eingabe über die Schaltfläche **Gerät hinzufügen**.



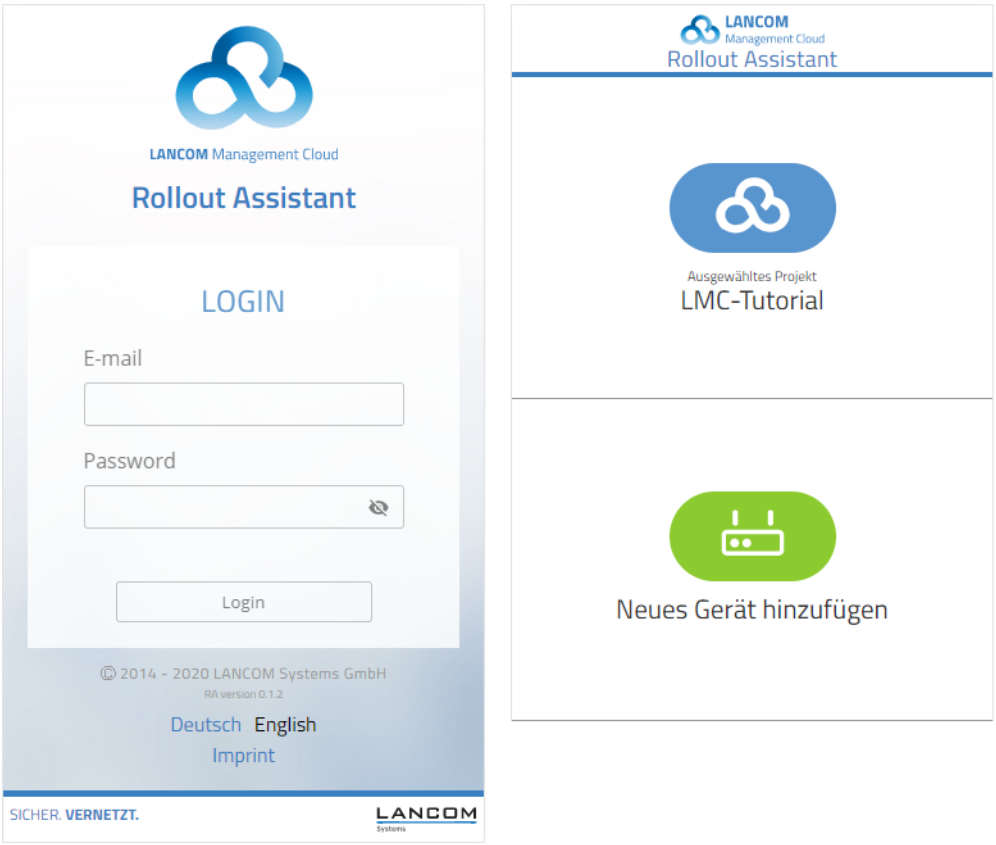
Das LANCOM Gerät wird sich bei dem nächsten Kontakt mit der LANCOM Management Cloud (Public) automatisch koppeln.

Aufnahme in die LMC über den LMC Rollout Assistant

Bei dem Rollout Assistant handelt es sich um eine Web-Applikation. Über den Rollout Assistant können Sie über ein Gerät mit Kamera und Internetzugang, z. B. einem Smartphone, Tablet oder auch einem Notebook, die Seriennummer und PIN einlesen. Damit verbinden Sie das Gerät auf einfachste Weise mit der LANCOM Management Cloud.

1. Geben Sie in einem Browser die URL *cloud.lancom.de/rollout* ein.

Es öffnet sich der Rollout Assistant mit diesem Login-Screen:



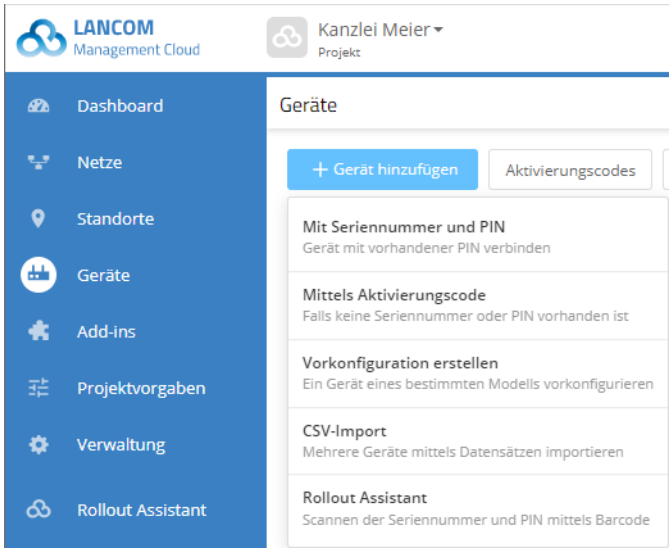
2. Wählen Sie unten die gewünschte Sprache aus und melden Sie sich mit Ihren LMC-Login-Daten an.
3. Auf der nächsten Seite wählen Sie zuerst das gewünschte Projekt aus und können danach neue Geräte zu diesem Projekt hinzufügen. Tippen Sie dazu auf die grüne Schaltfläche und beginnen Sie mit dem Einscannen der Seriennummer. Ggfs. müssen Sie hierfür dem Rollout Assistant den Zugriff auf die Kamera des Gerätes erlauben. Für den Scan können Sie die Seriennummer von der Unterseite des hinzuzufügenden Gerätes nehmen oder aber den auf dem Verpackungskarton aufgeklebten Barcode der Seriennummer verwenden. Alternativ geben Sie die Seriennummer manuell ein.
4. Als nächstes scannen Sie die Cloud-PIN von dem mit dem Gerät gelieferten Beileger ab. Auch hier können Sie die PIN optional manuell eingeben. Nun können Sie einen der in diesem Projekt vorhandenen Standorte auswählen oder optional diesen über **Kein Standort** noch offen lassen. Der Standort ist allerdings Voraussetzung für eine sinnvolle Konfiguration über SDN (Software-defined Networking).
5. Im nächsten Schritt weisen Sie dem Gerät bestimmte Eigenschaften zu. Sie vergeben einen Gerätenamen, geben eine Adresse ein und erstellen ein Installationsfoto. Die Adresse können Sie ebenfalls über die GPSInformationen Ihres Gerätes bestimmen.
6. Im letzten Schritt werden alle Angaben nochmals zur Kontrolle angezeigt. Sollte etwas nicht korrekt sein, gehen Sie einfach wieder zurück und korrigieren Sie die entsprechende Eingabe.
7. Mit **Gerät hinzufügen** wird das Gerät mit der LMC gekoppelt und Sie können dieses auch sofort in Ihrem Projekt sehen und ggfs. weitere Einstellungen vornehmen. Sobald Sie das Gerät anschließen, es also Verbindung mit der LMC aufnehmen kann, wird es basierend auf den SDN-Einstellungen mit einer ersten Betriebskonfiguration versorgt und der Status auf „Online“ wechseln.

Aufnahme in die LMC über Aktivierungscode

Über diese Methode können Sie in nur wenigen Schritten ein oder mehrere LANCOM Geräte gleichzeitig, aus LANconfig heraus, in die LANCOM Management Cloud aufnehmen.

Erstellen eines Aktivierungscodes

1. Öffnen Sie die Ansicht **Geräte** in der LANCOM Management Cloud und betätigen die Schaltfläche **Neues Gerät hinzufügen** und wählen anschließend die gewünschte Methode, hier **Mittels Aktivierungscode**.



2. Erstellen Sie einen Aktivierungscode, indem Sie dem Dialog folgen. Mit diesem Aktivierungscode können Sie das LANCOM Gerät später in dieses Projekt aufnehmen.

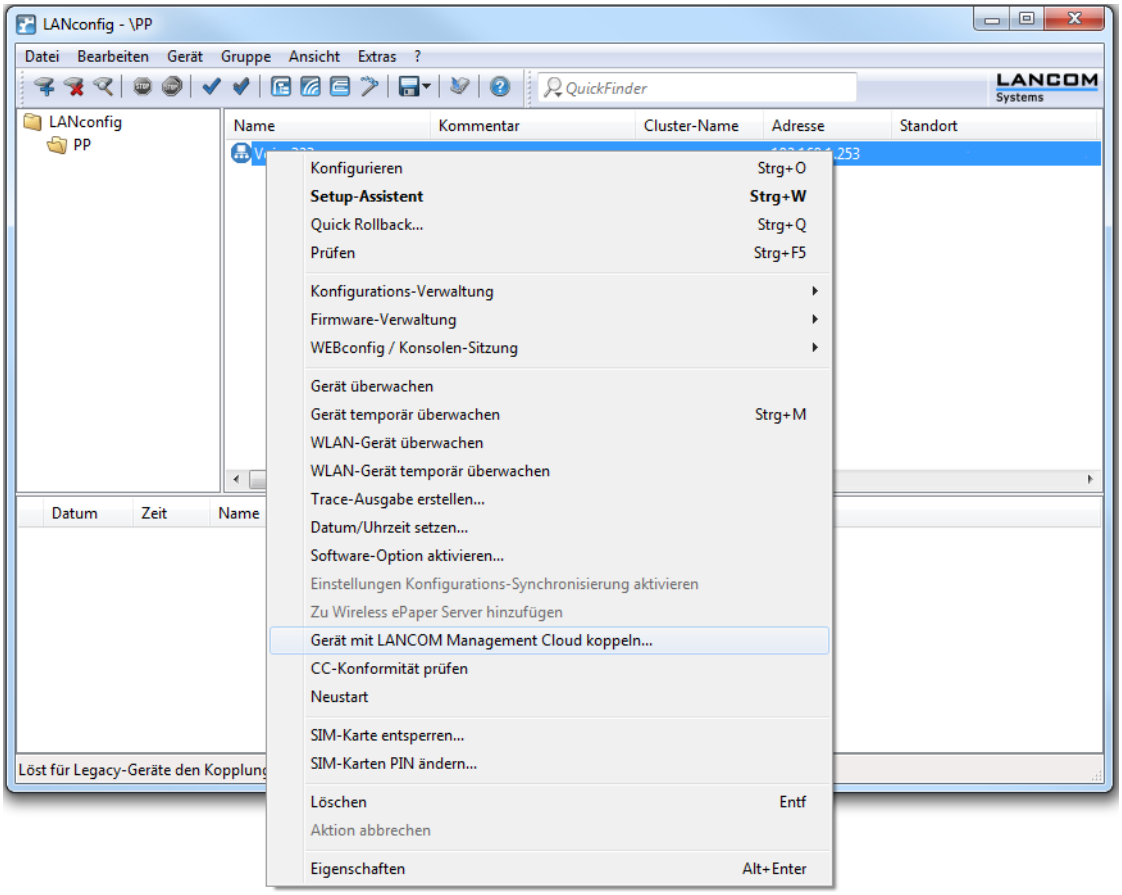
> Über die Schaltfläche **Aktivierungscodes** können Sie in der Ansicht Geräte jederzeit alle Aktivierungscodes für dieses Projekt einsehen.

Den Aktivierungscode können Sie in LANconfig, WEBconfig oder auf der Konsole für die Kopplung mit der LANCOM Management Cloud verwenden.

Koppeln von Geräten via LANconfig

1. Generieren Sie im ersten Schritt einen Aktivierungscode in der LANCOM Management Cloud.
2. Klicken Sie mit rechten Maustaste auf Ihr LANCOM Gerät.

3. Wählen Sie im Kontextmenü den Eintrag **Gerät mit LANCOM Management Cloud koppeln...** aus.



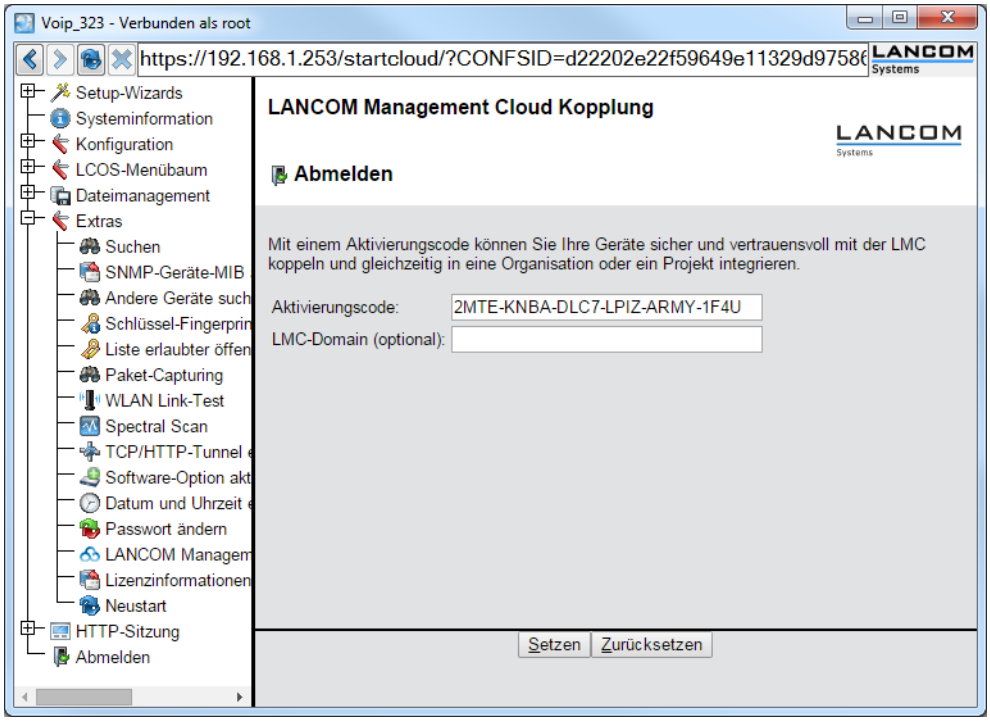
4. Folgen Sie den Anweisungen zur Eingabe des Aktivierungscodes.
Hier stehen drei Optionen zur Auswahl:

   - Public Cloud (Default): Sie verwenden die öffentliche LANCOM Management Cloud.
   - Private Cloud: Sie verwenden Ihre eigene Cloud.
   - Aktuell im Gerät gespeicherte Einstellungen verwenden: Je nach bereits vorhandener Konfiguration des Gerätes wird eine Public bzw. Private Cloud verwendet.



Koppeln von Geräten via WEBconfig

1. Starten Sie WEBconfig.
2. Geben Sie unter **Extras** > **LANCOM Management Cloud Kopplung** Ihren Aktivierungscode ein.



3. Klicken Sie die Schaltfläche **Setzen**.

Koppeln von Geräten via Konsole

Das Pairing über die Konsole erfolgt mit der Eingabe des Befehls `startlmc`.

1. Starten Sie eine Konsolensitzung.
2. Geben Sie den Pairing-Befehl mit dem Aktivierungscode als Parameter ein, z. B. `startlmc 2MTE-KNBA-DLC7-LPIZ-ARMY-1F4U`.

Sie erhalten eine Rückmeldung auf dem Bildschirm, ob der Pairing-Prozess erfolgreich gestartet wurde oder eine entsprechende Fehlermeldung.

2.2.3.3 Auslieferung der LMC-Domain durch den LCOS-DHCP-Server

Ab LCOS-Version 10.0 erhalten LCOS-Geräte bei der automatischen Zuweisung ihrer IP-Adresse durch den DHCP-Server zusätzlich eine in den DHCP-Paketen angegebene DHCP-Option 43.

Siehe *Parameter der LANCOM Management Cloud durch den DHCP-Server ausliefern* auf Seite 1640.

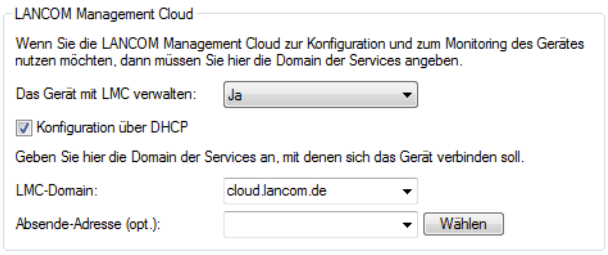
2.2.3.4 Manuelles Vorabkonfigurieren Ihres Gerätes für die Verwaltung durch die LANCOM Management Cloud

Hier erfahren Sie die notwendigen Schritte für die Konfiguration und das Monitoring Ihres Gerätes durch die LANCOM Management Cloud. Sie legen fest:

- ob Ihr Gerät durch die LMC zu verwalten ist.
- ob die LMC-Domain von einem DHCP-Server zu beziehen ist.
- mit welcher Domain sich Ihr Gerät verbindet.

- die Absende-Adresse (optional).

1. Navigieren Sie zu **Management** > **LMC**.



2. Wählen Sie unter **Das Gerät mit LMC verwalten:** zwischen drei Optionen:
   - **Nein**: Das Gerät stellt keine Verbindung zur LMC her.
   - **Ja**: Das Gerät wird von der LMC verwaltet. (Default für Geräte ohne WLAN-Schnittstelle)
   - **Nur ohne WLC**: Geräte innerhalb eines von einem WLC verwalteten Netzes bauen keine Verbindung zur LANCOM Management Cloud auf. (Default für Geräte mit WLAN-Schnittstelle)
3. Um die LMC-Domain von einem DHCP-Server zu beziehen, setzen Sie ein Häkchen in **Konfiguration über DHCP**.

   Um die LMC-Domain von einem DHCP-Server bereitzustellen, konfigurieren Sie am DHCP-Server innerhalb der DHCP-Option 43 die Sub-Option 18 mit der LMC-Domain. Weitere Informationen zur Konfiguration der LMC Parameter finden Sie im Abschnitt *Auslieferung der LMC-Domain durch den LCOS-DHCP-Server* auf Seite 46.
4. Wählen Sie unter **LMC-Domain** die Domain der LANCOM Management Cloud, mit der sich das Gerät verbinden soll.
5. Geben Sie optional unter **Absende-Adresse** eine Absendeadresse an, die statt der sonst automatisch für die Zieladresse gewählten Absendeadresse verwendet wird. Falls Sie z. B. eine Loopback-Adresse konfiguriert haben, können Sie diese hier als Absendeadresse angeben.

2.2.4 Terminalprogramm

Ihr Gerät unterstützt den kommandozeilen-basierten Zugriff durch ein Terminalprogramm über verschiedene Schnittstellen (wie [W]LAN, [W]WAN oder Serial) und Protokolle (wie Telnet, SSH oder TFTP) hinweg. Durch die Installation eines geeigneten Clients haben Sie somit die Möglichkeit, unabhängig von einer grafischen Benutzeroberfläche an der LCOS-Konsole Gerätedaten auszulesen, zu verändern und zu analysieren, und mittels selbstgeschriebener Skripte diese Vorgänge für mehrere Geräte zu automatisieren, um z. B. via Fernkonfiguration mehrere Geräte in einem Arbeitsschritt zu warten.

In Windows gibt es keinen Telnet-Client als Bestandteil des Betriebssystems. Sie können aber auf eine alternative Software wie z. B. den freien Multi-Protokoll-Client PuTTY ausweichen. PuTTY selbst ist sowohl für Windows- als auch Linux-Betriebssysteme erhältlich.

2.2.4.1 Terminalsitzung starten

Bei vielen Betriebssystemen starten Sie eine Terminalsitzung an der Kommandozeile mit einer Befehlskombination aus dem verwendeten Protokoll und der zu verbindenen IP-Adresse. Je nach Protokoll oder Client kann es jedoch einzelne Abweichungen geben. Die genaue Syntax entnehmen Sie bitte daher der dazugehörigen System- bzw. Programmdokumentation.

Nachfolgend finden Sie für ausgewählte Protokolle und Systeme gängige Befehle:

Telnet

Aus der Windows-Kommandozeile oder dem Linux-Terminal starten Sie eine Telnet-Sitzung mit dem Befehl `telnet <host>`. Telnet baut dann eine (unverschlüsselte) Verbindung zum Gerät mit der eingegebenen IP-Adresse auf. Nach

der Eingabe des Passworts – sofern Sie eines zum Schutz der Konfiguration vereinbart haben – stehen Ihnen alle Konfigurationsbefehle zur Verfügung.

Linux-Systeme unterstützen auch Telnet-Sitzungen über SSL-verschlüsselte Verbindungen. Je nach Distribution ist es dazu ggf. erforderlich, die Standard-Telnet-Anwendung durch eine SSL-fähige Version zu ersetzen bzw. einen SSL-fähigen Clienten nachzuinstallieren (z. B. telnet-ssl). Bei Distributionen mit integrierter Telnet-über-SSL-Unterstützung starten Sie eine verschlüsselte Telnet-Verbindung mit dem Befehl `telnet -z ssl <host> <port>`.

SSH

In Windows ist standardmäßig kein SSH-Client integriert. Unter Linux-Systemen nutzen Sie den Befehl `ssh <login-name>@<host>`, um eine verschlüsselte Verbindung zum Gerät herstellen und die bei der Konfiguration übertragenen Daten so vor dem Abhören innerhalb des Netzwerks schützen.

2.2.4.2 Sprache der Konsole ändern

Die Konsole Ihres Gerätes stellt Ihnen verschiedene Sprachen zur Verfügung. Werkseitig ist das Gerät auf „Englisch" als Konsolensprache eingestellt. Im weiteren Verlauf dieser Dokumentation sind Pfadangaben jedoch in ihrer deutschen Form angegeben. Um die Konsolensprache temporär, d. h. für die Dauer der Sitzung, zu verändern, verwenden Sie an der Konsole den `lang`-Befehl, gefolgt von der dazugehörigen Sprache oder deren Anfangsbuchstabe(n); also z. B. `lang Deutsch` oder `lang de`.

Folgende Spracheingaben werden derzeit von der Konsole unterstützt:

- `Deutsch`
- `English`

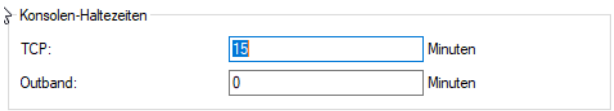
Um die bei der Anmeldung gewählte Standard-Sprache **dauerhaft** zu verändern, legen Sie im Setup-Menü unter **Config** > **Sprache** die gewünschte Sprache fest. Die in dem dazugehörigen Auswahlmenü befindlichen Sprachen stellen alle möglichen Spracheingaben dar, die Ihr Gerät zum gegenwärtigen Zeitpunkt unterstützt.

2.2.4.3 Terminalsitzung beenden oder abbrechen

Um eine Terminalsitzung zu beenden, geben Sie an der Konsole den Befehl `exit` ein.

Unter Linux-Systemen und manchen Clients (wie z. B. PuTTY) können Sie darüber hinaus die Tastenkombination `Strg+C` verwenden, um eine Terminalsitzung abzubrechen, falls ein Beenden mittels `exit` nicht möglich ist wie z. B. während des Anmeldevorgangs mit Passworteingabe.

Die Verbindung wird auch automatisch beendet, wenn über einen Zeitraum keine Aktivität mehr festgestellt wird. Den Zeitraum können Sie unter **Management** > **Erweitert** im Bereich **Konsolen-Haltezeiten** einstellen.



TCP

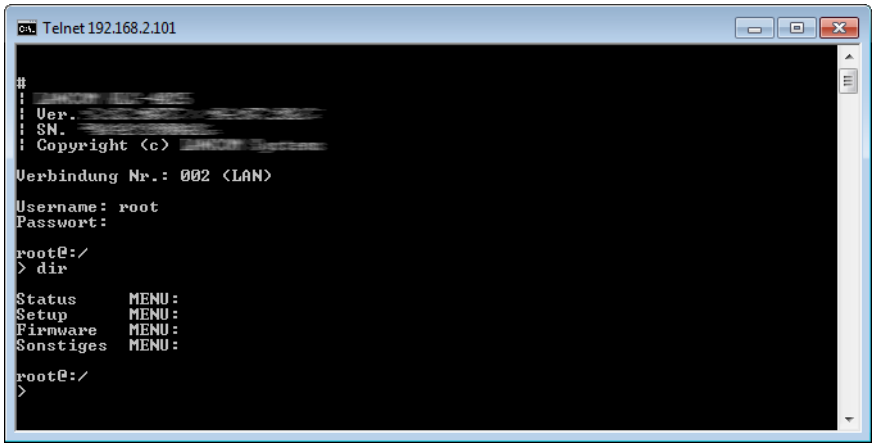
Hier können Sie angeben, nach wieviel Minuten der Inaktivität eine TCP-Verbindung (z. B. SSH-Verbindung) automatisch beendet wird.

Outband

Hier können Sie angeben, nach wieviel Minuten der Inaktivität eine serielle Verbindung (z. B. Hyper Terminal) automatisch beendet wird.

2.2.4.4 Die Menüstruktur der Konsole

Das LCOS-Kommandozeilen-Interface (die Konsole) ist wie folgt strukturiert:



Status

Enthält die Zustände und Statistiken aller internen Module des Gerätes sowie den Direktzugriff auf das Dateisystem.

Setup

Beinhaltet alle einstellbaren Parameter aller internen Module des Gerätes.

Firmware

Beinhaltet das Firmware-Management.

Sonstiges

Enthält Aktionen für Verbindungsauf- und -abbau, Reset, Reboot und Upload.

2.2.4.5 Befehle für die Konsole

Das LCOS-Kommandozeilen-Interface wird mit den folgenden Befehlen bedient. Die verfügbaren Menübefehle lassen sich z. T. auch durch Aufrufen des HELP-Kommandos auf der Kommandozeile anzeigen.

Die verfügbaren Befehle sind abhängig vom Funktionsumfang des jeweiligen Gerätes.

Zum Ausführen einiger Befehle sind spezielle Rechte erforderlich, die beim jeweiligen Befehl aufgeführt sind. Befehle ohne Angabe von Rechten besitzen keine Einschränkungen.

Tabelle 2: Übersicht aller auf der Kommandozeile eingebbaren Befehle

Befehl	Beschreibung
`add|set [<Path>] <Value(s)>`	Setzt einen Konfigurationsparameter auf einen bestimmten Wert. Handelt es sich beim Konfigurationsparameter um einen Tabellenwert, so muss für jede Spalte ein Wert angegeben werden. Dabei übernimmt das Zeichen `*` als Eingabewert einen vorhandenen Tabelleneintrag unverändert. **Zugriffsrecht**: Supervisor-Write,Local-Admin-Write,Limited-Admin-Write
`add|set [<Path>] ?`	Listet alle möglichen Eingabewerte für einen Konfigurationsparameter auf. Wird kein spezifischer Pfad angegeben, so werden die möglichen Eingabewerte für alle Konfigurationsparameter im aktuellen Verzeichnis angegeben. **Zugriffsrecht**: Supervisor-Write,Local-Admin-Write,Limited-Admin-Write

Befehl	Beschreibung
`beginscript [-u] [-C d] [-s <password>]`	Versetzt eine Konsolensitzung in den Skript-Modus. In diesem Zustand werden die im Folgenden eingegebenen Befehle nicht direkt in den Konfigurations-RAM des Geräts übertragen, sondern zunächst in den Skript-Speicher. Mögliche Optionsschalter sind: › `-u`: Erzwingt die unbedingte ("**u**nconditional") Ausführung eines Skriptes oder einer Konfiguration. › `-C d`: Überspringt die standardmäßige Differenzprüfung ("**C**heck for **d**ifference"). Gilt auch, wenn die Option `-u` gesetzt ist. › `-s`: Entschlüsselt die Skript-Datei auf Basis des bei `readscript -s` angegebenen Passwortes. **Zugriffsrecht**: Supervisor-Write
`bootconfig [-s (1|2|all)] [-r (1|2|all)]`	Ermöglicht das Speichern und Löschen von Boot-Konfigurationen. Mögliche Optionen sind: › `-s`: Speichert die aktuelle Konfiguration eines Gerätes wahlweise als kundenspezifische Standard-Einstellung (1), Rollout-Konfiguration (2) oder beides (all). › `-r`: Löscht wahlweise die aktuelle kundenspezifische Standard-Einstellung (1), die Rollout-Konfiguration (2) oder beide (all). **Zugriffsrecht**: Supervisor-Write ⓘ Weitere Informationen zu Boot-Konfigurationen finden Sie im Kapitel *Alternative Boot-Konfiguration* auf Seite 84
`cd <Path>`	Wechselt das aktuelle Verzeichnis. Verschiedene Kurzformen werden unterstützt, z. B. `cd ../..` kann verkürzt werden zu `cd ...` etc.
`clear`	Löscht die aktuelle Konsolenausgabe. Im Log lassen sich weiter alle bisher eingegebenen Befehle einsehen.
`default [-r] [<Path>]`	Setzt einzelne Parameter, Tabellen oder ganze Menübäume in die Grundkonfiguration zurück. Zeigt `<Path>` auf einen Zweig des Menübaums, muss zwingend die Option `-r` (recursive) angegeben werden. **Zugriffsrecht**: Supervisor-Write
`del|delete|rm [<Path>] <Row>|*`	Löscht die Tabellenzeile `<Row>` in der aktuellen Tabelle bzw. in der mittels `<Path>` im Zweig des Menübaums referenzierten Tabelle. Als `<Row>` geben Sie dabei die Nummer der Zeile an. Das Wildcard-Zeichen `*` leert eine Tabelle, z. B. `del Config/Cron-Tabelle *`. **Zugriffsrecht**: Supervisor-Write,Local-Admin-Write,Limited-Admin-Write
`deletebootlog`	Löscht den Inhalt des persistenten Bootlog-Speichers.
`dir|list|ls|llong|l [-a] [-r] [-s] [<Path>] [<Filter>]`	Zeigt den Inhalt des aktuellen Verzeichnisses an. Mögliche Optionsschalter sind: › `-a`: Gibt zusätzlich zu den Inhalten der Abfrage auch die zugehörigen SNMP-IDs aus. Dabei beginnt die Ausgabe mit der SNMP-ID des Gerätes, gefolgt von der SNMP-ID des aktuellen Menüs. Vor den einzelnen Einträgen finden Sie dann die SNMP-IDs der Unterpunkte. › `-r`: Listet auch alle Unterverzeichnisse sowie die darin befindlichen Tabellen auf.

Befehl	Beschreibung
	› `-s`: Sortiert die Anzeige des aktuelles Verzeichnisses; gruppiert nach Unterverzeichnissen, Tabellen, Werten und Aktionen; jeweils in aufsteigender alphabetischer Reihenfolge.

`dnsquery [-t <type>] [-d <destination>] name[@rtg-tag]`	Löst DNS-Anfragen auf. Mögliche Parameter:
	› `name`: Der aufzulösende DNS-Name.
	› `@rtg-tag`: Optionales Routing Tag, um die DNS-Server erreichen zu können.
	› `-t <type>`: Typ: A, AAAA, PTR, SRV, NAPTR
	› `-d <destination>`: Ziel, über das die DNS-Server erreicht werden können.
	Wie in der Weiterleitungs-Tabelle kann auch ein Routing-Tag mit angegeben werden, wenn das Weiterleitungsziel eine IP-Adresse ist (z. B. 8.8.8.8@4095). Außerdem können auch zwei kommaseparierte IP-Adressen (mit optionalem Routing-Tag) angegeben werden (z. B. 8.8.4.4@4095,8.8.8.8@4095). Der DNS-Client wechselt dann zwischen den Servern, wenn einer nicht antwortet
	Wird das Kommando ohne Optionen, also nur mit dem obligatorischen Domainnamen, aufgerufen, dann wird sowohl eine Anfrage vom Typ AAAA als auch eine vom Typ A gemacht. Beispiel:
	`> dnsquery www.lancom.de`
	
	`DNS result:`
	`==========`
	`www.lancom.de: type A, class IN, ttl 1 hour, addr 176.9.82.168`
	`www.lancom.de: type AAAA, class IN, ttl 1 hour, addr 2a01:4f8:151:20a3::2`
	ⓘ Die Antwort vom Typ AAAA wird nur ausgegeben, wenn die IPv6-Adresse auch erreichbar ist.
	Der Typ kann auch explizit über die Option `-t` angegeben werden. Möglich sind dabei AAAA, A, PTR, SRV und NAPTR. Bei einer PTR-Anfrage muß die angefragte IP-Adresse direkt angegeben werden und darf nicht in den „ARPA"-String gewandelt werden:
	`> dnsquery -tptr 176.9.82.168`
	
	`DNS result:`
	`==========`
	`168.82.9.176.in-addr.arpa: type PTR, class IN, ttl 5 hours, 32 minutes, 30 seconds, www.lancom-systems.de`
	Da das dnsquery-Kommando den DNS-Client des LANCOM Gerätes benutzt, wird sein Verhalten über die DNS-Konfiguration des Gerätes bestimmt (also Weiterleitungen, Loopback-Adressen etc.). Da sich die DNS-Konfiguration abhängig vom Routing-Tag unterscheiden kann, kann beim dnsquery Kommando das zu verwendende Tag per @-Erweiterung an den angefragten Namen (oder bei PTR-Anfragen an die angefragte Adresse) angehängt werden:
	`> dnsquery www.lancom.de@4095`
	
	`DNS result:`
	`==========`
	`www.lancom.de: type A, class IN, ttl 1 hour, addr 176.9.82.168`
	`www.lancom.de: type AAAA, class IN, ttl 1 hour, addr 2a01:4f8:151:20a3::2`
	Es ist aber auch möglich, die Anfragen an der Weiterleitungskonfiguration vorbei zu senden, indem über den Parameter -d eine Zialangabe gemacht wrid. Als Zielangabe ist alles möglich, was auch in der Weiterleitungs-Tabelle als Ziel angegeben werden kann. Zudem wird auch bei einer manuellen Zielvorgabe die Loopback-Adresse entsprechend der Loopback-Konfiguration bestimmt. Beispiel: AAAA+A Anfrage über WAN-Verbindung INTERNET
	`> dnsquery -dinternet www.lancom.de`
	
	`DNS result:`
	`==========`
	`www.lancom.de: type A, class IN, ttl 1 hour, addr 176.9.82.168`
	`www.lancom.de: type AAAA, class IN, ttl 1 hour, addr 2a01:4f8:151:20a3::2`

Befehl	Beschreibung

	Dazu muß der WAN-Verbindung INTERNET natürlich ein DNS-Server zugewiesen worden sein, z. B. per PPP, DHCP oder manuell in der IP-Parameter-Liste.
	
	Beispiel: PTR-Anfrage über Google-Server
	`> dnsquery -d8.8.8.8 -tptr 176.9.82.168`
	
	`DNS result:`
	`==========`
	`168.82.9.176.in-addr.arpa: type PTR, class IN, ttl 5 hours, 32 minutes, 30 seconds, www.lancom-systems.de`
	
	Wenn kein Server andwortet macht der Client drei Wiederholungen mit sich erhöhender Wartezeit, d. h. nach jeder gesendeten Anfrage wartert er 1, 2, 4 und beim letzten Mal 8 Sekunden. Kommt bis dann keine Antwort, so wird die Anfrage abgebrochen. Wenn während einer laufenden Anfrage <CR> gedrückt wird, so wird diese abgebrochen.

`do <Path> [<Parameter>]`	Führt die angegebene Aktion im aktuellen bzw. referenzierten Verzeichnis aus, z. B. `do Sonstiges/Kaltstart`. Sofern die Aktion über zusätzliche Parameter verfügt, lassen sich diese nachfolgend angeben.
`echo <Argument>`	Gibt ein Argument auf der Konsole aus.
`enable <Parameter>`	Erweitert die Rechte von angemeldeten TACACS+-Benutzern. Mögliche Parameter sind: › `0`: Keine Rechte › `1`: Read-Only › `3`: Read-Write › `5`: Read-Only-Limited Admin › `7`: Read-Write-Limited Admin › `9`: Read-Only Admin › `11`: Read-Write Admin › `15`: Supervisor (Root)
`ethping -i <Schnittstelle> [-?] [-c Anzahl] [-v VLAN] [-s Groesse] [-l MD-Level] <Zieladdresse>`	CFM-Ethernet-Ping.Siehe auch *Kommandos auf der Konsole* auf Seite 1744.
`exit|quit|x`	Beendet die Terminalsitzung.
`feature <Code>`	Schaltet eine Software-Option mit dem angegebenen Aktivierungsschlüssel frei. **Zugriffsrecht**: Supervisor-Write **Optionen:** **Feature <Aktivierungsschlüssel>** Aktivierung mit Aktivierungsschlüssel **Feature -Q** Abfrage des Status aktueller und vergangener Fernaktivierungsanfragen **Feature -q** <query-id> Abfrage des Status einer einzelnen Anforderung Feature -l <Lizenz-Schlüssel> -t <Lizenz-Typ> [-i <Lizenz-Index>] [-a <Quell-Adresse>] [-u <Server-URL>] [-c <Kontaktinformationen>] startet eine neue Fernaktivierungsanforderung. Der Fortschritt kann mit -q/-Q verfolgt werden **-a <Quell-Adresse>** Quell-IP-Adresse oder Schnittstelle, z.B. INT, DMZ, LBx

Befehl	Beschreibung
	-l <Lizenz-Schlüssel> 16/19 Zeichen langer Lizenzschlüssel **-t <Lizenz-Typ>** Typ der Lizenz, z.B. VPN25 **-i <Lizenz-Index>** Index der vorhandenen Lizenz für die Erweiterung, 0 für zusätzliche Lizenz **-u <Server-URL>** URL des Lizenzservers **-c <Kontaktinformationen>** kommagetrennte Liste von Kontaktinformationen
`find <Begriff>`	Sucht nach dem <Begriff> und gibt alle Menüeinträge aus, die den Suchbegriff enthalten.
`flash yes|no`	Regelt die Speicherung von Konfigurationsänderungen über die Kommandozeile. Die Änderungen an der Konfiguration über die Befehle an der Kommandozeile werden standardmäßig (`yes` bzw. `ja`) direkt in den boot-resistenten Flash-Speicher der Geräte geschrieben. Wenn das Aktualisieren der Konfiguration im Flash unterdrückt wird (`no` bzw. `nein`), werden die Änderungen nur im RAM gespeichert, der beim Booten gelöscht wird. **Zugriffsrecht**: Supervisor-Write
`getenv <Name>`	Gibt den Wert der betreffenden Umgebungsvariable aus (ohne Zeilenvorschub). Beachten Sie dazu auch den Befehl 'printenv'.
`history`	Zeigt eine Liste der letzen ausgeführten Befehle. Mit dem Befehl `!#` können die Befehle der Liste unter Ihrer Nummer (#) direkt aufgerufen werden: Mit `!3` wird z. B. der dritte Befehl der Liste ausgeführt.
`ikectl [-[r|d|D] <peer-name-list>] [-[e|r|d] <ipsec-name-list>] [-[r|d] [<ike-cookies-list>|<esp-spi-list>]] [-R <peer-name-list> <redirect-target>]`	Dieser Befehl erweitert die Analyse-Möglichkeiten, indem z. B. in einem Fehlerfall gezielt Aktionen durchgeführt werden, mit denen sich ein Problem eingrenzen lässt. Diese Funktion erlaubt es u. a., ein VPN schnell automatisiert zu modifizieren und zu testen. › `-e <ipsec-name-list>`: Erzeugt eine Phase 2-SA / CHILD_SA unter Angabe des VPN-Regelnamens › `-r <peer-name-list>`: Führt ein Rekeying der Phase 1-SA / IKE_SA unter Angabe des Namens der VPN-Gegenstelle durch › `-r <ike-cookies-list>`: Führt ein Rekeying unter Angabe des IKE-Cookies durch › `-r <ipsec-name-list>`: Führt ein Rekeying der Phase 2-SA / Child_SA unter Angabe des VPN-Regelnamens durch › `-r <esp-spi-list>`: Führt ein Rekeying der Phase 2-SA / Child_SA unter Angabe der eingehenden oder ausgehenden ESP-SPI durch › `-d <peer-name-list>`: Löscht eine Phase 1-SA / IKE_SA unter Angabe des Namens der VPN-Gegenstelle › `-d <ike-cookies-list>`: Löscht eine Phase 1-SA / IKE_SA unter Angabe von IKEv1-Cookies / IKEv2 SPIs › `-d <ipsec-name-list>`: Löscht eine Phase 2-SA / CHILD_SA unter Angabe des VPN-Regelnamens › `-d <esp-spi-list>`: Löscht eine Phase 2-SA / Child_SA unter Angabe der eingehenden bzw. ausgehenden ESP-SPI › `-D <peer-name-list>`: Start der Liveness-Check-Prozedur (Dead Peer Detection – DPD) unter Angabe des Namens der VPN-Gegenstelle › `-R <peer-name-list> <redirect-target`: Leitet IKEv2-Gegenstellen per IKEv2-Redirect-Mechanismus zu einem neuen Ziel um. Falls die Gegenstellen-Liste leer ist, werden alle Gegenstellen umgeleitet. Mit

Befehl	Beschreibung
	diesem Befehl können VPN-Gegenstellen zu Wartungszwecken von dem aktuellen VPN-Gateway auf ein anderes Gateway sicher verschoben werden. › `<peer-name-list>`: Durch Leerzeichen getrennte Liste von Gegenstellennamen aus aus max. 16 Zeichen › `<ipsec-name-list>`: Durch Leerzeichen getrennte Liste von Namen der VPN-Regeln, wie sie in „show vpn“ als ipsec-0-PEER-pr0-l0-r0 angezeigt werden. Um eine bestimmte CHILD_SA / Phase 2-SA eines road-warrior zu finden, ist es wichtig, auch den Gegenstellennamen wie folgt anzugeben: `"peer-name ipsec-name"`. › `<ike-cookies-list>`: Besteht aus einer durch Leerzeichen getrennten Liste von jeweils 16 hexadezimalen Werten, z. B. 0x00010203040506070809 0A0B0C0D0E0F › `<esp-spi-list>`: Besteht aus einer durch Leerzeichen getrennten Liste von jeweils 4 hexadezimalen Werten, z. B. 0x00010203 › `<redirect-target>`: Ziel, zu dem die Gegenstelle(n) umgeleitet werden sollen. Ziel kann eine IPv4-Adresse, IPv6-Adresse oder ein DNS-Name sein Beispiel: `ikectl -r peer ipsec-name-peer-2 -D peer3 -d peer4 0x12345678 -e "RoadWarrior IPSEC-0-DEFAULT-PR0-L0-R0"`
`importfile -a <application> [-p <passphrase>] [-n] [-h <Hash> -f <Fingerprint>] [-c] [-r]`	Ihr Gerät unterstützt das Laden von Dateien in Datei-Slots sowohl von der Konsole als auch aus einem Skript. Somit können Dateien komfortabel per Skript zusammen mit der Konfiguration ausgerollt oder z. B. SSH-Schlüssel und VPN-Zertifikate importiert werden. **Notwendige Parameter:** **-a <application>** <application> bestimmt den Speicherort und somit die Nutzung für die eingegebenen Daten. Für eine vollständige Liste der in Ihrem Gerät vorhandenen Speicherorte geben Sie importfile -? ein. **Optionale Parameter:** **-n** -n startet den nicht-interaktiven Modus. Es gibt keine Eingabeaufforderungen oder andere Ausgaben auf der CLI. Der nicht-interaktive Modus ist für die Nutzung in Skripten vorgesehen. **-p <passphrase>** <passphrase> ist das Passwort, was zum Entschlüsseln eines eingegebenen privaten Schlüssels benötigt wird. **-h <hash>** Der Hash-Algorithmus, mit dem der Fingerprint des Root-CA-Zertifikats ermittelt wurde. **-f <fingerprint>** Der Fingerprint des Root-CA-Zertifikats, erstellt mit –h. Der Fingerprint kann sowohl mit Doppelpunkten eingegebenen werden, als auch ohne. **-c** Es werden nur CA-Zertifikate hochgeladen. **-r** Hochgeladene CA-Zertifikate ersetzen bereits vorhandene.

Befehl	Beschreibung
`iperf [-s|-c <Host>] [options]`	Startet iPerf auf dem Gerät, um eine Bandbreitenmessung mit einer iPerf2-Gegenstelle durchzuführen. Mögliche Optionsschalter sind: › **Client/Server** › `-u, --udp`: Verwendet UDP statt TCP. › `-p, --port <Port>`: Verbindet mit oder erwartet Datenpakete auf diesem Port (Standard: 5001). › `-q, --quiet`: Setzt den quiet-Modus bei dem der CLI-Output unterdrückt wird, da der Befehl auch über die Aktionstabelle aufgerufen werden kann. Außerdem wird im Client-Modus verhindert, dass die Ausführung abgebrochen werden kann. › **Server-spezifisch** › `-s, --server`: Startet iPerf im Server-Modus und wartet auf die Kontaktaufnahme durch einen iPerf-Client. › **Client-spezifisch** › `-c, --client <Host>`: Startet iPerf im Client-Modus und verbindet mit dem iPerf-Server <Host> (IP-Adresse oder DNS-Name). › `-b, --bandwidth [<Bandw>/]<Bandw>{kKmM}`: Begrenzung der Bandbreite bei der Analyse einer UDP-Verbindung im [Down-]/Up-Stream. Die Angabe erfolgt in Kilo- (kK) oder Megabyte (mM) pro Sekunde (Standard: 1 Mbps). › `-l, --len <Length>`: Bestimmt die Länge der UDP-Datenpakete. › `-t, --time <Time>`: Bestimmt die Dauer der Verbindung in Sekunden (Standard: 10 Sekunden). › `-d, --dualtest`: Der Test erfolgt bidirektional: iPerf-Server und -Client senden und empfangen dabei gleichzeitig. › `-r, --tradeoff`: Der Test erfolgt sequentiell: iPerf-Server und -Client senden und empfangen nacheinander. › `-R, --reverse`: Kehrt die Messrichtung um. › `-L, --listenport <Port>`: Gibt den Port an, auf dem das Gerät im bidirektionalen Betrieb Datenpakete vom entfernten iPerf-Server erwartet (Standard: 5001). › `-P, --parallel <Number>`: Anzahl der parallel auszuführenden Client-Aufträge (Maximum: 20). › `-B, --bind <Interface>`: Erlaubt die Verbindung nur über die angegebene Schnittstelle (IP-Adresse oder Schnittstellenname). › `-E, --peer <Interface>`: Verbindung über die mit dem Peer-Namen angegebene Schnittstelle herstellen und rx/tx-Grenzwerte auf der Grundlage des Ergebnisses/der Ergebnisse festlegen. Wenn nicht im Dual- oder Tradeoff-Modus ausgeführt, wird der Wert der nicht gemessenen Richtung entsprechend der letzten Messung festgelegt, sofern verfügbar. Das Ergebnis wird in der Statustabelle **Status** > **Iperf** > **Last-Results** > **Peer-Result** (1.96.1.3) in den Werten **Peer**, **Server-Bandwidth-kbps** und **Client-Bandwidth-kbps** eingetragen. › `--retry #`: Anzahl der Wiederholungsversuche, wenn keine Verbindung möglich ist. Maximum: 99. › `--force`: Wenn bereits eine andere Client-Instanz läuft, wartet das System, bis diese beendet ist, bevor es fortfährt.

Befehl	Beschreibung
	› `--ratediffperc #`: Maximal erlaubte Ratenabweichung in Prozent im Peer-Modus (Maximum: 99). › `--expbandwidth #/#{kKmM}`: Erwartete Down- / Up-Stream-Bandbreite im Peer-Modus. Werte für nicht gemessene Richtungen werden ignoriert. Beispiel: 10/10M › `--minbandwidth #{kKmM}`: Setzt den angegeben Wert, falls die Messung einen niedrigeren Wert ermittelt hat. › **Verschiedenes** › `-h, --help`: Gibt den Hilfetext aus.
`killscript <Name>`	Löscht den noch nicht verarbeiteten Inhalt einer Skript-Session. Die Skript-Session wählen Sie über deren Namen aus. **Zugriffsrecht**: Supervisor-Write
`language`	Wählt eine Sprache für die Konsolen-Anzeige aus. Der Befehl `language ?` listet die verfügbaren Sprachen auf.
`lig [[-i <instance>] | [-m <server>]] [-id <num>] destination-eid [-retries <num>] [-rtg-tag <num>] [-source-eid <num>]`	LIG (Locator/ID Separation Protocol Internet Groper) ist ein in RFC 6835 spezifiziertes Kommandozeilentool um LISP Mappings bei einem Map-Resolver abzufragen. Mögliche Optionsschalter sind: › `-i <instance>`: Name der LISP-Instanz, die für die Zielabfrage verwendet wird › `-m <server>`: LISP Map-Server, der für die Zielabfrage verwendet wird › `-id <num>`: LISP-Instanz-ID [0-16777215], die für die Zielabfrage verwendet wird › `destination-eid`: Abgefragte Ziel-EID › `-retries <num>`: LISP-Wiederholungen zum Map-Server [0-10] › `-rtg-tag <num>`: Verwendetes Routing-Tag › `-source-eid <num>`: Verwendete Source-EID Bespiel: `lig -i LISP-INST 172.16.200.1`
`linktest`	Nur auf WLAN-Geräten verfügbar. Zeigt die Ergebnisse des WLAN Link-Tests an. **Zugriffsrecht**: Supervisor-Write **Ausführungsrecht**: WLAN-Linktest
`ll2mdetect`	Sucht Geräte per LL2M im LAN. Weitere Informationen zu dem Befehl erhalten Sie gesondert im Abschnitt *Befehle für den LL2M-Client* auf Seite 78. **Zugriffsrecht**: Supervisor-Write
`ll2mexec`	Sendet ein Kommando per LL2M an ein Gerät im LAN. Weitere Informationen zu dem Befehl erhalten Sie gesondert im Abschnitt *Befehle für den LL2M-Client* auf Seite 78. **Zugriffsrecht**: Supervisor-Write
`loadconfig (-s <Server-IP-Addresse> -f <Dateiname>)|<URL>`	Lädt eine Konfigurationsdatei via TFTP in das Gerät. Geben Sie dazu wahlweise die Server-Adresse und den Dateinamen oder die komplette URL an. Weitere Informationen zu dem Befehl erhalten Sie gesondert im Abschnitt *Datei-Download von einem TFTP- oder HTTP(S)-Server* auf Seite 99. Die Cron-Tabelle verwendet den konfigurierten Benutzer, daher kann „loadconfig“, sofern es über die Cron-Tabelle ausgeführt wird, die Konfiguration nur komplett lesen, wenn dies mit dem Root-Administrator erfolgt.

Befehl	Beschreibung
	Zugriffsrecht: Supervisor-Write

`loadfile [-a <Adresse>] [-s <Server-IP-Adresse>] [-n] [-f <Dateiname>] [-o <Dateiname>] [-c <Dateiname>] [-p <Dateiname>] [-d <Passphrase>] [-C n|d] [-m <Version>] [-u] [-x <Dateiname>] [-i]`	Lädt eine Zertifikatsdatei in das Gerät. Mögliche Optionsschalter sind:
	› `-a`: Bestimmt die Quelladresse der Datei:
	  › `a.b.c.d`: Quell-IP-Adresse
	  › `INT`: Adresse des ersten Intranet-Interfaces als Quelladresse verwenden
	  › `DMZ`: Adresse des ersten DMZ-Interfaces als Quelladresse verwenden
	  › `LBx`: Loopback-Adresse x (0..f) als Quelladresse verwenden
	  › `<Schnittstelle>`: Adresse des LAN-Interfaces <Schnittstelle> als Quelladresse verwenden
	› `-s`: Adresse des TFTP Servers
	› `-n`: Server-Namen auf SSL/TLS-Verbindungen ignorieren
	› `-f`: <Dateiname> der Konfigurationsdatei auf dem TFTP-Server
	› `-o`: Zieldatei <Dateiname> für Datei-Download
	› `-c`: Datei <Dateiname> mit Root-Zertifikat für HTTPS
	› `-p`: Datei <Dateiname> mit unverschlüsseltem PKCS#12-Container für HTTPS CA-Zertifikate und / oder Client-seitige Authentisierung
	› `-d`: <Passphrase>, um heruntergeladenen, verschlüsselten PKCS#12-Container zu entschlüsseln
	› `-C`: Überprüfe, ob Firmware neuer (n) als oder unterschiedlich (d) zu der momentan vorhandenen ist
	› `-m`: Minimal-<Version> für Firmware setzen
	› `-u`: Firmware-Datei unbedingt herunterladen, Versionsüberprüfung überspringen.
	› `-x`: Datei <Dateiname> mit zusätzlichen CA-Zertifikaten zur Überprüfung bei HTTPS, der Wert 'none' verhindert das Laden der Standardzertifikate
	› `-i`: Sende Sysinfo als POST request (nur bei HTTP(S))
	
	Die Optionen [-f] und [-s] sowie die URL sind nicht gleichzeitig nutzbar. Für HTTP(S)-Downloads müssen Sie die Quelle mittels URL spezifizieren. Die Maximallänge der URL beträgt 252 Zeichen.

	Zugriffsrecht: Supervisor-Write
`loadfirmware [-e] (-s <Server-IP-Addresse> -f <Dateiname>)|<URL>`	Lädt eine Firmware via TFTP in das Gerät. Geben Sie dazu wahlweise die Server-Adresse und den Dateinamen oder die komplette URL an. Über den Optionsschalter `-e` wird veranlasst, dass die Firmwaredatei zuerst komplett im lokalen Dateisystem gespeichert wird, bevor das Firmware-Update startet. Weitere Informationen zu dem Befehl erhalten Sie gesondert im Abschnitt *Datei-Download von einem TFTP- oder HTTP(S)-Server* auf Seite 99.
	Zugriffsrecht: Supervisor-Write
`loadscript (-s <Server-IP-Addresse> -f <Dateiname>)|<URL>`	Lädt ein Konfigurationsskript via TFTP in das Gerät. Geben Sie dazu wahlweise die Server-Adresse und den Dateinamen oder die komplette URL an. Weitere Informationen zu dem Befehl erhalten Sie gesondert im Abschnitt *Datei-Download von einem TFTP- oder HTTP(S)-Server* auf Seite 99. Die Cron-Tabelle verwendet den konfigurierten Benutzer, daher kann „loadscript“, sofern es über die Cron-Tabelle ausgeführt wird, die Konfiguration nur komplett lesen, wenn dies mit dem Root-Administrator erfolgt.

Befehl	Beschreibung
	Zugriffsrecht: Supervisor-Write
`lspci`	Ausgabe von Informationen über PCI-Geräte
	Zugriffsrecht: Supervisor-Read
`ping <IPv4-Address|Hostname>` `ping -6 <IPv6-Address>%<Scope>`	Sendet einen ICMP echo request an die angegebene IP-Adresse. Weitere Informationen zu dem Befehl und den Besonderheiten beim Anpingen von IPv6-Adressen finden Sie im Kapitel *Übersicht der Parameter im ping-Befehl* auf Seite 64.
`printenv`	Gibt eine Übersicht aller Umgebungsvariablen und deren Werte aus.
`readconfig [-h] [-s <password>]`	Gibt die komplette Konfiguration in Form der Geräte-Syntax aus. › `-h`: Ergänzt die Konfigurationsdatei um eine Prüfsumme. › `-s <password>`: Verschlüsselt die Konfigurationsdatei auf Basis des angegebenen Passwortes.
	Zugriffsrecht: Supervisor-Read
`readmib`	Anzeige der SNMP Management Information Base. Nur auf Geräten ohne Unified-MIB vorhanden.
	Zugriffsrecht: Supervisor-Read,Local-Admin-Read
`readscript [-n] [-d] [-i] [-c] [-m] [-h] [-s <password>] [-o]`	Erzeugt eine Textausgabe aller Befehle und Parameter, die für die Konfiguration des Gerätes im aktuellen Zustand benötigt werden. Dabei können Sie folgende Optionsschalter angeben: › `-n`: Die Textausgabe erfolgt nur auf numerischer Basis ohne Bezeichner. Die Ausgabe enthält somit nur die aktuellen Zustandswerte der Konfiguration sowie die zugehörigen SNMP-IDs. › `-d`: Nimmt die Default-Werte in die Textausgabe mit auf. › `-i`: Nimmt die Bezeichnungen der Tabellen-Felder in die Textausgabe mit auf. › `-c`: Nimmt eventuelle Kommentare, die sich in der Skriptdatei befinden, in die Textausgabe mit auf. › `-m`: Die Textausgabe erfolgt in einer kompakten, am Bildschirm jedoch schwer lesbaren Darstellung (ohne Einrückungen). › `-h`: Ergänzt die Skriptdatei um eine Prüfsumme. › `-s <password>`: Verschlüsselt die Skriptdatei auf Basis des angegebenen Passwortes. › `-o`: Ersetzt die Passwörter durch ein "*", sodass diese nicht in der Textausgabe sichtbar sind.
	Zugriffsrecht: Supervisor-Read
`readstatus`	Gibt den Status aller SNMP-IDs des Gerätes aus.
`release [-x] *|<Interface_1…Interface_n>`	Der DHCPv6-Client gibt seine IPv6-Adresse und / oder sein Präfix an den DHCPv6-Server zurück. Anschließend fragt er erneut den DHCPv6-Server nach einer Adresse oder einem Präfix. Je nach Provider vergibt der Server dem Client eine neue oder die vorherige Adresse. Ob der Client eine andere Adresse oder ein anderes Präfix erhält, bestimmt alleine der Server. Der Optionsschalter `-x` unterdrückt eine Bestätigungsmeldung. Der Platzhalter `*` wendet das Kommando auf alle Interfaces und Präfix-Delegationen an. Alternativ können Sie ein oder mehrere spezifische Interfaces angeben.
`repeat <Interval> <Command>`	IPv6-Adressfreigabe: Wiederholt das angegebene Kommando alle `<Interval>` Sekunden, bis der Vorgang durch neue Eingaben beendet wird.

Befehl	Beschreibung
`rollout (-r|-remove) <RelatedFile>`	Löscht die Dateien des benutzerdefinierten Rollout-Assistenten aus dem Dateisystem des Gerätes. Mögliche Dateien sind: › `wizard`: Löscht den Assistenten › `template`: Löscht das Template › `logo`: Löscht das Logo › `alle`: Löscht den Assistenten, das Template und das Logo **Zugriffsrecht**: Supervisor-Write
`setenv <Name> <Value>`	Setzt eine Umgebungsvariable auf den angegebenen Wert. **Zugriffsrecht**: Supervisor-Write, Local-Admin-Write, Limited-Admin-Write
`setpass|passwd [-u <User>][-n <new> <old>]`	Ändert das Passwort des aktuellen Benutzerkontos. Um das Passwort ohne die darauf folgende Eingabeaufforderung zu ändern, verwenden Sie den Optionsschalter `-n` mit Angabe des neuen und alten Passwortes. Das Passwort darf maximal **128 Zeichen** haben und den folgenden Zeichensatz verwenden: `#ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()*+-,/:;<=>?[\]^_.0123456789abcdefghijklmnopqrstuvwxyz` Wird der Befehl `passwd` in einem Skript eingesetzt und ein `$` im Passwort verwendet, muss ein weiteres `$` vorangestellt werden, da dies ansonsten als Variable interpretiert wird und das Setzen des Passworts fehlschlägt. Um bei aktivierter TACACS+-Authentifizierung das Passwort des lokalen Benutzerkontos zu ändern, verwenden Sie den Optionsschalter `-u` mit dem Namen des entsprechenden Benutzers. Existiert der lokale Benutzer nicht oder fehlt die Angabe des Benutzernamens, bricht der Befehl ab. Der Benutzer benötigt außerdem Supervisorrechte bzw. die TACACS-Autorisierung muss aktiv sein.
`show <Options> <Filter>`	Zeigt ausgewählte interne Daten, wie z. B. › `admin-distance` – zeigt die administrative (Routing-)Distanz aller internen Anwendungen bzw. Routing-Protokolle › `bootlog` – die letzten Boot-Vorgänge › `filter` – Firewall-Filterregeln › `fw-dns-destinations` – nimmt optional eine leerzeichen-separierte Liste von Namen der DNS-Ziele der Firewall an. Es werden alle DNS-Ziele oder die in der Parameterliste angegebenen in ihrer Reihenfolge aufgeführt. Für jedes Ziel werden die Zähler aus **Status** > **Firewall** > **DNS-Datenbank** > **Zielverwendung** angezeigt, gefolgt von der Liste ihrer Wildcardausdrücke. Für jeden Wildcardausdruck werden die aktuell aufgelösten Adressen und die direkt oder indirekt passenden Datensätze angezeigt. › `ip-addresses` – zeigt alle IPv4- und IPv6-Adressen des Gerätes für LAN- und WAN-Schnittstellen mit erweiterten Status-Informationen an › `ipv4-addresses` – zeigt alle IPv4-Adressen des Gerätes für LAN- und WAN-Schnittstellen mit erweiterten Status-Informationen an › `lisp instance` – zeigt Statusinformationen über alle konfigurierten LISP-Instanzen an › `lisp instance [instance]` – zeigt Statusinformationen über die LISP-Instanz mit dem Namen [instance] an

Befehl	Beschreibung
	› `lisp map-cache` – zeigt Statusinformationen über die vorhandenen Map-Cache-Einträge aller Instanzen an › `lisp map-cache [instance]` – zeigt Statusinformationen über die vorhandenen Map-Cache-Einträge der Instanz mit dem Namen [instance] an › `lisp registrations` – zeigt Statusinformationen über die beim Map-Server registrierten EIDs / RLOCs aller Instanzen an › `lisp registrations [instance]` – zeigt Statusinformationen über die beim Map-Server registrierten EIDs / RLOCs der Instanz mit dem Namen [instance] an › `lta` – zeigt Informationen zu Gruppen oder Benutzern des LANCOM Trusted Access. Dieser wird über die LANCOM Management Cloud eingerichtet und verwaltet. › `mem`, `heap` – Speicherauslastung › `netflow collectors` – Zeigt Informationen über die konfigurierten NetfFlow-Kollektoren › `netflow interfaces` – Zeigt Informationen über Interfaces sowie die entsprechenden NetFlow-Parameter an › `netflow metering-profiles` – Zeigt Informationen über die Mess-Profile von NetFlow / IPFIX an ⓘ Mehr Informationen zu NetFlow / IPFIX finden Sie unter *Netflow / IPFIX* auf Seite 1678. › `VLAN` – dynamisch hinzugefügte VLANs und VLAN-Mitgliedschaften, die z. B. vom CAPWAP oder vom WLAN/802.1X zur Laufzeit zur statischen Konfiguration hinzugefügt wurden › `VPN` – VPN-Regeln Über zusätzliche Filter-Argumente lässt sich die Ausgabe weiter einschränken. Um eine Übersicht aller möglichen Optionen zu erhalten, geben Sie `show ?` ein. Die jeweils möglichen Filter einer Option erhalten Sie über `show <Option> ?`. `show VPN ?` zeigt z. B. die möglichen Filter für die VPN-Regeln. Für die Anzeige IPv6-spezifischer Daten lesen Sie auch das Kapitel *Übersicht der IPv6-spezifischen show-Befehle* auf Seite 71. **Zugriffsrecht**: Supervisor-Read, Local-Admin-Read
`sleep [-u] <Value><Suffix>`	Verzögert die Verarbeitung der Konfigurationsbefehle um eine bestimmte Zeitspanne oder terminiert sie auf einen bestimmten Zeitpunkt. Als `<Suffix>` sind `s`, `m` oder `h` für Sekunden, Minuten oder Stunden erlaubt; ohne Suffix arbeitet der Befehl in Millisekunden. Mit dem Optionsschalter `-u` nimmt das `sleep`-Kommando Zeitpunkte im Format `MM/DD/YYYY hh:mm:ss` (englisch) oder im Format `TT.MM.JJJJ hh:mm:ss` (deutsch) entgegen. Die Parametrierung als Termin wird nur akzeptiert, wenn die Systemzeit gesetzt ist.
`smssend [-s <SMSC-Number>] (-d <Destination>) (-t <Text>)`	Nur auf Geräten mit 3G- / 4G / 5G-WWAN-Modul verfügbar: Versendet eine Kurznachricht an die angegebene Ziel-Rufnummer. › `-s <SMSC-Number>`: Alternative SMSC-Rufnummer (optional). Wenn Sie diesen Befehlsbestandteil weglassen, verwendet das Gerät die in der USIM-Karte hinterlegte oder die unter SNMP-ID 2.83.1 konfigurierte Rufnummer. › `-d <Destination>`: Ziel-Rufnummer

Befehl	Beschreibung
	› `-t <Text>`: Inhalt der Kurznachricht mit <=160 Zeichen. Eine Übersicht der verfügbaren Zeichen finden Sie im Abschnitt *Zeichensatz für den SMS-Versand* auf Seite 1727. Sonderzeichen sind nur in UTF8-kodierter Form möglich.
`ssh [-?|h] [-o "option=value"] [-<a|b> Loopback-Adresse] [-p Port] [-C] [-j Keepalive-Intervall] <Host>`	Stellt eine SSH-Verbindung zum <Host> her. Mögliche Optionsschalter sind: › `-?|h`: gibt den Hilfetext aus. › `-o "option=value"`: es können zusätzliche Optionen mit entsprechenden Werten angegeben werden. › `-a|b`: erlaubt die Angabe einer Route bzw. Loopback-Adresse, die das Gerät verwenden soll, wenn das Ziel auf mehreren Routen erreichbar ist. Die Funktion von `-a` und `-b` ist identisch. `-b` ist die übliche Option eines OpenSSH-Clients auf UNIX-Systemen, während einige andere im LCOS eingebaute Kommandos das `-a` zur Angabe einer Loopback-Adresse benutzen. › `-p`: bestimmt den <Port> des Hosts › `-C`: erzwingt eine komprimierte Datenübertragung › `-j`: gibt an, in welchen Abständen der Client ein Keepalive senden soll.
`sshcopyid`	Zur Speicherung des SSH-Public-Keys per SSH **Zugriffsrecht**: Supervisor-Write

`sshkeygen [-h] [-q] [-t dsa|rsa|ecdsa|ed25519|ed448] [-b <bits>] [-f <Dateiname>] [-R <Hostname>]`	Erzeugt oder löscht SSH-Schlüssel im Gerät. Mögliche Optionsschalter sind:
	› `-h`: Zeigt eine kurze Hilfe der möglichen Parameter.
	› `-q`: Das Gerät überschreibt bereits existierende Schlüssel ohne Rückfrage (Quiet-Modus)
	› `-t`: Dieser Parameter bestimmt den Typ des erzeugten Schlüssels. Insgesamt unterstützt SSH folgende Typen von Schlüsseln:
	  › RSA
	  › DSA
	  › ECDSA
	  › ED25519
	  › ED448
	› `-b`: Dieser Parameter bestimmt die Länge des Schlüssels in Bit für RSA-Schlüssel. Wenn Sie keine Länge angeben, erzeugt das Kommando immer einen Schlüssel mit einer Länge von 1024 Bit.
	› `-f`: Über diesen Parametern geben Sie den Dateinmanen der erzeugten Schlüsseldatei im Dateisystem des Gerätes an. Die Wahl des Dateinmanens hängt davon ab, was für einen Schlüssel Sie erzeugen. Zur Auswahl stehen Ihnen in diesem Fall:
	  › **ssh_rsakey** für RSA-Schlüssel
	  › **ssh_dsakey** für DSA-Schlüssel
	  › **ssh_ecdsakey** für ECDSA-Schlüssel
	  › **ssl_privkey** für SSL-RSA-Schlüssel
	  › **ssh_ed25519key** für Ed25519-Schlüssel
	  › **ssh_ed448key** für Ed448-Schlüssel
	› `-R`: Entfernt alle Schlüssel zu einem bestimmten Hostnamen. Geben Sie gegebenenfalls optional einen Schlüsseltyp an.
	Weitere Informationen zu geräteinternen SSH / SSL-Schlüsseln finden Sie im Kapitel *Geräteinterne SSH- / SSL-Schlüssel* auf Seite 113

Befehl	Beschreibung
`ssldefaults [-j]`	Dieses Kommando setzt nach einer Sicherheitsabfrage die SSL- / TLS-Einstellungen in allen Untermenüs der aktuellen Konfiguration auf die Standardwerte zurück. Im LCOS bringt jedes Modul sein eigenes Untermenü für SSL- / TLS-Einstellungen mit. Hiermit gibt es eine Methode, alle Einstellungen in diesen verteilten Untermenüs auf die aktuellen sicheren Voreinstellungen zurückzusetzen. Mit dem Parameter `-j` wird die Sicherheitsabfrage automatisch beantwortet, sodass das Kommando aus Skripten heraus non-interaktiv aufgerufen werden kann.
`stop`	Beendet den ping-Befehl
`sysinfo`	Zeigt Systeminformationen an (z. B. Hardware-Release, Softwareversion, MAC-Adresse, Seriennummer etc.).
`tab`	Zur Verwendung in Skript-Dateien: Setzt für ein nachfolgendes Kommando in einer Tabelle die Reihenfolge der Spalten für die Argumente, falls die Spalten in der Tabelle vom Standard abweichen (z. B. eine zusätzliche Spalte). **Zugriffsrecht**: Supervisor-Write,Local-Admin-Write,Limited-Admin-Write
`telnet <Adresse>`	Stellt eine Telnet-Verbindung zur angegebenen <Adresse> her.
`testmail <From> <To_1…To_n> [<Realname> <Subject> <Body>]`	Verschickt eine Test-E-Mail. Notwendige Angaben sind eine Absendeadresse und Empfängeradresse; Realname, Betreffzeile und Nachrichteninhalt sind optional. **Zugriffsrecht**: Supervisor-Write,Local-Admin-Write,Limited-Admin-Write
`time <DateTime>`	Setzt einen Zeitpunkt im Format `MM/DD/YYYY hh:mm:ss` (englisch) oder im Format `TT.MM.JJJJ hh:mm:ss` (deutsch). **Zugriffsrecht**: Supervisor-Write,Local-Admin-Write,Limited-Admin-Write **Ausführungsrecht**: Time-Wizard
`trace <Parameter> <Filter>`	Startet einen Trace-Befehl zur Ausgaben von Diagnose-Daten. Über zusätzliche Filter-Argumente lässt sich die Ausgabe weiter einschränken. Weitere Informationen zu dem Befehl erhalten Sie gesondert im Abschnitt *Übersicht der Parameter im trace-Befehl* auf Seite 67. **Zugriffsrecht**: Supervisor-Read,Limited-Admin-Read,Limited-Admin-Write
`unmount [-?][-f] <Volume>`	Gibt die aktuelle Volumetabelle aus. › `-f`: Gibt das angegebene Volume frei. <Volume> kann die Volume-ID oder ein beliebiger Mountpunkt sein. › `-?`: Gibt den Hilfetext aus.
`unsetenv <Name>`	Löscht die angegebene Umgebungsvariable. **Zugriffsrecht**: Supervisor-Write,Local-Admin-Write,Limited-Admin-Write
`wakeup [MAC]`	Führt ein Wake-On-LAN für das Gerät mit der MAC-Adresse [MAC] aus. **Zugriffsrecht**: Supervisor-Write,Local-Admin-Write,Limited-Admin-Write
`who`	Listet aktive Konfigurationssitzungen auf.
`writeconfig [-u] [-C d] [-s password] [-b index]`	Schreibt eine neue Konfiguration in Form der Geräte-Syntax in das Gerät. Das System interpretiert alle folgenden Zeilen solange als Konfigurationswerte, bis zwei Leerzeilen auftreten. Mögliche Optionsschalter sind: › `-u`: Erzwingt die unbedingte ("**u**nconditional") Ausführung eines Skriptes oder einer Konfiguration. › `-C d`: Überspringt die standardmäßige Differenzprüfung ("**C**heck for **d**ifference"). Gilt auch, wenn die Option `-u` gesetzt ist.

Befehl	Beschreibung
	› `-s password`: Entschlüsselt die Konfigurationsdatei auf Basis des angegebenen Passwortes. › `-b index`: Schreibt die Konfiguration als alternative Bootkonfiguration. Index muss `1`, `2` oder `all` sein. **Zugriffsrecht**: Supervisor-Write
`writeflash`	Laden einer neuen Firmware-Datei (nur via TFTP). **Zugriffsrecht**: Supervisor-Write
`!!`	Letztes Kommando wiederholen
`!<num>`	Kommando <num> wiederholen
`!<prefix>`	Letztes mit <prefix> beginnendes Kommando wiederholen
`#<blank>`	Kommentar

Legende

› Zeichen- und Klammernregelung:

  › Objekte – hier: dynamische oder situationsabhängige Eingaben – stehen in spitzen Klammern.
  › Runde Klammern gruppieren Befehlsbestandteile zur besseren Übersicht.
  › Vertikale Striche (Pipes) trennen alternative Eingaben.
  › Eckigen Klammern beschreiben optionale Schalter.

  Somit sind alle Befehlsbestandteile, die nicht in eckigen Klammern stehen, notwendigen Angaben zuzurechnen.

› `<Path>`:

  › Beschreibt den Pfadnamen für ein Menü, eine Tabelle oder einen Parameter, getrennt durch "/" oder "\".
  › `..` bedeutet: eine Ebene höher.
  › `.` bedeutet: aktuelle Ebene.

› `<Value>`:

  › Beschreibt einen möglichen Eingabewert.
  › `""` ist ein leerer Eingabewert.

› `<Name>`:

  › Beschreibt eine Zeichensequenz von [0…9] [A…Z] [a…z] [_].
  › Das erste Zeichen darf keine Ziffer sein.
  › Es gibt keine Unterscheidung zwischen Groß- und Kleinschreibung.

› `<Filter>`:

  › Die Ausgaben einiger Kommandos können durch die Angabe eines Filterausdrucks eingeschränkt werden. Die Filterung erfolgt dabei nicht zeilenweise, sondern blockweise abhängig vom jeweiligen Kommando.
  › Ein Filterausdruck beginnt mit einem alleinstehenden '@' und endet entweder am Zeilenende oder an einem alleinstehenden ';', welches das aktuelle Kommando abschliesst.
  › Ein Filterausdruck besteht des weiteren aus einem oder mehreren Suchmustern, die durch Leerzeichen voneinander getrennt sind und denen entweder kein Operator ('Oder'-Muster) oder einer der Operatoren '+' ('Und'- Muster) oder '-' ('Nicht'-Muster) vorangestellt ist.

- Bei der Ausführung des Kommandos wird ein Informationsblock genau dann ausgegeben, wenn mindestens eines der 'Oder'-Muster, alle 'Und'-Muster und keines der 'Nicht'-Muster passen. Dabei wird die Groß- und Kleinschreibung nicht beachtet.
- Soll ein Suchmuster Zeichen enthalten, die zur Strukturierung in der Filtersyntax verwendet werden (z. B. Leerzeichen), dann kann das Suchmuster als Ganzes mit '"' umschlossen werden. Alternativ kann den speziellen Zeichen ein '\' vorangestellt werden. Wenn ein '"' oder ein '\' gesucht werden soll, muss diesem ein '\' vorangestellt werden.

  Es reicht die Eingabe des eindeutigen Wortanfangs.

- Beispiele für den Einsatz des Ausgabefilters finden Sie im Abschnitt *Trace-Ausgabe filtern* auf Seite 296.

Erläuterungen zur Adressierung, Schreibweise und Befehlseingabe

- Alle Befehle, Verzeichnis- und Parameternamen können verkürzt eingegeben werden, solange sie eindeutig sind. Zum Beispiel kann der Befehl `sysinfo` zu `sys` verkürzt werden, oder aber `cd Management` zu `c ma`. Die Eingabe `cd /s` dagegen ist ungültig, da dieser Eingabe sowohl `cd /Setup` als auch `cd /Status` entspräche.
- Verzeichnisse können über die entsprechende SNMP-ID angesprochen werden. Der Befehl `cd /2/8/10/2` bewirkt z. B. das gleiche wie `cd /Setup/IP-Router/Firewall/Regel-Tabelle`.
- Mehrere Werte in einer Tabellenzeile können mit **einem** Befehl verändert werden, z. B. in der Regeltabelle der IPv4-Firewall:
  - `set WINS UDP` setzt das Protokoll der Regel WINS auf UDP.
  - `set WINS UDP ANYHOST` setzt das Protokoll der Regel WINS auf UDP und die Destination auf ANYHOST.
  - `set WINS * ANYHOST` setzt ebenfalls die Destination der Regel WINS auf ANYHOST, durch das Sternchen wird das Protokoll unverändert übernommen.
- Die Werte in einer Tabellenzeile können alternativ über den Spaltennamen oder die Positionsnummer in geschweiften Klammern angesprochen werden. Der Befehlt `set ?` in der Tabelle zeigt neben dem Namen und den möglichen Eingabewerten auch die Positionsnummer für jede Spalte an. Die Destination hat in der Regeltabelle der Firewall z. B. die Nummer 4:
  - `set WINS {4} ANYHOST` setzt die Destination der Regel WINS auf ANYHOST.
  - `set WINS {destination} ANYHOST` setzt auch die Destination der Regel WINS auf ANYHOST.
  - `set WINS {dest} ANYHOST` setzt die Destination der Regel WINS auf ANYHOST, weil die Angabe von `dest` hier ausreichend für eine eindeutige Spaltenbezeichnung ist.
- Namen, die Leerzeichen enthalten, müssen in Anführungszeichen ("") eingeschlossen werden.

Kommandospezifische Hilfe

- Für Aktionen und Befehle steht eine kommandospezifische Hilfefunktion zur Verfügung, indem die Funktion mit einem Fragezeichen als Optionsschalter aufgerufen wird. Zum Beispiel zeigt der Aufruf `ping ?` die Optionen des eingebauten PING-Kommandos an.
- Eine vollständige Auflistung der zur Verfügung stehenden Konsolen-Befehle erhalten Sie durch die Eingabe von `help` oder `?`.

Übersicht der Parameter im ping-Befehl

Das ping-Kommando an der Eingabeaufforderung einer Terminal-Verbindung sendet ein „ICMP Echo-Request"-Paket an die Zieladresse des zu überprüfenden Hosts. Wenn der Empfänger das Protokoll unterstützt und es nicht in der Firewall gefiltert wird, antwortet der angesprochene Host mit einem „ICMP Echo-Reply". Ist der Zielrechner nicht erreichbar,

antwortet das letzte Gerät vor dem Host mit „Network unreachable“ (Netzwerk nicht erreichbar) oder „Host unreachable“ (Gegenstelle nicht erreichbar).

Die Syntax des ping-Kommandos lautet wie folgt:

```
ping [-46dfnoqrmb] [-s n] [-i n] [-c n] [-x x][-p <dscp>][-a ...] destination [%scope] [%scope@rtg-tag] [%%interface] [@rtg-tag]
```

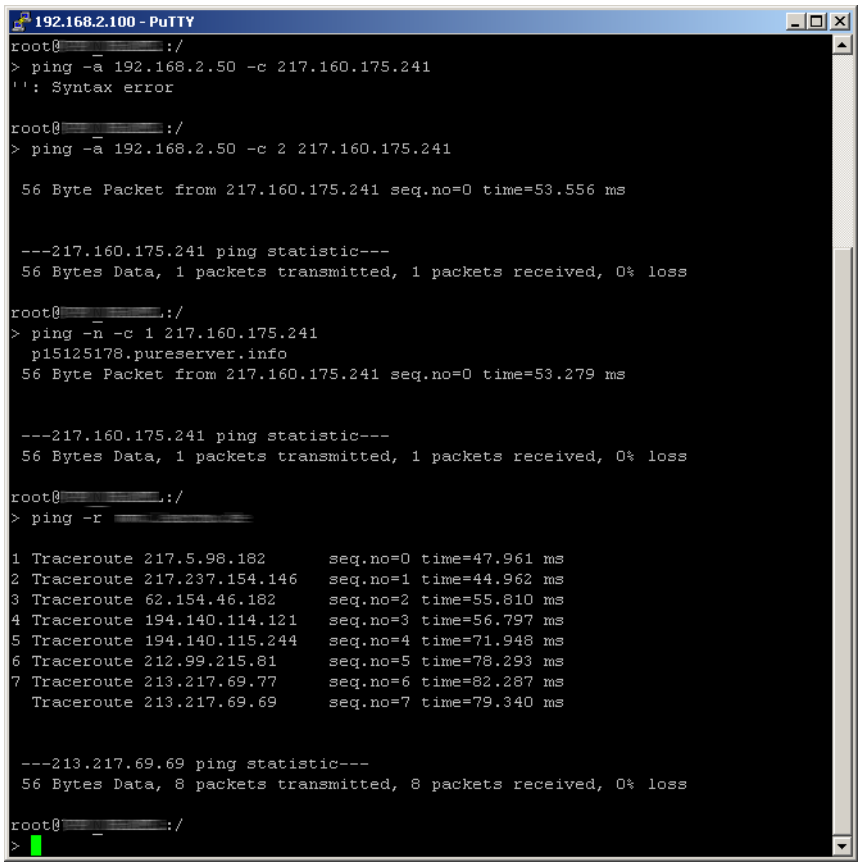
Die Bedeutung der optionalen Parameter können Sie der folgenden Tabelle entnehmen:

Tabelle 3: Übersicht aller optionalen Parameter im ping-Befehl

Parameter	Bedeutung
`-4`	Verwendung von IPv4 erzwingen
`-6`	Verwendung von IPv6 erzwingen
`-d`	Fragmentierung verbieten
`-f`	flood ping: Sendet eine große Anzahl von ping-Signalen in kurzer Zeit. Kann z. B. zum Testen der Netzwerkbandbreite genutzt werden.  flood ping kann leicht als Denial-of-Service-Angriff (DoS) fehlinterpretiert werden.
`-n`	Liefert den Computernamen zu einer eingegebenen IP-Adresse zurück.
`-o`	Schickt nach einer Antwort sofort eine weitere Anfrage.
`-q`	ping-Kommando liefert keine Ausgaben auf der Konsole.
`-r`	Wechselt in den traceroute-Modus: Der Weg der Datenpakete zum Zielcomputer wird mit allen Zwischenstationen angezeigt.
`-m`	Wechselt in den tracepath-Modus zur Ermittlung der Pfad-MTU zu der angegebenen IP-Adresse.
`-b`	Nicht aufhören zu pingen, wenn ein PacketTooBig(DF) empfangen wird, damit man „Path MTU Discovery“ hat.
`-s n`	Setze Größe der Pakete auf n Byte (max. 65500).
`-i n`	Zeit zwischen den einzelnen Paketen in Sekunden.
`-c n`	Sende n Ping-Signale.
`[-x x]`	Atomare Fragmente: (n)ever, (f)orce, (a)automatic
`[-p <dscp>]`	Verwende einen spezifischen DSCP-Wert für diesen Ping. DSCP (Differentiated Services Code Point) wird für QoS (Quality of Service) verwendet. Mögliche DSCP-Werte: BE/CS0, CS1, CS2, CS3, CS4, CS5, CS6, CS7, AF11, AF12, AF13, AF21, AF22, AF23, AF31, AF32, AF33, AF41, AF42, AF43, EF
`-a a.b.c.d`	Setzt die Absenderadresse des Pings (Standard: IP-Adresse des Gerätes)
`-a <name>`	Verwendet ein benanntes Netzwerk, Interface oder Loopback-Adresse als Absendeadresse
`-l <Load-Balancer-Policy>`	Wenn das Ping-Ziel über einen Load Balancer erreichbar ist, wird beim Versand der Pings anhand der Policy eine Load-Balancer-Entscheidung getroffen. Mögliche Werte sind Default, Traffic, Bandwidth, Round-Robin, Most-Used sowie alle definierten Dynamic-Path-Selection-Policies. Die Angabe einer ungültigen Policy sorgt dafür, dass keine Pings versendet werden können

Parameter	Bedeutung
	Es ist nicht möglich, diese Kommandozeilen-Option zusammen mit der Angabe eines Scopes oder einer Interface-Bindung in der Destination zu verwenden.
`-6 <IPv6-Address>%<Scope>`	Führt ein Ping-Kommando über das mit <Scope> bestimmte Interface auf die Link-Lokale-Adresse aus. Der Parameter-Bereich ist bei IPv6 von zentraler Bedeutung: Da ein IPv6-Gerät sich mit mehreren Schnittstellen (logisch oder physikalisch) pro Schnittstelle eine Link-Lokale-Adresse (fe80::/10) teilt, müssen Sie beim Ping auf eine Link-Lokale-Adresse immer den Bereich (Scope) angeben. Nur so kann das Ping-Kommando die Schnittstelle bestimmen, über die es das Paket senden soll. Den Namen der Schnittstelle trennen Sie durch ein Prozentzeichen (%) von der IPv6-Adresse. **Beispiele:** › `ping -6 fe80::1%INTRANET` Ping auf die Link-Lokale-Adresse „fe80::1“, die über die Schnittstelle bzw. das Netz „INTRANET“ zu erreichen ist. › `ping -6 2001:db8::1` Ping auf die globale IPv6-Adresse „2001:db8::1“.
`destination`	Adresse oder Hostname des Zielcomputers.
`%scope`	Name des Interfaces über welches das Paket bei der Verwendung von Link-Lokalen-Adressen als Ziel versendet werden soll.
`%scope@rtg-tag`	Name des Interfaces über welches das Paket bei der Verwendung von Link-Lokalen-Adressen als Ziel versendet werden soll mit zusätzlicher Angabe des Routing-Tags.
`%%interface`	Name des Ziel-Interfaces. Das Paket wird direkt und ohne Berücksichtigung der Routing-Tabelle an das Interface gesendet.
`@rtg-tag`	Routing-Tag, das zum Senden des Pakets verwendet werden soll.

Parameter	Bedeutung
`stop /<RETURN>`	Die Eingabe von `stop` oder das Drücken der RETURN-Taste beenden das Ping-Kommando.



Übersicht der Parameter im trace-Befehl

Die jeweils für ein bestimmtes Modell verfügbaren Traces können über die Eingabe von `trace` ohne Argumente auf der Konsole angezeigt werden.

Tabelle 4: Übersicht einiger durchführbarer Traces

Dieser Parameter ...	... ruft beim Trace die folgende Anzeige hervor:
`Status`	Status-Meldungen der Verbindungen
`Fehler`	Fehler-Meldungen der Verbindungen
`ACME`	Automatic Certificate Management Environment (ACME) Client
`ADSL`	ADSL-Verbindungsstatus
`ARP`	Address Resolution Protocol
`ATM-Cell`	ATM-Paketebene
`ATM-Error`	ATM-Fehler
`Bridge`	Informationen über die WLAN-Bridge

Dieser Parameter ...	... ruft beim Trace die folgende Anzeige hervor:
Connact	Meldungen aus dem Aktivitätsprotokoll
Cron	Aktivitäten der Zeitautomatik (Cron-Tabelle)
D-Kanal-Dump	Trace des D-Kanals des angeschlossenen ISDN-Busses
DFS	Trace zur Dynamic Frequency Selection, der automatischen Kanalwahl im 5-GHz-WLAN-Band
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Service Protocol
EAP	Trace zum EAP, dem bei WPA/802.11i und 802.1X verwendeten Protokoll zur Schlüsselaushandlung
Ethernet	Informationen über die Ethernet-Schnittstellen
Firewall	Zeigt die Aktionen der Firewall
FW-DNS	Änderungen an der Firewall-Datenbank der DNS-Ziele: › Wenn ein DNS-Paket eintrifft, werden das Paket und die betroffenen Wildcardausdrücke und Ziele ausgegeben. › Wenn die TTL (Time-to-Live – Lebensdauer) eines Eintrags abläuft, dann werden dieser Datensatz und die betroffenen Wildcardausdrücke und Ziele ausgegeben. › Wenn eine der beiden Firewalls ein DNS-Ziel registriert oder deregistriert, weil sich ihre Konfiguration geändert hat. › Wenn sich die Tabellen **Setup** > **Firewall** > **DNS-Ziele** oder **Setup** > **Firewall** > **DNS-Ziel-Liste** ändern.
GRE	Meldungen zu GRE-Tunneln
hnat	Informationen zum Hardware-NAT
IAPP	Trace zum Inter Access Point Protocol, zeigt Informationen über das WLAN-Roaming.
ICMP	Internet Control Message Protocol
IGMP	Informationen über das Internet Group Management Protocol
IP-Masquerading	Vorgänge im Masquerading-Modul
IPv6-Config	Informationen über die IPv6-Konfiguration
IPv6-Firewall	Ereignisse der IPv6-Firewall
IPv6-Interfaces	Informationen der IPv6-Schnittstellen
IPv6-LAN-Packet	Datenpakete über die IPv6-LAN-Verbindung
IPv6-Router	Informationen über das IPv6-Routing
IPv6-WAN-Packet	Datenpakete über die IPv6-WAN-Verbindung
L2TP	L2TPv2 / v3-Protokoll
LANAUTH	LAN-Authentifizierung (z. B. Public Spot)
Load-Balancer	Informationen zum Load-Balancing
Mail-Client	E-Mail-Verarbeitung des integrierten Mail-Clients

Dieser Parameter ...	... ruft beim Trace die folgende Anzeige hervor:
VPN-Mesh	Trace für *LANCOM Advanced Mesh VPN (AMVPN)* auf Seite 893.
NETFLOW-Common	Mehr Informationen zu NetFlow / IPFIX finden Sie unter *Netflow / IPFIX* auf Seite 1678.
NETFLOW-Error	
NETFLOW-Export	
NETFLOW-Metering	
NTP	Timeserver Trace
Paket-Dump	Anzeige der ersten 64 Bytes eines Pakets in hexadezimaler Darstellung
PPP	Verhandlung des PPP-Protokolls
RADIUS	RADIUS-Trace
RIP	IP Routing Information Protocol
Script	Script-Verhandlung
Serial	Informationen über den Zustand der seriellen Schnittstelle
SIP-Packet	SIP-Informationen, die zwischen einem VoIP Router und einem SIP-Provider bzw. einer übergeordneten SIP-TK-Anlage ausgetauscht werden
SMTP-Client	E-Mail-Verarbeitung des integrierten Mail-Clients
SNTP	Simple Network Time Protokoll
Spgtree	Informationen zum Spanning Tree Protokoll
USB	Informationen über den Zustand der USB-Schnittstelle
VLAN	Informationen über virtuelle Netzwerke
VPN-Packet	IPSec und IKE Pakete
VPN-Status	IPSec und IKE Verhandlungen
VRRP	Informationen über das Virtual Router Redundancy Protocol
WLAN	Informationen über die Aktivitäten in den Funknetzwerken
WLAN-ACL	Status-Meldungen über MAC-Filterregeln. Die Anzeige ist abhängig von der Konfiguration des WLAN-Data-Trace. Ist dort eine MAC-Adresse vorgegeben, zeigt der Trace nur die Filterergebnisse an, die diese spezielle MAC-Adresse betreffen.
XML-Interface-PbSpot	Meldungen des Public-Spot-XML-Interfaces

Übersicht der capwap-Parameter im show-Befehl

Über die Konsole lassen sich folgende Informationen zum CAPWAP-Dienst aufrufen:

Tabelle 5: Übersicht aller capwap-Parameter im show-Befehl

Parameter	Bedeutung
`-addresses [<IfcNum>]`	Zeigt die Adresstabellen eines einzelnen oder aller WLC-Tunnel. Im Falle eines einzelnen WLC-Tunnels geben Sie für `<IfcNum>` die Nummer der logischen WLC-Tunnel-Schnittstelle an, z. B. `10`.
`-groups`	Zeigt Informationen zu einzelnen oder allen vorhandenen Zuweisungs- / Tag-Gruppen.

Den Befehl `show capwap groups` erweitern Sie um die nachfolgend gelisteten Parameter, wodurch sich der Umfang der angezeigten Informationen regulieren lässt:

Tabelle 6: Übersicht aller 'capwap group'-Parameter im show-Befehl

Parameter	Bedeutung
`all`	Zeigt die im Setup-Menü konfigurierten Namen und die geräteinternen Namen sämtlicher eingerichteten Zuweisungs- / Tag-Gruppen sowie der Default-Gruppe. Die Default-Gruppe stellt eine interne Gruppe dar, die sämtliche APs enthält.
`<group1> <group2> <…>`	Zeigt alle APs der betreffenden Zuweisungs-/Tag-Gruppen.
`-l <location>`	Zeigt alle APs des betreffenden Standorts.
`-c <country>`	Zeigt alle APs des betreffenden Landes.
`-i <city>`	Zeigt alle APs der betreffenden Stadt.
`-s <street>`	Zeigt alle APs der betreffenden Straßen.
`-b <building>`	Zeigt alle APs des betreffenden Gebäudes.
`-f <floor>`	Zeigt alle APs der betreffenden Etage.
`-r <room>`	Zeigt alle APs der betreffenden Raumbezeichnung.
`-d <device>`	Zeigt alle APs, die den angegebenen Gerätenamen tragen.
`-v <firmware>`	Zeigt alle APs, welche die angegebene Firmware besitzen. Geben Sie dazu für `<firmware>` die Versionsnummer gefolgt von der Build-Nummer an, z. B. `9.00.0001`.
`-x <firmware>`	Zeigt alle APs, deren Firmware-Version kleiner ist als die auf dem aktuellen Gerät installierte.
`-y <firmware>`	Zeigt alle APs, deren Firmware-Version gleich groß oder kleiner ist als die auf dem aktuellen Gerät installierte.
`-z <firmware>`	Zeigt alle APs, deren Firmware-Version größer ist als die auf dem aktuellen Gerät installierte.
`-t <firmware>`	Zeigt alle APs, deren Firmware-Version gleich groß oder größer ist als die auf dem aktuellen Gerät installierte.
`-n <intranet>`	Zeigt alle APs, deren IP zur angegebenen Intranet-Adresse gehört.
`-p <profile>`	Zeigt alle APs, denen das angegebene WLAN-Profil zugeordnet ist.
`rmgrp <group1 intern_name> <group2 intern_name> …`	Löscht die Gruppe(n) mit dem angegebenen internen Namen aus dem Arbeitsspeicher des Gerätes. Nutzen Sie diesen Befehl, um die Arbeitsspeicher freizugeben, falls eine zu hohe Zahl von Gruppen die Perfomanz des Gerätes verschlechtert. Der Eintrag im Setup-Menü bleibt von dieser Aktion unberührt.

Parameter	Bedeutung
`resetgrps`	Löscht alle Gruppen bis auf die Default-Gruppe.

Für die Standort-Informationen wertet das Gerät die in der Access-Point-Tabelle unter **Standort** eingetragenen Informationen aus. Folgende Feld-Bezeichnungen stehen Ihnen zur Verfügung:

- co=Country
- ci=City
- st=Street
- bu=Building
- fl=Floor
- ro=Room

Der Standort-Eintrag `co=Deutschland,ci=Aachen` z. B. ermöglicht Ihnen, über den Befehl `+show capwap group -i Aachen` an der Konsole alle vom WLC verwalteten APs in Aachen aufzulisten.

Befehlsbeispiele

```
show capwap group all
show capwap group group1
show capwap group -l yourlocation
show capwap group -s yourstreetname
show capwap group -d yourdevicename
show capwap group -p yourprofilename
show capwap group -d yourdevicename -p yourprofile -v yourfirmversion …
```

Übersicht der IPv6-spezifischen show-Befehle

Über die Konsole besteht die Möglichkeit, diverse IPv6-Funktionen abzufragen. Folgende Kommando-Funktionen stehen Ihnen zur Verfügung:

- *IPv6-Adressen*: `show ipv6-addresses`
- *IPv6-Präfixe*: `show ipv6-prefixes`
- *IPv6-Interfaces*: `show ipv6-interfaces`
- *IPv6-Neighbour Cache*: `show ipv6-neighbour-cache`
- *IPv6-DHCP-Server*: `show dhcp6-server`
- *IPv6-DHCP-Client*: `show dhcpv6-client`
- *IPv6-Route*: `show ipv6-route`

Darüber hinaus lässt sich die IPv6-Kommunikation über das `trace`-Kommando mitverfolgen.

IPv6-Adressen

Der Befehl `show ipv6-adresses` zeigt eine aktuelle Liste der genutzten IPv6-Adressen. Diese ist nach Interfaces sortiert. Hierbei ist zu beachten, dass ein Interface mehrere IPv6-Adressen haben kann. Eine dieser Adressen ist immer die Link-lokale-Adresse, welche mit `fe80:` beginnt.

Die Ausgabe ist folgendermaßen formatiert:

```
<Interface> :
<IPv6-Adresse>, <Status>, <Attribut>, (<Typ>)
```

Tabelle 7: Bestandteile der Konsolennausgabe `show ipv6-addresses`

Ausgabe	Erläuterung
Interface	Der Name des Interfaces.
IPv6-Adresse	Die IPv6-Adresse.
Status	Das Statusfeld kann folgende Werte beinhalten: › TENTATIVE – Die Duplicate Address Detection (DAD) prüft die Adresse momentan. Sie steht daher einer Verwendung für Unicast noch nicht zu Verfügung. › PREFERRED – Die Adresse ist gültig. › DEPRICATED – Die Adresse ist noch gültig, befindet sich aber im Status der Abkündigung. Eine Adresse mit dem Status PREFERRED wird für die Kommunikation bevorzugt. › INVALID – Die Adresse ist ungültig und kann nicht zur Kommunikation genutzt werden. Eine Adresse erhält diesen Status, nachdem die Lifetime ausgelaufen ist.
Attribut	Zeigt ein Attribut der IPv6-Adresse an. Mögliche Attribute sind: › None – keine besonderen Eigenschaften › (ANYCAST) – es handelt sich um eine Anycast-Adresse › (AUTO CONFIG) – es handelt sich um eine über die Autokonfiguration bezogene Adresse › (NO DAD PERFORMED) – es wird keine DAD durchgeführt
Type	Der Typ der IP-Adresse.

IPv6-Präfixe

Der Befehl `show ipv6-prefixes` zeigt alle bekannten Präfixe an. Die Sortierung erfolgt nach folgenden Kriterien:

Delegated prefixes

Alle Präfixe, die der Router delegiert bekommen hat.

Advertised prefixes

Alle Präfixe, die der Router in seinen Router-Advertisements ankündigt.

Deprecated prefixes

Alle Präfixe, die derzeit abgekündigt werden. Diese sind noch funktional, werden allerdings nach einem bestimmten Zeitrahmen gelöscht.

IPv6-Interfaces

Der Befehl `show ipv6-interfaces` zeigt eine Liste der IPv6 Interfaces und deren jeweiligen Status.

Die Ausgabe ist folgendermaßen formatiert:

<Interface> : <Status>, <Forwarding>, <Firewall>

Tabelle 8: Bestandteile der Konsolennausgabe `show ipv6-interfaces`

Ausgabe	Erläuterung
Interface	Der Name des Interfaces.
Status	Der Status des Interfaces. Mögliche Einträge sind: › oper Status is up › oper Status is down

Ausgabe	Erläuterung
Forwarding	Der Forwarding Status des Interfaces. Mögliche Einträge sind: › forwarding is enabled › forwarding is disabled
Firewall	Der Status der Firewall. Mögliche Einträge sind: › firewall is enabled › firewall is disabled

IPv6-Neighbour Cache

Der Befehl `show ipv6-neighbour-cache` zeigt den aktuellen Neighbour Cache an.

Die Ausgabe ist folgendermaßen formatiert:

```
<IPv6-Adresse> iface <Interface> lladdr <MAC-Adresse> (<Switchport>) <Gerätetyp> <Status> src <Quelle>
```

Tabelle 9: Bestandteile der Konsolenausgabe `show ipv6-neighbour-cache`

Ausgabe	Erläuterung
IPv6-Adresse	Die IPv6-Adresse des benachbarten Gerätes.
Interface	Das Interface, über das der Nachbar erreichbar ist.
MAC-Adresse	Die MAC-Adresse des Nachbarn.
Switchport	Der Switchport, auf dem der Nachbar festgestellt wurde.
Gerätetyp	Gerätetyp des Nachbarn (Host oder Router).
Status	Der Status der Verbindung zum benachbarten Gerät. Mögliche Einträge sind: › INCOMPLETE – Die Auflösung der Adresse ist noch im Gange und die Link Layer Adresse des Nachbarn wurde noch nicht bestimmt. › REACHABLE – Der Nachbar ist in den letzten zehn Sekunden erreichbar gewesen. › STALE – Der Nachbar ist nicht länger als REACHABLE qualifiziert, aber eine Aktualisierung wird erst durchgeführt, wenn versucht wird ihn zu erreichen. › DELAY – Der Nachbar ist nicht länger als REACHABLE qualifiziert, aber es wurden vor kurzem Daten an ihn gesendet und auf Verifikation durch andere Protokolle gewartet. › PROBE – Der Nachbar ist nicht länger als REACHABLE qualifiziert. Es werden Neighbour Solicitation Probes an ihn gesendet um die Erreichbarkeit zu bestätigen.
Quelle	Die IPv6-Adresse, über die der Nachbar entdeckt wurde.

IPv6-DHCP-Server

Der Befehl `show dhcpv6-server` zeigt den aktuellen Status des DHCP-Servers. Die Anzeige beinhaltet Informationen darüber, auf welchem Interface der Server aktiv ist, welche DNS-Server und Präfixe er hat sowie welche Präferenz er für die Clients besitzt.

IPv6-DHCP-Client

Der Befehl `show dhcpv6-client` zeigt den aktuellen Status des DHCP-Clients. Die Anzeige beinhaltet Informationen darüber, auf welchem Interface der Client aktiv ist sowie darüber, welche DNS-Server und Präfixe er hat.

IPv6-Route

Der Befehl `show ipv6-route` zeigt die vollständige Routing-Tabelle für IPv6 an. Die Anzeige kennzeichnet die im Router fest eingetragenen Routen durch den Anhang [static] und die dynamisch gelernten Routen durch den Anhang

[connected]. Die Loopback-Adresse ist durch [loopback] gekennzeichnet. Weitere automatisch generierte Adressen sind mit [local] markiert.

2.2.4.6 Umgebungsvariablen

Umgebungsvariablen sind geräteeigene globale Variablen mit vordefinierten Werten, die Sie überall an der Kommandozeile als dynamische Platzhalter einfügen können. Eine Übersicht der Umgebungsvariablen sowie deren Werte können Sie sich über die entsprechenden Kommandozeilen-Befehle ausgeben lassen (siehe unten).

Alle vordefinierten Umgebungsvariablen beginnen mit zwei Unterstrichen. In den Befehlen an der Kommandozeile leiten Sie die Variablen mit einem vorangestellten Dollarzeichen ein, wenn Sie explizit auf den Inhalt der Variablen zugreifen wollen.

Tabelle 10: Übersicht aller Umgebungsvariablen

Variablenname	Inhalt
`__BLDDEVICE`	Das Sub-Projekt des Gerätes. Das Sub-Projekt besteht in der Regel aus einer Zeichenkette ohne Leerzeichen und steht für das Hardware-Modell des aktuellen Gerätes.
`__DEVICE`	Der Typ des Gerätes, so wie er z. B. in LANconfig oder auf dem Typenschild des Gerätes angezeigt wird.
`__DEVICE_URL`	Der Typ des Gerätes, so wie er z. B. in LANconfig oder auf dem Typenschild des Gerätes angezeigt wird, wobei Leerzeichen durch ein '+' ersetzt werden.
`__FWBUILD`	Die Build-Nummer der aktuell im Gerät verwendeten Firmware. Die Build-Nummer ist eine vierstellige Zahl.
`__FWVERSION`	Die Versionsbezeichnung der aktuell im Gerät verwendeten Firmware in der Form 'x.yy'. Die Firmware-Version besteht aus der Major-Release vor dem Punkt und der Minor-Release nach dem Punkt.
`__LDRBUILD`	Die Build-Nummer des aktuell im Gerät installierten Loaders. Die Build-Nummer ist eine vierstellige Zahl.
`__LDRVERSION`	Die Versionsbezeichnung des aktuell im Gerät installierten Loaders in der Form 'x.yy'. Die Loader-Version besteht aus der Major-Release vor dem Punkt und der Minor-Release nach dem Punkt.
`__MACADDRESS`	Der Typ des Gerätes, angegeben als 12-stellige Zeichenkette hexadezimaler Werte in Kleinschreibung ohne Trennzeichen.
`__SERIALNO`	Die Seriennummer des Gerätes.
`__SYSNAME`	Die Systembezeichnung des Gerätes.
`__BOOTCAUSE`	Der Grund für den letzten Neustart des Gerätes, z. B. 'firmware upload'.

Nutzen Sie die folgenden Befehle in der Kommandozeile, um Umgebungsvariablen anzuzeigen oder zu verändern:

- `printenv`: Zeigt alle Umgebungsvariablen und deren aktuelle Werte an. Wenn Sie einer oder mehreren Umgebungsvariablen mit dem Befehl `setenv` einen Wert zugewiesen haben, zeigt die Ausgabe des Befehls `printenv` im oberen Teil den benutzerdefinierten Wert und im unteren Teil den Standardwert an.
- `echo $__device`: Zeigt den aktuellen Werte einer einzelnen Umgebungsvariablen an, in diesem Beispiel den Wert der Variablen `__DEVICE`.
- `setenv __device MeinWert`: Setzt den Wert einer Umgebungsvariablen auf den gewünschten Wert.
- `unsetenv __device`: Setzt den Wert einer Umgebungsvariablen auf den Standardwert zurück.

2.2.4.7 Tastenkombinationen für die Konsole

Mit den folgenden Tastenkürzeln lassen sich die Befehle auf der Kommandozeile bearbeiten.

Tabelle 11: Übersicht der Tastaturbefehle für die Kommandozeile

Tastenkürzel	Beschreibung
Pfeil nach oben	Springt in der Liste der letzten ausgeführten Befehle eine Position nach oben, in Richtung älterer Befehle.
Pfeil nach unten	Springt in der Liste der letzten ausgeführten Befehle eine Position nach unten, in Richtung neuerer Befehle.
Pfeil nach rechts	Bewegt die Einfügemarke eine Position nach rechts.
Pfeil nach links	Bewegt die Einfügemarke eine Position nach links.
Home oder Pos1	Bewegt die Einfügemarke an das erste Zeichen der Zeile.
Ende	Bewegt die Einfügemarke an das letzte Zeichen der Zeile.
Einfg	Schaltet um zwischen Einfügemodus und Überschreibemodus.
Entf	Löscht das Zeichen an der aktuellen Position der Einfügemarke oder beendet die Terminalsitzung, wenn die Zeile leer ist.
Backspace	Löscht das nächste Zeichen links neben der Einfügemarke.
Ctrl-U	Löscht alle Zeichen links neben der Einfügemarke.
Ctrl-K	Löscht alle Zeichen rechts neben der Einfügemarke.
Tabulator	Komplettiert die Eingabe von der aktuellen Position der Einfügemarke zu einem Befehl oder Pfad der LCOS-Menüstruktur: **1.** Wenn es genau eine Möglichkeit gibt, den Befehl bzw. den Pfad zu vervollständigen, so wird diese Möglichkeit in die Zeile übernommen. **2.** Wenn es mehrere Möglichkeiten gibt, den Befehl bzw. den Pfad zu vervollständigen, so wird dies durch einen Hinweiston beim Drücken der Tab-Taste angezeigt. Mit einem erneuten Druck auf die Tab-Taste wird eine Liste mit allen Möglichkeiten angezeigt, mit denen die Eingabe vervollständigt werden kann. Geben Sie dann z. B. einen weiteren Buchstaben ein, um ein eindeutiges Vervollständigen der Eingabe zu ermöglichen. **3.** Wenn es keine Möglichkeit gibt, den Befehl bzw. den Pfad zu vervollständigen, so wird dies durch einen Hinweiston beim Drücken der Tab-Taste angezeigt. Es werden keine weiteren Aktionen ausgeführt. Weitere Informationen zu den Besonderheiten der Tab-Taste beim Skripten finden Sie gesondert im Abschnitt *Tab-Kommando beim Scripting* auf Seite 75.

Tab-Kommando beim Scripting

Das `tab`-Kommando aktiviert beim Scripten die gewünschten Spalten einer Tabelle für das nachfolgende `set`-Kommando.

Bei der Konfiguration über die Konsole ergänzen Sie das set-Kommando in der Regel durch die Werte, die Sie den entsprechenden Spalten des Tabelleneintrags zuweisen möchten.

Die Werte für die Performance-Einstellungen eines WLAN-Interfaces setzen Sie z. B. wie folgt:

```
> cd /Setup/Interfaces/WLAN/Performance
> set ?

Possible Entries for columns in Performance:
[1][Ifc]                : WLAN-1 (1)
[5][QoS]                : No (0), Yes (1)
[2][Tx-Bursting]        : 5 chars from: 1234567890

> set WLAN-1 Yes *
```

In diesem Beispiel umfasst die Tabelle Performance drei Spalten:

- Ifc, also die gewünschte Schnittstelle
- Aktivieren oder Deaktivieren von QoS
- gewünschter Wert für das TX-Bursting

Mit dem Kommando `set WLAN-1 Yes *` aktivieren Sie für das Interface WLAN-1 die QoS-Funktion, den Wert für Tx-Bursting lassen Sie durch die Angabe des * unverändert.

Diese Schreibweise des `set`-Kommandos eignet sich gut für Tabellen mit wenigen Spalten. Tabellen mit sehr vielen Spalten hingegen stellen eine große Herausforderung dar. Die Tabelle unter **Setup** > **Interfaces** > **WLAN** > **Transmission** umfasst z. B. 22 Einträge:

```
> cd /Setup/Interfaces/WLAN/Transmission
> set ?

Possible Entries for columns in Transmission:
[1][Ifc]                 : WLAN-1 (1), WLAN-1-2 (16), WLAN-1-3 (17), WLAN-1-4 (18), WLAN-1-5 (19), WLAN-1-6
(20), WLAN-1-7 (21), WLAN-1-8 (22)
[2][Packet-Size]         : 5 chars from: 1234567890
[3][Min-Tx-Rate]         : Auto (0), 1M (1), 2M (2), 5.5M (4), 11M (6), 6M (8), 9M (9), 12M (10), 18M (11), 24M
 (12), 36M (13), 48M (14), 54M (15)
[9][Max-Tx-Rate]         : Auto (0), 1M (1), 2M (2), 5.5M (4), 11M (6), 6M (8), 9M (9), 12M (10), 18M (11), 24M
 (12), 36M (13), 48M (14), 54M (15)
[4][Basic-Rate]          : 1M (1), 2M (2), 5.5M (4), 11M (6), 6M (8), 9M (9), 12M (10), 18M (11), 24M (12), 36M
 (13), 48M (14), 54M (15)
[19][EAPOL-Rate]         : Like-Data (0), 1M (1), 2M (2), 5.5M (4), 11M (6), 6M (8), 9M (9), 12M (10), 18M (11),
 24M (12), 36M (13), 48M (14), 54M (15), HT-1-6.5M (28), HT-1-13M (29), HT-1-19.5M (30),
HT-1-26M (31), HT-1-39M (32), HT-1-52M (33), HT-1-58.5M (34), HT-1-65M (35), HT-2-13M (36), HT-2-26M (37),
HT-2-39M (38), HT-2-52M (39), HT-2-78M (40), HT-2-104M (41), HT-2-117M (42), HT-2-130M (43)
[12][Hard-Retries]       : 3 chars from: 1234567890
[11][Soft-Retries]       : 3 chars from: 1234567890
[7][11b-Preamble]        : Auto (0), Long (1)
[16][Min-HT-MCS]         : Auto (0), MCS-0/8 (1), MCS-1/9 (2), MCS-2/10 (3), MCS-3/11 (4), MCS-4/12 (5), MCS-5/13
 (6), MCS-6/14 (7), MCS-7/15 (8)
[17][Max-HT-MCS]         : Auto (0), MCS-0/8 (1), MCS-1/9 (2), MCS-2/10 (3), MCS-3/11 (4), MCS-4/12 (5), MCS-5/13
 (6), MCS-6/14 (7), MCS-7/15 (8)
[23][Use-STBC]           : No (0), Yes (1)
[24][Use-LDPC]           : No (0), Yes (1)
[13][Short-Guard-Interval]  : Auto (0), No (1)
[18][Min-Spatial-Streams] : Auto (0), One (1), Two (2), Three (3)
[14][Max-Spatial-Streams] : Auto (0), One (1), Two (2), Three (3)
[15][Send-Aggregates]    : No (0), Yes (1)
[22][Receive-Aggregates]: No (0), Yes (1)
[20][Max-Aggr.-Packet-Count]    : 2 chars from: 1234567890
[6][RTS-Threshold]       : 5 chars from: 1234567890
[10][Min-Frag-Len]       : 5 chars from: 1234567890
[21][ProbeRsp-Retries]   : 3 chars from: 1234567890
```

Mit dem folgenden Befehl setzen Sie in der Transmission-Tabelle das Short-Guard-Interval für das Interface WLAN-1-3 auf den Wert Nein:

```
> set WLAN-1-3 * * * * * * * * * * * * No
```



Die Sternchen für die Werte nach der Spalte für das Short-Guard-Interval sind in diesem Beispiel nicht erforderlich, die Spalten werden automatisch beim Setzen der neuen Werte ignoriert.

Alternativ zu dieser eher unübersichtlichen und fehleranfälligen Schreibweise definieren Sie im ersten Schritt mit dem `tab`-Kommando, welche Spalten der nachfolgende `set`-Befehl verändert:

```
> tab Ifc Short-Guard-Interval
> set WLAN-1-3 No
```

Der `tab`-Befehl erlaubt dabei auch, die Reihenfolge der gewünschten Spalten zu verändern. Das folgende Beispiel setzt für das Interface WLAN-1-3 den Wert für das Short-Guard-Interval auf `Nein` und den Wert für Use-LDPC auf `Ja`, obwohl die Tabelle die entsprechenden Spalten in einer anderen Reihenfolge anzeigt:

```
> tab Ifc Short-Guard-Interval Use-LDPC
> set WLAN-1-3 No Yes
```


Je nach Hardware-Modell enthalten die Tabellen nur einen Teil der Spalten. Der `tab`-Befehl ignoriert Spalten, die in der Tabelle des jeweiligen Geräts fehlen. So haben Sie die Möglichkeit, gemeinsame Scripte für unterschiedliche Hardware-Modelle zu entwickeln. Die `tab`-Anweisungen in den Scripten referenzieren dabei alle maximal erforderlichen Spalten. Je nach Modell führt das Script die `set`-Anweisungen allerdings nur für die tatsächlich vorhandenen Spalten aus.

Den `tab`-Befehl können Sie auch verkürzt über geschweifte Klammern darstellen. Mit dem folgenden Befehl setzen Sie in der Transmission-Tabelle das Short-Guard-Interval für das Interface WLAN-1-3 auf den Wert Nein:

```
> set WLAN-1-3 {short-guard} No
```

Die geschweiften Klammern ermöglichen ebenfalls, die Reihenfolge der gewünschten Spalten zu verändern. Das folgende Beispiel setzt für das Interface WLAN-1-3 den Wert für das Short-Guard-Interval auf `Nein` und den Wert für Use-LDPC auf `Ja`, obwohl die Tabelle die entsprechenden Spalten in einer anderen Reihenfolge anzeigt:

```
> set WLAN-1-3 {Short-Guard-Interval} No {Use-LDPC} Yes
```

2.2.4.8 Funktionstasten für die Konsole

Mit den Funktionstasten (den F-Tasten) auf der Tastatur haben Sie die Möglichkeit, häufig genutzte Befehlssequenzen zu speichern und an der Kommandozeile komfortabel aufzurufen.

Sie konfigurieren diese Funktion über das Setup-Menü unter **Config** > **Funktionstasten**. Wählen Sie dazu aus dem Auswahlmenü **Taste** eine der Funktionstasten F1 bis F12 aus und tragen Sie unter **Abbildung** die Befehlssequenz in der Form ein, wie Sie sie auch auf der Kommandozeile eingeben würden. Erlaubt sind alle an dem LCOS-Kommandozeilen-Interface möglichen Befehle bzw. Tastenkombinationen.

Besonderheiten beim Caret-Zeichen

Sofern Sie in Ihren Befehlen das Caret-Zeichen (^) verwenden, beachten Sie dabei, dass dieses auch dafür genutzt wird, um spezielle Steuerungsbefehle mit ASCII-Werten unterhalb von 32 abzubilden:

- ^A steht für Strg-A (ASCII 1)
- ^Z steht für Strg-Z (ASCII 26)
- ^[steht für Escape (ASCII 27)
- ^^ Ein doppeltes Caret-Zeichen steht für das Caret-Zeichen selbst.

Wenn Sie ein Caret-Zeichen direkt gefolgt von einem anderen Zeichen in ein Dialogfeld oder in einem Editor eingeben, wird das Betriebssystem diese Sequenz möglicherweise als ein anderes Sonderzeichen deuten. Aus der Eingabe von `Caret-Zeichen + A` macht ein Windows-Betriebssystem z. B. ein Â. Um das Caret-Zeichen selbst aufzurufen, geben Sie vor dem folgenden Zeichen ein Leerzeichen ein: Aus `Caret-Zeichen + Leerzeichen + A` wird dann die Sequenz ^A.

2.2.5 SNMP Management-Programm

Das Simple Network Management Protocol (SNMP) ermöglicht die Überwachung und Konfiguration von Geräten in einem Netzwerk von einer zentralen Instanz aus. Seit der ersten Veröffentlichung im Jahr 1988 entwickelte es sich im Laufe der Zeit weiter, um einer immer komplexeren Netzwerk-Infrastruktur sowie gesteigerten Ansprüchen an Sicherheit, Flexibilität und Komfort gerecht zu werden.

LCOS unterstützt die folgenden SNMP-Versionen:

- SNMPv1
- SNMPv2c
- SNMPv3

Neben den LANtools gibt es noch weitere Konfigurations- und Management-Programme, um mit einem entsprechenden SNMP-Agent ausgestattete Netzwerkkomponenten wie Router, Switche, Drucker, Firewalls etc. über SNMP zu überwachen oder zu steuern. Hierzu zählen insbesondere kommerzielle Programme, allerdings existieren auch zahlreiche Anwendungen auf Open-Source-, Freeware- oder Shareware-Basis.

Die für die Verwendung in SNMP-Programmen benötigte Geräte-MIB-Datei (Management Information Base) lässt sich bequem über WEBconfig (vgl. *SNMP-Geräte-MIB abrufen* auf Seite 38) oder an der Konsole über den Befehl `readmib` erzeugen.

2.3 LANCOM Layer 2 Management Protokoll (LL2M)

2.3.1 Einleitung

Alle Wege zur Konfiguration eines Geräts setzen eine IP-Verbindung zwischen dem Konfigurationsrechner und dem Gerät voraus. Egal ob LANconfig, WEBconfig oder Telnet – ohne IP-Verbindung können keine Befehle zur Konfiguration an das Gerät übertragen werden. Im Falle einer Fehlkonfiguration der TCP/IP-Einstellungen oder der VLAN-Parameter kann es vorkommen, dass diese benötigte IP-Verbindung nicht mehr hergestellt werden kann. In diesen Fällen hilft nur der Zugriff über die serielle Konfigurationsschnittstelle, die allerdings nicht bei allen Geräten verfügbar ist oder ein Reset des Gerätes auf den Auslieferungszustand. Beide Möglichkeiten setzen aber den physikalischen Zugriff auf das Gerät voraus, der z. B. bei der verdeckten Montage von Access Points nicht immer gegeben ist oder in größeren Szenarien erheblichen Aufwand darstellen kann.

Um auch ohne IP-Verbindung einen Konfigurationszugriff auf ein Gerät zu ermöglichen wird das **LANCOM Layer 2 Management Protokoll (LL2M)** verwendet. Dieses Protokoll benötigt nur eine Verbindung auf Layer 2, also auf dem direkt oder über Layer-2-Switches angebundenen Ethernet, um eine Konfigurationssitzung aufzubauen. LL2M-Verbindungen werden auf LAN- oder WLAN-Verbindungen unterstützt, nicht jedoch über das WAN. Die Verbindungen über LL2M sind passwortgeschützt und gegen Replay-Attacken resistent.

LL2M etabliert dazu eine Client-Server-Struktur: Der LL2M-Client schickt Anfragen oder Befehle an den LL2M-Server, der die Anfragen beantwortet oder die Befehle ausführt. Der LL2M-Client ist im LCOS integriert und wird über die Konsole ausgeführt. Der LL2M-Server ist ebenfalls im LCOS integriert und wird üblicherweise nur für eine kurze Zeitspanne nach dem Einschalten des Gerätes aktiviert. In diesem Zeitfenster kann ein Administrator mit Hilfe des LL2M-Clients Änderungen an der Konfiguration des Gerätes mit dem LL2M-Server vornehmen.

2.3.2 Konfiguration des LL2M-Servers

Die Aktivierung und Konfiguration des LL2M-Servers erfolgt ausschließlich über das Setup-Menü eines Gerätes. Die nachfolgenden Handlungsschritte zeigen Ihnen, welche Einstellungen erforderlich sind:

1. Wechseln Sie in WEBconfig oder in einem Terminalprogramm in den Menü-Zweig `Setup/Config/LL2M`.
2. Setzen Sie den Parameter **In-Betrieb** auf **ja**.
3. Tragen für das **Zeit-Limit** eine Zeitspanne in Sekunden ein, in der ein LL2M-Client den LL2M-Server nach dem Booten/Einschalten des Gerätes ansprechen kann.
   Nach Ablauf des Zeit-Limits wird der LL2M-Server automatisch deaktiviert. Der Wert '0' deaktiviert das Zeit-Limit; in diesem Zustand bleibt der LL2M-Server dauerhaft aktiv.

2.3.3 Befehle für den LL2M-Client

Für jeden LL2M-Befehl wird ein verschlüsselter Tunnel aufgebaut, der die bei der Übertragung übermittelten Anmeldeinformationen schützt. Zur Nutzung des integrierten LL2M-Clients starten Sie eine Terminalsitzung auf einem Gerät, das lokalen Zugriff über das verfügbare physikalische Medium (LAN, WLAN) auf den LL2M-Server hat. In dieser Konsolensitzung können Sie den LL2M-Server über die folgenden Befehle ansprechen:



Zum Ausführen der Befehle für den LL2M-Client müssen Sie über Root-Rechte auf dem LL2M-Server verfügen.

`LL2Mdetect`

Mit diesem Befehl schickt der LL2M-Client eine SYSINFO-Anfrage an den LL2M-Server. Der Server sendet daraufhin seine Systeminformationen wie Hardware, Seriennummer etc. zur Anzeige an den Client zurück. Der LL2Mdetect-Befehl lässt sich mit folgenden Parametern einschränken:

-a <MAC-Adresse>

Schränkt den Befehl nur auf die Geräte mit der angegebenen MAC-Adresse ein. Die MAC-Adresse geben Sie in der Form `00a057010203`, `00-a0-57-01-02-03` oder `00:a0:57:01:02:03` an.

Wird keine MAC-Einschränkung gesetzt, geht der detect als Multicast (oder via `-b` alternativ als Broadcast) an alle LL2M-fähigen Geräte. Einzelne Stellen der MAC-Adresse können mit einem `*` oder `x` als Platzhalter besetzt werden, um Gruppen von MAC-Adressen anzusprechen, z. B. `00-a0-57-xx-xx-xx` für alle Geräte-MAC-Adressen.

In einer Befehlszeile mit mehreren Parametern **muss** `-a` der abschließende Parameter sein. Eine andere Reihenfolge ist nicht zulässig.

-b

Versendet die LL2Mdetect-Anfrage explizit als Broadcast und nicht als Multicast.

-f <Version>

Schränkt den Befehl nur auf die Geräte der entsprechenden Firmware-Version ein.

-r <Hardware-Release>

Schränkt den Befehl nur auf die Geräte des entsprechenden Hardware-Releases ein.

-s <Serialnumber>

Schränkt den Befehl nur auf die Geräte der entsprechenden Seriennummer ein.

-t <Hardware-Type>

Schränkt den Befehl nur auf die Geräte des entsprechenden Hardware-Typs ein.

-v <VLAN-ID>

Versendet die LL2Mdetect-Anfrage nur auf dem angegebenen VLAN. Wenn keine VLAN-ID angegeben ist, wird die VLAN-ID des ersten definierten IP-Netzwerks verwendet.

Die Befehlszeile `ll2mdetect -r A` zum Beispiel versendet eine SYSINFO-Anfrage an alle Geräte mit der Hardware-Release 'A'. Die Antwort des LL2M-Servers enthält dann die folgenden Angaben:

- Name des Gerätes
- Gerätetyp
- Seriennummer
- MAC-Adresse
- Hardware-Release
- Firmware-Version mit Datum

LL2Mexec

Mit diesem Befehl schickt der LL2M-Client ein einzeiliges Kommando zur Ausführung an den LL2M-Server. Mehrere Kommandos lassen sich durch Semikola getrennt in einem LL2M-Befehl kombinieren. Je nach Kommando werden Aktionen auf dem entfernten Gerät ausgeführt und die Rückmeldungen des entfernten Gerätes zur Anzeige an den LL2M-Client übertragen. Der LL2Mexec-Befehl entspricht folgender Syntax:

```
ll2mexec <User>[:<Password>]@<MAC-Address>
```

Der LL2Mexec-Befehl lässt sich mit folgenden Parametern einschränken:

`-i <WLAN-Interface>`

Versendet den LL2Mexec-Befehl nur über das angegebene WLAN-Interface.

`-v <VLAN-ID>`

Versendet den LL2Mexec-Befehl nur auf dem angegebenen VLAN. Wenn keine VLAN-ID angegeben ist, wird die VLAN-ID des ersten definierten IP-Netzwerks verwendet.

Die Befehlszeile `ll2mexec root@00a057010203 set /setup/name MyDevice` zum Beispiel meldet den LL2M-Client als 'root' auf dem LL2M-Server mit der MAC-Adresse '00a057010203' an. Da das Passwort weggelassen wurde, sucht das Gerät zunächst nach dem entsprechenden Nutzernamen in der lokalen Datenbank und setzt automatisch das für diesen Nutzer gespeicherte Passwort ein. Wird auch der Nutzername weggelassen, werden die Anmeldedaten des aktuell für die CLI-Sitzung registrierten Nutzers verwendet. Dann setzt der LL2M-Client den Namen des entfernten Gerätes auf den Wert 'MyDevice'.

2.4 Speichern und Laden von Gerätekonfiguration und Skriptdateien

Die Konfigurationsdatei eines Gerätes umfasst seine kompletten Einstellungen. Und mit Hilfe von Script-Dateien lassen sich die Einstellungen eines Gerätes automatisiert verwalten. Zum Schutz dieser Dateien vor unberechtigtem Zugriff oder Übertragungsfehlern ist es möglich, sie verschlüsselt und mit einer Prüfsumme versehen aus dem Gerät zu exportieren oder in das Gerät zu laden.

Es existieren somit grundsätzlich drei verschiedene Dateitypen:

- Keine Prüfsumme, keine Verschlüsselung: Eine Textdatei, deren Inhalt mit einem Texteditor lesbar ist.
- Prüfsumme: Die Textdatei enthält Informationen über die Prüfsumme sowie den Hash-Algorithmus zur Berechnung dieser Prüfsumme. Der Inhalt dieser Textdatei ist mit einem einfachen Texteditor lesbar.

  Ein LANconfig vor Version 9.10 erkennt auch Dateien mit Prüfsummen.

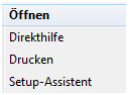
- Verschlüsselung: Vor dem Export verschlüsselt das Gerät die Datei mit einem vom Administrator gewählten Passwort. Die Textdatei enthält Informationen über den verwendeten Verschlüsselungsalgorithmus sowie eine Prüfsumme. Der Inhalt der Textdatei ist bis auf den Dateiheader mit einem Texteditor nicht mehr entzifferbar.

  Ein LANconfig vor Version 9.10 erkennt verschlüsselte Dateien nicht.

Die Dateiendungen dieser Dateien sind jeweils `.lcf` für Konfigurationsdateien oder `.lcs` für Skriptdateien.

Die Erkennung, ob es sich um verschlüsselte oder mit Prüfsummen versehene Dateien handelt, geschieht ausschließlich über den Dateiheader.

Über den Kontextdialog des Windows-Explorers können Sie die folgenden Funktionen ausführen:



Öffnen

Dieser Menüpunkt öffnet die Konfiguration der Datei über LANconfig.

Dieser Punkt erscheint nur bei Konfigurations-Dateien mit der Endung `.lcf`.

Direkthilfe

Dieser Menüpunkt öffnet einen Hilfetext, der Benutzerinformationen über den Umgang mit dieser Datei gibt.

Drucken

Mit diesem Menüpunkt drucken Sie die Datei aus.

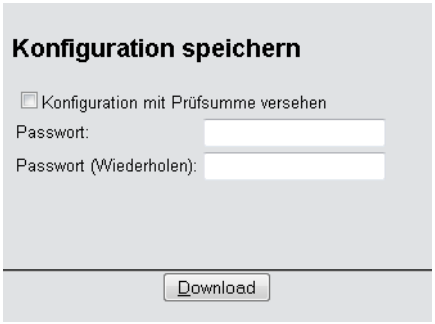
Setup-Assistent

Dieser Menüpunkt startet den LANconfig-Setup-Assistenten.

Dieser Punkt erscheint nur bei Konfigurations-Dateien mit der Endung `.lcf`.

2.4.1 Konfigurationsverwaltung über WEBconfig und Konsole

Um über WEBconfig eine Konfigurationsdatei zu exportieren, wechseln Sie in die Ansicht **Extras** > **Dateimanagement** > **Konfiguration speichern**.



Folgende Optionen stehen zur Auswahl:

Keine Angaben

In der Standardeinstellung sind alle Optionen deaktiviert. Nach einem Klick auf **Download** startet der Dialog zum Download einer unverschlüsselten Konfigurationsdatei ohne Prüfsumme.

Konfiguration mit Prüfsumme versehen

Nach einem Klick auf **Download** startet der Dialog zum Download einer unverschlüsselten Konfigurationsdatei mit Prüfsumme.

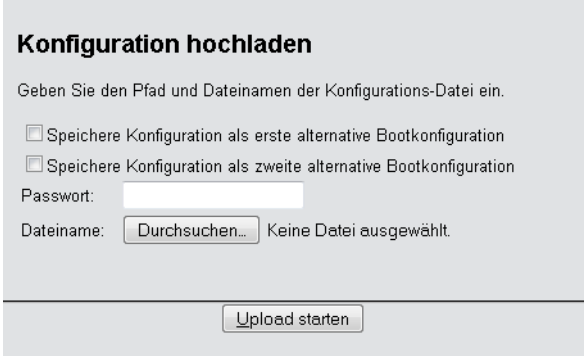
Passwort

Geben Sie ein Passwort an, wenn Sie die Konfigurationsdatei vor dem Download verschlüsseln möchten.

Um die Konfiguration über die Konsole zu sichern, verwenden Sie die folgenden Parameter:

- `readconfig`: Sichert die Konfiguration ohne Prüfsumme und Verschlüsselung.
- `readconfig -h`: Ergänzt die Konfigurationsdatei um eine Prüfsumme.
- `readconfig -s <password>`: Verschlüsselt die Konfigurationsdatei auf Basis des angegebenen Passwortes.

Um über WEBconfig eine Konfigurationsdatei in das Gerät zu laden, wechseln Sie in die Ansicht **Extras** > **Dateimanagement** > **Konfiguration hochladen**.

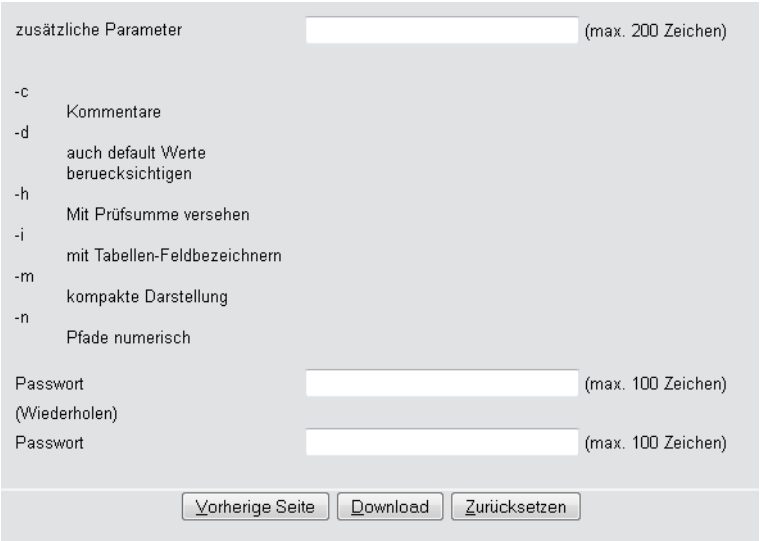


Geben Sie zusätzlich das entsprechende Passwort ein, wenn die Konfigurationsdatei verschlüsselt ist, und klicken Sie auf **Upload starten**.

Weitere Informationen zu alternativen Boot-Konfigurationen finden Sie im Abschnitt *Alternative Boot-Config*.

2.4.2 Skriptverwaltung über WEBconfig und Konsole

Um über WEBconfig eine Skriptdatei zu exportieren, wechseln Sie in die Ansicht **Extras** > **Dateimanagement** > **Konfigurations-Skript speichern**.



Folgende Optionen stehen zur Auswahl:

zusätzliche Parameter

In der Standardeinstellung sind alle Optionen deaktiviert. Nach einem Klick auf **Download** startet der Dialog zum Download einer unverschlüsselten Skriptdatei ohne Prüfsumme.

Passwort

Geben Sie ein Passwort an, wenn Sie die Skriptdatei vor dem Download verschlüsseln möchten.

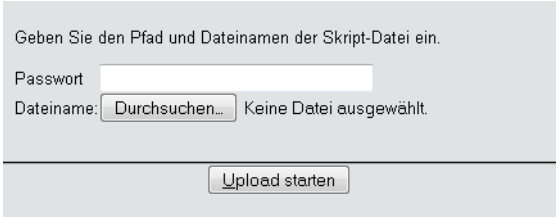
Um die Skriptdatei über die Konsole zu sichern, verwenden Sie z. B. die folgenden Parameter:

› `readscript`: Sichert die Konfiguration ohne Prüfsumme und Verschlüsselung.

- `readscript -h`: Ergänzt die Konfigurationsdatei um eine Prüfsumme.
- `readscript -s <password>`: Verschlüsselt die Konfigurationsdatei auf Basis des angegebenen Passwortes.
- `readscript -o <password>`: Verschlüsselt die Konfigurationsdatei auf Basis des angegebenen Passwortes.
- `readscript -o`: Ersetzt die Passwörter durch ein "*", sodass diese nicht in der Textausgabe sichtbar sind.

Mehr Informationen zu den Parametern finden Sie im Abschnitt *Befehle für die Konsole* in der Zeile für `readscript`.

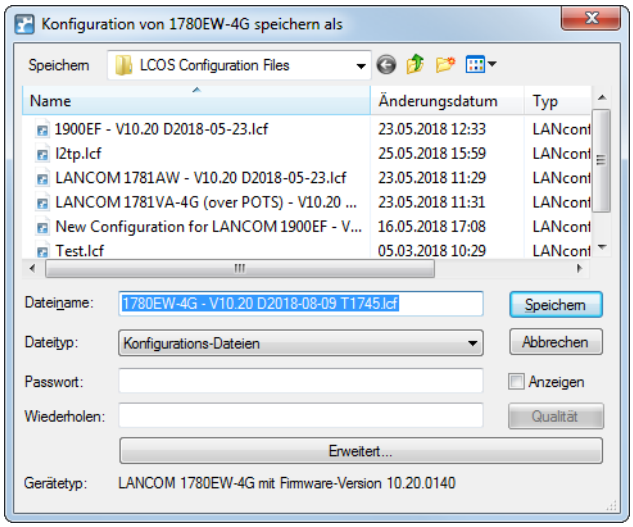
Um über WEBconfig eine Skriptdatei in das Gerät zu laden, wechseln Sie in die Ansicht **Extras** > **Dateimanagement** > **Konfigurations-Skript anwenden**.



Geben Sie zusätzlich das entsprechende Passwort ein, wenn die Skriptdatei verschlüsselt ist, und klicken Sie auf **Upload starten**.

2.4.3 Konfigurationsverwaltung über LANconfig

Um über LANconfig eine Konfigurationsdatei zu speichern, klicken Sie in der Liste der Geräte mit der rechten Maustaste auf das Gerät, dessen Konfiguration Sie speichern möchten. Öffnen Sie im Kontextdialog unter **Konfigurations-Verwaltung** > **Als Datei sichern** den Speicherdialog.



Folgende Angaben stehen zur Auswahl:

Dateiname

LANconfig belegt den Dateinamen mit verschiedenen Angaben vor (u. a. Versionsnummer, Datum und Uhrzeit). Ändern Sie den Namen Ihren Anforderungen entsprechend.

Dateityp

Wählen Sie, ob es sich um eine Konfigurationsdatei oder etwas anderes handelt.

Passwort

Geben Sie ein Passwort an, wenn Sie die Konfigurationsdatei vor dem Download verschlüsseln möchten.

Unter **Erweitert** bestimmen Sie weitere, optionale Parameter, die das Gerät beim automatischen Laden einer Konfigurations-Datei (Auto-Load) auswertet. Hiermit individualisieren Sie die Konfiguration.

Um über LANconfig eine Konfigurationsdatei in das Gerät zu laden, klicken Sie in der Liste der Geräte mit der rechten Maustaste auf das Gerät, in das Sie eine Konfiguration laden möchten. Öffnen Sie im Kontextdialog unter **Konfigurations-Verwaltung** > **Aus Datei wiederherstellen** den Uploaddialog.

Wählen Sie die gewünschte Konfigurationsdatei aus, geben Sie ggf. das benötigte Passwort an und klicken Sie auf **Öffnen**, um die Konfiguration in das Gerät zu laden.

2.5 Alternative Boot-Konfiguration

2.5.1 Einleitung

Das Verhalten der Geräte im Betrieb wird durch die Konfiguration bestimmt. Diese benutzerdefinierte Konfiguration wird in einem speziellen Bereich des Flash-Speichers abgelegt, der auch bei einem Neustart des Gerätes erhalten bleibt (Konfigurationsspeicher).

Im Auslieferungszustand ist der Konfigurationsspeicher leer, da das Gerät noch nicht über eine benutzerdefinierte Konfiguration verfügt. Im späteren Betrieb kann der Konfigurationsspeicher bei Bedarf durch einen Konfigurations-Reset wieder gelöscht werden. Wird ein Gerät mit leerem Konfigurationsspeicher gestartet oder gebootet, werden die Werte aus einer Boot-Konfiguration verwendet, welche die Standardwerte für das jeweilige Modell enthält.

Erst bei der Änderung von mindestens einem Konfigurationsparameter wird der Konfigurationsspeicher beschrieben. Dabei wird die komplette Konfiguration im Konfigurationsspeicher abgelegt. Auch wenn z. B. nur der Gerätename geändert wird, werden alle für das jeweilige Modell verfügbaren Parameter mit aktuellen Werten in der benutzerdefinierten Konfiguration gespeichert. Die Werte für die Parameter, die nicht geändert wurden, werden dabei aus einer Boot-Konfiguration übernommen.

Die Geräte können drei verschiedene Boot-Konfigurationen nutzen:

Werkseinstellungen

Diese enthält die Standardwerte für das jeweilige Modell im Auslieferungszustand. Die Standard-Boot-Konfiguration ist in der jeweiligen Firmware des Gerätes enthalten.

Kundenspezifische Standardeinstellungen

Diese enthält die kundenspezifischen Standardwerte für das jeweilige Modell für den Fall, dass der Konfigurationsspeicher leer ist, die Werkseinstellungen aber nicht verwendet werden sollen. Mit dieser Funktion werden die Geräte persistent (über beliebig viele Boot- / Reset-Vorgänge hinweg) mit kundenspezifischen Vorgabewerten für den Neustart versehen. Die kundenspezifischen Standardeinstellungen werden bei einem Konfigurations-Reset **nicht** gelöscht. Die kundenspezifischen Standardeinstellungen werden auf dem ersten Boot-Speicherplatz abgelegt.

Rollout-Konfiguration

Diese Konfiguration wird in größeren Roll-Out-Szenarien verwendet, wenn für zahlreiche Geräte eine von den Werkseinstellungen abweichende Boot-Konfiguration verwendet werden soll. Die Rollout-Konfiguration muss durch eine entsprechende Bedienung des Reset-Tasters aktiviert werden. Die spezielle Rollout-Konfiguration wird auf dem zweiten Boot-Speicherplatz abgelegt.

2.5.2 Verwenden der Boot-Konfigurationen

Bei einem normalen Start nutzen die Geräte die möglichen Konfigurationen in einer definierten Reihenfolge:

1. Benutzerdefinierte Konfiguration (im Konfigurationsspeicher)
2. Kundenspezifische Standardeinstellungen (auf dem ersten Boot-Speicherplatz)
3. Werkseinstellungen (in der Firmware des Gerätes)

Die kundenspezifischen Standardeinstellungen werden also automatisch und vorrangig vor den Werkseinstellungen verwendet, wenn der Konfigurationsspeicher leer ist.

Besonderheiten der Rollout-Konfiguration

Die Verwendung der Rollout-Konfiguration wird über den Reset-Taster ausgelöst. Der Reset-Taster hat verschiedene Funktionen, die durch unterschiedlich lange Betätigungszeiten des Tasters ausgelöst werden:

- **weniger als 5 Sekunden**:

  Booten (Neustart); dabei wird die benutzerdefinierte Konfiguration aus dem Konfigurationsspeicher geladen. Wenn die benutzerdefinierte Konfiguration leer ist, werden die kundenspezifischen Standardeinstellungen (erster Speicherplatz) geladen. Das Laden der kundenspezifischen Standardeinstellungen wird angezeigt, indem alle LEDs des Geräts einmal kurzzeitig rot aufleuchten. Wenn auch der erste Speicherplatz leer ist, werden die Werkseinstellungen geladen.

- **mehr als 5 Sekunden** bis zum **ersten** Aufleuchten aller LEDs am Gerät:

  Konfigurations-Reset (Löschen des Konfigurationsspeichers) und anschließender Neustart. Damit werden die kundenspezifischen Standardeinstellungen (erster Speicherplatz) geladen. Das Laden der kundenspezifischen Standardeinstellungen wird angezeigt, indem alle LEDs des Geräts einmal kurzzeitig rot aufleuchten. Wenn der erste Speicherplatz leer ist, werden die Werkseinstellungen geladen.

- **mehr als 15 Sekunden** bis zum **zweiten** Aufleuchten aller LEDs am Gerät:

  Aktivieren der Rollout-Konfiguration und Löschen der benutzerdefinierten Konfiguration. Nach dem Neustart wird die Rollout-Konfiguration (zweiter Speicherplatz) geladen. Das Laden der Rollout-Konfiguration wird angezeigt, indem alle LEDs des Geräts zweimal kurzzeitig rot aufleuchten. Wenn der zweite Speicherplatz leer ist, werden die Werkseinstellungen geladen.

Die Rollout-Konfiguration wird jeweils nur einmalig direkt nach dem Neustart verwendet, wenn der Reset-Taster für mehr als 15 Sekunden gedrückt wurde. Nach dem nächsten Neustart gilt automatisch wieder die normale Boot-Reihenfolge wie oben angegeben.

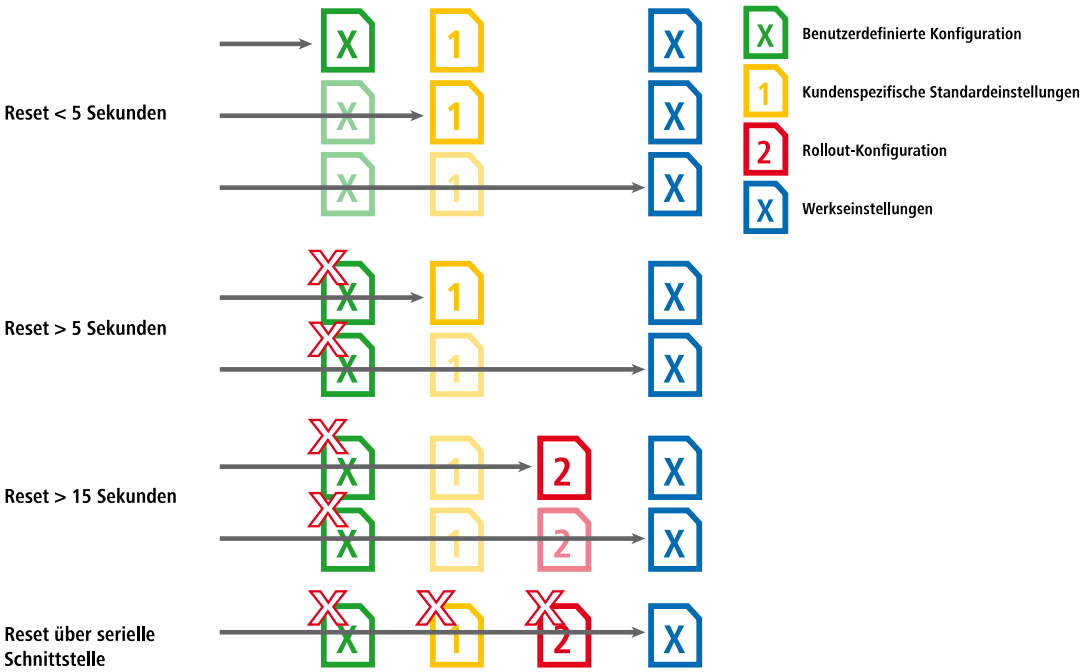
Wenn der Reset-Knopf in der Konfiguration deaktiviert ist (Einstellung **Ignorieren** oder **Nur-Booten**), wird das Laden der Rollout-Konfiguration unmöglich gemacht.

Beispiele

Die folgende Grafik zeigt, welche Konfiguration bei unterschiedlichen Reset-Vorgängen je nach Zustand des Gerätes geladen wird.

- Bei Drücken des Reset-Knopfs für **weniger als 5 Sekunden** wird die benutzerdefinierte Konfiguration geladen. Existiert keine benutzerdefinierte Konfiguration, greift das Gerät auf die kundenspezifischen Standardeinstellungen zurück. Sind diese ebenfalls nicht vorhanden, werden die Werkseinstellungen geladen.

› Bei Drücken des Reset-Knopfs für **mehr als 15 Sekunden** wird die benutzerdefinierte Konfiguration gelöscht und die Rollout-Konfiguration geladen. Wenn die Rollout-Konfiguration nicht vorhanden ist, werden die Werkseinstellungen geladen.



2.5.3 Speichern und Hochladen der Boot-Konfigurationen

Speichern

Sowohl die kundenspezifischen Standardeinstellungen als auch die Rollout-Konfiguration werden in einem komprimierten Format gespeichert. Über die Konsole haben Sie die Möglichkeit, die aktuelle Konfiguration eines Gerätes wahlweise als kundenspezifische Standardeinstellung oder Rollout-Konfiguration abzulegen. Nutzen Sie dazu einen der folgenden Befehle:

```
bootconfig --savecurrent [1,2,all]
```

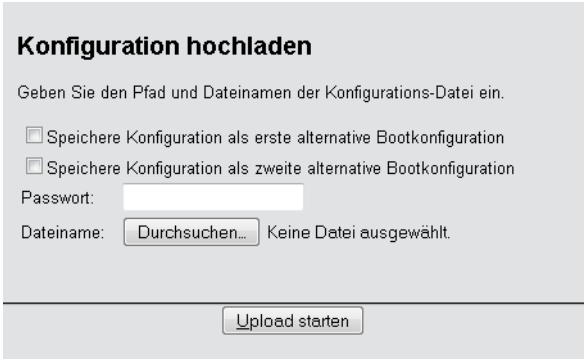
```
bootconfig -s [1,2,all]
```

Mit der entsprechenden Ziffer wird entweder der erste Boot-Speicherplatz für die kundenspezifischen Standardeinstellungen oder der zweite Boot-Speicherplatz für die Rollout-Konfiguration ausgewählt. Mit der Angabe des Parameters `all` wird die aktuelle Konfiguration gleichzeitig in beide Speicherplätze geschrieben.

Hochladen

Die kundenspezifischen Standardeinstellungen oder die Rollout-Konfiguration können Sie in WEBconfig unter **Extras** > **Dateimanagement** > **Konfiguration hochladen** in das Gerät zu laden: Wählen Sie die zu verwendende Konfigurationsdatei aus und aktivieren Sie den Verwendungszweck als kundenspezifische Standardeinstellungen (erster

Speicherplatz) und / oder Rollout-Konfiguration (zweiter Speicherplatz). Alternative Bootkonfigurationen müssen als *.lcf-Datei vorliegen.



Wenn beide Speicherplätze der Boot-Konfigurationen belegt (also kundenspezifische Standardeinstellungen **und** Rollout-Konfiguration gespeichert) sind, lässt sich das Gerät nicht mehr über den Reset-Taster auf die Werkseinstellungen zurücksetzen. Gehen Sie für einen Geräte-Reset stattdessen so vor, wie unter *Firmware-Upload über Outband mit Rücksetzen der Konfiguration* auf Seite 91 beschrieben.

Für Geräte, die ausschließlich eine Boot-Konfiguration erlauben, gilt die o. g. Einschränkung nicht. Sie lassen sich immer über den Reset-Taster auf die Werkseinstellungen zurücksetzen.

Geben Sie zusätzlich das entsprechende Passwort ein, wenn die Konfigurationsdatei verschlüsselt ist.

2.5.4 Löschen der Boot-Konfigurationen

Die alternative und die spezielle Boot-Konfiguration können nicht über die normalen Datei-Funktionen gelöscht werden. Nutzen Sie stattdessen an der Konsole einen der folgenden Befehle:

```
bootconfig --remove [1,2,all]
bootconfig -r [1,2,all]
```

Mit der entsprechenden Ziffer wird der zu löschende Boot-Speicherplatz ausgewählt. Mit der Angabe des Parameters `all` werden gleichzeitig beide Speicherplätze gelöscht.

2.5.5 Verwendung von Zertifikaten

Für die Nutzung durch VPN und SSL / TLS nach einem Konfigurations-Reset kann ein **Standardzertifikat** als **PKCS#12-Container** im Gerät gespeichert werden. Dieses Standardzertifikat wird nur von den kundenspezifischen Standardeinstellungen und der Rollout-Konfiguration verwendet:

- Wenn die kundenspezifischen Standardeinstellungen geladen werden, wird das Standardzertifikat in den normalen Zertifikatsspeicher für VPN und SSL / TLS kopiert; somit steht es auch nach einem Reboot zur Verfügung.
- Wenn die Rollout-Konfiguration geladen wird, wird das Standardzertifikat für VPN verwendet, aber nicht kopiert; d. h. nach einem Neustart (auch ohne Konfigurations-Reset) kann das Gerät darauf nicht mehr zugreifen.

Das Standardzertifikat können Sie wahlweise über LANconfig oder WEBconfig in das Gerät laden.

Das Hochladen von Zertifikaten ist u. a. im Kapitel *Zertifikate in das Gerät laden* auf Seite 784 erklärt.

2.6 FirmSafe

2.6.1 Einleitung

FirmSafe macht das Einspielen der neuen Software zur sicheren Sache: Die gerade verwendete Firmware wird dabei nicht einfach überschrieben, sondern es wird eine zweite Firmware zusätzlich im Gerät gespeichert (symmetrisches FirmSafe). Damit ist Ihr Gerät insbesondere auch gegen die Folgen eines Stromausfalls oder einer Verbindungsunterbrechung während des Firmware-Uploads geschützt.

Von den beiden im Gerät gespeicherten Firmware-Versionen kann immer nur eine aktiv sein. Beim Laden einer neuen Firmware wird die nicht aktive Firmware überschrieben. Sie können durch Auswahl des FirmSafe-Modus selbst entscheiden, welche Firmware nach dem Upload aktiviert werden soll.

2.6.2 Konfiguration

Den Modus für den Firmware-Upload stellen Sie im Setup-Menü unter **Firmware** > **Modus-Firmsafe** ein. Dabei stehen Ihnen drei verschiedene Modi zur Auswahl. In LANconfig haben Sie im Rahmen des Firmware-Uploads die Möglichkeit, entweder eine dem Modus 'unmittelbar' oder 'manuell' äquivalente Einstellung zu treffen (vgl. *Firmware-Upload über LANconfig* auf Seite 90).

- **unmittelbar**: In diesem Modus aktiviert das Gerät eine hochgeladene Firmware nach dem Ende des Uploads sofort und endgültig. Folgende Szenarien sind daraufhin denkbar:
  - Der Start mit der neuen Firmware verläuft erfolgreich und das Gerät arbeitet anschließend wie gewünscht.
  - Das Gerät ist nach dem Ladevorgang der neuen Firmware nicht mehr ansprechbar. Sofern das Gerät nicht automatisch auf eine vorherige Firmware zurückfällt oder mit einer Minimal-Firmware startet, können Sie den Upload z. B. via LL2M wiederholen. Tritt schon während des Uploads ein Fehler auf, aktiviert das Gerät automatisch die bisherige Firmware und startet damit neu.
- **login**: In diesem Modus aktiviert das Gerät eine hochgeladene Firmware nur temporär, um Probleme mit einem fehlerhaften Upload vorzubeugen. Nach der Aktivierung wartet das Gerät für die im Setup-Menü unter **Firmware** > **Timeout-Firmsafe** eingestellte Zeit (in Sekunden) auf einen erfolgreichen Login über ein Terminalprogramm oder WEBconfig. Nur wenn dieser Login erfolgt, wird die neue Firmware auch dauerhaft aktiviert.

  Wenn das Gerät nach dem Aktivieren der Firmware nicht mehr ansprechbar ist oder ein Login aus anderen Gründen unmöglich ist, dann aktiviert es nach Ablauf des Timeouts automatisch wieder die vorherige Firmware und startet neu.
- **manuell**: In diesem Modus aktiviert das Gerät eine hochgeladene Firmware nur temporär, um Probleme mit einem fehlerhaften Upload vorzubeugen. Nach der Aktivierung wartet das Gerät für die im Setup-Menü unter **Firmware** > **Timeout-Firmsafe** eingestellte Zeit (in Sekunden) darauf, dass Sie die geladene Firmware von Hand endgültig aktivieren und damit dauerhaft wirksam machen.

  Unter LANconfig aktivieren Sie die neue Firmware über den Menüpunkt **Gerät** > **Firmware-Verwaltung** > **Im Test laufende Firmware freischalten**. Im Setup-Menü aktivieren Sie die Firmware unter **Firmware** > **Tabelle-Firmsafe**. Auf der Konsole verwenden Sie dafür den Befehl `set # active`; '#' steht dabei für die Position der Firmware in der FirmSafe-Tabelle.

  Auch hier wechselt das Gerät nach Ablauf des Timeouts automatisch wieder auf die vorherige Firmware und startet neu.



Das Laden einer zweiten Firmware ist nur dann möglich, wenn das Gerät über ausreichenden Speicherplatz für zwei vollständige Firmwareversionen verfügt. Aktuelle Firmwareversionen (ggf. mit zusätzlichen Software-Optionen) können bei älteren Hardwaremodellen manchmal mehr als die Hälfte des verfügbaren Speicherplatzes beanspruchen. In diesem Fall wird das *asymmetrische FirmSafe* verwendet.

2.6.3 Aktive Firmware über Konsolenbefehl umschalten

Ab LCOS-Version 10.12 kann mit einem Kommando die aktuelle Firmware auf die alternative Firmware umgeschaltet werden. Hierbei wird die zuvor inaktive Firmware auf „aktiv" gesetzt und die bislang aktive Firmware auf „inaktiv". Das Gerät führt nach Eingabe des Kommandos automatisch ohne weitere Bestätigung einen Neustart aus.

Geben Sie unter **/Firmware** den Befehl `do Switch-Firmware` ein.

Der Neustart wird automatisch ausgeführt.

2.6.4 Asymmetrisches FirmSafe

Durch den großen und sich stetig erweiternden Funktionsumfang der Firmware ist es nicht bei allen Geräten möglich, zwei vollwertige Firmware-Versionen gleichzeitig zu speichern. Für solche Geräte existiert stattdessen das asymmetrische FirmSafe.

Beim asymmetrischen FirmSafe enthält das Gerät immer eine „vollständige Firmware" sowie eine sogenannte „Minimal-Firmware". Die Minimal-Firmware wird normalerweise nicht gestartet – sie erlaubt jedoch nach einem fehlgeschlagenen Upload einer vollständigen Firmware (z. B. durch Stromausfall während des Uploads) den lokalen Zugriff auf das Gerät (über LAN, WLAN oder die Config-Schnittstelle), um eine funktionsfähige Firmware in das Gerät zu laden.

Die Minimal-Firmware ist **nicht** konfigurierbar! Änderungen in der Konfiguration über LANconfig, WEBconfig oder Telnet werden nicht in das Gerät gespeichert. Auch alle erweiterten Funktionalitäten – insbesondere die Remote-Administration über WAN – sind **nicht** verfügbar, solange die Minimal-Firmware aktiv ist! Allerdings ist auch in einer Minimal-Firmware der LL2M-Server aktiv und bietet so eine Zugriffsmöglichkeit auf das Gerät, sofern es über Layer 2 (Ethernet) von einem LL2M-Client erreichbar ist.

2.6.4.1 Umstellung auf asymmetrisches FirmSafe

Zur Umstellung der Geräte auf das asymmetrische FirmSafe laden Sie zunächst eine Konverter-Firmware in das Gerät. Dieser Konverter wandelt die vom Gerät aktuell **nicht aktive** Firmware in eine Minimal-Firmware um und schafft so Platz für eine neue, umfangreichere Firmware. Dieser Vorgang muss nur einmal vorgenommen werden.

Anschließend können Sie eine neue vollständige Firmware in das Gerät laden, die bei einem erfolgreichen Upload aktiviert wird. Die Minimal-Firmware verbleibt zur Sicherung der Erreichbarkeit im Gerät.

2.6.4.2 Firmware-Upgrade mit asymmetrischem FirmSafe

Bei jedem folgenden Firmware-Upload wird automatisch immer die **aktive** Firmware durch eine neue Firmware ersetzt.

2.7 Firmware über einen Client ins Gerät laden

Der Upload einer Firmware – also das Einspielen der Geräte-Software – kann auf verschiedenen Wegen erfolgen: beispielsweise über LANconfig, WEBconfig oder ein Terminalprogramm. Dabei stehen Ihnen unterschiedliche Protokolle zur Auswahl.

Bei einem Upload bzw. Update der Firmware bleiben im Normalfall alle Einstellungen Ihres Gerätes erhalten (Ausnahme: *Upload mit Reset*). Trotzdem sollten Sie sicherheitshalber ein vollständiges Backup Ihrer Konfiguration anlegen. Außerdem sollten Sie ein Backup der bisherigen Firmware bereithalten für den Fall, dass der Update-Vorgang fehlschlägt und das Gerät z. B. auf eine Minimal-Firmware zurückfällt, welche keinen Internet-Zugang zulässt. Wenn Ihnen die entsprechende Firmware-Datei nicht mehr zur Verfügung steht, suchen Sie auf *www.lancom-systems.de*.

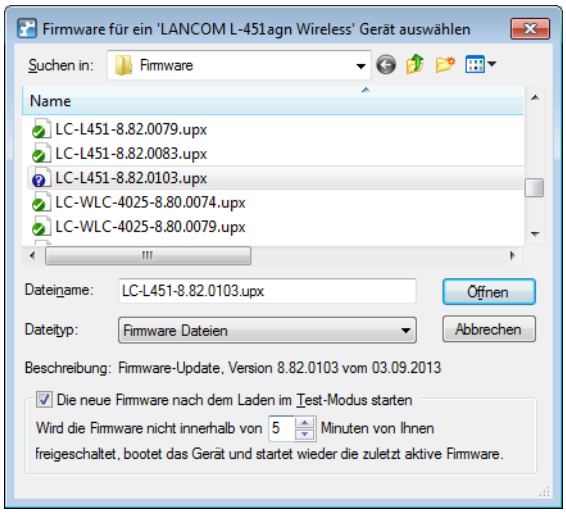
Enthält die neu eingespielte Firmware Parameter, die in der aktuellen Firmware des Gerätes nicht vorhanden sind, werden die fehlenden Werte mit den Default-Einstellungen ergänzt.

2.7.1 Firmware-Upload über LANconfig

Dieser Abschnitt beschreibt, wie Sie über LANconfig eine andere Firmware in das Gerät laden.

1. Markieren Sie das gewünschte Gerät in der Auswahlliste und wählen Sie **Gerät** > **Firmware-Verwaltung** > **Neue Firmware hochladen**.
2. Wählen Sie im sich öffnenden Dialogfenster das Verzeichnis aus, in dem sich die neue Version befindet, und markieren die entsprechende *.upx-Datei.

   LANconfig informiert Sie dann in der Beschreibung über Art, Version und Release-Datum der Firmware.



3. Optional: Wählen Sie aus, ob das Gerät die Firmware nach dem Laden dauerhaft aktivieren oder zunächst in einem Test-Modus betreiben soll. Sofern Sie sich für den Test-Modus entscheiden, geben Sie einen Zeitraum an, nach dem das Gerät wieder zur vorherigen Firmware wechselt, wenn Sie die Firmware über die ***Konfigurations-Verwaltung*** nicht aus diesem Modus heraus freischalten.

   Diese Auswahlmöglichkeit besteht nicht für Geräte, die mit *asymmetrischem FirmSafe* arbeiten.

4. Klicken Sie auf **Öffnen**, um die vorhandene Firmware durch die ausgewählte Version zu ersetzen.

LANconfig beginnt nun mit dem Firmware-Upload. Sie können den Fortschritt über die Verlaufsspalte sowie Log-Informationsbereich verfolgen. Nach erfolgreichem Upload startet LANconfig das Gerät automatisch neu.

2.7.2 Firmware-Upload über WEBconfig

Innerhalb von WEBconfig laden Sie eine neue Firmware z. B. über das *Dateimanagement* hoch. Wählen Sie dafür eine geeignete Firmware-Datei aus und klicken Sie auf **Upload**. Überdies haben Sie genau wie unter LANconfig die Möglichkeit, die Firmware im Test-Modus hochzuladen (siehe *Firmware-Upload über LANconfig* auf Seite 90).

2.7.3 Firmware-Upload über Terminalprogramm

Dieser Abschnitt beschreibt, wie Sie mit Hilfe eines Terminalprogramms eine andere Firmware in das Gerät laden. Dabei stehen Ihnen prinzipiell zwei Möglichkeiten zur Auswahl:

- Upload über die serielle Konfigurationsschnittstelle
- Upload über TFTP oder SCP

Für den Upload über die serielle Verbindung benötigen Sie ein Programm, welches das XModem-Protokoll unterstützt, z. B. Windows HyperTerminal, Telix oder die freie Software Tera Term. Der Upload über TFTP oder SCP hingegen erfolgt über ein lokales oder externes Netzwerk.

Der nachfolgende Abschnitt beschreibt den Upload einer Firmware über die serielle Konfigurationsschnittstelle am Beispiel von HyperTerminal. Der Upload einer Firmware über TFTP oder SCP unterscheidet sich kaum vom allgemeinen

Datei-Upload. Mehr Informationen hierzu finden Sie unter *Dateien über TFTP, HTTP(S) oder SCP direkt in das/aus dem Gerät laden* auf Seite 95.

1. Schließen Sie das Gerät über das serielle Konfigurationskabel an einen Rechner an.
2. Starten Sie auf diesem Rechner ein serielles Terminal-Programm.
3. Bauen Sie eine Verbindung mit folgenden Einstellungen auf und melden Sie sich mit Ihren Login-Daten am Gerät an:
   - Geschwindigkeit in bps: `115200`
   - Datenbits: `8`
   - Stopbits: `1`
   - Parität: `keine`
   - Flusssteuerung: `RTS/CTS` bzw. `RFR/CTS`
4. Wechseln Sie in das **Firmware**-Menü und legen Sie über den Befehl `set Modus-FirmSafe <Value>` den gewünschten FirmSafe-Modus fest, wobei `<Value>` für einen der möglichen Modi steht. Stellen Sie ggf. zusätzlich mit `set Timeout-FirmSafe <Time>` eine Zeit in Sekunden für den Firmware-Test ein.

   Eine Erläuterung zu den möglichen Modi sowie daran anknüpfende Konfigurationsschritte finden Sie im FirmSafe-Abschnitt *Konfiguration* auf Seite 88.
5. Versetzen Sie das Gerät mit dem Aktions-Befehl `do Firmware-Upload` in Empfangsbereitschaft.
6. Starten Sie den Upload-Vorgang von Ihrem Terminalprogramm aus.
   - Bei Telix klicken Sie auf die Schaltfläche **Upload**, stellen **XModem** für die Übertragung ein und wählen die gewünschte Firmware-Datei zum Upload aus.
   - Bei HyperTerminal klicken Sie auf **Übertragung** > **Datei senden**, wählen die Firmware-Datei aus, stellen **XModem** als Protokoll ein und starten mit **OK**.
   - Bei Tera Term klicken Sie auf **File** > **Transfer** > **XMODEM** > **Send** und wählen die gewünschte Firmware-Datei zum Upload aus.

Der Firmware-Upload wird nun durchgeführt. Nach dem erfolgreichen Firmware-Upload startet das Gerät schließlich neu.

2.7.4 Firmware-Upload über Outband mit Rücksetzen der Konfiguration

Wenn beide Speicherplätze der Boot-Konfigurationen belegt (also kundenspezifische Standardeinstellungen **und** Rollout-Konfiguration gespeichert) sind, lässt sich das Gerät nicht mehr über den Reset-Taster auf die Werkseinstellungen zurücksetzen. Gleiches gilt, wenn die Funktion des Reset-Taster auf **Ignorieren** oder **Nur-Booten** beschränkt ist und das Konfigurationskennwort nicht mehr vorliegt. In diesem Fall können Sie einen Reset auf die Werkseinstellungen nur noch über den seriellen Zugang (Outband) durchführen.

Über die serielle Schnittstelle besteht die Möglichkeit, eine Firmware ins Gerät zu laden. Wenn Sie dabei statt des Konfigurations-Passwortes die Seriennummer des Gerätes verwenden, wird die Konfiguration wie bei einem Reset vollständig auf den Auslieferungszustand zurückgesetzt. Auf diese Weise können Sie sich stets Zugang zu einem Gerät verschaffen, wenn sich die Werkseinstellungen nicht auf einem anderen Weg wiederherstellen lassen.

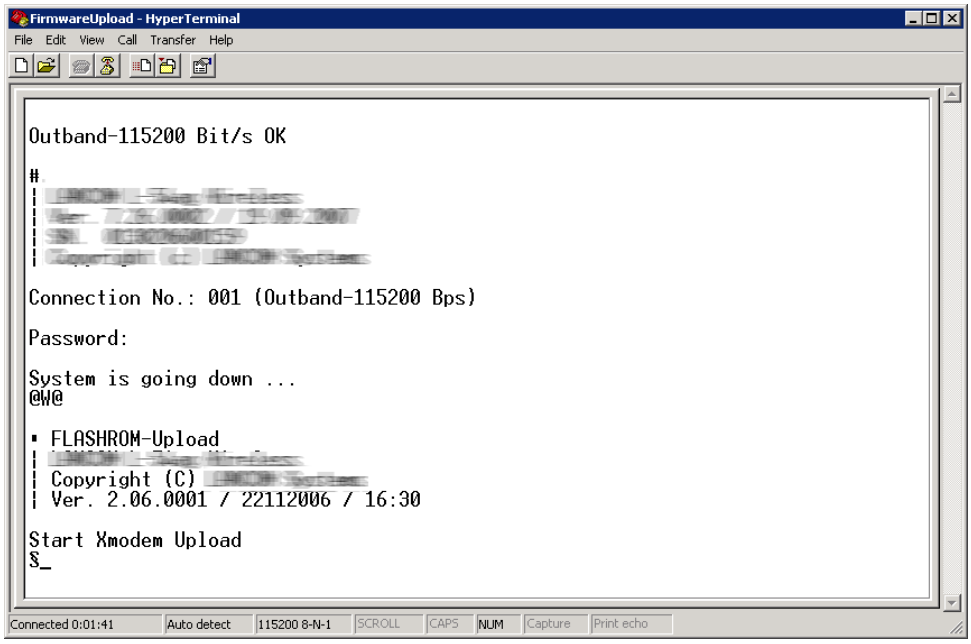


Bei diesem Vorgang werden neben der Konfiguration auch die gespeicherten *Boot-Konfigurationen* vollständig gelöscht! Gleiches gilt für im Gerät abgelegte Dateien, z. B. vorhandene Rollout-Zertifikate. Nutzen Sie diese Möglichkeit daher nur, wenn Sie keinen anderen Zugang zum Gerät herstellen können. Die Konfiguration und die Boot-Konfigurationen werden auch dann gelöscht, wenn der Firmware-Upload abgebrochen wird.

Das nachfolgende Anwendungsbeispiel beschreibt den Firmware-Upload über die serielle Schnittstelle mit Rücksetzen der Konfiguration exemplarisch mittels HyperTerminal.

1. Schließen Sie das Gerät über das serielle Konfigurationskabel an einen Rechner an.

2. Starten Sie auf diesem Rechner ein serielles Terminal-Programm, hier: Windows HyperTerminal.
3. Bauen Sie eine Verbindung mit folgenden Einstellungen auf:
   - Geschwindigkeit in bps: `115200`
   - Datenbits: `8`
   - Stopbits: `1`
   - Parität: `keine`
   - Flusssteuerung: `RTS/CTS` bzw. `RFR/CTS`
4. Drücken Sie im Begrüßungsbildschirm des Terminal-Programms die Eingabe-Taste, bis die Aufforderung zur Eingabe des Passwortes erscheint.
5. Geben Sie als Passwort die Seriennummer ein, die unter der Firmware-Version angezeigt wird und drücken Sie erneut die Eingabe-Taste. Das System fährt daraufhin herunter und erwartet den Firmware-Upload.



6. Bei HyperTerminal klicken Sie auf **Übertragung** > **Datei senden**, wählen die Firmware-Datei aus, stellen **XModem** als Protokoll ein und starten mit **OK**.

Der Firmware-Upload wird nun durchgeführt. Nach dem erfolgreichen Firmware-Upload startet das Gerät schließlich neu.

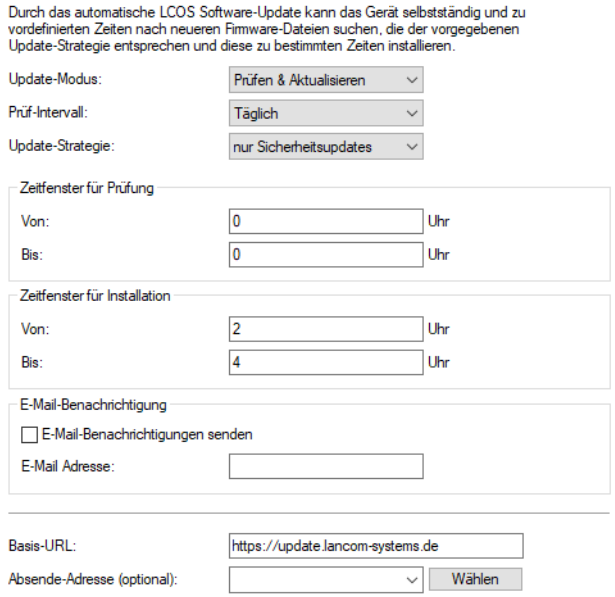
2.8 LANCOM Auto Updater

Der LANCOM Auto Updater ermöglicht die automatische Aktualisierung von im Feld befindlichen LANCOM Geräten ohne weiteren Benutzereingriff. LANCOM Geräte können auf Wunsch ohne Nutzerinteraktion nach neuen Software-Updates suchen, diese herunterladen und einspielen. Sie wählen, ob Sie Security Updates, Release Updates oder alle Updates automatisch installieren möchten. Sollen keine automatischen Updates durchgeführt werden, so kann das Feature auch zur Prüfung auf neue Updates verwendet werden.

Der LANCOM Auto Updater kontaktiert zur Update-Prüfung und zum Firmware-Download den LANCOM Update-Server. Die Kontaktaufnahme erfolgt via HTTPS. Bei der Kontaktaufnahme wird der Server mittels der im LANCOM Gerät bereits hinterlegten TLS-Zertifikate validiert. Zusätzlich sind Firmware-Dateien für aktuelle LANCOM Geräte signiert. Der LANCOM Auto Updater validiert vor dem Einspielen einer Firmware diese Signatur.

2.8.1 Konfiguration des Auto Updaters

Die Konfiguration des LANCOM Auto Updaters finden Sie in LANconfig unter **Management** > **Software-Update**.



Update-Modus

Stellen Sie hier den Betriebsmodus ein. Die folgenden Modi werden unterstützt:

Prüfen & Aktualisieren

- Der Auto Updater prüft regelmäßig beim Update-Server auf neue Updates.
- Der Update-Server ermittelt anhand der **Update-Strategie** das passende Update, bestimmt den Zeitpunkt für Download und Installation des Update innerhalb des vom Benutzer konfigurierten Zeitfensters und übermittelt dies an den Auto Updater.
- Die Installation der Firmware erfolgt im Testmodus. Nach der Installation führt der Auto Updater eine Verbindungsprüfung durch. Hierbei wird geprüft, ob weiterhin eine Verbindung zum Update-Server aufgebaut werden kann, der Internetzugang also weiterhin gewährleistet ist. Dies wird mehrere Minuten lang versucht, um eine eventuelle VDSL-Synchronisation oder einen WWAN-Verbindungsaufbau abzuwarten. Konnte der Update-Server erfolgreich kontaktiert werden, wird der Testmodus beendet, die Firmware ist nun regulär aktiv. Konnte der Updateserver nicht kontaktiert werden, muss davon ausgegangen werden, dass der Internetzugang nicht mehr möglich ist und es wird wieder die zweite (und damit die vorher aktive) Firmware gestartet.

nur Prüfen

- Der Auto Updater prüft regelmäßig beim Update-Server auf neue Updates.
- Die Verfügbarkeit eines neuen Updates wird dem Benutzer im LCOS-Menübaum und via Syslog signalisiert.
- Der Benutzer hat die Gelegenheit, manuell – aber über den Auto Updater gesteuert – auf das neueste verfügbare Update zu aktualisieren.



Ein manuelles Update wird über den folgenden Befehl auf der Kommandozeile gestartet:

```
do /setup/Automatisches-Firmware-Update/Aktualisiere-Firmware-jetzt
```

Manuell

- Der Auto Updater prüft nur nach Aufforderung durch den Benutzer auf neue Updates.

› Der Benutzer hat die Gelegenheit, manuell – aber über den Auto Updater gesteuert – auf das neueste verfügbare Update zu aktualisieren.

Ein manuelles Update wird über den folgenden Befehl auf der Kommandozeile gestartet:

```
do /setup/Automatisches-Firmware-Update/Aktualisiere-Firmware-jetzt
```

Prüf-Intervall

Stellen Sie ein, ob die Überprüfung auf ein verfügbares Update täglich oder wöchentlich stattfinden soll.

Der Auto Updater bestimmmt beim ersten Start einen zufälligen Zeitraum innerhalb eines Tages oder einer Woche, an dem die Prüfung durchgeführt wird. Das eigentliche Update soll dann im nächsten Zeitraum zwischen 2-4 Uhr (Voreinstellung) durchgeführt werden.

Update-Strategie

neueste Version

Releaseübergreifend immer die neueste Version. Beispiel: 10.20 Rel ist installiert; es wird auf 10.20 RU1 aktualisiert, aber auch auf 10.30 Rel. Es wird also immer auf die neueste Version aktualisiert, aber nicht wieder auf ein vorheriges Release zurückgewechselt.

aktuelle Version

Innerhalb eines Releases die neueste RU/SU/PR. Beispiel: 10.20 Rel ist installiert; es wird auf 10.20 RU1 aktualisiert, aber nicht auf 10.30 Rel.

nur Sicherheitsupdates

Innerhalb eines Releases das neueste SU. Beispiel: 10.20 Rel ist installiert; es wird auf 10.20 SU1 aktualisiert, aber nicht auf 10.20 RU2.

neueste Version ohne Rel.

Releaseübergreifend das neueste RU/SU/PR. Es wird erst bei Verfügbarkeit eines RU aktualisiert. Beispiel: Eine beliebige 10.20 ist installiert; es wird auf 10.30 RU1 aktualisiert, aber nicht auf 10.30 Rel.

Zeitfenster für Prüfung

Stellen Sie hier das Zeitfenster für die Prüfung und den Download neuer Aktualisierungen ein. Die tägliche Start- und Endzeit für dieses Zeitfenster kann stundengenau eingestellt werden. Die Standardeinstellung für beide Werte ist 0, es kann also rund um die Uhr auf Updates geprüft und ein Download gestartet werden. Innerhalb des konfigurierten Zeitfensters wird vom Auto Updater ein zufälliger Zeitpunkt für die Update-Prüfung und den Download geplant.

Zeitfenster für Installation

Stellen Sie hier das Zeitfenster für die Update-Installation ein. Die tägliche Start- und Endzeit für dieses Zeitfenster kann stundengenau eingestellt werden. Die Standardeinstellung definiert ein Zeitfenster zwischen 2:00 Uhr und 4:00 Uhr. Wenn ein Update gefunden wurde, dann wird dieses also in diesem Zeitraum installiert und das Gerät neu gestartet, um das Update zu aktivieren. Innerhalb des konfigurierten Zeitfensters wird vom Auto Updater ein zufälliger Zeitpunkt für die Installation geplant.

E-Mail-Benachrichtigungen senden

Stellen Sie hier ein, ob der LANCOM Auto Updater E-Mail-Benachrichtigungen an die angegebene E-Mail-Adresse versendet. Mittels der E-Mail-Benachrichtigungen kann sich der Administrator zu Ereignissen rund um das automatische Firmware-Update mit dem Auto-Updater informieren lassen. Eine E-Mail wird zu folgenden Ereignissen gesendet:

› ein Update wurde gefunden (bei Update-Modus "nur Prüfen")

- ein Update wurde gefunden und ein Zeitpunkt zur automatischen Installation wurde geplant (bei Update-Modus „Prüfen & Aktualisieren")
- ein Update wurde erfolgreich installiert (inklusive erfolgreicher Erreichbarkeitsprüfung)
- ein Update konnte nicht erfolgreich installiert werden und es wurde ein Rückfall auf die zuvor installierte Firmware durchgeführt
- Fehlermeldungen des Auto-Updaters (z. B. Update-Server konnte nicht erreicht werden)

Eine Benachrichtigung erfolgt nur bei automatisch ausgeführten Aktionen. Werden Aktionen von Hand gestartet, z. B. eine Update-Prüfung via LANmonitor oder WEBconfig, dann erfolgt keine E-Mail-Benachrichtigung.

E-Mail-Adresse

Stellen Sie hier die E-Mail-Adresse ein, die verwendet werden soll, wenn die E-Mail-Benachrichtigungen aktiviert werden.

Basis-URL

Gibt die URL des Servers an, der die aktuellen Firmware-Versionen zur Verfügung stellt.

Absende-Adresse

Über die Angabe einer Loopback-Adresse kann das Routing Tag automatisch bestimmt werden.

2.9 Dateien über TFTP, HTTP(S) oder SCP direkt in das/aus dem Gerät laden

Verschiedene Anwendungen – wie z. B. das Laden von Konfigurationen, Firmware-Versionen sowie Skripten oder die Prüfung einer Server-Identität mit Zertifikaten – erfordern das Speichern der betreffenden Dateien im Gerät. Sie können diese Dateien mit LANconfig oder WEBconfig in das Gerät einspielen.

Alternativ haben Sie aber auch die Möglichkeit, über die Konsole mittels TFTP, HTTP(S) oder SCP die entsprechenden Dateien direkt in das Gerät zu laden. Dieses Vorgehen erleichtert vor allem in größeren Installationen mit regelmäßigen Update-Intervallen von Firmware und / oder Konfiguration die Administration der Geräte. Dabei können Sie wählen, ob Sie eine Datei von einer Maschine aus durch einen Client zum Gerät übertragen, oder das Gerät selbst auf der Konsole die Datei von einem Server laden lassen.

2.9.1 Datei laden über einen TFTP-Client

TFTP (Trivial File Transfer Protocol) ist ein sehr einfaches Dateiübertragungsprotokoll zum Lesen oder Schreiben von Dateien. Es ermöglicht den einfachen Dateitransfer auf andere Geräte über das Netzwerk. Weitere Funktionen wie die des wesentlich mächtigeren FTPs (z. B. Rechtevergabe mittels chmod, Anzeige vorhandener Dateien, Benutzerauthentifizierung) sind allerdings nicht implementiert.

In LANconfig haben Sie die Möglichkeit, die Geräte-Kommunikation über TFTP abzuwickeln. Die Bedienung unterscheidet sich dabei aber nicht von der mit anderen Kommunikationsprotokollen. Daher richtet sich dieses Kapitel an alternative TFTP-Programme, welche Sie für die Geräte-Kommunikation nutzen können.

Unter vielen Windows-und Linux-Betriebssystemen z. B. ist standardmäßig ein kommandozeilenbasierter TFTP-Client enthalten. In Windows-Versionen 7 und neuer muss der TFTP-Client allerdings erst aktiviert werden. Alternativ können Sie auch einen anderen Client verwenden, wie z. B. die freie TFTP-Client-Server-Anwendung Tftpd32. Als Port geben Sie dann den Standardport `69` an. Die Blockgröße für Datenpakete entnehmen Sie dem Parameter **Bytes-pro-Hashmark** im Setup-Menü des Gerätes (normalerweise `8192`).

2.9.1.1 Syntax

Die Syntax des TFTP-Aufrufs ist abhängig vom verwendeten Betriebssystem bzw. Programm. Für den Windows-eigenen TFTP-Client lautet die Syntax beispielsweise:

```
tftp [-i] <Host> get|put <LocalFile|Command> <RemoteFile|Command>
```

Bei zahlreichen TFTP-Clients ist das ASCII-Format voreingestellt. Für die Übertragung binärer Daten (z. B. einer Firmware-Datei) muss daher meist die binäre Übertragung explizit gewählt werden. Unter Windows erreichen Sie dies durch den Parameter `-i`.

Sofern das Gerät mit einem Passwort geschützt ist, müssen Sie zudem Benutzername und Passwort in den TFTP-Befehl miteinbauen. Im TFTP wird der Benutzername und das Passwort im Quell- (TFTP-Read-Request) oder Ziel-Filename (TFTP-Write-Request) kodiert. Der Filename setzt sich dann entweder aus dem Root-Passwort und dem auszuführenden Kommando (für Supervisoren), oder aus der Kombination von Benutzername, Passwort und dem nachgestelltem Kommando (für lokale Administratoren) zusammen. Ein über TFTP abgesetzter Befehl sieht daher wie folgt aus:

- `<Root-Password> <Command>`
- `<Username>:<Password>@<Command>`

Als Kommandos ('<Command>') sind folgende Eingaben möglich:

- `readmib`: Kommando für das Einspielen einer Geräte-MIB-Datei (SNMP Management Information Base).
- `readconfig`: Kommando für das Auslesen einer Konfigurationsdatei.
- `writeconfig`: Kommando für das Einspielen einer Konfigurationsdatei.
- `writeflash`: Kommando für das Einspielen einer Firmware-Datei.



Die Rechte zur Nutzung von TFTP lassen sich für verschiedene Administrator-Typen einschränken, siehe *Rechteverwaltung für verschiedene Administratoren* auf Seite 109.

2.9.1.2 Anwendungsbeispiele

- Um z. B. eine Firmware in das Gerät zu laden, verwenden Sie das Kommando `writeflash`, wobei `10.0.0.1` für die IP-Adresse des Gerätes und `LC-L451-8.82.0083.upx` für die hochzuladende Datei stehen:

  ```
  tftp -i 10.0.0.1 put LC-L451-8.82.0083.upx writeflash
  tftp -i 10.0.0.1 put LC-L451-8.82.0083.upx MyAdmin:MyPasswd@writeflash
  ```

- Um z. B. die Geräte-MIB auszulesen, verwenden Sie das Kommando `readmib`:

  ```
  tftp 10.0.0.1 get readmib device.mib
  ```

- Um z. B. die Konfiguration unter Verwendung von Zugangsdaten aus dem Gerät auszulesen, verwenden Sie das Kommando `readconfig`:

  ```
  tftp 10.0.0.1 get root:MyPasswd@readconfig device.lcf
  ```

- Um z. B. die Konfiguration unter Verwendung von Zugangsdaten in das Gerät zu schreiben, verwenden Sie das Kommando `writeconfig`:

  ```
  tftp 10.0.0.1 put device.lcf root:MyPasswd@writeconfig
  ```



Die im Rahmen von *FirmSafe getätigten Einstellungen* gelten auch für Firmware-Uploads via TFTP.

2.9.1.3 Fehlersuche

Sollten Sie keine Verbindung zum Gerät herstellen können, kann es sein, dass die Firewall Ihres Betriebssystems TFTP-Verbindungen blockiert. Sofern Sie die Firewall-Einstellungen des Gerätes verändert haben, prüfen Sie auch hier, ob diese Verbindungen über TFTP erlaubt. Stellen Sie außerdem sicher, dass Sie im Gerät den Zugriff über das TFTP-Protokoll

aus dem für den Upload verwendeten Netzwerk-Typ freigegeben haben (in LANconfig einstellbar unter **Management** > **Admin** > **Zugriffs-Rechte**).

2.9.2 Datei laden über einen SCP-Client

SCP (Secure Copy Protocol) ist ein Protokoll zur sicheren Übertragung von Daten zwischen zwei Rechnern in einem Netzwerk. Administratoren nutzen SCP häufig beim Datenaustausch zwischen Servern bzw. zwischen Server und Arbeitplatzrechner. Mit einem geeigneten Tool (unter Windows z. B. mit dem PuTTY-Zusatzprogramm PSCP oder unter Linux z. B. mit Konqueror oder Midnight Commander) lassen sich auch Daten zwischen einer Maschine und dem Gerät über das SCP-Protokoll austauschen.

2.9.2.1 Syntax

Die Syntax des SCP-Aufrufs ist abhängig vom verwendeten Programm. Für PSCP lautet die Syntax an der Windows-Kommandozeile:

- **Senden von Dateien**

```
pscp.exe -scp [-pw <Password>] <LocalFile> <User>@<IP-Address>:target
```

- **Empfangen von Dateien**

```
pscp.exe -scp [-pw <Password>] <User>@<IP-Address>:target <LocalFile>
```

Das Ziel (`target`) auf dem entfernten Gerät leiten Sie durch einen Doppelpunkt hinter der IP-Adresse ein. Als Ziel geben Sie entweder einen Dateinamen (siehe *Dateinamen für die SCP-Dateiübertragung* auf Seite 97) im internen Dateisystem des Gerätes an oder `config`, `firmware` bzw. `firmwarewithreset`. Die Ziele `firmware` und `firmwarewithreset` sind ausschließlich für das Einspielen von Firmware-Updates reserviert, wobei bei letzterem im Anschluss ein Konfigurationsneustart durchgeführt wird; `config` benutzen Sie für das Ein- und Ausspielen von Konfigurationsdateien.

2.9.2.2 Dateinamen für die SCP-Dateiübertragung

Neben den bereits aufgeführten `config`, `firmware` bzw. `firmwarewithreset` zeigt die folgende Tabelle, welche Dateien Sie konkret über über SCP aus dem Gerät auslesen und / oder in das Gerät schreiben können. Diese entsprechen den Dateien, die auch über den WEBconfig-Datei-Upload bzw. -Download verfügbar sind. Beim Upload kann ggf. über die Umgebungsvariable `LCS_PASSWORD` ein Passwort übergeben werden.

Tabelle 12: Übersicht der Dateinamen für die SCP-Dateiübertragung

Dateiname	Lesen	Schreiben	Beschreibung
ssl_cert	Ja	Ja	SSL – Zertifikat (*.pem, *.crt. *.cer [BASE64])
ssl_privkey	Nein	Ja	SSL – Privater-Schlüssel (*.key [BASE64 unverschlüsselt])
ssl_rootcert	Ja	Ja	SSL – Root-CA-Zertifikat (*.pem, *.crt. *.cer [BASE64])
ssl_pkcs12	Nein	Ja	SSL – Container als PKCS#12-Datei (*.pfx, *.p12)
ssh_rsakey	Nein	Ja	SSH – RSA-Schlüssel (*.key [BASE64 unverschlüsselt])
ssh_dsakey	Nein	Ja	SSH – DSA-Schlüssel (*.key [BASE64 unverschlüsselt])
ssh_authkeys	Ja	Ja	SSH – akzeptierte öffentliche Schlüssel
ssh_ed25519key	Nein	Ja	SSH – ED25519-Schlüssel (*.key [BASE64 unverschlüsselt])
ssh_ed448key	Nein	Ja	SSH – ED448-Schlüssel (*.key [BASE64 unverschlüsselt])
vpn_rootcert	Ja	Ja	VPN – Root-CA-Zertifikat (*.pem, *.crt. *.cer [BASE64])
vpn_devcert	Ja	Ja	VPN – Geräte-Zertifikat (*.pem, *.crt. *.cer [BASE64])

Dateiname	Lesen	Schreiben	Beschreibung
vpn_devprivkey	Nein	Ja	VPN – Privater-Geräte-Schlüssel (*.key [BASE64 unverschlüsselt])
vpn_pkcs12	Nein	Ja	VPN - Container (VPN1) als PKCS#12-Datei (*.pfx, *.p12)
vpn_pkcs12_2	Nein	Ja	VPN – Container (VPN2) als PKCS#12-Datei (*.pfx, *.p12)
vpn_pkcs12_3	Nein	Ja	VPN – Container (VPN3) als PKCS#12-Datei (*.pfx, *.p12)
vpn_pkcs12_4	Nein	Ja	VPN – Container (VPN4) als PKCS#12-Datei (*.pfx, *.p12)
vpn_pkcs12_5	Nein	Ja	VPN – Container (VPN5) als PKCS#12-Datei (*.pfx, *.p12)
vpn_pkcs12_6	Nein	Ja	VPN – Container (VPN6) als PKCS#12-Datei (*.pfx, *.p12)
vpn_pkcs12_7	Nein	Ja	VPN – Container (VPN7) als PKCS#12-Datei (*.pfx, *.p12)
vpn_pkcs12_8	Nein	Ja	VPN – Container (VPN8) als PKCS#12-Datei (*.pfx, *.p12)
vpn_pkcs12_9	Nein	Ja	VPN – Container (VPN9) als PKCS#12-Datei (*.pfx, *.p12)
vpn_add_cas	Nein	Ja	VPN – zusätzliche CA-Zertifikate hinzufügen (*.pfx, *.p12, *.pem, *.crt. *.cer [BASE64])
eaptls_rootcert	Ja	Ja	EAP/TLS – Root-CA-Zertifikat (*.pem, *.crt. *.cer [BASE64])
eaptls_devcert	Ja	Ja	EAP/TLS – Geräte-Zertifikat (*.pem, *.crt. *.cer [BASE64])
eaptls_privkey	Nein	Ja	EAP/TLS – Privater-Geräte-Schlüssel (*.key [BASE64 unverschlüsselt])
eaptls_pkcs12	Nein	Ja	EAP/TLS – Container als PKCS#12-Datei (*.pfx, *.p12)
radsec_rootcert	Ja	Ja	RADSEC – Root-CA-Zertifikat (*.pem, *.crt. *.cer [BASE64])
radsec_devcert	Ja	Ja	RADSEC – Geräte-Zertifikat (*.pem, *.crt. *.cer [BASE64])
radsec_privkey	Nein	Ja	RADSEC – Privater-Geräte-Schlüssel (*.key [BASE64 unverschlüsselt])
radsec_pkcs12	Nein	Ja	RADSEC – Container als PKCS#12-Datei (*.pfx, *.p12)
radiuss_accnt_total	Ja	Ja	RADIUS-Server – Summarisches Accounting (*.csv)
scep_cert_list	Ja	Ja	SCEP-CA – Zertifikats-Liste
scep_cert_serial	Ja	Ja	SCEP-CA – Seriennummer
scep_ca_backup	Ja	Nein	Backup für SCEP-CA – PKCS12 Container
scep_ra_backup	Ja	Nein	Backup für SCEP-RA – PKCS12 Container
scep_ca_pkcs12	Nein	Ja	SCEP-CA – PKCS12 Container
scep_ra_pkcs12	Nein	Ja	SCEP-RA – PKCS12 Container
pbspot_template_welcome	Ja	Ja	Public Spot – Willkommensseite (*.html, *.htm)
pbspot_template_login	Ja	Ja	Public Spot – Login-Seite (*.html, *.htm)
pbspot_template_error	Ja	Ja	Public Spot – Fehlerseite (*.html, *.htm)
pbspot_template_start	Ja	Ja	Public Spot – Startseite (*.html, *.htm)
pbspot_template_status	Ja	Ja	Public Spot – Statusseite (*.html, *.htm)
pbspot_template_logoff	Ja	Ja	Public Spot – Logoff-Seite (*.html, *.htm)
pbspot_template_help	Ja	Ja	Public Spot – Hilfeseite (*.html, *.htm)
pbspot_template_noproxy	Ja	Ja	Public Spot – Kein-Proxy-Seite (*.html, *.htm)
pbspot_template_voucher	Ja	Ja	Public Spot – Voucher-Seite (*.html, *.htm)
pbspot_template_agb	Ja	Ja	Public Spot – AGB-Seite (*.html, *.htm)

Dateiname	Lesen	Schreiben	Beschreibung
pbspot_formhdrimg	Ja	Ja	Public Spot – Kopfbild Seiten (*.gif, *.png, *.jpeg)
WLC_Script_1.lcs	Ja	Ja	CAPWAP – WLC_Script_1.lcs
WLC_Script_2.lcs	Ja	Ja	CAPWAP – WLC_Script_2.lcs
WLC_Script_3.lcs	Ja	Ja	CAPWAP – WLC_Script_3.lcs
default_pkcs12	Nein	Ja	
rollout_wizard	Nein	Ja	
rollout_template	Nein	Ja	
rollout_logo	Nein	Ja	
hip_cert_0	Nein	Ja	
issue	Ja	Ja	Text zum Anzeigen beim Login auf der Konsole (z. B. ASCII Logos)
config	Ja	Ja	Ein- und Ausspielen von Konfigurationsdateien
firmware	Nein	Ja	Einspielen eines Firmwarefiles in den passiven Firmwareslot
firmwarewithreset	Nein	Ja	Wie firmware, nur mit einem anschließenden Konfigurationsneustarts

2.9.2.3 Anwendungsbeispiele

› Um z. B. eine Datei von Ihrem Rechner auf das Gerät zu übertragen, nutzen Sie einen Befehl wie den folgenden:

```
C:\>pscp.exe -scp -pw MyPwd c:\path\myfile.ext root@10.0.0.1:target
```

Um z. B. eine Datei vom Gerät auf Ihren Rechner zu übertragen, wechseln Sie die Reihenfolge von Quelle und Ziel:

```
C:\>pscp.exe -scp -pw MyPwd root@10.0.0.1:target c:\path\myfile.ext
```

Als `target` setzen Sie dabei die Bezeichnung eines Dateinamens mit Pfad ein.

› Um z. B. die Konfiguration aus dem Gerät auf Ihrem Rechner unter dem Namen `config.lcf` zu speichern, nutzen Sie einen Befehl wie den folgenden:

```
C:\>pscp.exe -scp -pw MyPwd root@10.0.0.1:config c:\config.lcf
```

› Um z. B. eine neue Firmware von Ihrem Rechner in das Gerät zu laden, nutzen Sie einen Befehl wie den folgenden:

```
C:\>pscp.exe -scp -pw MyPwd  c:\firmware.upx root@10.0.0.1:firmware
```

2.9.3 Datei-Download von einem TFTP- oder HTTP(S)-Server

Neben den Möglichkeiten, eine Firmware, eine Konfigurationsdatei oder ein Konfigurationsskript von einer Maschine aus an das Gerät zu übertragen, kann der Datei-Upload bzw. -Download auch durch das Gerät selbst von einem HTTP(S)- oder TFTP-Server im lokalen Netzwerk oder dem Internet erfolgen. Dazu werden die betreffenden Dateien auf einem HTTP(S)- bzw. TFTP-Server abgelegt und nach Anmeldung am Gerät mit den weiter unten gelisteten LCOS-Befehlen aufgerufen.

Ein TFTP-Server gleicht in der Funktionsweise einem FTP-Server, verwendet allerdings zur Datenübertragung ein anderes Protokoll. Bei der Verwendung eines HTTPS-Servers können Sie im Gerät ein Zertifikat hinterlegen, mit dem sich später die Identität des Servers verifizieren lässt. In der Praxis ist es zumeist sehr viel leichter, einen HTTP(S)-Server zentral mit eindeutiger Adresse (URI) im Internet bereit zu stellen als einen TFTP-Server – ggf. lässt sich z. B. ein bestehender Webserver um diese Funktionalität erweitern.

Von einem solchen Server lassen sich die unterschiedlichen Dateitypen dann mit folgenden Befehlen abrufen:

› `LoadConfig`: Lädt eine Konfigurationsdatei (mit der Dateierweiterung *.lcf) in das Gerät.

- `LoadFirmware`: Lädt eine Firmware-Datei (mit der Dateierweiterung *.upx) in das Gerät.
- `LoadScript`: Lädt eine Skript-Datei (mit der Dateierweiterung *.lcs) – z. B. mit Teilkonfigurationen – in das Gerät.
- `LoadFile`: Lädt Dateien verschiedenen Typs in das Gerät.

Der Befehl `LoadFile` unterstützt ausschließlich die Protokolle HTTP und HTTPS.

2.9.3.1 Syntax

Die genaue Syntax der Load-Befehle ist abhängig vom verwendeten Protokoll (HTTP[S] oder TFTP). Allgemein betrachtet setzt sich ein Aufruf aber immer aus dem entsprechenden Befehl, eventuellen Parametern und der URL zusammen, welche die zu ladende Datei referenziert. Diese URL können Sie auch im Setup-Menü unter **Automatisches-Laden** > **Netzwerk** > **…** > **URL** hinterlegen, sodass sich eine Firmware, Konfiguration oder Skriptdatei auch allein durch Eingabe des Kommandos ins Gerät laden lässt.

Verbindungen zu einem HTTP(S)-Server

Bei Nutzung von HTTP(S) kann der Befehl in der üblichen URL-Schreibweise angegeben werden. Als Protokoll tragen Sie entweder `http` oder `https` ein:

```
<Command> <Parameter> <Protocol>://<Host>/<Directory>/<File>
```

Sofern Sie dabei auf einen passwortgeschützten Bereich zugreifen wollen, authentisieren Sie sich mit der üblichen Benutzername/Passwort-Schreibweise:

```
<Command> <Parameter> <Protocol>://<Username>:<Password>@<Host>/<Directory>/<File>
```

Verbindungen zu einem TFTP-Server

Bei Nutzung von TFTP steht Ihnen ebenfalls die URL-Schreibweise zur Verfügung. Als Protokoll tragen Sie in diesem Fall `tftp` ein:

```
<Command> <Parameter> <Protocol>://<Host>/<Directory>/<File>
```

Alternativ können Sie stattdessen auch die URL durch die entsprechenden Parameter ersetzen:

```
<Command> <Parameter> -s <Host> -f <Directory>/<File>
```

2.9.3.2 Parameter

Die Befehle zur Verbindung mit einem HTTP(S)- oder TFTP-Server können durch Angabe zusätzlicher Parameter modifiziert werden. Dabei sind nicht alle Parameter für alle Protokolle verfügbar. Sofern über das Setup-Menü bestimmte Default-Werte konfigurierbar sind, verwendet das Gerät diese Werte, solange Sie die Werte nicht durch die dazugehörigen Parameter explizit überschreiben. Dies gilt z. B. für die Parameter der Versionsprüfung.

Parameter für die Verbindung

Über folgende Parameter können Sie die Art und Weise verändern, wie sich das Gerät mit dem Server verbindet.

-a <Address>

Verfügbar für Protokoll: HTTP, HTTPS, TFTP

Verfügbar für Befehl: alle

Über diesen Parameter benennen Sie eine optionale Loopback-Adresse. Durch Angabe einer optionalen Loopback-Adresse verändern Sie die Quelladresse bzw. Route, mit der das Gerät den Server anspricht. Dies kann z. B. dann sinnvoll sein, wenn der Server über verschiedene Wege erreichbar ist und dieser einen bestimmten Weg für seine Antwort-Nachrichten wählen soll. Mögliche Werte sind:

- Name des IP-Netzwerks, dessen Adresse eingesetzt werden soll
- `INT` für die Adresse des ersten Intranets

- `DMZ` für die Adresse der ersten DMZ
- `LB0` bis `LBF` für die 16 Loopback-Adressen
- Beliebige, gültige IP-Adresse

Standardmäßig schickt der Server seine Antworten zurück an die IP-Adresse Ihres Gerätes, ohne dass Sie diese hier angeben müssen.

-f <Directory>/<File>

Verfügbar für Protokoll: TFTP

Verfügbar für Befehl: alle

Über diesen Parameter geben Sie den Pfad und den Namen der Datei auf dem Server an. Der Parameter ersetzt zusammen mit `-s` die Angabe einer URL.

-s <Host>

Verfügbar für Protokoll: TFTP

Verfügbar für Befehl: alle

Über diesen Parameter geben Sie den DNS-Namen oder die IP-Adresse des Servers an. Der Parameter ersetzt zusammen mit `-f` die Angabe einer URL.

Parameter für die Versionsprüfung

In der Default-Einstellung sind die Bedingungen für Firmware, Konfiguration und Skript im Setup-Menü (unter **Automatisches-Laden** > **Netzwerk** > **…**) auf **unbedingt** eingestellt. Dadurch laden oder starten die Befehle LoadFirmware, LoadConfig oder LoadScript die entsprechende Firmware, Konfiguration oder Skriptdatei **ohne** dass eine Versionsprüfung stattfindet. Durch Angabe des entsprechenden Parameters können Sie diese Einstellung jedoch für eine zu ladende Datei individuell übergehen.

-Cd

Verfügbar für Protokoll: HTTP, HTTPS, TFTP

Verfügbar für Befehl: LoadFirmware, LoadConfig, LoadScript

Dieser Parameter überprüft, ob die verwendete Datei **unterschiedlich** ist im Vergleich zur im Gerät vorhandenen Firmware oder Konfiguration bzw. neuer als das zuletzt ausgeführte Skript. Bei der Verwendung mit LoadScript aktualisiert dieser Parameter die im Gerät gespeicherte Prüfsumme des zuletzt ausgeführten Skriptes.

-Cn

Verfügbar für Protokoll: HTTP, HTTPS, TFTP

Verfügbar für Befehl: LoadFirmware

Dieser Parameter überprüft, ob die verwendete Datei **neuer** ist im Vergleich zur im Gerät vorhandenen Firmware.

-m

Verfügbar für Protokoll: HTTP, HTTPS, TFTP

Verfügbar für Befehl: LoadFirmware

Dieser Parameter gibt die Minimalversion für eine Firmware an. Die für den Befehl verwendete Firmware muss mindestens dieser Version entsprechen, damit der Befehl ausgeführt wird.

-u

Verfügbar für Protokoll: HTTP, HTTPS, TFTP

Verfügbar für Befehl: LoadFirmware, LoadConfig, LoadScript

Dieser Parameter deaktiviert die Versionsprüfung. Die mit dem Befehl verwendete Datei wird auf jeden Fall geladen oder ausgeführt. Bei der Verwendung mit LoadScript belässt dieser Parameter die im Gerät gespeicherte Prüfsumme des zuletzt ausgeführten Skriptes unverändert.



Der Parameter -u hat immer Vorrang vor anderen mit dem Befehl übergebenen Parametern.

Parameter für die Zertifikatsprüfung

Bei der Übertragung von Dateien von einem HTTPS-Server zu einem Client-Gerät prüfen die beteiligten Netzwerkkomponenten die Identität der Gegenstelle mit Hilfe von Zertifikaten. Beim automatischen Laden von HTTPS-Servern stehen Ihnen zusätzliche Parameter für den Download der Zertifikate und deren anschließende Prüfung zur Verfügung. Das betreffende Zertifikat laden Sie z. B. über das Datenmanagement von LANconfig oder WEBconfig als **SSL - Root-CA-Zertifikat (*.pem, *.crt *.cer [BASE64])** in das Gerät.

-c <MainDir>/<File>

Verfügbar für Protokoll: HTTPS

Verfügbar für Befehl: alle

Über diesen Parameter geben Sie den Namen des Zertifikats an, mit dem das Gerät die Identität des Servers prüft, bevor es die angeforderte Datei lädt.

-d <Passphrase>

Verfügbar für Protokoll: HTTPS

Verfügbar für Befehl: LoadFile

Mit dieser Passphrase verschlüsselt das Gerät einen unverschlüsselten PKCS#12-Container.

-p <MainDir>/<File>

Verfügbar für Protokoll: HTTPS

Verfügbar für Befehl: LoadFile

Über diesen Parameter geben Sie beim Download einer Datei den Namen des PKCS#12-Containers an. Der PKCS#12-Container kann mehrere CA-Zertifikate enthalten und unterstützt so die Identitätsprüfung von HTTPS-Servern mit Zertifikatsketten. Außerdem kann ein PKCS#12-Container ein Gerätezertifikat und den zugehörigen privaten Schlüssel enthalten und so die Identität des Geräts gegenüber dem HTTPS-Server bestätigen, wenn der HTTPS-Server die Authentifizierung mit einem Zertifikat erfordert.

-n

Verfügbar für Protokoll: HTTPS

Verfügbar für Befehl: LoadFile

Über diesen Parameter deaktivieren Sie die Prüfung des Server-Namens beim Laden einer Datei. Wenn Sie den Server in der betreffenden URL als DNS-Name angeben (und nicht als IP-Adresse), dann überprüft das Gerät das Zertifikat auf den zugehörigen Server-Namen. Wenn es sich bei dem HTTPS-Server um einen virtuellen Server handelt, kann dieser Server mit den passenden Zertifikaten für den übermittelten DNS-Namen antworten. Ohne Angabe dieses Parameters prüft das Gerät, ob der DNS-Name in der betreffenden URL mit dem 'common name' der übermittelten Zertifikate übereinstimmt. Das Gerät lädt die Datei nur dann, wenn diese Prüfung erfolgreich verläuft.

-o <MainDir>/<File>

Verfügbar für Protokoll: HTTPS

Verfügbar für Befehl: LoadFile

Über diesen Parameter geben Sie das Ziel für den Download einer Datei an. Verwenden Sie diese Option, um z. B. ein Zertifikat für die spätere Identitätsprüfung bei Zugriff auf einen HTTPS-Server in Ihrem Gerät zu speichern.

Verwenden Sie dabei als `<MainDir>` eines der beiden folgenden Hauptverzeichnisse:

- Sofern das Ziel eine Datei im internen Dateisystem des Geräts darstellt, verwenden Sie das Hauptverzeichnis `/minifs/`. In Kombination mit einem Parameter lautet eine mögliche Eingabe z. B. `-c /minifs/sslroot.crt`. Die möglichen Dateinamen finden Sie im Status-Menü unter **Dateisystem** > **Inhalt**.

  Alternativ finden Sie eine allgemeine Übersicht auch im Abschnittt *Dateinamen für die SCP-Dateiübertragung* auf Seite 97.
- Sofern das Ziel eine Datei auf einem externen USB-Datenträger darstellt, verwenden Sie das Hauptverzeichnis `/mountpoint/`. In Kombination mit einem Parameter lautet eine mögliche Eingabe z. B. `-o /mountpoint/Device-9.00.0244.upx`.

Sofern der angegebene Speicherpfad Unterverzeichnisse enthält, müssen diese bereits existieren. Das Gerät legt keine neuen Verzeichnisse an.

Darüber hinaus können Sie in nicht bereits vom Gerät vorgegebenen Dateinamen und -pfaden Variablen verwenden, um z. B. dynamische Verzeichnisstrukturen zu realisieren (siehe *Variablen* auf Seite 103.

2.9.3.3 Variablen

Sie haben die Möglichkeit, in den Load-Befehlen dynamische Pfadangaben zu verwenden, wann immer Sie innerhalb eines Parameters oder einer URL auf eine Datei referenzieren. Die Inhalte der einzelnen Variablen werden dabei vom Gerät vorgegeben und lassen sich nicht manuell verändern.

Folgende Variablen sind in Ihren Verzeichnis- und Dateinamen erlaubt:

%m

MAC-Adresse des Gerätes in hexadezimaler Schreibweise, mit Kleinbuchstaben und ohne Trennzeichen

%s

Seriennummer des Gerätes

%n

Gerätename

%l

Standort des Gerätes, wie in der Konfiguration angegeben

%d

Gerätetyp

Neben diesen allgemeinen Variablen können Sie auch die folgenden *Umgebungsvariablen* der Geräte nutzen, um die Ausführung der Load-Befehle flexibler zu gestalten.

2.9.3.4 Anwendungsbeispiele

Mit dem folgenden Befehl laden Sie – nachdem Sie sich auf der Konsole am Gerät angemeldet haben – …

- eine Firmware-Datei mit dem Namen 'Device-8.80.0103.upx' aus dem Verzeichnis 'LCOS/880' vom TFTP-Server mit der IP-Adresse '192.168.2.200' in das Gerät:

```
LoadFirmware -s 192.168.2.200 -f LCOS/880/Device-8.80.0103.upx
```

- ein zur MAC-Adresse passendes Script (mit z. B. dem Namen '00a0571735da.lcs') vom TFTP-Server mit der IP-Adresse '192.168.2.200' in das Gerät:

```
LoadScript -s 192.168.2.200 -f %m.lcs
```

- eine Firmware-Datei mit dem Namen 'Device-8.80.0103.upx' aus dem Verzeichnis 'download' vom HTTPS-Server mit der Adresse 'www.myserver.com' in das Gerät. Dabei wird die Identität des Servers mit dem Zertifikat 'sslroot.crt' geprüft, das im internen Dateisystem des Gerätes gespeichert ist:

```
LoadFirmware -c /minifs/sslroot.crt https://www.myserver.com/download/Device-8.80.0103.upx
```

- ein zur Seriennummer und zur aktuellen Firmware-Version passendes Script in das Gerät. Das Gerät entnimmt die Werte für Seriennummer und Firmware aus den entsprechenden Umgebungsvariablen:

```
LoadScript $__SERIALNO-$__FWVERSION.lcs
```

> Dieser Befehl funktioniert ohne Angabe einer URL, wenn diese unter **Setup** > **Autoload** > **Netzwerk** > **Skript** im Parameter **URL** angegeben ist. Fehlt dieser Eintrag, ist die Angabe einer URL im Befehl erforderlich:
>
> ```
> LoadScript -s 192.168.2.200 $__SERIALNO-$__FWVERSION.lcs
> ```

Firmware und / oder Konfiguration regelmäßig updaten

Dieses Szenario beschreibt, wie Sie an der Kommandozeile das Gerät so konfigurieren, dass zu einer festgelegten Uhrzeit ein regelmäßiges Update der Firmware und / oder der Konfiguration erfolgt. Der Download von Firmware und Konfiguration erfolgt dabei von einem externen Server (siehe *Datei-Download von einem TFTP- oder HTTP(S)-Server* auf Seite 99) über die Befehle 'LoadFirmware' und 'LoadConfig' unter Verwendung fixer Dateinamen. Die Zeitplanung realisieren Sie mittels Cron-Jobs.

1. Geben Sie die URL an, von dem der Befehl 'LoadFirmware' die Firmware lädt, wenn keine anderen Parameter vorliegen. Für das Laden der Firmware von einem HTTP-Server z. B. verwenden Sie einen Befehl ähnlich dem folgenden:

```
set /Setup/Automatisches-Laden/Netzwerk/Firmware/URL http://www.mycompany.de/firmware/LCOS.upx
```

2. Stellen Sie die Bedingung für das Laden der Firmware so ein, dass nur eine neuere als die im Gerät vorhandene Firmware geladen wird:

```
set /Setup/Automatisches-Laden/Netzwerk/Firmware/Bedingung wenn-neuer
```

3. Geben Sie den Pfad an, von dem der Befehl 'LoadConfig' eine Konfiguration lädt, wenn keine anderen Parameter vorliegen. Für das Laden der Konfiguration von einem HTTP-Server z. B. verwenden Sie einen Befehl ähnlich dem folgenden:

```
set /Setup/Automatisches-Laden/Netzwerk/Firmware/URL http://www.mycompany.de/configuration/LCOS.lcf
```

4. Stellen Sie die Bedingung für das Laden der Konfiguration so ein, dass nur eine andere als die im Gerät vorhandene Konfiguration geladen wird:

```
set /Setup/Automatisches-Laden/Netzwerk/Konfiguration/Bedingung wenn-unterschiedlich
```

5. Erstellen Sie einen Cron-Job, der regelmäßig um 23:55 Uhr das Kommando 'LoadFirmware' ausführt:

```
cd /Setup/Config/Cron-Tabelle
set 1 * * * 55 23 * * * LoadFirmware
```

6. Erstellen Sie einen Cron-Job, der regelmäßig um 23:59 Uhr das Kommando 'LoadConfig' ausführt:

```
set 2 * * * 59 23 * * * LoadConfig
```

Fertig! Damit haben Sie das automatische Update von Firmware und Konfiguration eingerichtet.

> Die Reihenfolge (erst Firmware, anschließend Konfiguration) stellt sicher, dass die Konfiguration auch Menüpunkte beinhalten kann, die erst in der neuen Firmware vorhanden sind.

Konfiguration erst im Anschluss an die Firmware updaten

Dieses Szenario beschreibt, wie Sie an der Kommandozeile das Gerät so konfigurieren, dass es in einem festgelegten Intervall Firmware und Konfiguration aktualisiert. Das Update der Firmware erfolgt dabei **vor** dem Update der Konfiguration. Der Download von Firmware und Konfiguration geschieht von einem externen Server (siehe *Datei-Download*

von einem TFTP- oder HTTP(S)-Server auf Seite 99) über die Befehle 'LoadFirmware' und 'LoadConfig' unter Verwendung dynamischer Dateinamen. Die Zeitplanung realisieren Sie mittels Cron-Jobs.

1. Geben Sie die URL an, von dem der Befehl 'LoadFirmware' die Firmware lädt, wenn keine anderen Parameter vorliegen. Für das Laden der Firmware von einem HTTP-Server z. B. verwenden Sie einen Befehl ähnlich dem folgenden:
   ```
   set /Setup/Automatisches-Laden/Netzwerk/Firmware/URL http://www.mycompany.de/firmware/
   ```
   Der Dateiname wird später durch den Cron-Job definiert.

2. Stellen Sie die Bedingung für das Laden der Firmware so ein, dass nur eine neuere als die im Gerät vorhandene Firmware geladen wird:
   ```
   set /Setup/Automatisches-Laden/Netzwerk/Firmware/Bedingung wenn-neuer
   ```

3. Geben Sie den Pfad an, von dem der Befehl 'LoadConfig' eine Konfiguration lädt, wenn keine anderen Parameter vorliegen. Für das Laden der Konfiguration von einem HTTP-Server z. B. verwenden Sie einen Befehl ähnlich dem folgenden:
   ```
   set /Setup/Automatisches-Laden/Netzwerk/Firmware/URL http://www.mycompany.de/configuration
   ```
   Der Dateiname wird später durch den Cron-Job definiert.

4. Stellen Sie die Bedingung für das Laden der Konfiguration so ein, dass nur eine andere als die im Gerät vorhandene Konfiguration geladen wird:
   ```
   set /Setup/Automatisches-Laden/Netzwerk/Konfiguration/Bedingung wenn-unterschiedlich
   ```

5. Erstellen Sie einen Cron-Job, der regelmäßig alle 10 Minuten das Kommando 'LoadFirmware' ausführt:
   ```
   cd /Setup/Config/Cron-Tabelle
   set 1 * * * 10 * * * * LoadFirmware\ $__SERIALNO-Device.upx
   ```
   Im obigen Beispiel muss die Firmware auf dem HTTP-Server also in der Form `<SerialNumber>-Device.upx` vorliegen, z. B. `000018100060-Device.upx`.

   Im cron-Befehl `LoadFirmware\ $__SERIALNO-Device.upx` ist das Leerzeichen zwischen dem Load-Kommando und der Umgebungsvariablen mit einem Backslash geschützt. Eine denkbare alternative Schreibweise, bei welcher der komplette Befehl mit Anführungszeichen eingeschlossen wird, führt zu einem Fehler. LCOS behandelt Umgebungsvariablen in Anführungszeichen wie normalen Text; die Umsetzung in den Inhalt der Variablen entfällt.

6. Erstellen Sie einen Cron-Job, der regelmäßig alle 10 Minuten das Kommando 'LoadConfig' ausführt:
   ```
   set 2 * * * 10 * * * * LoadScript\ $__SERIALNO-$__FWVERSION.lcs
   ```
   Im obigen Beispiel muss das Konfigurationsskript auf dem HTTP-Server also in der Form `<SerialNumber>-<FirmwareVersion>.lcs` vorliegen, z. B. `000018100060-8.84.lcf`.

Fertig! Bei dieser Konfiguration lädt das Gerät in jedem Fall zuerst die aktuelle Firmware.

Wenn das Gerät – nach dem Hochladen der aktuellen Firmware und des aktuellen Konfigurationsskriptes (z. B. für Version 8.84) auf den HTTP-Server – zuerst den Befehl 'LoadScript' ausführt, enthält die Umgebungsvariable '__FWVERSION' zu diesem Zeitpunkt den Wert der vorangegangenen Firmware (z. B. '8.80'). Der Befehl `LoadScript\ $__SERIALNO-$__FWVERSION.lcs` findet zu diesem Zeitpunkt also kein passendes Konfigurationsskript. Anschließend führt das Gerät den Befehl `LoadFirmware 000018100060-Device.upx` aus; nach dem Neustart enthält die Umgebungsvariable '__FWVERSION' den Wert '8.84'. Der Befehl `LoadScript\ $__SERIALNO-$__FWVERSION.lcs` findet dann ein passendes Skript zum Updaten der Konfiguration.

2.10 Automatisches Laden von Firmware oder Konfiguration über USB

Geräte mit USB-Anschluss können Sie mit Hilfe eines externen Datenträgers sehr komfortabel in Betrieb nehmen. Loader und Firmware-Dateien lassen sich ebenso wie vollständige Konfigurationen oder Skripte automatisch von einem USB-Medium in das Gerät laden.

2.10.1 Automatisches Laden von Loader- und / oder Firmware-Dateien

Wenn die Funktion aktiviert ist, sucht das Gerät beim Mounten eines USB-Mediums nach Loader- und / oder Firmware-Dateien im Verzeichnis 'Firmware'. In diesem Verzeichnis werden alle Dateien mit der Dateiendung '*.upx' für den automatischen Ladevorgang in Betracht gezogen, die zum aktuellen Gerätetyp passen. Dazu liest das Gerät den Header der Dateien aus und verwendet die Dateien anschließend nach folgenden Regeln:

- Wurde mindestens eine upx-Datei mit Loader gefunden, wird der Loader mit der höchsten Versionsnummer geladen, sofern im Gerät nicht schon ein Loader mit höherer Versionsnummer vorhanden ist.
- Wurde mindestens eine Firmware-Datei gefunden, wird die Firmware mit der höchsten Versionsnummer geladen, wenn die Version ungleich der im Gerät aktiven oder inaktiven Firmwareversionen ist.

Während des automatischen Ladevorgangs blinken die Power- und die Online-LED am Gerät abwechselnd. Wird zunächst ein Loader geladen, erfolgt nach dem Ladevorgang ein Neustart des Gerätes und anschließend evtl. ein zweiter automatischer Ladevorgang für eine Firmware. Auch bei dem zweiten Ladevorgang blinken die Power- und die Online-LED am Gerät abwechselnd.

An den automatischen Ladevorgang von Loader- und / oder Firmware-Dateien können sich evtl. noch weitere Ladevorgänge für Konfigurations- und / oder Skript-Dateien anschließen, siehe *Automatisches Laden von Konfigurations- und / oder Skript-Dateien* auf Seite 106.

Wenn der automatische Ladevorgang vollständig abgeschlossen ist, leuchten alle LEDs des Geräts für 30 Sekunden grün. Sie können das USB-Medium dann entfernen.

2.10.2 Automatisches Laden von Konfigurations- und / oder Skript-Dateien

Konfigurations- und / oder Skript-Dateien werden nur dann automatisch in das Gerät geladen, wenn sich das Gerät im Auslieferungszustand befindet. Durch einen Konfigurations-Reset kann ein Gerät jederzeit wieder auf den Auslieferungszustand zurückgesetzt werden.

Das Gerät sucht beim Mounten eines USB-Mediums nach Loader- und / oder Firmware-Dateien im Verzeichnis „Config“. In diesem Verzeichnis werden alle Dateien mit der Dateiendung „*.lcf“ (Konfigurationen) sowie „*.lcs“ (Skripte) für den automatischen Ladevorgang in Betracht gezogen, die zum aktuellen Gerätetyp passen. Dazu liest das Gerät den Header der Dateien aus und verwendet die Dateien anschließend nach folgenden Regeln:

- Eine Voll-Konfiguration wird immer vor einem Skript geladen. Es werden nur Voll-Konfigurationen geladen, deren Gerätetyp-Eintrag gleich dem Typ des ladenden Gerätes ist und deren Firmware-Versions-Eintrag im Header gleich der im ladenden Gerät aktiven Firmware ist. Liegen mehrere passende Voll-Konfigurationen vor, erfolgt die Auswahl nach den folgenden Kriterien in dieser Reihenfolge:
  - Der Konfigurationsheader enthält eine Geräte-Seriennummer und diese stimmt mit der Seriennummer des ladenden Gerätes überein.
  - Der Konfigurationsheader enthält eine MAC-Adresse und diese stimmt mit der MAC-Adresse des ladenden Gerätes überein.
  - Sollten danach mehrere Konfigurationsdateien ohne die zuvor genannten Kriterien verbleiben, verwendet das Gerät die Konfiguration mit dem aktuellsten Datum.
- Sollte keine Voll-Konfiguration vorliegen, wählt das Gerät eine eventuell vorhandene Skript-Datei. Liegen mehrere passende Skripte vor, erfolgt die Auswahl nach den folgenden Kriterien in dieser Reihenfolge:

- Der Skript-Header enthält eine Geräte-Seriennummer und diese stimmt mit der Seriennummer des ladenden Gerätes überein.
- Der Skript-Header enthält eine MAC-Adresse und diese stimmt mit der MAC-Adresse des ladenden Gerätes überein.
- Der Skript-Header enthält eine Firmware-Version und diese stimmt mit der Firmware-Version des ladenden Gerätes überein.

Sollten danach mehrere Skripte ohne die zuvor genannten Kriterien verbleiben, verwendet das Gerät das Skript mit der aktuellsten Versionsnummer bzw. dem Datum.

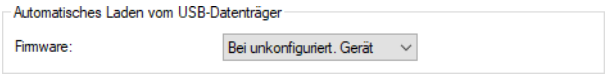
Die Meta-Daten zur verwendeten Firmwareversion und zum Erstellungsdatum werden automatisch beim Speichern einer Konfigurations- bzw. Skript-Datei generiert. Die Speicherung einer MAC-Adresse und / oder Geräte-Seriennummer ist optional. Mehr dazu erfahren Sie unter *Erweiterte Meta-Daten für Konfigurationsdateien* auf Seite 194.

Wenn der automatische Ladevorgang vollständig abgeschlossen ist, leuchten alle LEDs des Geräts für 30 Sekunden grün. Sie können das USB-Medium dann entfernen.

2.10.3 Konfiguration des automatischen Ladens via USB

Die nachfolgenden Schritte zeigen Ihnen, wie Sie das automatische Laden von einem USB-Datenträger konfigurieren.

1. Starten Sie LANconfig und öffnen Sie den Konfigurationsdialog für das Gerät.
2. Wechseln Sie in den Dialog **Management** > **Erweitert**.



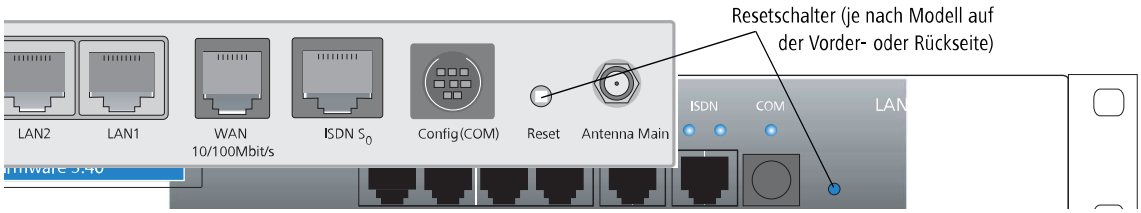
3. (De-)Aktivieren Sie das automatische Laden von Loader- und / oder Firmware-Dateien über die Auswahlliste **Firmware**. Dazu wählen Sie die entsprechende Rahmenbedingung aus.
   - **Aus**: Das automatische Laden von Loader- und / oder Firmware-Dateien für das Gerät ist deaktiviert.
   - **Bei unkonfiguriert. Gerät**: Das automatische Laden von Loader- und / oder Firmware-Dateien für das Gerät ist nur dann aktiviert, wenn sich das Gerät im Auslieferungszustand befindet. Nach erfolgreicher Erstkonfiguration durch den Assistenten für Sicherheitseinstellungen bzw. Grundeinstellungen setzt dieser die Einstellung auf **Aus**.
   - **Ein**: Das automatische Laden von Loader- und / oder Firmware-Dateien für das Gerät ist aktiviert. Beim Mounten eines USB-Mediums wird versucht, eine passende Loader- und / oder Firmware-Datei in das Gerät zu laden. Das USB-Medium wird beim Einstecken in den USB-Anschluss am Gerät oder beim Neustart gemountet.
4. (De-)Aktivieren Sie das automatische Laden von Konfigurations- und / oder Skript-Dateien über die Auswahlliste **Konfiguration**. Dazu wählen Sie die entsprechende Rahmenbedingung aus.
   - **Aus**: Das automatische Laden von Konfigurations- und / oder Skript-Dateien für das Gerät ist deaktiviert.
   - **Bei unkonfiguriert. Gerät**: Das automatische Laden von Konfigurations- und / oder Skript-Dateien für das Gerät ist nur dann aktiviert, wenn sich das Gerät im Auslieferungszustand befindet. Nach erfolgreicher Erstkonfiguration durch den Assistenten für Sicherheitseinstellungen bzw. Grundeinstellungen setzt dieser die Einstellung auf **Aus**.
   - **Ein**: Das automatische Laden von Konfigurations- und / oder Skript-Dateien für das Gerät ist aktiviert. Beim Mounten eines USB-Mediums wird versucht, eine passende Konfigurations- und / oder Skript-Datei in das Gerät zu laden. Das USB-Medium wird beim Einstecken in den USB-Anschluss am Gerät oder beim Neustart gemountet.

Fertig! Damit haben Sie die Konfiguration des automatischen Ladens von einem USB-Datenträger abgeschlossen.

Wenn Sie verhindern wollen, dass ein Gerät durch manuellen Reset auf Werkseinstellungen und Einstecken eines USB-Datenträgers mit einer unerwünschten Konfiguration versehen werden kann, müssen Sie den Reset-Schalter deaktivieren.

2.11 Geräte-Reset durchführen

Wenn Sie unabhängig von den evtl. vorhandenen Einstellungen das Gerät neu konfigurieren müssen oder selbst nach einem Neustart keine Verbindung zur Gerätekonfiguration zustande kommt, besteht die Möglichkeit, mit einem Reset das Gerät in den Auslieferungszustand zurückzusetzen. Dazu betätigen Sie den Reset-Knopf **bis zum ersten Aufleuchten** sämtlicher LEDs des Gerätes (ca. 5 Sekunden).



Das Gerät startet nach dem Reset neu im unkonfigurierten Zustand, **alle** Einstellungen gehen dabei verloren. Sichern Sie daher **vor** dem Reset nach Möglichkeit die aktuelle Konfiguration des Gerätes!

Ein Access Point befindet sich nach dem Reset im Managed-Modus. In diesem Modus ist kein WLAN-Zugriff auf die Konfiguration möglich.

Bei einem Reset werden die im Gerät definierten WLAN-Verschlüsselungseinstellungen auf den Standard-WPA-Schlüssel zurückgesetzt. Der Standard-WPA-Schlüssel besteht aus der MAC-Adresse der physikalischen WLAN-Schnittstelle mit vorangestelltem "L". Die drahtlose Konfiguration mit dem WLAN-Gerät gelingt nach einem Reset lediglich dann, wenn Sie den Standard-WPA-Schlüssel unter **Wireless-LAN** > **Verschlüsselung** > **WLAN-Verschlüsselungs-Einstellungen** eingetragen haben.

Bei Outdoor Access Points ist der Geräte-Reset von der Bauform abhängig. Die genaue Vorgehensweise für ein spezifisches Gerät finden Sie in der entsprechenden Hardware-Schnellübersicht.

2.11.1 Konfiguration des Reset-Knopfes

Der Reset-Knopf hat mit Booten (Neustart) und Reset (Rücksetzen auf Werkseinstellung) grundsätzlich zwei verschiedene Funktionen, die durch unterschiedlich lange Betätigungszeiten des Knopfes ausgelöst werden.

Manche Geräte können jedoch nicht unter Verschluss aufgestellt werden. Hier besteht die Gefahr, dass die Konfiguration versehentlich gelöscht wird, wenn ein Mitarbeiter den Reset-Knopf zu lange gedrückt hält. Mit einer entsprechenden Einstellung lässt sich das Verhalten des Reset-Knopfes gezielt steuern.

Bei Geräten ohne serielle Schnittstelle können Sie den Reset-Knopf nicht umkonfigurieren, da sich bei diesen Geräten ansonsten ein Reset der Konfiguration nicht mehr durchführen ließe.

1. Wechseln Sie im LCOS-Menübaum in den Zweig **/Setup/Config**.
2. Legen Sie über den Parameter **Reset-Knopf** das Verhalten des Gerätes beim Betätigen des Reset-Knopfes fest. Mögliche Einstellungen sind:
   - **ignorieren**: Der Druck auf den Knopf löst keine Aktion aus.
   - **nur-booten**: Der Druck auf den Knopf löst einen Neustart aus, unabhängig von der gedrückten Dauer.
   - **reset-oder-booten**: In dieser Einstellung hat der Reset-Knopf verschiedene Funktionen, die Sie durch unterschiedlich lange Betätigungszeiten des Knopfes auslösen. Mehr zu den unterschiedlichen Betätigungszeiten finden Sie im Abschnitt *Besonderheiten der Rollout-Konfiguration* auf Seite 85.

   Mit der Einstellung **ignorieren** oder **nur-booten** wird das Rücksetzen der Konfiguration in den Auslieferungszustand sowie das Laden der Rollout-Konfiguration durch einen Reset unmöglich gemacht. Falls für ein Gerät in diesem Zustand das Konfigurationspasswort nicht mehr vorliegt, gibt es keine Möglichkeit

mehr, auf das Gerät zuzugreifen! In diesem Fall kann über die serielle Konfigurationsschnittstelle eine neue Firmware in das Gerät geladen werden; dabei wird das Gerät in den Auslieferungszustand zurückgesetzt und die bisherige Konfiguration gelöscht.

3. Klicken Sie **Setzen**, um die Konfiguration zurück in das Gerät zu schreiben.

2.12 Rechteverwaltung für verschiedene Administratoren

Sie haben die Möglichkeit, in der Konfiguration Ihres Gerätes mehrere Administratoren anzulegen, die über unterschiedliche Zugriffs- und Funktionsrechte verfügen.

Neben den in der Konfiguration angelegten Administratoren gibt es auch noch den Root-Administrator mit dem Hauptgerätepasswort. Dieser Administrator hat immer die vollen Rechte und kann auch nicht gelöscht, eingeschränkt oder umbenannt werden. Um sich als Root-Administrator anzumelden, benutzen Sie beim Login via LANconfig, WEBconfig oder Terminalprogramm den Benutzternamen `root` oder lassen das betreffende Eingabefeld leer.

Sobald in der Geräte-Konfiguration ein Hauptgerätepasswort gesetzt ist, erscheint beim HTTP(S)-Zugriff auf das Gerät mit einem Webbrowser die Anmeldemaske von WEBconfig. Sofern neben dem Root-Administrator noch andere Administratoren eingerichtet sind, umfasst die Maske die Eingabefelder **Login** und **Passwort**; andernfalls nur **Passwort**. Nach der Eingabe der korrekten Zugangsdaten gelangt ein Benutzer weiter zum Hauptmenü. In diesem Menü sind nur die Punkte vorhanden, für die ein Administrator auch die entsprechenden Zugriffs- bzw. Funktionsberechtigungen hat.

2.12.1 Die Rechte für die Administratoren

Die Rechte für Administratoren unterteilen sich in zwei Bereiche:

- *Zugrifftsrechte*: Jeder Administrator gehört zu einer bestimmten Gruppe, der global definierte Zugriffsrechte zugewiesen sind.
- *Funktionsrechte*: Jeder Administrator verfügt außerdem über sogenannte Funktionsrechte, die den persönlichen Zugriff auf bestimmte Funktionen – wie z. B. die Setup-Assistenten – regeln.

2.12.1.1 Zugriffsrechte

Die nachfolgende Tabelle zeigt Ihnen eine Übersicht aller Berechtigungslevel, die Sie an Administratoren vergeben können. Folgende Zugriffsrechte bzw. Gruppen von Administrator-Konten sind konfigurierbar:

Tabelle 13: Übersicht der Zugriffsrechte

Bezeichnung unter LANconfig	Bezeichnung im Setup-Menü	Rechtebeschreibung
Alle	Supervisor	Supervisor. Ist Mitglied in allen Gruppen und hat mit Ausnahme der Einrichtung bzw. Bearbeitung von anderen Administratoren vollen Zugriff auf die Konfiguration.
Eingeschr. und Tracen	Admin-RW	Lokaler Administrator mit Lese- und Schreibzugriff. Hat vollen Zugriff auf die Konfiguration, jedoch sind folgende Möglichkeiten gesperrt: › Firmware in das Gerät hochladen › Konfiguration in das Gerät einspielen › Konfiguration über LANconfig › Kann andere Administratoren nicht anlegen oder bearbeiten
Eingeschränkt	Admin-RW-Limit	Lokaler Administrator mit Lese- und Schreibzugriff, aber ohne Trace-Rechte. Hat vollen Zugriff auf die Konfiguration, jedoch sind folgende Möglichkeiten gesperrt: › Firmware in das Gerät hochladen › Konfiguration in das Gerät einspielen

Bezeichnung unter LANconfig	Bezeichnung im Setup-Menü	Rechtebeschreibung
		› Konfiguration über LANconfig › Kann andere Administratoren nicht anlegen oder bearbeiten › Trace-Ausgaben über die Konsole oder LANmonitor
Lesen und tracen	Admin-RO	Lokaler Administrator mit Lesezugriff, aber ohne Schreibzugriff. Kann die Konfiguration über die Konsole auslesen, aber keine Werte verändern.
Nur lesen	Admin-RO-Limit	Lokaler Administrator mit Lesezugriff, aber ohne Schreibzugriff und ohne Trace-Rechte. Kann die Konfiguration über die Konsole auslesen, aber keine Werte verändern und Trace-Ausgaben anfordern.
Keine	Kein	Hat keinen Zugriff auf die Konfiguration.

Lokale Administratoren können die Admintabelle nicht bearbeiten oder einsehen. Dies ist dem Root-Administrator vorbehalten.

2.12.1.2 Funktionsrechte

Die nachfolgende Tabelle zeigt Ihnen eine Übersicht aller Funktionsrechte, die insgesamt für Administrator-Konten konfigurierbar sind. Die Verfügbarkeit einzelner Funktionsrechte kann dabei – je nach Funktionsumfang des Gerätes – variieren. Sofern Sie Funktionsrechte auf der Konsole oder in einem Skript setzen möchten, haben Sie die Möglichkeit, alternativ zur Klartext-Bezeichnung des jeweiligen Rechtes die Hexschreibweise zu verwenden. Mehr dazu erfahren Sie im Abschnitt *Hexadezimale Kombination von Funktionsrechten auf der Konsole* auf Seite 111.

Tabelle 14: Übersicht der Funktionsrechte

Bezeichnung: [1]LANconfig, [2]Setup-Menü	Hexschreibweise an der Konsole	Rechtebeschreibung
1. AP-Assignment-Assistent **2.** WTP-Zuordnungs-Assistent	0x00000400	Assistent für die Zuweisung von WLAN-Profilen
1. Content-Filter-Assistent **2.** CF-Profil-Assistent	0x00040000	Assistent für die Einrichtung des Content-Filters
1. Dynamic-DNS-Assistent **2.** Dynamic-DNS-Assistent	0x00004000	Assistent für die Konfiguration von Dynamic DNS
1. Einstellen von Datum und Uhrzeit **2.** Zeit-Setzen	0x00000040	Setzen von Uhrzeit und Datum (gilt auch für Telnet und TFTP)
1. Grundeinst.-Assistent **2.** Grundkonfigurations-Assistent	0x00000001	Assistent für die Grundeinstellungen
1. Internet-Assistent **2.** Internet-Assistent	0x00000004	Assistent für die Einrichtung des Internetzugangs
1. LAN-LAN-Assistent **2.** LANLAN-Assistent	0x00000020	Assistent für die Verbindung zweier lokaler Netze (VPN)
1. Public-Spot-Assistent (Benutzer anlegen) **2.** Public-Spot-Assistent	0x00000800	Assistent für die Einrichtung von Public Spot-Benutzern*
1. Public-Spot-Assistent (Benutzer verwalten) **2.** Public-Spot-Benutzerverwaltungs-Assistent	0x00100000	Assistent für die Verwaltung von Public Spot-Benutzern*
1. – **2.** Public-Spot-Konfigurations-Assistent	0x00200000	Assistent für die Einrichtung eines Public Spots

Bezeichnung: [1]LANconfig, [2]Setup-Menü	Hexschreibweise an der Konsole	Rechtebeschreibung
1. Public-Spot-XML-Interface **2.** Public-Spot-Xml-Schnittstelle	0x00080000	Zugriff auf die XML-Schnittstelle des Public Spot-Moduls Ein „normaler" Public Spot-Administrator benötigt dieses Recht nicht. Das Recht dient vielmehr dazu, einem externen Gateway – z. B. einer Maschine oder einem Programm (Webserver, Skript etc.) – die Kommunikation mit dem Modul zu ermöglichen, um komplexe Anmeldeszenarien zu realisieren.
1. RAS-Assistent **2.** RAS-Assistent	0x00000010	Assistent für die Einrichtung eines Einwahlzugangs (RAS, VPN)
1. Rollout-Assistent **2.** Rollout-Assistent	0x00002000	Assistent für den Rollout*
1. Sicherheits-Assistent **2.** Sicherheits-Assistent	0x00000002	Assistent für die Kontrolle der Sicherheitseinstellungen
1. Senden von SMS **2.** SMS-Versand	0x400000	Versand von SMS-Nachrichten über das geräteeigene 3G/4G WWAN-Modul
1. SSH-Client **2.** SSH-Kommando	0x00020000	Herstellen einer SSH-/Telnet-Verbindung von Ihrem Gerät zu anderen LCOS-Geräten oder SSH-/Telnet-Servern
1. Suche weiterer Geräte im LAN **2.** Geraetesuche	0x00000080	Suche nach weiteren Geräten in lokalen und entfernten Netzen*
1. VoIP-Provider-Assistent **2.** VoIP-Provider-Zugang-Vorbereiten	0x800000	Assistent für die Einrichtung eines Zugangs zu Ihrem VoIP-Provider
1. VoIP-CallManager-Wizard **2.** VoIP-CallManager-Wizard	0x8000	Assistent für die Einrichtung Ihres VoIP-CallManagers
1. WLAN-Assistent **2.** WLAN-Assistent	0x00001000	Assistent für die Konfiguration der WLAN-Schnittstelle
1. WLAN-Linktest **2.** WLAN-Linktest	0x00000100	Ausführen des WLAN Link-Tests* (gilt auch für Telnet)
1. WLC-Profil-Assistent **2.** WLC-Profil-Assistent	0x00010000	Assistent für die Einrichtung eines WLC-Profils
1. CA-Web-Schnittstellen-Assistent **2.** CA-Web-Schnittstelle	0x1000000	Erstellen für Profile der CA-Web-Schnittstelle

*) Die Berechtigung bzw. das Ausführen dieses Assistenten oder dieser Funktion bezieht sich – sofern nicht anders erwähnt – ausschließlich auf WEBconfig. Entweder ist der betreffende Assistent oder die betreffende Funktion nur dort verfügbar (z. B. Einrichten und Verwalten von Public Spot-Benutzern) oder nur dort beschränkbar (z. B. Suche nach Geräten).

Hexadezimale Kombination von Funktionsrechten auf der Konsole

Da die Konfiguration mehrerer Funktionsrechte über die Klartext-Bezeichnung beim Skripten einen hohen Schreibaufwand verursacht, haben Sie alternativ auch die Möglichkeit, an Stelle der Bezeichnungen deren Hexwerte zu verwenden und diese Einzelwerte als kombinierte Summe in Ihr Skript-Kommando einzubauen.

Die Summe mehrerer Hex-Werte ergibt sich aus der hexadezimalen Addition der ersten, zweiten, dritten … n-ten Stelle von rechts. Soll der Benutzer z. B. die Funktionen **Sicherheits-Assistent**, **Provider-Auswahl**, **RAS-Assistent**, **Zeit-Setzen** und **WLAN-Linktest** ausführen dürfen, berechnet sich die Summe der einzlnen Hexwerte wie folgt:

- 1. Stelle rechts: `2` (Sicherheits-Assistent) + `8` (Provider-Auswahl) = `a`
- 2. Stelle rechts: `1` (RAS-Assistent) + `4` (Zeit-Setzen) = `5`
- 3. Stelle rechts: `1` (WLAN-Linktest) = `1`

Für dieses Beispiel tragen die Funktionsrechte somit den Wert `0x0000015a`. Anders ausgedrückt handelt es sich hierbei um eine ODER-Verknüpfung der Hexadezimal-Werte:

Bezeichnung auf der Konsole	Wert
Sicherheits-Assistent	`0x00000002`
Provider-Auswahl	`0x00000008`
RAS-Assistent	`0x00000010`
Zeit-Setzen	`0x00000040`
WLAN-Linktest	`0x00000100`
ODER-verknüpft	`0x0000015a`

Alternativ zur Schreibweise `0x0000015a` stehen Ihnen auch die verkürzten Kurzschreibweisen `0000015a`, `0x15a` und `15a` zur Option.

Konfigurationsbeispiel auf der Konsole

Mit dem folgenden Befehl legen Sie in der Kurzschreibweise einen neuen Benutzer in der Admintabelle (im Setup-Menü unter **Config** > **Admins**) an, der als lokaler Administrator `NetAdmin` mit dem Passwort `BW46zG29` den Internetprovider auswählen darf. Der Benutzer wird dabei sofort aktiviert:

```
set NetAdmin BW46zG29 ja Admin-RW 8
```

Nur der Root-Administrator darf diesen Befehl ausführen, da andere Administratoren keinen Zugriff auf die Admintabelle haben.

Mit dem folgenden Befehl erweitern Sie die Funktionsrechte dahingehend, das Benutzer `NetAdmin` auch den WLAN-Link-Test ausführen darf. Die Sternchen im Kommando stehen dabei für die nicht zu verändernden Werte:

```
set NetAdmin * * * 108
```

Nur der Root-Administrator darf diesen Befehl ausführen, da andere Administratoren keinen Zugriff auf die Admintabelle haben.

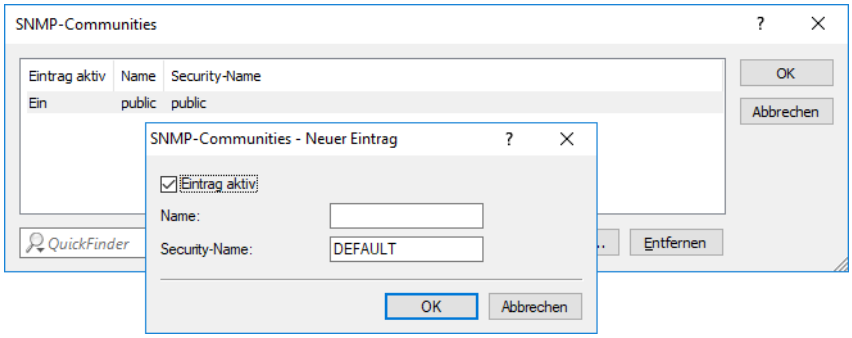
2.12.2 Konfigurieren des SNMP-Lesezugriffs

Auch bei der Verwaltung von Netzwerken mit SNMP-Management-Systemen lassen sich die Rechte über verschiedene Zugriffsebenen für Administratoren präzise steuern. SNMP kodiert dazu bei den Versionen SNMPv1 und SNMPv2c die Zugangsdaten als Teil einer sogenannten „Community“, welche die Bedeutung eines Passworts bzw. Zugangsschlüssels inne hat. Die Authentifizierung kann hierbei wahlweise

- über die Community `public` (uneingeschränkter SNMP-Lesezugriff),
- ein Master-Passwort (beschränkter SNMP-Lesezugriff), oder

- eine Kombination aus Benutzername und Passwort, getrennt durch einen Doppelpunkt (beschränkter SNMP-Lesezugriff),

erfolgen. Standardmäßig beantwortet Ihr Gerät alle SNMP-Anfragen, die es von LANmonitor oder einem anderen SNMP-Management-System mit der Community `public` erhält. Da dies jedoch (v. a. bei externer Erreichbarkeit) ein potentielles Sicherheitsrisiko darstellt, haben Sie die Möglichkeit, in LANconfig unter **Management** > **Admin** mit einem Klick auf **SNMP-Einstellungen** und **SNMP-Communities** eigene Communities zu definieren.



Um eine autorisierte Abfrage von Zugangsdaten beim SNMP-Lesezugriff über SNMPv1 oder SNMPv2c zu erzwingen, deaktivieren Sie die Community `public` in der Liste der SNMP-Communities. Dadurch lassen sich Informationen über den Zustand des Gerätes, aktuelle Verbindungen, Reports, etc. erst dann via SNMP auslesen, nachdem sich der betreffende Benutzer am Gerät authentifiziert hat. Die Autorisierung erfolgt wahlweise über die Zugangsdaten des Administrator-Accounts oder über den in der individuellen SNMP-Community definierten Zugang.

Das Deaktivieren der Community `public` hat keine Auswirkung auf den Zugriff über eine weitere angelegte Community.

Eine individuelle SNMP Read-Only Community bleibt z. B. stets ein alternativer Zugangsweg, der nicht an ein Administrator-Konto gebunden ist.

Der SNMP-Schreibzugriff bleibt ausschließlich Administratoren mit entsprechenden Berechtigungen vorbehalten.

2.13 Geräteinterne SSH- / SSL-Schlüssel

Das Gerät übermittelt Fingerprints beim Aufbau gesicherter Verbindungen (z. B. via SSH oder SSL) an die anfragende Gegenstelle. Die Gegenstelle kann anhand des Fingerprints erstens das Gerät eindeutig identifizieren und zweitens für sich verifizieren, den Verbindungsaufbau mit dem korrekten als vertrauenswürdig eingestuften Gerät durchgeführt zu haben.

Wenn Sie also z. B. in LANconfig als Kommunikationsprotokoll SSH auswählen und darüber erstmalig eine Verbindung zum betreffenden Gerät aufbauen, hinterfragt LANconfig in einer Sicherheitsabfrage, ob Ihnen der zugehörige ssh-rsa-Schlüssel vertraut ist und LANconfig das Gerät darüber zukünftig als „bekannt“ registrieren soll.

2.13.1 Automatische Erzeugung gerätespezifischer SSH- / SSL-Schlüssel

Sofern Sie keinen individuellen Schlüssel ins Gerät geladen haben, versucht der interne SSH-Server nach einem Konfigurations-Reset direkt beim Systemstart, eigene gerätespezifische SSH-Schlüssel zu kompilieren. Dazu gehören

- ein SSH-2-RSA-Schlüssel mit 2048 Bit Länge;
- ein SSH-2-DSS-Schlüssel mit 1024 Bit Länge (Definition nach FIPS 186-2);
- ein SSH-2-ECDSA-Schlüssel mit 256, 384 oder 521 Bit Länge;
- ein SSL-RSA-Schlüssel mit 2048 Bit Länge;

welche das Gerät als `ssh_rsakey`, `ssh_dsakey`, `ssl_privkey` oder `ssh_ecdsakey` in seinem internen Dateisystem ablegt.

Im Falle einer erfolgreichen Schlüsselerzeugung erfolgt der Eintrag `SSH: … host key generated` als „Hinweis“ ins SYSLOG; bei fehlgeschlagener Erzeugung der Eintrag `SSH: host key generation failed, try later again with '…'` als „Alarm“. Bei fehlgeschlagener Erzeugung (z. B. wegen mangelnder Entropie) erfolgt ein Rückfall auf den werksseitig implementierten Kryptographie-Schlüssel.

Wenn Sie von einer älteren LCOS-Version ein Update auf 8.84 oder höher ohne anschließenden Konfigurations-Reset durchführen, generiert das Gerät keinen gerätespezifischen SSH- / SSL-Schlüssel, um die Kompatibilität zu Bestandsinstallationen zu wahren. Sie haben jedoch die Möglichkeit, die Schlüsselerzeugung manuell zu initiieren. Geben Sie dazu an der Konsole die folgenden Befehle ein:

```
sshkeygen -t rsa -b 3072 -f ssh_rsakey
sshkeygen -t dsa -b 1024 -f ssh_dsakey
sshkeygen -t ecdsa -b 256 -f ssh_ecdsakey
sshkeygen -t rsa -b 3072 -f ssl_privkey
```

2.13.2 Individuelle SSH-Schlüssel manuell erzeugen

Sie haben die Möglichkeit, die automatisch generierten SSH- / SSL-Schlüssel durch eigene RSA- und DSA- oder DSS-Schlüssel zu ersetzen, um z. B. eine höhere Verschlüsselungsstärke zu realisieren. Dafür stehen Ihnen mehrere Wege zur Auswahl:

- Sie lassen den individuellen Schlüssel auf der Konsole direkt durch LCOS erzeugen.
- Sie erzeugen mit einem externen Programm einen OpenSSH-Private-Key und laden diesen Schlüssel anschließend als `SSH - DSA-Schlüssel […]` oder `SSH - RSA-Schlüssel (*.key [BASE64 unverschlüsselt])` in das Gerät.

Der Weg über ein externes Programm bietet sich z. B. dann an, wenn Ihr Gerät über keine hinreichende Entropie verfügt und dadurch die Schlüsselerzeugung unter LCOS fehlschlägt.

SSH-Schlüsselerzeugung unter LCOS

Die Erzeugung eines Schlüsselpaares – bestehend aus einem öffentlichen und einem privaten Schlüssel – starten Sie an der Konsole des Gerätes mit folgendem Befehl:

```
sshkeygen [-h] [-q] [-t dsa|rsa|ecdsa|ed25519|ed448] [-b <bits>] [-f <Dateiname>]
```

-?, -h

Zeigt eine kurze Hilfe der möglichen Parameter.

-t (dsa|rsa|ecdsa|ed25519|ed448)

Dieser Parameter bestimmt den Typ des erzeugten Schlüssels. Insgesamt unterstützt SSH folgende Typen von Schlüsseln:

- RSA-Schlüssel sind am weitesten verbreitet und haben eine Länge von 512 bis zu 16384 Bit. Verwenden Sie nach Möglichkeit Schlüssel mit einer Länge von 3072 Bit.
- DSA-Schlüssel folgen dem Digital Signature Standard (DSS) des National Institute of Standards and Technology (NIST) und werden z. B. in Umgebungen eingesetzt, die eine Compliance mit dem Federal Information Processing Standard (FIPS) erfordern. DSA- oder DSS-Schlüssel haben immer eine Länge von 1024 Bit, sind aber langsamer als die entsprechenden RSA-Schlüssel.
- ECDSA-Schlüssel sind eine Variante von DSA-Schlüsseln, bei der das Gerät für die Schlüsselerzeugung elliptische Kurven verwendet (Elliptic Curve Cryptography, ECC). Die ECC ist eine Alternative zu den klassischen Signatur- und Schlüsselaustauschverfahren wie RSA und Diffie-Hellman. Der Hauptvorteil von elliptischen Kurven liegt darin, dass Sie durch deren mathematische Eigenschaften die gleiche Schlüsselstärke wie bei RSA oder Diffie-Hellman mit einer deutlich kürzeren Schlüssellänge erreichen. Dies erlaubt eine bessere Leistung bei äquivalenter Hardware. ECC und deren Integration in SSL und TLS sind in den RFCs *5656* und *4492* beschrieben.
- Ed25519 ist ein Verfahren basierend auf dem Edwards-curve Digital Signature Algorithm (EdDSA) (*RFC 8709*) basierend auf elliptischen Kurven.

- Ed448 ist ebenfalls ein Verfahren basierend auf elliptischen Kurven, welches in *RFC 8709* spezifiziert ist.

Wenn Sie keinen Typ angeben, erzeugt das Kommando immer einen RSA-Schlüssel.

-b <Bits>

Dieser Parameter bestimmt die Länge des Schlüssels in Bit für RSA-Schlüssel. Wenn Sie keine Länge angeben, erzeugt das Kommando immer einen Schlüssel mit einer Länge von 1024 Bit.

-f <OutputFile>

Über diesen Parameter geben Sie den Dateinamen der erzeugten Schlüsseldatei im Dateisystem des Gerätes an. Die Wahl des Dateinamens hängt davon ab, was für einen Schlüssel sie von welchem Typ erzeugen. Zur Auswahl stehen Ihnen in diesem Fall:

- `ssh_rsakey` für RSA-Schlüssel
- `ssh_dsakey` für DSA-Schlüssel
- `ssh_ecdsakey` für ECDSA-Schlüssel
- `ssl_privkey` für SSL-RSA-Schlüssel
- `ssh_ed25519key` für Ed25519-Schlüssel
- `ssh_ed448key` für Ed448-Schlüssel

-q

Dieser Parameter aktiviert den 'Quiet'-Modus für die Schlüsselerzeugung. Wenn Sie diesen Parameter setzen, überschreibt LCOS bereits existierende RSA- oder DSA-Schlüssel ungefragt; Ausgaben über den Fortschritt der Operation entfallen. Nutzen Sie diesen Parameter z. B. in einem Skript, um die Bestätigung von Sicherheitsabfragen durch den Benutzer zu unterdrücken.

SSH-Schlüsselerzeugung unter Linux-Systemen

Zahlreiche Linux-Distributionen haben das OpenSSH-Paket bereits installiert. Hier genügt ein einfacher Befehl an der Shell, um die gewünschte Schlüsseldatei zu erzeugen. Die verwendete Syntax entspricht dabei der des LCOS-Befehls `sshkeygen`:

```
ssh-keygen [-t (dsa|rsa)] [-b <Bits>] [-f <OutputFile>]
```

Mit einem Befehl `ssh-keygen -t rsa -b 4096 -f hostkey` erzeugen Sie also einen RSA-Schlüssel mit 4096 Bit Länge, welcher sich aus dem privaten Bestandteil 'hostkey' und dem öffentlichen Bestandteil 'hostkey.pub' zusammensetzt.

SSH-Schlüsselerzeugung unter Windows-Systemen

Windows-Systeme sind von Haus aus nicht dazu in der Lage, SSH-Schlüssel zu kompilieren. Nutzen Sie stattdessen entsprechende Hilfsprogramme wie die freie Software PuTTYgen.

Eine Anleitung, wie Sie mit PuTTYgen einen individuellen Schlüssel erstellen, finden Sie im Abschnitt *SSH-Schlüsselpaar erzeugen mit PuTTY* auf Seite 116. Befolgen Sie darin die einzelnen Schritte; speichern Sie den Schlüssel nach seiner Erzeugung jedoch **nicht** über die Schaltflächen **Save public key** und **Save private key**, sondern wählen Sie **Conversions** > **Export OpenSSH key**. Der so erstellte OpenSSH-Private-Key lässt sich anschließend ohne weitere Bearbeitung ins Gerät laden.

2.14 SSH-Authentifizierung mit Hilfe eines Public-Keys

Das SSH-Protokoll und der LCOS-eigene SSH-Server unterstützen zwei verschiedene Authentifizierungs-Mechanismen:

1. interaktiv durch Eingeben eines Benutzernamens und Passworts über die Tastatur;
2. automatisiert durch Übermitteln eines öffentlichen Schlüssels (Public-Key)

Beim Public-Key-Verfahren wird ein Schlüsselpaar aus privatem und öffentlichem Schlüssel verwendet – ein digitales Zertifikat. Der private Teil des Schlüsselpaares wird beim Client bzw. Nutzer gespeichert (häufig mit einem Passwort – auch Passphrase genannt – geschützt); der öffentliche Teil wird in das Gerät geladen. Da die Schlüssel individuell und anwenderbezogen sein müssen, existieren keine vordefinierten Standardschlüssel. Im Auslieferungszustand unterstützt Ihr Gerät daher nur die interaktive Authentifizierung über Zugangsdaten.

Die nachfolgenden Abschnitte beschreiben, wie Sie einen eigenen SSH-Schlüssel generieren und die Authentifizierung mit Hilfe eines öffentlichen Schlüssels realisieren. Als Anwendungen dienen exemplarisch LANconfig sowie der freie SSH-Client PuTTY, über dessen Hilfsprogramm PuTTYgen auch die Erzeugung des benötigten Schlüsselpaares erfolgen kann. PuTTY selbst ist sowohl für Windows- als auch Linux-Betriebssysteme erhältlich; die nachfolgenden Abschnitte beschränken sich jedoch – analog zu LANconfig – vorwiegend auf die Windows-Variante.

Ihr Gerät unterstützt sowohl RSA als auch DSA- bzw. DSS-Schlüssel. RSA-Schlüssel sind etwas kleiner und erlauben so einen etwas schnelleren Betrieb. Weitere Informationen zu diesen Schlüsseln finden Sie auch im VPN-Kapitel des Referenzhandbuchs im Abschnitt *Einsatz von digitalen Zertifikaten* auf Seite 770.

2.14.1 Ablauf der Zertifikatsprüfung beim SSH-Zugang

Beim Aufbau der SSH-Verbindung erkundigt sich der Client zunächst beim Gerät, welche Authentifizierungs-Methoden für diesen Zugang zugelassen sind. Sofern das Public-Key-Verfahren erlaubt ist, sucht der Client nach installierten privaten Schlüsseln und übergibt diese mit der Angabe des Benutzernamens zur Prüfung an das Gerät.

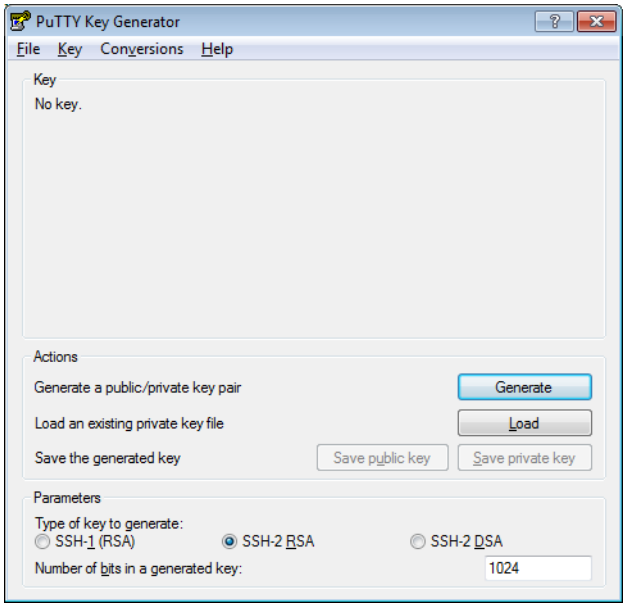
Findet das Gerät in der Liste seiner öffentlichen SSH-Schlüssel einen passenden Eintrag, in dem der Benutzername enthalten ist, wird der Zugang über SSH erlaubt. Hat der Client keinen passenden privaten Schlüssel installiert oder auf Seiten des Gerätes gibt es keine Übereinstimmung mit Benutzernamen oder öffentlichem Schlüssel, fordert das Gerät die Authentifizierung mit Benutzername/Passwort an (sofern diese Authentifizierungs-Methode erlaubt ist) oder bricht den Authentifizierungsprozess ab.

2.14.2 SSH-Schlüsselpaar erzeugen mit PuTTY

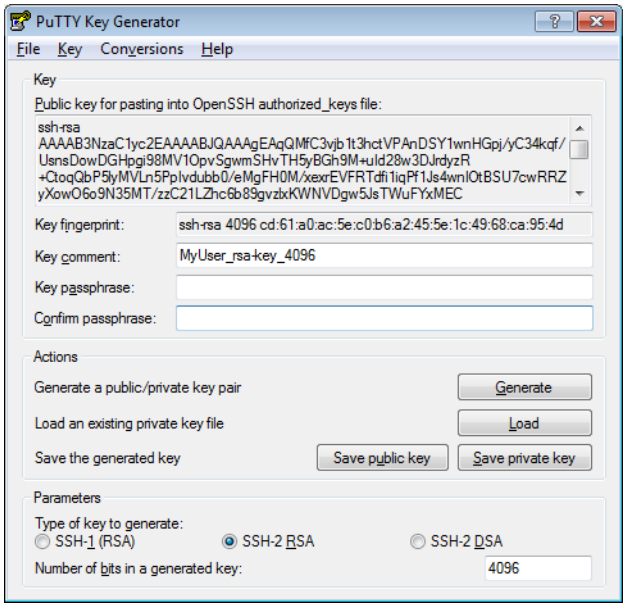
Für die SSH-Authentifizierung mit Hilfe eines Public-Keys benötigten Sie zu allererst ein persönliches Schlüsselpaar. Dieses Tutorial beschreibt, wie Sie mit PuTTYgen ein RSA-Schlüsselpaar – bestehend aus Public Key und Private Key – erzeugen.

Unter Linux-Betriebssystemen erstellt der Befehl `ssh-keygen` an der Shell ein RSA-Schlüsselpaar aus dem öffentlichen Teil 'id_rsa.pub' und dem privaten Teil 'id_rsa'. Siehe auch *SSH-Schlüsselerzeugung unter Linux-Systemen* auf Seite 115.

1. Starten Sie das PuTTY-Hilfsprogramm **PuTTYgen**. Es öffnet sich das Hauptfenster des **PuTTY Key Generator**s.



2. Wählen Sie die Art des zu erzeugenden Schlüssels (hier: **SSH-2-RSA**) und dessen Bit-Stärke (z. B. `4096`). Klicken Sie dann auf **Generate**, um mit der Schlüsselerzeugung zu beginnen.
3. Bewegen Sie die Maus danach solange willkürlich im Programmfenster, bis der Fortschrittsbalken das Ende erreicht hat. PuTTYgen generiert die für die Schlüsselerzeugung notwendigen Zufallszahlen aus den Bewegungen des Mauszeigers, die Sie innerhalb des Programmfensters vollziehen. Bewegen Sie die Maus daher solange willkürlich im Programmfenster, bis der Forschrittsbalken das Ende erreicht hat. Nach Abschluss der Erzeugung zeigt Ihnen das Programm die erzeugten Schlüsseldaten im Hauptfenster an.



4. Optional: Sofern Sie Ihren Private-Key mit einer zusätzlichen Passphrase absichern möchten, tragen Sie diese im Feld **Key passphrase** ein und bestätigen die Eingabe im Feld darunter.
   Bitte beachten Sie, dass einige SSH-Clients das Speichern einer Passphrase nicht oder nur für die aktuelle Sitzung erlauben (PuTTY z. B. nur über Pageant). Es kann daher sinnvoll sein, auf die Eingabe einer Passphrase zu verzichten, sofern Sie diese beim Verbindungsaufbau nicht manuell eingeben wollen. LANconfig selbst unterstützt das persistente Speichern einer Passphrase.

5. Klicken Sie auf die Schaltflächen **Save public key** und **Save private key**, um Ihren öffentlichen und Ihren privaten Schlüssel zu speichern.
   Den so erstellten öffentlichen Schlüssel hinterlegen Sie nach anschließender Bearbeitung im Gerät; den privaten Schlüssel verwenden Sie in Kombination mit PuTTY für die Authentisierung.
6. Wählen Sie außerdem **Conversions** > **Export OpenSSH key**, um den Schlüssel gleichzeitig als OpenSSH Private-Key abzuspeichern.
   Den so erstellten privaten Schlüssel verwenden Sie in Kombination mit LANconfig für die Authentisierung.
7. Beenden Sie PuTTYgen.

2.14.3 Syntax und Benutzer öffentlicher Schlüssel anpassen

Nachdem Sie ein Schlüsselpaar erzeugt haben, müssen Sie den dazugehörigen Public Key in eine vom Gerät akzeptierte und lesbare Form bringen. Ein LCOS-Gerät erwartet die öffentlichen Schlüssel in der folgenden Syntax:

```
<EncryptionAlgorithm> <PublicKey> <Admin1> [<Admin2> … <AdminN>]
```

Sie können somit einem einzigen öffentlichen Schlüssel mehrere Benutzerkonten zuweisen. Ebenso ist es möglich, mehrere Schlüssel für unterschiedliche Benutzer in das Gerät zu laden. Die nachfolgenden Schritte beschreiben anhand einer mit PuTTYgen erzeugten Public-Key-Datei, wie Sie einen öffentlichen Schlüssel korrekt anpassen.

1. Öffnen Sie die Public-Key-Datei in einem Texteditor. Es zeigt sich Ihnen folgender oder ähnlicher Inhalt:

```
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "rsa-key_myuser"
AAAAB3NzaC1yc2EAAAABJQAAAgEAqQMfC3vjb1t3hctVPAnDSY1wnHGpj/yC34kq
f/UsnsDowDGHpgi98MV1OpvSgwmSHvTH5yBGh9M+uId28w3DJrdyzR+CtoqQbP5l
…
0N8V3ydp+qbx+8FNbBQCVhxxiKZwXxmMh70pTWHxixOFte4HBxGHxcRaiSoMyNdv
wCkWlx8=
---- END SSH2 PUBLIC KEY ----
```

2. Löschen Sie die Kopf- und Fußzeile sowie die Kommentarzeile, sodass nur noch der eigentliche Schlüssel in der Datei verbleibt. Entfernen Sie anschließend sämtliche Zeilenumbrüche, sodass der öffentliche Schlüssel in einer einzigen Zeile steht.

```
AAAAB3NzaC1yc2EAAAABJQAAAgEAqQMfC3vjb1t3hctVPAnDSY1…wCkWlx8=
```

3. Ergänzen Sie den Anfang des Schlüssels um den Verschlüsselungsalgorhytmus `ssh-rsa` und das Ende um den Namen des Benutzerkontos, für den dieser Key Gültigkeit hat (z. B. `root`); getrennt mit je einem Leerzeichen.

   Sie haben die Möglichkeit, einem Schlüssel mehrere Benutzer zuzuweisen oder mehrere Schlüssel in einer einzigen Public-Key-Datei unterzubringen. **Beispiele**:

```
ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAAgEAqQMfC3vjb1t3hctVPAnDSY1j…wCkWlx8= root
```

```
ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAAgEAqQMfC3vjb1t3hctVPAnDSY1…wCkWlx8= root admin user
ssh-rsa VLn5PpIvdubb0/eMgFH0M/xexrEVFRTdfi1iqPf1Js4wnIOtBSU…xKWNVDg/ backup
```

   Achten Sie darauf, dass jeder Schlüssel (inklusive Verschlüsselungsalgorhytmus und Benutzer[n]) für sich in einer separaten Zeile steht. Zeilenumbrüche machen die Datei ungültig und führen zu einem Fehler bei der späteren Authentifizierung!

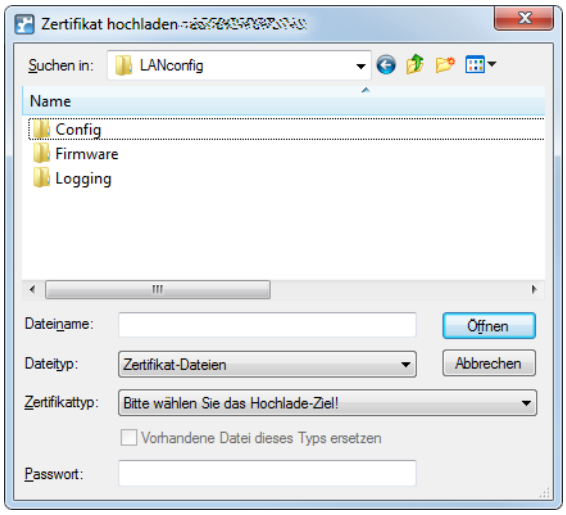
4. Speichern Sie die Datei und schließen Sie den Texteditor.

2.14.4 Gerät für die Public-Key-Authentifizierung einrichten

Dieses Tutorial beschreibt, wie Sie die Schlüsseldatei ins Gerät laden und das Gerät für die SSH-Authentifizierung vorbereiten.

1. Starten Sie LANconfig und markieren Sie das Gerät, für das Sie die SSH-Authentifizierung einrichten wollen.

2. Wählen Sie **Gerät** > **Konfigurations-Verwaltung** > **Zertifikat oder Datei hochladen** und ändern Sie im sich öffnenden Fenster die Auswahllisten **Dateityp** auf **Alle Dateien** sowie **Zertifikattyp** auf **SSH – akzeptierte öffentliche Schlüssel**.



3. Wählen Sie die zuvor erstellte Public-Key-Datei aus und klicken Sie **Öffnen**. LANconfig beginnt daraufhin mit dem Upload des öffentlichen Schlüssels in das Gerät.

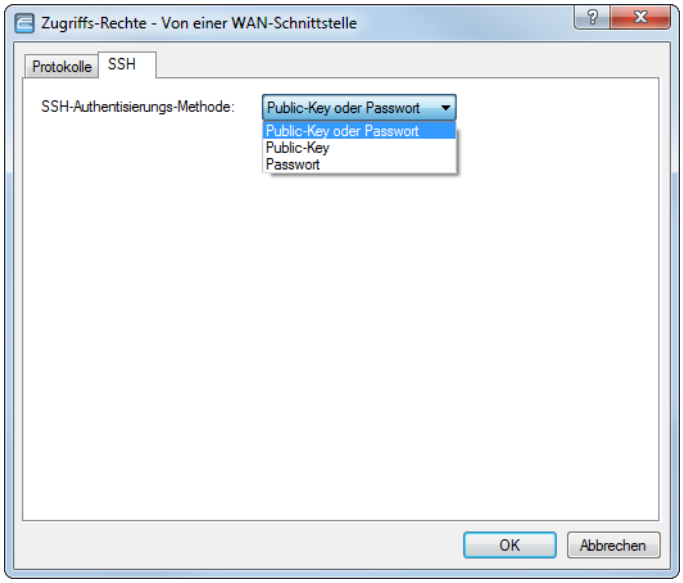
   Die hochgeladene Datei ersetzt die Liste der bisher ggf. im Gerät vorhandenen akzeptierten Schlüssel. Alternativ können Sie in WEBconfig die Schlüssel auch direkt editieren und einzelne Schlüssel an die bestehende Liste anhängen (siehe *Erlaubte öffentliche SSH Schlüssel* auf Seite 38).

4. Öffnen Sie den Konfigurationsdialog des Gerätes und wechseln Sie in den Dialog **Management** > **Admin** > **Zugriffseinstellungen>**.

5. Konfigurieren Sie im Abschnitt **Konfigurations-Zugriffs-Wege** unter **Zugriffsrechte** > **…** > **SSH** für jedes Netz die **SSH-Authentisierungs-Methode**.
   Die zulässigen Authentifizierungs-Methoden für den SSH-Zugang können für LAN, WAN und WLAN getrennt eingestellt werden. Folgende Möglichkeiten stehen zur Auswahl:

   - **Public-Key oder Passwort**: Hier wird zuerst die Authentisierungs-Methode Public-Key versucht. Sollte dieses scheitern wird die Passwort-Abfrage gewählt.
   - **Public-Key**: Hier wird nur die Authentisierungs-Methode Public-Key versucht.

› **Passwort**: Die Authentisierungs-Methode Public-Key wird abgeschaltet und es erfolgt die Passwort-Abfrage.

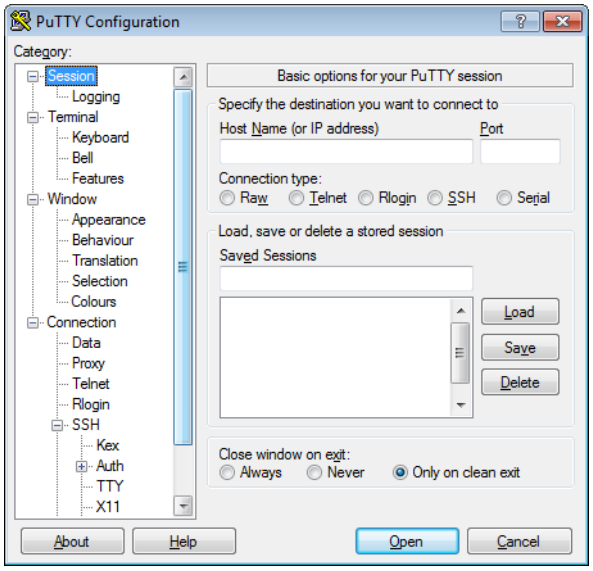


6. Schließen Sie den Konfigurationsdialog und schreiben Sie die Konfiguration auf das Gerät zurück.

2.14.5 Public-Key-Authentifizierung mit PuTTY

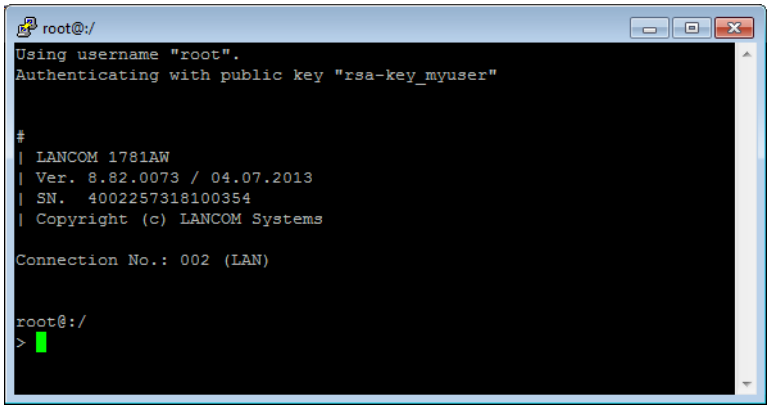
Dieses Tutorial beschreibt, wie Sie in PuTTY die SSH-Authentifizierung mit Hilfe eines Public-Keys konfigurieren und sich anschließend am konfigurierten Gerät anmelden.

1. Starten Sie PuTTY.
2. Geben Sie im sich öffnenden Fenster den Host-Namen oder die IP-Adresse des Gerätes an, und wählen Sie als **Connection type** die Option **SSH**. Der Standardport für SSH-Verbindungen ist `22`.



3. Wechseln Sie in den Dialog **Connection** > **Data** und tragen Sie in das Eingabefeld **Auto-login username** den Benutzernamen ein, auf den Sie den Public-Key zuvor ausgestellt haben (z. B. `root`).
4. Wechseln Sie in den Dialog **Connection** > **SSH** > **Auth** und geben Sie im Eingabefeld **Private key file for authentication** den Pfad sowie den Dateinamen der Private-Key-Datei an, die Sie speziell für PuTTY erstellt haben.

5. Klicken Sie abschließend auf **Open**. PuTTY beginnt daraufhin mit dem Verbindungsaufbau unter Verwendung der SSH-Authentifizierung mit Hilfe eines Public-Keys.



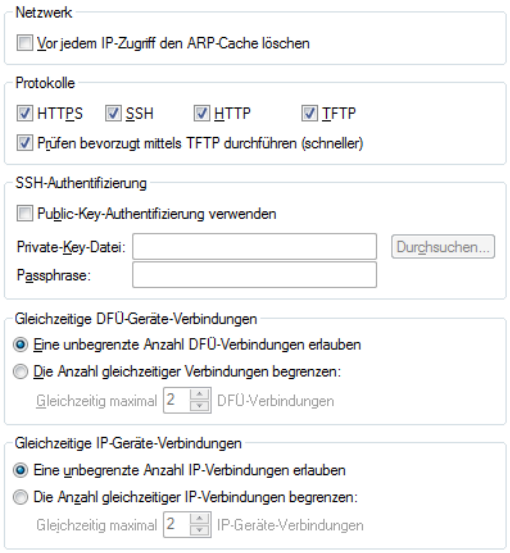
Sofern Sie Ihre Private-Key-Datei mit einer optionalen Passphrase gesichert haben, fragt PuTTY diese im Rahmen des Anmeldevorgangs bei Ihnen ab.

Fertig!

2.14.6 Public-Key-Authentifizierung mit LANconfig

Dieses Tutorial beschreibt, wie Sie in LANconfig die SSH-Authentifizierung mit Hilfe eines Public-Keys konfigurieren.

1. Starten Sie LANconfig.
2. Öffnen Sie über die Menüleiste den Dialog **Extras** > **Optionen** > **Kommunikation**.



3. Deaktivieren Sie im Bereich **Protokoll** mit Ausnahme von **SSH** und **Prüfen bevorzugt mittels TFTP durchführen** alle anderen Auswahlkästchen bzw. Protokolle.
   Dadurch verhindern Sie, dass LANconfig ein anderes Protokoll bei der Gerätekommunikation bevorzugt (z. B. HTTPS) oder bei Fehlschlagen der Authentifizierung auf ein anderes, womöglich unverschlüsseltes Protokoll (z. B. HTTP) ausweicht.
4. Aktivieren Sie die Option **Public-Key-Authentifizierung verwenden**.
5. Geben Sie passend dazu den Pfad und den Dateinamen der OpenSSH Private-Key-Datei an, und benennen Sie ggf. die Passphrase, mit der Ihr Schlüssel gesichert ist.
6. Schließen Sie den Dialog mit einem Klick auf **OK**, um den Einstellungsdialog zu schließen.

Fertig! Wenn Sie nun für ein Gerät den Konfigurationsdialog oder den Setup-Assistenten öffnen, wählt LANconfig die Kommunikation über das SSH-Protokoll und versucht, sich mit dem angegebenen Private-Key zu authentisieren.

2.15 SSH- und Telnet-Client im LCOS

2.15.1 Einleitung

Neben einem SSH-Server, der Ihnen eine sichere und authentifizierte Einwahl in das Gerät ermöglicht (siehe *SSH-Authentifizierung mit Hilfe eines Public-Keys* auf Seite 115), verfügt das Betriebssystem Ihres Gerätes auch über einen SSH-Client. Über diesen SSH-Client haben Sie die Möglichkeit, von Ihrem Gerät aus SSH-Verbindungen zu einem entfernten Server – z. B. einem weiteren Gerät oder einem Linux-Server – aufzubauen. Diese Funktion ist auch dann nützlich, wenn eine direkte Verbindung zu einem entfernten System nicht möglich ist, aber eine indirekte Verbindung über ein anderes Gerät existiert, welches aus beiden Subnetzen erreichbar ist.

Sie starten den LCOS-eigenen SSH-Client über einfache Befehle an der Konsole, ähnlich dem OpenSSH-Client auf einem Linux-System.

2.15.2 Syntax des SSH-Clients

Die SSH-Verbindung zu einem entfernten System über den LCOS-eigenen SSH-Client starten Sie an der Konsole mit folgendem Befehl:

```
ssh [-(?|h)] [-(b|a) <Loopback-Address>] [-p <Port>] [-C] [-j <keepalive-interval>] [-l login_name] [-o
"option=value"] [<User>@]<Host> <Command>
```

Die einzelnen Parameter haben dabei die folgende Bedeutung:

-?, -h

Zeigt eine kurze Hilfe der möglichen Parameter.

-b, -a <Loopback-Address>

Ermöglicht die Angabe einer Absenderadresse (Loopback-Adresse). Diese Option ist besonders im Zusammenhang mit ARF wichtig: Durch Angabe einer optionalen Loopback-Adresse verändern Sie die Quelladresse bzw. Route, mit der das Gerät das entfernte System anspricht. Dies kann z. B. dann sinnvoll sein, wenn das System über verschiedene Wege erreichbar ist und dieses einen bestimmten Weg für seine Antwort-Nachrichten wählen soll.

-p <Port>

Gibt den zu verwendenden Port an. Wenn Sie keinen Port angeben, verwendet das Gerät den für SSH standardisierten TCP-Port 22.

-C

Wenn Sie diesen Parameter setzen, versucht der SSH-Client, eine Datenkompression über den zlib-Algorithmus mit dem entfernten System auszuhandeln. Wenn das entfernte System diese Kompression nicht unterstützt, werden die Daten ohne Kompression übertragen.

Der Einsatz der Kompression ist in den meisten Fällen nur auf sehr langsamen Verbindungen sinnvoll. Auf schnellen Verbindungen ist der zusätzliche Overhead der Kompression meistens größer als der Gewinn durch die Datenreduzierung.

-j <keepalive-interval>

Wenn die Verbindung zu dem entfernten System über einen NAT-Router oder eine Firewall geführt wird, ist es möglicherweise sinnvoll, die Verbindung dauerhaft aufrecht zu erhalten. Bei einer interaktiven SSH-Sitzung werden jedoch phasenweise keine Daten übertragen, was zu einer Unterbrechung der Verbindung im Gateway aufgrund von Timeouts führen kann. In diesen Fällen kann der SSH-Client regelmäßig Keep-Alive-Pakete

senden, die das entfernte System als Leerlaufprozess interpretiert, dem Gateway aber das Fortbestehen der Verbindung signalisieren.

Über diesen Parameter geben Sie das Interval in Sekunden an, in dem Ihr Gerät die Keep-Alive-Pakete verschickt. Die Keep-Alive-Pakete werden dabei nur versendet, wenn der SSH-Client für die Dauer des Intervalls keine anderen Daten an das entfernte System schicken muss.

-o <option=Wert>
Mögliche Werte:

- StrictHostKeyChecking=<yes|no|off|ask|accept-new>: Prüfung des Hostschlüssels aktivieren/deaktivieren (Standardwert: ask)
- SignHostKeyAlgorithms=[+|-]<alg-list>: die Liste der zulässigen Unterschriftsalgorithmen erweitern/reduzieren/festlegen
- VerifyHostKeyAlgorithms=[+|-]<alg-list>: Liste der akzeptierten Unterschriftsalgorithmen erweitern/reduzieren/festlegen
- KeyAlgorithms=[+|-]<alg-list>: Liste der zulässigen Schlüsselaustausch-Algorithmen erweitern/reduzieren/festlegen
- Ciphers=[+|-]<alg-list>: Liste der zulässigen Verschlüsselungsalgorithmen erweitern/reduzieren/festlegen
- MACs=[+|-]<alg-list>: Liste der zulässigen (H)MAC-Algorithmen erweitern/reduzieren/einstellen
- Password=<password>: Passwort festlegen (deaktiviert die tastaturinteraktive Authentifizierungsmethode)

<User>

Benutzername für die Anmeldung am entfernten System. Wenn Sie keinen expliziten Benutzernamen angeben, verwendet LCOS Ihren aktuellen Benutzernamen, mit dem Sie sich an der Konsole angemeldet haben.

<Host>

DNS-Name oder IP-Adresse des entfernten Systems.

<Command>

Der LCOS-eigene SSH-Client kann entweder eine interaktive Shell auf dem entfernten System starten oder nur einen einzelnen Befehl ausführen. Wenn Sie keinen Befehl angeben, wird eine interaktive Shell gestartet.

2.15.3 Syntax des Telnet-Clients

Als Alternative zu SSH können Sie auch mit dem LCOS-eigenen Telnet-Client eine Verbindung zu einem entfernten System aufbauen. Den Telnet-Client starten Sie an der Konsole mit folgendem Befehl:

```
telnet [-(?|h)] [-b <Loopback-Address>] <Host> [<Port>]
```

-?, -h

Zeigt eine kurze Hilfe der möglichen Parameter.

-b <Loopback-Address>

Ermöglicht die Angabe einer Absenderadresse (Loopback-Adresse). Diese Option ist besonders im Zusammenhang mit ARF wichtig: Durch Angabe einer optionalen Loopback-Adresse verändern Sie die Quelladresse bzw. Route, mit der das Gerät das entfernte System anspricht. Dies kann z. B. dann sinnvoll sein, wenn das System über verschiedene Wege erreichbar ist und dieses einen bestimmten Weg für seine Antwort-Nachrichten wählen soll.

<Host>

DNS-Name oder IP-Adresse des entfernten Systems.

<Port>

Gibt den zu verwendenen Port an. Wenn Sie keinen Port angegeben, verwendet das Gerät den für Telnet standardisierten TCP-Port 23.

2.15.4 Öffentliche Schlüssel für die Authentifizierung

SSH nutzt für die Authentifizierung öffentliche Schlüssel, die vom entfernten System übermittelt werden. Wenn ein SSH-Client eine Verbindung zu einem SSH-Server aufbauen will, übermittelt der Server den öffentlichen Schlüssel an den Client, der diesen Schlüssel dann in seinen Dateien sucht. Die folgenden Situationen können dabei auftreten:

- Der SSH-Client findet den Schlüssel in seiner Liste der bekannten Server-Schlüssel, und der Schlüssel ist dem entsprechenden Hostnamen bzw. der IP-Adresse zugeordnet. Die SSH-Verbindung kann dann ohne weitere Benutzeraktivität aufgebaut werden.
- Der SSH-Client findet den Schlüssel **nicht** in seiner Liste der bekannten Server-Schlüssel, und auch keinen anderen Schlüssel vom gleichen Typ (RSA bzw. DSA / DSS) für den entsprechenden Hostnamen bzw. die IP-Adresse. Der SSH-Client geht davon aus, dass es die erste Verbindung zu diesem Server ist und zeigt den öffentlichen Schlüssel und den zugehörigen Fingerabdruck (Fingerprint) an. Der Anwender kann den Schlüssel mit einer auf anderem Wege übermittelten Version verifizieren und entscheiden, ob der Server in der Liste der bekannten SSH-Server gespeichert werden darf. Wenn der Anwender diese Verifizierung ablehnt, wird die SSH-Verbindung sofort beendet.
- Der SSH-Client findet einen Schlüssel für den entsprechenden Hostnamen bzw. die IP-Adresse, dieser weicht aber von dem aktuell verwendeten Schlüssel ab. Beide Schlüssel werden angezeigt, dann wird die SSH-Verbindung beendet, weil der SSH-Client eine Man-in-the-middle-Attacke vermutet. Sofern das entfernte System den öffentlichen Schlüssel kürzlich geändert hat, muss der Administrator den veralteten Eintrag aus der Liste der bekannten Server löschen (siehe *Bekannte SSH-Serverschlüssel manuell entfernen* auf Seite 124.

Nach der erfolgreichen Verifikation des Server-Schlüssels kann der Administrator das Passwort zur Anmeldung am entfernten System eingeben. Das Passwort kann nicht direkt über den Kommandozeilenbefehl eingegeben werden.

SSH-Verbindungen werden üblicherweise durch den Server beendet, z. B. durch Eingabe von `exit` an der Konsole. In manchen Fällen ist es nötig, die SSH-Verbindung durch den Client zu beenden, z. B. wenn die Anwendung auf der Server-Seite gestört ist. Der SSH-Client im LCOS verwendet die gleiche Zeichenfolge wie OpenSSH zum Beenden einer Verbindung, also die Folge 'Tilde – Punkt'.

Wenn die LCOS-Konsolensitzung selbst durch einen OpenSSH-Client geöffnet wurde, wird die Folge 'Tilde – Tilde – Punkt'verwendet, da ansonsten die falsche Verbindung beendet werden würde.

2.15.4.1 Liste der bekannten SSH-Server

Der SSH-Client im LCOS speichert alle ihm bekannten SSH-Schlüssel entfernter Systeme automatisch in einer eigenen Schlüsseldatei. Diese Schlüsseldatei trägt im internen Dateisystem die Bezeichnung **ssh_known_hosts**. Der Inhalt dieser Datei ändert sich jedes Mal, wenn Sie eine Verbindung zu einem Ihrem Gerät unbekannten SSH-Server aufbauen und den Ihnen als Sicherheitsabfrage angezeigten Schlüssel des entfernten Systems akzeptieren.

Jeder Schlüssel ist in dieser Datei in einer Zeile gespeichert und enthält drei Felder:

- Der Name oder die IP-Adresse des entfernten Systems, so wie es beim Aufbau der Verbindung im SSH-Befehl eingegeben wird.
- Der Typ des Schlüssels, also ssh-rsa oder ssh-dss.
- Die binäre Ausgabe des Schlüssels selbst, kodiert als Base64.

Sobald ein Administrator den öffentlichen Schlüssel eines SSH-Servers akzeptiert hat, gilt dieser Eintrag auch für alle übrigen Administratoren; es findet keine benutzerbezogene Unterscheidung statt.

Die hier benannte(n) Datei(en) sind auf dem Gerät ausschließlich für den Root-Administrator über SCP (siehe *Datei laden über einen SCP-Client* auf Seite 97) zugänglich. Das Hoch- und Herunterladen über LANconfig oder WEBconfig ist nicht möglich.

2.15.4.2 Bekannte SSH-Serverschlüssel manuell entfernen

Sie haben die Möglichkeit, Ihrem Gerät bekannte SSH-Schlüssel externer Systeme gezielt zu entfernen. Dies ist z. B. dann notwendig, wenn sich der SSH-Schlüssel des externen Servers geändert hat und Ihr Gerät die Verbindung zu diesem

System aufgrund eines ihm bereits vorliegenden SSH-Schlüssels verweigert. Dazu verwenden Sie den `sshkeygen`-Befehl im Zusammenhang mit dem Parameter `-R`:

```
sshkeygen [-h] [-q] [-t dsa|rsa|ecdsa|ed25519|ed448] [-R <Hostname>]
```

-?, -h

Zeigt eine kurze Hilfe der möglichen Parameter.

-t (dsa|rsa|ecdsa|ed25519|ed448)

Dieser optionale Parameter bestimmt den Typ des Schlüssels, den das Gerät löscht. Wenn Sie keinen Typ angeben, löscht das Kommando alle SSH-Schlüssel des angegebenen Hosts.

-R <Host>

Über diesen Parameter benennen Sie die IP-Adresse oder den DNS-Namen des externen Systems, dessen SSH-Schlüssel Sie gezielt von Ihrem Gerät löschen wollen.

Um die komplette Liste aller bekannten SSH-Serverschlüssel auf einmal zu löschen, entfernen Sie die Datei **ssh_known_hosts** aus dem Dateisystem Ihres Gerätes.

2.15.5 Schlüssel für den SSH-Client im LCOS erzeugen

Die Erzeugung eines Schlüsselpaares – bestehend aus einem öffentlichen und einem privaten Schlüssel – starten Sie an der Konsole des Gerätes, dessen LCOS-internen SSH-Client Sie nutzen wollen, mit folgendem Befehl:

```
sshkeygen [-h] [-q] [-t dsa|rsa|ecdsa|ed25519|ed448] [-b <bits>] [-f <Dateiname>]
```

Eine detaillierte Beschreibung der Parameter im `sshkeygen`-Befehl finden Sie im Abschnitt *SSH-Schlüsselerzeugung unter LCOS* auf Seite 114. Das Gerät legt die Schlüssel im PEM-Format automatisch unter dem Dateinamen **ssh_rsakey** (für RSA-Schlüssel), **ssh_dsakey** (für DSA- bzw. DSS-Schlüssel) oder **ssh_ecdsakey** (für ECDSA-Schlüssel) in seinem internen Dateisystem ab. Die ID-Dateien entsprechenden dem folgenden Aufbau, der die Nutzung eines Schlüssels für einen bestimmten LCOS-Administrator definiert:

```
*** User <MyAdmin>
<SSH-Key>
*** End
```

Öffentlichen Schlüssel abrufen

Nachdem das Gerät das Schlüsselpaar erzeugt hat, müssen Sie den öffentlichen Teil auf das entfernte System übertragen. Den öffentlichen Teil des Schlüssels rufen Sie mit dem folgenden Befehl ab:

```
show ssh idkeys
```

Diese Befehl erzeugt eine Ausgabe ähnlich der folgenden:

```
Configured Client-Side SSH Host Keys For User 'root':
ssh-rsa AAAAB3NzaC1yc2EAAAABEQAAAQEA28BtnFFInAi8I5B1aOwq5g2Y…0nkuNQ== root@
```

- Der erste Teil zeigt den Typ des Schlüssels (ssh-rsa oder ssh-dss).
- Der zweite Teil ist die binäre Ausgabe des Schlüssels selbst, kodiert als Base64.
- Der dritte Teil enthält den Hostnamen, der mehr als Kommentar gedacht ist.

Öffentlichen Schlüssel auf ein entferntes System übertragen

Sofern es sich bei dem entfernten System um ein Gerät mit LCOS handelt, laden Sie den betreffenden DSA- oder RSA-Schlüssel entweder über das *Dateimanagement* ins Gerät oder ergänzen die Liste der öffentlichen Schlüssel in WEBconfig über den Menüpunkt **Extras** > **Liste erlaubter öffentlicher SSH-Schlüssel bearbeiten** direkt. Kopieren Sie dazu den ersten und zweiten Teil und ersetzen Sie den dritten Teil mit einer Liste von Anwendern, um die Nutzung dieses Schlüssels auf einen Teil der LCOS-Administratoren einzugrenzen.

Weitere Informationen zur geforderten Syntax eines öffentlichen Schlüssels, dem Einsatz unterschiedlicher Schlüssel und deren Verknüpfung mit unterschiedlichen Administratoren finden Sie im Abschnitt *Syntax und Benutzer öffentlicher Schlüssel anpassen* auf Seite 118.

2.15.6 Prioritäten für die SSH-Authentifizierung

Die Reihenfolge der SSH-Authentifizierung an einem entfernten System folgt einer festen Prioritätenfolge:

1. Als erste Methode versucht Ihr Gerät immer die Authentifizierung über einen öffentlichen Schlüssel; es sei denn, das entfernte System unterstützt diese Methode nicht oder der sich anmeldende Administrator besitzt keinen öffentlichen Schlüssel.
2. Als zweite Methode verwendet Ihr Gerät die interaktive Authentifizierung über die Tastatur, wenn die Authentifizierung über öffentliche Schlüssel prinzipiell nicht verwendet werden kann oder wenn das entfernte System alle öffentlichen Schlüssel des sich anmeldenden Administrators abgelehnt hat. Die interaktive Authentifizierung kann je nach Anwendung aus dem Austausch mehrerer Nachrichten zwischen SSH-Client und SSH-Server bestehen; im einfachsten Fall z. B. reicht die Eingabe eines gültigen Zugangspassworts aus.

2.15.7 Berechtigung zur Nutzung des SSH- / Telnet-Clients

Sie haben die Möglichkeit, das Recht zur Nutzung des SSH- / Telnet-Clients für jeden einzelnen Administrator explizit zu vergeben. Dazu setzen Sie beim Hinzufügen oder Bearbeiten von Administratorkonten (in LANconfig unter **Management** > **Admin** > **Weitere Administratoren**) das Funktionsrecht **SSH-Client**. Ohne dieses Funktionsrecht kann sich ein Administrator nicht zu einem anderen SSH- / Telnet-Gerät weiterverbinden.

2.16 Dateiimport auf der Konsole per Copy&Paste

Ihr Gerät unterstützt das Laden von Dateien in Datei-Slots sowohl von der Konsole als auch aus einem Skript.

Somit können Dateien komfortabel per Skript zusammen mit der Konfiguration ausgerollt oder z. B. SSH-Schlüssel und VPN-Zertifikate importiert werden.

- Das entsprechende Dateiformat muss vom Typ Text bzw. ASCII sein, Binärformate werden nicht unterstützt.
- Bei Zertifikaten muss das Dateiformat entsprechend PEM-codiert (ASCII / Base64) sein. DER-codierte Zertifikate werden nicht unterstützt.
- Eine **Liste der möglichen Dateien und Formate** erhalten Sie am Ende dieses Kapitels.

Syntax des CLI-Befehls **importfile**:

importfile -a <application> [-p <passphrase>] [-n] [-h <Hash> -f <Fingerprint>] [-c] [-r]

Notwendige Parameter:

-a <application>

<application> bestimmt den Speicherort und somit die Nutzung für die eingegebenen Daten. Für eine vollständige Liste der in Ihrem Gerät vorhandenen Speicherorte geben Sie **importfile -?** ein.

Optionale Parameter:

-n

-n startet den nicht-interaktiven Modus. Es gibt keine Eingabeaufforderungen oder andere Ausgaben auf der CLI. Der nicht-interaktive Modus ist für die Nutzung in Skripten vorgesehen.

-p <passphrase>

<passphrase> ist das Passwort, was zum Entschlüsseln eines eingegebenen privaten Schlüssels benötigt wird.

-h <hash>

Der Hash-Algorithmus, mit dem der Fingerprint des Root-CA-Zertifikats ermittelt wurde.

-f <fingerprint>

Der Fingerprint des Root-CA-Zertifikats, erstellt mit **–h**. Der Fingerprint kann sowohl mit Doppelpunkten eingegebenen werden, als auch ohne.

-c

Es werden nur CA-Zertifikate hochgeladen.

-r

Hochgeladene CA-Zertifikate ersetzen bereits vorhandene.

Mit STRG + Z kann eine aktive Eingabe abgebrochen werden.

Beispiel:

In diesem Beispiel ist die Eingabe des Benutzers in **`Fett`** dargestellt und Eingabeaufforderungen für den Benutzer in *`Kursiv`*. Zertifikate und weitere lange, mehrzeilige Ausgaben werden zur Übersichtlichkeit mit **[...]** abgekürzt. Am Ende des Beispiels finden Sie die Erläuterungen zu den einzelnen Schritten.

```
root@test:/
    i m p o r t f i l e     - a     V P N 2     - p     l a n c o m     - h     S H A 5 1 2     - f
4F:A7:5E:C9:D4:77:CE:D3:06:4C:79:93:D8:FA:3A:8E:7B:FE:19:61:B2:0C:37:4F:BB:7A:E6:46:36:04:46:EE:F6:DA:97:15:6B:BB:
2D:8F:B6:66:E6:7C:54:1E:B4:02:79:54:D6:DF:1E:9B:27:7C:9C:EA:B8:CB:1B:6D:90:1C

The input can be aborted by pressing CTRL+Z.
Please enter the PEM-encoded (Base64) device certificate, the end of the input will be detected automatically:
importfile>-----BEGIN CERTIFICATE-----
importfile>MIID9DCCAtwCCQDgaoWRCmWaLjANBgkqhkiG9w0BAQ0FADAkMQswCQYDVQQG[…]
importfile>[…]s7pM5l0L0d0=
importfile>-----END CERTIFICATE-----
Importing device certificate:
        Version: 1 (0x0)
        Serial Number:
            e0:6a:85:91:0a:65:9a:2e
    Signature Algorithm: sha512WithRSAEncryption
        Issuer: CN=OCSP-TEST-CA,C=DE
        Validity
            Not Before: Jul  4 12:34:07 2017 GMT
            Not After : Oct  5 12:34:07 2024 GMT
        Subject: CN=TEST,O=Internet Widgits Pty Ltd,ST=Some-State,C=DE
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (4096 bit)
                Modulus:
                    00:bb:93:f6:b9:9a:41:b2:3e:30:2b:09:7f:d1:f9:
                    49:54:5a:82:c9:17:10:1f:79:6d:ab:55:df:b8[…]
                […]2f:0c:8a:69:7b:a9:82:32:f3:ca:9c:02:20:14:
                    bd:8b:0d
                Exponent: 65537 (0x10001)
    Signature Algorithm: sha512WithRSAEncryption
         06:5b:a4:1a:a2:69:c1:bf:6f:b1:d2:6c:b0:21:e1:10:43:[…]
         […]50:e6:a3:1d:f3:15:b7:87:8c:65:2f:25:f6:b3:ba:4c:e6:
         5d:0b:d1:dd

The input can be aborted by pressing CTRL+Z.
Please enter the PEM-encoded (Base64) device private key, the end the input will be detected automatically:
importfile>-----BEGIN RSA PRIVATE KEY-----
importfile>Proc-Type: 4,ENCRYPTED
importfile>DEK-Info: AES-128-CBC,8FB95ED0568DA9AE17D7573BC294ACD8
importfile>[…]5Cuf2p798Obhw3isAe04XRwmdLno8ZcPDyB33ZKPjmhUzB0WsdzGdSSq5iYjD
importfile>-----END RSA PRIVATE KEY-----
The private key was read successfully.
The private key matches the device certificate.
The input can be aborted by pressing CTRL+Z.
Please enter the chain of PEM-encoded (Base64) CA certificates.
The input is closed with "endcachain":
importfile>-----BEGIN CERTIFICATE-----
importfile>MIIDGzCCAgOgAwIBAgIJAMlNxBFGQqpoMA0GCSqGSIb3DQEBDQUAMCQxCzAJB[…]
importfile>[…]EUDI9giYt9tnAT8hJfLkkyN/PHSiP+e+vopjSpKuyg==
importfile>-----END CERTIFICATE-----
importfile>endcachain
```

```
Importing CA certificate:
        Version: 3 (0x2)
        Serial Number:
            c9:4d:c4:11:46:42:aa:68
    Signature Algorithm: sha512WithRSAEncryption
        Issuer: CN=OCSP-TEST-CA,C=DE
        Validity
            Not Before: Jun  6 13:56:49 2017 GMT
            Not After : Jun 19 13:56:49 2045 GMT
        Subject: CN=OCSP-TEST-CA,C=DE
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:e9:ba:04:74:7d:78:5a:84:b3:63:cc:ad:4d:[…]
                    […]14:0e:27:c8:8c:5a:00:a3:4c:ed:4f:02:e8:0b:
                    fb:07
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                57:13:BB:94:3B:89:C5:3B:B7:A0:0E:BB:BF:39:05:67:8B:FB:84:30
            X509v3 Authority Key Identifier:
                keyid:57:13:BB:94:3B:89:C5:3B:B7:A0:0E:BB:BF:39:05:67:8B:FB:84:30

            X509v3 Basic Constraints:
                CA:TRUE
    Signature Algorithm: sha512WithRSAEncryption
         c8:cf:3b:97:1a:56:61:13:9c:61:ed:21:23:7a:37:b4:a8:[…]
        […]3f:21:25:f2:e4:93:23:7f:3c:74:a2:3f:e7:be:be:8a:63:
         4a:92:ae:ca

Content of the PKCS12 file: private key: 1, device certificate: 1, CA certificates: 1
root@test:/
```

1. Es wird der Befehl importfile für den Speicherplatz VPN2 aufgerufen, somit handelt es sich um ein Zertifikat für die Nutzung im VPN. Das Passwort für den privaten Schlüssel ist lancom und das Root-CA-Zertifikat kann mit SHA512 und dem angegebenen Fingerprint geprüft werden.
2. Es folgt die Aufforderung an den Benutzer das Zertifikat einzugeben.
3. Nach Eingabe des Zertifikats wird dieses importiert.
4. Es folgt die Aufforderung an den Benutzer den privaten Schlüssel einzugeben.
5. Nach der Eingabe wird der Schlüssel geprüft.
6. Es folgt die Aufforderung an den Benutzer die Kette der CA-Zertifikate einzugeben. Das Ende der Eingabe wird nicht automatisch erkannt. Nach dem letzten Zertifikat muss das Ende über die Eingabe von endcachain ausgelöst werden. Geben Sie den Befehl in einer neuen Zeile ein, da alle Eingaben innerhalb der Zeile, welche die Zeichenfolge **endcachain** enthält, verworfen werden.
7. Nach der Eingabe werden die CA-Zertifikate importiert und der Vorgang abgeschlossen.

Tabelle 15: Mögliche Dateien & Formate

Datei	Format	Datei	Format
CONFIG-SYNC	PEM	SCEP-TLS	PEM
CWMP	PEM	SIPS1	PEM
CWMP-ROOT-CA	PEM	SIPS2	PEM
DEFAULT	PEM	SIPS3	PEM
DEFAULT-ADD-CAS	PEM	SSH-AUTH-KEYS	TEXT
EAP-TLS	PEM	SSH-DSA	PEM
ISSUE	TEXT	SSH-ECDSA	PEM
LBS	PEM	SSH-ED25519	PEM
OCSP-SERVER	PEM	SSH-ED448	PEM
PBSPOT-TEMPLATE-AGB	TEXT	SSH-KNOWN-HOSTS	TEXT

Datei	Format	Datei	Format
PBSPOT-TEMPLATE-ERROR	TEXT	SSH-RSA	PEM
PBSPOT-TEMPLATE-HELP	TEXT	TLS	PEM
PBSPOT-TEMPLATE-LOGIN	TEXT	USER-WIZARD-1	TEXT
PBSPOT-TEMPLATE-LOGIN-EMAIL	TEXT	USER-WIZARD-2	TEXT
PBSPOT-TEMPLATE-LOGIN-SMS	TEXT	USER-WIZARD-3	TEXT
PBSPOT-TEMPLATE-LOGOFF	TEXT	USER-WIZARD-4	TEXT
PBSPOT-TEMPLATE-NOPROXY	TEXT	VCM-TLS	PEM
PBSPOT-TEMPLATE-REG-EMAIL	TEXT	VPN-ADD-CAS	PEM
PBSPOT-TEMPLATE-REG-SMS	TEXT	VPN1	PEM
PBSPOT-TEMPLATE-START	TEXT	VPN2	PEM
PBSPOT-TEMPLATE-STATUS	TEXT	VPN3	PEM
PBSPOT-TEMPLATE-VOUCHER	TEXT	VPN4	PEM
PBSPOT-TEMPLATE-WELCOME	TEXT	VPN5	PEM
PROVISIONING-SERVER	PEM	VPN6	PEM
RADIUS-ACCOUNT-TOTAL	TEXT	VPN7	PEM
RADSEC	PEM	VPN8	PEM
ROLLOUT-TEMPLATE	TEXT	VPN9	PEM
ROLLOUT-WIZARD	TEXT	WLC-SCRIPT1	TEXT
SCEP-CA	PEM	WLC-SCRIPT2	TEXT
SCEP-RA	PEM	WLC-SCRIPT3	TEXT
Wireless-ePaper	PEM		

2.17 Basic HTTP Fileserver für externe Speichermedien

2.17.1 Einleitung

Der eingebaute HTTP-Server in LCOS bietet Ihnen die Möglichkeit, Dateien von einem USB-Speichermedium über das HTTP-Protokoll bereitzustellen und arbeitet so als einfacher Dateiserver.

Diese Funktion wird ausschließlich von Geräten mit USB-Anschluss unterstützt.

2.17.2 Vorbereitung des USB-Speichermediums

Bevor Sie von Ihrem Gerät auf ein externes Speichermedium zugreifen können, müssen Sie einige Vorbereitungen treffen. Der nachfolgende Abschnitt beschreibt, wie Sie ein USB-Medium für den Einsatz am Gerät einrichten.

1. Formatieren Sie das USB-Medium mit einem FAT16- oder FAT32-Dateisystem.
2. Erstellen Sie auf dem USB-Medium das Verzeichnis `public_html`.

   Der HTTP-Server von LCOS greift nur auf Dateien in diesem Verzeichnis und den evtl. vorhandenen Unterverzeichnissen zu. Alle anderen Dateien auf dem USB-Medium werden ignoriert.

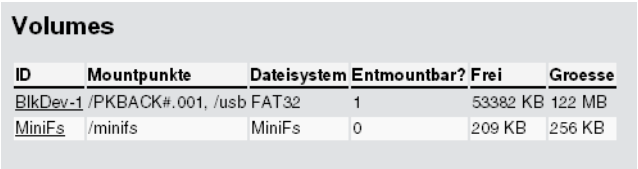
Sie können den Namen des Verzeichnisses im Setup-Menü auch ändern unter **HTTP** > **Datei-Server** > **Oeffentliches-Unterverzeichnis**.

Die Vorbereitung des USB-Mediums ist damit abgeschlossen.

2.17.3 Einhängepunkt des USB-Mediums im LCOS ermitteln

Beim Anschließen eines USB-Mediums erzeugt Ihr Gerät automatisch einen Einhängepunkt, der von LCOS zur internen Verwaltung des Mediums verwendet wird. Dieser Einhängepunkt bleibt für ein bestimmtes USB-Medium immer gleich, auch nach einem Neustart. Verschiedenen Medien wird jeweils ein eigener, eindeutiger Einhängepunkt zugewiesen.

Um auf die Daten des USB-Mediums zugreifen zu können, muss der zugehörige Einhängepunkt bekannt sein. Den Einhängepunkt der USB-Medien ermitteln Sie über das Status-Menü unter **Dateisystem** > **Volumes**.



Die Status-Tabelle zeigt alle Datenträger (Volumes), die dem Gerät bekannt sind:

- `MiniFs` ist das eingebaute Flash-Dateisystem, das es auf fast allen Geräten gibt.
- `BlkDev-n` bezeichnen die bekannten USB-Medien. Wenn nur ein USB-Massenspeichergerät angeschlossen ist, wird es `BlkDev-1` genannt und unter `/usb` eingehangen.

2.17.4 Zugriff auf die Dateien eines USB-Mediums

Um auf die Dateien auf dem USB-Medium über den HTTP-Server im LCOS zuzugreifen, verwenden Sie die folgende URL:

```
http://<Device-IP-Address>/filesrv/<Mounting-Point>/<File>
```

Wenn z. B. eine Datei `coupon.jpeg` benannt ist und auf dem einzigen USB-Medium im Basisverzeichnis unter `\public_html` gespeichert ist, dann können Sie mit folgendem Link darauf zugreifen:

```
http://<Device-IP-Address>/filesrv/usb/coupon.jpeg
```

Der Zugriff kann auch über HTTPS anstatt HTTP erfolgen.

2.17.5 Regeln für den Verzeichniszugriff

Das Verzeichnis `\public_html` darf Unterverzeichnisse beinhalten. Sie haben die Möglichkeit, auf diese Verzeichnisse zuzugreifen, ohne eine darin enthaltene Datei anzugeben. Wenn in einem Verzeichnis eine Datei mit dem Namen `index.html` oder `index.htm` existiert, dann wird diese zum HTTP-Client übertragen. Andernfalls gibt der Fileserver eine Liste aller Dateien und Verzeichnisse aus, die im aufgerufenen Verzeichnis existieren.

2.17.6 Unterstützte Inhaltstypen

Der HTTP-Server im LCOS nutzt die Dateierweiterung, um den MIME-Inhaltstyp zu bestimmen, der für die korrekte Darstellung der Inhalte im Browser benötigt wird. Momentan sind die folgenden Erweiterungen bekannt und werden in einen korrekten MIME-Inhaltstyp übersetzt:

- .htm und .html für HTML-Dateien
- .gif, .jpg, .jpeg, .png, .bmp, .pcx für entsprechende Formate der Bilddateien
- .ico für Icon-Dateien

- .pdf für Adobe Acrobat PDF-Dateien
- .css für Cascading-Style-Sheet-Dateien

2.18 Rollout-Assistent

In größeren Projekten zur Vernetzung richten die Administratoren eines Unternehmens oft zahlreiche Geräte vom gleichen oder ähnlichen Typ an unterschiedlichen Standorten ein. Um die persönliche Anwesenheit an den jeweiligen Standorten zu reduzieren oder ganz zu vermeiden, führen Administoren oft einen sogenannten Rollout durch. Ein „Rollout" bezeichnet im Netzwerkumfeld einen weitgehend automatisiert ablaufenden Vorgang, der dazu dient, ein Gerät auf eine standardisierte Weise für den geplanten Einsatzzweck vorzukonfigurieren. Dabei stehen den Administratoren zwei grundlegende Möglichkeiten zur Verfügung:

1. Die Administratoren bereiten die Geräte in ihrer Zentrale lokal für den Rollout vor. Am Einsatzort führt ein Mitarbeiter oder ein Kunde dann einen speziell angepassten (benutzerdefinierten) Rollout-Assistenten aus, über den er die standortbezogenen Teile der Konfiguration ergänzt und das Gerät in den gewünschten Betriebszustand bringt.
2. Die Administratoren setzen in ihrer Zentrale *Large Scale Rollout & Management (LSR)* ein. Sämtliche Konfigurationseinstellungen für ein bestimmtes Gerät werden über das Management-System vorgenommen und verwaltet. Am Einsatzort führt ein Mitarbeiter oder ein Kunde dann den standardmäßig im Gerät vorhandenen (Default-)Rollout-Assistenten aus und lädt die Konfiguration vom LSR-Server, um das Gerät in den gewünschten Betriebszustand zu bringen.

Im Unterschied zum benutzerdefinierten Rollout-Assistenten ist es bei Verwendung des Default-Rollout-Wizards zusammen mit LSR also nicht erforderlich, die Konfiguration eines Gerätes in mehreren Etappen durchzuführen; das Einspielen einer aktuellen Komplettkonfiguration kann nach dem Anschluss des Gerätes unmittelbar durch das LSR erfolgen.

Sofern LSR jedoch nicht zum Einsatz kommen kann oder soll, haben Sie als Administrator mit dem benutzerdefinierten Rollout-Assistenten auch weiterhin die Möglichkeit, einen eigenen Assistenten mit beliebig komplexem Umfang für spezielle Aufgaben in das Gerät zu implementieren.

Ein Parallelbetrieb beider Assistenten ist ausgeschlossen. Die Einrichtung benutzerdefinierter Rollout-Assistenten ersetzt den Default-Rollout-Wizard; die Fernkonfiguration durch ein LSR-System ist dann nicht mehr möglich. Um wieder zum Default-Rollout-Wizard zurückzukehren, müssen Sie den benutzerdefinierten Rollout-Assistenten aus dem Dateisystem des Gerätes löschen.

2.18.1 Default-Rollout-Assistent

Ihr Gerät beinhaltet standardmäßig einen vorkonfigurierten Rollout-Assistenten, welcher es Ihnen ermöglicht, mit wenigen Klicks von einem *Large Scale Rollout & Management (LSR)*-Server eine Konfigurationen zu beziehen. Dieser **Default-Rollout-Assistent** erscheint immer dann, wenn Sie den Rollout-Assistenten im LCOS aktiviert und keinen benutzerdefinierten Rollout-Assistenten eingerichtet haben.

Beim Aufruf des Default-Rollout-Assistenten fragt der Assistent alle Informationen ab, die er für einen erfolgreichen Verbindungsaufbau zum LSR benötigt. Hierzu gehören:

- das für den Verbindungsaufbau verwendete Protokoll (HTTP oder HTTPS);
- die IP-Adresse oder den DNS-Namen des LSR-Servers;
- den Benutzernamen und das Passwort für die Authentisierung am LSR;
- der Name oder die Nummer des Rollout-Projektes;
- die Geräte-ID (optional); sowie
- die zum Gerät gehörende Rollout-TAN.

Dieser Prozess lässt sich auch teilweise bis vollständig automatisieren, indem Sie die betreffenden Angaben dauerhaft im Gerät hinterlegen. Die dazugehörige Tabelle finden Sie im Setup-Menü unter **HTTP** >

Rollout-Wizard > **Vorbelegungen**. Standardmäßige Vorbelegungen sind der vom Assistenten verwendete Port sowie die Loopback-Adresse.

Sofern Ihr Gerät über einen USB-Anschluss verfügt, lässt sich dessen automatische Ladefunktion auch dafür nutzen, um ein beliebiges unkonfiguriertes Gerät per USB-Stick mit den relevanten Basisinformationen für den Rollout-Wizard zu versorgen. Mehr Informationen zu der Funktion erhalten Sie unter *Automatisches Laden von Firmware oder Konfiguration über USB* auf Seite 106.

Bevor das Gerät mit dem Rollout-Vorgang beginnt, zeigt Ihnen der Assistent die verwendeten Verbindungsdaten in einer Zusammenfassung noch einmal an. Außerdem überprüft das Gerät mit einem ICMP Echo Request (Ping), ob der angegebene Server erreichbar ist. Schlägt diese Prüfung fehl, haben Sie die Möglichkeit, den Assistenten neu zu konfigurieren oder den Rollout-Vorgang trotzdem fortzusetzen. Ist der angegebene Host erreichbar, beginnt das Gerät im weiteren Verlauf damit, seine Zielkonfiguration beim LSR abzufragen.

Sofern der LSR-Server über das Internet erreichbar ist, Sie den Rollout-Wizard aber auf einem Gerät ausführen, auf dem noch keine Internet-Verbindung eingerichtet ist, müssen Sie zunächst den Einrichtungsassistenten für das Internet durchlaufen.

2.18.2 Benutzerdefinierter Rollout-Assistent

Der benutzerdefinierte Rollout-Assistent ist ein individuell programmierbarer Setup-Assistent in WEBconfig, der es Ihnen als ausrollender Administrator erlaubt, einen auf Ihre Kunden oder andere (z. B. beschränkte) Administratoren abgestimmten Konfigurationsassistenten zu implementieren. Dazu bedienen Sie sich einer speziellen Beschreibungssprache, mit der sich auch sehr komplexe Assistenten definieren lassen.

Ein solcher benutzerdefinierter Assistent unterstützt folgende Funktionen:

- Definition von beliebigen internen Variablen
- Bedingte Verzweigungen
- Bedingte Sprunganweisungen zu beliebigen URL
- Bedingte Anzeige von Hinweisen
- Ausführen von allen (nicht interaktiven) Aktionen, die in der LCOS-Konsole zur Verfügung stehen
- Auslesen von aktuellen Werten aus der Konfiguration des Gerätes
- Schreiben von neuen Werten in die Konfiguration des Gerätes
- Statusprüfungen, wie z. B. Prüfen der Uhrzeit im Gerät
- Verbindungsprüfungen, wie z. B. die erfolgreiche VPN-Verbindung zu einer bestimmten Gegenstelle

Sie erstellen den neuen Assistenten nach den Regeln der Beschreibungssprache in Form einer Text-Datei, die Sie anschließend in das Gerät laden. Der Anwender am Einsatzort kann den benutzerdefinierten Assistenten dann unter WEBconfig über den gewählten Namen ausführen.

Sie können bestimmte Administrator-Accounts gezielt auf die Ausführung des Rollout-Assistenten beschränken und so auch ungeübten Anwendern die Konfiguration bestimmter Funktionen ermöglichen, ohne einen kompletten Konfigurationszugriff zu erlauben.

2.18.2.1 Struktur des benutzerdefinierten Assistenten

Die Beschreibung eines benutzerdefinierten Assistenten besteht aus den folgenden Abschnitten:

- String-Tabellen mit den benötigten Texten in Deutsch und Englisch.
- Eine Definition des Assistenten.
- Beliebig viele Sektionen zur Beschreibung der einzelnen HTML-Seiten, die der Assistent anzeigen kann.
- Ein Initialisierungs-Bereich, der die Aktionen beim Starten des Assistenten definiert.
- Ein abschließender Bereich, der die Aktionen beim Beenden des Assistenten definiert.

Beachten Sie für die Beschreibung des Assistenten die folgenden Konventionen:

- Die Elemente der Beschreibung folgen genau der oben genannten Struktur.
- Die Textdatei mit der Beschreibung ist nach ISO 8859-1 kodiert.
- Kommentare beginnen mit einem Semikolon und dienen nur der Lesbarkeit der Beschreibung.
- Interne Variablen beginnen mit dem Schlüsselwort `wizard.` (inklusive des Punktes) und speichern Informationen für die interne Vearbeitung des Assistenten.
- Konfigurationsvariablen beginnen mit dem Schlüsselwort `config.` (inklusive des Punktes) und lesen Informationen aus der aktuellen Gerätekonfiguration aus oder schreiben Werte in die aktuelle Konfiguration hinein. Geben Sie die Konfigurationsvariablen in einer der folgenden Schreibweisen an:
  - Dedizierte Parameter der Konfiguration referenzieren Sie über `config.1.<SNMP-ID>`, also z. B. `config.1.2.1` für den Zugriff auf den Namen des Gerätes (auf der Konsole unter **Setup** > **Name**).

    Die SNMP-ID zu einem Parameter der Konfiguration ermitteln Sie z. B. mit dem Befehl `ls -a` an der Konsole in dem entsprechenden Untermenü.
  - Die Werte in einer Tabelle referenzieren Sie über:
    ```
    config.1.<SNMP-ID>.<Zeile>.ID:<Spalte>
    ```
    Beispiel für den Wert in der ersten Zeile und der Spalte mit der ID '2' in der Routing-Tabelle '1.2.8.2':
    ```
    config.1.2.8.2.1.ID:2
    ```
  - Wenn Ihnen die ID der Spalte nicht bekannt ist, referenzieren Sie die Werte in einer Tabelle alternativ über:
    ```
    config.1.<SNMP-ID>.<Zeile>.<Spalte>
    ```
    Beispiel für den Wert in der ersten Zeile und der zweiten Spalte:
    ```
    config.1.2.8.2.1.2
    ```
  - Wenn Ihnen die benötigte Zeile der Tabelle nicht bekannt ist, referenzieren Sie die Werte in einer Tabelle über einen bekannten Wert in der ersten Spalte mit:
    ```
    config.<SNMP-ID>."<Bekannter-Wert>".ID:<Spalte>
    ```
    Beispiel für den Wert der Spalte mit der ID '2' von genau der Zeile, die in der ersten Spalte den Wert der Default-Route enthält:
    ```
    config.1.2.8.2."255.255.255.0".ID:2
    ```
    Enthält die Tabelle mehrere Zeilen mit dem gleichen Wert in der ersten Spalte, referenziert die Konfigurationsvariable die erste dieser Zeilen.
  - Wenn die benötigte Zeile der Tabelle erst bei der Ausführung des Assistenten durch eine Benutzereingabe definiert wird, referenzieren Sie den Wert in der Tabelle über die Verwendung einer Variablen mit:
    ```
    config.<SNMP-ID>.\"<Interne-Variable>\".ID:<Spalte>
    ```
    Beispiel für die Zeile, deren Wert in der ersten Spalte mit dem aktuellen Wert der internen Variablen wizard.target_network übereinstimmt:
    ```
    config.1.2.8.2."\wizard.target_network"\.ID:2
    ```
- Geräte-Variablen für Geräteeigenschaften beginnen mit dem Schlüsselwort `device.` (inklusive des Punktes) und lesen bestimmte Geräteeigenschaften aus dem Gerät aus. Weitere Informationen über die Geräte-Variablen finden Sie im Abschnitt *Geräte-Variablen für Geräteeigenschaften* auf Seite 140.

String-Tabellen

Die Beschreibung des benutzerdefinierten Assistenten basiert auf der Definition der zur Anzeige benötigten Texte in deutscher und englischer Sprache.

Die Zeile `stringtable "English"` leitet die englischen Texte ein, die Zeile `stringtable "Deutsch"` die deutschen Texte. Jede String-Definition besteht aus dem Schlüsselwort `string`, gefolgt vom Namen des Strings und dem in doppelte Hochkommata gesetzen Wert.

Das folgende Beispiel zeigt die String-Tabellen mit nur einem Eintrag:

```
; -String tables start-----------------------------------------------
   stringtable "English"
   string title_test, "Test wizard"
   stringtable "Deutsch"
   string title_test, "Test-Assistent"
; -String tables end-------------------------------------------------
```

Der Interpreter für die Beschreibung des benutzerdefinierten Assistenten im LCOS erwartet alle Texte zwingend mit einer deutschen und einer englischen Definition. LCOS führt den Assistenten nicht aus, wenn zu einem Eintrag in der englischen String-Tabelle kein gleichnamiger Eintrag in der deutschen String-Tabelle gefunden wird (oder umgekehrt).

Definition des Assistenten

Die Definition legt den Namen des Assistenten fest. Nach dem Schlüsselwort `wizard` folgt der interne Name in doppelten Hochkommata, gefolgt von der Referenz auf einen Eintrag der String-Tabelle (*String-Tabellen*). Der Assistent zeigt den mit diesem String definierten externen Namen bei der Ausführung in der HTML-Seite an:

```
; -Assistenten-Definition Start--------------------------
   wizard "Mein_Test-Assistent", title_test
; -Assistenten-Definition Ende---------------------------
```

Sektionen

Die Sektionen stellen die eigentlichen HTML-Seiten dar, die der Anwender während der Ausführung des Assistenten im Browser angezeigt bekommt.

Jede Sektion beginnt mit dem Schlüsselwort `section` und endet mit dem Beginn der nächsten Sektion. Die letzte Sektion endet mit dem Beginn des Bereiches `on-init`; die Sektionen enden also ohne ein explizites Schlüsselwort für das Ende.

Die Sektionen beinhalten die folgenden Elemente in beliebieger Reihenfolge und Menge:

- Bedingungen
- Optional: Eigene Bezeichnung für die Sektion, beginnend mit dem Schlüsselwort `label`, gefolgt von einer Zeichenkette aus Groß- und Kleinbuchstaben und dem Unterstrich ('_'):

  ```
  Label Mein_RolloutAssistent
  ```

  Die Beschreibung des Assistenten kann die eigene Bezeichnung (das Label) als Sprungziel nutzen.

- Statischer Text, beginnend mit dem Schlüsselwort `static_text`, gefolgt von einer Referenz auf einen Eintrag der *String-Tabelle*:

  ```
  static_text str.conf_general
  ```

- Felder für verschiedene Datentypen wie Text oder IP-Adresse: Eingabefelder, Kontrollkästchen, Optionsfelder, Auswahllisten etc.

  Hinweise zu den verfügbaren Feldern finden Sie im Abschnitt *Felder und Attribute* auf Seite 136.

- Aktionen, die der Assistent je nach Schlüsselwort zu Beginn des Blocks in unterschiedlichen Situationen ausführt:
  - `on_show`: Der Assistent führt die Aktionen in diesem Block aus, bevor eine Sektion (HTML-Seite) angezeigt wird.
  - `on_skip`: Der Assistent führt die Aktionen in diesem Block aus, wenn eine Sektion (HTML-Seite) aufgrund der darin enthaltenen Bedingungen nicht angezeigt wird.
  - `on_next`: Der Assistent führt die Aktionen in diesem Block aus, wenn der Benutzer die Schaltfläche **Weiter** in der Sektion (HTML-Seite) klickt.

- `on_back`: Der Assistent führt die Aktionen in diesem Block aus, wenn der Benutzer die Schaltfläche **Zurück** in der Sektion (HTML-Seite) klickt.

Hinweise zum Aufbau der Blöcke mit den Aktionen und den darin verfügbaren Elementen finden Sie im Abschnitt *Aktionen* auf Seite 141.

Bedingungen

Die Beschreibung des Assistenten kann alle Elemente einer Sektion mit Bedingungen versehen. Über eine Bedingung lässt sich die ausgegebene HTML-Seite kontextabhängig verändern, indem bestimmte Konfigurationsmöglichkeiten in Abhängigkeit der zuvor getätigten Einstellungen ein- oder ausgeblendet werden.

Die Bedingungen beziehen sich dabei immer auf das vorhergehende Element und bestehen aus der Angabe einer Klasse und einem oder mehreren Bedingungsmustern. Ein Muster wiederum besteht aus zwei Operanden und einem Operator. Hierbei gilt:

- Wenn eine Bedingung mehrere Bedingungsmuster in einer Zeile enthält, wertet der Assistent diesen Ausdruck als ODER-Verknüpfung.
- Wenn die Beschreibung mehrere Bedingungen in separaten Zeilen zu einem übergeordneten Element enthält, wertet der Assistent diesen Ausdruck als UND-Verknüpfung.

Eine Klasse darf beliebig viele Bedingungsmuster und ein Element beliebig viele Bedingungen enthalten. Die folgenden Bedingungen z. B. zeigen die Sektion nur dann an, wenn die interne Variable `wizard.test_select1` gleich `1`, und `wizard.test_select4` oder `wizard.test_select5` gleich `0` sind:

```
section
only_if wizard.test_select1, "1", equal
only_if wizard.test_select4, "0", equal, wizard.test_select5, "0", equal
```

Klassen

Die Beschreibung kann die folgenden Klassen enthalten:

- `only-if`: Das vorhergehende Element wird nur ausgeführt oder angezeigt, wenn mindestens eines der folgenden Bedingungsmuster erfüllt ist.
- `skip-if`: Das vorhergehende Element wird nicht ausgeführt oder angezeigt, wenn alle der folgenden Bedingungsmuster erfüllt sind.

Operanden

Das Bedingungsmuster kann folgende Operanden enthalten:

- Statische Texte
- Interne Variablen des Assistenten
- Variablen zur Referenzierung von Werten aus der aktuellen Konfiguration des Gerätes (Konfigurations-Variablen)
- Das Zeichen '*' als Platzhalter (Wildcard)

Operatoren

Das Bedingungsmuster kann folgende Operatoren enthalten:

- `equal`: Prüft, ob die beiden Operanden gleich sind.
- `exists`: Prüft, ob die angegebene Konfigurations-Variable gesetzt ist, also der Wert des Parameters in der Konfiguration nicht leer ist.
- `empty`: Prüft, ob der erste Operand leer ist. Der zweite Operand wird als Platzhalter (Wildcard) '*' angegeben.
- `contains`: Prüft, ob der erste Operand den zweiten Operanden enthält.
- `!`: Verneint die Bedingung.

Beispiele

Die folgende Bedingung zeigt die Sektion nur dann an, wenn die interne Variable 'wizard.test_select' gleich '0' ist.

```
section
only_if wizard.test_select, "0", equal
```

Die folgende Bedingung setzt die interne Variable 'wizard.intranet_name' auf den Wert 'INTRANET', wenn diese Variable bisher leer ist.

```
set wizard.intranet_name, "INTRANET"
only_if wizard.intranet_name, *, empty
```

Die folgende Bedingung setzt die interne Variable 'wizard.target_1' auf den Wert 'ZIEL_1', wenn die interne Variable 'wizard.select_target' entweder den Wert '1' oder den Wert '5' hat.

```
set wizard.target_1,"ZIEL_1"
only_if wizard.select_target,"1",equal,wizard.select_target,"5",equal
```

Felder und Attribute

Der Assistent verwendet Felder, um dem Benutzer Informationen anzuzeigen und ihm die Möglichkeit zur Eingabe von Informationen zu geben. Jedes Feld entspricht einer internen Variablen.

Der Assistent definiert ein Feld durch die Angabe des entsprechenden Schlüsselwortes, gefolgt von einer internen Variablen in der gleichen Zeile. In weiteren Zeilen folgen optional die Attribute für das Feld.

Ein Beispiel für eine Felddefinition im Assistenten:

```
selection_buttons select_inet
 description   str.inet_Selection
 button_text   str.inet_PPPoE, str.inet_IPoE
```

Dieses Feld erzeugt eine Gruppe von Optionsschaltflächen, von denen der Benutzer nur eine aktivieren kann. Der Assistent setzt den in der String-Tabelle definierten Text `str.inet_Selection` als Beschreibung neben das Feld. Für die Optionsschaltflächen selbst zeigt der Assistent die Texte `str.inet_PPPoE` und `str.inet_IPoE` an. Nach der Auswahl einer Option durch den Benutzer schreibt der Assistent den gewählten Wert in die interne Variable `wizard.select_inet`.

Folgende Felder können Sie im Assistenten verwenden:

`check_local_ip`

Dieses Feld prüft, ob der Assistent zuvor die IP-Adresse des Gerätes verändert hat und leitet den Benutzer auf die entsprechende HTML-Seite weiter. Mögliche Attribute:

- `destination`: Ziel für die Weiterleitung als FQDN oder IPv4-Adresse.
- `timeout`: Wartezeit vor der Weiterleitung.

`check_time`

Dieses Feld prüft, ob das Gerät über eine gültige Zeitinformation verfügt. Mögliche Attribute:

- `success_jump`: Label der Seite, die der Assistent bei erfolgreicher Prüfung öffnet.
- `fail_jump`: Label der Seite, die der Assistent bei nicht erfolgreicher Prüfung öffnet.
- `limit`: Maximale Anzahl der Prüfungen, bevor der Assistent die Prüfung als erfolglos ansieht. Setzen Sie das Limit auf den Wert '0', um die Prüfungen ohne Limit fortzusetzen.
- `timeout`: Wartezeit zwischen zwei Prüfungen.

`entryfield_hex`

Dieses Feld dient zur Eingabe von hexadezimalen Werten, z. B. MAC-Adressen. Mögliche Attribute:

- `description`: Beschreibung des Feldes in der HTML-Darstellung

- `max_len`: Maximale Anzahl der Zeichen, die der Benutzer in dieses Feld eintragen kann
- `never_empty`: Der Wert '1' für dieses Attribut kennzeichnet ein Feld, welches der Benutzer nicht freilassen darf.
- `add_to_charset`: Fügt zusätzliche Zeichen zum standardmäßig verwendeten Eingabezeichensatz hinzu.
- `default_value`: Standardwert

`entryfield_ipaddress`

Dieses Feld dient zur Eingabe von IPv4-Adressen. Mögliche Attribute:

- `description`: Beschreibung des Feldes in der HTML-Darstellung
- `never_empty`: Der Wert '1' für dieses Attribut kennzeichnet ein Feld, welches der Benutzer nicht freilassen darf.
- `never_zero`: Der Wert '1' für dieses Attribut kennzeichnet ein Feld, welches nicht den Wert '0' enthalten darf.
- `add_to_charset`: Fügt zusätzliche Zeichen zum standardmäßig verwendeten Eingabezeichensatz hinzu.
- `default_value`: Standardwert

`entryfield_numbers`

Dieses Feld dient zur Eingabe von Telefonnummern. Mögliche Attribute:

- `description`: Beschreibung des Feldes in der HTML-Darstellung
- `max_len`: Maximale Anzahl der Zeichen, die der Benutzer in dieses Feld eintragen kann
- `never_empty`: Der Wert '1' für dieses Attribut kennzeichnet ein Feld, welches der Benutzer nicht freilassen darf.
- `add_to_charset`: Fügt zusätzliche Zeichen zum standardmäßig verwendeten Eingabezeichensatz hinzu.
- `default_value`: Standardwert

`entryfield_numeric`

Dieses Feld dient zur Eingabe von Zahlen. Mögliche Attribute:

- `description`: Beschreibung des Feldes in der HTML-Darstellung
- `range_min`: Minimaler Wert, den der Benutzer in dieses Feld eintragen kann
- `range_max`: Maximaler Wert, den der Benutzer in dieses Feld eintragen kann
- `signed_value`: Ermöglicht die Angabe eines numerischen Wertes mit Vorzeichen
- `never_empty`: Der Wert '1' für dieses Attribut kennzeichnet ein Feld, welches der Benutzer nicht freilassen darf.
- `add_to_charset`: Fügt zusätzliche Zeichen zum standardmäßig verwendeten Eingabezeichensatz hinzu.
- `default_value`: Standardwert
- `unit`: Die Einheit des Wertes, welchen der Assistent in der HTML-Darstellung nach dem Eingabefeld anzeigt.

entryfield_text

Dieses Feld dient zur Eingabe von Texten. Mit dem Attribut `hidden` dient das Feld zur Eingabe von Passwörtern. Mögliche Attribute:

- `description`: Beschreibung des Feldes in der HTML-Darstellung
- `hidden`: Kennzeichnet ein Feld, in welches der Benutzer Kennwörter einträgt.
- `add_to_charset`: Fügt zusätzliche Zeichen zum standardmäßig verwendeten Eingabezeichensatz hinzu.
- `convert_to_upper`: Wandelt die Eingabe des Benutzers in Großbuchstaben um
- `max_len`: Maximale Anzahl der Zeichen, die der Benutzer in dieses Feld eintragen kann
- `min_len`: Minimale Anzahl der Zeichen, die der Benutzer in dieses Feld eintragen kann
- `never_empty`: Der Wert '1' für dieses Attribut kennzeichnet ein Feld, welches der Benutzer nicht freilassen darf.
- `unit`: Die Einheit des Wertes, welchen der Assistent in der HTML-Darstellung nach dem Eingabefeld anzeigt.

entryfield_textwithlist

Dieses Feld dient zur Eingabe von Texten. Außerdem kann der Benutzer aus einer Reihe von vordefinierten Werten auswählen. Mögliche Attribute:

- `description`: Beschreibung des Feldes in der HTML-Darstellung
- `default_value`: Standardwert
- `max_len`: Maximale Anzahl der Zeichen, die der Benutzer in dieses Feld eintragen kann
- `item_value`: Liste mit vordefinierten Werten, die der Benutzer für dieses Feld auswählen kann

onoff_switch

Dieses Feld erzeugt ein einfaches Kontrollkästchen. Mögliche Attribute:

- `description`: Beschreibung des Feldes in der HTML-Darstellung
- `value_list`: Liste der beiden Werte, welche das Kontrollkästchen annehmen kann
- `default_selection`: Standardwert

page_switch

Dieses Feld erzeugt einen Link, über den der Benutzer zu einer von mehreren anderen HTML-Seiten des Assistenten wechseln kann. Mögliche Attribute:

- `page_description`: Kommaseparierte Liste mit Text-Strings oder Referenzen auf Strings zur Beschreibung der möglichen Link-Ziele.
- `page_label`: Kommaseparierte Liste mit Seiten-Labels der möglichen Link-Ziele.
- `description`: Beschreibung des Feldes in der HTML-Darstellung

ping_barrier

Dieses Feld verzögert die weitere Ausführung des Assistenten, bis ein Ping zu dem verwendeten Ziel erfolgreich beantwortet wurde. Mögliche Attribute:

- `destination`: Zieladresse für den Ping.
- `loopback`: Loopback-Adresse, die der Ping anstelle der standardmäßigen Antwortadresse verwendet

- `success_jump`: Label der Seite, die der Assistent bei erfolgreichem Ping öffnet.
- `fail_jump`: Label der Seite, die der Assistent bei nicht erfolgreichem Ping öffnet.
- `limit`: Maximale Anzahl der Pings, bevor der Assistent die Prüfung als erfolglos ansieht. Setzen Sie das Limit auf den Wert '0', um die Pings ohne Limit fortzusetzen.
- `timeout`: Wartezeit zwischen zwei Pings.

`popup`

Dieses Feld öffnet die angegebene Zieladresse in einem Popup-Fenster.

Die Zieladresse kann Variablen enthalten (siehe *Variablen* auf Seite 139).

`readonly_text`

Dieses Feld erzeugt ein Feld ohne Eingabemöglichkeit. Der Assistent kann diese Felder nutzen, um Text anzuzeigen. Mit dem Attribut `hidden` kann der Assistent interne Variablen definieren. Mögliche Attribute:

- `description`: Beschreibung des Feldes in der HTML-Darstellung
- `unit`: Die Einheit des Wertes, welchen der Assistent in der HTML-Darstellung nach dem Eingabefeld
- `hidden`: Kennzeichnet ein verstecktes Feld.

`selection_buttons`

Dieses Feld erzeugt eine Gruppe von Optionsschaltflächen, von denen der Benutzer nur eine aktivieren kann. Mögliche Attribute:

- `description`: Beschreibung des Feldes in der HTML-Darstellung
- `button_text`: Kommaseparierte Liste mit Text-Strings oder Referenzen auf Strings zur Beschreibung der einzelnen Optionsschaltflächen.
- `button_value`: Kommaseparierte Liste mit Text-Strings mit den Werten der einzelnen Optionsschaltflächen.

`selection_list`

Dieses Feld erzeugt eine Auswahlliste (Drop-Down-Liste), aus welcher der Benutzer einen Wert auswählen kann. Mögliche Attribute:

- `description`: Beschreibung des Feldes in der HTML-Darstellung
- `item_text`: Kommaseparierte Liste mit Text-Strings oder Referenzen auf Strings zur Beschreibung der einzelnen Listeneinträge.
- `item_value`: Kommaseparierte Liste mit Text-Strings mit den Werten der einzelnen Listeneinträge.
- `default_selection`: Standardwert

`static_text`

Dieses Feld erzeugt einen statischen Text auf der HTML-Seite, der als Referenz auf einen Text-String dem Feldnamen folgt.

Variablen

In einigen Attributen der Felder sind Variablen einsetzbar, um den Wert des Attributs durch eine andere Zeichenkette zu ersetzen oder mit einer zusätzlichen Zeichenkette zu ergänzen. Dabei haben Sie die Wahl zwischen den internen Variablen des benutzerdefinierten Assistenten und den vordefinierten Umgebungsvariablen der Konsole, welche Sie über besondere Platzhalter einfügen.

Einfügen von Assistenten-Variablen

Um eine interne Variable in den Wert eines Attributs einzusetzen, verwenden Sie die Syntax `$(VariablenName)`. Um den Benutzernamen aus der internen Variablen `wizard.username` in eine URL einzusetzen, fügen Sie z. B. das folgende Attribut ein: `http://host/directory?param=$(username)`.

Einfügen von Umgebungsvariablen

Um eine Umgebungsvariable in den Wert eines Attributs einzusetzen, verwenden Sie die Syntax `%VariablenName`. Folgende Umgebungsvariablen lassen sich in den Attributen verwenden:

- `%` fügt ein Prozentzeichen ein.
- `f` fügt die Version und das Datum der aktuellen im Gerät aktiven Firmware ein.
- `r` fügt die Hardware-Release des Gerätes ein.
- `v` fügt die Version des aktuellen im Gerät aktiven Loaders ein.
- `m` fügt die MAC-Adresse des Gerätes ein.
- `s` fügt die Seriennummer des Gerätes ein.
- `n` fügt den Namen des Gerätes ein.
- `l` fügt den Standort des Gerätes ein.
- `d` fügt den Typ des Gerätes ein.

Geräte-Variablen für Geräteeigenschaften

In manchen Situationen soll ein Assistent Entscheidungen aufgrund der Geräteeigenschaften treffen. So soll der Assistent z. B. bestimmte Werte nur dann in die Konfiguration schreiben, wenn das jeweilige Gerät über eine bestimmte Art von WAN-Schnittstelle verfügt. Als Basis für diese Entscheidungen kann der Assistent mit bestimmten Variablen auf die Geräteeigenschaften zugreifen. Diese Variablen beginnen mit dem Schlüsselwort `device.` (inklusive des Punktes), gefolgt von dem Bezeichner der jeweiligen Eigenschaft. Der Assistent kann folgende Variablen für den lesenden Zugriff auf Geräteeigenschaften nutzen:

`device.flags.dhcp_addr`

Diese Variable gibt an, ob ein DHCP-Server dem Gerät eine IP-Adresse zugewiesen hat (in diesem Fall hat die Variable den Wert '128') oder nicht ('0').

`device.hasADSL`

Diese Variable gibt an, ob das Gerät über eine ADSL-Schnittstelle verfügt ('1') oder nicht ('0').

`device.hasISDN`

Diese Variable gibt an, ob das Gerät über eine ISDN-Schnittstelle verfügt ('1') oder nicht ('0').

`device.hasUMTS`

Diese Variable gibt an, ob das Gerät über eine UMTS-Schnittstelle verfügt ('1') oder nicht ('0').

`device.hasDSL`

Diese Variable gibt an, ob das Gerät über eine DSL-Schnittstelle verfügt ('1') oder nicht ('0').

`device.FirmwareVersion`

Diese Variable gibt die aktuelle Firmware-Version des Gerätes an.

`device.HardwareRelease`

Diese Variable gibt die Hardware-Release des Gerätes an.

`device.LoaderVersion`

Diese Variable gibt die aktuelle Loader-Version des Gerätes an.

`device.MacAddress`

Diese Variable gibt die MAC-Adresse des Gerätes in hexadezimaler Schreibweise ohne Trennzeichen an.

`device.SerialNumber`

Diese Variable gibt die Seriennummer des Gerätes an.

`device.Location`

Diese Variable gibt den Standort des Gerätes an, wie er im Setup-Menü unter **Setup** > **SNMP** > **Standort** eingetragen ist.

`device.DeviceString`

Diese Variable gibt den Typ des Gerätes an.

`device.Name`

Diese Variable gibt den Namen des Gerätes an, wie er im Setup-Menü unter **Setup** > **Name** eingetragen ist.

Aktionen

Der Assistent verwendet die Aktionen, um Werte in der Konfiguration der Geräte zu verändern. Für jede Aktion können Sie eine oder mehrere Bedingungen definieren, bei deren Eintreffen der Assistent die Aktion ausführt.

set

Diese Aktion ersetzt den Inhalt der Ziel-Variablen durch die angegebene Quelle. Die Quelle enthält in Form einer kommaseparierten Liste entweder Variablen oder Text-Strings.

```
set $target, $sourcelist
```

Wenn es sich bei der Ziel-Variablen um einen einzelnen Konfigurationsparameter handelt, geben Sie als Quelle nur einen Wert an, weitere Werte werden ansonsten ignoriert.

Wenn es sich bei der Ziel-Variablen um eine Tabelle handelt, geben Sie in der Quelle zuerst den Wert aus der Zeile an, die der Assistent ändern soll. Der Assistent durchsucht die erste Indexspalte nach diesem Wert und ändert die erste Zeile, in der er diesen Wert findet. Findet der Assistent keine passende Zeile mit diesem Wert, fügt er eine neue Zeile in die Tabelle ein.

Wenn es sich bei der Ziel-Variablen um einen numerischen Wert handelt, können Sie mit Hilfe der `add`- oder `sub`-Aktion den als `$number` definierten Betrag addieren oder subtrahieren.

```
set $target, $number, add
set $target, $number, sub
```

Beispiele

Die folgende Aktion setzt die Default-Route auf die gewünschten Werte:

```
set config.1.2.8.2, "255.255.255.255", "0.0.0.0", "0", "INTERNET", "0", "on", "Yes", ""
```

Die folgende Aktion erhöht den Wert der ARP-Aging-Minuten um '5':

```
set config.1.2.7.11, "5", add
```

Die folgende Aktion reduziert den Wert der ARP-Aging-Minuten um '5':

```
set config.1.2.7.11, "5", sub
```

del

Diese Aktion löscht den Inhalt der Ziel-Variable. Wenn es sich bei dieser Variablen um eine Tabelle handelt, geben Sie den Wert der ersten Indexspalte aus der zu löschenden Zeile an.

Beispiel

Die folgende Aktion löscht die Default-Route aus der Routing-Tabelle:

```
del config.1.2.8.2, "255.255.255.0"
```

cat

Diese Aktion hängt den Inhalt der Quell-Variablen an die Ziel-Variable an.

Beispiel

Die folgende Aktion fügt den Inhalt der Variablen `wizard.user` und die Variable `wizard.name` an:

```
cat wizard.name, wizard.user
```

cut

Diese Aktion löscht eine bestimmte Anzahl von Zeichen aus der Ziel-Variablen. Geben Sie die Position der zu löschenden Stelle von links gesehen sowie optional die Anzahl der zu löschenden Zeichen als Parameter an.

Beispiele

Die folgende Aktion löscht in der Variablen `wizard.name` alle Zeichen nach dem 2. Zeichen.

```
cut wizard.name, 2
```

Die folgende Aktion löscht in der Variablen `wizard.name` genau 4 Zeichen nach dem 2. Zeichen.

```
cut wizard.name, 2, 4
```

trigger_config_change

Änderungen der Konfiguration durch den Wizard sind je nach Teil der Firmware nicht sofort wirksam, da einige Module interne Strukturen für die Konfiguration verwenden.

Die Aktion `trigger_config_change` löst eine Aktualisierung dieser internen Strukturen aus. Setzen Sie diese Aktion in einer Sektion ein, wenn Sie beim Wechsel einer Seite im Rollout-Assistenten sichergehen möchten, dass die Konfiguration aktualisiert wurde.



Beim Beenden führt der Assistent diese Aktion automatisch aus.

exec

Den auf diesen Aktionsbefehl folgenden String führt das Gerät als Befehl auf der Konsole aus. Dabei ist auch die Nutzung von Variablen im String möglich, z. B. um ein `LoadScript` zu starten.

2.18.2.2 Trace für Rollout-Assistenten (Debugging)

Die HTML-Seiten des Assistenten zeigen nur das jeweilige Ergebnis einer internen Verarbeitung an. Während der Entwicklung eines Assistenten kann der Trace zum Assistenten dem Administrator zusätzliche Informationen z. B. über die Auswertung der einzelnen Bedingungen liefern, die er für die weitere Optimierung nutzt.

Den Trace des Rollout-Assistenten starten Sie an der Konsole mit dem Befehl `trace + Rollout-Wizard`.

2.18.2.3 Benutzerdefiniertes HTML-Template nutzen

Zur Anpassung des Assistenten an die Gestaltungsrichtlinien Ihres Unternehmens haben Sie optional die Möglichkeit, ein benutzerdefiniertes HTML-Template in das Gerät zu laden. In diesem Template legen Sie den grundlegenden Aufbau der HTML-Seiten und die Gestaltung von Farben, Schriften etc. über CSS-Regeln fest.

Der Assistent verwendet im HTML-Template folgende Platzhalter, um die Inhalte des Assistenten in die jeweiligen HTML-Seiten einzufügen:

- `<WIZARD_LOGO>`: An dieser Stelle setzt der Assistent das Logo ein, welches Sie im Format GIF, JPEG oder PNG in das Gerät geladen haben.
- `<WIZARD_CONTENT>`: An dieser Stelle setzt der Assistent den Inhalt der Sektionen in Form einer zweispaltigen Tabelle mit den zugehörigen Schaltflächen ein.

Ein sehr einfaches Beispiel für ein HTML-Template sieht folgendermaßen aus:

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd">
<html>
    <head>
        <title>Titel des Assistenten</title>
        <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
    </head>
    <body>
        <div>
            <WIZARD_LOGO>
        </div>
        <WIZARD_CONTENT>
    </body>
</html>
```

Der Assistent verwendet einige vordefinierte CSS-Klassen, die Sie durch die Angabe von entsprechenden Werten in Ihrem HTML-Template einfach anpassen können, u. a.:

- `class="header"`: Die CSS-Klasse für den Kopfbereich mit dem Logo.
- `class="wizardName"`: Die CSS-Klasse Absatz mit dem Namen des Assistenten im Kopfbereich.
- `class="headerLogo"`: Die CSS-Klasse für den Bereich des Logos im Kopfbereich.
- `class="wizardTable"`: Die CSS-Klasse für eine Tabelle mit den angezeigten Feldern.
- `class="footer"`: Die CSS-Klasse für den Fußbereich mit den Schaltflächen.

2.18.2.4 Dateien für den Assistenten hochladen

Um den Assistenten verfügbar zu machen, laden Sie die folgenden Dateien in das Gerät:

- **Rollout-Assistent (einfacher Text)**: Die Beschreibung des Assistenten (erforderlich). Diese ISO-8859-1-kodierte Text-Datei ist für den Betrieb des Assistenten notwendig und in der Größe nicht beschränkt.
- **Rollout-Assistent – Template (*.html, *.htm)**: Ein HTML-Template für den Assistenten (optional). Mit diesem Template steuern Sie die Darstellung der Sektionen in den HTML-Seiten des Assistenten im Browser des Anwenders. In diesem Template können Sie u. a. eigene CSS-Informationen zur Definition des Layouts verwenden. Wenn Sie kein eigenes HTML-Template in das Gerät laden, verwendet der Assistent ein vordefiniertes Template.
- **Rollout-Assistent – Logo (*.gif, *.png, *.jpeg)**: Das Logo Ihres Unternehmens (optional). Der Assistent setzt diese Bilddatei an der Stelle des Markers `<WIZARD_LOGO>` im HTML-Template ein.Wenn Sie kein eigenes Logo in das Gerät laden, verwendet der Assistent ein vordefiniertes Logo.

2.18.2.5 Dateien des Assistenten aus dem Gerät entfernen

Um die Dateien des Assistenten aus dem Gerät zu entfernen, haben Sie mehrere Möglichkeiten: Entweder Sie löschen die betreffenden Dateien gezielt aus dem Dateisystem Ihres Gerätes oder Sie verwenden dazu an der Konsole den Befehl `rollout` mit den entsprechenden Parametern.

Löschen über den rollout-Befehl

Die Löschfunktion des `rollout`-Befehls besitzt die folgende Syntax:

```
rollout (-r|-remove) <RelatedFile>
```

Mögliche Dateien sind:

- `wizard`: Löscht den Assistenten
- `template`: Löscht das Template
- `logo`: Löscht das Logo
- `alle`: Löscht den Assistenten, das Template und das Logo

Löschen über das Dateisystem

Im Dateisystem löschen Sie die Dateien des Assistenten über die analog lautenden Dateinamen:

- **rollout_wizard**
- **rollout_template**
- **rollout_logo**

2.18.2.6 Beispiel für einen benutzerdefinierten Rollout-Assistenten

Dieses Kapitel stellt ein Programmierungsbeispiel für einen benutzerdefinierten Rollout-Assistenten vor. Der Assistent ermöglicht die Einrichtung eines Internet-Zugangs.

Im ersten Abschnitt definiert der Assistent die Texte, die das Gerät auf den verschiedenen HTML-Seiten anzeigt.

```
stringtable "Deutsch"
 string title_MyCompany,   "MyCompany Rollout"
 string txt_Welcome,       "Willkommen beim MyCompany Rollout Assistenten"
 string dev_serial_number, "Seriennummer"
 string dev_type,          "Gerätetyp"
 ;---Seite: Auswahl der Internetverbindung
 string inet_Selection,    "Typ der Internetverbindung"
 string inet_PPPoE,        "PPPoE"
 string inet_IPoE,         "IPoE"
 ;---Seite: IPoE
 string inet_ipoe,         "Bitte geben Sie die Details für die Verbindung ein."
 string con_ipaddress,     "IP-Adresse"
 string con_subnet,        "Netzmaske"
 string con_gateway,       "Gateway"
 string con_dns,           "DNS"
 ;---Seite: PPPoE
 string inet_pppoe,        "Bitte geben sie Benutzername und Kennwort ein."
 string con_username,      "Benutzername"
 string con_password,      "Passwort"
 ;---Seite: Ende
 string ende,              "Die Konfiguration wird nun abgeschlossen."
```

Die erste Zeile des nächsten Abschnitts leitet den Assistenten mit dem Namen 'MyCompany Rollout' ein. Das Gerät zeigt den Text-String `str.title_MyCompany` als Titel in den HTML-Seiten an.

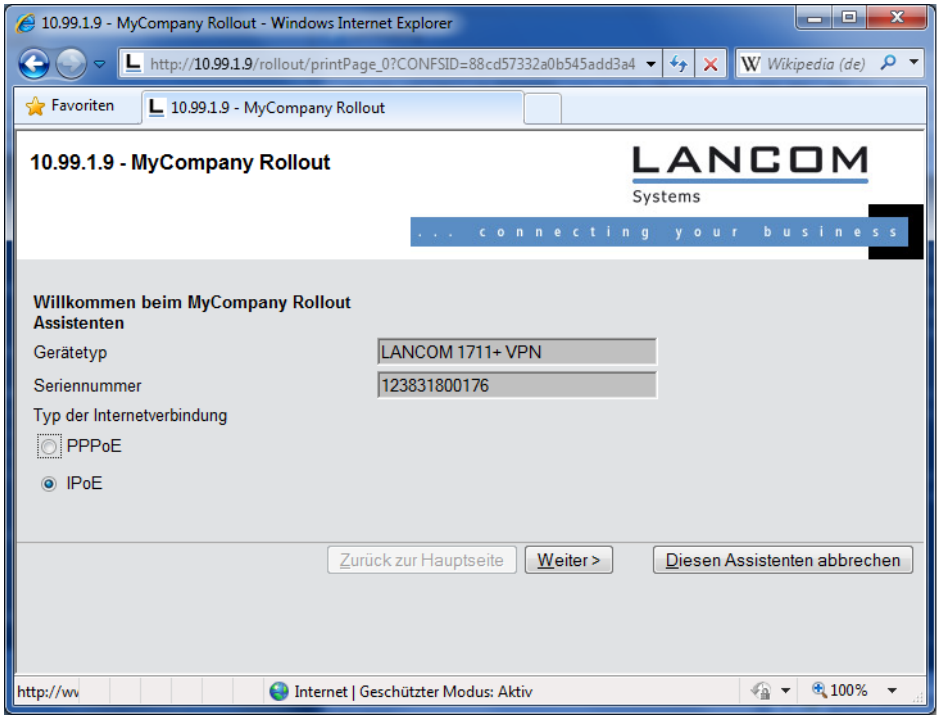
Danach definiert der Assistent die Sektionen, also die benötigten HTML-Seiten.

Die Sektion 'Start' zeigt zunächst einen statischen Text zur Begrüßung an. Darunter zeigt der Assistent in zwei Read-Only-Feldern den Gerätetyp und die Seriennummer an. Der Assistent liest diese beiden Werte beim Öffnen der Seite über den Bereich `on_show` aus dem Gerät aus. In einer Optionsliste bietet der Assistent dem Benutzer die Auswahl

für einen Internetzugang über 'PPPoE' oder 'IPoE' an. Da keine Werte für die Optionsfelder definiert sind, setzt der Assistent die Variable `select_inet` je nach Auswahl des Benutzers für PPPoE auf '0' und für IPoE auf '1'.

```
wizard "MyCompany Rollout", str.title_MyCompany

section ;---Start---
 static_text    str.txt_Welcome

 readonly_text device_string
  description   str.dev_type
```

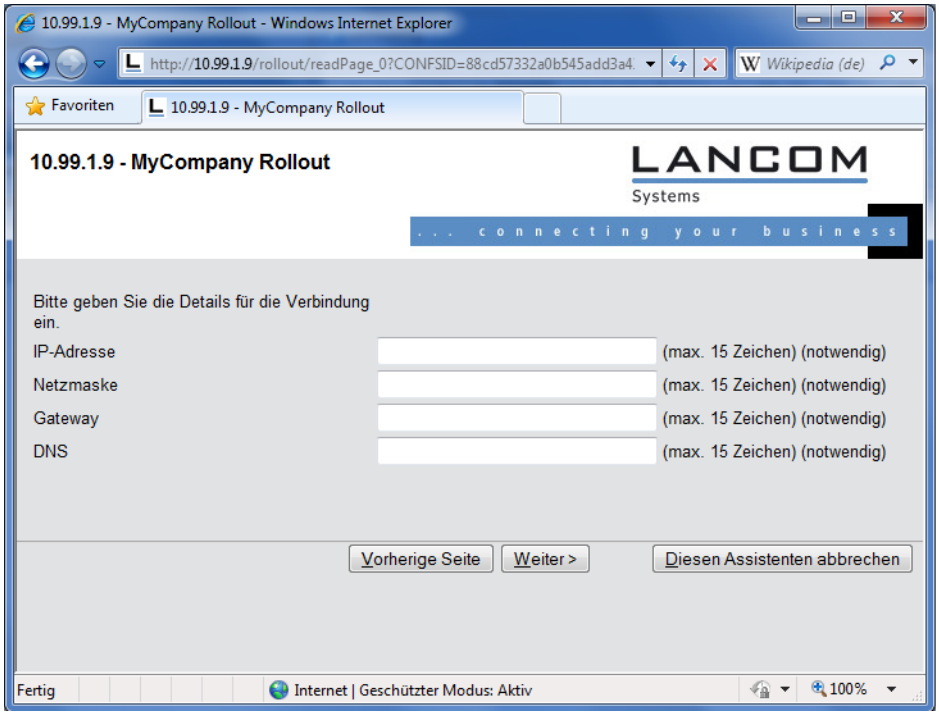
```
readonly_text device_serial_number
 description   str.dev_serial_number

selection_buttons select_inet
 description   str.inet_Selection
 button_text   str.inet_PPPoE, str.inet_IPoE

on_show
 set wizard.device_string, device.DeviceString
 set wizard.device_serial_number, device.SerialNumber

on_next
```



Der Assistent zeigt die Sektion IPoE nur dann an, wenn die Variable select_inet den Wert '1' hat.

Auf dieser Seite fragt der Assistent vom Benutzer die Werte für die IP-Adresse, die Netzmaske, das Gateway und den DNS-Server ab. Alle Felder sind für die Ausführung des Assistenten notwendig.

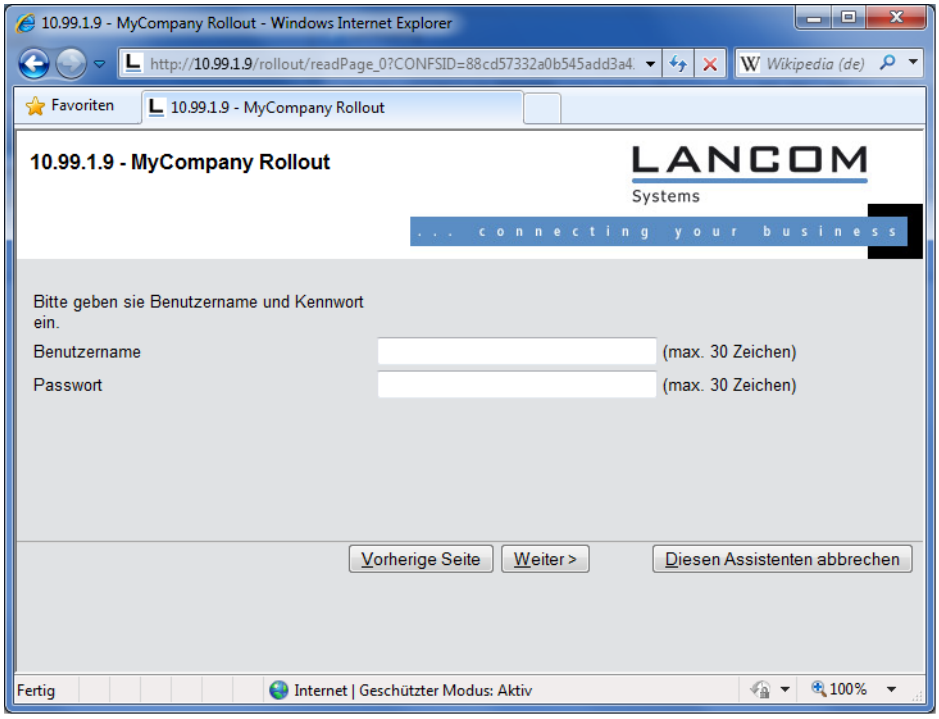
```
section ;---IPoE---
 only_if wizard.select_inet, "1", equal

 static_text   str.inet_ipoe

 entryfield_ipaddress inet_ipaddress
  description  str.con_ipaddress
  never_empty  1
 entryfield_ipaddress inet_subnet
  description  str.con_subnet
  never_empty  1
 entryfield_ipaddress inet_gateway
  description  str.con_gateway
  never_empty  1
 entryfield_ipaddress inet_dns
  description  str.con_dns
  never_empty  1
```



Der Assistent zeigt die Sektion PPPoE nur dann an, wenn die Variable select_inet den Wert '0' hat.

Auf dieser Seite fragt der Assistent vom Benutzer den Benutzernamen und das Passwort mit einer Länge von jeweils maximal 30 Zeichen ab.

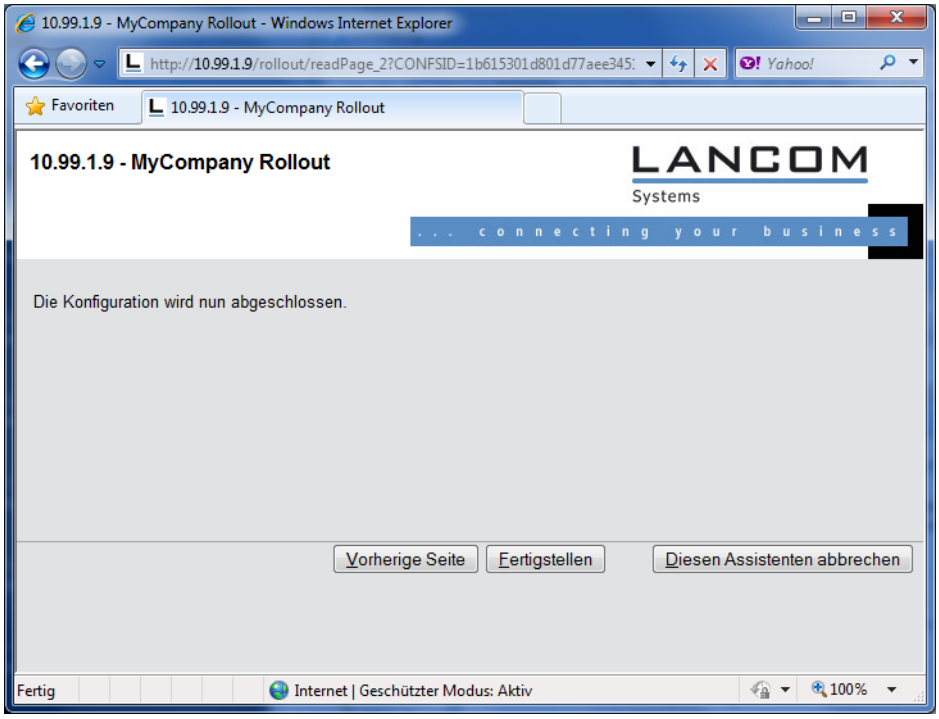
```
section ;---PPPoE---
 only_if wizard.select_inet, "0", equal

 static_text   str.inet_pppoe

 entryfield_text inet_username
  description  str.con_username
  max_len   30
 entryfield_text inet_password
  description  str.con_password
  max_len   30
```



Auf der letzten Seite zeigt der Assistent zunächst einen zusammenfassenden, statischen Text an. Folgende Aktionen führt der Assistent beim Fertigstellen des Assistenten aus:

- Wenn der Benutzer 'IPoE' ausgewählt hat, legt der Assistent eine passende Gegenstelle und einen Eintrag in der Liste der IP-Parameter an.
- Wenn der Benutzer 'PPPoE' ausgewählt hat, legt der Assistent eine passende Gegenstelle und einen Eintrag in der PPP-Liste an.
- Unabhängig von der Auswahl legt der Assistent eine Default-Route an, die den Router 'INTERNET' verwendet.

```
section ;---ende---
 static_text   str.ende

on_init  ;---Befehle, die bei der Initialisierung des Wizards durchgeführt werden.---

on_apply ;---Befehle, die bei der Fertigstellung des Wizards durchgeführt werden.---

 ;---Wenn IPoE ausgewählt wurde, werden die entsprechenden Daten nun eingetragen.
 ;---Gegenstelle
 set config.1.2.2.19, "INTERNET", "9999", "", "", "IPOE", "0", "000000000000"
  only_if wizard.select_inet, "1", equal
 ;---IP-Parameter
 set config.1.2.2.20, "INTERNET", wizard.inet_ipaddress, wizard.inet_subnet, "0.0.0.0", wizard.inet_gateway,
wizard.inet_dns, "0.0.0.0", "0.0.0.0", "0.0.0.0"
  only_if wizard.select_inet, "1", equal

 ;---Wenn PPPoE ausgewählt wurde, werden die entsprechenden Daten eingetragen.
 ;---Gegenstelle
 set config.1.2.2.19, "INTERNET", "9999", "", "", "PPPOE", "0", "000000000000"
  only_if wizard.select_inet, "0", equal
 ;---PPP-Liste
  set  config.1.2.2.5,  "INTERNET",  "none",  "60",  wizard.inet_password,  "5",  "5",  "10",  "5",  "2",
wizard.inet_username, "1"
  only_if wizard.select_inet, "0", equal

 ;---Setzen der Default Route.
 set config.1.2.8.2, "255.255.255.255", "0.0.0.0", "0", "INTERNET", "0", "on", "Yes", ""
```



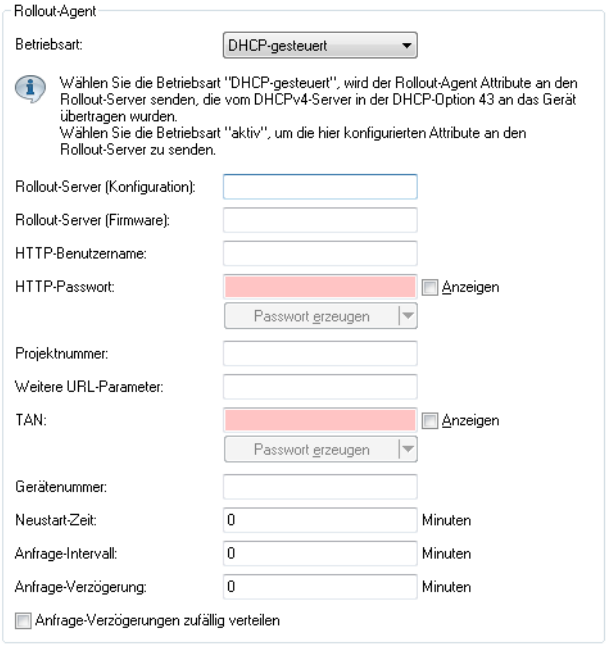
2.18.3 Aktivierung des Rollout-Assistenten im WEBconfig

Um den Rollout-Assistenen allgemein verfügbar zu machen, setzen Sie im Setup-Menü den Parameter **HTTP** > **Rollout-Wizard** > **In-Betrieb** auf **ja**. Dies aktiviert zunächst den Default-Rollout-Wizard. Im WEBconfig erscheint dann unter **Setup-Wizards** ein neuer Assistent mit dem unter **HTTP** > **Rollout-Wizard** > **Titel** vergebenen Namen.

Um ihn anschließend durch einen benutzerdefinierten Rollout-Assistenten zu ersetzen, laden Sie die Beschreibung des Assistenten in das Gerät (siehe hierzu *Dateien für den Assistenten hochladen* auf Seite 143).

2.18.4 Konfiguration mit LANconfig

Mit LANconfig konfigurieren Sie den Rollout-Agent über **Management** > **Rollout-Agent**.



Betriebsart

Wählen Sie die Betriebsart „DHCP-gesteuert“, wenn der Rollout-Agent des Gerätes die Attribute an den Rollout-Server übertragen soll, die er zuvor über die Vendor-spezifische DHCP-Option 43 vom DHCP-Server erhalten hat. In der Betriebsart „Aktiv“ überträgt das Gerät die in diesem Dialog konfigurierten Attribute (z. B., wenn im Netzwerk kein DHCP verfügbar ist). Die Betriebsart „Aus“ deaktiviert den Rollout-Agenten.

Die Betriebsart „DHCP-gesteuert“ überschreibt manuell konfigurierte Attribute nicht. Somit ist eine umfangreiche Vorkonfiguration möglich, bei der das Gerät z. B. nur die vom DHCP-Server übertragene aktuelle Kontaktinformation des Rollout-Servers verwendet (Adresse, Login-Daten).

Rollout-Server (Konfiguration)

Mit diesem Eintrag definieren Sie die Adresse des Rollout-Servers, der für das Rollout der Konfiguration zuständig ist.

Ein Eintrag ist in folgenden Formen möglich:

- IP-Adresse (HTTP, HTTPS, TFTP)
- FQDN

Rollout-Server (Firmware)

Mit diesem Eintrag definieren Sie die Adresse des Rollout-Servers, der für das Rollout der Firmware zuständig ist.

Ein Eintrag ist in folgenden Formen möglich:

- IP-Adresse (HTTP, HTTPS, TFTP)
- FQDN

HTTP-Benutzername

Legen Sie mit diesem Eintrag den Benutzernamen fest, mit dem sich der Rollout-Agent am Rollout-Server anmeldet.

HTTP-Passwort

Legen Sie mit diesem Eintrag das Benutzerpasswort fest, mit dem sich der Rollout-Agent am Rollout-Server anmeldet.

Projektnummer

Bestimmen Sie mit diesem Eintrag die Rollout-Projektnummer für den Rollout-Agenten.

Weitere URL-Parameter

Legen Sie mit diesem Eintrag weitere Parameter fest, die der Rollout-Agent zum Rollout-Server übertragen soll.

TAN

Legen Sie mit diesem Eintrag die Rollout-TAN fest.

Gerätenummer

Enthält die Gerätenummer des Gerätes, auf dem der Rollout-Agent ausgeführt wird.

Neustart-Zeit

Legen Sie hier die Zeit für einen Neustart des Gerätes nach einem Rollout fest.

Anfrage-Intervall

Legen Sie hier die Zeit in Sekunden für eine erneute Anforderung für ein Konfigurations-Rollout fest, nachdem eine Konfiguration gescheitert ist.



Bei einem Wert „0" startet der erneute Versuch in 1 Minute.

Anfrage-Verzögerung

Dieser Eintrag enthält die Verzögerungszeit für einen Rollout-Request in Sekunden.

Anfrage-Verzögerung zufällig verteilen

Legen Sie mit diesem Eintrag fest, dass die Anfrage nach einem Rollout zufällig erfolgt. Diese Einstellung verhindert, dass alle am Rollout beteiligten Geräte zeitgleich beim LSR-Server eine Konfiguration anfordern.

2.18.5 LSR-Informationen über DHCP-Server erhalten (Zero-Touch-Rollout)

Ein unkonfiguriertes LANCOM Gerät startet mit einem aktivierten DHCP-Client und bezieht dadurch IP-Adresse, Netzmaske, DNS-Adresse und Gateway-Adresse vom DHCP-Server im Netzwerk.

Über die Vendor-spezifische DHCP-Option 43 sendet ein entsprechend konfigurierter DHCP-Server u. a. auch Informationen darüber, wie ein LSR-Server (Large Scale Rollout) zu erreichen ist. Der Rollout-Agent des LANCOM Gerätes wertet diese Informationen aus, kontaktiert den LSR-Server und bezieht anschließend im Rahmen der bestehenden Rollout-Strategie seine Konfiguration oder aktualisiert seine Firmware. Zur DHCP-Option 43 siehe auch *DHCP-Optionen* auf Seite 1627

Diese Funktion erleichtert den Rollout-Prozess, da keine Vorkonfiguration der Geräte mehr notwendig ist.

Die Verbindung zum LSR-Server erfolgt über HTTP, HTTPS oder TFTP, wobei im LANCOM-Gerät für eine sichere Verbindung ein entsprechendes SSL-Zertifikat gespeichert sein muss.

Eine (auch partielle) Vorkonfiguration des Rollout-Agents ist ebenfalls möglich. So kann z. B. die vom DHCP-Server gesendete Rollout-Server-URL übernommen, eine Projektnummer im Gerät allerdings vorkonfiguriert werden.

2.18.5.1 Konfiguration des Zero-Touch-Rollouts

Ausgangslage

In einem Filial-Rollout ist es auf Grund der hohen Zahl an Geräten erforderlich, die LANCOM Geräte nicht vorkonfigurieren zu müssen. Sie sollen stattdessen in Betrieb gehen, nachdem sie die Konfiguration von einem zentralen LSR-Server erhalten haben, vergleichbar dem „Zero-Touch-Management" bei einem WLC.

Rahmenbedingungen

Damit dieser „Zero-Touch-Rollout" über den Rollout-Agenten des Gerätes funktioniert, sind einige Rahmenbedingungen zu erfüllen:

- Es muss ein zentraler Rollout-Server verfügbar und für die Zero-Touch-Geräte über HTTP/HTTPS erreichbar sein.
- Im Filial-Netz muss DHCP aktiv sein. D. h.,
  - ein filialnetz-eigener DHCP-Server ist erreichbar oder
  - ein DHCP-Relay-Server im Filialnetz vermittelt die DHCP-Datenpakete zwischen den Geräten im Filialnetz und einem DHCP-Server in der Zentrale.
- Der DHCP-Server muss die DHCP-Option 43 ausliefern können.

Der DHCP-Server überträgt sensitive Daten wie z. B. das Rollout-Passwort ungesichert als DHCP-Nachricht. Es ist also darauf zu achten, die Daten nur über entsprechend abgesicherte Verbindungen zu transportieren.

Ablauf

Der Konfigurations-Rollout läuft wie folgt ab:

1. Das unkonfigurierte Gerät wird an das Filial-Netz angeschlossen.
2. Über den DHCP-Server bezieht das Gerät die erforderlichen Verbindungsdaten wie IP-Adresse, Gateway, Netzmaske, DNS-Adresse und die DHCP-Option 43.
3. Aus der DHCP-Option 43 dekodiert das Gerät die URL des Rollout-Servers sowie zusätzliche Informationen und konfiguriert damit den Rollout-Agenten des Gerätes.
4. Der Rollout-Agent kontaktiert daraufhin den Rollout-Server und führt den Rollout nacheinander in zwei Schritten durch:
   - Firmware-Update
   - Konfigurations-Update

Der Rollout-Agent erwartet, dass der unter der konfigurierten Firmware-Server-URL erreichbare Rollout-Server eine Firmware im `.upx`-Format ausliefert, die er anschließend in das Gerät einspielt.

Nach dem Firmware-Update startet das Gerät neu und kontaktiert den Rollout-Server erneut. Der Rollout-Agent prüft, ob die vom Rollout-Server ausgelieferte Firmware bereits installiert ist. Diese Prüfung ist erfolgreich, da das Gerät im ersten Schritt die aktuelle Firmware erhalten hat. Der Rollout-Agent fährt mit dem Update der Konfiguration bzw. dem Download von Skriptdateien fort. Er erwartet, dass der unter der konfigurierten Config-Server-URL erreichbare Rollout-Server ein Skript im `.lcs`-Format ausliefert, das er anschließend auf in das Gerät einspielt.

Die DHCP-Option 43

Die DHCP-Option 43 ist herstellerspezifisch, d. h., jeder Hersteller kann selbst entscheiden, wie er diese Option strukturiert und welche Informationen er darin kodiert. Die Option kann mehrere sogenannter Sub-Typen enthalten, die die Daten detaillierter strukturieren.

Für den Rollout-Agenten des Gerätes sind die folgenden Sub-Typen spezifiziert:

Sub-Type 1: Config-Server-URL

Die Angabe der Server-Adresse ist in den folgenden Formaten möglich:

- HTTP, HTTPS, TFTP
- IP-Adresse, FQDN

Beispiele:

- https://rollout:443/
- tftp://10.1.1.1
- http://10.1.1.2/test

Auch die Angabe von LCOS-Variablen ist möglich

Der Rollout-Agent erwartet, dass der unter dieser Adresse erreichbare Rollout-Server auf seine Anfrage hin ein Konfigurations-Skript mit der Erweiterung `.lcs` sendet.

Handelt es sich beim Rollout-Server um einen LSR, muss der Adresse das Präfix `lsr:` vorangestellt sein, z. B. `lsr:https://rollout:443/`. Anschließend baut der Rollout-Agent die korrekte LSR-Rollout-URL aus den Sub-Types 5 und folgende zusammen. Entsprechend sind die Sub-Types ab 5 nur bei der Verwendung dieses Präfixes von Bedeutung.

Handelt es sich beim Rollout-Server um keinen LSR, ist die Angabe der URLs für Config-Server und Firmware-Server von Hand und unter Verwendung von Variablen notwendig.

Sub-Type 2: Firmware-Server-URL

Wie bei Sub-Type 1, allerdings erwartet der Rollout-Agent, dass der unter dieser Adresse erreichbare Rollout-Server auf seine Anfrage hin eine Firmware-Datei mit der Erweiterung `.upx` sendet.

Sub-Type 3: HTTP-Username

Enthält den Usernamen für die HTTP-Authentifizierung in der URL (entsprechend `http://username:password@server`)

Sub-Type 4: HTTP-Password

Enthält das Passwort für die HTTP-Authentifizierung in der URL (entsprechend `http://username:password@server`)

Sub-Type 5: LSR-Projektnummer

Enthält die im Rollout-Server für das erforderliche Rollout-Projekt gespeicherte Projektnummer.

Sub-Type 6: Zusätzliche URL-Parameter für LSR-Keyword

Der Rollout-Agent fügt diesen Inhalt an die konstruierte LSR-URL an (z. B. `?approval=yes`).

Sub-Type 7: Reboot-Time

Gibt die Wartezeit in Minuten für den Restart des Gerätes nach dem Update durch den Rollout-Server an.

Sub-Type 8: Request-Interval

Gibt den Intervall in Minuten an, in dem der Rollout-Agent seine Anfragen an den Rollout-Server sendet.

Sub-Type 9: TAN

Dieser Eintrag enthält die Rollout-TAN.

Sub-Type 10: Gerätenummer

Enthält die Gerätenummer des zu aktualisierenden Gerätes.

Sub-Type 11: Request-Delay

Enthält die Zeit in Minuten, die der Rollout-Agent zwischen Request 1 und Request 2 wartet.

Sub Type 12: Request-Random

Diese Einstellung verhindert, dass alle am Rollout beteiligten Geräte zeitgleich beim LSR-Server eine Konfiguration anfordern. Die folgenden Angaben sind möglich:

0

Die Anfragen erfolgen immer mit fest eingestellten Zeitangaben.

1

Legen Sie mit diesem Eintrag fest, dass die Anfrage nach einem Rollout zufällig erfolgt.

Sub-Type 13: Omit-Certificate-Check

Dieser Wert legt fest, ob der Rollout-Agent die Überprüfung des Rollout-Server-Zertifikats überspringen soll.

Fehlt dieser Sub-Type oder ist sein Inhalt leer, nimmt der Rollout-Agent den Wert „0" an und prüft somit das Server-Zertifikat.

Beachten Sie bitte, dass die vom Rollout-Server erhaltene Konfiguration den Rollout-Agent zum Abschluss abschalten sollte **(`Operating: no`)**, da das Gerät sonst nach der Reboot-Time rebootet und den Rollout-Prozess erneut durchführt.

Variablen

In den URLs sind alle Variablen verwendbar, die die LCOS-Konsole beinhaltet. Diese Variablen lassen sich in der Konsole über den Befehl `printenv` ausgeben.

Die Angabe der Variablen in den URLs erfolgt mit vorangestelltem „$" (z. B. `$__SERIALNO`).

Erzeugung der DHCP-Option 43

Die Erzeugung der DHCP-Option 43 erfolgt auf Grundlage der *RFC 2132, Abschnitt 8.4*.

Die DHCP-Option 43 kann beim DHCP-Server eines LANCOM Gerätes ebenfalls hinzugefügt werden. Siehe hierzu *DHCP-Optionen* auf Seite 1627.

Bei Verwendung eines ISC DHCPd DHCP-Server kann die Option 43 passend mit dem folgenden Konfigurationsabschnitt beispielhaft erzeugt werden:

Innerhalb der allgemeinen Konfiguration

```
option space Rollout;
option Rollout.config-server code 1 = text;
option Rollout.firmware-server code 2 = text;
option Rollout.HTTP-Username code 3 = text;
option Rollout.HTTP-Password code 4 = text;
option Rollout.Projectnumber code 5 = text;
option Rollout.AdditionalParams code 6 = text;
option Rollout.RebootTime code 7 = text;
option Rollout.RequestInterval code 8 = text;
option Rollout.Tan code 9 = text;
option Rollout.Devicenumber code 10 = text;
option Rollout.RequestDelay code 11 = text;
option Rollout.RequestRandom code 12 = text;
option Rollout.OmitCertCheck code 13 = text;
```

Innerhalb der Subnetz-spezifischen Konfiguration

```
vendor-option-space Rollout;
 option Rollout.config-server "LSR:https://10.200.50.1:443";
```

```
option Rollout.firmware-server "LSR:https:// 10.200.50.1:443";
option Rollout.HTTP-Username "RolloutUser";
option Rollout.HTTP-Password "Secret";
option Rollout.Projectnumber "1";
option Rollout.RebootTime "300";
option Rollout.RequestDelay "20";
option Rollout.RequestRandom "0";
option Rollout.OmitCertCheck "2";
```

Andere DHCP-Server (z. B. der Microsoft DHCP-Server) lassen keine Definition der Option 43 in der Konfiguration zu. Hier muss die vom Server als Option 43 auszuliefernde Bytefolge vorgefertigt in die Konfiguration eingefügt werden.

2.19 TCP-Port-Tunnel

In manchen Situationen ist es sinnvoll, einen vorübergehenden Zugriff – z. B. über HTTP (TCP-Port 80) oder TELNET (TCP-Port 23) – auf eine Station in einem Netz einzuräumen. Sofern beispielsweise bei der Konfiguration von Netzwerkgeräten Fragen auftauchen, kann der jeweilige Support besser weiterhelfen, wenn er direkten Zugriff auf das Gerät im Netz des Kunden hat. Die Standardmethode für den Zugriff auf Geräte im Netz über inverses Masquerading (Port-Forwarding) erfordert jedoch in manchen Fällen eine entsprechende Konfiguration der Firewall; zudem sind die dabei angelegten Zugänge schnell vergessen und stellen damit ein potentielles Sicherheitsrisiko dar.

Als Alternative zu den dauerhaften Zugängen über festes Port-Forwarding haben Sie die Möglichkeit, vorübergehende Fernwartungszugänge einzurichten, die nach einer bestimmten inaktiven Zeit automatisch wieder geschlossen werden. Dazu erzeugen Sie z. B. für den Support-Mitarbeiter einen **TCP / HTTP-Tunnel**, über welchen er einen temporären Zugang zum entsprechenden Gerät erhält.

Dieser Zugang ist nur für jene IP-Adresse gültig, von der aus Sie den Tunnel erzeugt haben. Der Zugriff auf das freizugebende Gerät im Netzwerk ist also nicht übertragbar!

2.19.1 TCP- / HTTP-Tunnel konfigurieren

Die Konfiguration eines TCP- / HTTP-Tunnels erfolgt über das Setup-Menü.

1. Wechseln Sie im Setup-Menü des Gerätes in das Verzeichnis **HTTP**.
2. Geben Sie für den Parameter **Max.-Tunnel-Verbindungen** die maximale Anzahl der gleichzeitig aktiven TCP- / HTTP-Tunnel an, die Sie erlauben wollen.
3. Geben Sie für den Parameter **Tunnel-Idle-Timeout** die Lebensdauer eines Tunnels ohne Aktivität an (in Sekunden). Nach Ablauf dieser Zeit wird der Tunnel automatisch geschlossen, wenn darüber keine Daten übertragen werden.

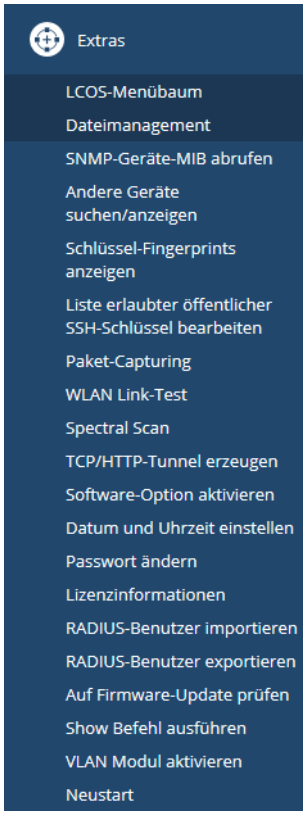
Fertig! Damit haben Sie die konfiguration der TCP- / HTTP-Tunnel abgeschlossen.

2.19.2 TCP- / HTTP-Tunnel per WEBconfig erzeugen

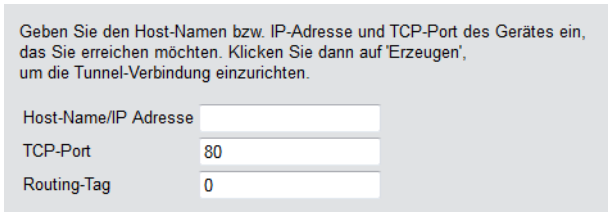
Einen TCP- / HTTP-Tunnel richten Sie über die WEBconfig-Oberfläche Ihres Gerätes ein.

1. Melden Sie sich im WEBconfig jenes Gerätes an, hinter dem das freizugebende Gerät erreichbar ist.

2. Wählen Sie im Bereich **Extras** den Eintrag **TCP/HTTP-Tunnel erzeugen**.



3. Geben Sie den DNS-Namen bzw. die IP-Adresse des Gerätes ein, das Sie vorübergehend für den Zugriff über HTTP freischalten möchten, und wählen Sie den Port aus, der für den HTTP-Tunnel verwendet werden soll.



> Anstelle von HTTP- oder HTTPS-Fernwartungszugängen sind auch Fernwartungstunnel mit beliebigen anderen TCP-Diensten möglich, beispielsweise TELNET-Verbindungen (TCP-Port 23) oder SSH (TCP-Port 22).

4. Geben Sie ggf. das Routing-Tag des IP-Netzwerks an, in dem sich das freizugebende Gerät befindet.
5. Bestätigen Sie die Angaben mit **Erzeugen**.

Der folgende Dialog zeigt eine Bestätigung über den neu erstellten Tunnel und bietet einen Link auf das freizugebende Gerät.



2.19.3 TCP- / HTTP-Tunnel per CLI erzeugen

Einen TCP- / HTTP-Tunnel richten Sie über die CLI Ihres Gerätes ein.

1. Melden Sie sich z. B. per SSH an dem Gerät an, hinter dem das freizugebende Gerät erreichbar ist.
2. Gehen Sie über `cd /setup/http` in dieses Verzeichnis
3. Rufen Sie das Kommando `do Start-TCP-HTTP-Tunnel -r <Routing Tag> -h <IP-Adresse> -p <Lokaler Port> [-a <Remote-Adresse>]` auf.

   -r

   Routing-Tag.

   -h

   Host-Adresse, auf die über den Tunnel zugegriffen werden soll.

   -p

   Lokaler Port.

   -a

   Optionale Remote-Adresse

Der TCP- / HTTP-Tunnel wurde erzeugt.

2.19.4 TCP- / HTTP-Tunnel vorzeitig löschen

Das Gerät löscht erstellte TCP- / HTTP-Tunnel automatisch nach Ablauf der Tunnel-Idle-Timeouts (siehe *TCP- / HTTP-Tunnel konfigurieren* auf Seite 154. Um einen Tunnel vorzeitig zu löschen, rufen Sie im Status-Menü unter **TCP-IP** > **HTTP** > **Aktive-Tunnel** die Liste der aktiven TCP- / HTTP-Tunnel auf und entfernen den nicht mehr benötigten Tunnel gezielt. Der Tunnel wird allerdinggs auch dann erst entfernt, sobald keine aktiven TCP-Verbindungen mehr vorhanden sind.

Aktive TCP-Verbindungen in diesem Tunnel werden mit dem Löschen des Tunnels **nicht** beendet, es können aber keine neuen Verbindungen mehr aufgebaut werden.

2.20 Die LANCOM High Availability Clustering Option

Mit der LANCOM High Availability Clustering Option haben Sie die Möglichkeit einer deutlich vereinfachten Administration sowie einer großen Zeitersparnis. Sie konfigurieren lediglich ein Gerät innerhalb einer definierten Gerätegruppe (Cluster). Die Änderungen werden automatisch auf die anderen Cluster-Mitglieder übertragen.

Bei Ausfall oder Wartung eines Gerätes (z. B. Firmware-Update) verbinden sich die APs oder aufgebauten VPNs automatisch mit einem anderen WLC, bzw. dem Backup Central Site VPN Gateway. Diese Geräte besitzen durch den automatischen Konfigurationsabgleich bereits die identische Konfiguration. Dadurch wird eine komfortable Hochverfügbarkeit realisiert.

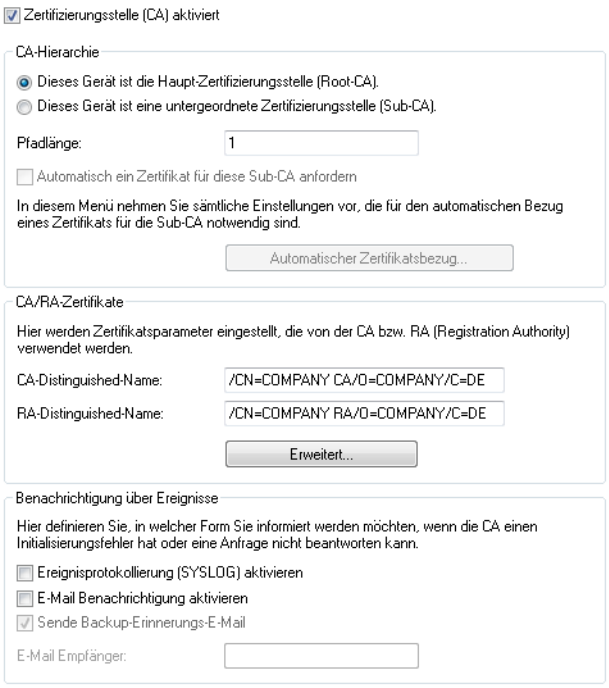
Die Voraussetzungen für eine gültige Gruppenmitgliedschaft eines Gerätes sind:

- Es muss eine LANCOM WLC High Availability Clustering XL Option vorhanden sein (ab LCOS-Version 9.10).
- Es muss zu allen Cluster-Mitgliedern eine IP-Kommunikation über LAN, WAN oder VPN aufbauen können.
- Es muss in der Gruppenliste aufgeführt sein, die in jedem Gerät gespeichert ist.
- Es muss ein gültiges Zertifikat besitzen.
- Es muss sich als Gruppenmitglied mit einem Zertifikat authentifizieren können.

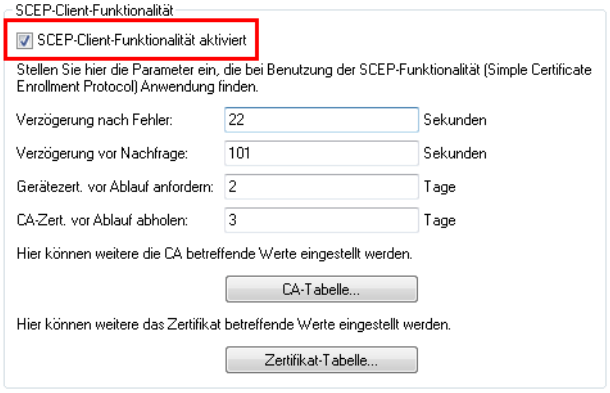
2.20.1 Konfigurations-Synchronisation einrichten

Damit die Konfigurations-Synchronisation möglich ist, müssen alle zu konfigurierenden Geräte gültige Zertifikate vorweisen können. Für eine einfache Zertifikatsverteilung konfigurieren Sie daher zuerst auf einem Gerät eine SCEP-CA.

1. Dazu ist es notwendig, unter **Zertifikate** > **Zertifizierungsstelle (CA)** den SCEP-Server zu aktivieren. Wenn Sie die Konfigurations-Synchronisation auf einem WLC einrichten, ist der SCEP-Server höchstwahrscheinlich schon aktiv.



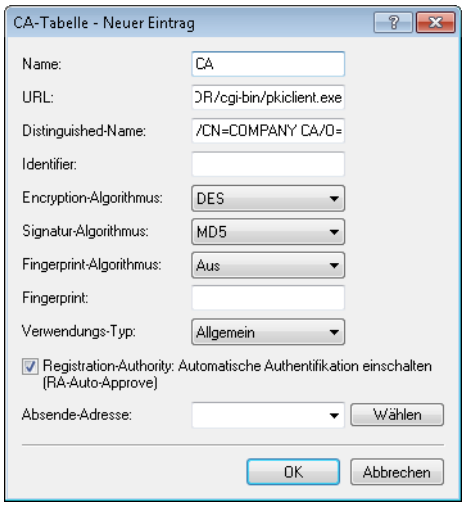
2. Aktivieren Sie anschließend auf jedem Gerät, auf dem Sie die Konfigurations-Synchronisation verwenden möchten (inklusive des SCEP-CA-Gerätes), die SCEP-Client-Funktion unter **Zertifikate** > **SCEP-Client**. Wenn Sie die Konfigurations-Synchronisation auf einem WLC einrichten, ist der SCEP-Client höchstwahrscheinlich schon aktiv.



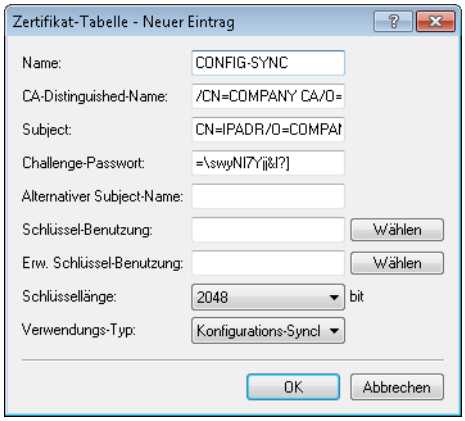
3. Ergänzen Sie die **CA-Tabelle** um einen neuen Eintrag für den SCEP-Server.

   Die Werte für die CA-Tabelle entsprechen den Einstellungen des SCEP-Servers aus Schritt 1 und sind somit für alle Stationen identisch. Für die URL tragen Sie `http://IPADR/cgi-bin/pkiclient.exe` ein, wobei Sie `IPADR` durch die IP-Adresse des als SCEP-CA konfigurierten Gerätes ersetzen.

Wenn Sie die Konfigurations-Synchronisation auf einem WLC einrichten, ist ein entsprechender Eintrag schon für den WLC-Betrieb vorhanden; dieser ist auch für den Bezug eines Zertifikates für die Konfigurations-Synchronisation einsetzbar, so dass in diesem Fall in der CA-Tabelle keine Änderung notwendig ist.



4. Ergänzen Sie die **Zertifikat-Tabelle** im SCEP-Client um einen neuen Eintrag für den Bezug eines Konfigurations-Synchronisation-Zertifikates. Als **CA-Distinguished-Name** verwenden Sie den bereits bei Erstellung des CA-Tabellen-Eintrages verwendeten Namen.

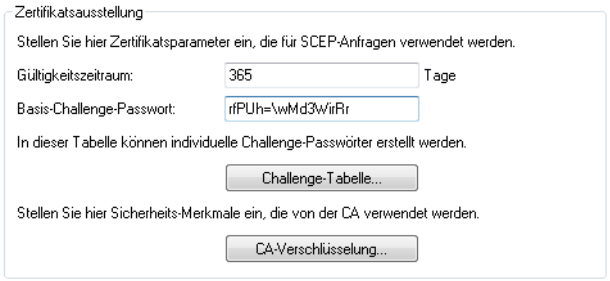


Als Subject tragen Sie die jeweils geräteeigene IP-Adresse ein (z. B. `/CN=IPADR /O=COMPANY/C=DE`, wobei Sie `IPADR` durch die IP-Adresse des als SCEP-CA konfigurierten Gerätes ersetzen.

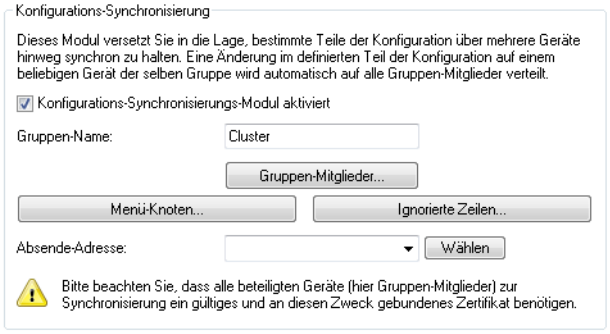
Es ist für die Funktion der Konfigurations-Synchronisation zwingend erforderlich, dass die IP-Adresse des Gerätes im Subject des Zertifikates enthalten ist.

Als **Verwendungs-Typ** geben Sie „Konfigurations-Synchronisation" an. Passen Sie außerdem die **Schlüssellänge** auf „2048 bit" an. Den **Namen** des Tabelleneintrages können Sie frei wählen.

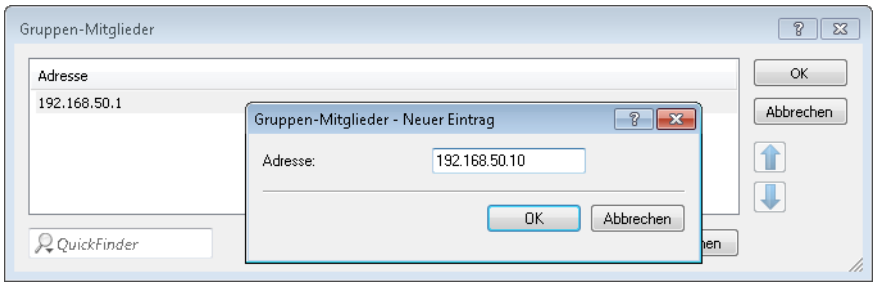
Das Challenge-Passwort des als SCEP-CA konfigurierten Gerätes finden Sie in dessen Konfiguration unter **Zertifikate** > **Zertifikats-Behandlung** > **Basis-Challenge-Passwort**.



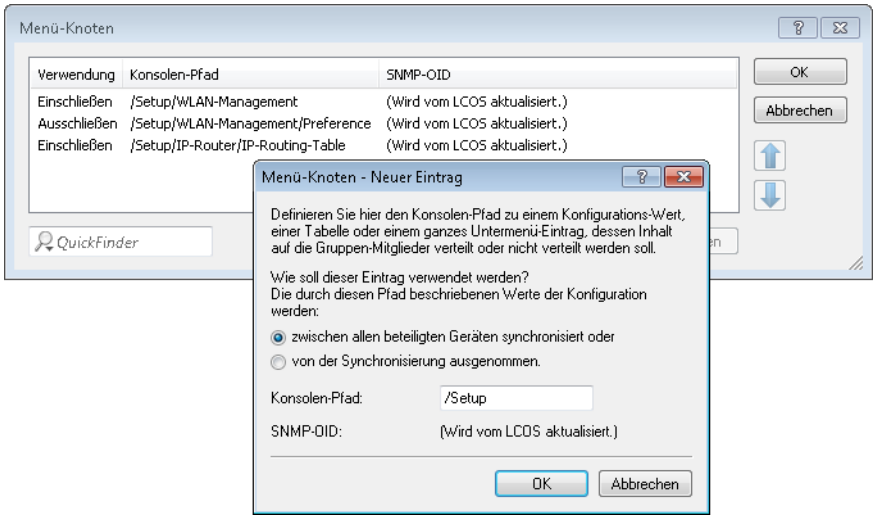
5. Hiermit ist die Einrichtung der SCEP-CA sowie des SCEP-Clients zum Bezug der Konfigurations-Synchronisations-Zertifikate abgeschlossen. Sie können die Konfiguration an diesem Punkt bereits einmal in das Gerät zurückschreiben, um den Bezug der Zertifikate zu bewirken.
6. Aktivieren Sie nun die Konfigurations-Synchronisation unter **Management** > **Synchronisierung** mit der Option **Konfigurations-Synchronisierungs-Modul aktiviert**. Unter **Gruppen-Name** können Sie ebenfalls einen benutzerdefinierten Namen für den Cluster festlegen, der anschließend auch in der LANconfig-Geräteliste erscheint.



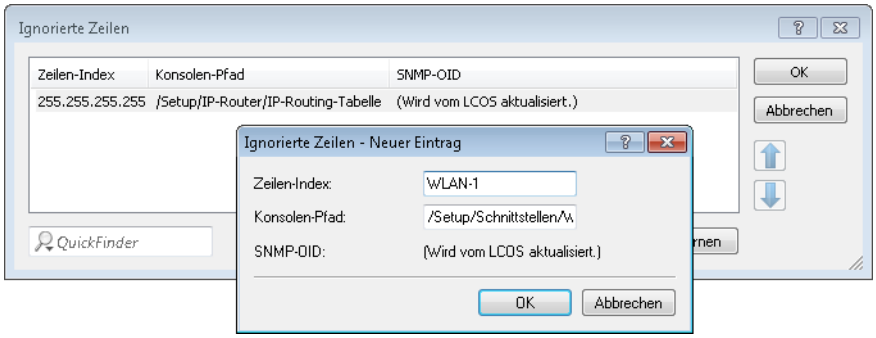
7. Tragen Sie unter **Gruppen-Mitglieder** die IP-Adressen **aller** Geräte ein, die Mitglieder des Clusters werden sollen.



8. Definieren Sie unter **Menü-Knoten** die zu synchronisierenden Menüs. Möchten Sie Menüknoten explizit von der Synchronisation ausnehmen, wählen Sie unter **Verwendung** "von der Synchronisation ausgenommen".



Definieren Sie optional unter "Ignorierte Zeilen", welche Zeilen einer Tabelle von der Synchronisation ausgenommen werden sollen. Beispiel: Default-Route auf VPN-Gateways, die für jedes Gateway unterschiedlich sein soll. Die restliche Routing-Tabelle kann durch einen Eintrag in den **Menü-Knoten** synchronisiert werden.



9. Die Einrichtung der Konfigurations-Synchronisation ist auf diesem Gerät nun abgeschlossen. Sie können die Konfiguration nun in das Gerät zurückschreiben.
10. Führen Sie die Schritte 2 bis 9 auf den weiteren zum Cluster gehörigen Geräten aus. Verweisen Sie dabei bei der Konfiguration des SCEP-Clients, wie oben angegeben, auf die SCEP-CA des ersten Gerätes.
11. Starten Sie nun den Cluster auf dem Gerät, welches initial seine Konfiguration auf alle Mitglieder des Clusters verteilen soll. Wählen Sie dazu in der LANconfig-Geräteliste im Kontextmenü des Gerätes **[Cluster starten…]**.
12. Der Cluster ist nun in Betrieb. Sie können den Zustand des Clusters in der WEBconfig unter **Status** > **Config** > **Sync** > **Zustand** überprüfen. Änderungen an der Konfiguration können nun an jedem Mitglied des Clusters vorgenommen werden und werden auf die anderen Mitglieder synchronisiert.

Beachten Sie folgende Anforderungen:

- Auf den beteiligten Geräten muss die korrekte Uhrzeit gesetzt sein (Zertifikatsprüfung).
- Die eigene IP-Adresse des Gerätes muss im Subject des eigenen Zertifikates auftauchen.
- Die zu synchronisierenden Menübäume müssen auf beiden Geräten gleich sein (bei unterschiedlichen Firmware-Versionen oder Geräte-Optionen nicht immer der Fall).
- Wenn die Konfiguration der Konfigurations-Synchronisation (Menüknoten etc.) geändert wird, nachdem der Cluster bereits gestartet wurde, muss der Cluster erneut gestartet werden.

2.20.2 1-Klick WLC High Availability Clustering-Assistent

Mit dem 1-Klick WLC High Availabilty Clustering-Assistenten konfigurieren Sie über LANconfig mehrere WLCs gleichzeitig unter den folgenden Voraussetzungen:

- Bei allen WLCs ist die WLC High Availability Clustering XL-Option aktiviert.
- Mindestens ein WLC ist vollständig konfiguriert. Das ist der Fall, wenn er bereits APs verwaltet.
- Mindestens ein WLC ist grundkonfiguriert (mindestens Name und IP-Adresse sind gesetzt).

Im Zweifelsfall starten Sie bei dem entsprechenden WLC den Erstkonfigurations-Assistenten.

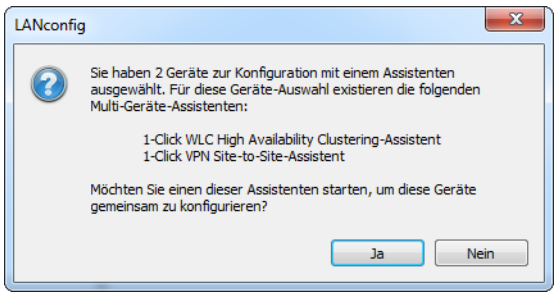
Alle WLCs des Clusters sind gleichberechtigt.

1. Wählen Sie in der Geräteliste die zwei WLCs aus, die Sie gemeinsam konfigurieren wollen.

   Sie haben zwei Möglichkeiten, den WLC-Clustering-Assistenten zu starten:

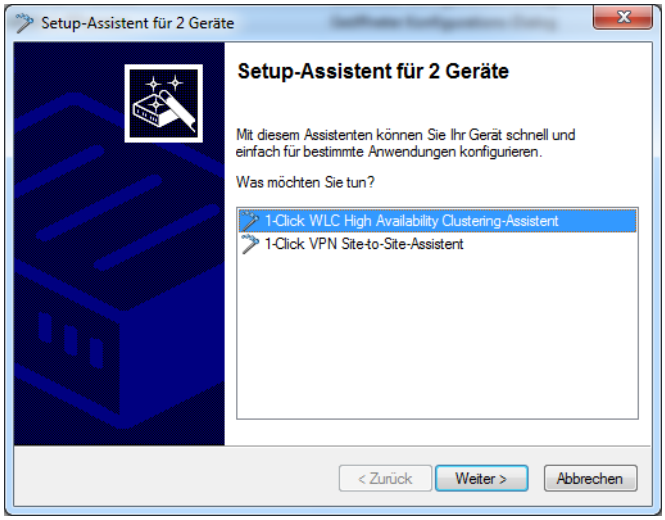
   - Ziehen Sie in der Geräteliste den unkonfigurierten WLC per Drag&Drop auf den konfigurierten WLC.
   - Markieren Sie in der Geräteliste beide WLCs und wählen Sie nach einem Rechtsklick darauf aus dem Kontextmenü den Punkt **Setup-Assistent**.

   LANconfig zeigt daraufhin die folgende Meldung:

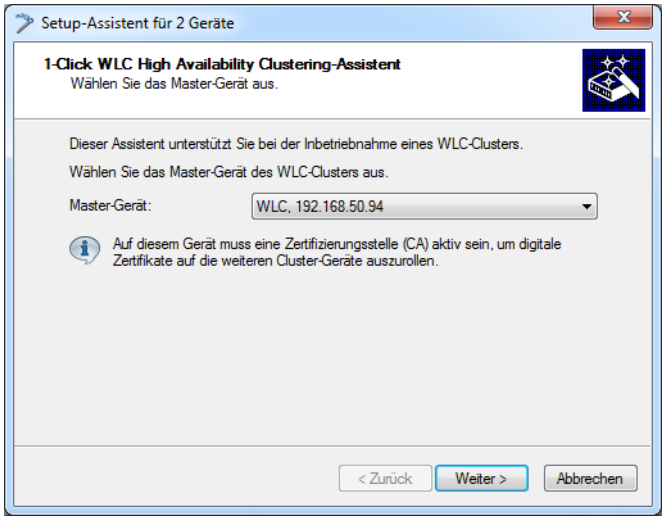


   Starten Sie den Setup-Assistenten mit einem Klick auf **Ja**. Der Setup-Assistent startet mit dem Auswahldialog für die Multi-Geräte-Assistenten.

2. Wählen Sie den „1-Klick WLC High Availability Clustering-Assistenten" aus und klicken Sie auf **Weiter**.



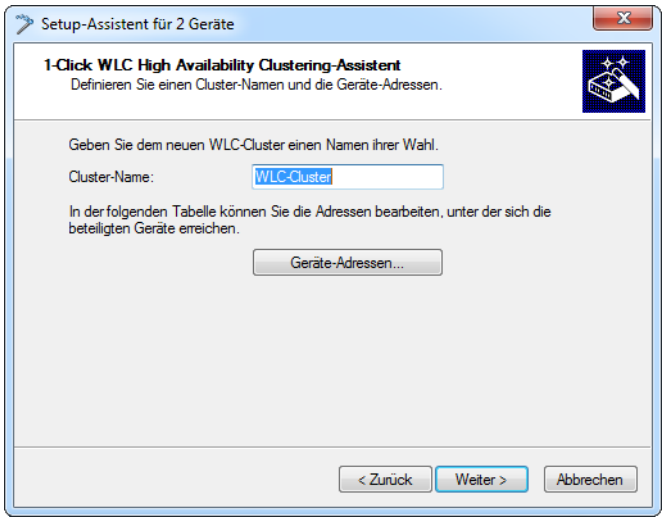
3. Wählen Sie das Master-Gerät aus und klicken Sie auf **Weiter**



Das Master-Gerät ist der vorkonfigurierte WLC. Der Setup-Assistent überträgt dessen Konfiguration nach dem Fertigstellen auf alle anderen ausgewählten WLCs.

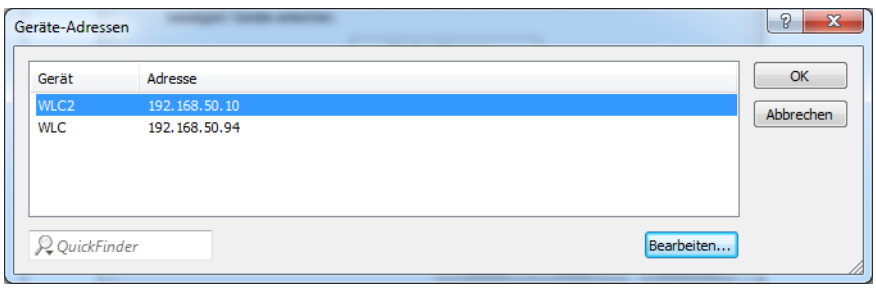
Diese Abfrage erscheint nicht, wenn Sie die Konfiguration per Drag&Drop auf einen anderen WLC übertragen. In diesem Fall verwendet der Setup-Assistent den „gezogenen" WLC automatisch als Master-Gerät.

4. Vergeben Sie eine Cluster-Bezeichnung und klicken Sie auf **Geräte-Adressen**.



Der Setup-Assistent gibt einen Cluster-Namen vor, den Sie jedoch verändern können.

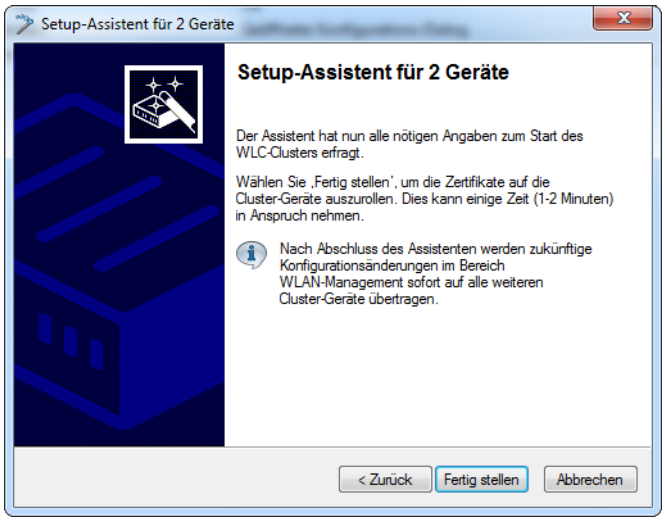
5. Tragen Sie die Geräte-Adressen aller WLCs des Clusters ein.



Standardmäßig trägt der Setup-Assistent hier die Geräte ein, die LANconfig erreicht. Nehmen Sie Änderungen vor, um z. B. Geräte einzutragen, die über VPN erreichbar sind.

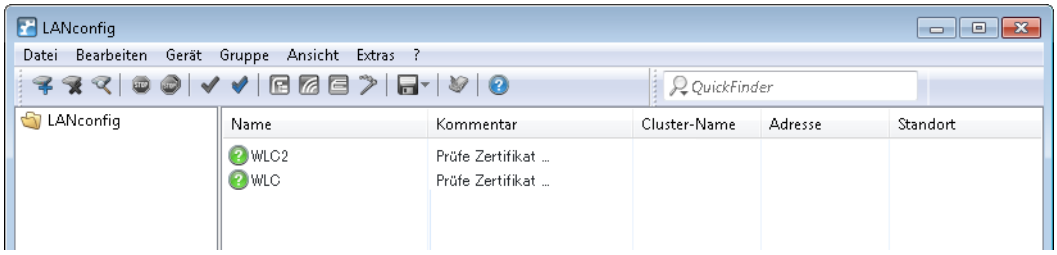
Klicken Sie auf **OK** und anschließend auf **Weiter**.

6. Mit einem Klick auf **Fertig stellen** schließen Sie den Setup-Assistenten ab.



Der Setup-Assistent lädt nun die Konfiguration des Master-Gerätes in die gewählten WLCs.

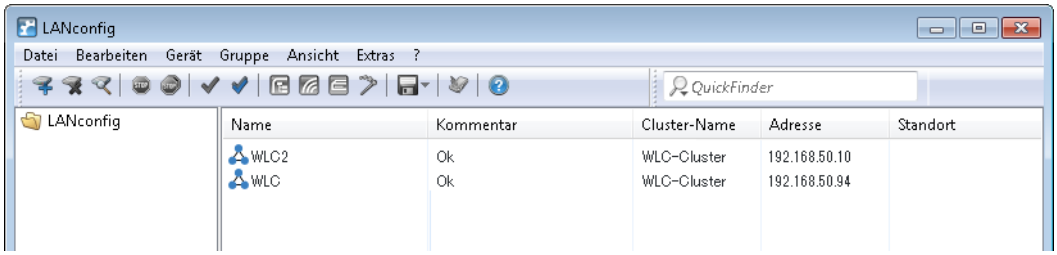
7. Die Geräteliste zeigt die WLCs wie folgt an:



Der Setup-Assistent hat auf allen WLCs den SCEP-Client für den Bezug eines Config-Syncs konfiguriert. LANconfig wartet nun, bis die Zertifikate für alle WLCs verfügbar sind.

Die Erstellung der Zertifikate kann bis zu einer Minute dauern.

8. Sobald die Zertifikate aller WLCs verfügbar sind, zeigt LANconfig für diese WLCs den Status „Ok" sowie das Cluster-Icon an und blendet den konfigurierten Cluster-Namen ein.



Config-Sync konfiguriert von nun an den kompletten Pfad **Setup** > **WLAN-Management** zwischen allen beteiligten Cluster-Mitgliedern. Konfigurationsänderungen, die auf einem der WLCs erfolgen, synchronisiert Config-Sync sofort auf alle anderen WLCs des Clusters.

Das Master-Gerät betreibt eine Master-CA, alle anderen WLCs betreiben eine Sub-CA dieser Master-CA. APs, die sich mit einem anderen als dem Master-WLC verbinden, erhalten bei Bedarf von diesen ein gültiges Zertifikat.

2.21 CPE WAN Management Protokoll (CWMP)

Über das CPE WAN Management Protokoll (CWMP) lassen sich Endgeräte mit einem entsprechenden Konfigurationsserver über eine WAN-Verbindung fernkonfigurieren. Die Kommunikation zwischen dem Gerät (Customer Premises Equipment, CPE) und dem Konfigurationsserver (Auto Configuration Server, ACS) erfolgt über SOAP/HTTP(S) in Form von Remote Procedure Calls (RPC). Im CWMP ist eine Vielzahl von RPCs festgelegt, von denen im LCOS die folgenden realisiert sind:

- GetRPCMethods
- SetParameterValues
- GetParameterValues
- GetParameterNames
- FactoryReset
- Reboot
- Download
  - Firmware-Update
  - Script-Download (*.lcs-Dateien)

Zusätzlich unterstützt LCOS die herstellerspezifischen RPCs:

- X_LANCOM_DE_Command
- X_LANCOM_DE_CommandResponse

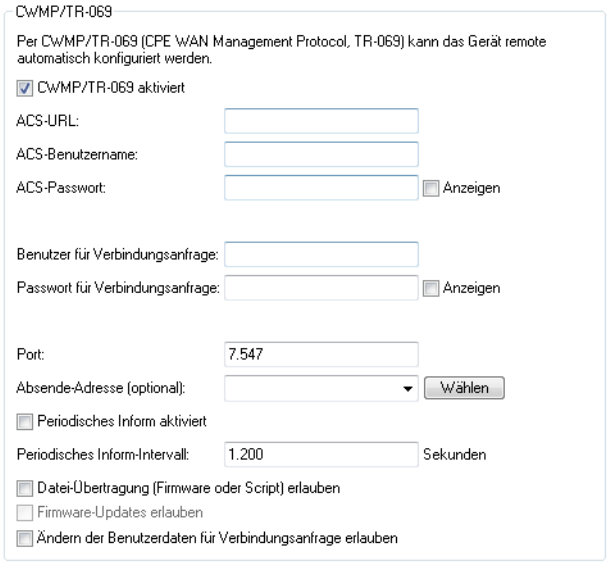
Weitere Informationen zu den Parametern der RPCs finden Sie im *Broadband-Forum*.

Die folgenden Authentifizierungsarten unterstützt das CPE gegenüber einem ACS:

- HTTP Basic
- HTTP Digest
- HTTPS durch Client-Zertifikat

2.21.1 CWMP mit LANconfig einrichten

In LANconfig konfigurieren Sie das CPE WAN Management Protokoll unter **Management** > **CWMP/TR-069**.



CWMP aktiviert

Aktiviert oder deaktiviert das CWMP.

ACS-URL

Bestimmen Sie hier die Adresse des ACS (Auto Configuration Server), mit dem sich das CPE (Customer Premises Equipment) verbindet. Die Eingabe der Adresse erfolgt im IPv4-, IPv6- oder FQDN-Format.

Erlaubt sind HTTP und HTTPS, wobei der Einsatz von HTTPS zu bevorzugen ist, da die Geräte ansonsten gerätespezifische Parameter wie Passwörter oder Zugangsdaten unverschlüsselt übertragen. Vor dem Einsatz von HTTPS müssen Sie das vertrauenswürdige Stammzertifikat zur Überprüfung der Serveridentität in das Gerät laden.

ACS-Benutzername

Vergeben Sie einen Benutzernamen, den das Gerät zur Verbindung mit dem ACS (Auto Configuration Server) verwendet.

ACS-Passwort

Vergeben Sie ein Passwort, das das Gerät zur Verbindung mit dem ACS (Auto Configuration Server) verwendet.

Benutzer für Verbindungsanfrage

Benennen Sie einen Benutzer, den der ACS (Auto Configuration Server) beim Verbindungs-Aufbau zu diesem Gerät verwenden soll.

Passwort für Verbindungsanfrage

Vergeben Sie ein Passwort, dass der ACS (Auto Configuration Server) für Verbindungsanfragen verwendet.

Port

Geben Sie den lokalen Port an, den der ACS (Auto Configuration Server, Auto-Konfigurations-Server) beim Verbindungsaufbau zu diesem Gerät verwendet.

Sofern Sie IPv6 verwenden, ist es erforderlich, in der IPv6-Firewall unter **Firewall/QoS** > **IPv6-Regeln** > **IPv6-Inbound-Regeln** zusätzlich den Zugriff auf den entsprechenden Port zu gewähren.

Absende-Adresse

Hier können Sie optional eine Absendeadresse konfigurieren, die statt der ansonsten automatisch für die Zieladresse gewählten Absendeadresse verwendet wird. Falls Sie z. B. Loopback-Adressen konfiguriert haben, können Sie diese hier als Absendeadresse angeben.

Sofern die hier eingestellte Absendeadresse eine Loopback-Adresse ist, verwendet das Gerät diese auch auf maskiert arbeitenden Gegenstellen unmaskiert.

Als Adresse akzeptiert das Gerät verschiedene Eingabeformate:

- Name des IP-Netzwerkes (ARF-Netz), dessen Adresse eingesetzt werden soll.
- "INT" für die Adresse des ersten Intranets.
- "DMZ" für die Adresse der ersten DMZ (Achtung: Wenn es eine Schnittstelle Namens "DMZ" gibt, dann nimmt das Gerät deren Adresse).
- LB0 ... LBF für eine der 16 Loopback-Adressen oder deren Name.
- Eine beliebige IP-Adresse in der Form x.x.x.x.

Periodisches Inform aktiviert

Aktiviert oder deaktiviert das Senden von periodischen Inform-Nachrichten vom Gerät zum ACS (Auto Configuration Server).

Periodisches Inform-Intervall

Dies ist das Intervall in Sekunden zwischen zwei durch das Gerät zum ACS (Auto Configuration Server) eingeleiteten periodischen Inform-Nachrichten. Der ACS erfragt daraufhin weitere Informationen vom Gerät.

Der Standard-Wert beträgt 1200 Sekunden, d. h. 20 Minuten. Wählen Sie diesen Wert nicht zu klein, da Inform-Nachrichten einen erhöhten Netzwerk-Verkehr verursachen. Das Intervall startet nicht, bevor Gerät und Server alle Informationen ausgetauscht haben.

Datei-Übertragung (Firmware oder Script) erlauben

Dieser Schalter erlaubt die Übertragung einer Firmware oder einer Skript-Datei vom ACS (Auto Configuration Server) zu diesem Gerät.

Firmware-Updates erlauben

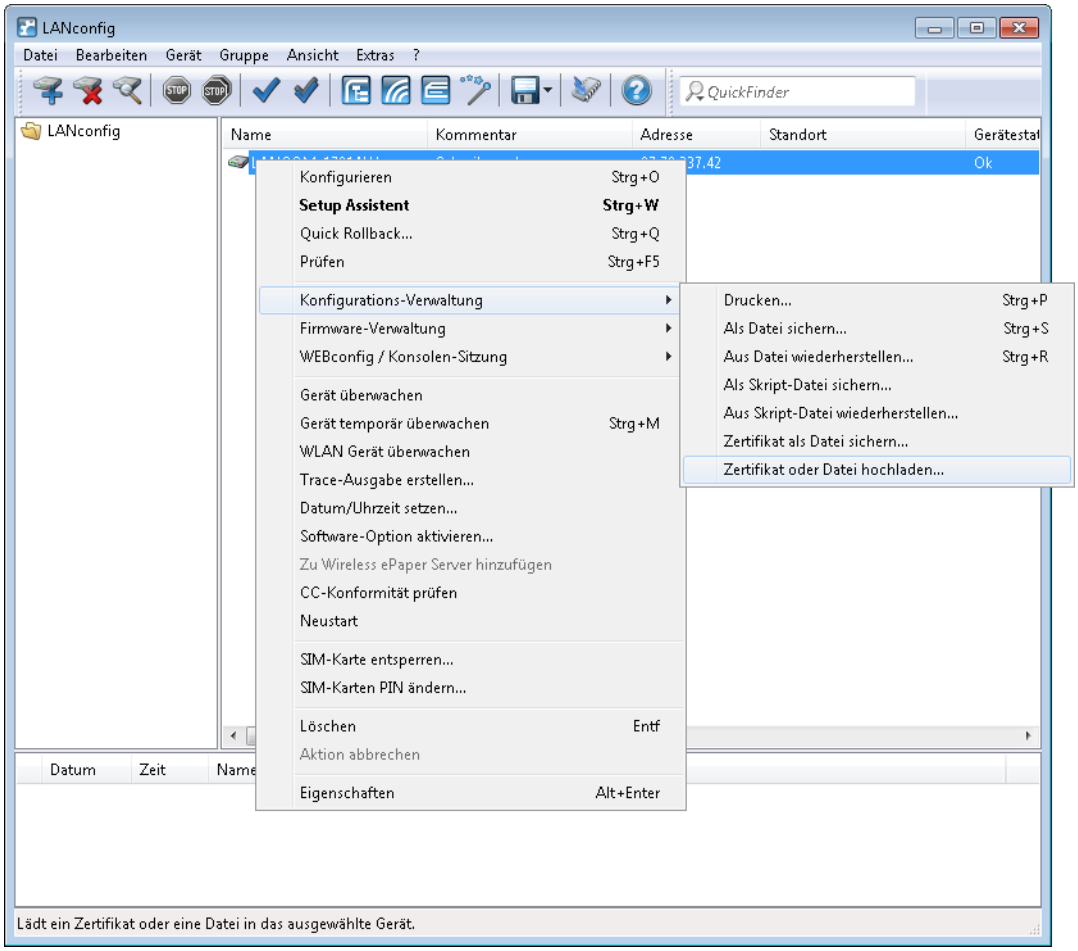
Dieser Schalter erlaubt dem ACS (Auto Configuration Server), Firmware-Änderungen am Gerät vorzunehmen.

Ändern der Benutzerdaten für Verbindungsanfrage erlauben

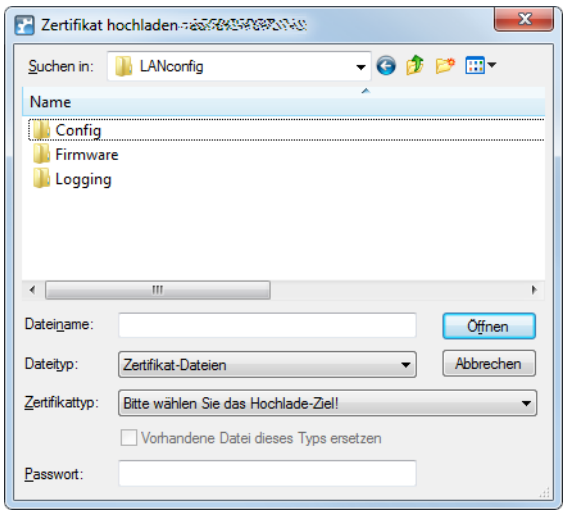
Dieser Schalter erlaubt dem ACS (Auto Configuration Server), den Geräte-Administrator zu wechseln oder den Namen und das Passwort des Geräte-Administrators, den er zur Verbindung mit dem Gerät verwendet, zu ändern.

Bei der Verwendung von HTTPS in der ACS-URL validiert das CPE das ACS-Zertifikat. Dazu speichern Sie zuvor das CWMP Root-CA-Zertifikat im CPE. Kann das CPE das Serverzertifikat nicht gegen das vorhandene Root-CA-Zertifikat validieren, so lehnt es die Verbindung ab. Der Zertifikatsupload erfolgt entweder durch LANconfig oder WEBconfig. In LANconfig gehen Sie dazu wie folgt vor:

1. Rechtsklicken Sie in der Geräteübersicht das entsprechende Gerät und wählen Sie unter **Konfigurationsverwaltung** den Menüpunkt **Zertifikat oder Datei hochladen**.



2. Wählen Sie im folgenden Dialog als Zertifikattyp „CWMP-Root-CA-Zertifikat“ aus und klicken Sie auf **Öffnen**.



Bei der Verwendung von SSL/TLS zur CPE-Authentifizierung laden Sie das Client-Zertifikat und den privaten Schlüssel per PKCS#12-Datei (CWMP-Container als PKCS#12-Datei) in das CPE.

2.21.2 Gerätekonfiguration über CWMP

Alle CWMP-Parameter konfigurieren Sie auf der Konsole entweder durch eine Skript-Datei oder durch das herstellerspezifische RPC `X_LANCOM_DE_Command`.

Konfiguration per Skript

Über das CWMP-Download-Kommando `<cwmp:download>` konfigurieren Sie das Gerät per Skipt-Datei (`*.lcs`). Filetype ist hierbei `3 Vendor Configuration File` und als URL geben Sie die Adresse des Servers an, auf dem das Konfigurationsskript gespeichert ist.

LANconfig-Dateien mit Format *.lcf werden nicht unterstützt.

Konfiguration per herstellerspezifischem RPC `X_LANCOM_DE_Command`

Die Funktion `X_LANCOM_DE_Command` ist wie folgt definiert:

Anfrage

```
<cwmp:X_LANCOM_DE_Command>
<Command> CLI-Kommando </Command>
</cwmp:X_LANCOM_DE_Command>
```

Antwort

```
<cwmp:X_LANCOM_DE_CommandResponse>
<Status>1</Status>
<Result>1</Result>
</cwmp:X_LANCOM_DE_CommandResponse>
```

Das folgende Beispiel setzt die IPv4-Adresse des Gerätes auf dem „INTRANET“:

```
<cwmp:X_LANCOM_DE_Command>
<Command>set /Setup/TCP-IP/Network-list/INTRANET {IP-address} 192.168.80.1</Command>
</cwmp:X_LANCOM_DE_Command>
```

Aufgrund der asynchronen Ausführung der Konsolen-Befehle meldet `X_LANCOM_DE_Command` immer eine erfolgreiche Ausführung des Kommandos zurück, unabhängig davon, ob der Befehl korrekt ausgeführt werden konnte oder nicht. Die erfolgreiche Ausführung erfolgt durch Auslesen des Config-Status unter **Status** > **Config**.

Zur Überprüfung des Konfigurationsstatus können Sie die folgenden CWMP-Parameter vor oder nach Anwendung des Skripts oder von `X_LANCOM_DE_Command` auslesen:

- InternetGatewayDevice.DeviceInfo.X_LANCOM_DE_ConfigVersion
- InternetGatewayDevice.DeviceInfo.X_LANCOM_DE_LastScriptComment
- InternetGatewayDevice.DeviceInfo.X_LANCOM_DE_LastScriptErrorLine
- InternetGatewayDevice.DeviceInfo.X_LANCOM_DE_LastScriptSuccessful

Die Werte entsprechen den Status-Werten unter **Status** > **Config**.

Konfiguration per herstellerspezifischem RPC `X_LANCOM_DE_CommandResponse`

Die Funktion `X_LANCOM_DE_CommandResponse` wird synchron ausgeführt und liefert einen Rückgabewert. Sie ist wie folgt definiert:

Anfrage

```
<cwmp:X_LANCOM_DE_Command_Response>
  <Command>ls /Status/Current-Time</Command>
</cwmp:X_LANCOM_DE_Command_Response>
```

Antwort

```
<cwmp:X_LANCOM_DE_Command_ResponseResponse>
  <Status xsi:type="xsi:unsignedInt">1</Status>
  <Result xsi:type="xsi:string">Current-Time  INFO:    11/30/2017 09:54:49</Result>
</cwmp:X_LANCOM_DE_Command_ResponseResponse>
```

Die Funktion liefert folgende Rückgabewerte:

1. Parameter: `<Status type="xsd:unsignedInt">[1/0]</Status>`

   1 = keine Fehler, 0 = Fehler bei der Ausführung

2. Parameter: `<Result type="xsd:string">[Output]</Result>`

   Output = Ausgabe entsprechend Konsole (max. 2048 Zeichen, mehr Zeichen werden abgeschnitten)

2.22 LANCOM Battery Pack

Das LANCOM Battery Pack ist eine Notstromversorgung zum Weiterbetrieb von bis zu zwei LANCOM Geräten und stellt eine effiziente Notstromversorgung von geschäftskritischen LANCOM Netzwerkkomponenten dar.

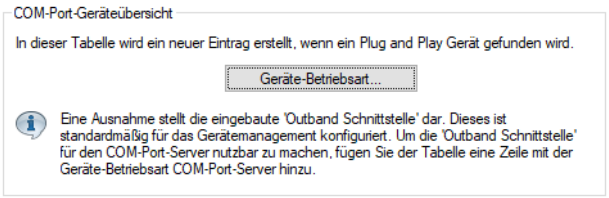
Im Falle eines Stromausfalls werden maximal zwei angeschlossene LANCOM Router oder APs mindestens zwei Stunden lang mit Strom versorgt. So bleibt an IP-basierten Amtsanschlüssen auch in Notfällen der Betrieb von an LANCOM Routern angeschlossenen analogen Telefonen oder Gefahrenmeldeanlagen gewährleistet.

2.22.1 Konfiguration mit LANconfig

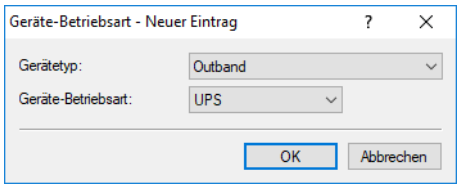
Die Überwachung des angeschlossenen Battery Packs erfolgt über die serielle Schnittstelle (COM-Port) Ihres LANCOM Gerätes. Um den Zustand Ihres Battery Packs kontrollieren zu können, gehen Sie wie folgt vor:

Konfiguration des COM-Ports

Konfigurieren Sie die Gerätebetriebsart über **Sonstige Dienste** > **COM-Ports**. Klicken Sie auf die Schaltfläche **Geräte-Betriebsart** und fügen Sie der Tabelle einen neuen Eintrag hinzu oder bearbeiten Sie einen bestehenden Eintrag.

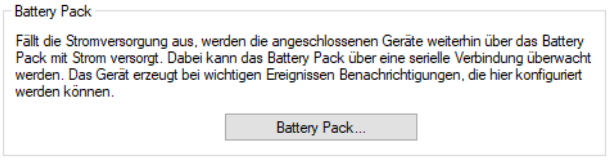


Wählen Sie für den Betrieb als Gerätetyp die Einstellung "Outband" und als Gerätebetriebsart "UPS" (**U**ninterruptable **P**ower **S**upply) aus. Diese Betriebsart stellt sicher, dass der Status des angeschlossenen Battery Packs abgefragt werden kann.

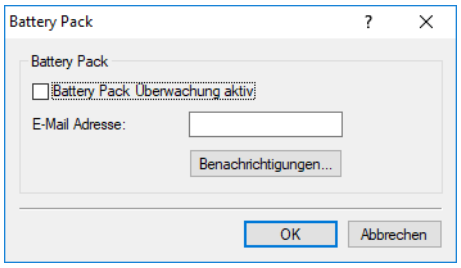


Konfiguration der Battery Pack-Überwachung

Sie konfigurieren die Überwachung des Battery Packs über **Meldungen** > **Allgemein** im Abschnitt "Battery Pack".



Klicken Sie auf die Schaltfläche **Battery Pack** und aktivieren Sie die Checkbox **Battery Pack-Überwachung aktiv**. Definieren Sie eine gültige E-Mail Adresse für die Übermittlung von Statusmeldungen.



Battery Pack-Überwachung aktiv

Aktivieren Sie hier die Statusüberwachung des seriell verbundenen Battery Packs.

Bitte beachten Sie, dass für eine Überwachung die Gerätebetriebsart der Outband-Schnittstelle im Bereich **Sonstige Dienste** > **COM-Ports** > **Geräte-Betriebsart** auf "UPS" konfiguriert und Ihr Gerät über das Outbandkabel mit dem Battery Pack verbunden sein muss.

E-Mail-Adresse

Bei kritischen Ereignissen wird eine Nachricht an die hier konfigurierte E-Mail-Adresse versendet, damit der Geräteadministrator rechtzeitig reagieren kann.

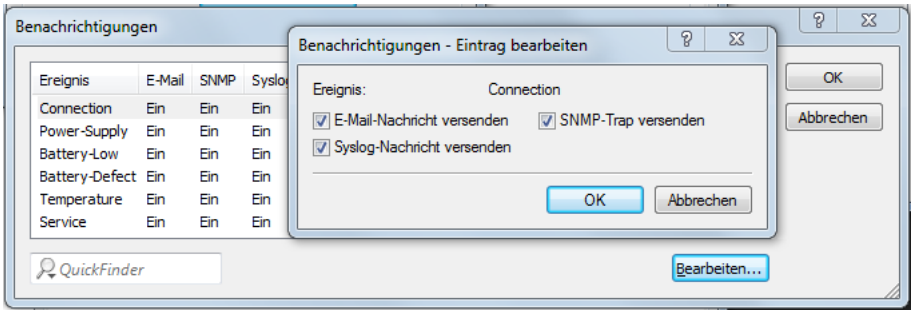
Bitte beachten Sie, dass für einen erfolgreichen E-Mail-Versand der Bereich **Meldungen** > **SMTP-Konto** konfiguriert sein muss.

Benachrichtigungen

Legen Sie die Benachrichtigungseinstellungen fest.

Benachrichtigungen konfigurieren

Definieren Sie, welche Benachrichtenteinstellungen für kritische Ereignisse gelten sollen.



E-Mail-Nachricht versenden

Tritt dieses Ereignis ein, wird der Administrator via E-Mail benachrichtigt. Die E-Mail wird dabei an die Adresse geschickt, die unter **Meldungen** > **Allgemein** > **Battery Pack** konfiguriert ist.

SNMP-Trap versenden

Tritt dieses Ereignis ein, wird der Administrator via SNMP benachrichtigt. Die SNMP-Meldung wird dabei an den SNMP-Server geschickt, der unter **Management** > **Admin** > **SNMP-Einstellungen** > **Empfängeradressen** konfiguriert ist.

SYSLOG-Nachricht versenden

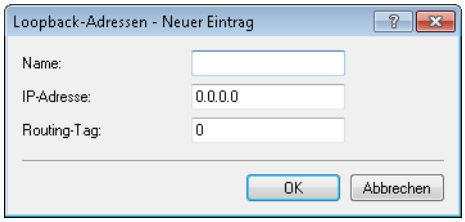
Tritt dieses Ereignis ein, dann wird der Administrator via SYSLOG benachrichtigt. Die SYSLOG-Meldung wird dabei an den SYSLOG-Server geschickt, der unter **Meldungen** > **Allgemein** > **SYSLOG-Server** konfiguriert ist.

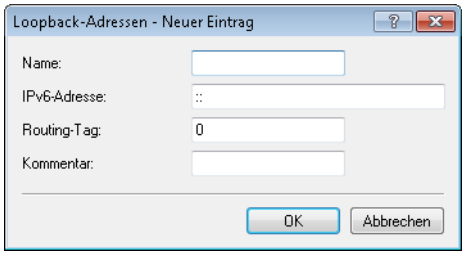
2.23 Benannte Loopback-Adressen einrichten

Ihrem Gerät lassen sich bis zu 16 IPv4- bzw 8 IPv6-Loopback-Adressen zuweisen, unter denen sich das Gerät (z. B. zum Management größerer Netz-Strukturen) ansprechen lässt. Um die Loopback-Adressen für bestimmte Netzwerke (z. B. im Zusammenhang mit "Advanced Routing and Forwarding") zu nutzen, ordnen Sie den Adressen ausgewählte Routing-Tags zu. Zur leichteren Identifizierung in anderen Konfigurationsteilen erhalten die Loopback-Adressen außerdem einen frei wählbaren Namen.

Die folgenden Schritte zeigen Ihnen, wie Sie eine Loopback-Adresse einrichten.

1. Starten Sie LANconfig und öffnen Sie den Konfigurationsdialog für das Gerät.
2. Wechseln Sie in den Dialog **IPv4** > **Allgemein** > **Loopback-Adressen** bzw. **IPv6** > **Allgemein** > **Loopback-Adressen** und klicken Sie **Hinzufügen**.





3. Geben Sie im Eingabefeld **Name** einen frei wählbaren Namen für die Loopback-Adresse ein, z. B. `LOOPBACK_1`.
4. Tragen Sie im Eingabefeld **IP-Adresse** bzw. **IPv6-Adresse** die Loopback-Adresse ein, die dieses Gerät erhalten soll, z. B. `10.0.0.99` für einen IPv4-Adresse bzw. `::1` für eine IPv6-Adresse.

   Das Gerät sieht jede dieser Adressen als eigene Adresse an und verhält sich, als hätte es das Paket auf dem (W)LAN empfangen. Dies gilt insbesondere auf maskierten Verbindungen. Antworten auf Pakete an eine Loopback-Adresse werden **nicht** maskiert!
5. Geben Sie im Eingabefeld **Routing-Tag** ein optionales Routing-Tag für die Loopback-Adresse an.

Loopback-Adressen mit dem Routing-Tag '0' (ungetaggt) sind in allen Netzen sichtbar. Loopback-Adressen mit einem anderen Routing-Tag sind nur in Netzen mit dem gleichen Routing-Tag sichtbar.

6. Bei IPv6-Loopback-Adressen können Sie im Feld **Kommentar** zusätzlich einen Kommentar angeben.

2.24 Konfigurationsmöglichkeit für IPv4/IPv6-Auflösung bei DNS-Auflösungen

Bei Parametern, bei denen DNS-Hostnamen konfiguriert werden können, wird optional mit einem Schalter übergeben, wie IPv4 bzw. IPv6 beim Verbindungsaufbau priorisiert werden sollen.

Konkrete Anwendungsfälle sind beispielsweise die Verwendung von DNS-Namen bei VPN-Verbindungen oder SIP-Registraren, wo gesteuert werden soll, ob die Verbindung über IPv4 oder IPv6 aufgebaut werden soll.

Beispiel 1: Wird der Hostname `vpn.example.org` auf eine IPv4- und eine IPv6-Adresse aufgelöst, so bevorzugt ein Host normalerweise IPv6 vor IPv4. Soll nun aber IPv4 verwendet werden, so kann dies durch Anhängen von `?4` an den Hostnamen gesteuert werden, d. h. hier: `vpn.example.org?4`.

Beispiel 2: Soll beim CLI-Ping IPv4 bei einem IPv4/IPv6 DNS-Hostnamen bevorzugt werden, so kann die folgende Syntax verwendet werden: `ping www.example.org?4`.

Die folgenden Suffixe sind erlaubt:

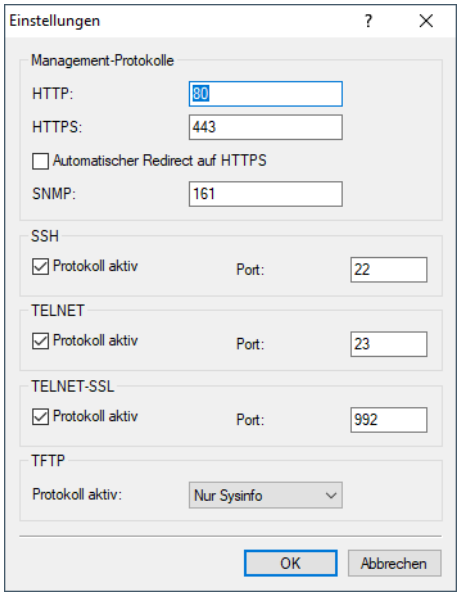
- `?4`: Auflösung nur über IPv4
- `?6`: Auflösung nur über IPv6
- `?46`: IPv4 vor IPv6 bevorzugen, d. h. falls IPv4 nicht aufgelöst werden kann, so wird IPv6 verwendet.
- `?64`: IPv6 vor IPv4 bevorzugen, d. h. falls IPv6 nicht aufgelöst werden kann, so wird IPv4 verwendet.

2.25 Management-Ports für den Gerätezugriff anpassen

Sie haben im LANconfig die Möglichkeit, die Portnummern für die Management-Protokolle zu ändern.

1. Starten Sie LANconfig und öffnen Sie den Konfigurationsdialog für das Gerät.
2. Wechseln Sie in den Dialog **Management** > **Admin** > **Management-Protokolle** und klicken Sie dort auf **Einstellungen**.

3. Geben Sie die Portnummern für die gewünschten Management-Protokolle ein.



4. Schließen Sie alle geöffneten Dialoge durch einen Klick auf **OK**.

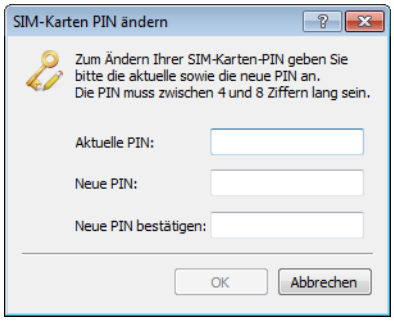
LANconfig schreibt die eingegebene Konfiguration zurück auf das Gerät.

2.26 Ändern der SIM-Karten-PIN

Bei Geräten mit Mobilfunkmodem haben Sie über LANconfig die Möglichkeit, die PIN der SIM-Karte zu ändern. Die Änderung kann einfach vollzogen werden, indem Sie sowohl die alte PIN als auch die neue PIN eingeben. Zur Sicherheit verlangt LANconfig zusätzlich eine Bestätigung der neuen PIN. Alternativ haben Sie auch die Möglichkeit, die Änderung auf der Kommandozeile über die Aktion **PIN-Aendern** durchzuführen.

Die nachfolgenden Schritte beschreiben den Änderungsweg in LANconfig.

1. Wählen Sie in der Geräteübersicht von LANconfig das Gerät aus, dessen PIN Sie ändern wollen.
2. Wählen Sie über die Menüleiste **Gerät** > **SIM-Karten PIN ändern**. Ein neuer Dialog öffnet sich.



3. Geben Sie die bisher aktuelle PIN und die neue PIN ein. Bestätigen Sie die neue PIN durch wiederholte Eingabe.
4. Klicken Sie **OK**, um die Änderung zu übernehmen.

3 LANtools

Das Gerät unterstützt verschiedene Mittel (sprich Software) und Wege (in Form von Kommunikationszugängen) für die Konfiguration. Die Situationen, in denen konfiguriert wird, unterscheiden sich ebenso wie die persönlichen Ansprüche und Vorlieben der Ausführenden. Das Gerät verfügt daher über ein breites Angebot von Konfigurationsmöglichkeiten.

Eine Möglichkeit ist die Konfiguration mit der menügeführten und übersichtlichen Software **LANconfig**, mit der sich nahezu alle relevanten Parameter des Geräts einstellen lassen.

Der aktuelle Zustand des Geräts, der Verbindungen und der Status-Werte wird übersichtlich im **LANmonitor** angezeigt. Bei WLAN-Geräten sind darüber hinaus noch weitere Informationen über die drahtlosen Netze sowie die verbundenen Clients über den **WLANmonitor** abrufbar.

Mit **LANtracer** haben Sie die Möglichkeit, erweiterte Trace-Funktionen auszuführen, mit denen Sie bestimmte Informationen (wie z. B. Statuswerte und Funktionsmeldungen) einmal abrufen oder über einen längeren Zeitraum gezielt überwachen. Die dabei erzeugten Trace-Daten können Sie z. B. zur Protokollierung oder Fehlerdiagnose einsetzen.

Die folgenden Abschnitte behandeln ausführlich die Bedienung der angesprochenen Anwendungen.

Vorraussetzung für die einzelnen Anwendungen der LANtools ist ein Konfigurationsrechner mit einem Windows-Betriebssystem.

3.1 LANconfig – Geräte konfigurieren

Von der komfortablen Inbetriebnahme eines Einzelplatzgerätes mit den einfach zu bedienenden Installationsassistenten bis zum ganzheitlichen Management mit Firmware- und Konfigurationsverteilung größerer Installationen reicht das Anwendungsspektrum von LANconfig.

Basisfunktionen

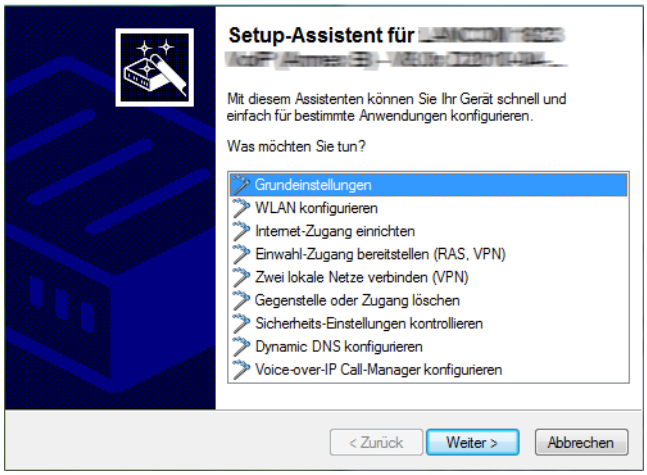
- Automatisches Erkennen von neuen, unkonfigurierten Geräten
- (Fern-)Konfiguration von Geräten über IP-Adresse, URL oder über die serielle Schnittstelle
- Integration von Telnet-, SSH-, HTTPS- und TFTP-Konfiguration
- Kontext-basiertes Hilfesystem zu den Konfigurations-Parametern
- In allen Installationsschritten bieten die Assistenten angepasste Eingabemasken
- Einrichtung von Backup-Verbindungen

Management von größeren Installationen

- Gruppenbildung
- Zentrale Firmware-Verteilung (Multi-Tasking, auch parallel mit mehreren DFÜ-Verbindungen)
- Simultankonfiguration mehrerer Geräte
- Verteilen von Konfigurations-Scripten
- WLAN-Gruppenkonfiguration
- Logging aller Aktionen
- Erstellung von neuen "Offline"-Konfigurationen für alle Geräte und LCOS-Versionen

3.1.1 LANconfig starten

Starten Sie LANconfig, z. B. mit einem Doppelklick auf das Desktop-Symbol. LANconfig sucht nun automatisch im lokalen Netz nach Geräten. Wird dabei ein noch nicht konfiguriertes Gerät im lokalen Netz gefunden, startet LANconfig selbstständig den Setup-Assistenten.



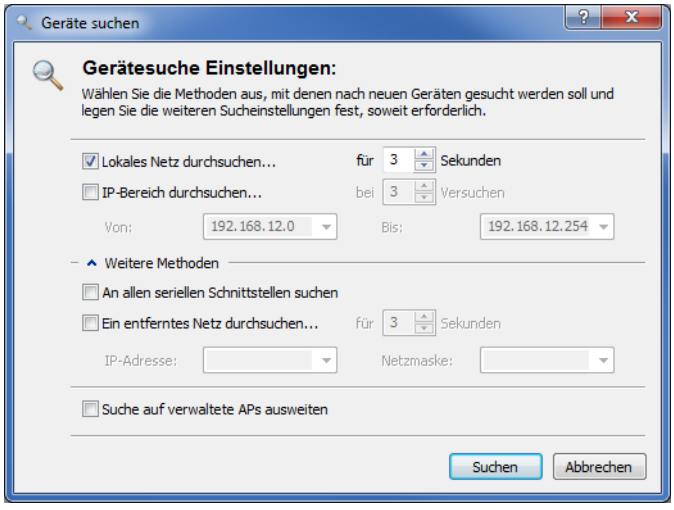
Eine aktivierte "Internetverbindungsfirewall" oder eine andere "Personal Firewall" auf dem Konfigurationsrechner kann dazu führen, dass LANconfig neue Geräte im LAN nicht findet. Deaktivieren Sie ggf. die Firewall für die Dauer der Konfiguration, wenn die unkonfigurierten Geräte nicht gefunden werden.

Ihr Gerät verfügt über eine umfangreiche eingebaute Firewall. Diese schützt Ihre Rechner auch dann, wenn keine weitere Firewall auf den Rechnern selbst – wie die "Internetverbindungsfirewall" – eingeschaltet ist.

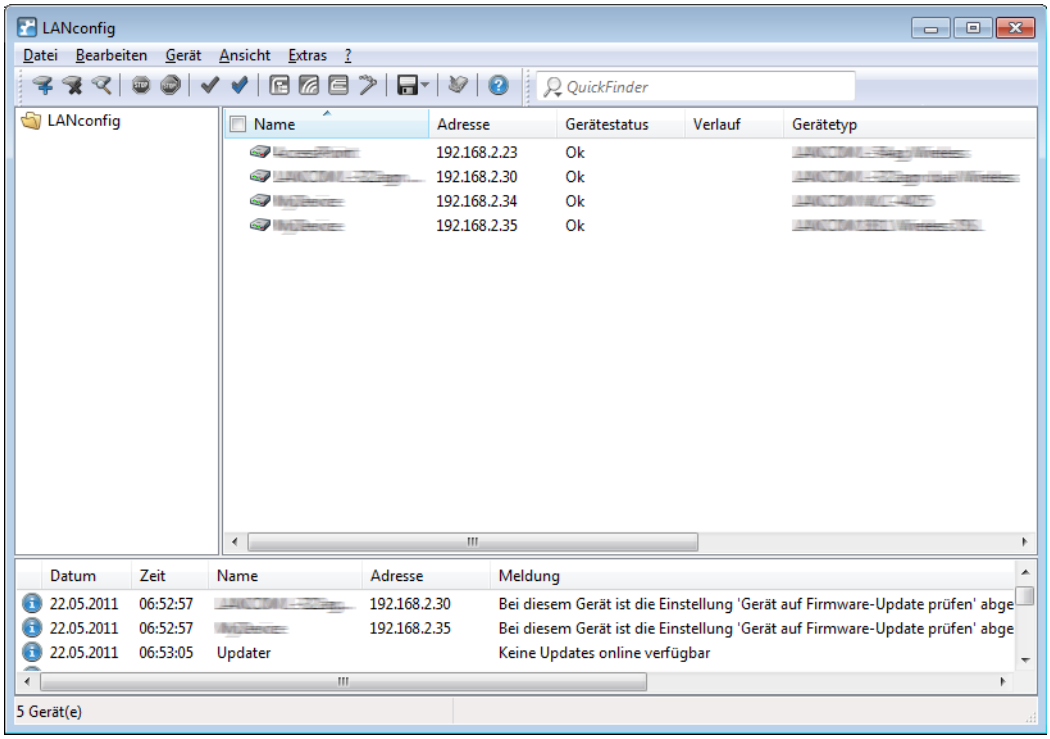
LANconfig kann beim Start des Betriebssystems automatisch geladen werden. Näheres dazu erfahren Sie im Kapitel *Applikation* auf Seite 237.

Neue Geräte suchen

Um die Suche eines neuen Geräts manuell einzuleiten, klicken Sie auf die Schaltfläche**Geräte suchen** ( )oder rufen den Befehl über **Datei** > **Geräte suchen** suchen auf. LANconfig erkundigt sich dann, wo es suchen soll. Um weitere Einstellung der Suche vorzunehmen, klicken Sie auf **Extras** > **Optionen** und wählen Menüpunkt **Start** aus.



Sobald LANconfig mit der Suche fertig ist, zeigt es in der Liste alle gefundenen Geräte mit Namen, evtl. einer Beschreibung, der IP-Adresse und dem Status an.



Ein Klick auf die Schaltfläche **Konfigurieren** ( ) oder den Menüeintrag **Gerät** > **Konfigurieren** liest die aktuellen Einstellungen aus dem Gerät aus und zeigt die allgemeinen Geräteinformationen an. Ein Doppelklick auf den Geräteeintrag öffnet wahlweise den Konfigurations-Assistenten oder direkt die Konfiguration des Gerätes.

Die eingebaute Hilfe-Funktion

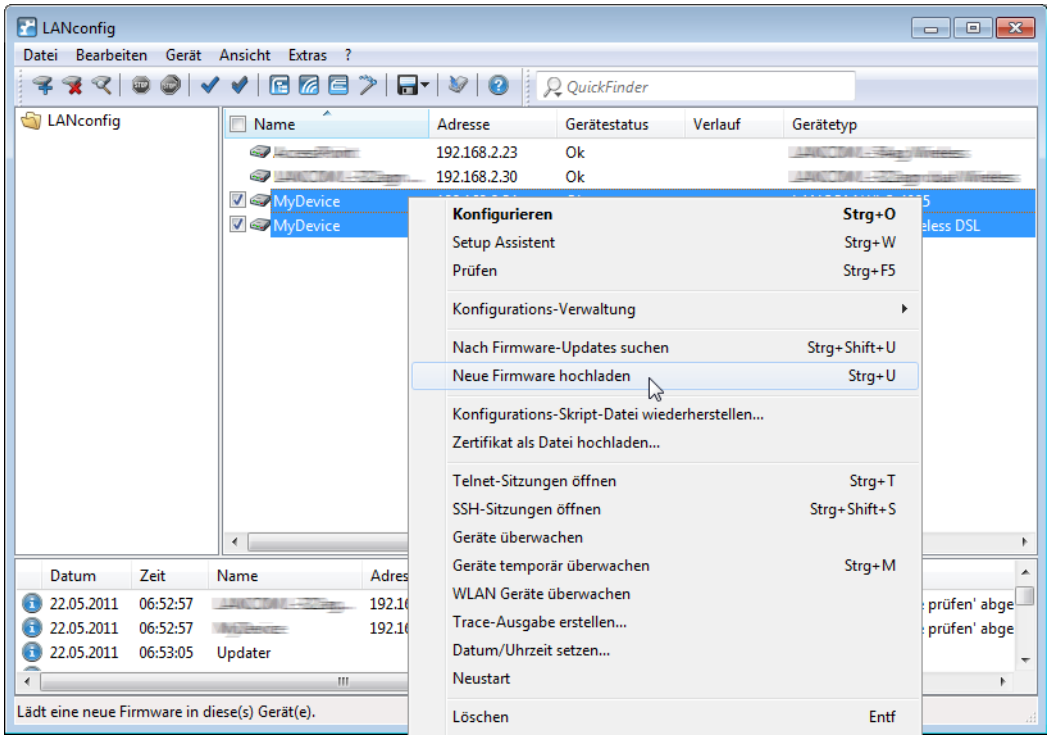
Die weitere Bedienung des Programms erklärt sich selbst bzw. über die Online-Hilfe. Indem Sie in einem Dialog-Fenster auf das Fragezeichen-Symbol ( ) oben rechts und anschließend auf eine Dialogabschnitt klicken, rufen Sie die kontextsensitive Hilfe auf, um weiterführende Informationen zu einer Einstellung zu erhalten. Alternativ genügt auch ein Rechtsklick auf den zu klärenden Dialogabschnitt.

Mehrfachauswahl

Mit LANconfig können mehrere Geräte gleichzeitig komfortabel (fern-)gewartet werden. Um mehrerer Geräte auszuwählen, haben Sie folgende Möglichkeiten:

- Ziehen Sie mit gedrückter Maustaste einen Auswahlrahmen über mehrere Geräte.
- Markieren Sie mehrere untereinander stehende Geräte mit gedrückter Shift-Taste und einem Klick auf das erste und das letzte Gerät der Liste.
- Markieren Sie beliebige Geräte mit gedrückter Strg-Taste und einem Klick auf die gewünschten Geräte.
- Aktivieren Sie die Option **Ansicht** > **Kontrollkästchen** und wählen Sie die Geräte über die entsprechenden Kontrollkästchen an.

LANconfig führt dann alle Aktionen für die ausgewählten Geräte nacheinander durch. So können Sie z. B. gleichzeitg für mehrere Geräte neue Firmwares hochladen.



Zur bequemen Verwaltung lassen sich Geräte zu Gruppen zusammenfassen. Dazu muss die Ansicht **Verzeichnisbaum** aktiviert sein. Im Verzeichnisbaum lassen sich neue Ordner über das Kontextmenü oder durch Auswahl von **Datei** > **Neuer Ordner** anlegen. Anschließend können Sie die Geräte durch einfaches Verschieben per 'drag und drop' in die gewünschten Ordner gruppieren.

In der Mehrgeräte-Konfiguration zeigt LANconfig nur die für die Mehrgeräte-Konfiguration geeigneten Eingabefelder an, z. B. bei Access Points die MAC Access-Control-Liste.

3.1.2 Arbeiten mit LANconfig

LANconfig bietet zahlreiche Funktionen, mit denen Sie die Arbeitsumgebung an Ihre speziellen Anforderungen anpassen können. Der Quickfinder bringt Sie schnell zu der gesuchten Einstellung; das Software-Update für die LANtools hält Ihre Anwendung auf Wunsch automatisch aktuell.

3.1.2.1 Benutzerspezifische Einstellungen für LANconfig

Die Progammeinstellungen von LANconfig werden beim Beenden des Programms in der Datei 'lanconf.ini' im Programmverzeichnis gespeichert. Dazu gehören z. B. die angezeigten Geräte, die Ordnerstruktur, die derzeit gewählte Sprache etc. Beim Programmstart liest LANconfig diese ini-Datei ein und stellt den vorherigen Zustand der Software wieder her. Zum Speichern der ini-Datei benötigt der angemeldete Benutzer Schreibrechte in dem Programmverzeichnis.

Alternativ zum Programmverzeichnis kann LANconfig die ini-Datei auch von einem anderen Pfad laden. Dies kann z. B. das Benutzerverzeichnis des aktuellen Benutzers oder ein beliebiger anderer Speicherort sein:

- Mit der Auswahl des Benutzerverzeichnisses können auch Benutzer ohne Schreibrechte für das Programmverzeichnis ihre persönlichen Einstellungen speichern.
- Mit der Auswahl eines beliebigen anderen Speicherortes können Sie die Programmeinstellungen komfortabel in andere LANconfig-Installationen übertragen oder über eine Netzwerkressource für mehrere Benutzer zentral verwalten.

Sie konfigurieren den Speicherort der Programmeinstellung im Dialog **Extras** > **Optionen** > **Applikation**. Lesen Sie dazu auch das Kapitel *Applikation* auf Seite 237.

3.1.2.2 Sprache der grafischen Oberfläche umschalten

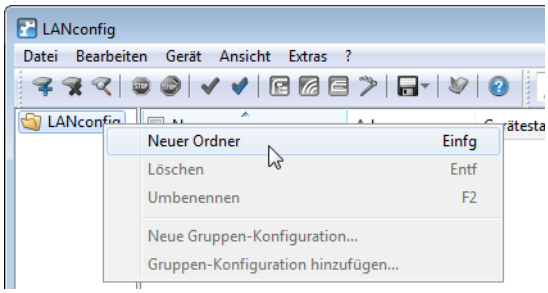
Die Sprache für die grafische Oberfläche von LANconfig können Sie unter **Extras** > **Optionen** > **Applikation** wahlweise auf **Deutsch**, **Englisch** oder **Spanisch** einstellen.

3.1.2.3 Verzeichnisbäume zur Organisation nutzen

LANconfig erlaubt mit dem Verzeichnisbaum die übersichtliche Verwaltung einer Vielzahl von Geräten. Für jedes Projekt oder jeden Kunden können Sie einen eigenen Ordner anlegen, in dem Sie die entsprechenden Geräte organisieren:

- Einen neuen Ordner legen Sie mit einem rechten Mausklick auf das übergeordnete Verzeichnis über den Kontextmenü-Eintrag **Neuer Ordner** an. Alternativ können Sie auch auf **Datei** > **Neuer Ordner** im Anwendungsmenü klicken.
- Die einzelnen Geräte lassen sich dann via 'drag and drop' aus der Liste mit der Maus in den entsprechenden Ordner ziehen. Auch das Verschieben der Geräte in einen anderen Ordner erfolgt auf diese Weise.

Die Zuordnung von einem Gerät zu einem bestimmten Ordner bezieht sich nur auf die Anzeige im LANconfig. Die Organisation der Ordner hat keine Auswirkung auf die Konfiguration der Geräte.

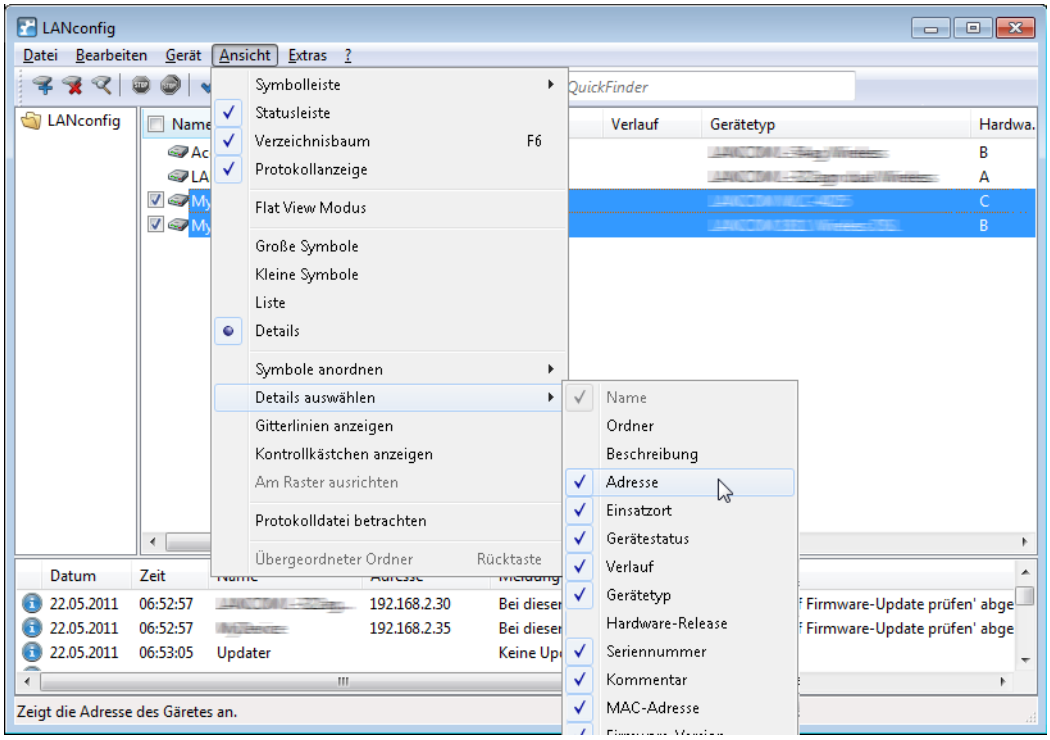


Die Ordnerstruktur am linken Rand des LANconfig-Fensters kann mit der Funktionstaste F6 oder über das Menü **Ansicht** > **Verzeichnisbaum** ein- und ausgeschaltet werden.

3.1.2.4 Bessere Übersicht in LANconfig durch mehr Spalten

Für eine bessere und schnellere Übersicht und Orientierung auch in großen Projekten können Sie in LANconfig die Spalten mit gerätebezogenen Informationen einzeln ein- und ausblenden. Wählen Sie unter **Ansicht** > **Details auswählen** die anzuzeigenden Spalten. Über den Menüpunkt **Ansicht** > **Symbole anordnen** können Sie außerdem die gewünschte Sortierung auswählen.

Die Sortierung der Ansicht können Sie auch direkt durch einen Klick mit der linken Maustaste in die entsprechende Spaltenüberschrift ändern. Mit jedem erneuten Klick wechselt die Sortierung.

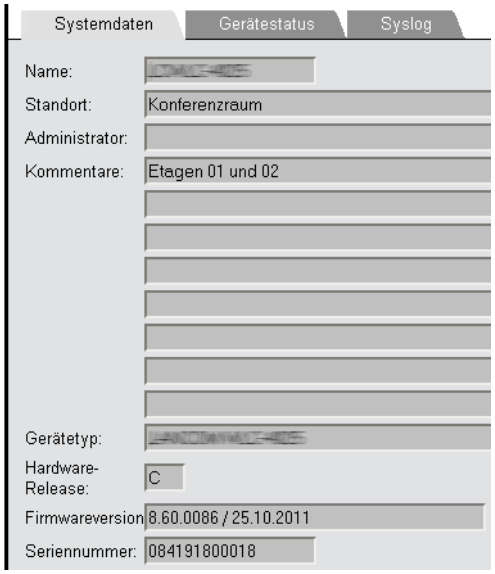


Im Einzelnen können Sie folgende Informationen in den Spalten anzeigen:

- Name
- Ordner
- Beschreibung
- Kommentar
- Adresse
- Standort
- Gerätestatus
- Verlauf
- Gerätetyp
- Produkt-Code
- Hardware-Release
- Seriennummer
- MAC-Adresse
- Firmware-Version
- Firmsafe
- 1. Image-Version
- 2. Image-Version

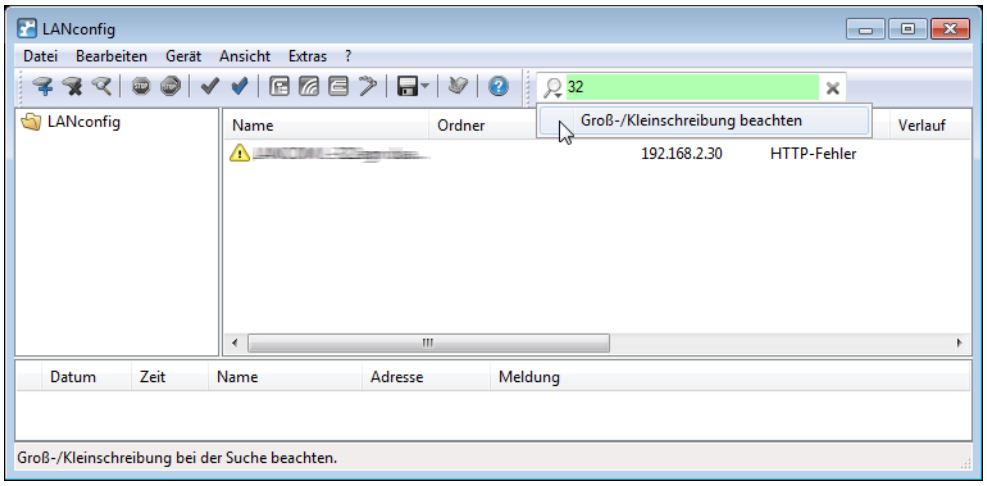
Mit **Alles einblenden** bzw. **Alles ausblenden** zeigen bzw. verbergen Sie alle Spalten mit einem Klick.

Die Spalte **Kommentar** enthält die Informationen des Kommentarfeldes 1 im Gerät.



3.1.2.5 QuickFinder in LANconfig

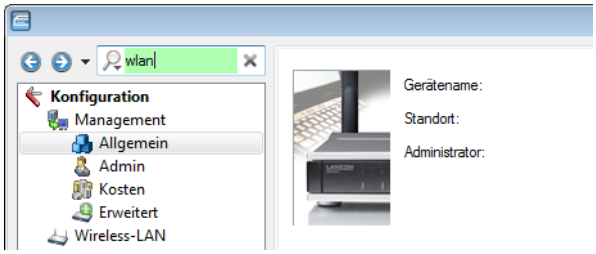
In der Hauptansicht von LANconfig finden Sie den QuickFinder in der Symbolleiste. Geben Sie im Suchfenster einen Suchbegriff ein, um die Liste der angezeigten Geräte zu reduzieren. LANconfig durchsucht dabei alle Werte, die in den Spalten der Geräte-Liste verfügbar sind – auch die derzeit ausgeblendeten Spalten. Klicken Sie auf der Symbol neben der Lupe, um bei der Suche die Groß-/Kleinschreibung zu beachten.



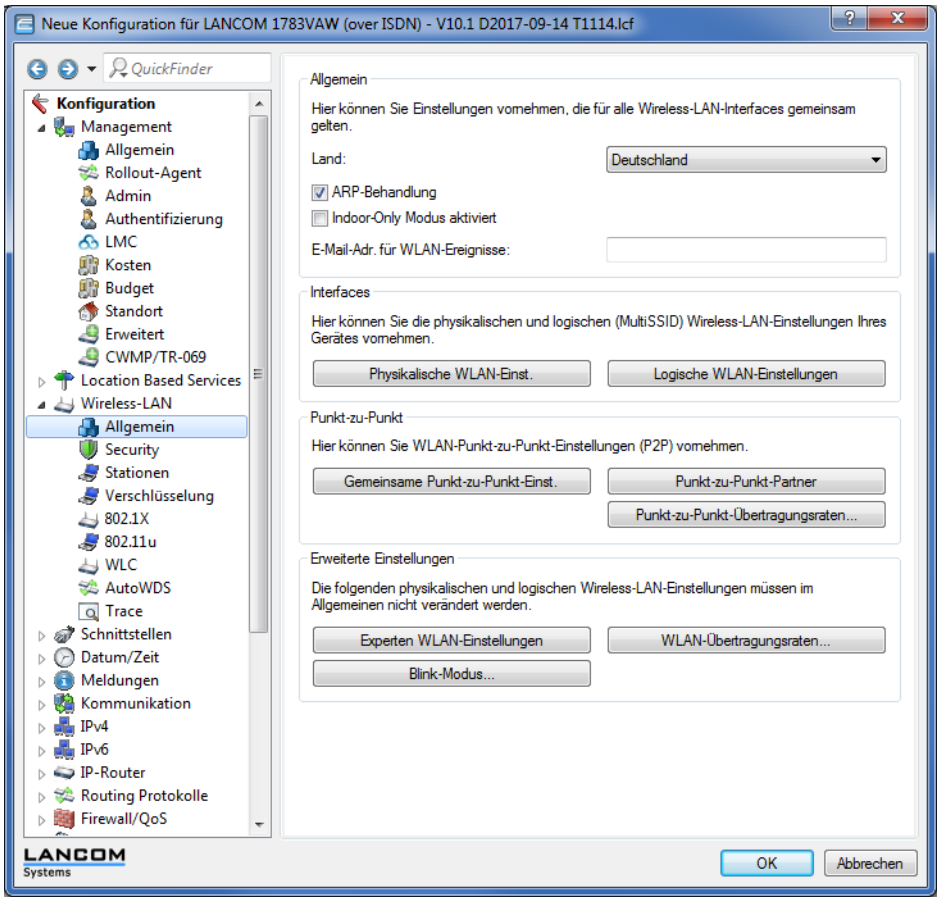
Wenn Sie einen bestimmten Wert oder Begriff in LANconfig oder der Konfiguration suchen, zeigt Ihnen der QuickFinder in den Konfigurationsdialogen von LANconfig schnell alle Stellen, in denen die gesuchte Zeichenkette enthalten ist.

1. Starten Sie LANconfig.
2. Öffnen Sie die Konfiguration des Gerätes, welche Sie durchsuchen möchten.
3. Geben Sie im Suchfeld den gewünschten Begriff ein, z. B. `wlan`. Die Suche unterscheidet nicht nach Groß- und Kleinschreibung. Sie können Teile von Worten oder Zahlen ebenso eingeben wie komplette Suchbegriffe. Leerzeichen in den Suchbegriffen suchen auch nur nach Zeichenketten, welche die entsprechenden Leerzeichen enthalten. Die Suchfunktion unterstützt jedoch keine Wildcards.

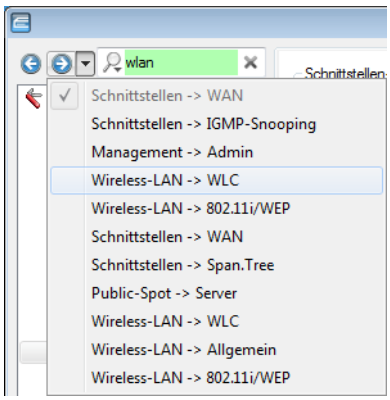
Der Konfigurationsbaum im linken Bereich von LANconfig ist nun reduziert auf alle Bereiche an, in denen der Suchbegriff enthalten ist:



Wählen Sie einen der Bereiche im Konfigurationsbaum (z. B. **Wireless-LAN** > **Allgemein**'), um die entsprechenden Suchergebnisse im Konfigurationsdialog farbig eingerahmt anzuzeigen:

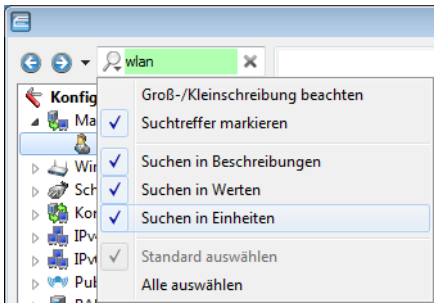


Nutzen Sie die Navigationsschaltflächen 'Zurück' und 'Vor' links neben dem Suchfeld, um in den zuletzt besuchten Dialogen zu blättern. Für einen besonders schnellen Zugriff auf die letzten 10 besuchten Dialoge klicken Sie auf den Pfeil rechts neben der Schaltfläche 'Vor':



Klicken Sie auf das Kreuz rechts neben dem Suchfeld, um die Suche zu löschen und um im Konfigurationsbaum wieder alle Einträge anzuzeigen.

Um die Suchergebnisse optional zu reduzieren, wählen Sie Bereiche aus, die LANconfig in die Suche einbeziehen soll. Klicken Sie dazu auf die Lupe links neben dem Suchfeld und aktivieren oder deaktivieren Sie die gewünschten Bereiche. Legen Sie hier außerdem fest, ob die Suche die Treffer farbig markiert oder nur den Konfigurationsbaum auf die gefundenen Dialoge reduziert:



LANconfig löscht die Einstellung der Suchbereiche und die Liste der zuletzt besuchten Dialoge beim Schließen der Konfiguration.

Wenn Sie z. B. in der Konfiguration bestimmte Einstellungen für Ihren Internet-Provider vorgenommen haben, können Sie einfach mit der Eingabe des Namens alle Stellen in der Konfiguration finden, die sich auf diesen Provider beziehen.

Konkret erfasst die Suche dabei die folgenden Bereiche:

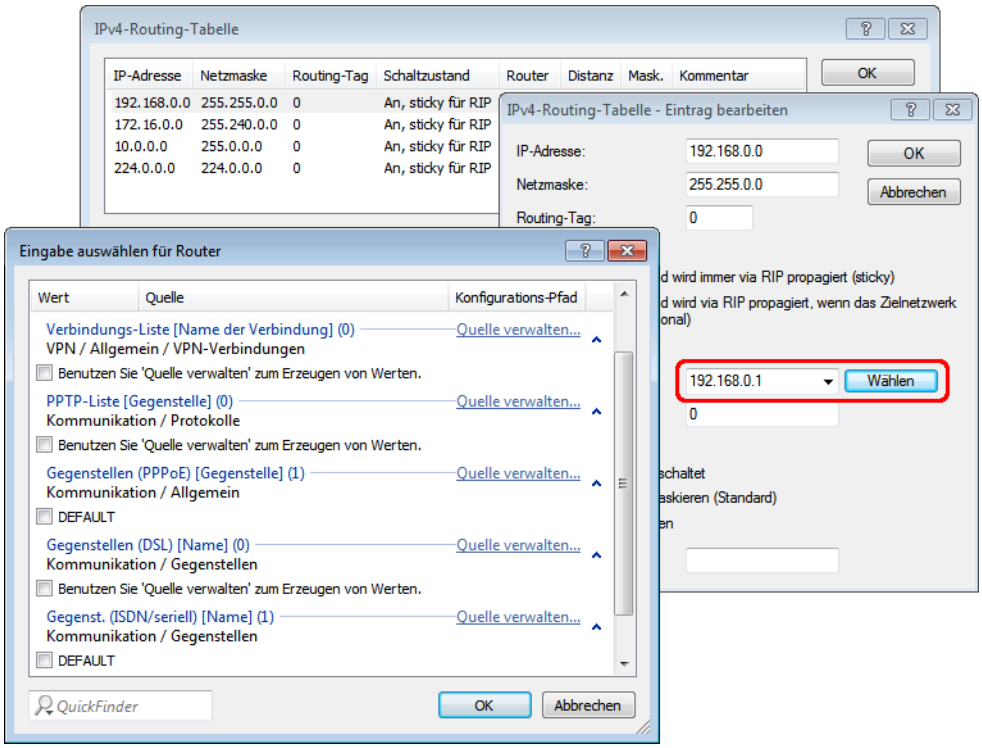
- Einträge im Konfigurationsbaum
- Bezeichnungen der Bereiche (Sektionen) in den einzelnen Konfigurationsdialogen
- Parameter
- Werte der Parameter
- Erläuternde Texte in den Dialogen
- Namen der Tabellen
- Namen der Tabellenspalten

3.1.2.6 Quicklinks zur Verwaltung von Quelltabellen

Lassen sich in einem Eingabefeld Werte auswählen, die bereits in einer oder mehreren anderen Tabellen vordefiniert sind, steht mit den sogenannten Quicklinks eine direkte Möglichkeit zur Verwaltung dieser Quelltabellen zur Verfügung. Dies ermöglicht es, die vorgegebene Konfigurationsreihenfolge zu umgehen. Statt zur Neuanlage von gewünschten

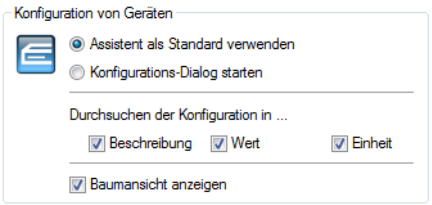
Elementen zunächst die aktuelle Auswahl verlassen zu müssen, können Sie diese Elemente direkt bei Bedarf anlegen. Diese neuen Elemente stehen sofort für eine Selektion zur Verfügung.

Um die Konfigurationsstruktur zu verdeutlichen, zeigt LANconfig neben den einzelnen Quellen den Konfigurations-Pfad an. Ist die Auswahl der Konfigurationsparameter aus mehreren Quelltabellen möglich, gruppiert LANconfig die Einträge entsprechend. Zu jeder Gruppe gibt LANconfig zusätzlich die Anzahl der enthaltenen Einträge an.



3.1.2.7 Assistent oder Konfigurationsdialog wählbar

Beim Doppelklick auf einen Eintrag in der Geräteliste von LANconfig kann ausgewählt werden, ob sich der Dialog zur manuellen Bearbeitung der Konfiguration oder ein Setup-Assistent öffnen soll. Das Standardverhalten von LANconfig legen Sie im Dialog **Extras** > **Optionen** auf der Seite **Allgemein** fest.

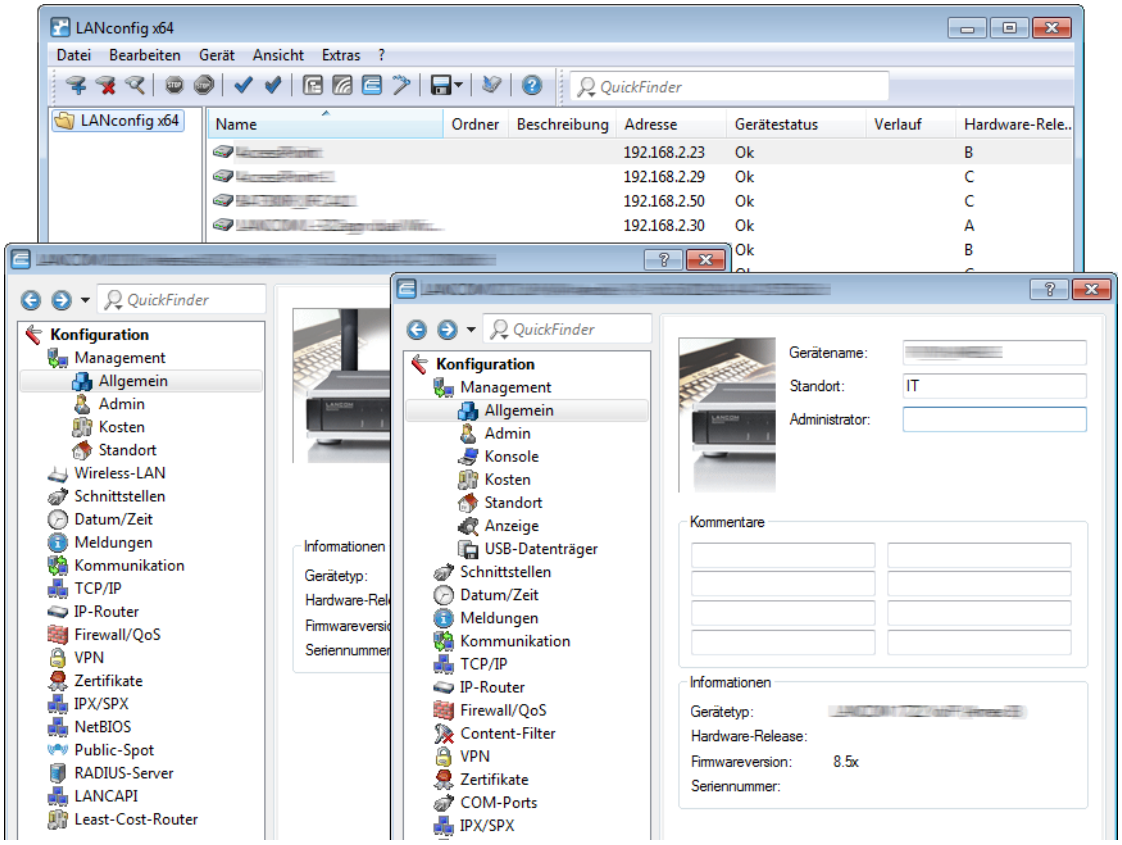


- **Assistent als Standard verwenden:** Startet beim Doppelklick auf den Geräte-Eintrag in LANconfig den Auswahldialog für die Assistenten.
- **Konfigurations-Dialog starten:** Startet beim Doppelklick auf den Geräte-Eintrag in LANconfig den Konfigurations-Dialog.

3.1.2.8 Multithreading

Bei der Verwaltung von Projekten ist es oft hilfreich, die Konfigurationen von mehreren Geräte gleichzeitig zu öffnen, um darin Gemeinsamkeiten oder Unterschiede abzugleichen. LANconfig erlaubt das gleichzeitige Starten von mehreren

Konfigurationsdialogen ("Multithreading"). Nach dem Öffnen einer Konfiguration können aus der Liste der Geräte im LANconfig einfach weitere Konfigurationen geöffnet werden. Alle Konfigurationen können parallel bearbeitet werden.

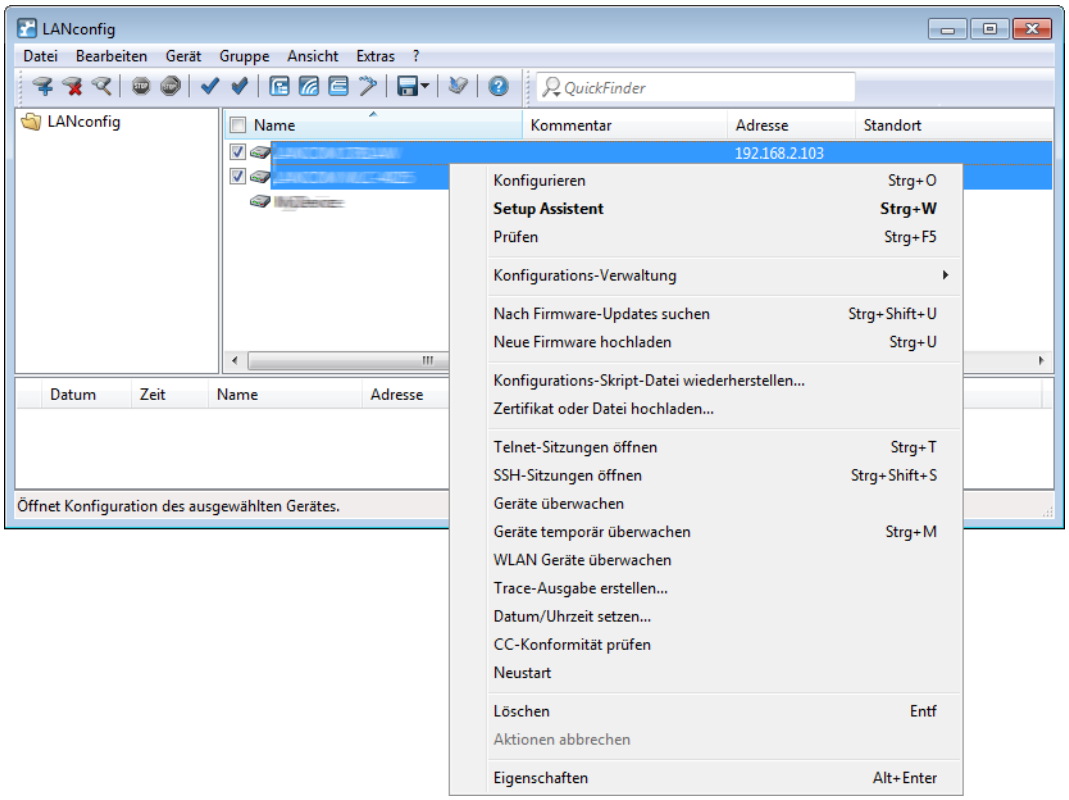


Zwischen den geöffneten Konfigurationen können Inhalte mit "Copy and Paste" über die Zwischenablage übertragen werden.

Beim Multithreading können auch aus den erreichbaren Geräten ausgelesene Konfigurationen und Konfigurationsdateien bearbeitet werden. Jede Konfiguration wird separat beim Schließen des entsprechenden Dialogs in die Datei bzw. das Gerät zurückgeschrieben.

3.1.2.9 Projektmanagement mit LANconfig

LANconfig erleichtert die Konfiguration von verschiedenen Geräten in einem Projekt mit einigen Funktionen, die gleichzeitig auf mehreren Geräten ausgeführt werden können. Sind in der Liste der Geräte im LANconfig mehrere Einträge markiert, können mit einem rechten Mausklick über das Kontextmenü folgende Aktionen aufgerufen werden:



- **Konfigurieren**

  Öffnet für die ausgewählten Geräte den Konfigurationsdialog unter LANconfig.

- **Prüfen**

  Prüft die ausgewählten Geräte auf Erreichbarkeit.

- **Konfigurationsverwaltung**

  Sichern Sie die aktuelle Gerätekonfiguration als Konfigurationsskript oder als *.lcf-Datei.

- **Nach Firmware-Updates suchen**

  Sucht im unter **Extras** > **Optionen** > **Update** konfigurierten **Firmware-Archiv**-Ordner nach verfügbaren Firmware-Updates.

- **Neue Firmware hochladen**

  Lädt eine Firmware parallel in alle ausgewählten Geräte.

- **Konfigurations-Skript-Datei wiederherstellen**

  Führt ein Konfigurationsscript für alle ausgewählten Geräte aus.

- **Telnet-Sitzungen öffnen**, **SSH-Sitzungen öffnen**

  Öffnet mehrere Konsolen-Fenster und startet zu jedem Gerät eine separate Telnet- bzw. SSH-Verbindung. LANconfig greift dafür auf die in den Einstellungen konfigurierten, externen Client-Programme zurück. Wenn Sie keine Client-Programme installiert und angegeben haben, bricht LANconfig diese Aktion mit einer Fehlermeldung ab.

- **Zertifikat oder Datei hochladen**

Öffnet den Upload-Dialog für das geräteinterne Dateimanagement.

- **Geräte überwachen**, **Geräte temporär überwachen**

  Öffnet die ausgewählten Geräte im LANmonitor zur Überwachung.

- **WLAN Geräte überwachen**

  Öffnet die ausgewählten Geräte im WLANmonitor zur Überwachung.

- **Trace-Ausgabe erstellen**

  Öffnet mehrere LANtracer-Fenster und erstellt für jedes Gerät eine separate Trace-Ausgabe.

- **Datum/Uhrzeit setzen**

  Stellt auf allen ausgewählten Geräten die Uhrzeit gleich ein.

  Beachten Sie für die Einstellung der Uhrzeit auch die Funktionen des Geätes als NTP-Client und NTP-Server.

- **CC-Konformität prüfen**

  Prüft, ob die Konfiguration der ausgewählten Geräte CC-konform ist. Diese Aktion ist nur bei CC-Geräten sinnvoll.

- **Neustart**

  Startet die ausgewählten Geräte neu.

- **Löschen**

  Löscht die ausgewählten Geräte aus der Geräteliste im LANconfig.

- **Aktion abbrechen**

  Erzwingt denn Abbruch einer laufenden LANconfig-Aktion (z. B. den Upload einer Datei).

- **Eigenschaften**

  Öffnet einen gemeinsamen Eigenschaften-Dialog, in dem Sie für mehrere Geräte gleichzeitig identische allgemeine und backupbezogene Einstellungen vornehmen können. Berücksichtigen Sie dabei, dass Ihnen in diesem Sammeldialog –gegenüber einem gerätespezifischen Eigenschaften-Dialog – nicht alle Einstellungsmöglichkeiten zur Verfügung stehen.

3.1.2.10 Flexible Gruppen-Konfiguration mit LANconfig

Die flexible Gruppen-Konfiguration unterstützt Sie bei der Verwaltung vieler Geräte: eine gezielte Auswahl an Konfigurations-Parametern wenden Sie gemeinsam auf eine Gruppe von Geräten an. Dies ist komfortabler als die Parameter einzeln in jedem Gerät manuell zu setzen, z. B. bei identischen SSID-Einstellungen in WLAN-Access-Points. So vermeiden Sie, komplette Konfigurationsdateien anderer Geräte zu übertragen. Denn dabei werden gerätespezifische Parameter wie die IP-Adresse ebenfalls übernommen. Die Gruppen-Konfiguration von LANconfig ermöglicht das einfache gemeinsame Setzen von Gruppen-Konfigurationsparametern und damit das gleichzeitige Verwalten mehrerer Geräte.

Durch das Zuordnen mehrerer Geräte zu einer Gruppen-Konfiguration fassen Sie diese zu einer gemeinsam verwalteten Gruppe zusammen. Die Gruppen-Konfigurationsdateien, die gemeinsame Parameter für eine Gruppe von Geräten enthalten, speichern Sie wie komplette Konfigurationsdateien auf der Festplatte oder einem Server. Für die Konfiguration von ganzen Geräte-Gruppen legt LANconfig Verweise auf diese Gruppen-Konfigurationsdateien an. Diese Verweise sind eine komfortable Verbindung zwischen den Geräte-Einträgen in LANconfig und den Gruppen-Konfigurationsdateien.

LANconfig stellt in Form der Group Templates allgemeine Vorlagen bereit, die zur Erzeugung von Gruppen-Konfigurationen dienen. Den Umfang der verwendeten Parameter für eine Gruppe definieren Sie individuell für Ihre Bedürfnisse. Verwenden Sie diese Funktion, wenn Sie zusätzliche Konfigurations-Parameter als Gruppen-Parameter aufnehmen oder vorgeschlagene Gruppen-Parameter entfernen. Diese von Ihnen erstellten Konfigurationen speichern Sie wahlweise als Gruppen-Konfiguration oder als kundenspezifische Vorlage für die Erzeugung von weiteren Gruppen-Konfigurationen.

Sie haben später ausschließlich die Option, Ihre erstellten Gruppen-Konfigurations-Vorlagen zu ändern, nicht jedoch die LANconfig-Basis-Vorlagen.

Folgende Vorlagen für Gruppen-Konfigurationen stehen in LANconfig zur Verfügung:

- **Group Template WLAN:** Beinhaltet die Parameter, die auf WLAN-Geräten gemeinsam verwaltet werden.
- **Group Template WLC:** Beinhaltet möglichst viele Parameter von WLC-Geräten, die im Betrieb eines Clusters von WLCs den Bedarf an individueller Konfiguration minimieren.
- **Group Template Empty:** Enthält keine Vorauswahl von Gruppen-Parametern und dient als Basis zur Erstellung eigener Gruppenvorlagen, welche über die Gruppenvorlagen für WLAN und WLC hinausgehen. Wählen Sie hier aus der Gesamtmenge aller verfügbaren Konfigurationsparameter in allen Geräte-Typen diejenigen aus, welche Sie für Ihre Gruppen-Konfiguration nutzen möchten.

Wenn Sie stattdessen die Einstellung **Verwende alternative Basiseinstellungen** aktivieren, bietet Ihnen LANconfig eine Liste an, aus der Sie alternativ eine Gruppen-Vorlage für bestimmte Gerätetypen wählen können. Mit den Group Templates haben Sie die Möglichkeit, die gemeinsamen Parameter für verschiedene Geräte-Typen in die Gruppen-Vorlage zu übernehmen. Einige Parameter überschneiden sich jedoch bei verschiedenen Gerätetypen (z. B. DSL und DSLoL). Die Group Templates stellen daher immer auch einen Kompromiss dar, in dem einige Parameter möglicherweise fehlen. Für homogenen Gruppen, die ausschließlich einen speziellen Gerätetyp umfassen, bietet es sich daher an, eine spezielle Gerätekonfiguration mit einer bestimmten Firmware als Vorlage für die Gruppe auszuwählen. Diese Bassiseinstellung bietet so exakt die für diesen Gerätetyp benötigten Konfigurationsparameter zur Auswahl an.

Neue Gruppen-Konfigurationsdatei anlegen

Voraussetzung für die Verwendung der Gruppen-Konfiguration ist die Gruppierung der Geräte in Ordnern. Diese LANconfig-Ordner enthalten die Geräte-Einträge, für die eine gemeinsame Konfiguration der Gruppen-Konfigurationsparameter sinnvoll ist, sowie einen Verweis auf die Gruppen-Konfiguration. Die nachfolgenden Handlungsschritte beschreiben, wie sie eine neue Gruppen-Konfiguration anlegen.

Mit einer Gruppen-Konfiguration verwalten Sie die Geräte-Parameter, die allen zugeordneten Geräten gemeinsam sind. Eine Geräte-Individualkonfiguration bezieht sich auf die Parameter, die gerätespezifisch sind.

1. Erstellen Sie einen neuen Ordner für die zu gruppierenden Geräte.

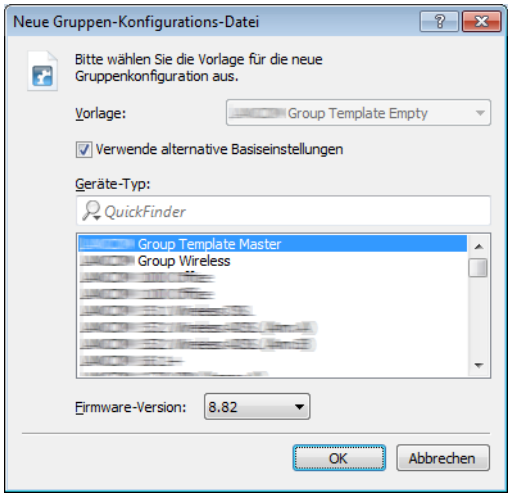
   Sie haben zwei Möglichkeiten, diesen Ordner anzulegen:

   - Klicken Sie mit der rechten Maustaste auf einen existierenden Ordner in der Ordner-Ansicht. Wählen Sie **Neuer Ordner mit Gruppen-Konfiguration**. Der Konfigurationsdialog erstellt zunächst unterhalb der angeklickten Verzeichnis-Ebene einen neuen Ordner und startet mit der Template-Auswahl zur Erstellung einer neuen Gruppen-Konfiguration.
   - Klicken Sie mit der rechten Maustaste in der Ordneransicht auf das Verzeichnis, in dem Sie den neuen Ordner erstellen möchten. Wählen Sie im Kontext-Dialog **Neuer Ordner** aus und vergeben Sie einen Namen. Verschieben Sie die zu gruppierenden Geräte mit der Maus in diesen neuen Ordner. Klicken Sie anschließend mit der rechten Maustaste auf den neuen Ordner und wählen Sie im Kontextmenü den Eintrag **Neue Gruppen-Konfiguration**. Es öffnet sich die Template-Auswahl zur Erstellung einer neuen Gruppen-Konfiguration.

2. Wählen Sie eine **Vorlage** sowie die entsprechende **Firmware-Version** aus. Wenn Sie zuvor eigene Gruppen-Vorlagen gespeichert haben, finden Sie diese ebenfalls in der Auswahlliste der Vorlagen.

   Alternativ haben Sie auch die Möglichkeit, durch aktivieren der Schaltfläche **Verwende alternative Basiseinstellungen** die grundlegenden Einstellungen eines speziellen Geräte-Typs als Basis für die neue

Gruppen-Konfiguration zu verwenden. Die neue Gruppen-Konfiguration übernimmt in diesem Fall die Standardwerte vom gewählten Geräte-Typ.

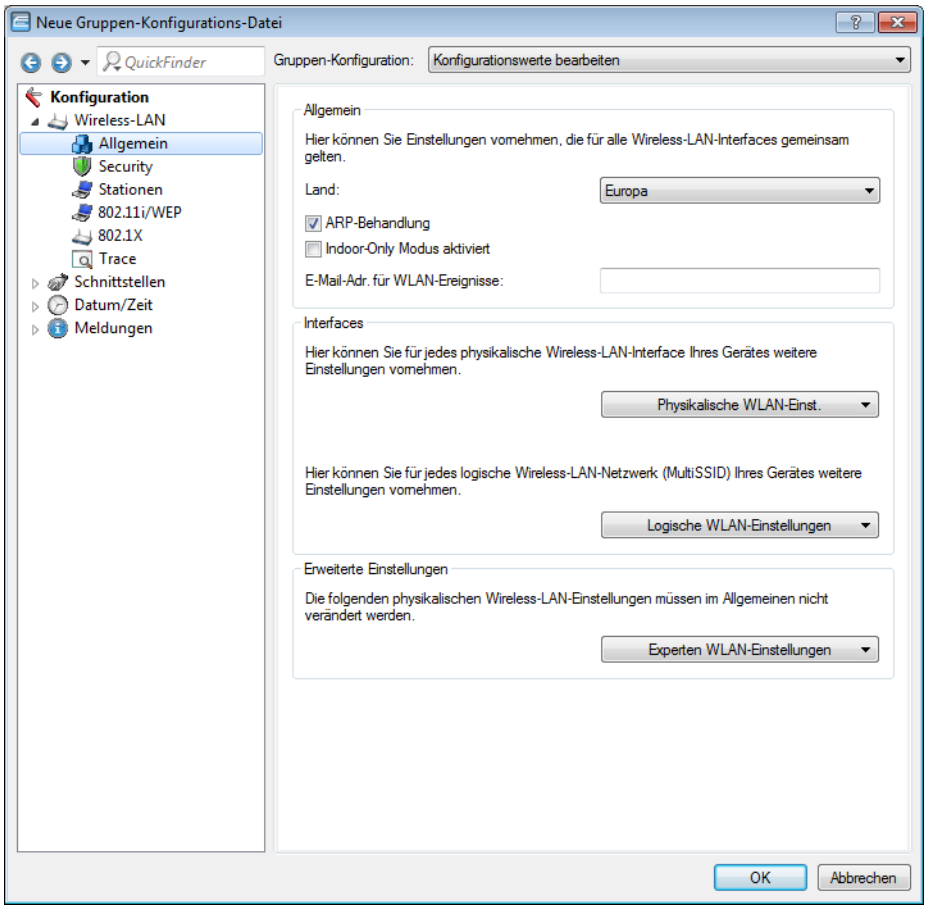


Um inkonsistente Sätze von Konfigurationsparametern zu vermeiden, basieren die alternativen Basiseinstellungen auf einer leeren Vorlage entsprechend dem **Group Template Empty**.

3. Klicken Sie auf **OK**. Es öffnet sich der Konfigurationsdialog für die Geräteparameter.
Hier stehen Ihnen über die Auswahlliste **Gruppen-Konfiguration** zwei Bearbeitungsmodi zur Auswahl:

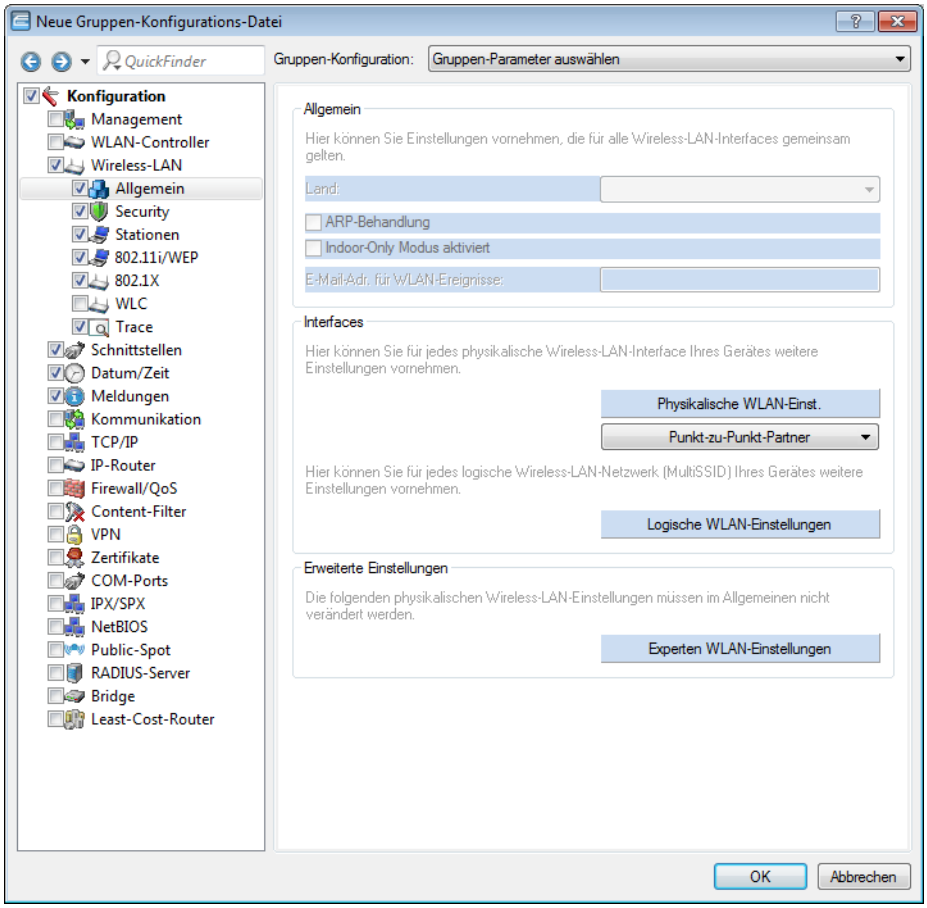
   - Modus **Konfigurationswerte bearbeiten**.
   - Modus **Gruppen-Parameter auswählen**.

Der Konfigurationsdialog startet mit der Ansicht **Konfigurationswerte bearbeiten**. In dieser Ansicht finden Sie ausschließlich die gemeinsam zu verwaltenden Parameter der Gruppe. Hier ist die Einstellung auf die gewünschten Werte und Inhalte möglich. Alle Parameter, die für die einzelnen Geräte gelten, sind ausgeblendet.



Sofern Sie ein leeres Gruppen-Template gewählt haben, ist der angezeigte Dialog leer. Sie müssen dann zunächst die Gruppen-Parameter auswählen, die Sie im o. g. Modus bearbeiten wollen.

Im Konfigurations-Modus **Gruppen-Parameter auswählen** wählen Sie aus allen verfügbaren Parametern diejenigen an- oder ab, die Sie für eine angepasste Gruppen-Konfiguration benötigen.



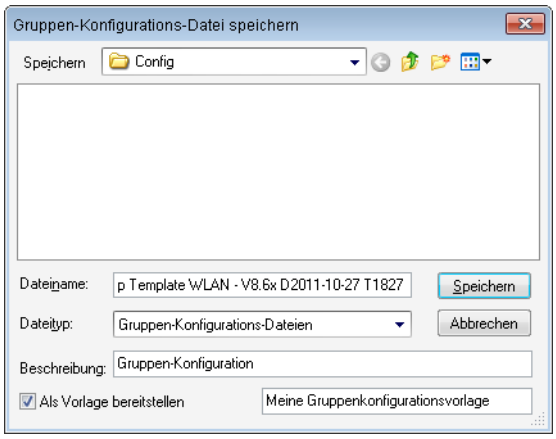
Hellblau eingefärbte Elemente sind für die Verwendung in der Gruppen-Konfiguration ausgewählt. Klicken Sie einmal mit der linken Maustaste auf ein Element, um dessen Auswahlstatus zu ändern.

Beachten Sie folgende Besonderheiten:

- Bei Tabellen mit statisch vorgegebenen Zeilen (z. B. interfacebezogenen Tabellen wie **Logische WLAN-Einstellungen**) haben Sie die Möglichkeit, auch einzelne Parameter in die Gruppen-Konfiguration zu übernehmen. In LANconfig erkennen Sie diese Tabellen oft daran, dass sich bei Anklicken der dazugehörigen Schaltfläche ein Pulldown-Menü öffnet.
- Bei Tabellen mit dynamisch erzeugten Zeilen (wie z. B. der **Routing-Tabelle**) ist ausschließlich die gesamte Tabelle für die Gruppen-Konfiguration an- oder abwählbar.
- Die Firewall ist ebenfalls ausschließlich komplett für die Gruppen-Konfiguration an- oder abwählbar.

4. Bearbeiten Sie gemäß der im vorangegangenen Schritt gegebenen Erläuterungen nun die Konfigurationswerte, und fügen Sie ggf. weitere Gruppenparameter zur Konfiguration hinzu. Klicken Sie zum Abschluss auf **OK**.
5. Geben Sie für die erstellte Gruppen-Konfiguration einen aussagekräftigen **Dateinamen** an und wählen Sie einen Speicherpfad.

Sie haben zudem die Möglichkeit, diese Gruppen-Konfiguration zukünftig als eigene Vorlage für die Erstellung weiterer Gruppen-Konfigurationen angeboten zu bekommen. Aktivieren Sie hierzu die Option **Als Vorlage bereitstellen** und vergeben Sie eine aussagekräftige Bezeichnung.



Sie haben auch später noch die Gelegenheit, aus einer bereits existierenden Gruppen-Konfiguration eine Vorlage zu erstellen. Klicken Sie dazu mit der rechten Maustaste im entsprechenden Gruppen-Ordner auf die entsprechende Gruppen-Konfiguration. Wählen Sie anschließend im Kontextmenü **Als Vorlage bereitstellen** und vergeben Sie eine aussagekräftige Bezeichnung.

6. Klicken Sie auf **Speichern**, um die Aktion abzuschließen.

Fertig! Die zugeordnete Gruppen-Konfigurationsdatei erscheint nun in der Geräteliste mit dem vorgegebenen Namen. Um diesen Namen individuell anzupassen, klicken Sie die Gruppen-Konfiguration mit der rechten Maustaste und ändern unter **Eigenschaften** > **Allgemein** den Text für die **Beschreibung.**

Die Gruppen-Konfiguration speichert alle Parameter in eine Gruppen-Konfigurationsdatei, einschließlich solcher Parameter mit voreingestellten Standardwerten. Verwenden Sie die Scripting-Funktionen, um ausschließlich die von der Standardeinstellung abweichenden Parameter aus dem Gerät auszulesen und ggf. auf andere Geräte zu übertragen.

Bestehende Gruppen-Konfigurationsdatei verwenden

In manchen Fällen ist eine andere Struktur der mit LANconfig verwalteten Geräte sinnvoll, als es die Gruppen-Konfiguration erfordern würde. Die Geräte in standortspezifischen Ordnern sind z. B. teilweise durchaus denselben Gruppen zuzuordnen. Um redundante Gruppen-Konfigurationsdateien für jeden Ordner zu vermeiden, empfiehlt es sich, in mehreren Ordnern Verweise auf eine gemeinsam verwendete Datei zu erstellen.

Wollen Sie eine vorhandene Gruppen-Konfigurationsdatei für eine Gruppe von Geräten verwenden, klicken Sie mit der rechten Maustaste auf den gewünschten Ordner. Wählen Sie anschließend im Kontextmenü den Eintrag **Gruppen-Konfiguration hinzufügen**.

Wählen Sie im folgenden Dialog die bereits bestehende Gruppen-Konfigurationsdatei aus und erstellen Sie so in dem Ordner einen Verweis auf diese Datei.

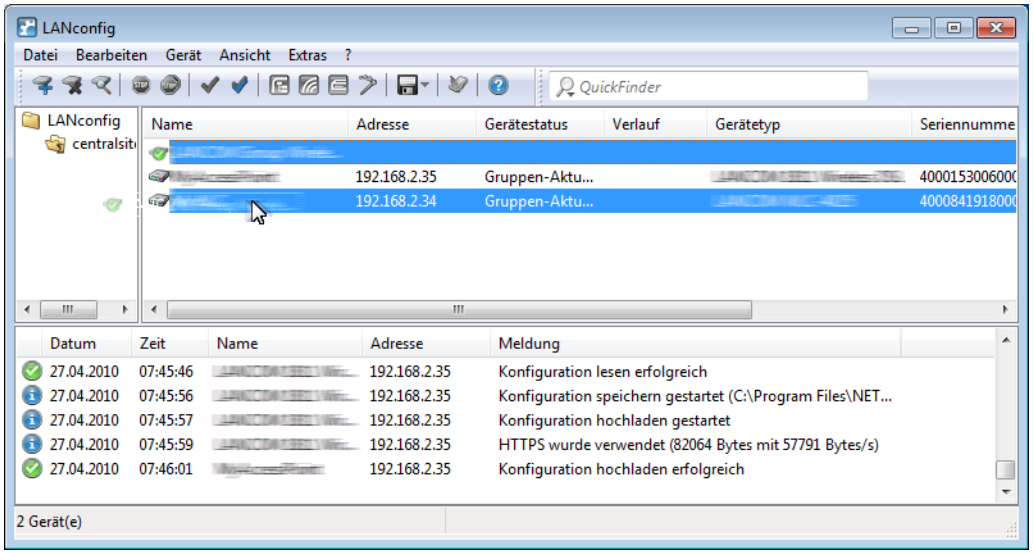
Beachten Sie, dass Änderungen der Gruppen-Konfigurationsdatei auch Änderungen der jeweiligen Gruppen-Konfigurationen in verschiedenen Ordnern zur Folge haben.

Erstellen Sie in einem Gruppen-Ordner weitere Geräte, oder ändern Sie eine bestehende Gruppen-Konfiguration, informiert Sie LANconfig, dass für die entsprechenden Geräte eine Aktualisierung vorliegt. Diese Aktualisierung ist direkt im Anschluss oder später über das Kontextmenü durchführbar.

Gerätekonfigurationen mit Gruppen-Konfigurationen aktualisieren

Beim Aufrufen oder Aktualisieren eines Ordners prüft LANconfig, ob die Konfiguration der Geräte in diesem Ordner mit den Einstellungen in der aktiven Gruppen-Konfiguration übereinstimmt. Über Abweichungen von der Gruppen-Konfiguration informiert der Gerätestatus **Gruppen-Aktualisierung empfohlen**.

Um die Gruppen-Konfiguration in das WLAN-Gerät zu laden, ziehen Sie den Gruppen-Konfigurationseintrag auf den entsprechenden Geräteeintrag. Nach erfolgreicher Übertragung der Parameter ändert sich der Gerätestatus auf **Ok**.



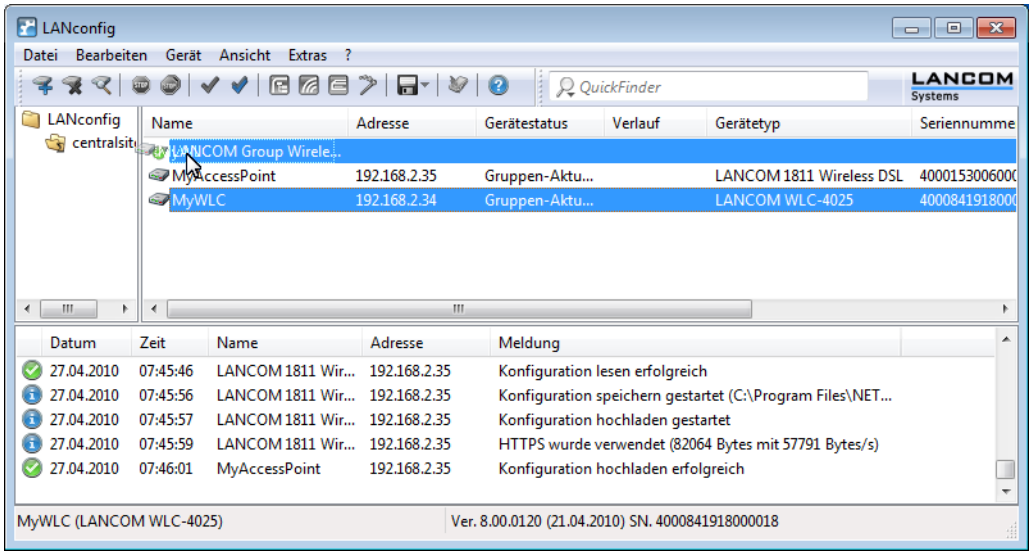
Es ist auch möglich, Teilkonfigurationen eines WLAN-Gerätes als Gruppen-Konfiguration zu verwenden. Ziehen Sie hierzu den Geräteeintrag auf den Gruppen-Konfigurationseintrag.

Gruppen-Konfigurationen mittels Master-Gerät aktualisieren

Neben dem manuellen Verändern der Parameter einer Gruppen-Konfiguration (siehe Kapitel *Gerätekonfigurationen mit Gruppen-Konfigurationen aktualisieren* auf Seite 192) kann auch die aktuelle Konfiguration eines Gerätes als Basis für eine Gruppen-Konfiguration verwendet werden. Ein Gerät wird damit zum "Master" für alle anderen Geräte im gleichen Ordner.

Um die Parameter einer Gruppen-Konfiguration von einer aktuellen Geräte-Konfiguration zu übernehmen, ziehen Sie einfach den Eintrag des Gerätes auf die gewünschte Gruppen-Konfiguration. Alle in der Gruppen-Konfiguration definierten Parameter werden dabei mit den Werten der Geräte-Konfiguration überschrieben.

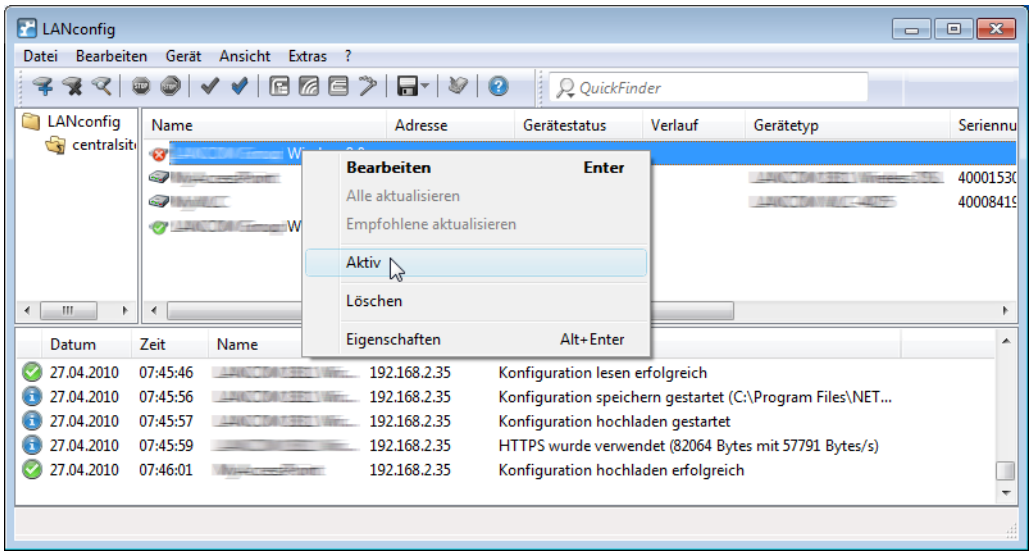
Beim folgenden Prüfen der Geräte wird LANconfig feststellen, dass die Konfigurationen der anderen Geräte im Ordner nicht mehr mit der neuen Gruppen-Konfiguration übereinstimmen und dies über den Gerätestatus entsprechend anzeigen.



Mehrere Gruppen-Konfigurationen verwenden

Innerhalb eines Ordners können mehrere Gruppen-Konfigurationen angelegt werden. Von diesen Gruppen-Konfigurationen darf jeweils nur eine aktiv sein, da sich der Gerätestatus nur auf eine einzelne Gruppen-Konfiguration beziehen kann. Aktive Gruppen-Konfigurationen sind mit einem blauen Häckchen, inaktive Gruppen-Konfigurationen mit einem roten Kreuz gekennzeichnet.Um eine Gruppen-Konfiguration zu aktivieren, klicken Sie mit der rechten Maustaste auf den Eintrag und wählen im Kontextmenü den Eintrag 'Aktiv'. Alle anderen Gruppen-Konfigurationen werden dabei automatisch deaktiviert.

Unterschiedliche Gruppenkonfigurationen in einem Ordner dürfen nicht auf die gleiche Teil-Konfigurationsdatei verweisen.



Übertragen von Gerätekonfigurationen auf ähnliche Modelle

Beim Wechsel auf einen anderen Gerätetyp ist es in manchen Fällen erwünscht, die Konfiguration des vorherigen Modells weitgehend zu übernehmen. Dazu bietet LANconfig die Möglichkeit, die Konfigurationsdatei (*.lcf) von einem

Ausgangsgerät in ein ähnliches Zielgerät einzuspielen. Dabei werden alle Konfigurationsparameter, die sowohl im Ausgangs- wie auch im Zielgerät vorhanden sind, nach Möglichkeit mit den bisher verwendeten Werten belegt:

- Wenn das Zielgerät über den entsprechenden Parameter verfügt und der Wert im möglichen Bereich liegt, wird der Wert des Ausgangsgerätes übernommen.
- Wird der Wert eines vorhandenen Parameters im Zielgerät nicht unterstützt, wird der Standardwert verwendet. Beispiel:
  - Das Ausgangsgerät verfügt über vier Ethernetschnittstellen.
  - Das Zielgerät verfügt nur über zwei Ethernetschnittstellen.
  - Die Schnittstelle für ein IP-Netzwerk ist im Ausgangsgerät auf LAN-4 eingestellt.
  - Dieser Wert wird im Zielgerät nicht unterstützt. Daher wird der Wert beim Einspielen der Konfigurationsdatei auf den Standardwert 'LAN-1' gesetzt.
- Alle Parameter im Zielgerät, die im Ausgangsgerät nicht vorhanden sind, behalten ihren jeweiligen Wert bei.

Handlungsschritte

So gehen Sie vor, um die Konfiguration auf ein neues Gerät zu übertragen:

1. Bringen Sie nach Möglichkeit das Ausgangs- und das Zielgerät auf den gleichen Firmware-Stand. Jede neue LCOS-Firmware enthält neue Parameter. Mit der gleichen Firmware auf beiden Geräten erzielen Sie die größtmögliche Übereinstimmung bei den verfügbaren Parametern.
2. Speichern Sie die Konfiguration des Ausgangsgerätes mit LANconfig z. B. über **Gerät** > **Konfigurations-Verwaltung** > **Als Datei sichern**.
3. Trennen Sie das Ausgangsgerät vom Netzwerk, um Adresskonflikte zu vermeiden.
4. Spielen Sie die Konfiguration über **Gerät** > **Konfigurations-Verwaltung** > **Aus Datei wiederherstellen** in das Zielgerät ein. Die Meldungen über die Konvertierung der Konfiguration werden in einem Info-Dialog angezeigt.

Bitte beachten Sie, dass diese Funktion in erster Linie für den Ersatz von Geräten gedacht ist und nicht für die Konfiguration von neuen Geräten, die parallel im gleichen Netz wie das Ausgangsgerät betrieben werden sollen. Da auch die zentralen Kommunikationseinstellungen wie z. B. die IP-Adresse des Gerätes und die DHCP-Einstellungen auf das Zielgerät übertragen werden, kann der parallele Betrieb von Ausgangs- und Zielgerät in einem Netzwerk zu unerwünschten Situationen führen. Für die Konfiguration von mehreren Geräten in einem Netzwerk steht die Gruppenkonfiguration oder die Konfiguration über Skripte zur Verfügung.

3.1.2.11 Automatische Sicherung der Gerätekonfiguration

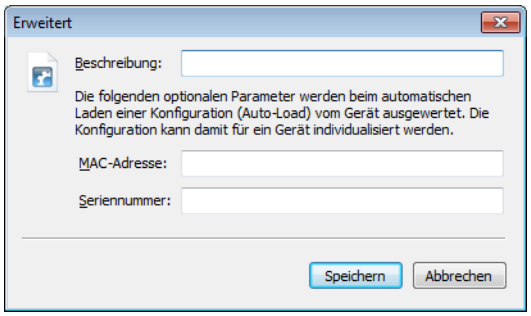
LANconfig kann vor Änderungen der Firmware oder der Konfiguration automatisch Backups der aktuellen Konfiguration speichern. Die globalen Einstellungen dazu, die für alle Geräte verwendet werden, finden Sie unter **Extras** > **Optionen** auf der Seite **Sicherung** (siehe *Sicherung* auf Seite 238).

Für die einzelnen Geräte können ergänzend spezielle Sicherungseinstellungen definiert werden. Klicken Sie dazu auf das entsprechende Gerät mit der rechten Maustaste und wählen Sie im Kontextmenü den Eintrag **Eigenschaften** > **Sicherung** (siehe *Sicherung* auf Seite 211).

3.1.2.12 Erweiterte Meta-Daten für Konfigurationsdateien

LANconfig bietet beim (manuellen) Speichern einer Geräte-Konfiguration die Möglichkeit, zusätzlich zu den üblichen Meta-Daten erweiterte Meta-Daten – bestehend aus MAC-Adresse und / oder Geräte-Seriennummer – in der Konfigurationsdatei (*.lcf) zu erfassen. Diese erweiterten Meta-Daten werden dann z. B. beim Quick Config Rollback oder Laden einer Gerätekonfiguration via USB berücksichtigt.

Um die erweiterten Meta-Daten in eine Konfigurationsdatei mit aufzunehmen, klicken Sie im Datei-speichern-Dialog von LANconfig auf die Schaltfläche **Erweitert** und geben die Daten – sofern nicht bereits vorausgefüllt – in die jeweiligen Felder ein.



Alternativ haben Sie auch die Möglichkeit, eine lcf-/lcs-Datei in einem Texteditor zu öffnen und die erweiterten Meta-Daten nachträglich von Hand zu ergänzen. Ergänzen Sie dazu die Zeile `(<Firmware>)(<Feature-Mask>;<Feature-IDs>;<Hardware-Mask>)` um die Klammer `(MAC:<MAC-Address>;SERIAL:<Serialnumber>)`.

Beispiel:

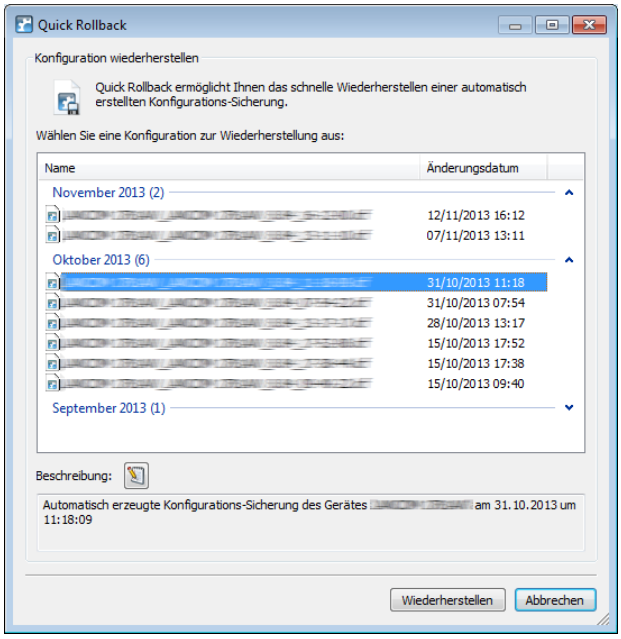
```
(Konfiguration von 'DEVICE-01' vom 12.08.2014)
(9.00.0212) (0x0000c010,IDs:4,e,f,2b;0x0c000002) (MAC:00a0571d12fc;SERIAL:4002578718100036)
```

3.1.2.13 Quick Rollback

Als Ergänzung zur automatischen Sicherung der Gerätekonfiguration haben Sie die Möglichkeit, die gesicherte Konfigurationen mit nur einem Klick wiederherzustellen. Dazu markieren Sie in der Geräteansicht das gewünschte Gerät und wählen **Gerät** > **Quick Rollback**, um die Funktion für das Quick Config Rollback aufzurufen. LANconfig listet Ihnen daraufhin alle geeigneten Gerätekonfigurationen auf, die sich unter dem Pfad für die automatischen Sicherung der Gerätekonfiguration befinden. Sofern LANconfig für das ausgewählte Gerät keine Sicherungsdatei finden kann, bricht diese Aktion mit einer Warnmeldung ab.

LANconfig nutzt für die Zuordnung von Konfigurationssicherungen zum betreffenden Gerät die in den Meta-Daten hinterlegte Seriennummer. Ab LCOS 8.84 wird diese bei der automatischen Sicherung miterfasst; in älteren Konfigurationssicherungen ohne Seriennummer müssen Sie diese jedoch manuell ergänzen, damit Quick Rollback die Dateien erkennt. Lesen Sie dazu auch *Erweiterte Meta-Daten für Konfigurationsdateien* auf Seite 194.

Um eine Konfigurationssicherung wiederherzustellen, markieren Sie einen Eintrag und klicken auf **Wiederherstellen**.



Darüber hinaus haben Sie die Möglichkeit, die Konfigurationssicherungen mit zusätzlichen Kommentaren zu versehen bzw. die darin enthaltenen Kommentare zu bearbeiten und ggf. zu ergänzen: Über die Schaltfläche **Beschreibung bearbeiten** ( ) aktivieren Sie das darunterliegende Kommentarfeld, um den darin enhaltenen Text zu bearbeiten. Über die Schaltfläche **Beschreibung speichern** ( ) schreiben Sie den Text des Kommentarfeldes anschließend in die Sicherungsdatei.

Quick Rollback ist nicht für Switches verfügbar.

3.1.2.14 CSV-Export

Exportieren Sie die Liste der im Netz gefundenen Geräte, um diese später bequem in einem Durchgang wieder in LANconfig zu importieren. LANconfig speichert die Liste der verwalteten Geräte in einer CSV-Datei.

Für den Datenexport gehen Sie wie folgt vor:

1. Wählen Sie im Menü **Datei** > **Geräte-Liste exportieren**.
2. Bestimmen Sie den Speicherort der Datei.
3. Geben Sie einen Dateinamen an.
4. Bestimmen Sie das Spalten-Trennzeichen, welches die jeweiligen Geräteparameter trennt.
5. Starten Sie die Sicherung mit Klick auf **Speichern**.
6. Ein Dialog bestätigt die Anzahl der gespeicherten Geräte-Datensätze.
7. Schließen Sie diesen Dialog mit Klick auf **OK**.

Die erzeugte CSV-Datei enthält folgende Daten (ein Datensatz pro Zeile):

```
DEVICE_PATH;DEVICE_INTERFACE;DEVICE_TIMEOUT;DEVICE_ADDRESS;
DEVICE_ADMIN;DEVICE_PASSWORD;DEVICE_SNMPCOMMUNITY;DEVICE_NAME;
DEVICE_STARTUP;DEVICE_PROTOCOLS;DEVICE_PORTS;DEVICE_DESCRIPTION;
DEVICE_COMMENT;DEVICE_LOCATION;DEVICE_TYPE;DEVICE_EXTENDED_NAME;
DEVICE_PRODUCTCODE;DEVICE_SERNO;DEVICE_HWADDR;DEVICE_HWREL;
DEVICE_BACKUP;DEVICE_VPN;DEVICE_SSH_FINGERPRINT;DEVICE_CREDENTIALS
MyGroup;IP;3;192.168.2.101;;;;LANCOM WLC-4025;1;263;;;;;
LANCOM WLC-4025;LANCOM WLC-4025;;4000841918000018;00a0571218bb;C;"31;
C:\Users\MyUser\AppData\Roaming\LANCOM\LANconfig\Config\;
\%y_%mn_%dn\%N_%G_%F[1-4]_%hh-%mm-%s;12|";;
02:5a:e5:42:ea:d2:da:f0:93:b5:d0:3d:0c:08:70:b8;
```

Die erste Zeile enthält die Namen der Geräte-Parameter. Darunter sind zeilenweise die einzelnen Geräte aufgeführt, deren Parameter jeweils durch Semikolons voneinander getrennt sind. Folgen 2 Semikolons direkt aufeinander, ist der eingeschlossene Parameter-Wert leer.

Die Variablen-Namen der ersten Zeile entsprechen den folgenden LANconfig-Einträgen:

- **DEVICE_PATH**: Pfad-Name in der Ordner-Ansicht
- **DEVICE_INTERFACE**: Anschlussart
- **DEVICE_TIMEOUT**: Maximale Antwortzeit des Gerätes
- **DEVICE_ADDRESS**: IP-Adresse oder Domain-Name und COM-Port oder Rufnummer
- **DEVICE_ADMIN**: Administrator-Name
- **DEVICE_PASSWORD**: Administrator-Passwort
- **DEVICE_SNMPCOMMUNITY**: SNMP Community des Gerätes
- **DEVICE_NAME**: Gerätename
- **DEVICE_STARTUP**: Überprüfung des Gerätes beim Start
- **DEVICE_PROTOCOLS**: Kommunikationsprotokolle
- **DEVICE_PORTS**: Ports
- **DEVICE_DESCRIPTION**: Beschreibung
- **DEVICE_COMMENT**: Kommentar
- **DEVICE_LOCATION**: Einsatz-Ort
- **DEVICE_TYPE**: Gerätetyp
- **DEVICE_EXTENDED_NAME**: Gerätename, ergänzt um eventuelle Zusätze
- **DEVICE_PRODUCTCODE**: Produkt-Code
- **DEVICE_SERNO**: Seriennummer
- **DEVICE_HWADDR**: MAC-Adresse
- **DEVICE_HWREL**: Hardware-Release
- **DEVICE_BACKUP**: Speicherort des von LANconfig angelegten Konfigurations-Backups
- **DEVICE_VPN**: Parametersatz für 1-Click-VPN
- **DEVICE_SSH_FINGERPRINT**: Zwischengespeicherter Fingerprint des eingespielten SSH-Schlüssels, siehe *Schlüssel-Fingerprints bei der Inbetriebnahme von CC-Geräten exportieren* auf Seite 208
- **DEVICE_CREDENTIALS**: Zwischengespeicherter Fingerprint des geräteinternen ssh-rsa-Schlüssels

Verwalten Sie die Liste der exportierten Geräte mit einem Text-Editor oder komfortabler in einer Tabellenkalkulation.

LANconfig speichert das Passwort unverschlüsselt in einer CSV-Datei, wenn LANconfig Zugangsdaten für den Zugriff auf Geräte enthält. Denken Sie daran, diese Zugangsdaten in der Datei zu löschen, bevor Sie diese Datei weitergeben oder auf einem frei zugänglichen Server speichern.

3.1.2.15 Import aus einer Datenquelle (CSV)

Importieren Sie in LANconfig eine große Anzahl Geräte aus einer Skript-Vorlage gleichzeitig, indem Sie einen Import-Assistenten für entsprechende Geräte-Dateien verwenden. Zusätzlich haben Sie die Möglichkeit, mit dieser Geräte-Datei und einer Konfigurations-Vorlagendatei eine individuelle Konfigurationsdatei pro Gerät erstellen zu lassen. Die Vorlagendatei enthält Variablen für die Werte der Geräte-Datei.

Die Geräte-Datei ist im CSV-Format gespeichert.

Anwendungsbeispiel für den Import aus einer Datenquelle

Das in den nachfolgenden Unterkapiteln behandelte Szenario beschreibt, wie Sie anhand einer allgemeinen Skript-Datei und einer einfachen CSV-Geräte-Datei eine eigene Datenquelle für den Daten-Import erzeugen:

Inhalt der CSV-Datei

Die CSV-Datei enthält Datensätze von Geräten, die LANconfig importieren kann. Sie haben somit die Möglichkeit, diese komfortabel im Netzwerk zu verwalten.

Nachfolgend ein Beispiel einer einfachen CSV-Datei:

```
CONFIG_FILENAME;DEVICE_PATH;DEVICE_INTERFACE;DEVICE_ADDRESS;DEVICE_LOCATION;DEVICE_NAME;KEY;USER
Fil52146.lcs;Filialen/NRW;IP;192.168.1.1;Wuerselen;Fil52146;secret1;user1@internet
Fil80637.lcs;Filialen/BAY;IP;192.168.2.1;Muenchen;Fil80637;secret2;user2@internet
```

Die erste Zeile enthält die Namen der Geräte-Parameter. Darunter sind zeilenweise die einzelnen Geräte aufgeführt, deren Parameter jeweils durch Semikolons voneinander getrennt sind. Folgen 2 Semikolons direkt aufeinander, ist der eingeschlossene Parameter-Wert leer.

Die Parameter-Bezeichnungen der ersten Zeile sind frei bestimmbar. Wenn Sie dennoch die verfügbaren Standardvariablennamen verwenden, ordnet LANconfig die Geräte-Parameter beim Import automatisch zu. Eine Übersicht der Standardvariablen finden Sie im Kapitel *CSV-Export* auf Seite 196.

Wenn Sie keine Standardvariablennamen verwenden, ist es ggf. notwendig, dass Sie im Verlauf des Imports die Werte den entsprechenden Geräte-Eigenschaften in LANconfig zuordnen.

Inhalt der Konfigurations-Vorlagendatei

Die Vorlagendatei beinhaltet Konsolenbefehle, die der Reihe nach ausgeführt werden. Daher bezeichnet man diese Vorlagendatei auch als „Skript-Datei“.



Eine Übersicht der verfügbaren Konsolen-Befehle finden Sie in *Befehle für die Konsole* auf Seite 49.

Eine Konfigurations-Vorlagendatei kann wie folgt aussehen:

```
lang English
flash No
set /Setup/Name "$DEVICE_NAME$"
set /Setup/SNMP/Location "$DEVICE_LOCATION$"
cd /Setup/TCP-IP/Network-list
tab Network-name IP-Address IP-Netmask VLAN-ID Interface Src-check Type Rtg-tag Comment
add "INTRANET" $DEVICE_ADDRESS$ 255.255.255.0 0 any loose Intranet 0 "local intranet"
cd /
cd /Setup/WAN/PPP
tab Peer Authent.request Authent-response Key Time Try Conf Fail Term Username Rights
add "INTERNET" none PAP "$KEY$" 6 5 10 5 2 "$USER$" IP
cd /
cd /Setup/WAN/DSL-Broadband-Peers
del *
tab Peer SH-Time AC-name Servicename WAN-layer ATM-VPI ATM-VCI MAC-Type user-def.-MAC DSL-ifc(s) VLAN-ID
add "INTERNET" 9999 "" "" "PPPOEOA" 1 32 local 000000000000 "" 0
cd /
cd /Setup/IP-Router/IP-Routing-Table
tab IP-Address IP-Netmask Rtg-tag Peer-or-IP Distance Masquerade Active Comment
add 255.255.255.255 0.0.0.0 0 "INTERNET" 0 on Yes "default route"
cd /
flash Yes

# done
exit
```

Die Variablen beginnen und enden mit einem Zeichen oder einer Zeichenfolge (hier: '$').

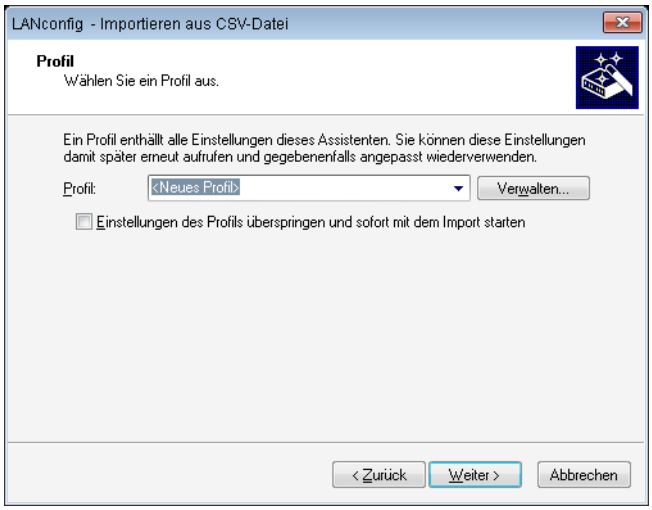
In dieser Vorlagendatei repräsentieren die Variablen bestimmte Geräte-Parameter. Während des Import-Vorgangs verknüpfen Sie diese Variablen mit den entsprechenden Einträgen der Geräte-Datei. Der Konfigurations-Assistent ersetzt die Variablen anschließend mit den zugewiesenen Geräte-Daten aus der CSV-Datei.

Anlegen von Konfigurationsdateien

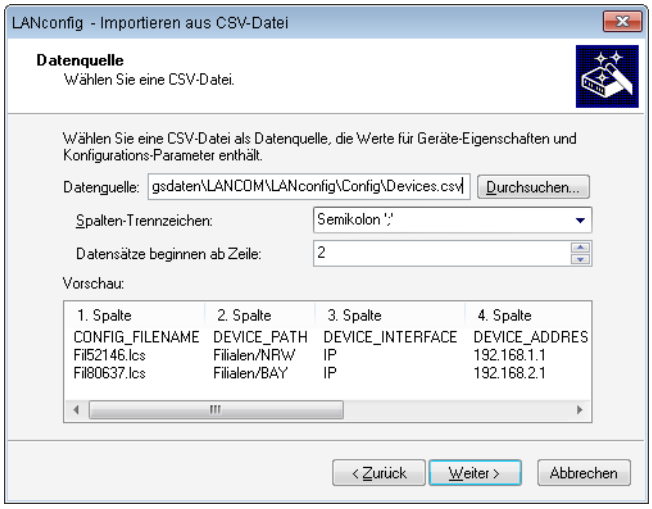
Sie erstellen gerätespezifische Konfigurationsdateien wie folgt:

1. Öffnen Sie den Import-Assistenten im Menü über **Datei** > **Geräte/Konfigurationen aus CSV-Datei...**.
2. Bestätigen Sie ggf. den Begrüßungsdialog mit **Weiter**. Die Option **Diese Seite demnächst überspringen** blendet den Begrüßungsdialog beim zukünftigen Aufruf des Assistenten aus.

3. Wählen Sie ggf. das gespeicherte Profil eines vorherigen Datenimports. Mit der Option **Einstellungen des Profils überspringen und sofort mit dem Import starten** übernehmen Sie die Einstellungen des gewählten Profils ohne Änderungen. Um ein neues Profil statt eines vorhandenen Profils zu verwenden, wählen Sie **<Neues Profil>**. Klicken Sie auf **Weiter**.

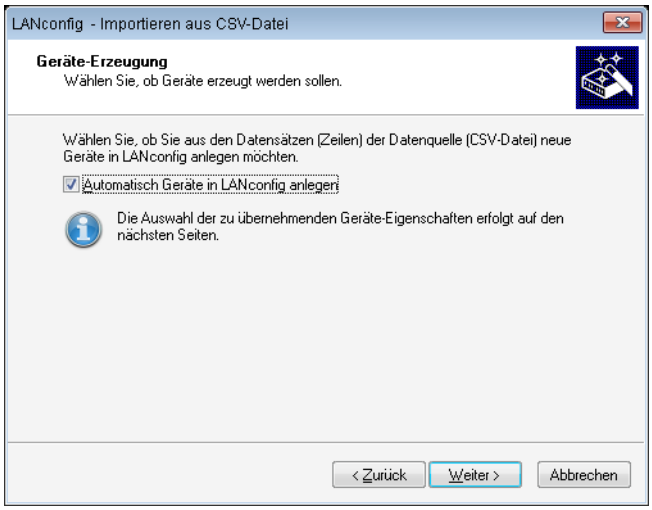


4. Im Feld **Datenquelle** geben Sie den Pfad zur CSV-Datei an. Mit **Durchsuchen...** wählen Sie diese Datei im lokalen Dateisystem aus.



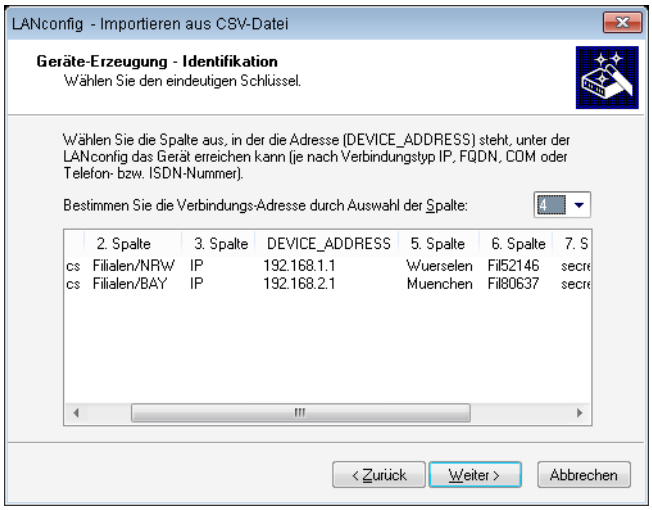
5. Sie können das Spalten-Trennzeichen der CSV-Datei wählen. Die Standardeinstellung ist das Semikolon.
6. Bestimmen Sie, ab welcher Zeile die Datensätze beginnen. Somit schließen Sie aus, dass Sie eventuell vorhandene Spaltentitel und mögliche Zusatzinformationen importieren. Enthält eine Zeile in der CSV-Datei ausschließlich Standardvariablennamen (siehe Abschnitt *Export von CSV-Datensätzen*), dann geschieht die Variablenzuordnung automatisch über diese Zeile. Damit ist gesichert, dass ein Export und der Import derselben Datei ohne manuelle Zuordnung funktioniert. Fügen Sie aber Variablen für die Konfigurationserzeugung hinzu, greift die Autoerkennung nicht.
7. Das Feld **Vorschau** zeigt sofort die anhand Ihrer ausgewählten Parameter zu importierenden Datensätze an. Bestätigen Sie Ihre Eingabe mit **Weiter**.

8. Um anhand der Datensätze neue Geräte in LANconfig anzulegen, aktivieren Sie die Option **Automatisch Geräte in LANconfig anlegen**. Nach einem Klick auf **Weiter** legen Sie auf den folgenden Seiten die Geräte-Eigenschaften fest, die Sie in LANconfig übernehmen.

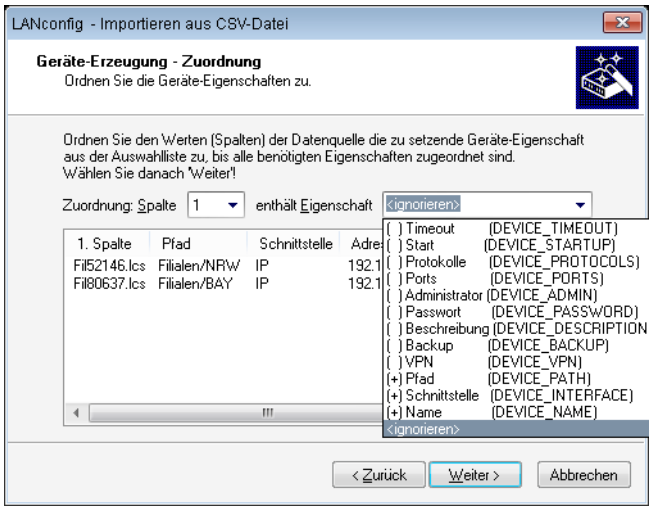


Bei deaktivierter Option überspringt der Assistent die folgenden 2 Schritte.

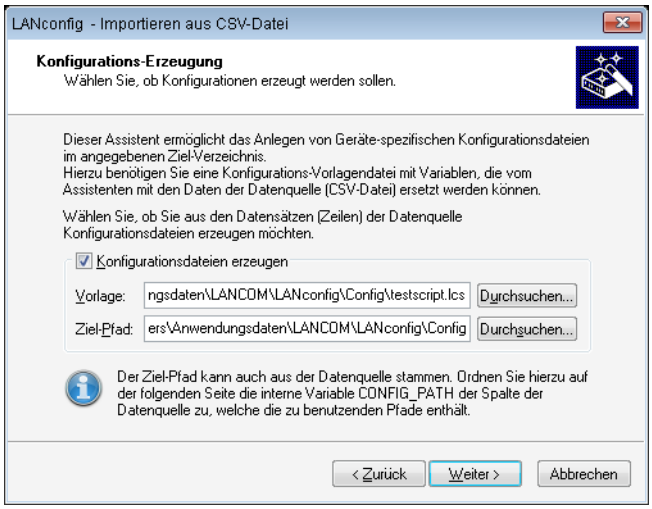
9. Die Identifikation der Geräte erfolgt über die Verbindungsadresse. Wählen Sie entsprechend in der Dropdown-Liste die Spalte des Datensatzes aus, die die Verbindungsadresse enthält, und klicken Sie auf **Weiter**. Bei Verwendung der Standardvariablennamen erfolgt diese Zuordnung automatisch.



10. Ordnen Sie die Spalten den Geräte-Eigenschaften zu. Zugeordnete Eigenschaften erkennen Sie in der Liste an dem vorangestellten "+". Klicken Sie danach auf **Weiter**. Bei Verwendung der Standardvariablennamen erfolgt diese Zuordnung automatisch.

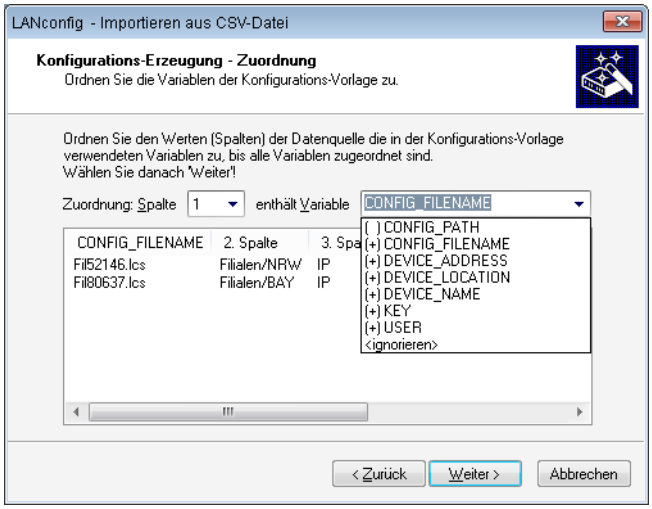


11. Sie haben die Möglichkeit, aus den Datensätzen individuelle Konfigurationsdateien zu erstellen. Aktivieren Sie dazu die Option **Konfigurationsdateien erzeugen**.



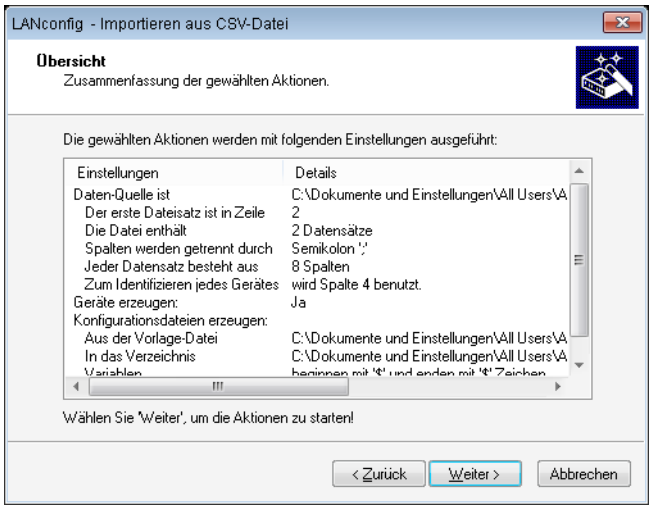
12. Bestimmen Sie im Feld **Vorlage** den Pfad zur Vorlagendatei, die als Basis für die individuellen Konfigurationsdateien vorgesehen ist. Mit Klick auf **Durchsuchen** öffnen Sie den Dialog zum Laden einer Konfigurations-Skript-Vorlage. In den Feldern **Variablen-Start** und **Variablen-Ende** definieren Sie, mit welchen Zeichen (oder Zeichenfolgen) die Variablen der Vorlagendatei beginnen und enden. Der Assistent identifiziert dadurch die Variablen der Vorlagendatei.
13. Im Feld **Ziel-Pfad** bestimmen Sie den Speicherpfad. Dort legt LANconfig die neuen Konfigurationsdateien ab. Klicken Sie auf **Durchsuchen**, um den Ziel-Pfad im lokalen Dateisystem festzulegen. Klicken Sie auf **Weiter**.
14. Ordnen Sie den Spalten der Datenquelle die in der Vorlagendatei verwendeten Variablen zu. Wählen Sie dazu die Spaltennummer aus der Spalten-Liste aus und weisen Sie dieser Nummer eine Variable aus der Variablen-Liste zu. Existieren im Spaltentitel dieselben Variablennamen, wie Sie sie im Skript zwischen den Start- und Endzeichen

angegeben haben, erfolgt ebenfalls eine automatische Zuordnung für alle gefundenen Variablen. Die Spaltentitel in der Ansicht darunter aktualisieren sich sofort bei jeder Änderung. Klicken Sie anschließend auf **Weiter**.



Bei unvollständigen Angaben weist Sie der Assistent auf mögliche Probleme beim Import hin und bietet Ihnen Korrekturen an.

15. Die Zusammenfassung zeigt Ihnen an, welche Aktionen LANconfig im nächsten Schritt ausführt. Sind Änderungen nötig, klicken Sie auf **Zurück**. Sie gelangen somit in die entsprechende Eingabemaske. Mit Klick auf **Weiter** starten Sie den Daten-Import.



Falls Sie ein bereits in LANconfig existierendes Gerät durch den Datenimport überschreiben würden, gibt Ihnen der Assistent die folgenden Optionen zur Auswahl:

- Das betroffene Gerät überschreiben.
- Trotzdem eine Konfigurations-Datei erzeugen.
- Diese Entscheidungen für alle übrigen bereits vorhandenen Geräte übernehmen.

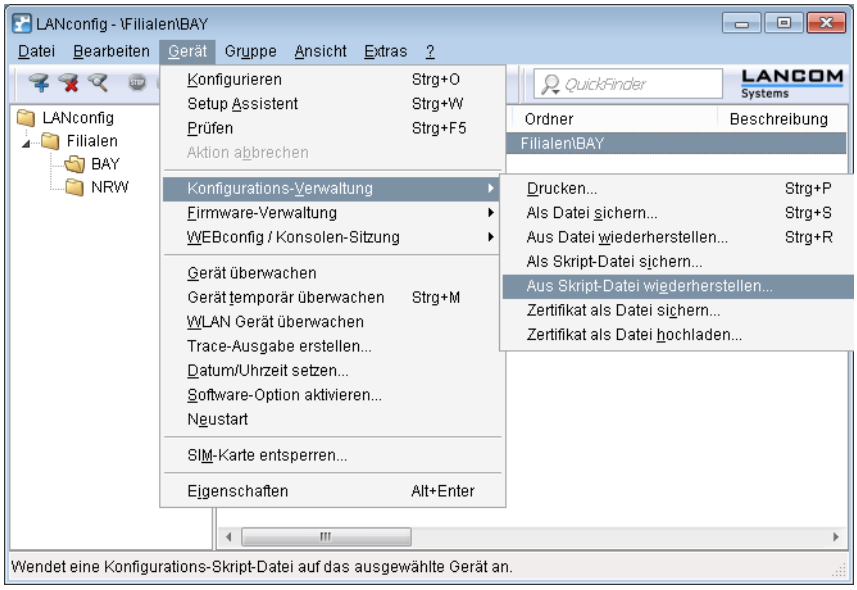
16. Der folgende Statusdialog ist ein Protokoll durchgeführter Aktionen. Mit Klick auf **Kopiere in Zwischenablage** speichern Sie die Statusmeldung in die Zwischenablage. Klicken Sie auf **Weiter**.
17. Zum Abschluss haben Sie die Möglichkeit, die aktuellen Import-Einstellungen für zukünftige Aktionen in einem Profil zu speichern.
18. Beenden Sie den Import mit Klick auf **Fertig stellen**.

Haben Sie die Erstellung einer individuellen Konfigurationsdatei ausgewählt, so speichert der Assistent im angegebenen Ordner je Gerät eine separate Konfigurationsdatei. Diese Konfigurationsdateien werden gemäß dem Dateinamen "<CONFIG_FILENAME>.lcs" benannt, den die CSV-Datei definiert:

```
lang English
flash No
set /Setup/Name "Fil52146"
set /Setup/SNMP/Location "Wuerselen"
cd /Setup/TCP-IP/Network-list
tab Network-name IP-Address IP-Netmask VLAN-ID Interface Src-check Type Rtg-tag Comment
add "INTRANET" 192.168.1.1 255.255.255.0 0 any loose Intranet 0 "local intranet"
cd /
cd /Setup/WAN/PPP
tab Peer Authent.request Authent-response Key Time Try Conf Fail Term Username Rights
add "INTERNET" none PAP "secret1" 6 5 10 5 2 "user1@internet" IP
cd /
cd /Setup/WAN/DSL-Broadband-Peers
del *
tab Peer SH-Time AC-name Servicename WAN-layer ATM-VPI ATM-VCI MAC-Type user-def.-MAC DSL-ifc(s) VLAN-ID
add "INTERNET" 9999 "" "" "PPPOEOA" 1 32 local 000000000000 "" 0
cd /
cd /Setup/IP-Router/IP-Routing-Table
tab IP-Address IP-Netmask Rtg-tag Peer-or-IP Distance Masquerade Active Comment
add 255.255.255.255 0.0.0.0 0 "INTERNET" 0 on Yes "default route"
cd /
flash Yes

# done
exit
```

Der Assistent hat alle Variablen durch die entsprechenden Geräte-Daten ersetzt.

Mit dieser Konfigurationsdatei haben Sie die Möglichkeit, die per Vorlagendatei definierten Geräte-Einstellungen mit LANconfig in weitere Geräte zu übertragen. Markieren Sie dazu das entsprechende Gerät und klicken Sie auf **Gerät** > **Konfigurations-Verwaltung** > **Aus Skript-Datei wiederherstellen**.



3.1.2.16 Software Update für LANtools

Das Software Update für die LANtools bietet Ihnen neue Versionen der LANtools und der Firmware zu Ihren Geräten automatisch zum Download an.

Neue Versionen der LANtools (LANconfig, LANmonitor und WLANmonitor) laden Sie direkt aus dem frei zugänglichen Download-Bereich des LANCOM Web-Servers.

LANCOM Software Update manuell starten

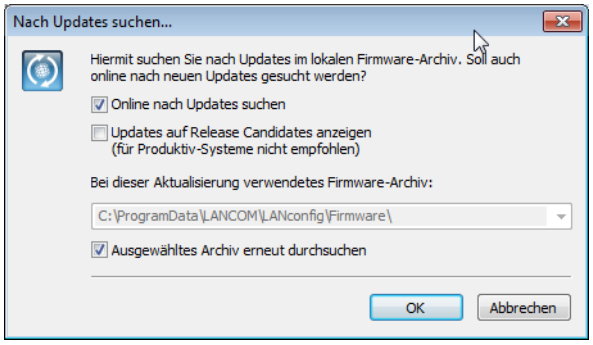
Um das Software Update für LANconfig manuell zu starten, gehen Sie vor, wie in den folgenden Schritten beschrieben:

1. Starten Sie LANconfig.
2. Wählen Sie im Menü **Extras** den Eintrag **Nach Updates suchen**.

LANconfig sucht im lokalen Firmware-Archiv nach verfügbaren Updates. Optional können Sie die Suche um die folgenden Punkte erweitern:

- Suchen Sie online nach weiteren Updates im Download-Bereich des LANCOM Web-Servers.
- Beziehen Sie Release Candidates in die Suche ein. Wenn Sie diese Option einschalten, wird das Software Update nicht nur die für den Einsatz in Produktivumgebungen freigegebenen Software-Versionen zum Download anbieten, sondern auch die verfügbaren Release Candidates.

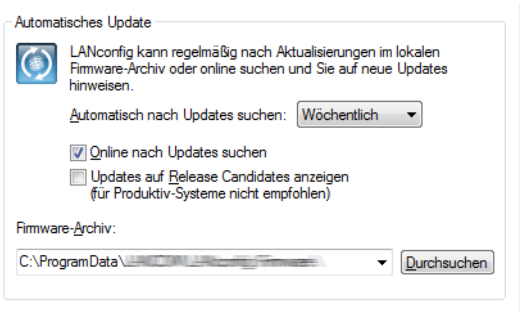
Release Candidates enthalten die neuen Features der kommenden Software-Version und sind ausführlich getestet. Bis zur endgültigen Freigabe der Version sind – u. a. aufgrund der Rückmeldungen der Anwender – noch weitere Optimierungen der Software möglich.



Automatisches Software-Update bei Programmstart

Um das Software-Update für LANconfig beim Start der Applikation automatisch zu starten, gehen Sie wie in den folgenden Schritten beschrieben vor:

1. Starten Sie LANconfig.
2. Wählen Sie im Menü **Extras** den Eintrag **Optionen**.
3. Wechseln Sie auf die Seite **Update**.



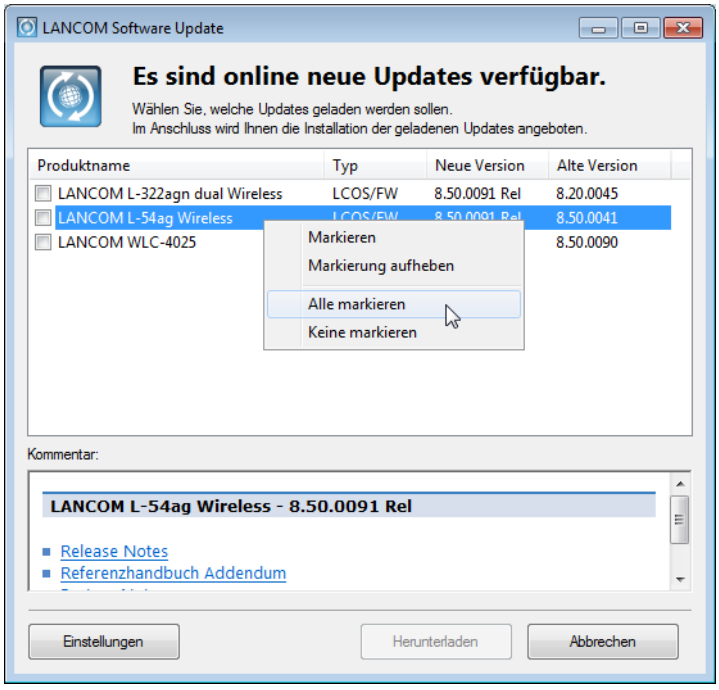
4. Wählen Sie das zeitliche Intervall für die automatische Suche nach Updates (**Täglich**, **Wöchentlich** oder **Monatlich**) aus.

Lesen Sie für die übrigen Einstellungsmöglichkeiten von Software-Update auch das Kapitel *Update* auf Seite 241.

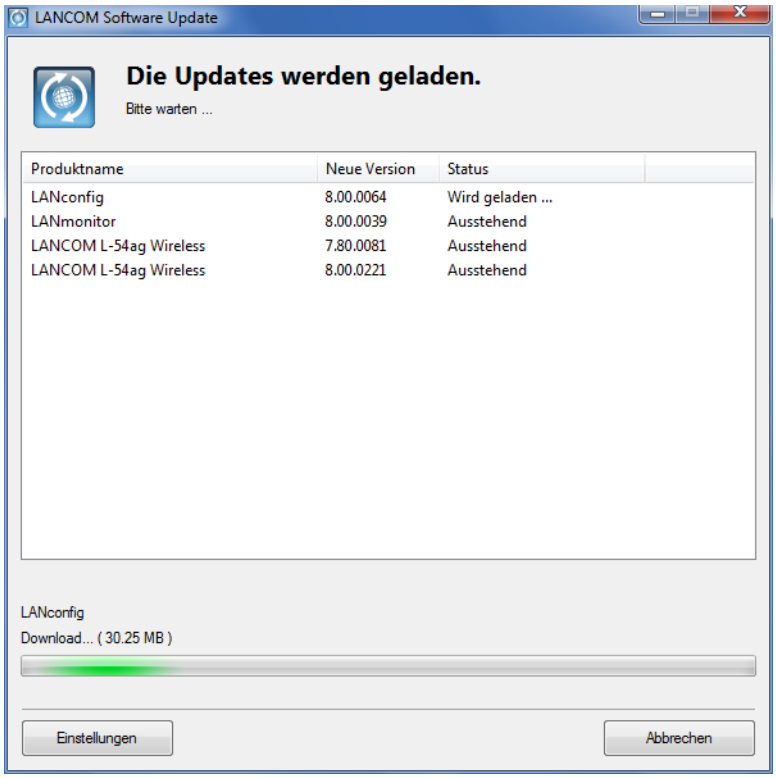
Auswahl und Installation der verfügbaren Updates

Nach einer erfolgreichen Verbindung zum Update-Server zeigt LANconfig die verfügbaren Updates an.

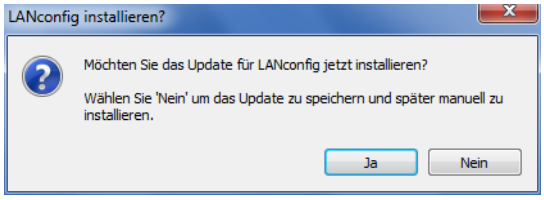
Wählen Sie die gewünschten Versionen aus und klicken Sie **Herunterladen**. Klicken Sie alternativ mit der rechten Maustaste auf einen der Einträge und wählen Sie im Kontextmenü **Alle markieren** oder **Keine markieren**.



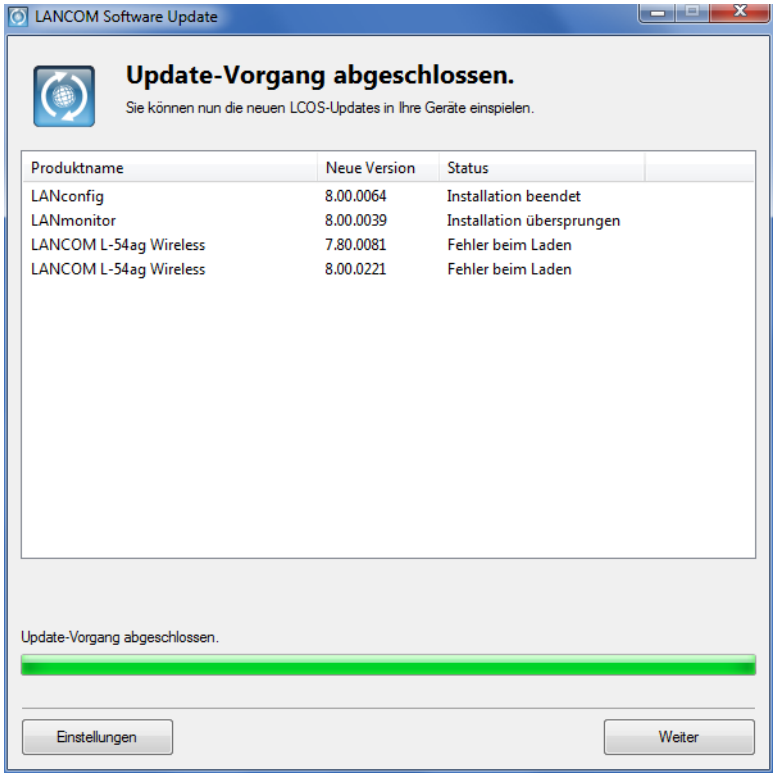
Software Update lädt die gewählte Software nun nacheinander herunter und speichert die Dateien im Firmware-Archiv.



Nach dem erfolgreichen Download bietet Software Update die Installation der geladenen Software an (nur LANconfig und LANmonitor):



Nach der Installation zeigt Software Update die Ergebnisse des Updates-Vorgangs an:

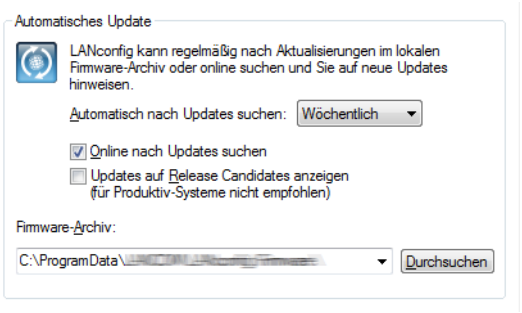


3.1.2.17 Suche nach Firmware-Updates im Archiv

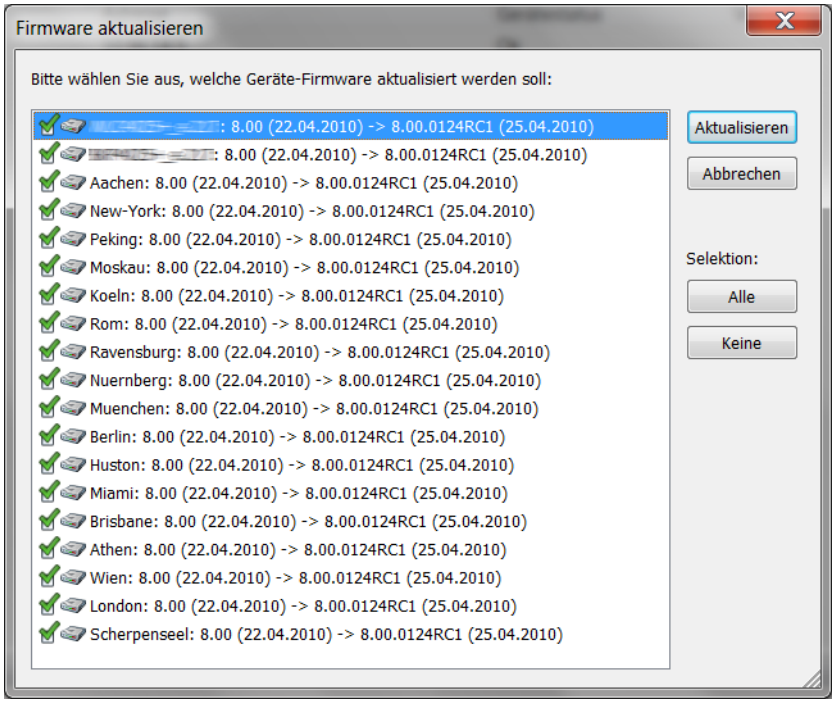
Um das Update auf neue Firmwareversionen in den Geräten möglichst komfortabel zu gestalten, werden die Firmware-Dateien für die verschiedenen Modelle und LCOS-Versionen idealerweise in einem zentralen Archiv-Verzeichnis abgelegt. Die Suche nach neuen Firmware-Versionen in diesem Verzeichnis kann entweder manuell angestoßen werden oder nach jedem Start von LANconfig automatisch durchgeführt werden.

Automatische Suche nach Firmware-Updates

Das Verzeichnis, in dem LANconfig nach den Updates sucht, konfigurieren Sie unter **Extras** > **Optionen** > **Update** > **Firmware-Archiv**.

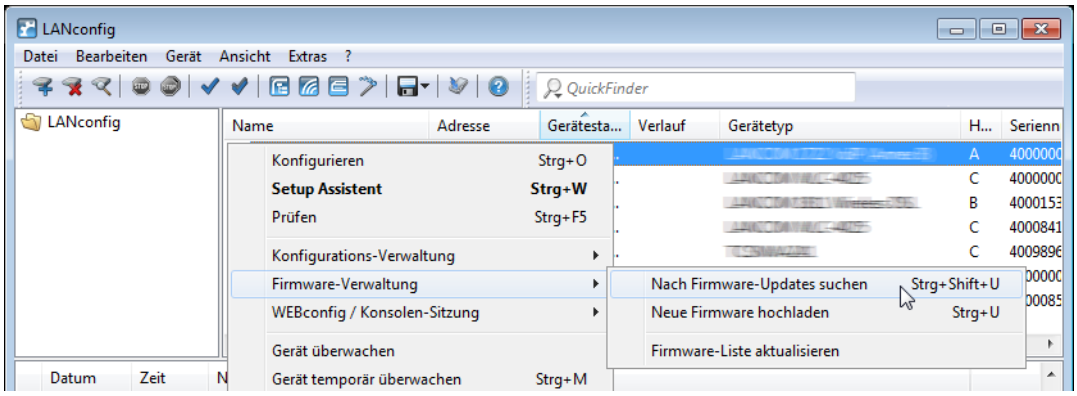


Wenn Sie ein Intervall für die automatische Suche nach Optionen festlegen, zeigt LANconfig nach dem Start automatisch die Geräte an, für die neue Updates zur Verfügung stehen.



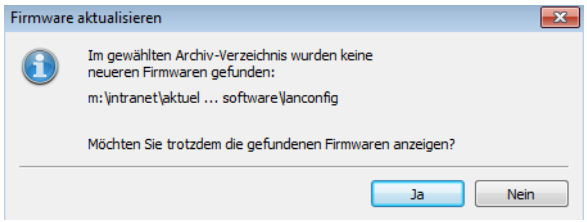
Manuelle Suche nach Firmware-Updates

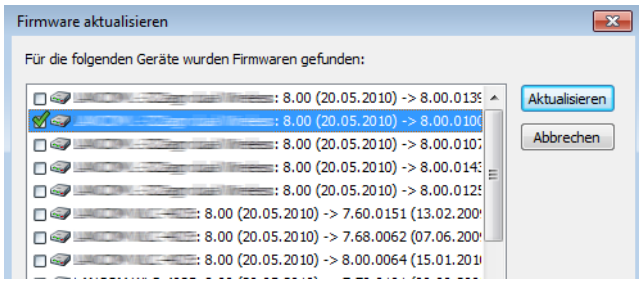
Für die manuelle Suche nach Firmware-Updates klicken Sie mit der rechten Maustaste auf einen markierten Eintrag in der Geräteliste und wählen im Kontextmenü den Punkt **Firmware-Verwaltung** > **Nach Firmware-Updates suchen**. Wenn Sie mehrere Geräte markiert haben, erscheint der Punkt **Nach Firmware-Updates suchen** direkt im Kontextmenü.



Komplette Liste der Firmware-Versionen einsehen

Wenn bei der Suche im Archiv keine neueren Firmware-Versionen gefunden wurden, können Sie alternativ die komplette Liste alle gefundenen Firmware-Dateien ansehen. So können Sie u. a. auch auf ältere Versionen zurückschalten. LANconfig zeigt alle gefundenen Versionen für alle markierten Geräte an, dabei auch den aktuellen Versionsstand der Geräte. Für jedes Gerät können Sie genau eine Firmware-Version auswählen, die dann in das Gerät eingespielt wird.





3.1.2.18 Schlüssel-Fingerprints bei der Inbetriebnahme von CC-Geräten exportieren

Ab LCOS 8.84 haben Sie die Möglichkeit, bei der Inbetriebnahme von CC-Geräten die eingespielten SSH-Key Fingerprints komfortabel mit LANconfig zu exportieren. LANconfig legt dazu beim Durchlaufen des CC-Inbetriebnahme-Assistenten die Datei **CCWizSummary.csv** an, welche die IP-Adresse des Gerätes, den Gerätenamen und dessen (SSH) Schlüssel-Fingerprint enthält. Über die so erzeugte Liste kann sich dann z. B. ein Systemadministrator bei der Fernwartung bzw. nach einem Rollout vor dem Login vergewissern, dass er mit dem korrekten Gerät verbunden ist.

Standardmäßig speichert LANconfig die CSV-Datei unter `C:\Program Files (x86)\LANCOM\LANconfig\Logging\`. Sie haben aber auch die Möglichkeit, diesen Pfad im Eingabefeld unter **Extras** > **CC-Inbetriebnahme-Assistent starten** > **Einstellungen** > **Pfad** zu verändern.

3.1.3 Die Menüstruktur in LANconfig

Über die Menüleiste können Sie Geräte und deren Konfigurationen verwalten sowie das Aussehen und die Funktionsweise von LANconfig anpassen.

3.1.3.1 Datei

Unter diesem Menüpunkt verwalten Sie Geräte allgemein und beenden LANconfig.

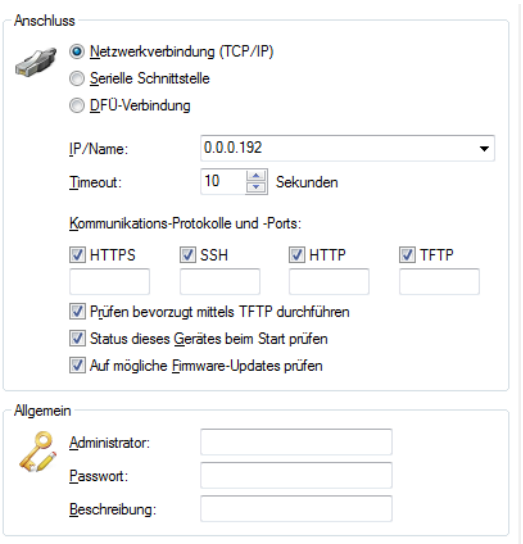
Gerät hinzufügen

Über **Datei** > **Gerät hinzufügen** fügen Sie der Geräteübersicht ein neues Gerät hinzu. Es öffnet sich ein Dialog, in dem Sie u. a. Einstellungen für die Verbindung zum das Gerät und die Sicherung vornehmen.

Allgemein

Auf dieser Seite legen Sie fest, wie sich LANconfig mit einem Gerät verbindet. Zudem können Sie die Zugangsdaten dauerhaft im Programm hinterlegen, um nicht nach jedem Start von LANconfig beim ersten Verbindungsaufbau die Daten manuell einzugeben.

Wenn Sie Benutzernamen und Passwort dauerhaft speichern, erhält jeder Nutzer Zugang zu dem Gerät, der auch LANconfig ausführen darf.



Anschluss

Im Bereich **Anschluss** nehmen Sie die Anschluss-Einstellungen für ein Gerät vor.

Wählen Sie hier aus, wie das Gerät erreichbar ist:

- **Netzwerkverbindung (TCP/IP)**: Wählen Sie diese Option, wenn das Gerät über ein IP-Netzwerk zu erreichen ist.
- **Serielle Schnittstelle**: Wählen Sie diese Option, wenn das Gerät über die serielle Schnittstelle dieses Computers angeschlossen ist.
- **DFÜ-Verbindung**: Wählen Sie diese Option aus, wenn Sie das Gerät über das DFÜ-Netzwerk erreichen wollen.

  Bitte beachten Sie, dass nicht jedes Gerät die Fernkonfiguration über eine DFÜ-Verbindung unterstützt.
- **IP/Name:**: Geben Sie die IP-Adresse des Gerätes an. Sie können auch einen Domain-Namen (DN oder FQDN) angeben. Dieser Name wird bei jedem Zugriff überprüft. LANconfig speichert und verwendet die

dabei aufgelöste IP-Adresse. Sollte die Überprüfung einmal nicht möglich sein, greift LANconfig auf die letzte erfolgreich aufgelöste IP-Adresse zurück.

- **Timeout**: Geben Sie hier an, wieviele Sekunden das Programm auf Antworten von diesem Gerät warten soll.
- **HTTPS**, **SSH**, **HTTP**, **TFTP**: Mit dieser Auswahl aktivieren Sie die einzelnen Protokolle für die Operationen Firmware-Upload sowie Konfigurations- und Script-Upload und -Download. Bei diesen Operationen versucht LANconfig, diese Protokolle in der Reihenfolge HTTPS, SSH, HTTP und TFTP zu verwenden. Schlägt die Übertragung mit einem der gewählten Protokolle fehl, versucht LANconfig automatisch das nächste Protokoll.
- **Prüfen bevorzugt mittels TFTP durchführen**: Diese Option bewirkt, dass LANconfig ungeachtet der ausgewählten Protokolle bevorzugt mit TFTP prüft. Dies ist vorteilhaft bei Geräten, die im LAN erreichbar sind. Die Prüfung erfolgt schneller und belastet den Rechner weniger, was sich bei der Bearbeitung einer größeren Anzahl von Geräten bemerkbar macht. Die fehlende HTTPS-Verschlüsselung stellt im LAN keinen Nachteil dar.
- **Status dieses Gerätes beim Start prüfen**: Markieren Sie die Option, wenn LANconfig den Status des Gerätes beim Start prüfen soll.
- **Auf mögliche Firmware-Updates prüfen**: Markieren Sie die Option, wenn LANconfig auf mögliche Firmware-Updates prüfen soll.

Wie im Abschnitt *Kommunikationsprotokolle und Ports* auf Seite 210 erwähnt, testet LANconfig andere Protokolle und führt sie aus, wenn TFTP nicht verfügbar ist. Auch hier sind die globalen Einstellungen den gerätespezifischen übergeordnet.

Nachdem Sie die Einstellungen vorgenommen haben, versucht das Programm das Gerät zu erreichen und dessen Namen und Version abzufragen. Wenn dies fehlschlägt, zeigt LANconfig eine kurze Fehlermeldung in der Spalte **Status**.

Allgemein

In diesem Bereich hinterlegen Sie die Zugangsdaten und eine Beschreibung zum Gerät.

- **Administrator**: Geben Sie hier den Benutzernamen eines Administrators ein.
- **Passwort**: Geben Sie hier das zugehörige Passwort ein.
- **Beschreibung**: Geben Sie hier die Beschreibung des Gerätes ein, die LANconfig im Hauptfenster anzeigen soll.

Kommunikationsprotokolle und Ports

LANconfig führt sowohl die Prüfung der Geräte auf Erreichbarkeit als auch die Aktionen Firmware-Upload sowie Skript-/Konfigurations-Upload bzw. -Download über die hier ausgewählten Kommunikationsprotokolle durch.

LANconfig versucht in der Reihenfolge HTTPS, SSH, HTTP und TFTP, mit jedem gewählten Protokoll die oben aufgeführten Geräte-Aktionen auszuführen. Endet eine Aktion aufgrund des verwendeten Protokolls fehlerhaft, wiederholt LANconfig sie mit dem nächsten ausgewählten Protokoll.

Damit die Aktion überhaupt funktionieren kann, muss mindestens ein Protokoll ausgewählt sein.

Bei Verwendung von HTTP(S) und einem Proxyserver kann es notwendig sein, diesen Proxyserver zu umgehen, damit LANconfig die Geräte erreichen kann. In den Internetoptionen der Systemsteuerung von Windows können Sie den Proxyserver für lokale Adressen umgehen. In den erweiterten Einstellungen der Internetoptionen können Sie außerdem weitere Adressen definieren, die nicht über den Proxyserver kontaktiert werden sollen.

Zum Einstellen der Protokolle gibt es jeweils eine gerätespezifische und eine globale Einstellmöglichkeit. Die globalen Einstellungen im Options-Menü sind den gerätespezifischen übergeordnet. Dadurch ist es möglich, die einzelnen Protokolle mit Hilfe eines globalen Schalters für alle Geräte auszuschalten.

Tipps

- Wenn sich das Gerät noch im Auslieferungszustand befindet, hat es noch keine eigene IP-Adresse. In diesem Fall geben Sie die IP-Adresse Ihres Computers ein und ersetzen Sie den letzten Abschnitt der Ziffernfolge durch '254': Wenn ihr Computer die IP-Adresse '192.168.1.1' hat, dann weisen Sie dem Gerät die IP-Adresse '192.168.1.254' zu.
- Wenn Sie nicht wissen, welche Adresse ein Gerät hat, können Sie auch danach über **Datei** > **Geräte** suchen.

Mögliche für Probleme beim Herstellen einer Verbindung mit einem neuen Gerät

Wenn LANconfig ein Gerät nicht erreicht, erscheint unter Status eine der unten aufgeführten Fehlermeldungen. Um ein Gerät erneut zu überprüfen, markieren Sie es in der Liste, und klicken Sie dann auf in der Menüleiste auf **Gerät** > **Prüfen**.

- **Serieller Fehler**: LANconfig konnte die serielle Schnittstelle nicht öffnen. Schließen Sie alle Programme, die möglicherweise darauf zugreifen.
- **IP-Fehler**: Überprüfen Sie, ob die IP-Adresse des Gerätes richtig ist und ob Ihr Computer korrekt mit dem Netzwerk verbunden ist. Stellen Sie außerdem sicher, dass das TCP/IP-Protokoll installiert und richtig konfiguriert ist.
- **Keine Antwort**: Überprüfen Sie, ob die IP-Adresse des Gerätes richtig ist. Möglicherweise ist auch die Netzwerkverbindung zwischen Ihrem Rechner und dem Gerät zu langsam oder unzuverlässig.
- **Status unbekannt**: LANconfig hat das Gerät zwar über die angegebene IP-Adresse erreicht, konnte jedoch keine weiteren Informationen abfragen. Möglicherweise unterstützt LANconfig dieses Gerät nicht.
- **Zugriff verweigert:** Das Gerät ist für den Zugriff von Ihrem Rechner aus gesperrt.

Sicherung

Auf dieser Seite aktivieren und konfigurieren Sie die gerätespezifischen Sicherungseinstellungen. Die dazugehörigen Einstellungsmöglichkeiten sind mit den globalen identisch (siehe *Sicherung* auf Seite 238).

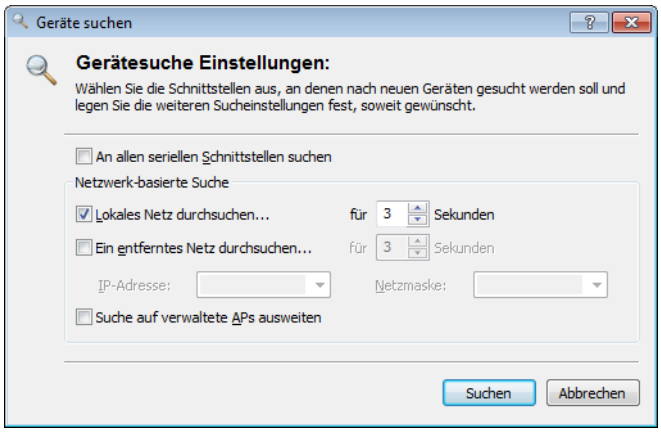
Gerät löschen

Wenn Sie ein Gerät markiert haben, können Sie es unter **Datei** > **Gerät löschen** entfernen. Sie können auch die Taste 'Entf' drücken, um ein Gerät zu löschen.

Mit dem Löschen entfernen Sie das Gerät nur aus der aktuellen Ansicht. Sie können es jederzeit wieder über **Datei** > **Gerät hinzufügen** oder **Datei** > **Geräte suchen** hinzufügen.

Geräte suchen

Über diesen Menüpunkt starten Sie die automatische Suche nach neuen Geräten, um Sie der Geräteübersicht hinzuzufügen.



Wählen Sie aus, wo nach Geräten gesucht werden soll:

- An allen seriellen Schnittstellen

- Im lokalen Netz
- In einem entfernten Netz

  Wenn Sie ein entferntes Netz durchsuchen wollen, müssen Sie die Adresse des Netzwerkes und die zugehörige Netzmaske angeben.

- Sie können die Suche bei Bedarf auch auf verwaltete Access Points (APs) ausweiten.

Klicken Sie auf **Suchen**, um die Suche zu starten. Die gefundenen Geräte werden automatisch der Liste hinzugefügt.

Wenn ein Gerät gefunden wird, das bereits in der Liste vorhanden ist, wird es nicht ein zweites Mal der Liste hinzugefügt. Daher kann es sein, dass weniger Geräte neu hinzukommen, als während des Suchvorgangs gemeldet werden.

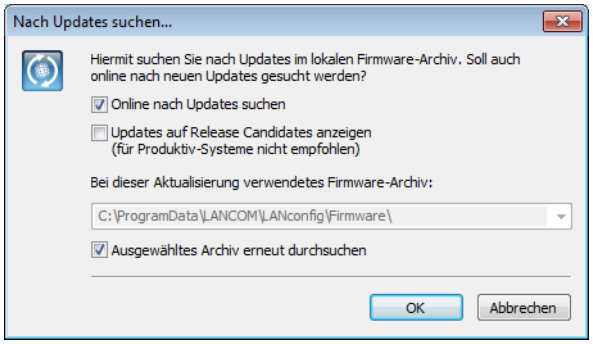
Geräte in dieser Ansicht prüfen

Unter **Datei** > **Geräte in dieser Ansicht prüfen** können Sie den Status von allen Geräten der aktuellen Ansicht abfragen. Der Gerätestatus zeigt z. B. an, dass eine neue Firmware hochgeladen wird oder ein Gerät nicht erreicht werden kann.

Gerät lassen sich nur konfigurieren, wenn der Gerätestatus **Ok** ist.

Alle Geräte auf Firmware-Updates prüfen

Startet manuell die automatische Suche nach Firmware-Updates. Dabei durchsuchen Sie die LANCOM Online-Datenbank sowie Ihr lokales Firmware-Archiv nach aktuelleren Firmware-Versionen als derzeit den Geräten installiert. Lesen Sie hierzu auch das Kapitel *Suche nach Firmware-Updates im Archiv* auf Seite 206.



Alle Aktionen abbrechen

Über diesen Menüpunkt brechen Sie alle laufenden Aktion für alle in der Ansicht gezeigten Geräte ab. Sie können diese Funktion nutzen, um z. B. das Laden einer Firmware oder eines Skripts abzubrechen. Insbesondere Vorgänge, die durch Mehrfachauswahl oder das Ausführen von Aktionen gestartetet wurden, können damit komplett gestoppt werden.

Geräte/Konfigurationen aus CSV-Datei

Importieren Sie in LANconfig eine große Anzahl Geräte aus einer Skript-Vorlage gleichzeitig, indem Sie einen Import-Assistenten für entsprechende Geräte-Dateien verwenden. Zusätzlich haben Sie die Möglichkeit, mit dieser Geräte-Datei und einer Konfigurations-Vorlagendatei eine individuelle Konfigurationsdatei pro Gerät erstellen zu lassen. Die Vorlagendatei enthält Variablen für die Werte der Geräte-Datei.

Weitere Informationen finden Sie im Abschnitt *Import aus einer Datenquelle (CSV)* auf Seite 197.

Geräte-Liste exportieren

Exportieren Sie die Liste der im Netz gefundenen Geräte, um diese später bequem in einem Durchgang wieder in LANconfig zu importieren. LANconfig speichert die Liste der verwalteten Geräte als CSV-Datei.

Weitere Informationen finden Sie im Abschnitt *Import aus einer Datenquelle (CSV)* auf Seite 197.

Neuer Ordner

Über diesen Menüpunkt legen Sie in der Verzeichnisstruktur einen neuen Ordner an. Siehe dazu auch *Verzeichnisbäume zur Organisation nutzen* auf Seite 178.

Beenden

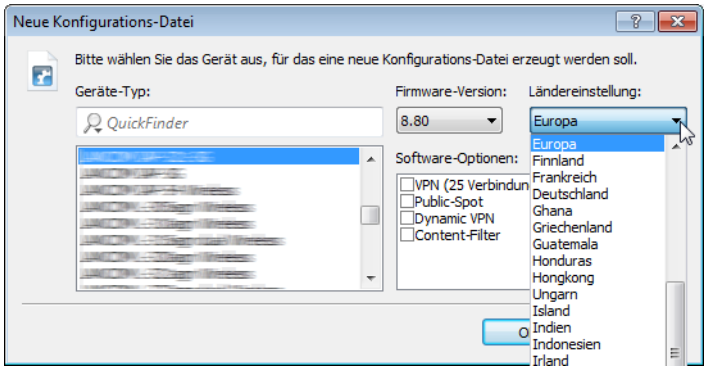
Über diesen Menüpunkt beenden und schließen Sie LANconfig.

3.1.3.2 Bearbeiten

Unter diesem Menüpunkt verwalten Sie die Konfigurations-Dateien aller Geräte in einer Geräteliste.

Neue Konfigurations-Datei

Mit dieser Funktion lassen sich eine Konfiguration und ein Geräte-Eintrag in der Geräteliste anlegen, ohne dass eine Verbindung zu einem real existierenden Gerät besteht.



Geräte-Typ

Wenn Sie eine Konfigurations-Datei anlegen wollen, müssen Sie angeben, für welches Gerät diese Konfiguration bestimmt ist, damit das Programm die richtigen Parameter für das Gerät anzeigen kann. Wählen Sie aus der Liste das von Ihnen gewünschte Gerät aus.

Nutzen Sie den QuickFinder, um die Liste der verfügbaren Geräte einzuschränken. Geben Sie dazu einen Teil des gewünschten Geräte-Typs in das QuickFinder-Feld ein, der Dialog reduziert die Auswahl automatisch auf die passenden Geräte.

Firmware-Version

Da verschiedene Firmware-Versionen oft voneinander abweichende Einstellungsmöglichkeiten bieten, muss das Programm wissen, für welche Version diese Konfiguration bestimmt ist. Geben Sie hier bitte die Versionsnummer der Firmware in dem gewünschten Gerät an. Das Programm wird Ihnen mitteilen, wenn diese Versionsnummer nicht korrekt ist oder nicht unterstützt wird

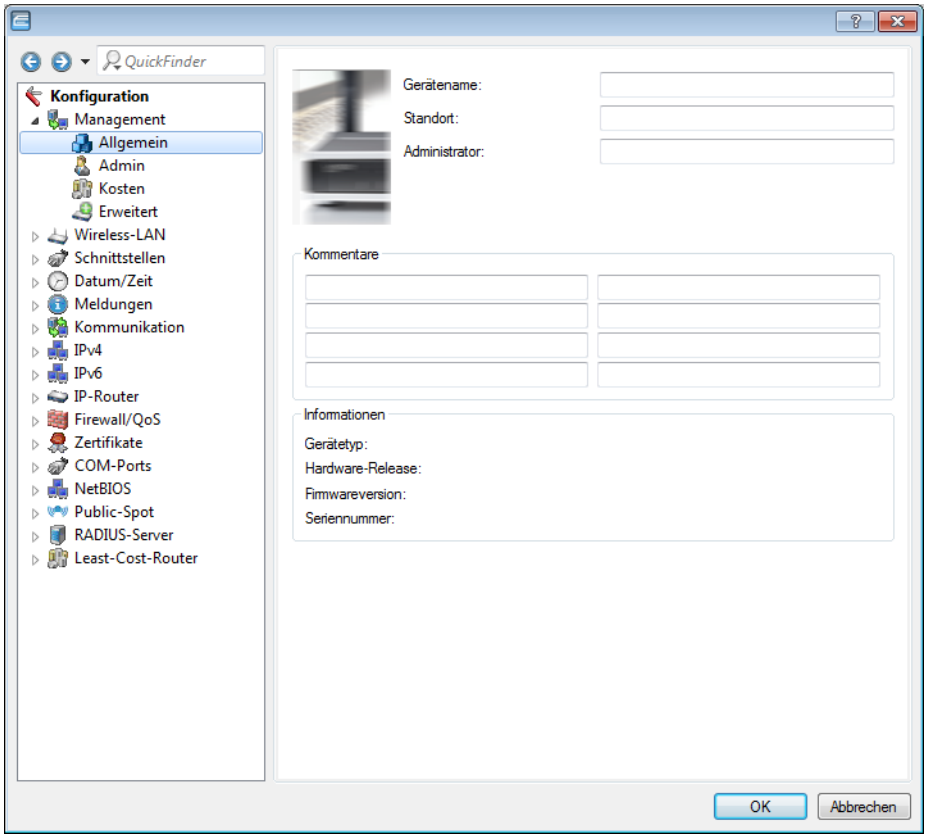
Ländereinstellung

Wählen Sie das Land bzw. die Region, für welche die Konfigurations-Datei gelten soll. Die Konfigurations-Datei bietet dann nur die Parameter an, welche in dem gewählten Land bzw. in der gewählten Region erlaubt sind.

Software-Optionen

Wählen Sie die entsprechenden Software-Optionen aus, die angezeigt werden sollen.

Mit einem Klick auf **OK** öffnet sich der Konfigurationsdialog.

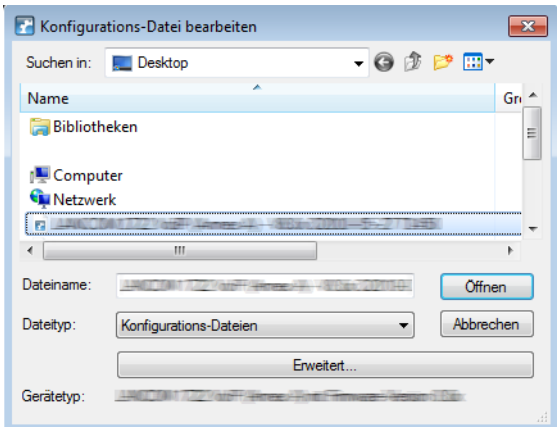


Sie können auch eine neue Konfigurationsdatei erstellen, indem Sie mit einem mit einem Rechtsklick auf Ihren Desktop im Kontext-Menü **Neu** > **LANconfig Konfiguration** auswählen.

Die Informationen zu den einzelnen Konfigurationsparametern finden Sie in der LCOS-Dokumentation.

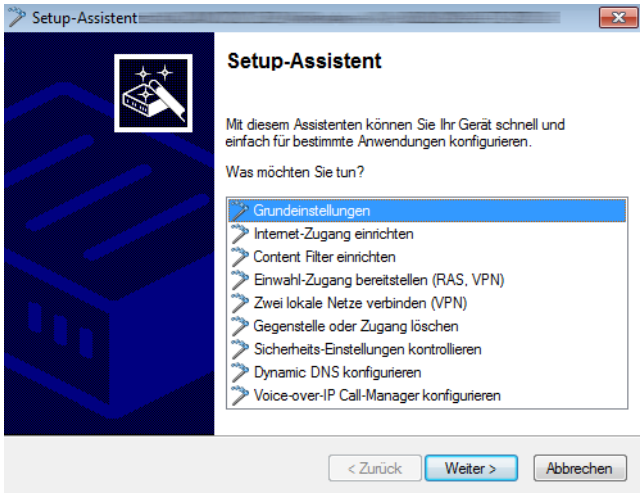
Konfigurations-Datei bearbeiten

Über diesen Menüpunkt wählen Sie eine gespeicherte Konfigurationsdatei aus, um sie im Kofigurationsdialog zu bearbeiten.



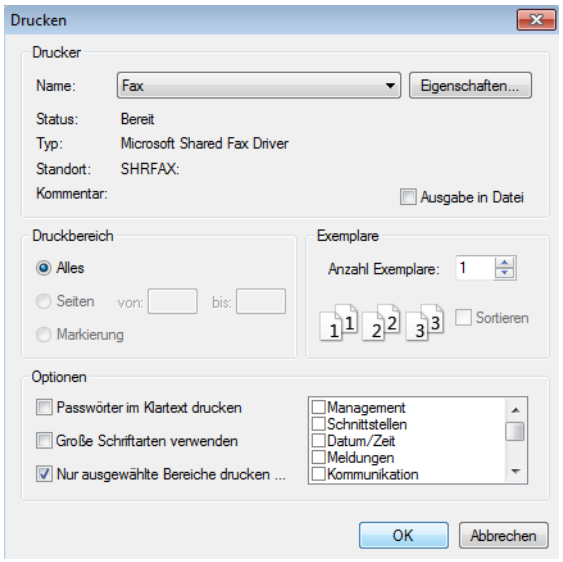
Konfigurations-Datei assistieren

Über diesen Menüpunkt wählen Sie eine gespeicherte Konfigurationsdatei aus, um sie mit dem Setup-Assistenten zu bearbeiten.



Konfigurations-Datei drucken

Über diesen Menüpunkt drucken Sie eine gespeicherte Konfigurationsdatei aus.



Zusätzlich zum normalen Druckdialog haben Sie im Abschnitt **Optionen** folgende Einstellungsmöglichkeiten:

Passwörter im Klartext drucken

Wenn Sie diese Funktion aktivieren werden Ihre Passwörter im Klartext gedruckt. Das Hauptgerätepasswort steht im Ausdruck auf der ersten Seite

Große Schriftarten verwenden

Der Ausrdruck erfolgt in einer größeren Schrift.

Nur ausgewählte Bereiche drucken

Drucken Sie nur bestimmte Konfigurationsbereiche, z. B. nur WLAN-Controller.

Geräte in dieser Ansicht markieren

Über diesen Menüpunkt markieren Sie alle aktuellen Geräteeinträge in der gewählten Ansicht.

Markierung umkehren

Über diesen Menüpunkt kehren Sie die Markierung aller aktuellen Geräteeinträge in der gewählten Ansicht um. Dadurch werden alle Einträge, die vorher markiert waren, unmarkiert und alle Einträge, die vorher nicht markiert waren, markiert.

3.1.3.3 Gerät

Unter diesem Menüpunkt können Sie die Konfiguration von am Netzwerk angeschlossenen Geräten bearbeiten, Firmware-Updates verwalten und Geräteverbindungen überwachen.

Die dazugehörigen Funktionen sind nur auswählbar, wenn Sie mindestens ein Gerät in der Geräteliste markiert haben. Dieses Menü können Sie ebenfalls über die rechte Maustaste für ein markiertes Gerät aufrufen.

Konfigurieren

Lädt die Konfiguration des markierten Gerätes über die in den Eigenschaften definierten Anschluss-Einstellungen, insofern eine Verbindung auf diesem Weg möglich ist. Die Konfiguration wird dann im Fenster zur Konfigurations-Einstellung angezeigt und kann bearbeitet werden.

Setup Assistent

Lädt die Konfiguration des markierten Gerätes über die in den Eigenschaften definierten Anschluss-Einstellungen, insofern eine Verbindung auf diesem Weg möglich ist. Die Konfiguration wird dann im Setup Assistent geöffnet, welcher Ihnen bei der Konfiguration ausgewählter Einsatzszenarien behilflich ist.

Bei WLCs mit „WLC High Availability Clustering XL-Option“ ist es möglich, alle aufgeführten WLCs zu markieren und gemeinsam über den WLC-Clustering-Assistenten zu konfigurieren (siehe *1-Klick WLC High Availability Clustering-Assistent*).

Quick Rollback

Über diesen Menüpunkt haben Sie die Möglichkeit, automatisch erstelle Konfigurationssicherungen für das ausgewählte Gerät mit nur einem Klick wiederherzustellen und die Gerätekonfiguration somit auf einen früheren Konfigurationsstand zurückzusetzen. Mehr zu dieser Funktion erfahren Sie unter *Quick Rollback* auf Seite 195.

Prüfen

Prüft die Geräte bzw. die Auswahl an Geräten durch Auslesen der Geräte-Information über den ausgewählten Anschluss. Aus dem Verlauf dieser Operation wird der Status generiert. Der Gerätestatus zeigt z. B. an, dass eine neue Firmware hochgeladen wird oder ein Gerät nicht erreicht werden kann.

Gerät lassen sich nur konfigurieren, wenn der Gerätestatus **Ok** ist.

Aktion abbrechen

Über diesen Menüpunkt brechen Sie eine laufende Aktion für das ausgewählte Gerät ab. Sie können diese Funktion nutzen, um z. B. das Laden einer Firmware oder eines Skripts abzubrechen. Aktionen auf anderen Geräten, die noch nicht abgeschlossen sind, laufen jedoch weiter.

Konfigurations-Verwaltung

Mit den Funktionen zur Konfigurations-Verwaltung können Sie Konfigurationen sichern und wiederherstellen, und so z. B. die Konfiguration eines Gerätes in ein anderes übertragen. Wenn die Firmware-Versionen der beiden Geräte verschieden sind, zeigt Ihnen das Programm die Unterschiede in der Konfiguration und warnt Sie davor, dass Parameter

verloren gehen. Darüber hinaus erfolgt über diesen Menüpunkt auch das Dateimanagement, bei dem Sie besondere Dateien wie Templates oder Zertifikate direkt in das Gerät laden.

Folgende konfigurationsspezifische Aktionen stehen Ihnen zur Auswahl:

Drucken

Lädt die Konfiguration des markierten Geräts über die in den Eigenschaften definierten Anschluss-Einstellungen, sofern eine Verbindung auf diesem Weg möglich ist. Im folgenden Druckdialog können dann dieselben Optionen zur Ausgabe wie unter **Bearbeiten** > **Konfigurations-Datei drucken** gewählt werden. Nach Bestätigung wird die Konfiguration ausgedruckt.

Als Datei sichern

Speichert die Konfiguration des ausgewählten Geräts an einem wählbaren Ort als Konfigurationsdatei. Geben Sie in dem Datei-Auswahldialog einen Namen für die Konfigurationsdatei ein. Klicken Sie anschließend auf **Speichern**.

Aus Datei wiederherstellen

Lädt in das ausgewählte Gerät eine im Folgenden zu bestimmende Konfigurationsdatei (z. B. aus der automatischen Sicherung). Wählen Sie in dem Datei-Auswahldialog die gespeicherte Konfiguration aus, und klicken Sie auf **Öffnen**.

Als Skript-Datei sichern

Speichert die Konfiguration des ausgewählten Geräts an einem wählbaren Ort als Skript-Datei. Dabei können dieselben Optionen für Skript-Dateien wie unter den Sicherungseinstellungen gewählt werden.

Aus Skript-Datei wiederherstellen

Lädt in das ausgewählte Gerät eine im Folgenden zu bestimmende Skript-Datei (z. B. aus der automatischen Sicherung).

Zertifikat als Datei sichern

Bestimmen Sie in dem sich öffnenden Dialog, welches Zertifikat aus dem gewählten Gerät in einer Datei gesichert werden soll. Der Dateityp hängt von der Auswahl des Zertifikats ab.

Zertifikat oder Datei hochladen

Über diesen Menüpunkt laden Sie Zertifikate und besondere Dateien in das Gerät. Zertifikate benötigen Sie z. B. für eine VPN-Verschlüsselung oder den Betrieb eines WLAN-Controllers. Die 'besonderen Dateien' hingegen stellen Dateien dar, mit denen Sie geräteeigene Vorlagen ersetzen können (z. B. indidivuelle Templates für den Rollout-Assistenten) oder die Sie für die Nutzung bestimmter Funktionen ins Gerät laden müssen (z. B. Nutzungsbedingungen für das Public Spot Modul).



Sie können für jede Konfiguration, die Sie speichern, eine Beschreibung eingeben. So lassen sich bequem verschiedene Konfigurationen für verschiedene Geräte verwalten.

Firmware-Verwaltung

Über diesen Menüpunkt aktualisieren Sie die Geräte-Firmware oder schalten das Gerät auf eine andere Firmware-Version um. Folgende Firmware-spezifische Aktionen stehen Ihnen zur Auswahl:

Nach Firmware-Updates suchen

Startet manuell die automatische Suche nach Firmware-Updates. Dabei durchsuchen Sie die LANCOM Online-Datenbank sowie Ihr lokales Firmware-Archiv nach aktuelleren Firmware-Versionen als derzeit auf dem ausgewählten Gerät installiert. Lesen Sie hierzu auch das Kapitel *Suche nach Firmware-Updates im Archiv* auf Seite 206.

Neue Firmware hochladen

Öffnet einen Datei-Auswahldialog, über den Sie eine bestimmte Firmware-Datei in das ausgewählte Gerät hineinladen können.

Weil die vorhandene Firmware eines Gerätes während des Uploads der neuen Firmware überschrieben wird, darf dieser Vorgang auf keinen Fall unterbrochen werden, da das Gerät anschließend möglicherweise nicht mehr lauffähig ist.

Im Testmodus laufende Firmware freischalten ([Speicherplatz-Nummer])

Sofern Sie für ein Gerät ein Firmware-Update durchgeführt und die zugehörige Firmware im (zeitlich beschränkten) Testmodus hochgeladen haben, können Sie über diesen Menüpunkt die Firmware dauerhaft aktivieren. Mehr zu der Funktion erfahren Sie im Abschnitt *FirmSafe* auf Seite 88.

1, 2 [Firmare-Version] vom [Datum]

Geräte mit FirmSafe sind dazu in der Lage, zwei Firmware-Versionen zu verwalten, um z. B. im Falle eines fehlgeschlagenen Updates oder bei Problemen auf die vorherige Firmware zurückzuschalten. Über die Speicherplatz-Nummern 1 und 2 haben Sie die Möglichkeit, einen Firmware-Stand auszuwählen und das Gerät mit einer anderen installierten Firmware zu starten.

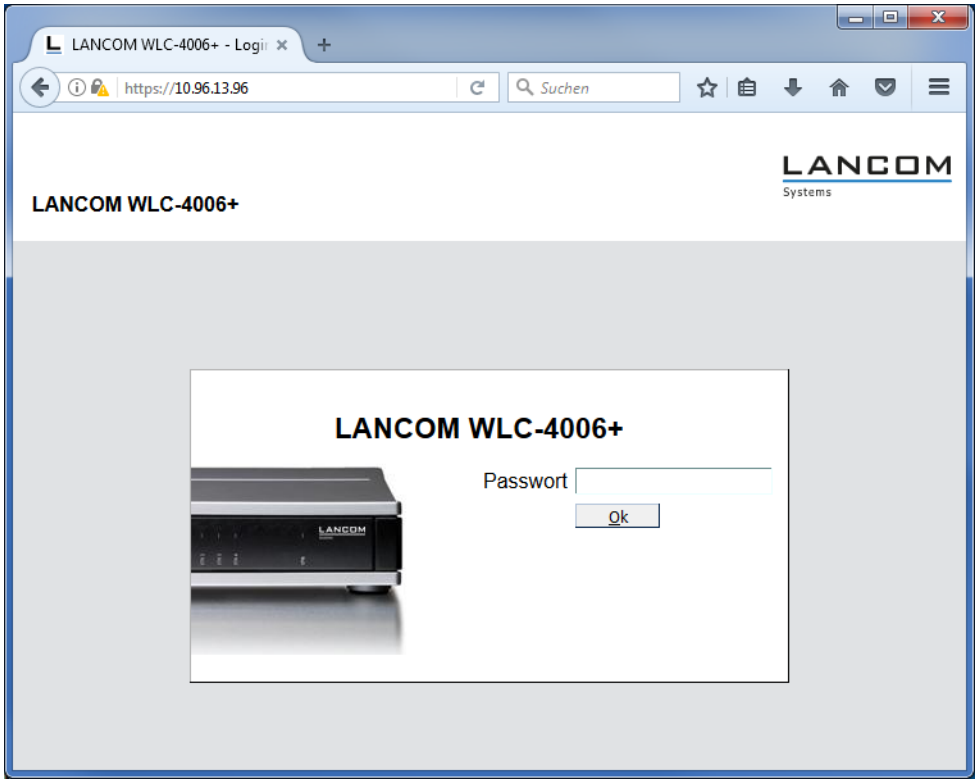
Beachten Sie, dass bei einem Umschalten alle bestehenden Verbindungen beendet sowie alle Statistiken und Gebühreninformationen gelöscht werden.

WEBconfig / Konsolen-Sitzung

Über diesen Menüpunkt starten Sie eine neue Konfigurationssitzung über einen alternativen Konfigurationsweg. Folgende Konfigurationswege stehen Ihnen zur Auswahl:

Web-Browser starten

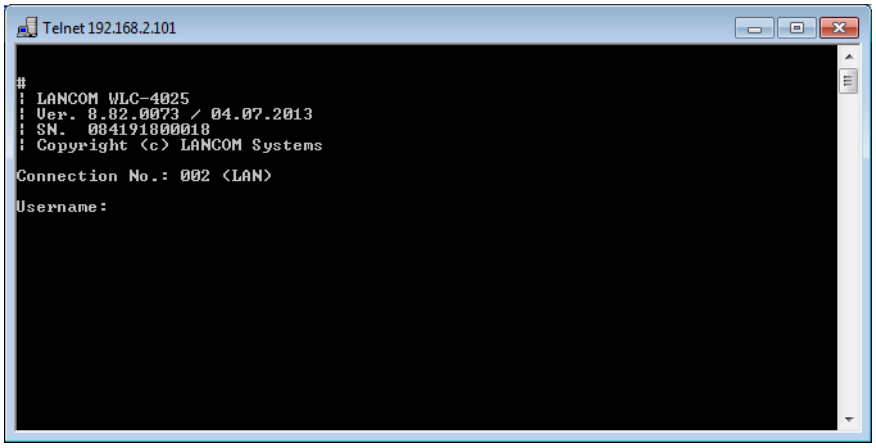
Öffnet die WEBconfig-Oberfläche für das markierte Gerät.



Unter **Extras** > **Optionen** > **Extras** > **Browser zur Darstellung von WEBconfig** können Sie auswählen, ob LANconfig zur Anzeige den Standardbrowser des Systems oder den internen Browser verwenden soll.

Telnet-Sitzung öffnen

Öffnet eine Verbindung zum Gerät mit dem in den Einstellungen konfigurierten Telnet-Client.



SSH-Sitzung öffnen

Öffnet eine Verbindung zum Gerät mit dem in den Einstellungen konfigurierten SSH-Client.

Gerät überwachen

Über diesen Menüpunkt aktivieren Sie die grundsätzliche Überwachung des Gerätes in LANmonitor.

Das Gerät wird dann in der Liste der zu überwachenden Geräte in LANmonitor ergänzt und liegt auch nach dem Öffnen und Schließen von LANmonitor wieder vor.

Gerät temporär überwachen

Über diesen Menüpunkt aktivieren Sie die temporäre Überwachung des Gerätes in LANmonitor.

Das Gerät wird in einem separaten Fenster von LANmonitor geöffnet. Die Einstellung wird nicht gespeichert, sodass LANmonitor das Gerät beim nächsten Start nicht automatisch wieder anzeigt. Lesen Sie hierzu auch *LANmonitor – Geräte im LAN überwachen* auf Seite 250.

WLAN Gerät überwachen

Über diesen Menüpunkt aktivieren Sie die Überwachung eines WLAN-Gerätes mit WLANmonitor. Lesen Sie hierzu auch *WLANmonitor – WLAN-Geräte überwachen* auf Seite 276

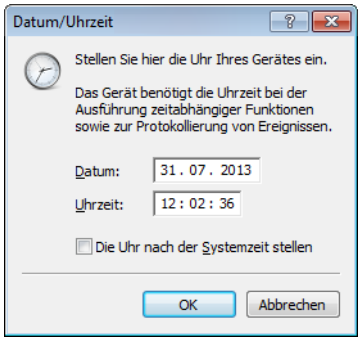
Trace-Ausgabe erstellen

Mit dieser Option starten Sie die Trace-Ausgabe in LANtracer.

Lesen Sie hierzu auch *LANtracer – Tracen mit LANconfig und LANmonitor* auf Seite 292.

Datum/ Uhrzeit setzen

Über diesen Menüpunkt setzen Sie das Datum und die Uhrzeit für das Gerät. Diese Aktion ist für einige Funktionen (z. B. Accounting) und Schritte im Setup Assistenten (z. B. Einrichtung eines Public Spots) zwingend erforderlich.



Wenn Sie die Option **Die Uhr nach der Systemzeit stellen** aktivieren, wird die Uhrzeit des Betriebssystems Ihres Computers übernommen.

Software-Option aktivieren

Wenn Sie zusätzliche Software-Optionen erworben haben, können Sie diese unter **Gerät** > **Software-Option aktivieren** aktivieren, indem Sie den Aktivierungsschlüssel eingeben.

Wenn Sie eine Option testen möchten, können Sie für jedes Gerät einmalig eine zeitlich befristete, 30-tägige Demo-Lizenz aktivieren. Klicken Sie dazu auf den Link unterhalb der Eingabefelder für den Lizenzschlüssel. Sie werden automatisch mit der Webseite des LANCOM Registrierungsservers verbunden, auf der Sie die gewünschte Demolizenz auswählen und für das Gerät registrieren können.

Bereits aktivierte Optionen sehen Sie im Dialog **Gerät** > **Eigenschaften** > **Features & Optionen** ein. Lesen Sie hierzu auch *Features & Optionen* auf Seite 224.

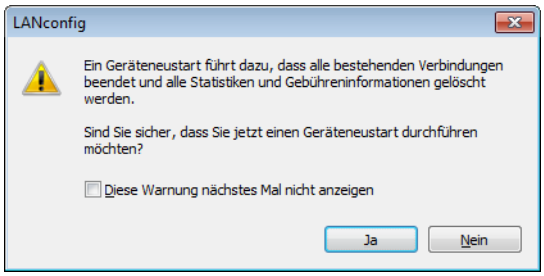
CC-Konformität prüfen

Über diesen Menüpunkt veranlassen Sie die Prüfung, ob die Konfiguration des ausgewählen Gerätes CC-konform ist.

Diese Aktion ist nur für CC-Geräte sinnvoll. Bei Nicht-CC-Geräten ruft diese Aktion stets eine Fehlermeldung hervor.

Neustart

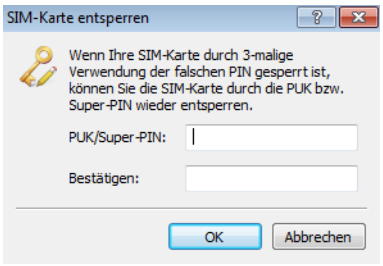
Über diesen Menüpunkt veranlassen Sie einen Neustart des Gerätes.



Bei einem Neustart werden die Zugangsdaten für den Admin-Account abgefragt, insofern diese nicht für das Gerät hinterlegt sind.

SIM-Karte entsperren

Wenn Sie dreimal den falschen PIN eingegeben haben, wird Ihre SIM-Karte gesperrt. Unter diesem Menüpunkt können Sie die SIM-Karte durch die Eingabe des PUK bzw. Super-PIN wieder entsperren.



Gilt nur für Geräte mit WWAN.

Eigenschaften

Über diesen Menüpunkt öffnen Sie den Eigenschaften-Dialog des markierten Geräts, in dem sich auf verschiedenen Seiten gerätespezifische Einstellungen vornehmen oder einsehen lassen.

Allgemein

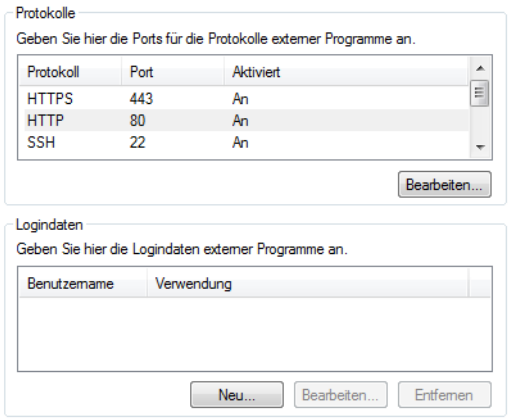
Auf dieser Seite nehmen Sie die gerätespezifischen Verbindungseinstellungen vor. Die dazugehörigen Einstellungsmöglichkeiten sind mit denen unter **Datei** > **Gerät hinzufügen** > **Allgemein** identisch (siehe *Allgemein* auf Seite 209).

Protokolle & Logins

Auf dieser Seite konfigurieren und verwalten Sie die Protokolle, Ports und Zugangsdaten, welche die übrigen Bestandteile der LANtools beim Aufruf aus LANconfig heraus verwenden. Zu den konfigurierbaren Programmen gehören:

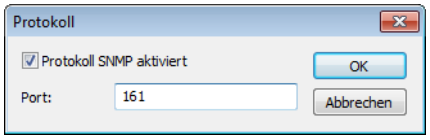
- LANmonitor
- LANtracer
- LANtools-interner sowie externer Webbrowser

Sofern im aufgerufenen Programm z. B. bestimmte Protokolle bereits deaktiviert bzw. anders konfiguriert sind, gelten ausschließlich die Übereinstimmungen.



Protokolle

Wählen Sie ein Protokoll aus und klicken Sie **Bearbeiten**, um das ausgewählte Protokoll zur Verwendung in externen Programmen zu erlauben oder zu verbieten und ggf. den Standard-Port zu verändern.



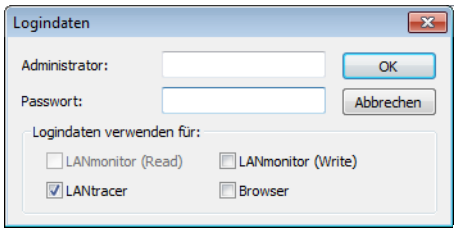
Logindaten

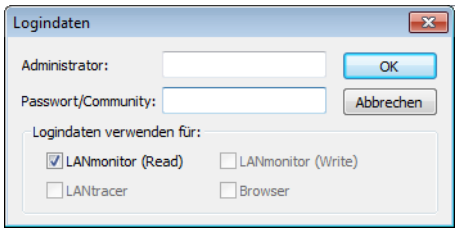
Hinterlegen Sie in diesem Bereich die Zugangsdaten für die externen Programme. Klicken Sie **Neu**, um ein oder mehrere Programm(e) auszuwählen und die dafür geltenden Zugangsdaten einzugeben. Je nach Auswahl fragt das Dialogfenster unterschiedliche Zugangsdaten ab. In jedem Fall haben Sie die Möglichkeit, sich mit dem Benutzernamen und Passwort Ihres Administrator-Zugangs zu authentisieren, wenn Sie das betreffende Programm aus LANconfig heraus aufrufen.

Im Falle von LANmonitor besteht für den reinen Lesezugriff (Read) die Möglichkeit, eine individuelle SNMP-Community anzugeben. Standardmäßig prüft LANconfig beim Öffnen einer Gerätekonfiguration, ob und in welchem Umfang Sie Zugangsdaten für externe Programme hinterlegt haben. Haben Sie für den Lesezugriff keine Zugangsdaten oder lediglich Zugangsdaten in Form einer SNMP-Community konfiguriert, übernimmt LANconfig beim Programmaufruf von LANmonitor die SNMP-Community ersatzweise aus der geladenen Gerätekonfiguration. Sofern Sie in LANconfig eine Konfiguration bearbeiten und in dieser eine SNMP-Community setzen, speichert LANconfig die SNMP-Community automatisch für das betreffende Gerät. Durch dieses Komfortverhalten wird der Authentisierungsumfang für LANmonitor reduziert, sodass keine gesonderte Konfiguration des Lesezugriffs erforderlich ist.

LANconfig wertet für das oben beschriebene Komfortverhalten ausschließlich den Setup-Parameter *2.9.15 Read-Only-Community* aus. Zusätzliche im Gerät konfigurierte, schreibgeschützte SNMP Communities bleiben unbeachtet.

Weitere Informationen zum SNMP-Zugriff über einzelne oder mehrere SNMP-Communities finden Sie im Abschnitt *Konfigurieren des SNMP-Lesezugriffs* auf Seite 112.





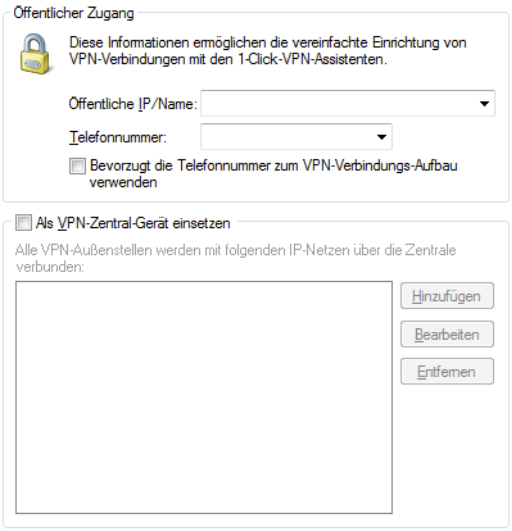
Sicherung

Auf dieser Seite aktivieren und konfigurieren Sie die gerätespezifischen Sicherungseinstellungen. Die dazugehörigen Einstellungsmöglichkeiten sind mit den globalen identisch (siehe *Sicherung* auf Seite 238).

VPN

Auf dieser Seite nehmen Sie Einstellungen für den VPN-Zugang vor.

Diese Dialogseite ist nur für Geräte verfügbar, die auch VPN anbieten.



Öffentlicher Zugang

Geben Sie für die vereinfachte Einrichtung von VPN-Verbindungen eine öffentliche IP bzw. einen Namen und eine Telefonnummer an. Sie können bestimmen, ob die Telefonnummer für den VPN-Verbindungs-Aufbau bevorzugt verwendet werden soll.

Eine Telefonnummer ist nur dann sinnvoll, wenn beide Geräte auch jeweils an das öffentliche Telefonnetz angeschlossen sind und sich über eine entsprechend zugeordnete Rufnummer ("MSN") erreichen können. Geräte können auch gleichzeitig für den Verbindungs-Aufbau per IP oder Telefonnummer konfiguriert werden. Die Verbindung per Telefonnummer ist als zuverlässiger einzustufen, jedoch nicht immer möglich und unter Umständen. aufgrund des Anschlusses mit zusätzlichen Kosten verbunden.

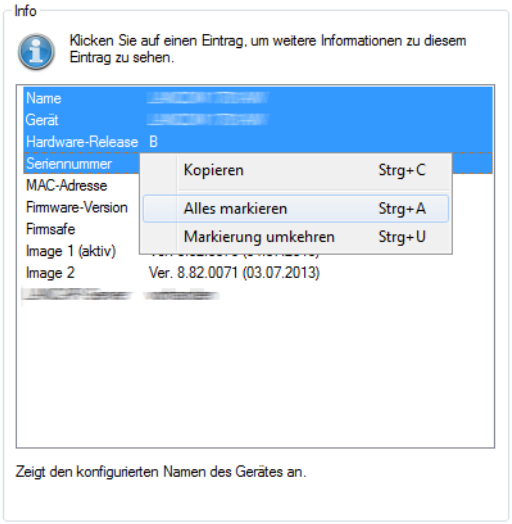
Als VPN-Zentral-Gerät einsetzen

Bestimmen Sie hier, welche IP-Netze mit allen VPN-Außenstellen über die Zentrale verbunden werden sollen.

Informationen

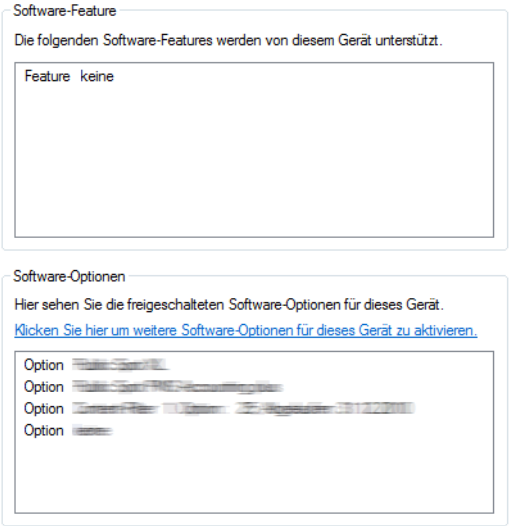
Auf dieser Seite erhalten Sie hardware- und systembezogene Informationen über das Gerät.

Durch einen Klick mit der rechten Maustaste auf die linke Spalte mit den Namen der Einträge, erhalten Sie ein Kontextmenü. Über dieses können Sie die Werte auch in die Zwischenablage übernehmen.



Features & Optionen

Auf dieser Seite erhalten Sie nähere Informationen zu den vom Gerät unterstützten Features und freigeschalteten Optionen.



3.1.3.4 Gruppe

Unter diesem Menüpunkt verwalten Sie die Gruppen-Konfigurationen.

Weitere Informationen finden Sie im Abschnitt *Flexible Gruppen-Konfiguration mit LANconfig* auf Seite 186.

Neue Gruppen-Konfiguration

Unter **Gruppe** > **Neue Gruppen-Konfiguration** erstellen Sie im aktuellen Ordner eine neue Gruppen-Konfiguration.

Weitere Informationen finden Sie im Abschnitt *Flexible Gruppen-Konfiguration mit LANconfig*.

Neuer Ordner mit Gruppen-Konfiguration

Unter **Gruppe** > **Neuer Ordner mit Gruppen-Konfiguration** erstellen Sie im aktuellen Ordner einen neuen Unterordner mit einer neuen Gruppen-Konfiguration.

Weitere Informationen finden Sie im Abschnitt *Flexible Gruppen-Konfiguration mit LANconfig*.

Gruppen-Konfiguration hinzufügen

Unter **Gruppe** > **Gruppen-Konfiguration hinzufügen** speichern Sie eine bereits bestehende Gruppen-Konfiguration in den aktiven Ordner. Wählen Sie hierzu die entsprechende Datei aus.

Weitere Informationen finden Sie im Abschnitt *Flexible Gruppen-Konfiguration mit LANconfig*.

Gruppen-Konfiguration bearbeiten

Unter **Gruppe** > **Gruppen-Konfiguration bearbeiten** haben Sie die Möglichkeit die ausgewählte Gruppen-Konfiguration zu bearbeiten.

Stellen Sie in der Konfiguration die Parameter so ein, dass sie für die gesamte Gruppe gültig sind. Beim Schließen des Konfigurationsdialogs fordert LANconfig Sie auf, die entsprechende Gruppen-Konfigurationsdatei an einem beliebigen Ort zu speichern.

Weitere Informationen finden Sie im Abschnitt *Flexible Gruppen-Konfiguration mit LANconfig*.

Alle Geräte aktualisieren

Unter **Gruppe** > **Alle Geräte aktualisieren** haben Sie die Möglichkeit, die ausgewählte und aktivierte Gruppe zu nutzen, um alle Geräte im aktuellen Ordner zu aktualisieren.

Weitere Informationen finden Sie im Abschnitt *Flexible Gruppen-Konfiguration mit LANconfig*.

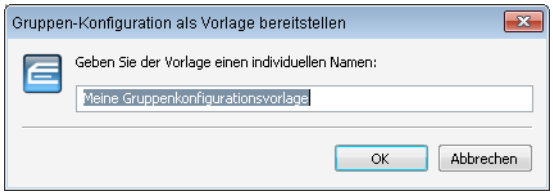
Empfohlene Geräte aktualisieren

Unter **Gruppe** > **Empfohlene Geräte aktualisieren** haben Sie die Möglichkeit die ausgewählte und aktivierte Gruppe zu nutzen, um die empfohlenen Geräte im aktuellen Ordner zu aktualisieren.

Weitere Informationen finden Sie im Abschnitt *Flexible Gruppen-Konfiguration mit LANconfig*.

Als Vorlage bereitstellen

Unter **Gruppe** > **Als Vorlage bereitstellen** haben Sie die Möglichkeit die ausgewählte Gruppen-Konfiguration als Vorlage für zukünftige Gruppen-Konfigurationen zu definieren.



Weitere Informationen finden Sie im Abschnitt *Flexible Gruppen-Konfiguration mit LANconfig*.

Aktiv

Unter **Gruppe** > **Aktiv** aktivieren oder deaktivieren Sie die ausgewählte Gruppen-Konfiguration.

Weitere Informationen finden Sie im Abschnitt *Flexible Gruppen-Konfiguration mit LANconfig*.

Löschen

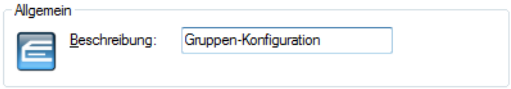
Mit **Gruppe** > **Löschen** löschen Sie die ausgewählte Gruppen-Konfiguration.

Weitere Informationen finden Sie im Abschnitt *Flexible Gruppen-Konfiguration mit LANconfig*.

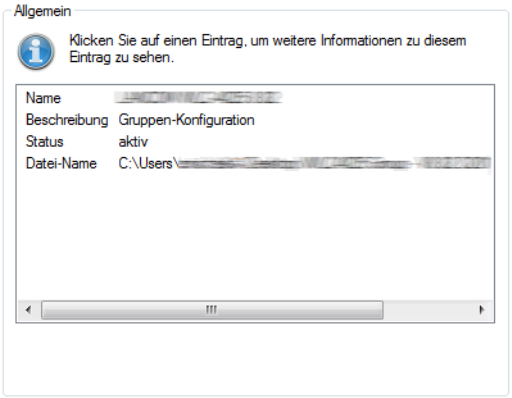
Eigenschaften

Unter **Gruppe** > **Eigenschaften** zeigen Sie Informationen einer bereits bestehenden Gruppen-Konfiguration an. Wählen Sie hierzu die entsprechende Datei aus.

Die Seite **Allgemein** zeigt die Beschreibung der Gruppen-Konfiguration an.



Auf der Seite **Info** finden Sie den Namen, den Status und den Datei-Namen der Gruppen-Konfiguration.



Weitere Informationen finden Sie im Abschnitt *Flexible Gruppen-Konfiguration mit LANconfig*.

3.1.3.5 Ansicht

Unter diesem Menüpunkt passen Sie das Verhalten der LANconfig-Bedienoberfläche an.

Symbolleiste

Zur benutzerdefinierten Anpassung der Symbolleiste können im LANconfig die folgenden Optionen gewählt werden:

Schaltflächen

Blendet die Schaltflächen ein oder aus.

QuickFinder

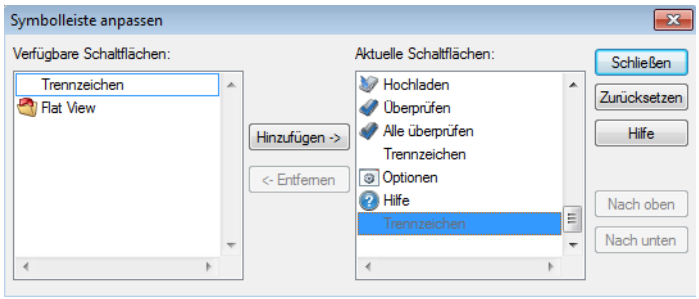
Blendet den QuickFinder ein oder aus.

Große Symbole

Zeigt eine größere Darstellung der Symbole.

Anpassen

Öffnet einen Dialog, in dem die angezeigten Symbole ausgewählt werden können. Zwischen inhaltlichen Gruppen von Symbolen kann dabei ein Trennzeichen eingefügt werden, außerdem kann die Reihenfolge der Symbole verändert werden.



Zurücksetzen

Setzt die Einstellungen für die Symbolleiste auf die Standardwerte zurück.

Eine Übersicht der Symbole finden Sie im Kapitel *Die Symbole der Symbolleiste* auf Seite 243.

Statusleiste

Über diesen Menüpunkt blenden Sie die Statusleiste ein- oder aus.

Verzeichnisbaum

Die Ordnerstruktur am linken Rand des LANconfig-Fensters kann über diesen Menüpunkt (oder alternativ mit der Funktionstaste F6) ein- und ausgeblendet werden. Lesen Sie dazu auch das Kapitel *Verzeichnisbäume zur Organisation nutzen* auf Seite 178.

Protokollanzeige

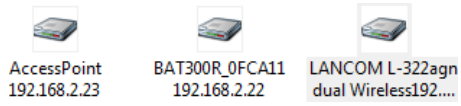
Über diesen Menüpunkt blenden Sie die Protokollanzeige im unteren Teil des LANconfig-Fensters – welche Datum, Zeit, Name, Adresse und Meldung beinhaltet – ein- oder aus.

Flat View Modus

Hier können Sie den Flat View Modus für LANconfig aktivieren.

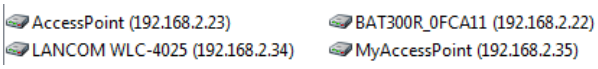
Große Symbole

Im Anzeigemodus 'Große Symbole' werden die Gerätesymbole in einer vergrößerten Darstellung angezeigt.



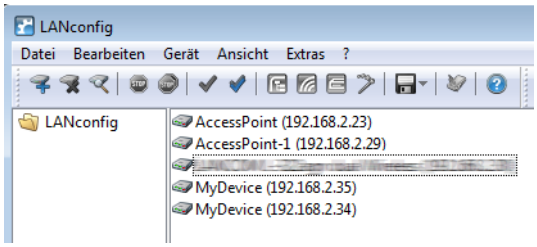
Kleine Symbole

Im Anzeigemodus 'Kleine Symbole' werden die Gerätesymbole klein dargestellt.



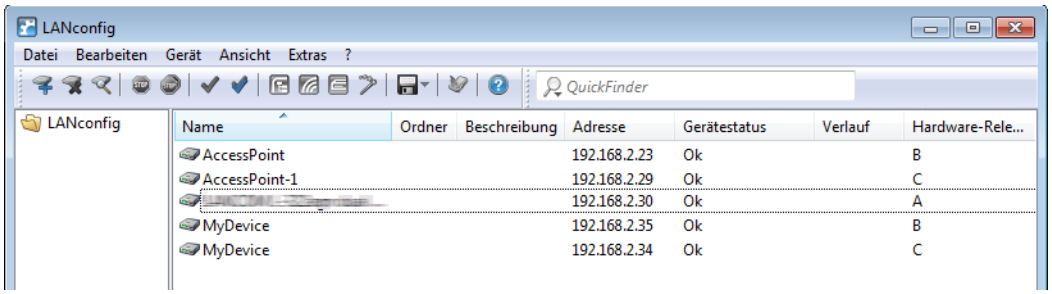
Liste

Im Anzeigemodus 'Liste' werden die Geräte als Liste angezeigt.



Details

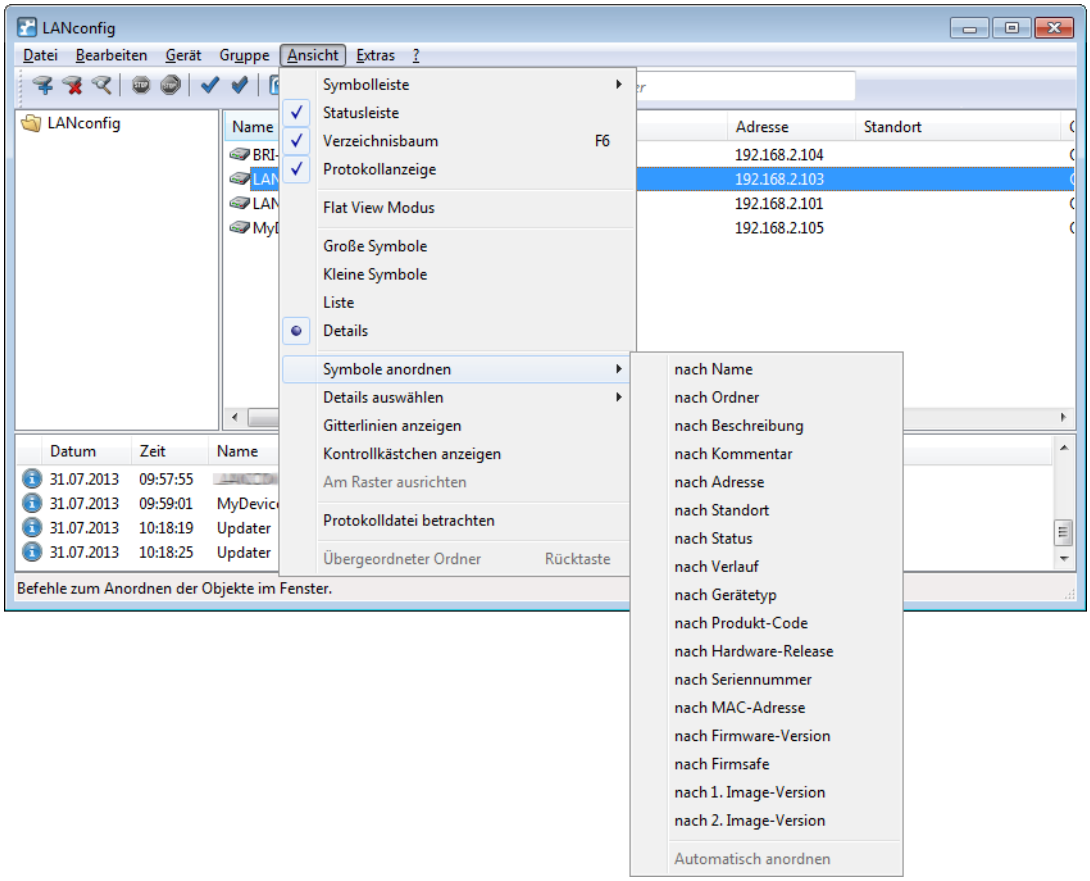
Im Anzeigemodus 'Details' werden Details zu den Geräten angezeigt.



Symbole anordnen

Für eine bessere und schnellere Übersicht und Orientierung auch in großen Projekten können in LANconfig die Spalten mit gerätebezogenen Informationen einzeln ein- bzw. ausgeblendet werden. Klicken Sie dazu mit der rechten Maustaste auf die Spaltenüberschriften und wählen Sie unter **Ansicht** > **Details auswählen** die anzuzeigenden Spalten. Über den

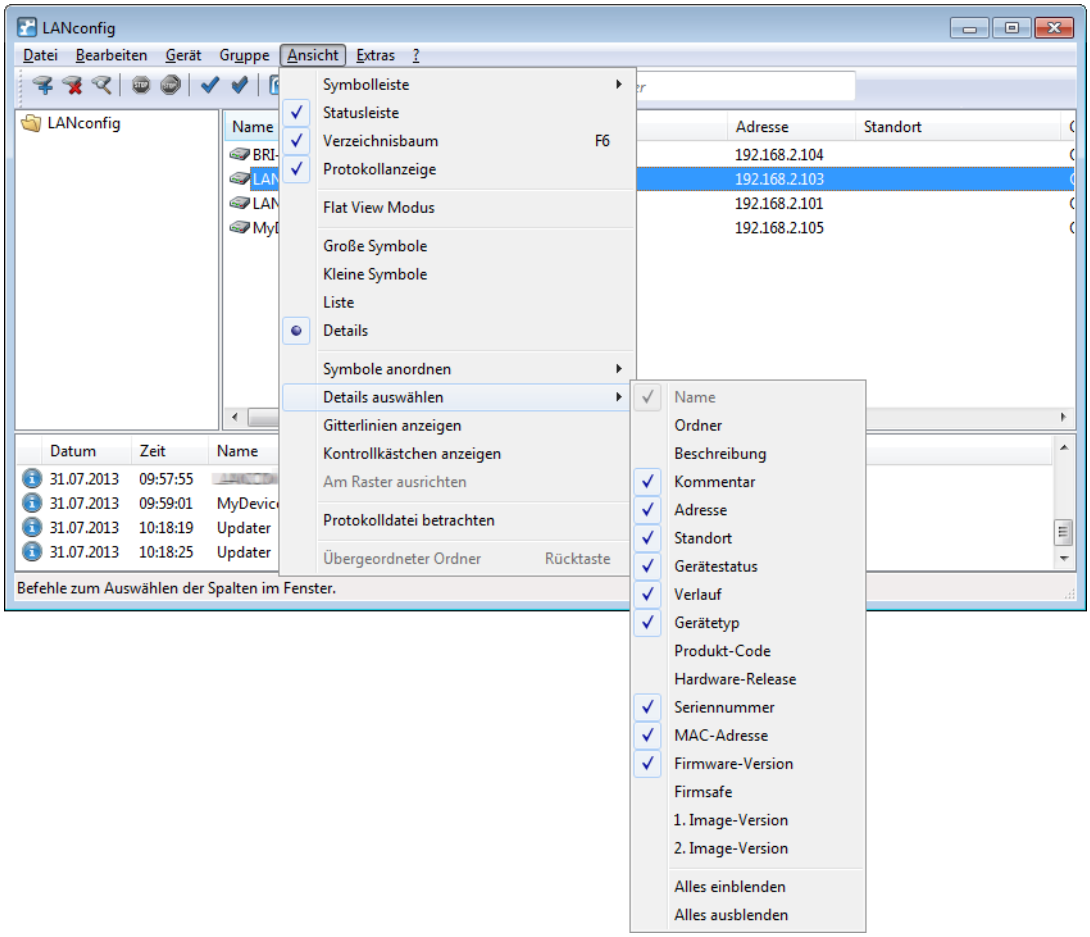
Menüpunkt **Symbole anordnen** können Sie ausserdem die gewünschte Sortierung auswählen. Wenn Sie **Automatisch anordnen** auswählen, werden die Symbole im Konfigurationsbereich automatisch angeordnet.



Details auswählen

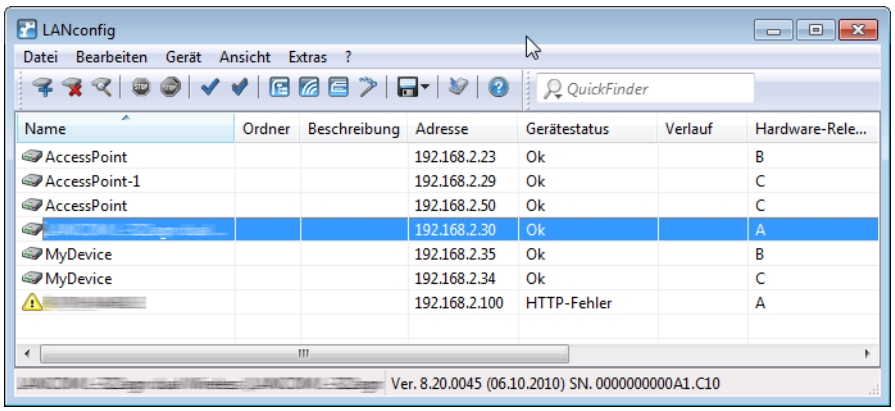
Für eine bessere und schnellere Übersicht und Orientierung auch in großen Projekten können in LANconfig die Spalten mit gerätebezogenen Informationen einzeln ein- bzw. ausgeblendet werden. Alternativ können Sie auch mit der rechten

Maustaste auf die Spaltenüberschriften klicken und im sich öffnenden Kontextmenü das Menü unter **Ansicht** > **Details auswählen** aufrufen.



Gitterlinien anzeigen

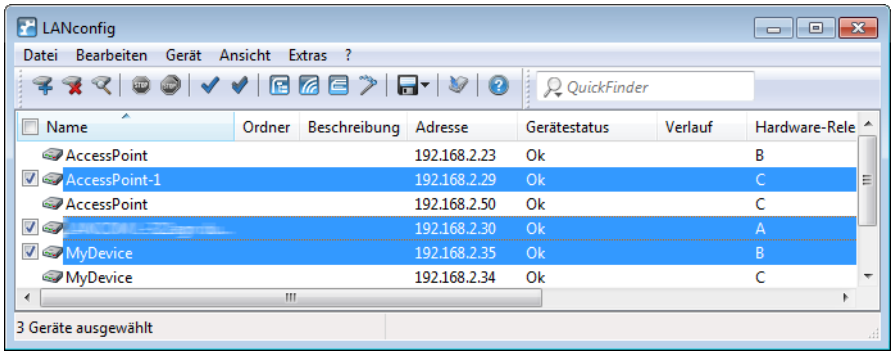
Über diesen Menüpunkt blenden Sie Gitterlinien in der Geräteansicht ein- oder aus.



Kontrollkästchen anzeigen

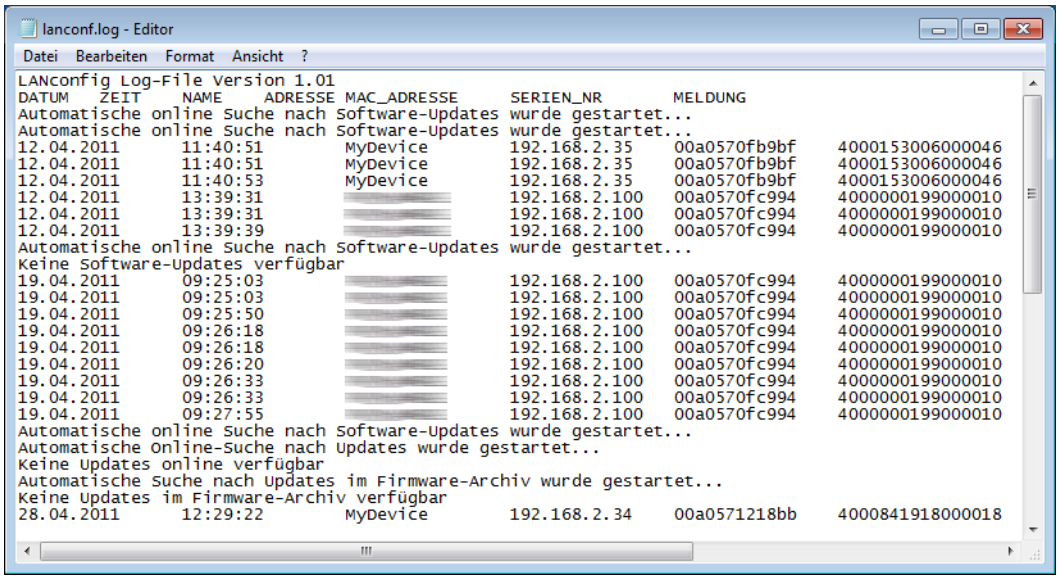
Über diesen Menüpunkt aktivieren Sie die Anzeige von Kontrollkästchen. Links neben dem Geräteintrag erscheint daraufhin ein Kontrollkästchen, mit dem Sie ein Gerät auswählen können. Sie haben so die Möglichkeit, ohne den Einsatz von

Tastaturkürzeln mehrere Geräte gezielt auszuwählen und dann Aktionen auf diese Geräte anzuwenden (z. B. neue Firmware hochladen).



Protokolldatei betrachten

Über diesen Menüpunkt können Sie die Protokolldatei von LANconfig ansehen und bearbeiten.



Übergeordneter Ordner

Über diesen Menüpunkt gelangen Sie in der jeweiligen Ordneransicht zu dem übergeordneten Ordner.

3.1.3.6 Extras

Unter diesem Menüpunkt finden Sie weitere Einstellungsmöglichkeiten LANconfig. Sie erreichen diese Dialogbox auch, indem Sie F7 drücken.

Optionen

Unter dem Menüpunkt **Optionen** können Sie zusätzliche Funktionen von LANconfig aufrufen, z. B. für die Kommunikation mit angeschlossenen Geräten, den Aufruf externer Anwendungen oder die automatische Suche nach Firmware-Updates.

Weitere Informationen finden Sie in den folgenden Abschnitten:

Allgemein

In diesem Dialog legen Sie die allgemeinen Programmeinstellungen fest.

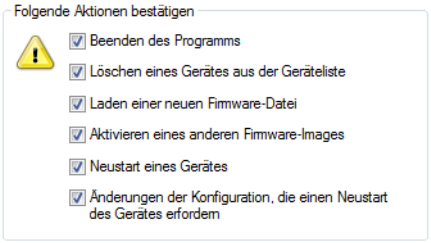
Konfiguration von Geräten



Sie können auswählen, ob Sie für die Konfiguration den Setup-Assistenten als Standard verwenden oder ob Sie standardmäßig den Konfigurations-Dialog zur manuellen Bearbeitung starten wollen, wenn Sie einen Doppeklick auf ein Gerät ausführen. In der Standard-Einstellung wird durch Doppelklick auf ein Gerät die Übersicht der Setup-Assistenten geöffnet.

- **Durchsuchen der Konfiguration in …**
  - **Beschreibung**: Durchsucht die Konfiguration in der Beschreibung
  - **Wert**: Durchsucht die Konfiguration in den Werten
  - **Einheit**: Durchsucht die Konfiguration in den Einheiten

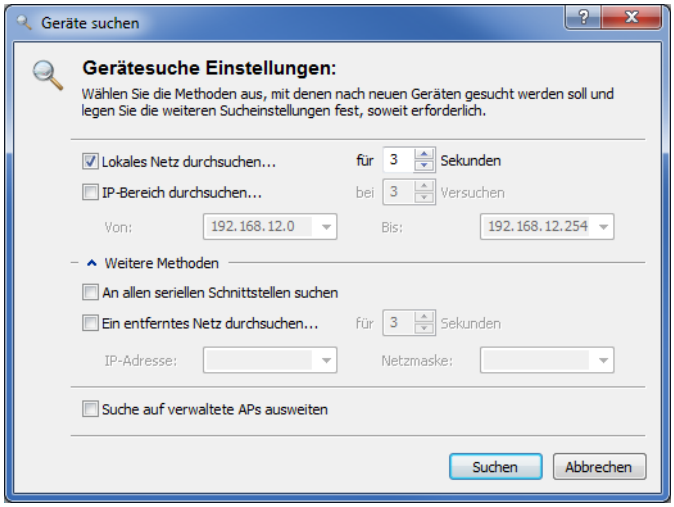
Folgenden Aktionen bestätigen



- **Beenden des Programms**: Schaltet die Sicherheitsabfrage beim Verlassen des Programms ein oder aus.
- **Löschen eines Gerätes aus der Geräteliste:** Schalten Sie diese Option aus, wenn Sie beim Löschen von Geräten nicht mehr von dem Programm gewarnt werden wollen.
- **Laden einer neuen Firmware-Datei:** Wenn Sie diese Option aktivieren, werden Sie gewarnt, wenn Sie eine neue Firmware in das Gerät laden wollen.
- **Aktivieren eines anderen Firmware-Images:** Wenn Sie diese Option aktivieren, werden Sie jedesmal gewarnt, wenn Sie ein anderes Firmware-Image aktivieren wollen.
- **Neustart eines Gerätes:** Wenn Sie diese Option aktivieren, werden Sie gewarnt, bevor das Gerät neu gestartet wird.
- **Änderungen der Konfiguration vornehmen, die einen Neustart erfordern:** Wenn Sie diese Option aktivieren, werden Sie jedesmal gewarnt, wenn Sie die Konfiguration des Gerätes ändern wollen.

Start

In diesem Dialog legen Sie das Verhalten und die Aktionen von LANconfig beim Programmstart fest.



- **Bei jedem Start nach neuen Geräten suchen**: Wenn Sie diese Option aktivieren, sucht das Programm bei jedem Start in vordefinierten Netzen nach neuen Geräten.

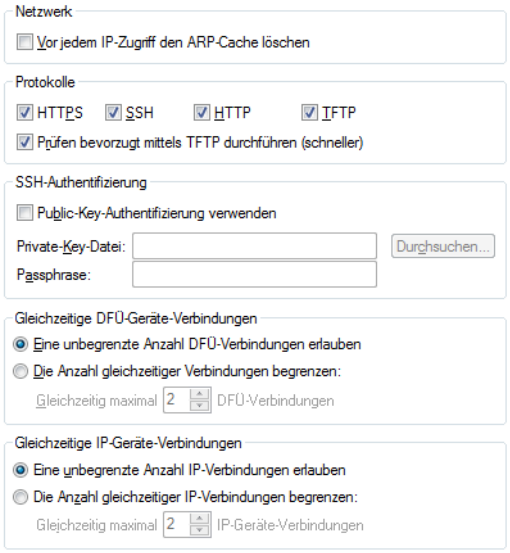
Bei großen Installationen mit vielen Geräten kann dieser Vorgang vergleichsweise viel Zeit in Anspruch nehmen bzw. aufgrund der Verbindungsaufnahme zu den Geräten unerwünscht sein.

- **Im lokalen Netz:** Wenn Sie diese Option aktivieren, sucht das Programm beim Start in Ihrem lokalen Netz nach Geräten und wartet auf die hier eingestellte Zeit auf Antworten.
- **In den folgenden entfernten Netzwerken:** Wenn Sie diese Option aktivieren, sucht das Programm beim Start in entfernten Netzen nach Geräten. Welche Netze durchsucht werden sollen, können Sie in der nachstehenden Liste definieren.
- **Suche auf verwaltete APs ausweiten:** Vollständig gemanagte Access Points (APs) werden normalerweise von der Suche übergangen, da ihre WLAN-Konfiguration gänzlich von einem WLAN-Controller verwaltet wird. Wählen Sie diese Option aus, um vollständig gemanagte APs dennoch zu finden.

Diese Option ist für Sie belanglos, wenn Sie weder über einen WLAN-Controller noch über gemanagte APs in Ihrem Netzwerk verfügen.

Kommunikation

In diesem Dialog nehmen Sie die globalen Einstellungen zu den Verbindungen zwischen LANconfig und den Geräten vor:



Netzwerk

Wenn Sie häufiger wechselnde Geräte mit gleicher IP-Adresse in Ihrem Netz haben, dann sollten Sie die Option **Vor jedem IP-Zugriff den ARP-Cache löschen** einschalten, damit Ihr Rechner diese Geräte erreichen kann.

Protokolle

Zur Übertragung der Daten bei der Konfiguration mit LANconfig stehen wahlweise die Protokolle HTTPS, SSH, HTTP oder TFTP Verfügung.

Die allgemein angebotenen Protokolle werden global definiert. Zusätzlich ist es möglich, Protokolle für bestimmte Geräte zu unterbinden. Es ist jedoch nicht möglich ein global deaktiviertes Protokoll für einzelne Geräte wieder zu aktivieren, da die globalen Kommunikationseinstellungen den gerätespezifischen Einstellungen übergeordnet sind.

Die Konfiguration der Kommunikationsprotokolle unterscheidet zwischen dem Protokoll für das reine Prüfen des Gerätes und den Protokollen für andere Operationen wie z. B. einen Firmware-Upload etc.:

- **HTTPS**, **SSH**, **HTTP**, **TFTP**

  Mit dieser Auswahl aktivieren Sie die einzelnen Protokolle für die Operationen Firmware-Upload sowie Konfigurations- und Script-Upload und -Download. Bei diesen Operationen versucht LANconfig, diese Protokolle in der Reihenfolge HTTPS, SSH, HTTP und TFTP zu verwenden. Schlägt die Übertragung mit einem der gewählten Protokolle fehl, versucht LANconfig automatisch das nächste Protokoll.

- **Prüfen bevorzugt mittels TFTP durchführen**

  Eine Prüfung der Geräte überträgt mit den Systeminformationen nur geringe Datenmengen. Gerade im LAN ist also die Geräteprüfung durchaus mit dem TFTP-Protokoll sinnvoll. Wenn diese Option aktiviert ist, verwendet LANconfig zum Prüfen der Geräte zunächst das TFTP-Protokoll, unabhängig von den zuvor eingestellten Kommunikationsprotokollen. Schlägt die Prüfung über TFTP fehl, versucht LANconfig im Anschluss die Protokolle HTTPS, SSH und HTTP.

SSH-Authentifizierung

Sofern Sie als Protokoll SSH ausgewählt haben, können Sie die Authentifizierung alternativ über einen privaten Schlüssel durchführen. In diesem Fall entfällt die Authentifizierung über eine Dialog zur Kenntworteingabe. Wenn Sie **Public-Key-Authentifizierung verwenden** aktivieren, tragen Sie in die Eingabefelder den Pfad

zu Ihrer privaten Schlüsseldatei und ggf. die Passphrase ein, mit der Sie die Datei zusätzlich verschlüsselt haben. Den dazugehörigen öffentlichen Schlüssel laden Sie über LANconfig oder WEBconfig in die einzelnen Geräte.

Eine detaillierte Anleitung zur Konfiguration der Public-Key-Authentifizierung für Ihre Geräte finden Sie im Kapitel *SSH-Authentifizierung mit Hilfe eines Public-Keys* auf Seite 115.

Gleichzeitige DFÜ-Geräte-Verbindungen

Die Anzahl der gleichzeitig über RAS aufgebauten Verbindungen kann künstlich begrenzt werden. Dies ist insbesondere dann sinnvoll, wenn die Menge der physikalisch verfügbaren RAS-Kanäle begrenzt ist oder eine zu hohe System- oder Netzlast vermieden werden soll.

Überschreitet die für entsprechende Aktionen notwendige Anzahl RAS-Verbindungen dieses Limit, so werden die überzähligen Aktionen in eine Warteschlange eingereiht und erst wieder gestartet, wenn ein RAS-Kanal verfügbar wird.

Wenn Sie die Anzahl nicht begrenzen oder eine höhere Begrenzung gewählt haben, als zu irgendeinem Zeitpunkt tatsächlich physikalisch verfügbar ist, so werden überzähligen Aktionen ebenfalls in die oben erwähnte Warteschlange eingereiht.

Mit dieser Option kann beim Start einer großen Zahl gleichzeitiger Aktionen die erzeugte System- oder Netzlast gemindert werden.

Wenn Sie die Anzahl nicht begrenzen und genügend Resourcen zur Verfügung stehen, kann die erzeugte System- oder Netzlast beliebig hoch werden!

Gleichzeitige IP-Geräte-Verbindungen

Die Anzahl der gleichzeitig über IP aufgebauten Verbindungen kann künstlich begrenzt werden. Dies ist insbesondere dann sinnvoll, wenn die Verbindungen über physikalisch begrenzt vorhanden Kanäle laufen oder eine zu hohe System- oder Netzlast vermieden werden soll.

Überschreitet die für entsprechende Aktionen notwendige Anzahl an IP-Verbindungen dieses Limit, so werden die überzähligen Aktionen in eine Warteschlange eingereiht und erst wieder gestartet, wenn ein logischer IP-Kanal verfügbar wird.

Wenn Sie die Anzahl nicht begrenzen oder eine höhere Begrenzung gewählt haben, als zu irgendeinem Zeitpunkt tatsächlich physikalisch verfügbar ist, so werden überzähligen Aktionen mit einem Fehler abgebrochen

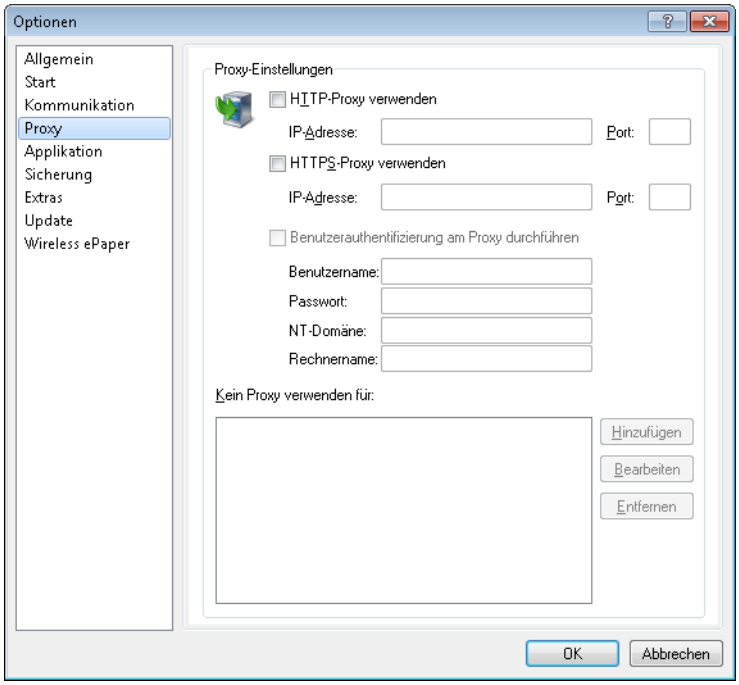
Mit dieser Option kann beim Start einer großen Zahl gleichzeitiger Aktionen die erzeugte System- oder Netzlast gemindert werden.

Wenn Sie die Anzahl nicht begrenzen und genügend Resourcen zur Verfügung stehen, kann die erzeugte System- oder Netzlast beliebig hoch werden!

Proxy

Wenn Sie für den Zugriff auf Ihre Geräte einen Proxy-Server verwenden möchten, können Sie diesen hier konfigurieren. Aktivieren Sie dazu das gewünschte Protokoll und tragen Sie die Adresse und den Port ein, über den der Proxy-Server erreichbar ist.

Protokollunabhängig ist die Angabe einer Liste von Netzen oder einzelnen Hosts möglich, für die die Proxy-Einstellungen nicht gelten.



HTTP-Proxy verwenden

Aktiviert die Verwendung eines HTTP-Proxys.

- **Adresse**: Tragen Sie hier die IP-Adresse ein, über die der HTTP-Proxy-Server erreichbar ist.
- **Port**: Tragen Sie hier ein, welchen Port der HTTP-Proxy-Server verwendet.

HTTPS-Proxy verwenden

Aktiviert die Verwendung eines HTTPS-Proxys.

- **Adresse**: Tragen Sie hier die IP-Adresse ein, über die der HTTPS-Proxy-Server erreichbar ist.
- **Port**: Tragen Sie hier ein, welchen Port der HTTPS-Proxy verwendet.

Benutzerauthentifizierung am Proxy durchführen

Falls der Proxy-Server eine Authentifizierung erfordert, geben Sie den Benutzernamen und das Passwort ein. Wenn die Authentifizierung über NTLM (NT LAN Manager) erfolgen soll, geben Sie zusätzlich die NT-Domäne und den Rechnernamen ein.

Diese Option ist nur bei aktivierter Proxy-Einstellung verfügbar.

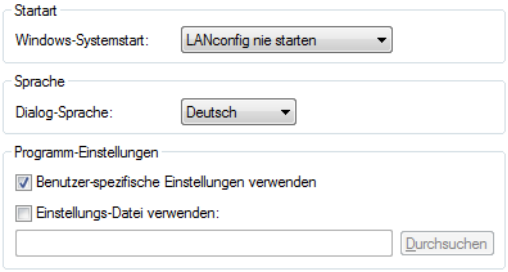
Kein Proxy verwenden für

Tragen Sie hier die IP-Adressen und die zugehörige Netzmaske ein, für die die Proxy-Einstellungen nicht gelten.

Diese Option ist nur bei aktivierter Proxy-Einstellung verfügbar.

Applikation

In diesem Dialog nehmen Sie die Einstellungen zur Benutzeroberfläche vor.



Startart

LANconfig kann beim Start des Betriebssystems automatisch geladen werden. Folgende **Windows-Systemstart**-Arten stehen Ihnen zur Verfügung:

- **LANconfig nie starten**

  Die Anwendung startet nicht automatisch mit dem Betriebssystem, sondern muss manuell gestartet werden.

- **LANconfig immer starten**

  Die Anwendung startet immer automatisch nach dem erfolgreichen Start des Betriebssystems.

- **LANconfig wie zuvor starten**

  Die Anwendung startet in dem Zustand, in dem Sie sich beim Herunterfahren des Betriebssystems befand. War die Anwendung aktiv, wird sie wieder gestartet; war sie nicht aktiv, wird sie auch nicht automatisch gestartet.

Beim Wechsel auf eine Einstellung, die ein automatisches Starten der Anwendung ermöglicht, wird ein Eintrag in der Registry des Betriebssystems vorgenommen. Firewall-Applikationen auf dem Rechner oder die Betriebssysteme selbst können diesen Eintrag ggf. als Angriff deuten und eine Warnung ausgeben bzw. den Eintrag verhindern. Um das gewünschte Startverhalten zu ermöglichen, ignorieren Sie diese Warnungen bzw. lassen Sie die durchzuführenden Aktionen zu.

Sprache

Hierüber ändern Sie die Sprache des Benutzer-Interfaces (GUI). Die Auswahl der Sprache erfolgt normalerweise automatisch anhand der Sprache des Betriebssystems.

Damit die Änderung der Spracheinstellung wirksam wird, ist ein Neustart der Anwendung erforderlich.

Programm-Einstellung

Hier kann die Verwendung benutzerspezifischer LANconfig-Einstellungen gewählt werden. Lesen Sie dazu auch das Kapitel *Benutzerspezifische Einstellungen für LANconfig* auf Seite 177.

- **Benutzerspezifische Einstellungen verwenden**

  Aktiviert die Verwendung der lanconf.ini aus dem aktuellen Benutzer-Verzeichnis unter `…\Anwendungsdaten\LANCOM\LANconfig\`.

  Wenn diese Option aktiviert ist, werden Änderungen an den Programmeinstellungen in dieser ini-Datei gespeichert.

- **Einstellungs-Datei verwenden**

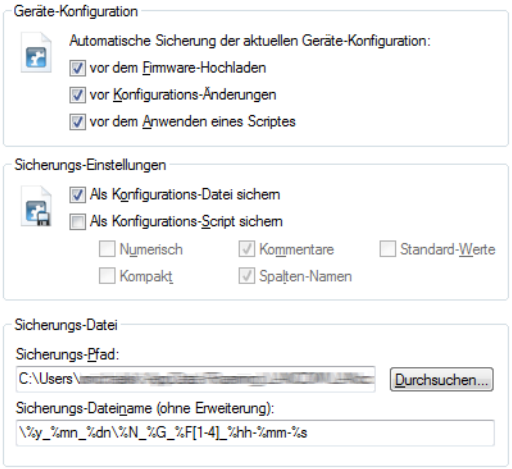
Aktiviert die Verwendung der lanconf.ini aus dem angegebenen Verzeichnis. Wenn diese Option aktiviert ist, werden Änderungen an den Programmeinstellungen in der im Eingabefeld angegebenen ini-Datei gespeichert.

Bei der gewählten Datei muss es sich um eine gültige LANconfig-Einstellungsdatei handeln.

Wenn keine der beiden Optionen aktiviert ist, wird die ini-Datei aus dem Programmverzeichnis verwendet.

Sicherung

Auf dieser Seite stellen Sie die globalen Sicherungseinstellungen ein.



Geräte-Konfiguration

Hier können Sie wählen, vor welcher Aktion eine automatische Sicherung der aktuellen Gerätekonfiguration durchgeführt werden soll. Um die automatische Sicherung zu aktivieren, müssen Sie mindestens eine der folgenden Einstellungen wählen:

- **Vor dem Firmware-Hochladen:** Vor dem Hochladen einer Firmware wird eine automatische Sicherung der Gerätekonfiguration durchgeführt.
- **Vor Konfigurations-Änderungen:** Vor dem Hochladen oder bei Änderungen der Gerätekonfiguration wird automatisch eine Sicherung der Gerätekonfiguration durchgeführt.
- **Vor dem Anwenden eines Scriptes:** Vor dem Anwenden eines Scriptes am Gerät wird automatisch eine Sicherung der Gerätekonfiguration durchgeführt.

Sicherungs-Einstellungen

Hier können Sie die Sicherungsart wählen. Mindestens eine der folgenden Sicherungsarten muss für die automatische Sicherung der aktuellen Gerätekonfiguration gewählt werden:

- **Als Konfigurations-Datei sichern:** Die automatische Sicherung sichert die aktuelle Gerätekonfiguration als Konfigurations-Datei.
- **Als Konfigurations-Script sichern:** Die automatische Sicherung sichert die aktuelle Gerätekonfiguration als Konfigurations-Script.
  - **Numerisch**: Mit dieser Option werden die Sektionsnamen in numerischer Form dargestellt.
  - **Kommentare**: Mit dieser Option werden zusätzliche Kommentare eingefügt.

- **Standard-Werte**: Normalerweise werden nur die von den Standardwerten abweichenden Einstellungen gesichert. Mit dieser Option werden zusätzlich die Standardwerte gesichert.
- **Kompakt**: Mit dieser Option wird die Ausgabe kompakt formatiert. Leerzeilen und Tabulatoren werden beispielsweise unterdrückt.
- **Spalten-Namen**: Normalerweise werden Tabellen befüllt, indem zuerst die Spalten mit dem Tab-Befehl beschrieben werden und danach jede Zeile mit einem Set-Befehl befüllt wird, welcher nur die zu setzenden Werte enthält. Wird diese Option eingeschaltet, werden die Tabellen-Spalten nicht mit dem Tab-Befehl beschrieben, sondern in jedem Tabellen-Set-Befehl werden die Spalten-Bezeichner eingefügt.

Sicherungs-Datei

- **Sicherungs-Pfad:** Geben Sie hier einen Pfad zu einem Ablage-Ordner auf Ihrem Rechner oder im Netzwerk an. Mit **Durchsuchen** können Sie auch einen Browser öffnen, um den Pfad zu bestimmen. In der Voreinstellung werden Sicherungen im Ordner 'Config' unterhalb des Programmverzeichnisses auf dem lokalen Rechner abgelegt.
- **Sicherungs-Dateiname (ohne Erweiterung):** Sie können hier einen frei wählbaren Dateinamen ohne Erweiterung angeben. Die Erweiterung wird je nach Sicherungs-Dateityp ergänzt. Der Dateiname kann die in der folgenden Tabelle aufgeführten Variablen enthalten, welche erst bei der entsprechenden Aktion zu einem konkreten Dateinamen expandiert werden. Ausserdem können dem Sicherungs-Dateinamen auch weitere Ordner mit diesen Variablen im Namen vorangestellt und infolgedessen erzeugt werden.

Tabelle 16: Geräteinformation

Name	%N
MAC-Adresse	%M
Gerätetyp	%G
Hardware-Release	%W
Firmware-Version	%F
IP-Adresse	%I
Firmware-Datum	%D
Adresse	%H
Seriennummer	%S

Mit den folgenden regulären Ausdrücken können Sie auch Teile der Geräteinformation anzeigen lassen. Zahlen in eckigen Klammern, welche den Variablen folgen, bilden eine Teilinformation, wie etwa %N[5]. Es wird das n-te Zeichen aus dieser Variable expandiert. Mit einem Bindestrich wird eine Zeichenkette definiert, etwa %H[2-5].

Tabelle 17: Beispiele der Variablen

[]	Expandiert alle Zeichen
[1]	Expandiert nur das erste Zeichen
[12], [12-12]	Expandiert nur das zwölfte Zeichen
[1-5]	Expandiert vom Anfang bis zum fünften Zeichen
[2-5]	Expandiert vom zweiten bis zum fünften Zeichen
[6-]	Expandiert alles ab dem sechsten Zeichen

Tabelle 18: Datum und Uhrzeit

%y	Jahr
%hh	Stunde
%mn	Monat des Jahres (1-12)
%mm	Minute
%ma	Monat des Jahres (Januar - Dezember)
%s	Sekunde
%dn	Tag des Monats (1-31)
%ms	Millisekunde
%da	Wochentag (Sonntag - Samstag)
%dw	Wochentag (Sonntag ist 0, 0-6)
%%	% (einzelnes Prozent-Zeichen)

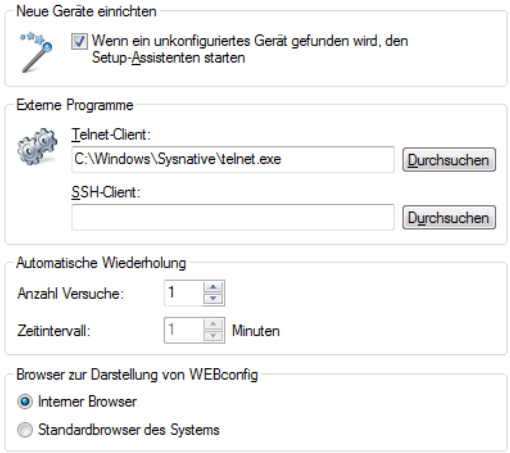
Falls eine Datei mit dem gleichen Namen im Ziel-Verzeichnis existieren sollte, so wird der Name der Sicherungs-Datei automatisch um einen aufsteigenden Zähler erweitert.

Tabelle 19: Beispiele

Sicherungs-Dateiname: MeinBackup_%N_%S_%I	Resultat: MeinBackup_MeinGeraet_12481632_10.10.1.1
Sicherungs-Dateiname: %d_%mn_%y\Ordner_2\%N	Resultat: 25_08_2008\Ordner_2\MeinGeraet

Extras

In diesem Dialog nehmen Sie zusätzliche Einstellungen vor.



Neue Geräte einrichten

Wenn diese Option markiert ist, startet LANconfig bei jedem gefundenen, aber noch nicht konfigurierten Gerät den Setup-Assistenten.

Externe Programme

Bestimmen Sie hier jeweils die Programmdatei des Telnet-Clients und des SSH-Clients, die LANconfig für Verbindungen zu den Geräten benutzen soll.

Automatische Wiederholung

Anzahl Versuche

Geben Sie hier die Anzahl der Versuche für einen Firmware- oder Konfigurations-Upload an. Die Anzahl können Sie im Bereich von 1 bis 9999 einstellen. Einen Verbindungsversuch führt LANconfig immer durch. Schlägt dieser fehl, erfolgt eine Wiederholung der Aktion nach abgelaufener Intervall-Zeit. Es erfolgen so viele Wiederholungen, bis LANconfig entweder die eingestellte Anzahl von Versuchen durchgeführt hat oder die Aktion erfolgreich war. Es ist jedoch auch möglich, dass LANconfig die Wiederholungen vorzeitig abbricht, wenn eine Situation eintritt, die voraussichtlich nicht ohne weitere Einflussnahme zum Erfolg führt. Dies kann z. B. eine Datei sein, die das Gerät nicht öffnen kann.

Zeitintervall

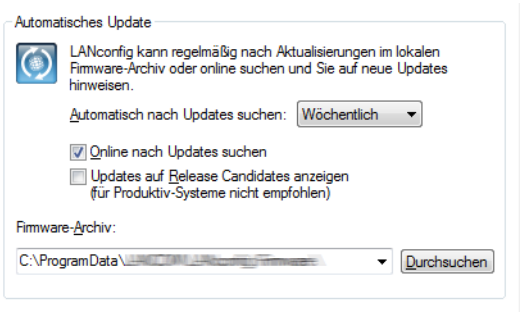
Geben Sie hier die Intervalldauer in Minuten an, die zwischen zwei Firmware- oder Konfigurations-Upload-Versuchen verstreichen soll. Die Intervalldauer können Sie im Bereich von 1 bis 9999 einstellen.

Browser zur Darstellung von WEBconfig

Bestimmen Sie hier, welchen Browser LANconfig standardmäßig für die Anzeige von WEBconfig verwenden soll. Zur Auswahl stehen der Standard-Browser des Betriebssystems und der LANconfig-interne Browser LCCEF (LANCOM Chromium Embedded Framework).

Update

In diesem Dialog nehmen Sie die Einstellungen für das Automatische Update vor.



Um das Update auf neue Firmwareversionen in den Geräten möglichst komfortabel zu gestalten, werden die Firmware-Dateien für die verschiedenen Modelle und LCOS-Versionen idealerweise in einem zentralen Archiv-Verzeichnis abgelegt. Die Suche nach neuen Firmware-Versionen in diesem Verzeichnis kann entweder manuell angestoßen werden oder nach jedem Start von LANconfig automatisch durchgeführt werden.

- **Automatisch nach Updates suchen**

  Wählen Sie das zeitliche Intervall für die automatische Suche nach Updates (**Täglich**, **Wöchentlich** oder **Monatlich**) aus. Alternativ deaktivieren Sie die automatische Suche mit der Einstellung **Nie**.

- **Online nach Updates suchen**

  Wählen Sie diese Option, um LANconfig online nach weiteren Updates im Download-Bereich des LANCOM Web-Servers suchen zu lassen.

- **Updates auf Release Candidates anzeigen**

Wenn Sie diese Option einschalten, wird das Software Update nicht nur die für den Einsatz in Produktivumgebungen freigegebenen Software-Versionen zum Download anbieten, sondern auch die verfügbaren Release Candidates.

Release Candidates enthalten die neuen Features der kommenden Software-Version und sind ausführlich getestet. Bis zur endgültigen Freigabe der Version sind – u. a. aufgrund der Rückmeldungen der Anwender – noch weitere Optimierungen der Software möglich.

› Wählen Sie für das lokale **Firmware-Archiv** einen geeigneten Speicherort. LANconfig sucht bei der automatischen Suche nach Updates an diesem Speicherort nach neuen Versionen der LANtools und der Firmware. LANCOM Software Update speichert die Updates vom Download-Bereich des LANCOM Web-Servers an diesem Speicherort.

LANmonitor starten

Startet LANmonitor. Mehr Informationen dazu erhalten Sie im Kapitel *LANmonitor – Geräte im LAN überwachen* auf Seite 250.

WLANmonitor starten

Startet den WLANmonitor. Mehr Informationen dazu erhalten Sie im Kapitel *WLANmonitor – WLAN-Geräte überwachen* auf Seite 276.

Trace-Ausgabe analysieren

Startet LANtracer. Mehr Informationen dazu erhalten Sie im Kapitel *LANtracer – Tracen mit LANconfig und LANmonitor* auf Seite 292.

CC-Inbetriebnahme-Assistent starten

Über diesen Menüpunkt starten Sie den CC-Inbetriebnahme-Assistenten, welcher Sie bei der Konfiguration Ihrer LANCOM CC-Produkte für den zertifizierten CC-Betrieb gemäß CC EAL 4+ unterstützt.

Weitere Informationen zum Umgang mit dem Assistenten sowie die Konfiguration von CC-Geräten erhalten Sie gesondert im "LANCOM CC Installation Guide". Diesen finden Sie zusammen mit dem "LANCOM CC Start-up Kit" auf *www.lancom-systems.de*.

Für Nicht-CC-Geräte ist dieser Assistent ohne Relevanz.

Nach Updates suchen

Startet manuell die automatische Suche nach Online-Updates. Lesen Sie dazu auch das Kapitel *Software Update für LANtools* auf Seite 203.

3.1.3.7 Hilfe

Unter diesem Menüpunkt finden Sie weitere Hilfe zum Programm und lassen sich Informationen zur Software anzeigen.

Hilfethemen

Über diesen Menüpunkt gelangen Sie zu den Hilfethemen. Alternativ können Sie auch F1 drücken.

Support

Dieser Menüpunkt ruft die Webseite des Supports auf.

Info

Unter diesem Menüpunkt werden Ihnen die Version und das Builddatum der Software angezeigt.

3.1.4 Die Symbole der Symbolleiste

Tabelle 20: Bedeutung der Symbole

	Hinzufügen		Hochladen
	Löschen		Überprüfen
	Suchen		Alle überprüfen
	Aktion abbrechen		Hilfe
	Aktionen abbrechen		Aufwärts
	Prüfen		Flat View
	Alle prüfen		Wiederherstellen
	Überwachen		Ordner
	WLAN überwachen		Protokollanzeige
	Konfigurieren		Optionen
	Setup-Assistent		Ansicht
	Sicherung		Eigenschaften

Informationen zu den Einstellungsmöglichkeiten der Symbolleiste finden Sie im Kapitel *Symbolleiste* auf Seite 226.

3.1.5 Das Kontextmenü in LANconfig

Das Kontextmenü in der Geräteansicht enthält die Funktionen, die Sie auch unter Menü **Gerät** finden.

3.1.6 LANconfig Tastaturbefehle

Einfg	Gerät hinzufügen
Entf	Gerät löschen
F3	Geräte suchen
F5	Alle Geräte prüfen
Alt+F4	Beenden
Strg+N	Neue Konfigurations-Datei
Strg+E	Konfigurations-Datei bearbeiten
Strg+Shift+W	Konfigurations-Datei assistieren
Strg+Shift+P	Konfigurations-Datei drucken
Strg+A	Alles markieren
Strg+O	Gerät > Konfigurieren
Strg+W	Gerät > Setup Assistent
Strg+F5	Gerät > Prüfen

Strg+P	Drucken
Strg+S	Als Datei sichern
Strg+R	Aus Datei wiederherstellen
Strg+Shift+U	Auf Firmware-Update prüfen
Strg+U	Neue Firmware hochladen
Strg+B	Web-Browser gesichert starten
Strg+T	Telnet-Sitzung öffnen
Strg+Shift+S	SSH-Sitzung öffnen
Strg+M	Gerät temporär überwachen
Alt+Enter	Eigenschaften
F6	Verzeichnisbaum
Rücktaste	übergeordneter Ordner
Leertaste, ENTER	Ausgewählten Tabelleneintrag bearbeiten
+	Tabelleneintrag nach oben springen (nur dynamische Tabellen)
-	Tabelleneintrag nach untern springen (nur dynamische Tabellen)
Einfg	Neuen Tabelleneintrag hinzufügen (nur dynamische Tabellen)
Entf	Markierten Tabelleneintrag entfernen (nur dynamische Tabellen)
F7	Extras > Optionen
F1	Hilfethemen

3.1.7 LANconfig Kommandozeilen-Parameter

Sie haben die Möglichkeit, LANconfig über die Windows-Kommandozeile mit bestimmten Optionen und Befehlen zu starten. Die Eingabe erfolgt gemäß der nachfolgend beschriebenen Syntax. Schrägstrich und Bindestrich werden als Parameter-Präfix unterstützt. Bei allen Parametern ist die Groß- und Kleinschreibung nicht relevant.

Die Syntax sieht folgendermaßen aus:

```
lanconf.exe [(-|/)<Option>[:<Value>]] [(-|/)<Command>[:<Value>]]
```

- In eckigen Klammern stehen die optionalen Parameter.
- In runden Klammern stehen die nötigen Parameter.
- Alternativen werden durch einen vertikalen Gedankenstrich getrennt.
- In spitzen Klammern stehen die Objekte, die unter *Optionen* auf Seite 244 und *Befehle* auf Seite 245 beschrieben werden.

Um also z. B. die LANconfig mit englischer Benutzeroberfläche zu starten, geben Sie `lanconf.exe /language:English` ein. Um zusätzlich noch den Konfigurationsassistenten für eine bestimmte Konfigurationsdatei zu öffnen, ergänzen Sie die Angabe um den Wizard-Befehl, also `lanconf.exe /language:English /wizard:MyConfig.lcf`.

3.1.7.1 Optionen

In diesem Abschnitt werden die Optionen für die Kommandozeile beschrieben.

Restart

Prüft die Startoptionen von LANconfig in der INI-Datei. Nutzen Sie diesen Parameter, um beim Start von Windows das Startverhalten von LANconfig zu beeinflussen. Ein automatischer Start von LANconfig erfolgt ausschließlich dann, wenn Sie in LANconfig unter **Extras** > **Optionen** > **Applikation** die Startart **LANconfig immer starten** oder **LANconfig wie zuvor starten** (Programm war beim Herunterfahren von Windows aktiv) ausgewählt haben.

WizStyle

Legt die Erscheinung der Konfigurationsassistenten fest. Mögliche Werte für `<Value>` sind:

- `0`: Alter Wizard Style. Kopfzeile (Titel und Untertitel) auf den Dialog-Seiten sind durch eine horizontale Linie von den übrigen Dialog-Inhalten abgegrenzt.
- `1`: Aktueller Wizard Style (seit Windows 98). Kopfzeile (Titel und Untertitel) auf den Dialog-Seiten sind durch eine horizontale Linie sowie einen andersfarbigen Hintergrund von den übrigen Dialog-Inhalten abgegrenzt.

Language

Verändert temporär die Sprache für die Benutzeroberfläche. Standardmäßig verwendet LANconfig die System-Sprache, sofern diese implementiert ist. Andernfalls ist die Sprache Englisch. Mögliche Werte für `<Value>` sind:

- `English`
- `German`
- `Spanish`

3.1.7.2 Befehle

In diesem Abschnitt werden die Befehle für die Konsole beschrieben. Befehle im Zusammenhang mit Konfigurationsdateien erfordern die Angabe eines Dateinamens als `<Value>`, z. B. `lanconf.exe /printto:MyConfig.lcf`.

Close

Beendet das Programm nach der Ausführung der noch ausstehenden Befehle. LANconfig startet nach der Ausführung der Befehle normal, es sei denn, eine andere Einstellung wird vorgenommen.

Owner

Übernimmt das Fenster mit Handle [hwndParent]. Optional wird es bei den Befehlen `Print`, `PrintTo` und `AutoUpdate` genutzt.

Edit

Bearbeitet eine Konfigurationsdatei, wenn diese nicht schon bearbeitet wird. Wenn eine Konfigurationsdatei bearbeitet wird, wird diese in den Fokus gebracht.

Wizard

Starten Sie den Assistenten für die Konfigurationsdatei. Wenn dieser bereits geöffnet wurde, gelangt er in den Vordergrund.

Print

Druckt die Konfigurationsdatei, wenn nicht bereits ein Druckaufttrag ausfgeführt wird.

PrintTo

Druckt die Konfigurationsdatei mit einem bestimmten Drucker.

ShellNew

Erstellt eine neue Konfigurationsdatei.

AutoUpdate

So starten Sie ein Firmware Auto-Update:

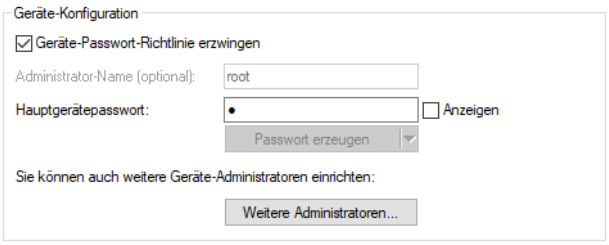
1. Suchen Sie die Geräte.
2. Suchen Sie die Firmware-Dateien.
3. Wählen Sie die neue Firmware.
4. Bestimmen Sie die Geräte, für die ein Firmware-Update durchgeführt werden soll.

3.1.8 Anwendungskonzepte für LANconfig

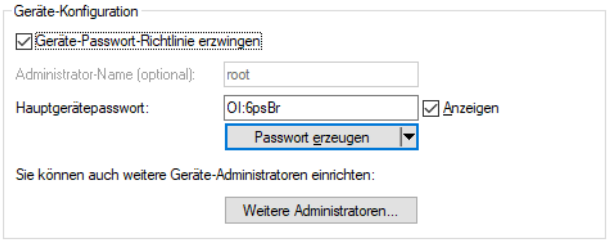
In diesem Abschnitt finden Sie verschiedene Anwendungskonzepte für LANconfig.

3.1.8.1 Passwort erzeugen in LANconfig

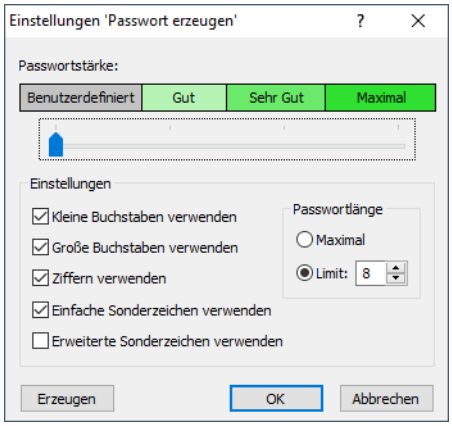
LANconfig bietet an allen Stellen der Konfiguration, welche die Eingabe eines Passworts oder einer Passphrase erfordern, die Möglichkeit zur automatischen Erzeugung eines Passwortvorschlags.



Aktivieren Sie die Option **Anzeigen** neben dem Feld zur Eingabe des Passworts. Klicken Sie dann auf die Schaltfläche **Passwort erzeugen**, um einen Passwortvorschlag zu erzeugen.



Klicken Sie optional auf den Pfeil neben der Schaltfläche **Passwort erzeugen**, um den Dialog für die Einstellungen der Passwort-Richtlinien zu öffnen.



Stellen Sie mit dem Schieberegler die gewünschte Passwortstärke ein. In der Einstellung **Benutzerdefiniert** haben Sie die Möglichkeit, die maximale Passwortlänge und die erforderlichen Zeichentypen zu definieren. In den Einstellungen **Gut**, **Sehr Gut** und **Maximal** sind die Einstellungen mit sinnvollen, nicht veränderbaren Werten vorbelegt.

Klicken Sie nach einer Änderung der Einstellungen erneut die Schaltfläche **Passwort erzeugen**, um einen neuen Passwortvorschlag entsprechend den aktuellen Passwort-Richtlinien zu erzeugen.

LANconfig speichert die gewählten Einstellungen in diesem Dialog für den aktuellen Benutzer.

3.1.8.2 Unterschiedliche Schreibweisen für MAC-Adressen

Um MAC-Adressen per Kopieren und Einfügen aus anderen Anwendungen einfach in LANconfig zu übernehmen, erlaubt LANconfig bei der Eingabe von MAC-Adressen die folgenden Formate:

- 000000000000
- 00:00:00:00:00:00
- 00-00-00-00-00-00
- 000000-000000

Es konvertiert die Eingabe anschließend automatisch in die Form `00:00:00:00:00:00`.

3.1.9 Koppeln von Geräten mit der LANCOM Management Cloud

3.1.9.1 Grundlagen der LANCOM Management Cloud

Die LANCOM Management Cloud (LMC) verwaltet beliebig große Netzwerke „software-defined“. Die LMC übernimmt die Konfiguration sämtlicher Netzwerkkomponenten und minimiert so den Kontrollaufwand und aufwändige Konfigurationen.

Weitere Informationen zur LANCOM Management Cloud finden Sie unter *www.lancom-systems.de/cloud*.

Wenn Sie die LANCOM Management Cloud für die Konfiguration und zur Überwachung Ihres Gerätes verwenden möchten, ist es erforderlich, das Gerät mit der LMC zu koppeln.

3.1.9.2 Koppeln von Geräten mit der LANCOM Management Cloud

In diesem Kapitel werden unterschiedliche Vorgehensweisen für das Koppeln von LANCOM Geräten mit der LMC beschrieben. Hierzu wird zwischen Cloud-ready-Geräten und Bestandsgeräten unterschieden.

Cloud-ready-Geräte sind LANCOM Geräte mit einer bereits vom Hersteller ausgelieferten LCOS-Version 10.0 oder höher (LANCOM Switches: Switch OS 3.30 oder höher) und besitzen eine PIN zur Kopplung mit der LMC. Die PIN finden Sie auf dem Beileger des jeweiligen Produktes.

Bestandsgeräte sind LANCOM Geräte, die von einer älteren LCOS-Version auf eine Version 10.0 (LANCOM Switches: Switch OS 3.30) oder höher aktualisiert wurden und mit dieser für die Verwaltung durch die LMC vorbereitet sind.

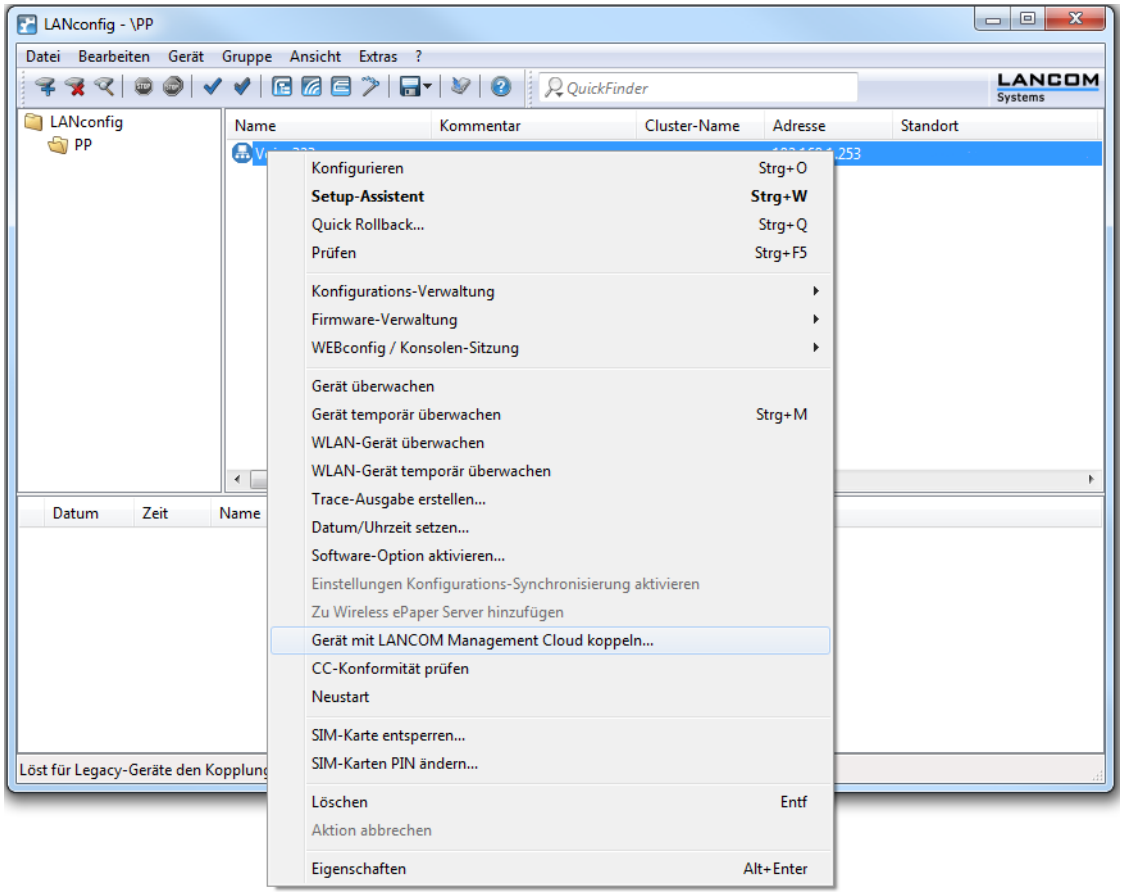
Besitzen Sie ein Cloud-Ready-Gerät, ist kein Pairing erforderlich. Fügen Sie in diesem Fall Ihr Gerät unter Angabe von Seriennummer und PIN Ihrem Konto in der LANCOM Management Cloud hinzu. Alternativ können Sie auch für Cloud-Ready-Geräte ein Pairing durchführen.

Im folgenden werden einige Pairing-Möglichkeiten beschrieben.

Koppeln von Geräten via LANconfig

1. Generieren Sie im ersten Schritt einen Aktivierungscode in der LANCOM Management Cloud.
2. Klicken Sie mit rechten Maustaste auf Ihr LANCOM Gerät.

3. Wählen Sie im Kontextmenü den Eintrag **Gerät mit LANCOM Management Cloud koppeln...** aus.



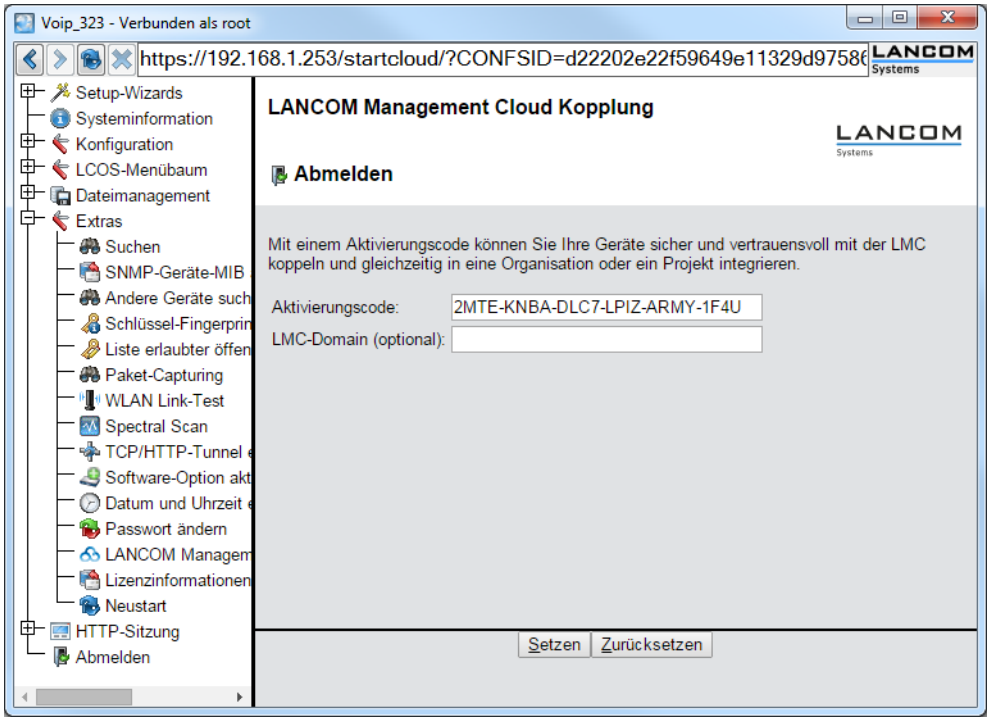
4. Folgen Sie den Anweisungen zur Eingabe des Aktivierungscodes.
Hier stehen drei Optionen zur Auswahl:

   - Public Cloud (Default): Sie verwenden die öffentliche LANCOM Management Cloud.
   - Private Cloud: Sie verwenden Ihre eigene Cloud.
   - Aktuell im Gerät gespeicherte Einstellungen verwenden: Je nach bereits vorhandener Konfiguration des Gerätes wird eine Public bzw. Private Cloud verwendet.



Koppeln von Geräten via WEBconfig

1. Starten Sie WEBconfig.
2. Geben Sie unter **Extras** > **LANCOM Management Cloud Kopplung** Ihren Aktivierungscode ein.



3. Klicken Sie die Schaltfläche **Setzen**.

Koppeln von Geräten via Konsole

Das Pairing über die Konsole erfolgt mit der Eingabe des Befehls `startlmc`.

1. Starten Sie eine Konsolensitzung.
2. Geben Sie den Pairing-Befehl mit dem Aktivierungscode als Parameter ein, z. B. `startlmc 2MTE-KNBA-DLC7-LPIZ-ARMY-1F4U`.

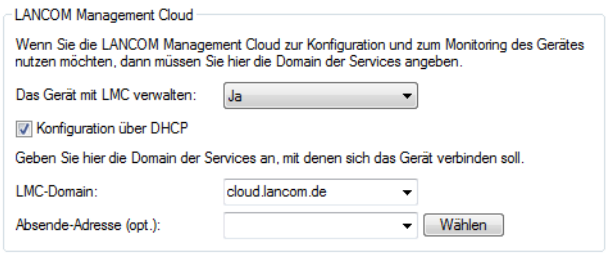
Sie erhalten eine Rückmeldung auf dem Bildschirm, ob der Pairing-Prozess erfolgreich gestartet wurde oder eine entsprechende Fehlermeldung.

3.1.9.3 Manuelles Vorabkonfigurieren Ihres Gerätes für die Verwaltung durch die LANCOM Management Cloud

Hier erfahren Sie die notwendigen Schritte für die Konfiguration und das Monitoring Ihres Gerätes durch die LANCOM Management Cloud. Sie legen fest:

- ob Ihr Gerät durch die LMC zu verwalten ist.
- ob die LMC-Domain von einem DHCP-Server zu beziehen ist.
- mit welcher Domain sich Ihr Gerät verbindet.
- die Absende-Adresse (optional).

1. Navigieren Sie zu **Management** > **LMC**.



2. Wählen Sie unter **Das Gerät mit LMC verwalten:** zwischen drei Optionen:
   - **Nein**: Das Gerät stellt keine Verbindung zur LMC her.
   - **Ja**: Das Gerät wird von der LMC verwaltet. (Default für Geräte ohne WLAN-Schnittstelle)
   - **Nur ohne WLC**: Geräte innerhalb eines von einem WLC verwalteten Netzes bauen keine Verbindung zur LANCOM Management Cloud auf. (Default für Geräte mit WLAN-Schnittstelle)
3. Um die LMC-Domain von einem DHCP-Server zu beziehen, setzen Sie ein Häkchen in **Konfiguration über DHCP**.

   Um die LMC-Domain von einem DHCP-Server bereitzustellen, konfigurieren Sie am DHCP-Server innerhalb der DHCP-Option 43 die Sub-Option 18 mit der LMC-Domain. Weitere Informationen zur Konfiguration der LMC Parameter finden Sie im Abschnitt *Auslieferung der LMC-Domain durch den LCOS-DHCP-Server* auf Seite 46.
4. Wählen Sie unter **LMC-Domain** die Domain der LANCOM Management Cloud, mit der sich das Gerät verbinden soll.
5. Geben Sie optional unter **Absende-Adresse** eine Absendeadresse an, die statt der sonst automatisch für die Zieladresse gewählten Absendeadresse verwendet wird. Falls Sie z. B. eine Loopback-Adresse konfiguriert haben, können Sie diese hier als Absendeadresse angeben.

3.2 LANmonitor – Geräte im LAN überwachen

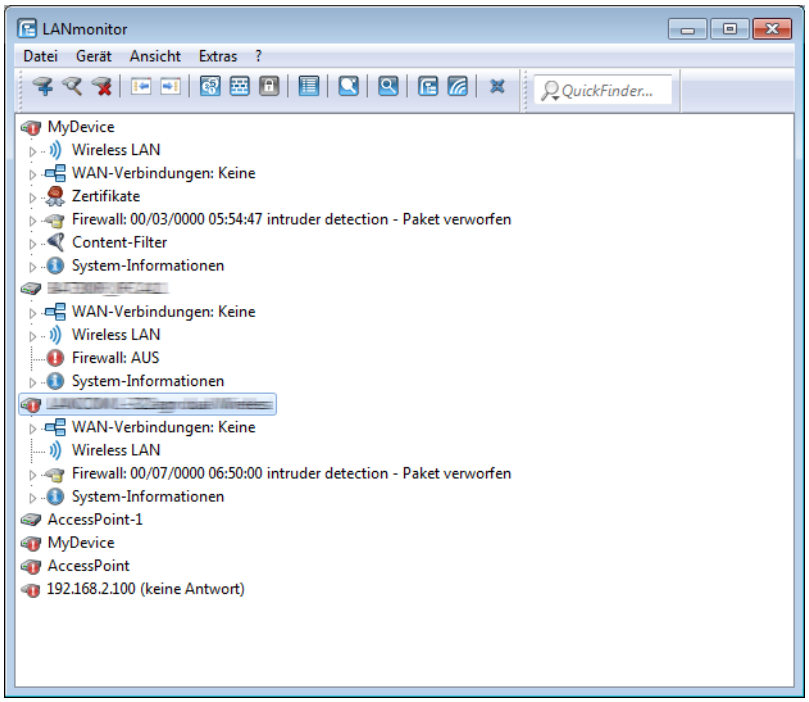
Mit dem Überwachungstool LANmonitor lassen sich unter Windows-Betriebssystemen die wichtigsten Informationen über den Status aller Geräte im Netz bequem und strukturiert überwachen:

- Anzeige von Verbindungen und Schnittstellen
- Interface-Stati
- Übertragungsraten, Protokolle und IP-Adressen
- Fehlerstati
- Anzeige von Geräteinformationen SW-Version, CPU-Last und Speicherverbrauch
- Anzeige von Accounting-Informationen (Online-Zeiten, Gebühren und Transfer-Volumina)
- Anzeige und Protokollierung von Geräteaktivitäten
- Auf- und Abbauten von WAN-, VPN- und WLAN-Verbindungen
- Firewall Ereignisanzeige(n)

Viele der internen Meldungen der Geräte werden dabei in Klartext umgewandelt, zeigen Ihnen den aktuellen Zustand des Gerätes und helfen Ihnen bei der Fehlersuche.

Sie können mit LANmonitor auch den Datenverkehr auf den verschiedenen Schnittstellen der Router beobachten und erhalten so wichtige Hinweise darüber, mit welchen Einstellungen Sie den Datenverkehr optimieren können.

Neben den Statistiken des Geräts, die Sie zum Beispiel auch in einer Telnet- oder Terminalsitzung oder mit WEBconfig auslesen können, stehen Ihnen im LANmonitor noch weitere nützliche Funktionen zur Verfügung, wie beispielsweise die Freischaltung eines Gebührenlimits.



Sie können mit LANmonitor nur solche Geräte überwachen, die Sie über IP erreichen (lokal oder remote). Über die serielle Schnittstelle können Sie ein Gerät mit diesem Programm nicht ansprechen.

Wenn Sie ein Gerät in LANmonitor nicht finden können, kann es sein, dass das Auslesen von Geräteinformationen über den von Ihnen gewählten Zugriffsweg (z. B. remote via VPN) nicht erlaubt ist. LANmonitor verwendet für das Auslesen von Geräteinformationen das SNMP-Protokoll, das vom Administrator für jedes Gerät individuell konfiguriert und eingeschränkt werden kann.

3.2.1 LANmonitor starten

Starten Sie LANmonitor, z. B. mit einem Doppelklick auf das Desktop-Symbol.

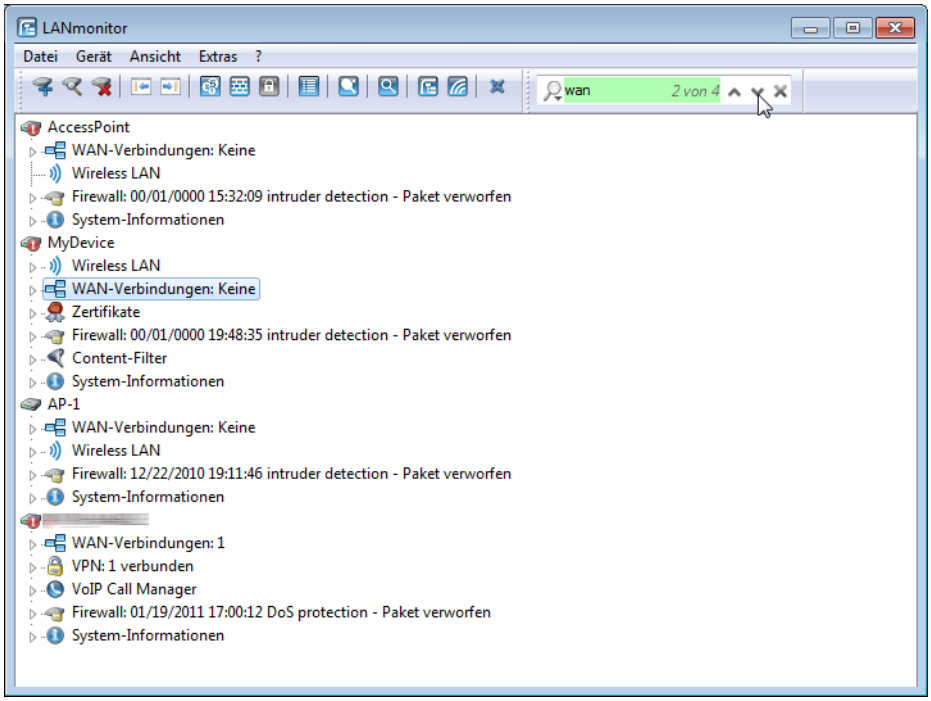
Sie können im LANmonitor das Startverhalten unter **Extras** > **Optionen** einstellen. Lesen Sie hierzu auch *Optionen* auf Seite 271.

Sie können den LANmonitor auch in LANconfig über das Kontextmenü für ein bestimmtes Gerät oder über die Tastenkombination 'Strg+M' starten.

3.2.2 QuickFinder im LANmonitor

Der LANmonitor zeigt je nach Anwendung zahlreiche Geräte, die den gesuchten Begriff enthalten können. Nach dem Start der Suche hebt LANmonitor zunächst die erste Fundstelle hervor. Wechseln Sie entweder mit den Pfeiltasten am

rechten Rand des Suchfensters oder mit den der Tastenkombination 'Strg+F3' zur nächsten Fundstelle oder mit der Tastenkombination 'Strg+Shift+F3' zur vorherigen Fundstelle.



3.2.3 Anzeige-Funktionen im LANmonitor

LANmonitor unterstützt den Administrator von umfangreichen Anwendungen mit einer Reihe von Funktionen, die das Überwachen von Geräten an verteilten Standorten erleichtern. Schon in der Übersicht der überwachten Geräte zeigt LANmonitor die wichtigsten Informationen über den Status der Geräte an. Zu den Informationen, die der Übersicht ablesbar sind, gehören u. a. die Details über die aktiven WAN-Verbindungen, die letzten fünf Meldungen der Firewall, die aktuellen VPN-Verbindungen, sowie die Systeminformationen mit Gebühren und Verbindungszeiten.

Mit einem rechten Mausklick auf die Geräte lassen sich im LANmonitor über das Kontextmenü Listen mit weiteren Informationen aufrufen, darunter u. a.:

- *Aktivitätsprotokoll*
- *DHCP-Zuweisungen*
- *VPN-Verbindungen*
- Firewall-Ereignisanzeigen für *IPv4* sowie *IPv6*
- *Syslog*
- *Accounting-Informationen*

3.2.4 Die Menüstruktur im LANmonitor

LANmonitor unterstützt den Administrator von umfangreichen Anwendungen mit einer Reihe von Funktionen, die das Überwachen von Geräten an verteilten Standorten erleichtern. Über die Menüleiste können Sie dabei Statusinformationen aus den Geräten abrufen, diese zurücksetzen oder weitere Analysen durchführen (z. B. Spectral Scan, Trace-Ausgabe). Zahlreiche Menüpunkte finden Sie auch im Kontextmenü in der Geräteübersicht wieder, verteilt auf die einzelnen Informationspunkte zu den Geräten.

Schon in der Übersicht der überwachten Geräte zeigt LANmonitor die wichtigsten Informationen über den Status der Geräte an. Zu den Informationen, die in der Übersicht abgelesen werden können, gehören u. a. die Details über die aktiven WAN-Verbindungen, die letzten fünf Meldungen der Firewall, die aktuellen VPN-Verbindungen, sowie die Systeminformationen mit Gebühren und Verbindungszeiten.

3.2.4.1 Datei

Unter diesem Menüpunkt verwalten Sie Geräte allgemein und beenden LANmonitor.

Gerät hinzufügen

Über **Datei** > **Gerät hinzufügen** fügen Sie der Geräteübersicht ein neues Gerät hinzu. Es öffnet sich ein Dialog, in dem Sie u. a. Einstellungen für die Verbindung zum das Gerät und die Protokollierung vornehmen.

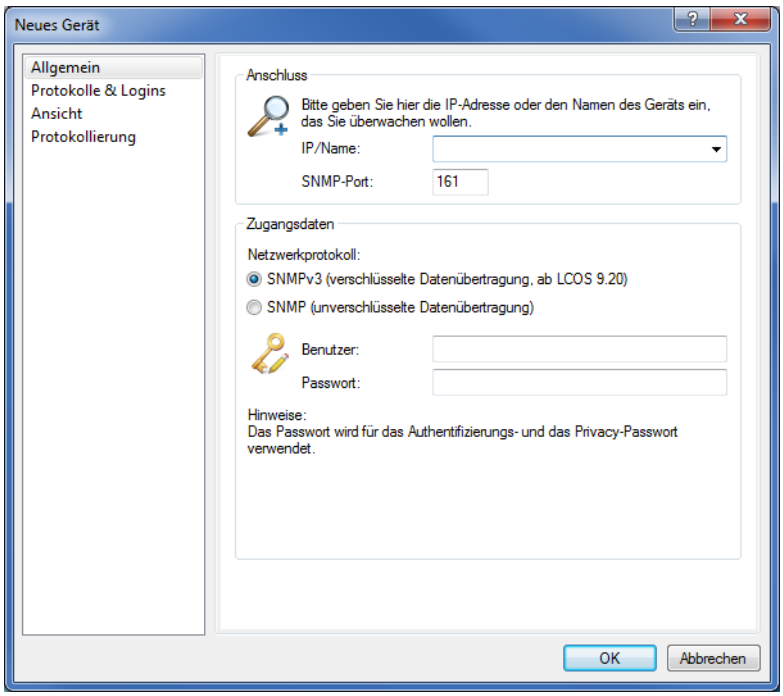
Sie haben alternativ aber auch die Möglichkeit, neue Geräte unter Angabe von IP-Adresse und SNMP-Port direkt beim Programmaufruf zu konfigurieren. Starten Sie LANmonitor dazu über die Syntax `lanmon /add:[<IPv6-Address>]:<Port>`, also z. B. `lanmon /add:[fe80::2a0:57ff:fe1b:3302]:161`.

Allgemein

Auf dieser Seite geben Sie die IP-Adresse und den SNMP-Port des neuen Gerätes an, das LANmonitor künftig überwachen soll. Sofern das Auslesen von Gerätedaten und / oder Durchführen von Aktionen eine Authentisierung am Gerät erfordert, müssen Sie außerdem diese Zugangsdaten in LANmonitor hinterlegen.

Das dauerhafte Hinterlegen der Daten ist mindestens für den Lesezugriff erforderlich; andernfalls kann das Programm keine Verbindung zum betreffenden Gerät aufbauen. Das dauerhafte Hinterlegen der Daten für den Schreibzugriff ist optional, um nicht nach jedem Start von LANmonitor bei der ersten ausgeführten Aktion die Daten manuell einzugeben.

Wenn Sie Benutzernamen und Passwort dauerhaft speichern, erhält jeder Nutzer Zugang zu dem Gerät, der auch LANmonitor ausführen darf.



Anschluss

- **IP/Name:**: Geben Sie die IP-Adresse des Gerätes an. Sie können auch einen Domain-Namen (DN oder FQDN) angeben. Dieser Name wird bei jedem Zugriff überprüft. LANmonitor speichert und verwendet die dabei aufgelöste IP-Adresse. Sollte die Überprüfung einmal nicht möglich sein, greift LANmonitor auf die letzte erfolgreich aufgelöste IP-Adresse zurück.

- **SNMP-Port:** Geben Sie den Port an, unter dem der SNMP-Dienst auf dem Gerät zu erreichen ist. Standardmäßig lautet dieser `161`. Je nach Einstellung im Gerät (vgl. Setup-Parameter 2.9.21) oder ARF-Kontext kann aber auch ein abweichender Port erforderlich sein.

Authentifizierung

Wählen Sie in diesem Abschnitt aus, wie und mit welchen Zugangsdaten Sie sich am Gerät authentisieren. Die zu wählende Einstellung hängt davon ab, ob Sie den SNMP-Lesezugriff auf dem Gerät eingeschränkt und eine eigene Community definiert haben. Mehr dazu erfahren Sie im Abschnitt *Konfigurieren des SNMP-Lesezugriffs* auf Seite 112.

Netzwerkprotokoll

Wählen Sie, ob der LANmonitor via SNMPv3 (verschlüsselt) auf das Gerät zugreift, oder via SNMPv2 (unverschlüsselt; nicht empfohlen). Der Zugriff via SNMPv3 wird ab LCOS 9.20 unterstützt.

SNMPv3

- **Benutzer**: Geben Sie den Benutzer für den SNMPv3-Zugriff an.
- **Passwort**: Geben Sie das Passwort für den SNMPv3-Zugriff an. In der Regel ist dies das Hauptgerätepasswort.

SNMPv2

- **SNMP-Read-Only-Community**: Wählen Sie diese Einstellung, wenn die Authentisierung am Gerät über
  - die öffentliche Community `public`; oder
  - eine eigene Community in Form eines Master-Passworts oder Benutzername:Passwort-Paares

  erfolgt. Diese geben Sie anschließend im Eingabefeld **Community** an.
- **Administrator/Passwort**: Wählen Sie diese Einstellung, wenn die Authentisierung am Gerät über
  - eine eigene Community in Form eines Benutzername:Passwort-Paares; oder
  - die Zugangsdaten eines Administratorkontos

  erfolgt. Den Benutzernamen geben Sie anschließend im Eingabefeld **Administrator**, das Passwort im Eingabefeld **Passwort** an.

Achten Sie dabei auf die korrekte Schreibweise, da bei Eingabe falscher Daten der SNMP-Zugang zum Gerät gesperrt wird.

Darüber hinaus haben Sie optional die Möglichkeit, die **Zugangsdaten für Geräte-Aktionen (SNMP-Write-Community)** wahlweise für die aktuelle Sitzung oder dauerhaft in LANmonitor zu speichern. Diese Daten sind für alle Geräte-Aktionen (z. B. das Löschen oder Zurücksetzen von Status-Werten) erforderlich. Wenn Sie keine Daten hinterlegen, fragt das Programm sie bei der nächsten Aktion ab.

Für den reinen Lesezugriff ist die Angabe einer Read-Only-Community anstelle eines Administratorkontos die bevorzugte Wahl, da SNMP-Pakete bei SNMPv2 im Klartext übertragen werden.

Protokolle & Logins

Auf dieser Seite konfigurieren und verwalten Sie die Protokolle, Ports und Zugangsdaten, welche die übrigen Bestandteile der LANtools beim Aufruf aus LANmonitor heraus verwenden. Zu den konfigurierbaren Programmen gehören:

- LANconfig
- LANtracer
- LANtools-interner sowie externer Webbrowser

Sofern im aufgerufenen Programm z. B. bestimmte Protokolle bereits deaktiviert bzw. anders konfiguriert sind, gelten ausschließlich die Übereinstimmungen.

Die Einstellungsmöglichkeiten sind äquivalent zu denen von LANconfig. Bitte entnehmen Sie die weitere Konfiguration dem Abschnitt *Protokolle & Logins* auf Seite 221.

Ansicht

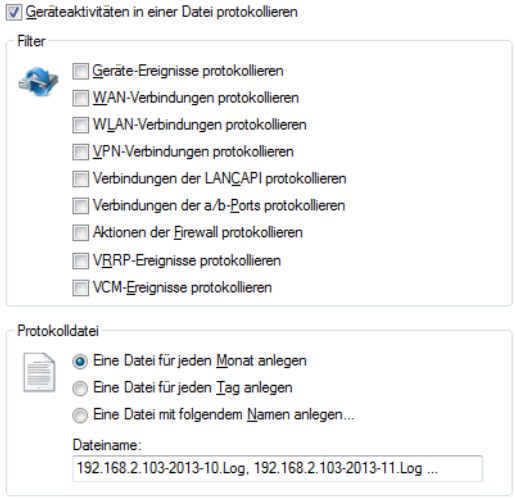
Auf dieser Seite nehmen Sie darstellungsspezifische Einstellungen vor.



Wenn Sie die Option **Tooltips im Systray für dieses Gerät verbergen** aktivieren, zeigt LANmonitor keine Tooltips für dieses Gerät im Systray an.

Protokollierung

Auf dieser Seite steuern Sie die Protokollierung der Geräteaktivitäten durch LANmonitor. Dafür bestimmen Sie nach Aktivieren der Protokollierung durch die **Filter**-Auswahl, welche Aktivitäten LANmonitor erfassen und in welche Protokoll-Datei schreiben soll.



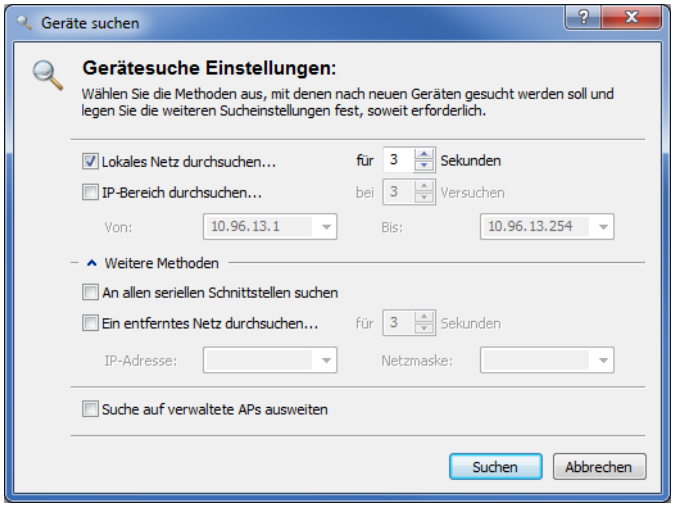
Gerät entfernen

Wenn Sie ein Gerät markiert haben, können Sie es unter **Datei** > **Gerät löschen** entfernen. Sie können auch die Taste 'Entf' drücken, um ein Gerät zu löschen.

Mit dem Löschen entfernen Sie das Gerät nur aus der aktuellen Ansicht. Sie können es jederzeit wieder über **Datei** > **Gerät hinzufügen** oder **Datei** > **Geräte suchen** hinzufügen.

Geräte suchen

Über diesen Menüpunkt starten Sie die automatische Suche nach neuen Geräten, um Sie der Geräteübersicht hinzuzufügen.



Wählen Sie aus, wo nach Geräten gesucht werden soll:

- Im lokalen Netz
- In einem entfernten Netz

  Wenn Sie ein entferntes Netz durchsuchen wollen, müssen Sie die Adresse des Netzwerkes und die zugehörige Netzmaske angeben.

- Sie können die Suche bei Bedarf auch auf verwaltete Access Points (APs) ausweiten.

Klicken Sie auf **Suchen**, um die Suche zu starten. Die gefundenen Geräte werden automatisch der Liste hinzugefügt.

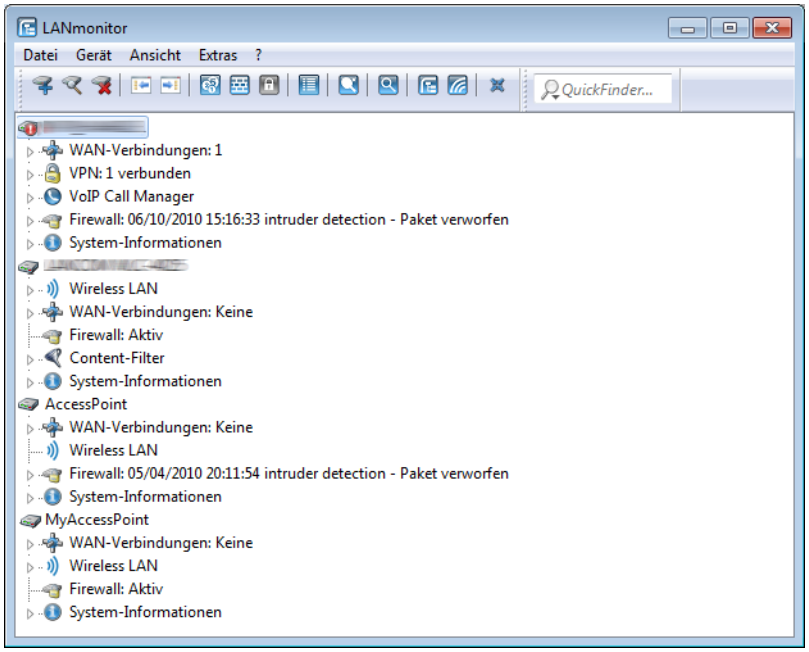
Wenn ein Gerät gefunden wird, das bereits in der Liste vorhanden ist, wird es nicht ein zweites Mal der Liste hinzugefügt. Daher kann es sein, dass weniger Geräte neu hinzukommen, als während des Suchvorgangs gemeldet werden.

Alle Geräte aktualisieren

Aktualisiert die Verbindung zu allen Geräten.

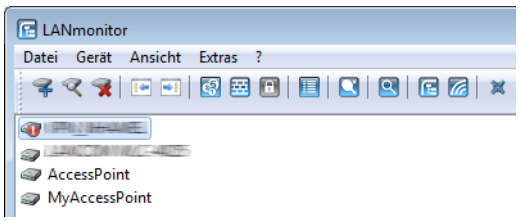
Geräte erweitern

Erweitert die Ansicht der Geräte in der Liste, das Gegenteil ist die *reduzierte Ansicht*. Die erweiterte Ansicht sieht folgendermaßen aus:



Geräte reduzieren

Reduziert die Ansicht der Geräte in der Liste, das Gegenteil ist die *erweiterte Ansicht*. Die reduzierte Ansicht sieht folgendermaßen aus:



Beenden

Schließt und beendet LANmonitor.

3.2.4.2 Gerät

Unter diesem Menüpunkt verwalten und überwachen Sie ein ausgewähltes Gerät im Netz.

Aktualisieren

Aktualisiert die Anzeige für ein ausgewähltes Gerät.

VPN-Verbindungen anzeigen

Sie können sich die VPN-Verbindungen von einem bestimmten Gerät anzeigen lassen. In der Liste der VPN-Verbindungen werden die letzten 100 VPN-Verbindungen protokolliert. Dabei werden folgende Detailinformationen erfasst:

Name

Name der Gegenstelle

Status

Status der Verbindung (z. B. **Verbunden** oder **Nicht Verbunden**)

Letzter Fehler

Zuletzt aufgetretener Fehler

Haltezeit

Für diese Verbindung festgelegte Haltezeit. Die Haltezeit gibt an, nach wieviel Sekunden das Gerät die Verbindung zur Gegenstelle trennt, wenn in dieser Zeit keine Daten mehr übertragen worden sind. Besondere Werte sind:

- '0': Die selbstständige Trennung durch das Gerät ist deaktiviert. Im Falle eines Verbindungsabbruchs bleibt die Verbindung getrennt und muss vom Benutzer manuell aufgebaut werden.
- '9999': Die selbstständige Trennung durch das Gerät ist deaktiviert. Im Falle eines Verbindungsabbruchs zur Gegenstelle baut der Router sie umgehend selbstständig wieder auf.

Verbindung

Kennung des Netzwerks, das für die physikalische Verbindung zur Gegenstelle genutzt wird

Gateway

IP-Adresse des enfernten VPN-Gateways bzw. der Gegenstelle

Nat-Erkennung

Zeigt an, ob ein NAT vorhanden ist

Verschlüsselungs-Algorythmus

Verwendeter Verschlüsselungsalgorithmus

Hash-Algorythmus

Verwendeter Hash-Algorithmus und Länge des Hash-Codes (in Bit)

Hmac-Algorythmus

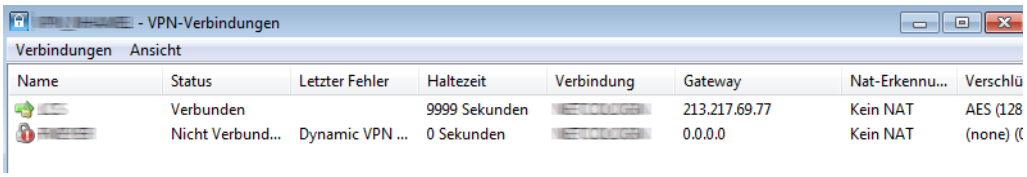
Verwendeter Hmac-Algorithmus und Länge des Hmac-Codes (in Bit)

Kompressions-Algorythmus

Verwendeter IPCOMP-Algorithmus

SSL-Kapselung

Zeigt an, ob eine SSL-Kapselung genutzt wird



Unter dem Menüpunkt **Verbindungen** finden Sie folgende Funktionen:

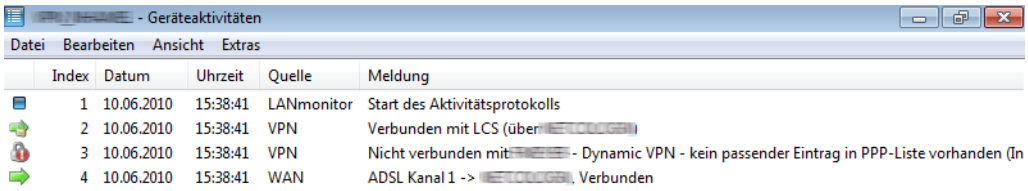
- **Aktualisieren**: Aktualisiert die angezeigten Angaben.
- **Schließen**: Schließt dieses Informationsfenster.

Unter dem Menüpunkt **Ansicht** finden Sie folgende Funktionen:

- **Immer im Vordergrund**: Das Fenster ist immer im Vordergrund.

Geräteaktivitäten anzeigen

Sie können sich die Geräteaktivitäten von einem bestimmten Gerät anzeigen lassen. Mit dem Aktivitätsprotokoll werden die Aktivitäten auf WAN-, WLAN-, VPN- und a/b-Port-Verbindungen sowie der Firewall protokolliert. Dabei werden folgenden Detailinformationen erfasst: **Index**, **Datum**, **Uhrzeit**, **Quelle** und **Meldung**. Das Aktivitätsprotokoll wird fortlaufend aktualisiert.



Unter dem Menüpunkt **Verbindungen** finden Sie folgende Funktionen:

- **Geräteaktivitäten speichern**: Speichert die angezeigten Geräteaktivitäten an einem Ort Ihrer Wahl in einem geeigneten Dateiformat (*.log).
- **Schließen**: Schließt dieses Informationsfenster.

Unter dem Menüpunkt **Bearbeiten** finden Sie folgende Funktionen:

- **Auswahl speichern**: Speichert die markierten Einträge an einem Ort Ihrer Wahl in einem geeigneten Dateiformat (*.log).
- **Auswahl löschen**: Löscht die markierten Einträge.

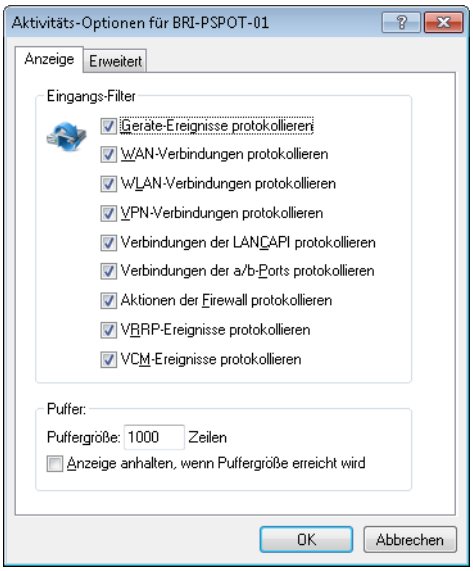
Unter dem Menüpunkt **Ansicht** finden Sie folgende Funktionen:

- **Immer im Vordergrund**: Das Fenster ist immer im Vordergrund.

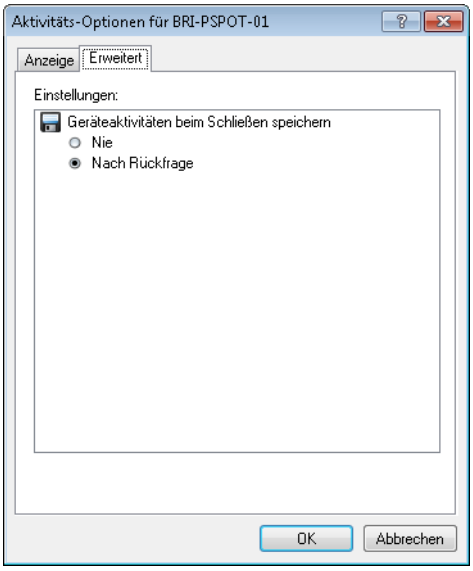
Unter dem Menüpunkt **Extras** finden Sie folgende Funktionen:

- **Optionen**:

  Über diesen Menüpunkt steuern Sie die Protokollierung der gerätespezifischen Aktivitäten durch LANmonitor. Dafür bestimmen Sie durch die **Eingangs-Filter**-Auswahl auf der Registerkarte **Anzeige**, welche Aktivitäten LANmonitor in welchem Umfang (**Puffer**) erfassen soll.



Auf der Registerkarte **Erweitert** legen Sie zusätzlich fest, ob LANmonitor die aufgezeichneten Daten in einer Datei speichert.



Unter **Gerät** > **Eigenschaften** > **Protokollierung** können Sie die Protokolldatei genauer definieren.

Syslog anzeigen

Sie können sich den Syslog von einem bestimmten Gerät anzeigen lassen. Dabei werden folgende Detailinformationen erfasst:

Zeit

Datum Uhrzeit des Syslog-Eintrags

Quelle

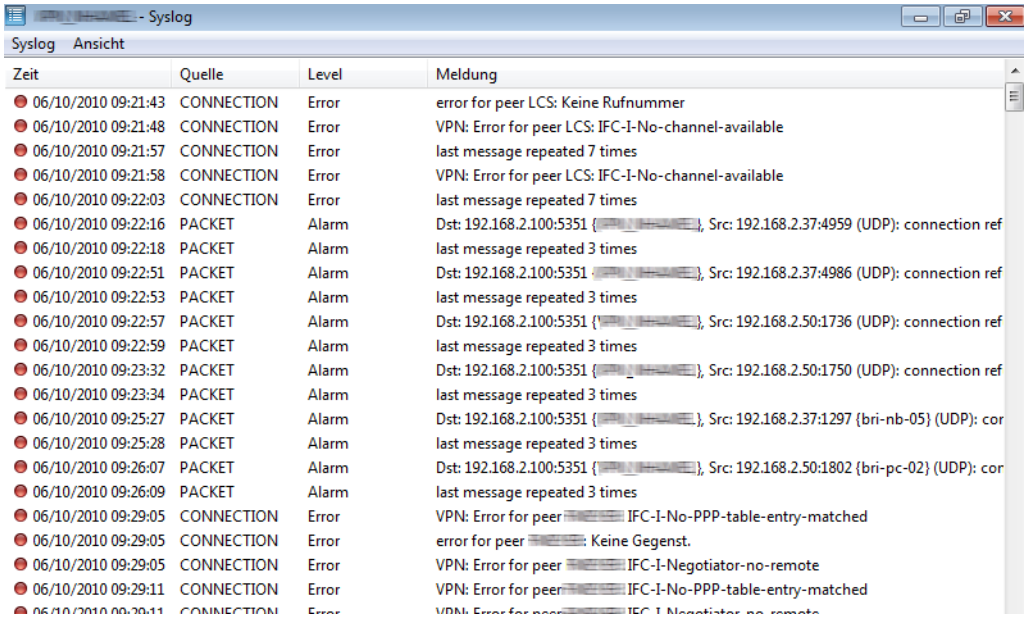
Quelle der Syslog-Meldung

Level

Level der Syslog-Meldung, z. B. Alarm oder Fehler

Meldung

Details der Syslog-Meldung



Unter dem Menüpunkt **Syslog** finden Sie folgende Funktionen:

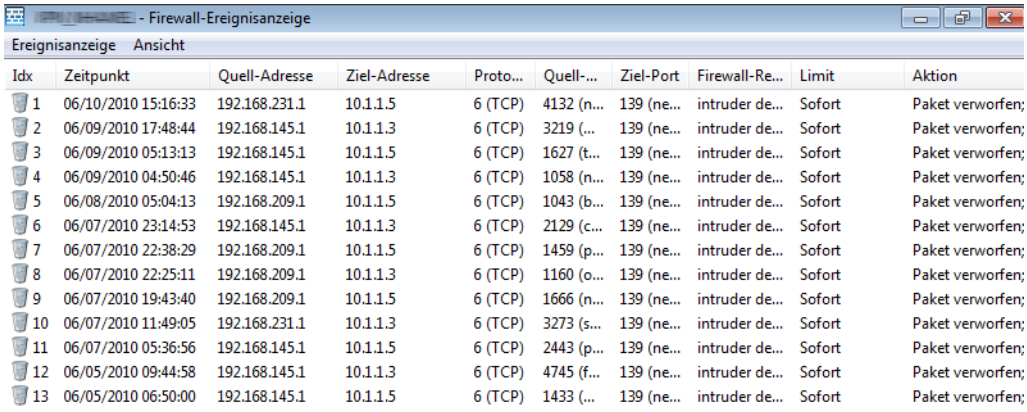
- **Aktualisieren**: Aktualisiert die angezeigten Angaben.
- **Syslog speichern**: Speichert die angezeigte Syslog-Ausgabe an einem Ort Ihrer Wahl in einem geeigneten Dateiformat (*.lsl).
- **Syslog laden**: Lädt eine gespeicherte Syslog-Datei.
- **Schließen**: Schließt dieses Informationsfenster.

Unter dem Menüpunkt **Ansicht** finden Sie folgende Funktionen:

- **Immer im Vordergrund**: Das Fenster ist immer im Vordergrund.

IPv6-Firewall-Ereignisse anzeigen

Über **Gerät** > **Firewall-Ereignisse anzeigen** lassen Sie sich im LANmonitor die Firewall-Ereignisse eines markierten Geräts anzeigen. Die Firewall-Ereignisanzeige listet die letzten 100 Aktionen der Firewall auf. Die angezeigten Detailinformationen und ihre Erläuterungen sind identisch mit denen der *IPv4-Firewall*.



Unter dem Menüpunkt **Ereignisanzeige** finden Sie folgende Funktionen:

- **Aktualisieren**: Aktualisiert die angezeigten Angaben.
- **Schließen**: Schließt dieses Informationsfenster.

Unter dem Menüpunkt **Ansicht** finden Sie folgende Funktionen:

- **Immer im Vordergrund**: Das Fenster ist immer im Vordergrund.

IPv4-Firewall-Ereignisse anzeigen

Sie können sich die Firewall-Ereignisse von einem bestimmten Gerät anzeigen lassen. Mit der Firewall-Ereignisanzeige werden die letzten 100 Aktionen der Firewall protokolliert. Dabei werden folgende Detailinformationen erfasst:

Idx

Fortlaufender Indexeintrag der Ereignisse

Zeitpunkt

Zeitpunkt des Eintrages

Quell-Adresse

Quell-Adresse des gefilterten Pakets

Ziel-Adresse

Ziel-Adresse des gefilterten Pakets

Protokoll

Protokoll (TCP, UDP etc.) des gefilterten Pakets

Quell-Port

Quell-Port des gefilterten Pakets (nur bei portbehafteten Protokollen)

Ziel-Port

Ziel-Port des gefilterten Pakets (nur bei portbehafteten Protokollen)

Firewall-Regel

Name der Regel, die den Eintrag erzeugt hat

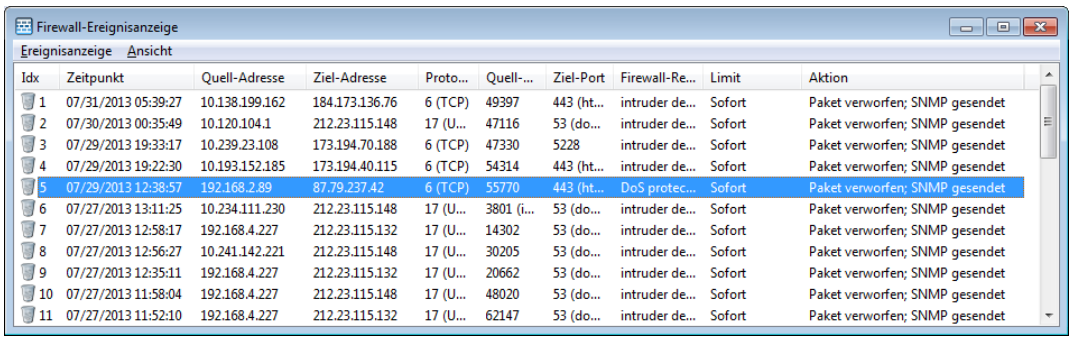
Limit

Limit, welches mit der betreffenden Firewall-Aktion verknüpft ist. Sofern eine Firewall-Aktion nicht mit einem Limit verknüpft ist, wird ein Paket-Limit impliziert, das sogleich beim ersten Paket überschritten wird. In diesem Fall zeigt die Spalte den Wert **Sofort**.

Weitere Informationen zu den Limits finden Sie in der Menüreferenz unter "2.8.10.4 Aktions-Tabelle" im Abschnitt "Limits".

Aktion

Kurzbeschreibung der ausgeführten Aktion



Unter dem Menüpunkt **Ereignisanzeige** finden Sie folgende Funktionen:

- **Aktualisieren**: Aktualisiert die angezeigten Angaben.
- **Schließen**: Schließt dieses Informationsfenster.

Unter dem Menüpunkt **Ansicht** finden Sie folgende Funktionen:

- **Immer im Vordergrund**: Das Fenster ist immer im Vordergrund.

DHCP-Tabelle anzeigen

Sie können sich die DHCP-Tabelle von einem bestimmten Gerät anzeigen lassen. Dabei werden folgende Detailinformationen erfasst:

IP-Adresse

IP-Adresse des lokalen Netzwerkgerätes

MAC-Adresse

MAC-Adresse des lokalen Netzwerkgerätes

Timeout

Gültigkeitsdauer der Adresszuweisung in Minuten.

Rechnername

Names des lokalen Netzwerkgerätes im Netzwerk (sofern bekannt)

Typ

Typ der Adresszuweisung

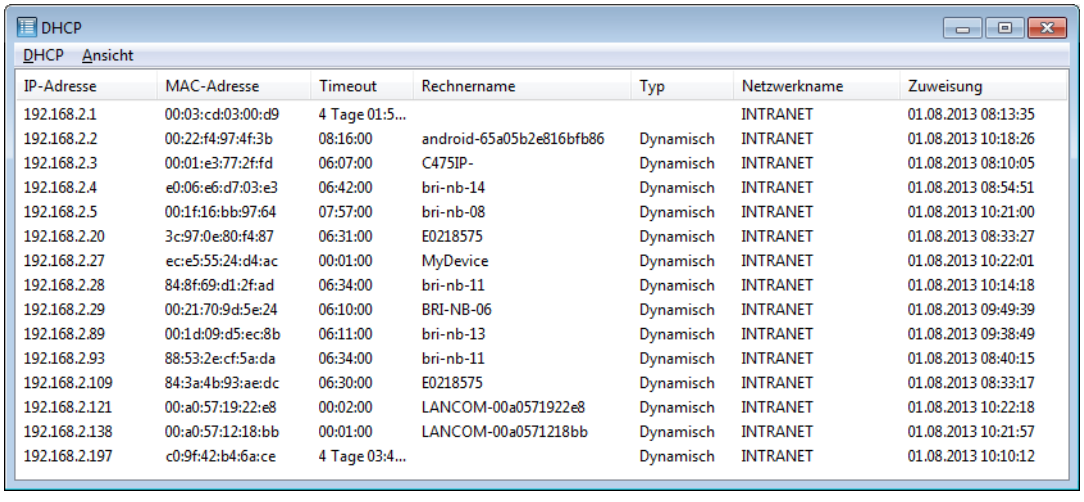
- **Neu**: Der Rechner hat zum ersten Mal angefragt. Der DHCP-Server überprüft die Eindeutigkeit der Adresse, die dem Rechner zugewiesen werden soll.
- **Unbekannt**: Bei der Überprüfung der Eindeutigkeit wurde festgestellt, dass die Adresse bereits an einen anderen Rechner vergeben wurde. Der DHCP-Server hat leider keine Möglichkeit, weitere Informationen über diesen Rechner zu erhalten.
- **Statisch**: Ein Rechner hat dem DHCP-Server mitgeteilt, dass er eine feste IP-Adresse besitzt. Diese Adresse darf nicht mehr für andere Stationen im Netz verwendet werden.
- **Dynamisch**: Der DHCP-Server hat dem Rechner eine Adresse zugewiesen.

Netzwerkname

Anzeige des Netzwerknamen, mit dem das lokale Netzwerkgerät verbunden ist

Zuweisung

Datum und Uhrzeit der Adresszuweisung.



IP-Adresse	MAC-Adresse	Timeout	Rechnername	Typ	Netzwerkname	Zuweisung
192.168.2.1	00:03:cd:03:00:d9	4 Tage 01:5...			INTRANET	01.08.2013 08:13:35
192.168.2.2	00:22:f4:97:4f:3b	08:16:00	android-65a05b2e816bfb86	Dynamisch	INTRANET	01.08.2013 10:18:26
192.168.2.3	00:01:e3:77:2f:fd	06:07:00	C475IP-	Dynamisch	INTRANET	01.08.2013 08:10:05
192.168.2.4	e0:06:e6:d7:03:e3	06:42:00	bri-nb-14	Dynamisch	INTRANET	01.08.2013 08:54:51
192.168.2.5	00:1f:16:bb:97:64	07:57:00	bri-nb-08	Dynamisch	INTRANET	01.08.2013 10:21:00
192.168.2.20	3c:97:0e:80:f4:87	06:31:00	E0218575	Dynamisch	INTRANET	01.08.2013 08:33:27
192.168.2.27	ec:e5:55:24:d4:ac	00:01:00	MyDevice	Dynamisch	INTRANET	01.08.2013 10:22:01
192.168.2.28	84:8f:69:d1:2f:ad	06:34:00	bri-nb-11	Dynamisch	INTRANET	01.08.2013 10:14:18
192.168.2.29	00:21:70:9d:5e:24	06:10:00	BRI-NB-06	Dynamisch	INTRANET	01.08.2013 09:49:39
192.168.2.89	00:1d:09:d5:ec:8b	06:11:00	bri-nb-13	Dynamisch	INTRANET	01.08.2013 09:38:49
192.168.2.93	88:53:2e:cf:5a:da	06:34:00	bri-nb-11	Dynamisch	INTRANET	01.08.2013 08:40:15
192.168.2.109	84:3a:4b:93:ae:dc	06:30:00	E0218575	Dynamisch	INTRANET	01.08.2013 08:33:17
192.168.2.121	00:a0:57:19:22:e8	00:02:00	LANCOM-00a0571922e8	Dynamisch	INTRANET	01.08.2013 10:22:18
192.168.2.138	00:a0:57:12:18:bb	00:01:00	LANCOM-00a0571218bb	Dynamisch	INTRANET	01.08.2013 10:21:57
192.168.2.197	c0:9f:42:b4:6a:ce	4 Tage 03:4...		Dynamisch	INTRANET	01.08.2013 10:10:12

Unter dem Menüpunkt **Accounting** finden Sie folgende Funktionen:

- **Aktualisieren**: Aktualisiert die angezeigten Angaben.
- **Schließen**: Schließt dieses Informationsfenster.

Unter dem Menüpunkt **Ansicht** finden Sie folgende Funktionen:

- **Immer im Vordergrund**: Das Fenster ist immer im Vordergrund.

Accounting-Informationen anzeigen

Sie können sich die Accounting-Informationen von einem bestimmten Gerät anzeigen lassen. Mit den Accounting-Informationen werden die Verbindungen der einzelnen Stationen im LAN zu den erreichbaren Gegenstellen im WAN protokolliert. Dabei werden folgende Detailinformationen erfasst:

Benutzer

Name der Verbindung, in der Regel der Name des Netzwerkgerätes, welches über das ausgewählte Gerät eine Verbindung aufgebaut hat.

Gegenstelle

Name der Gegenstelle, zu der das ausgewählte Gerät eine Verbindung aufgebaut hat.

Typ

Typ der Verbindung

Verbindungen

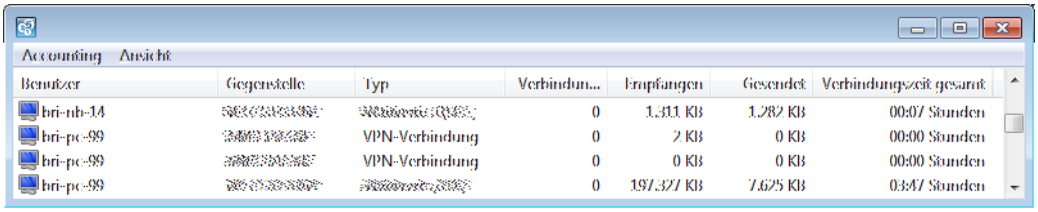
Anzahl der Verbindungen, die vom betreffenden Typ zur gelisteten Gegenstelle derzeit offen sind.

Empfangen, Gesendet

Datenmenge, die der Benutzer innerhalb der Verbindungszeit empfangen/gesendet hat.

Verbindungszeit insgesamt

Gesamte Verbindungszeit in Stunden, Minuten und Sekunden.



Unter dem Menüpunkt **Accounting** finden Sie folgende Funktionen:

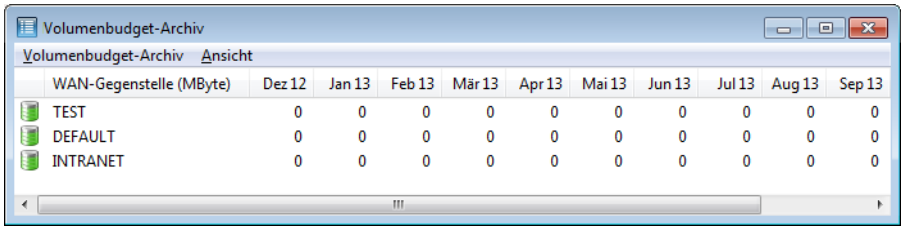
- **Zurücksetzen**: Löscht alle Accounting-Informationen und setzt alle Zähler auf '0' zurück.
- **Aktualisieren**: Aktualisiert die angezeigten Angaben.
- **Accounting-Informationen speichern**: Speichert die angezeigten Accounting-Informationen an einem Ort Ihrer Wahl in einem geeigneten Dateiformat (*.acc).
- **Accounting-Informationen laden**: Lädt eine gespeicherte Datei mit Accounting-Informationen.
- **Schließen**: Schließt dieses Informationsfenster.

Unter dem Menüpunkt **Ansicht** finden Sie folgende Funktionen:

- **Immer im Vordergrund**: Das Fenster ist immer im Vordergrund.
- **Accounting-Liste (aktuelle)**: Zeigt die aktuelle Accounting-Liste.
- **Accounting-Liste (letzter Abrechnungszeitraum)**: Zeigt die Accounting-Liste des letzten Abrechnungszeitraums.

Volumen-Budget-Archiv anzeigen

Zeigt das Volumen-Budget-Archiv aller WAN-Schnittstellen an.



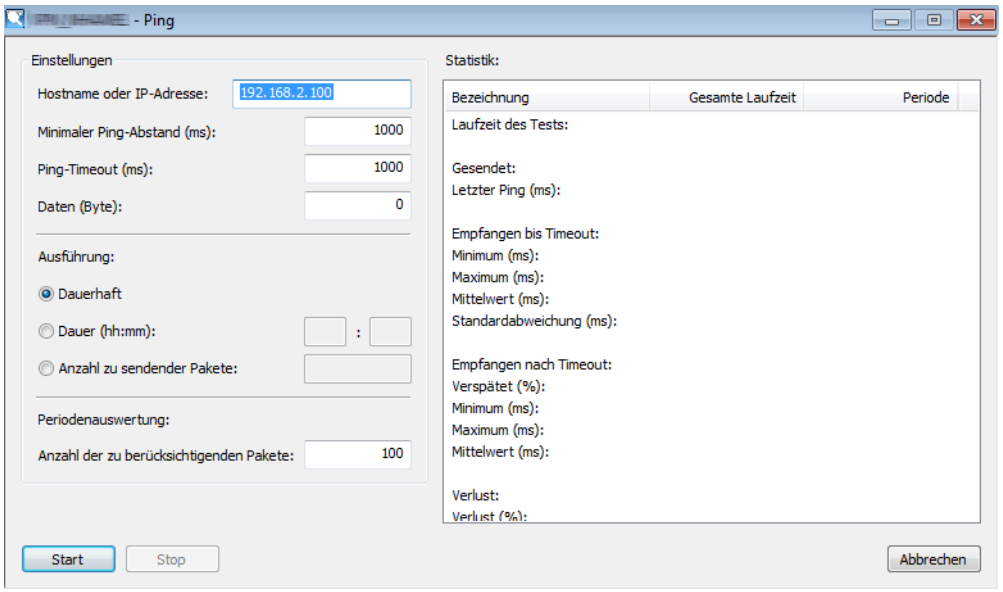
Zeit- und Gebührenlimits zurücksetzen

Hier können Sie das Zeit- und Gebührenlimit des markierten Geräts auf Null zurücksetzen. Damit beginnt die Zeit-/Gebührenzählung erneut, auch wenn der nächste Zeitrahmen zur Limitierung nicht erreicht ist.

Ping

Mit dem LANmonitor haben Sie die Möglichkeit, die Qualität der Verbindung zu Gegenstellen in LAN, WAN oder WLAN zu prüfen. Dazu sendet der LANmonitor von dem Arbeitsplatzrechner, auf dem er installiert ist, regelmäßig Ping-Befehle an eine Gegenstelle und erstellt mit den empfangenen Antworten zusammen einen Bericht.

Zur Eingabe der Parameter und zur Anzeige der Auswertung des Ping-Tests dient ein eigener Dialog, der aus dem LANmonitor heraus aufgerufen werden kann:



Konfiguration der Ping-Ausführung

- **Hostname oder IP-Adresse**: Hier wird die Gegenstelle eingetragen, die mit dem Ping erreicht werden soll. Möglich sind folgende Angaben für alle in LAN, WAN oder WLAN erreichbaren Netzwerkgeräte (Server, Clients, Router, Drucker etc.):

Sofern beim Öffnen des Ping-Dialogs über Gerät > Ping oder über das Kontextmenü im LANmonitor ein Gerät ausgewählt ist, wird die IP-Adresse des Geräts als Gegenstelle übernommen.

- **Minimaler Ping-Abstand**: Zeitlicher Abstand zwischen zwei Ping-Befehlen in [ms].

Die Abstände zwischen zwei Pings können nicht kleiner sein als die Paketlaufzeit, d. h. vor Versenden eines Pings muss der vorherige Ping beantwortet oder der Ping-Timeout abgelaufen sein.

- **Ping-Timeout**: Wartezeit für die Antwort auf den Ping in [ms]. Wenn nach Ablauf der Wartezeit keine Antwort empfangen wurde, wird das Paket als verloren gewertet.
- **Daten**: Größe der für den Ping verschickten Pakete [Byte]. Ein "Ping" ist ein ICMP-Paket, das üblicherweise ohne Inhalt verschickt wird, also nur aus seinem Header besteht. Um die Last der Verbindungsüberprüfung zu erhöhen, kann eine Payload, also ein Inhalt, künstlich erzeugt werden. Die gesamte Paketgröße ergibt sich dann aus IP-Header (20 Byte), ICMP-Header (8 Byte) und Nutzlast.

Wenn durch die Payload der ICMP-Pakete die maximale Paketgröße der IP-Pakete überschritten wird, werden die Pakete fragmentiert.

- **Ausführung**: Wiederholungsmodus für den Ping-Befehl. Sie haben die Möglichkeit, die Ping-Prüfung neben dem manuellen Stopp auch nach Ablauf einer bestimmten Zeit oder definierten Anzahl gesendeter Datenpakete zu beenden.
- **Periodenauswertung**: Im rechten Teil des Ping-Dialogs werden die Ergebnisse der Ping-Prüfung dargestellt. Die erste Spalte zeigt die summierten Werte der gesamten Laufzeit, die zweite Spalte zeigt nur die Ergebnisse der Prüfperiode, also die summierten Werte der letzten Pakete. Unbeantwortete Pings gehen nicht in die Auswertung mit ein.

Bei der Periodenauswertung werden nur die in der Periode gesendeten Pings ausgewertet.

Statistik

Folgende Daten werden zur Auswertung angezeigt:

- Laufzeit des Tests: Gesamte Laufzeit [Std. / Min. / Sek.]
- Gesendet: Gesamte Anzahl der gesendeten Pings
- Laufzeit des letzten Pings [ms]
- Empfangen bis Timeout: Anzahl der Pings, die im Timeout-Zeitraum beantwortet wurden
- Minimale Laufzeit
- Maximale Laufzeit
- Mittelwert
- Standardabweichung von der mittleren Laufzeit
- Empfangen nach Timeout: Anzahl der Pings, die nach dem Timeout beantwortet wurden
- Anteil der verspäteten Pakete an der Gesamtzahl
- Minimale Laufzeit
- Maximale Laufzeit
- Mittelwert
- Verlust
- Letzter Fehler

Trace-Ausgabe erstellen

Mit dieser Option starten Sie die Trace-Ausgabe in LANtracer.

Lesen Sie hierzu auch *LANtracer – Tracen mit LANconfig und LANmonitor* auf Seite 292.

Spectral-Scan anzeigen

Über diesen Menüpunkt starten Sie für das ausgewählte Gerät das Spectral-Scan-Modul im LANmonitor-internen Webbrowser. Weitere Informationen zur Konfiguration finden Sie unter *Funktionen des Software-Moduls* auf Seite 989

Punkt-zu-Punkt WLAN-Antennen einrichten

Wenn es sich bei dem ausgewählten Gerät um ein WLAN-Gerät handelt, können Sie die Punkt-zu-Punkt WLAN-Antennen einrichten.

Dieser Menüeintrag ist im LANmonitor nur sichtbar, wenn in dem überwachten Gerät mindestens eine Basisstation als Gegenstelle für eine P2P-Verbindung eingerichtet ist (in LANconfig unter **Wireless LAN** > **Allgemein** > **Physikalische WLAN-Einst.** > **Punkt-zu-Punkt**).

Ausrichten der Antennen für den P2P-Betrieb

Beim Aufbau von P2P-Strecken kommt der genauen Ausrichtung der Antennen eine große Bedeutung zu. Je besser die empfangende Antenne in der "Ideallinie" der sendenden Antenne liegt, desto besser ist die tatsächliche Leistung und damit die nutzbare Bandbreite. Liegt die empfangende Antenne jedoch deutlich neben dem idealen Bereich, sind erhebliche Leistungsverluste zu erwarten.

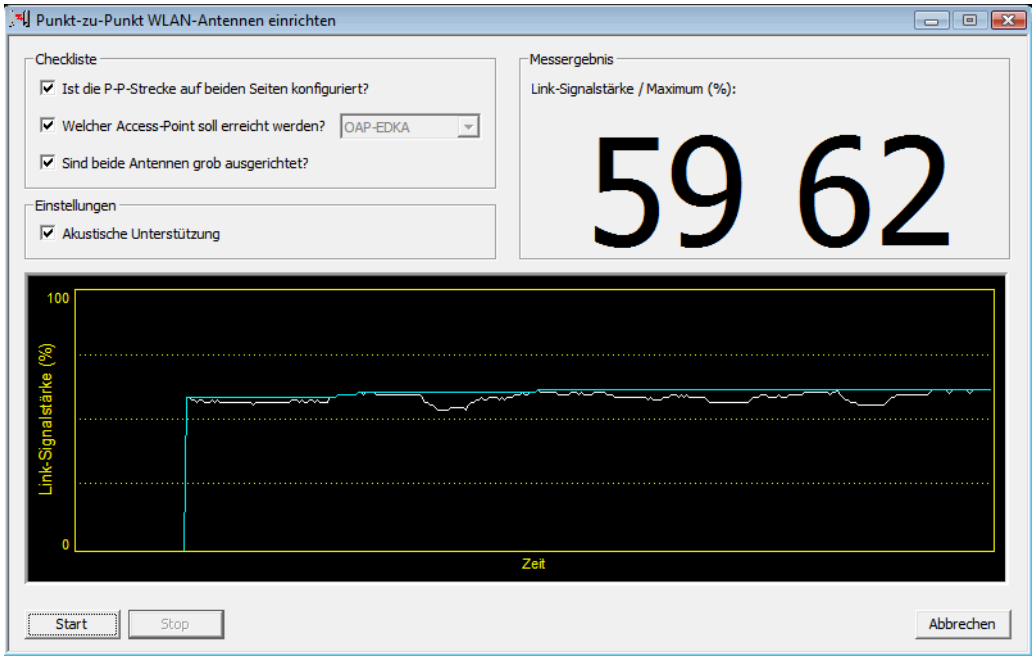
Um die Antennen möglichst gut auszurichten, kann die aktuelle Signalqualität von P2P-Verbindungen über die LEDs des Gerätes oder im LANmonitor angezeigt werden.

Die Anzeige der Signalqualität über die LEDs muss für die physikalische WLAN-Schnittstelle aktiviert werden. Je schneller die LED blinkt, umso besser ist die Verbindung (eine Blinkfrequenz von 1 Hz steht für eine Signalqualität von 10 dB, eine Verdoppelung der Frequenz zeigt die jeweils doppelte Signalstärke).

Im Dialog zur Einrichtung der Punkt-zu-Punkt-Verbindung fragt der LANmonitor die Voraussetzungen für den P2PVerbindungsaufbau ab:

- Ist die P2P-Strecke auf beiden Seiten konfiguriert (gegenüberliegende Basisstation mit MAC-Adresse oder Stations-Namen definiert)?
- Welcher Access Point soll überwacht werden? Hier können alle im jeweiligen Gerät als P2P-Gegenstelle eingetragenen Basis-Stationen ausgewählt werden.
- Sind beide Antennen grob ausgerichtet? Die Verbindung über die P2P-Strecke sollte schon grundsätzlich funktionieren, bevor die Einrichtung mit Hilfe des LANmonitors gestartet wird.

Der P2P-Dialog zeigt nach dem Start der Signalüberwachung jeweils die absoluten Werte für die aktuelle Signalstärke sowie den Maximalwert seit dem Start der Messung. Zusätzlich wird der zeitliche Verlauf mit dem Maximalwert in einem Diagramm angezeigt.



Bewegen Sie zunächst nur eine der beiden Antennen, bis sie den Maximalwert erreicht haben. Stellen Sie dann die erste Antenne fest und bewegen Sie auch die zweite Antenne in die Position, bei der Sie die höchste Signalqualität erreichen.

Konfigurieren

Startet LANconfig, um das ausgewählte Gerät zu konfigurieren.

Web-Browser starten

Startet den Standard-Web-Browser, um das ausgewählte Gerät über WEBconfig zu konfigurieren.

Content-Filter-Kategorien anzeigen

Sofern Ihr Gerät über ein aktiviertes Content-Filter-Modul verfügt, rufen Sie über diesen Menüpunkt die Content-Filter-Kategorien auf.



Unter dem Menüpunkt **Content-Filter-Kategorien** finden Sie folgende Funktionen:

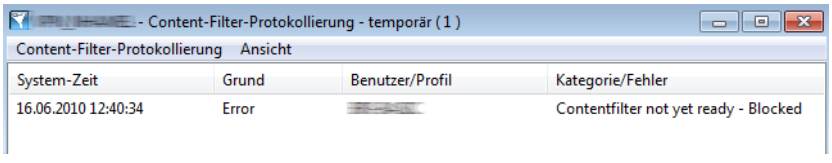
- **Zurücksetzen**: Löscht die angezeigten Informationen und setzt alle Zähler auf Null zurück.
- **Aktualisieren**: Aktualisiert die angezeigten Angaben.
- **Kategorien-Informationen speichern**: Speichert die angezeigten Kategorien-Informationen an einem Ort Ihrer Wahl in einem geeigneten Dateiformat (*.acc).
- **Kategorien-Informationen laden**: Lädt gespeicherte Kategorien-Informationen aus einer Datei.
- **Schließen**: Schließt dieses Informationsfenster.

Unter dem Menüpunkt **Ansicht** finden Sie folgende Funktionen:

- **Immer im Vordergrund**: Das Fenster ist immer im Vordergrund.
- **Content-Filter-Kategorien (Aktuell)**: Zeigt den aktuellen Status der Content-Filter-Kategorien.
- **Content-Filter-Kategorien (Last-Snapshot)**: Zeigt den Status der Content-Filter-Kategorien beim letzten Schnappschuss.

Content-Filter-Protokollierung anzeigen

Sofern Ihr Gerät über ein aktiviertes Content-Filter-Modul verfügt, sehen Sie über diesen Menüpunkt die Content-Filter-Protokollierung ein.



Unter dem Menüpunkt **Content-Filter-Protokollierung** finden Sie folgende Funktionen:

- **Zurücksetzen**: Löscht die angezeigten Informationen.
- **Aktualisieren**: Aktualisiert die angezeigten Angaben.
- **Schließen**: Schließt dieses Informationsfenster.

Unter dem Menüpunkt **Ansicht** finden Sie folgende Funktionen:

- **Immer im Vordergrund**: Das Fenster ist immer im Vordergrund.

Eigenschaften

Über diesen Menüpunkt öffnen Sie den Eigenschaften-Dialog des markierten Gerätes, in dem sich auf verschiedenen Seiten teils globale, teils gerätespezifische Einstellungen vornehmen oder einsehen lassen.

Die verfügbaren Seiten des Dialogs sind weitgehend identisch mit denen unter **Datei** > **Gerät hinzufügen**. Dieser Abschnitt behandelt daher nur jene Seiten, die ausschließlich im Eigenschaften-Dialog erscheinen. Für alle übrigen Seiten, siehe

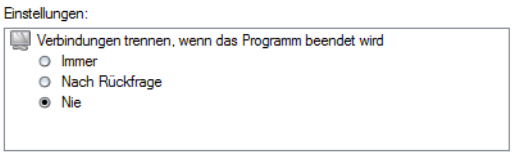
- *Allgemein* auf Seite 253
- *Protokolle & Logins* auf Seite 254
- *Ansicht* auf Seite 255
- *Protokollierung* auf Seite 255

Information

Auf dieser Seite finden Sie weitere Informationen zu Gerät und Hersteller.

Erweitert

Auf dieser Seite finden Sie erweiterte Einstellungen.



Unter **Verbindungen trennen, wenn das Programm beendet wird** stellen Sie ein, ob LANmonitor bestehende Verbindungen des Gerätes zu Gegenstellen beim Beenden trennen soll.

- **Immer**: LANmonitor trennt die Verbindungen stets ohne Rückfrage.
- **Nach Rückfrage**: LANmonitor trennt Verbindungen nur nach vorangehender Bestätigung durch den Benutzer.
- **Nie**: LANmonitor trennt die Verbindungen nicht. Die Verbindungen bleiben bestehen.

3.2.4.3 Ansicht

Unter diesem Menüpunkt passen Sie das Verhalten der LANmonitor-Bedienoberfläche an.

Immer im Vordergrund

Wenn Sie diese Einstellung aktivieren, wird das Fenster stets im Vordergrund angezeigt.

Zustand im Systray anzeigen

Wenn Sie diese Einstellung aktivieren, zeigt LANmonitor den Zustand der Geräte (Fehler) im Systray an.

LANmonitor in den Systray minimieren

Wenn Sie diese Einstellung aktivieren, wird LANmonitor beim Minimieren im Systray anstelle der Taskleiste abgelegt.

Symbolleiste

Blendet die Symbolleiste aus bzw. ein. Lesen Sie hierzu auch *Die Symbolleiste im LANmonitor* auf Seite 271.

Anzeigen

Unter diesem Menüpunkt stellen Sie folgende Anzeige-Optionen ein oder aus:

- Fehlermeldungen
- Diagnosemeldungen
- System-Informationen

Viele wichtige Details zum Status eines Gerätes werden erst angezeigt, wenn die Anzeige der System-Informationen aktiviert ist. Dazu gehören beispielsweise die Schnittstellen und das Gebührenmanagement. Wir empfehlen daher interessierten Benutzern, die Anzeige der System-Informationen einzuschalten.

3.2.4.4 Extras

Unter diesem Menüpunkt lesen Sie die gespeicherten Informationen ausgewählter Informationsfenster ein (z. B. gespeicherte Syslog- oder Accounting-Protokolle) und starten andere Programmbestandteile der LANtools.

LANmonitor (temporär) starten

Öffnet ein neues Fenster von LANmonitor zur temporären Überwachung von Geräten. Nach dem Schließen von LANmonitor gehen die Einstellungen des temporären LANmonitor-Fensters verloren.

WLANmonitor starten

Startet den WLANmonitor. Mehr Informationen dazu erhalten Sie im Kapitel *WLANmonitor – WLAN-Geräte überwachen* auf Seite 276.

LANconfig starten

Startet LANconfig. Mehr Informationen dazu erhalten Sie im Kapitel *LANconfig – Geräte konfigurieren* auf Seite 174.

Geräteprotokoll-Datei anzeigen

Öffnet die Sicherung eines Aktivitäten-Protokolls zur Ansicht. Lesen Sie dazu auch *Geräteaktivitäten anzeigen* auf Seite 259.

Accounting-Datei anzeigen

Hier können Sie eine Accounting-Datei laden. Lesen Sie dazu auch *Accounting-Informationen anzeigen* auf Seite 264.

Syslog-Datei anzeigen

Hier können Sie eine Syslog-Datei laden. Lesen Sie dazu auch *Syslog anzeigen* auf Seite 260.

Trace-Ausgabe analysieren

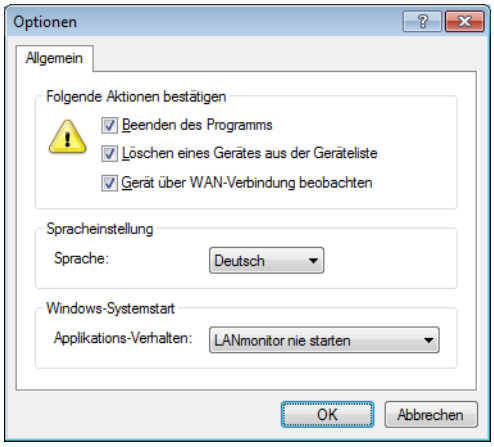
Startet LANtracer. Mehr Informationen dazu erhalten Sie im Kapitel *LANtracer – Tracen mit LANconfig und LANmonitor* auf Seite 292.

Ping

Hier können Sie einen Ping-Test durchführen. Lesen Sie dazu auch *Ping* auf Seite 265.

Optionen

Hier können Sie die Einstellungen zum Bestätigen von Aktionen, zur Spracheinstellung und zum Verhalten der Applikation beim Windows-Systemstart bearbeiten.



- **Folgende Aktionen bestätigen**: Geben Sie an, welche Aktionen durch den Nuter bestätigt werden müssen.
- **Spracheinstellung**: Wählen Sie hier die Sprache der grafischen Programmoberfläche (Deutsch, Englisch oder Spanisch).
- **Windows-Systemstart**: Wählen Sie hier, wie LANmonitor sich beim Starten von Windows verhalten soll.

3.2.4.5 Hilfe

Unter diesem Menüpunkt finden Sie weitere Hilfe zum Programm und lassen sich Informationen zur Software anzeigen.

Hilfethemen

Über diesen Menüpunkt gelangen Sie zu den Hilfethemen. Alternativ können Sie auch F1 drücken.

Info

Unter diesem Menüpunkt werden Ihnen die Version und das Builddatum der Software angezeigt.

3.2.5 Die Symbolleiste im LANmonitor



Die Symbolleiste im LANmonitor beinhaltet die folgenden Funktionen:

- Gerät hinzufügen
- Geräte suchen
- Gerät entfernen
- Geräte reduzieren
- Geräte erweitern
- Accounting-Informationen anzeigen
- IPv4-Firewall-Ereignisse anzeigen
- VPN-Verbindungen anzeigen
- Geräteaktivitäten anzeigen
- Ping
- Trace-Ausgabe erstellen
- Spectral Scan anzeigen

- LANmonitor (temporär) starten
- WLANmonitor starten
- Alle Fenster in den Systray minimieren
- QuickFinder

Unter **Ansicht** > **Symbolleiste** blenden Sie die Symbolleiste ein- oder aus.

3.2.6 Das Kontextmenü im LANmonitor

Das Kontextmenü zu jedem hinzugefügten Gerät in der LANmonitor-Ansicht zeigt dieselben Funktionen wie das Menü **Gerät** in der Menüleiste. Zusätzlich ist die Funktion **Löschen** enthalten, um das Gerät aus der LANmonitor-Ansicht zu entfernen.

3.2.7 LANmonitor Tastaturbefehle

Einfg	Gerät hinzufügen
Entf	Gerät entfernen
F3	Geräte suchen
F5	Alle Geräte aktualisieren
Alt+F4	Beenden
Pfeil hoch	Einen Eintrag in der Geräteliste aufwärts springen
Pfeil runter	Einen Eintrag in der Geräteliste abwärts springen
Pfeil links, ENTER	Menübaum in der Geräteliste reduzieren
Pfeil rechts, ENTER	Menübaum in der Geräteliste erweitern
Strg+F5	Aktualisieren
Space	Gerät > Optionen
F7	Extras > Optionen
F1	Hilfethemen

3.2.8 Anwendungskonzepte für LANmonitor

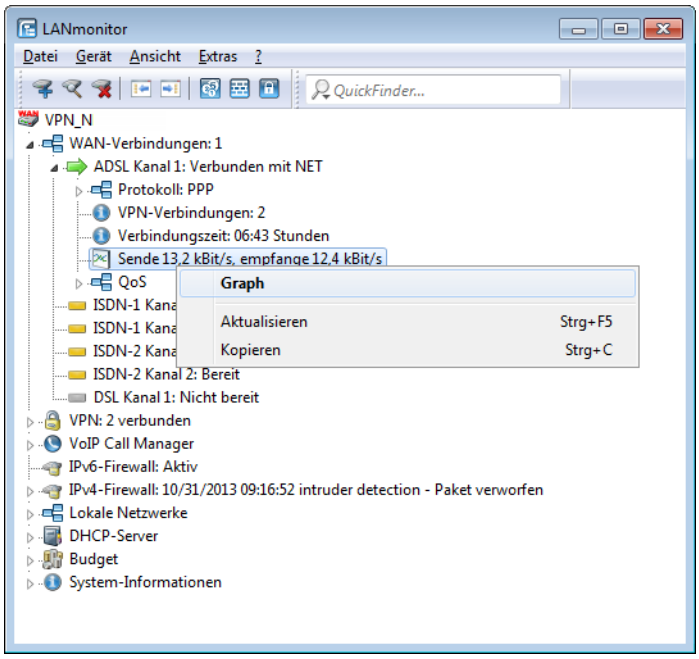
In diesem Abschnitt finden Sie verschiedene Anwendungskonzepte für LANmonitor.

3.2.8.1 Performance Monitoring im LANmonitor

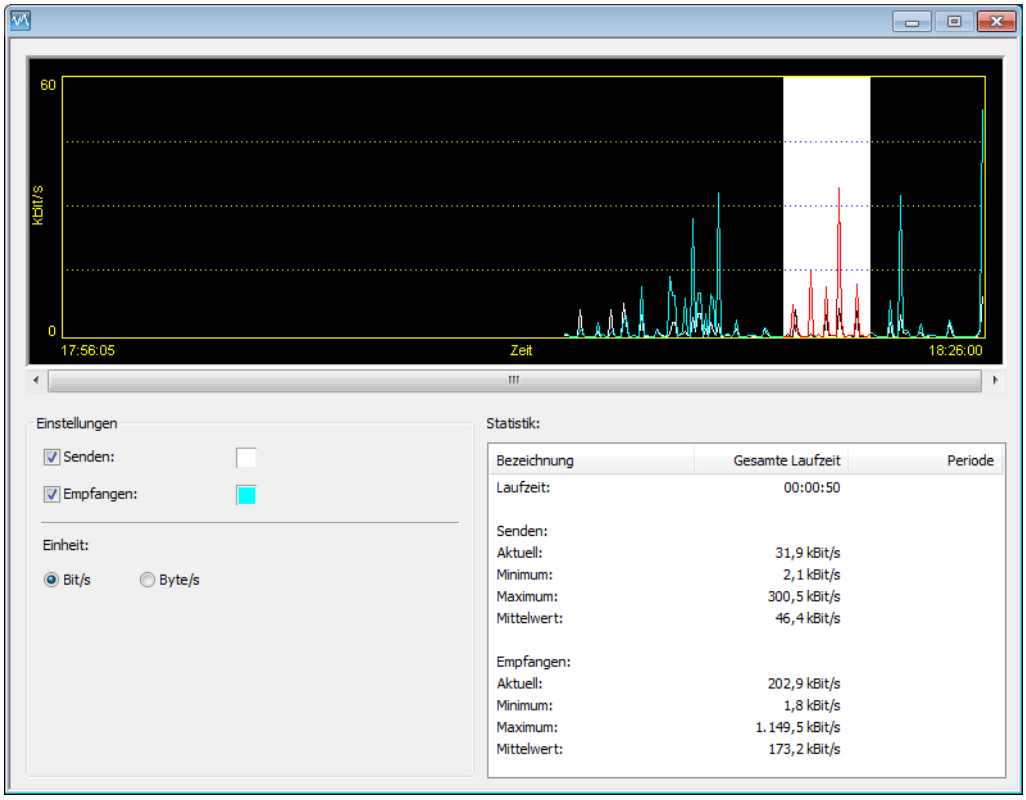
LANmonitor ist dazu in der Lage, verschiedene Kenngrößen eines Gerätes aufzuzeichnen und diese in Form einer Verlaufskurve graphisch darzustellen. Hierzu gehören u. a.:

- Sende- und Empfangsrate für WAN-Verbindungen
- Sende- und Empfangsrate für Point-to-Point-Verbindungen
- Empfangssignalstärke für Point-to-Point-Verbindungen
- Linksignalstärke für Point-to-Point-Verbindungen
- Durchsatz für Point-to-Point-Verbindungen
- CPU-Last
- Freier Speicher
- Temperatur (nicht für alle Modelle verfügbar)

Die aktuellen Werte einer Kenngröße zeigt LANmonitor direkt im entsprechenden Gruppenzweig der Geräteübersicht an. Um die graphische Aufzeichnung zu starten, öffnen Sie auf einer Kenngröße das Kontextmenü und wählen den Eintrag **Graph**.



Daraufhin öffnet sich ein weiteres Fenster, welches den zeitlichen Verlauf der Kenngröße dargestellt.



Indem Sie mit der linken Maustaste im aktuellen Graph eine Periode markieren, bekommen Sie deren Werte in der Statistik separat angezeigt.

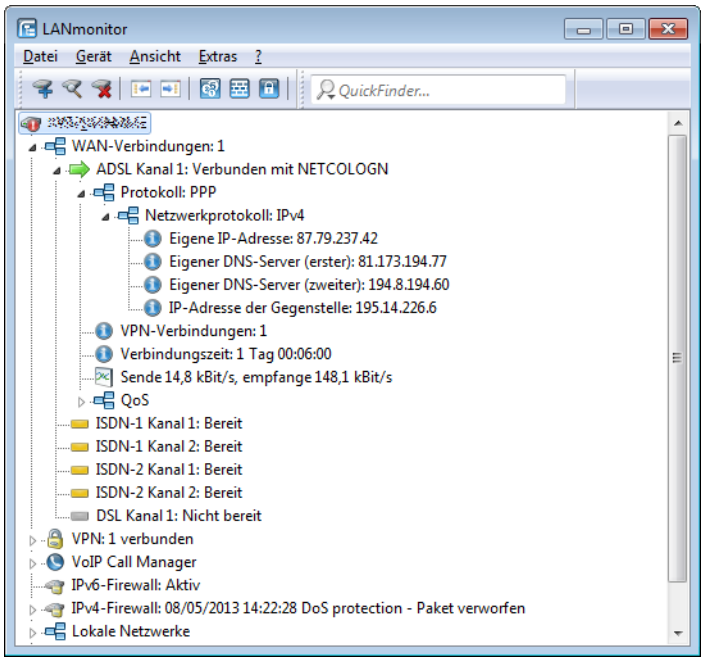
Bitte beachten Sie, dass die angezeigte Werte gelöscht werden, sobald der Dialog geschlossen wird. Für eine längere Überwachung lassen Sie das Fenster dauerhaft geöffnet. Der Dialog stellt maximal die Werte der letzen 24 Stunden dar.

3.2.8.2 Internet-Verbindung kontrollieren

Als Beispiel für die Funktionen von LANmonitor wird in diesem Abschnitt gezeigt, welche Informationen LANmonitor über den Verbindungsaufbau zu Ihrem Internet-Provider bereitstellt

1. Starten Sie LANmonitor, z. B. mit einem Doppelklick auf das Desktop-Symbol.
2. Legen Sie über **Datei** > **Gerät hinzufügen** ein neues Gerät an und geben im sich öffnenden Fenster die IP-Adresse für das Gerät an, das Sie überwachen wollen. Falls die Konfiguration des Gerätes mit einem Passwort gesichert ist, geben Sie dieses gleich mit ein. LANmonitor legt automatisch einen neuen Eintrag in der Geräteliste an und zeigt zunächst den Zustand der Übertragungskanäle.
3. Starten Sie Ihren Web-Browser und geben Sie eine beliebige Webseite ein.
4. Wechseln Sie zurück zu LANmonitor und öffnen Sie den Zweig **WAN-Verbindungen** des Gerätes. Unter **ADLS Kanal x: Verbunden mit …** zeigt Ihnen LANmonitor nun an, wie auf einem Kanal eine Verbindung aufgebaut und welche Gegenstelle dabei gerufen wird.

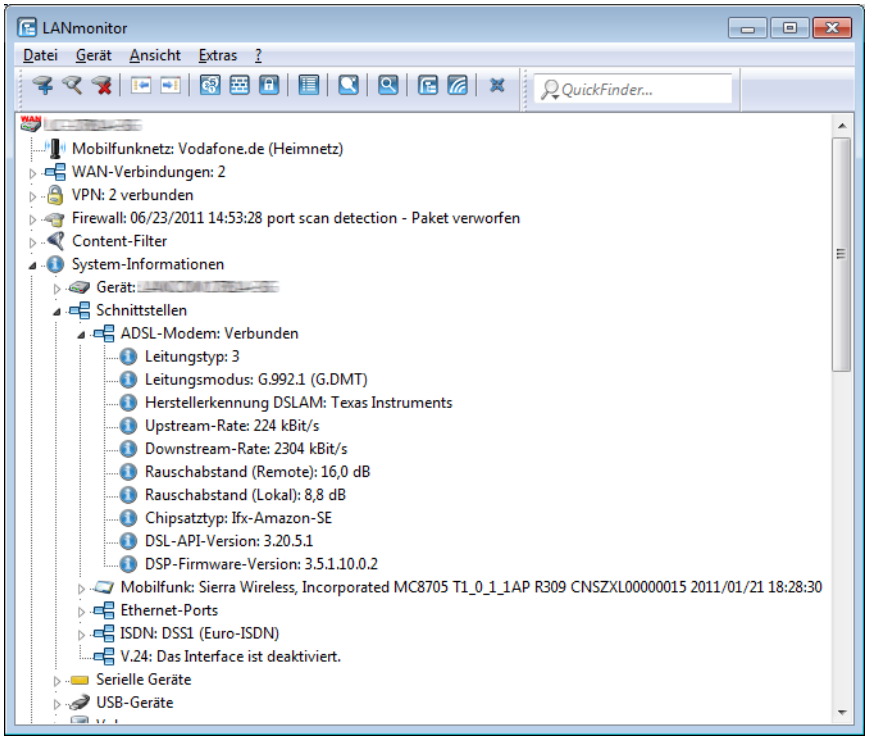
Sobald die Verbindung hergestellt ist, zeigt der Kommunikationskanal durch das Pluszeichen vor dem Eintrag an, dass zu diesem Kanal weitere Informationen vorliegen. Durch Klicken auf das Pluszeichen oder Doppelklick auf einen entsprechenden Eintrag öffnen Sie eine baumartige Struktur, in der Sie verschiedene Informationen ablesen können.



- In diesem Beispiel können Sie aus den Protokoll-Informationen zum PPP ablesen, welche IP-Adresse der Provider Ihrem Router für die Dauer der Verbindung zugewiesen hat und welche Adressen für DNS-Server übermittelt wurden.
- Unter den allgemeinen Informationen können Sie beobachten, mit welchen Übertragungsraten aktuell Daten mit dem Internet ausgetauscht werden.
- Durch einen Klick mit der rechten Maustaste auf den aktiven Kanal können Sie die Verbindung manuell trennen. Dazu benötigen Sie ggf. das Konfigurationspasswort.
- Wenn Sie ein Protokoll der LANmonitor-Ausgaben in Form einer Datei wünschen, starten Sie das Aktivitätsprotokoll (siehe auch *Geräteaktivitäten anzeigen* auf Seite 259).

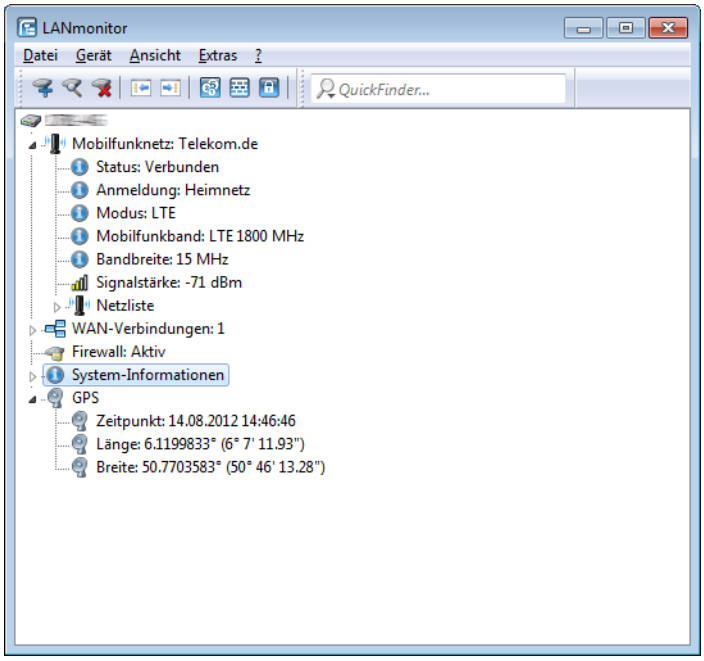
3.2.8.3 Aktuelles Protokoll für das ADSL-/VDSL-Interface anzeigen

LANmonitor zeigt für Geräte mit integriertem ADSL-/VDSL-Modem den aktuell verwendeten ADSL-Standard in den **System-Informationen** an. Wechseln Sie dazu in den Zweig **Schnittstellen** und wählen Sie **ADSL-/VDSL-Modem**.



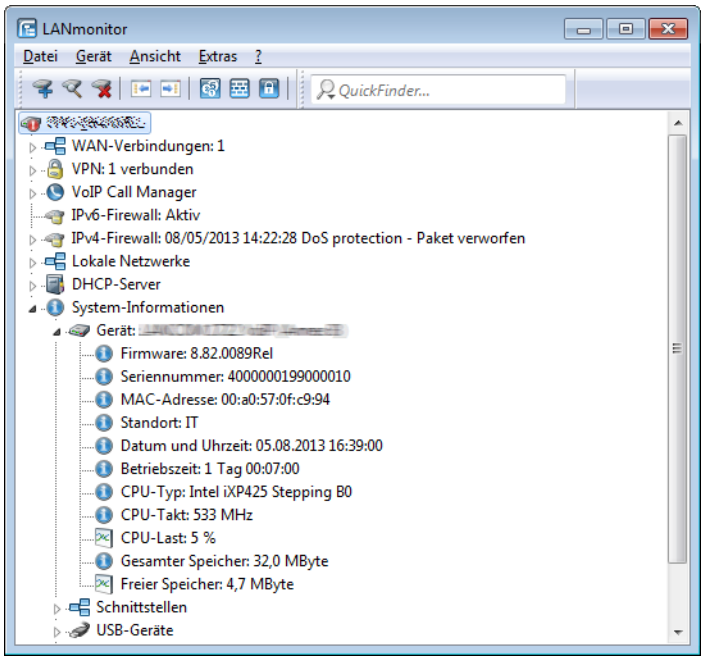
3.2.8.4 Anzeige der GPS-Zeit

LANmonitor bietet Ihnen ab LCOS-Version 8.80 die Möglichkeit, die aus dem GPS-Netz empfangene Zeit anzuzeigen. Öffnen Sie dazu im LANmonitor den Bereich **GPS** des Gerätes. Unter **Zeitpunkt** finden Sie die aktuelle GPS-Zeit.



3.2.8.5 Abfrage der CPU- und Speicherauslastung über SNMP

LANmonitor bietet Ihnen die Möglichkeit, die CPU- und Speicherauslastung eines Gerätes über SNMP abzufragen und anzuzeigen. Öffnen Sie dazu den Menübaum eines Gerätes, wechseln Sie in die **System-Informationen** und öffnen den Zweig **Gerät: ….**



3.2.8.6 Passwortschutz für SNMP-Lesezugriff

Der Lesezugriff auf ein Gerät über SNMP – z. B. über LANmonitor – kann über ein Passwort geschützt werden. Dabei werden die gleichen Benutzerdaten verwendet wie beim Zugriff auf LANconfig. Wenn der SNMP-Zugriff passwortgeschützt ist, können nur bei der Eingabe der entsprechenden Benutzerdaten Informationen über den Gerätezustand etc. über SNMP ausgelesen werden.

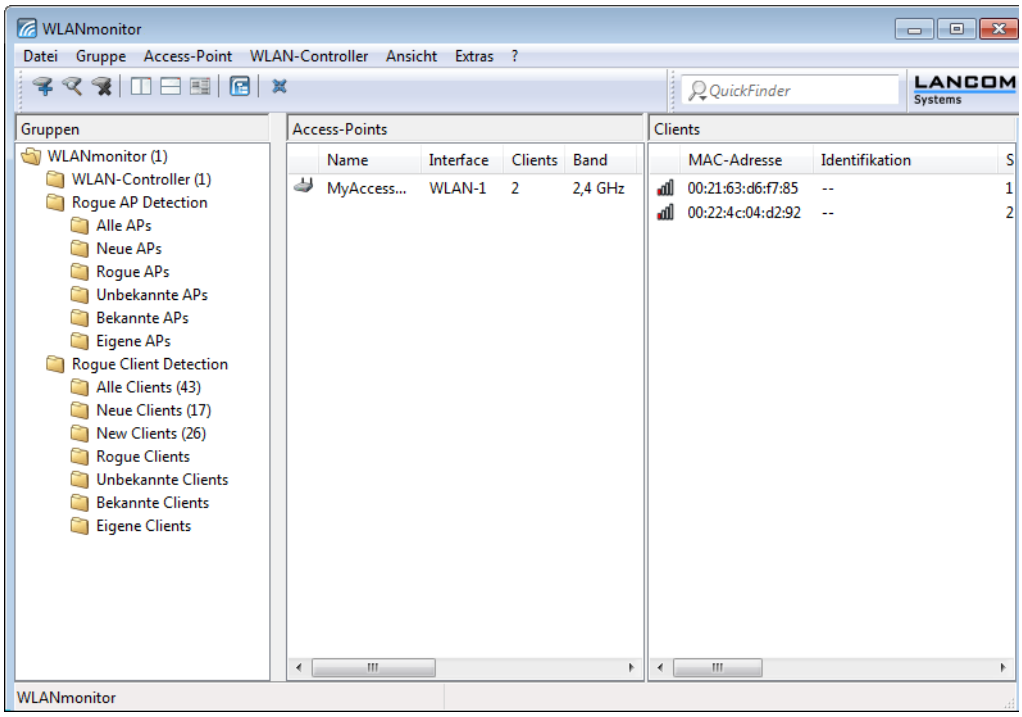
Die Benutzerinformationen können im LANmonitor für jedes Gerät getrennt eingetragen werden. Klicken Sie dazu mit der rechten Maustaste auf das gewünschte Gerät, wählen Sie im Kontextmenü den Eintrag **Optionen** und tragen Sie Ihre Benutzerdaten ein.

Die Zugriffsrechte im LANmonitor sind abhängig von den Rechten des Benutzers.

3.3 WLANmonitor – WLAN-Geräte überwachen

Der WLANmonitor ist ein separater Bestandteil von LANmonitor. Mit dem ihm überwachen Sie zentral den Status eines drahtlosen Netzwerkes (WLAN). Dabei können Sie sowohl Informationen über das gesamte Netzwerk als auch Detailinformationen zu einzelnen WLAN-Controllern, Access Points und eingeloggten Clients abrufen. Ebenso unterstützt Sie das Programm beim Aufspüren netzfremder Access Points (*Rogue AP Detection*).

Zudem bietet der WLANmonitor die Möglichkeit, Access Points zu Gruppen zusammenzufassen. Solche Gruppen können z. B. Etagen, Abteilungen oder Standorte umfassen. Dies erleichtert gerade bei großen WLAN-Infrastrukturen den Überblick über das gesamte Netzwerk.



Die Programmoberfläche von WLANmonitor ist in drei Spalten unterteilt:

In der linken Spalte (**Gruppen**) finden Sie eine Reihe vordefinierter die Gruppen-Ordner, in die WLANmonitor die verschiedenen Gerätetypen automatisch kategorisiert. Sie können diese Gruppen nach belieben umbenennen oder durch zusätzliche Gruppen erweitern.

In der mittleren Spalte (**Access-Points**) listet WLANmonitor die gefundenen Access Points auf. Zusätzlich erscheinen hier die wichtigsten Basisinformationen über die einzelnen Access Points:

- Name des Access Points
- Aktive physikalische Schnittstelle(n) (Interfaces)

  Geräte mit mehreren WLAN-Modulen tauchen mehrfach in der Liste auf. Jedes WLAN-Modul enthält dabei einen separaten Eintrag.
- Anzahl der auf ihm angemeldeten Clients
- Das verwendete Frequenzband
- Der verwendete Funkkanal
- Die vom Gerät ermittelte Sendeleistung
- Der vom Gerät ermittelte Rauschpegel
- Die derzeitige Auslastung des verwendeten Kanals (Kanallast)
- IP-Adresse des Access Point
- Der Aktivierungsstatus des *Background-Scans*

In der rechten Spalte (**Clients**) werden die auf dem ausgewählten Access Point eingeloggten Clients aufgelistet. Zu jedem Client werden folgende Informationen angezeigt:

- Verbindungsqualität in Form eines Balkendiagramms
- MAC-Adresse des WLAN-Clients
- Identifikation bzw. Name der eingeloggten Clients, sofern diese in der Access-Liste oder in einem RADIUS-Server eingetragen sind

- Signalstärke der Verbindung
- Name des Access-Points, auf dem der Client eingeloggt ist
- Bezeichnung des WLAN-Netzes (SSID)
- Für die Funkverbindung verwendetes Verschlüsselungsverfahren
- WPA-Version (WPA-1 oder WPA-2)
- Übertragungsrate beim Senden (TX-Rate)
- Übertragungsrate beim Empfangen (RX-Rate)
- Letzter Fehler, der im Zusammenhang mit dem Client aufgetreten ist
- IP-Adresse des WLAN-Clients

Sofern Sie keinen Access Point angewählt haben oder der betreffende Access Point über keinerlei Clients verfügt, zeigt Ihnen LANmonitor in der Client-Übersicht stattdessen sämtliche vorhandenen Clients an.

3.3.1 WLANmonitor starten

Der WLANmonitor ist Bestandteil des LANmonitor. Starten Sie den WLANmonitor aus dem LANmonitor über den Menüpunkt **Extras** > **WLANmonitor starten**; über die entsprechende Schaltfläche in der LANmonitor-Symbolleiste oder direkt über z. B. das Desktop-Symbol.

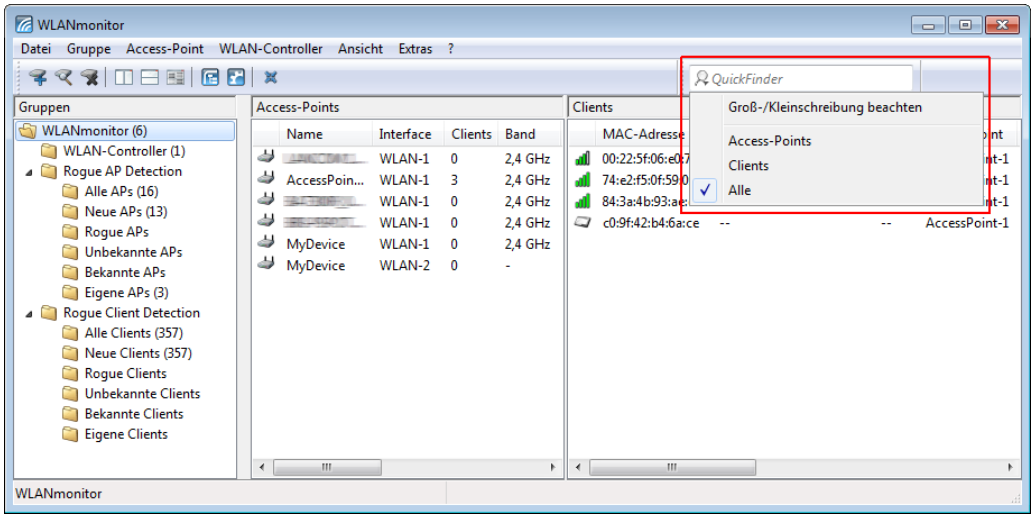
Alternativ kann der WLANmonitor von der Konsole aus mit folgendem Befehl gestartet werden:

```
[Installationspfad]lanmon -wlan
```

Wenn Sie LANconfig geöffnet haben, können Sie auch mit der rechten Maustaste auf ein WLAN-Gerät klicken und **WLAN Gerät überwachen** wählen; dann startet der WLANmonitor ebenfalls.

3.3.2 QuickFinder im WLANmonitor

Der WLANmonitor erfasst sowohl Access Points als auch WLAN-Clients. Mit einem Klick auf die Lupe am linken Rand des Suchfensters öffnen Sie ein Kontextmenü zur Auswahl des Suchumfangs. Wählen Sie je nach Anwendung nur die Access Points, nur die Clients oder alle Einträge aus.



3.3.3 Rogue-Detection-Funktion

WLANmonitor bietet Ihnen die Möglichkeit, sogenannte "Rogue Access Points (APs)" und "Rogue Clients" in Ihrem Netz aufzuspüren. Als "Rogue" bezeichnet man solche WLAN-Geräte, die unerlaubt versuchen, als Access Point oder Client Teilnehmer in einem WLAN zu werden.

- **Rogue Clients** sind Rechner mit WLAN-Adapter in Reichweite des eigenen WLANs, die sich bei einem der Access Points einzubuchen versuchen, um z. B. die Internetverbindung mit zu nutzen oder Zugang zu geschützten Bereichen des Netzwerks zu erhalten.
- **Rogue APs** sind Access Points, die z. B. von den Mitarbeitern einer Firma ohne Kenntnis und Erlaubnis der System-Administratoren an das Netzwerk angeschlossen werden und so über ungesicherte WLAN-Zugänge bewusst oder unbewusst Tür und Tor für potentielle Angreifer öffnen. Nicht ganz so gefährlich, aber zumindest störend, sind z B. Access Points in Reichweite des eigenen WLAN, die zu fremden Netzwerken gehören. Verwenden solche Geräte z. B. die gleiche SSID und den gleichen Kanal wie die eigenen APs (Default-Einstellungen), können die eigenen WLAN-Clients versuchen, sich beim fremden Netzwerk einzubuchen.

Da alle unbekannten Clients und Access Points in Reichweite des eigenen Netzwerks eine mögliche Bedrohung und Sicherleitslücke – oder zumindest aber eine Störung – darstellen, müssen diese Geräte erkannt werden, um ggf. weitere Maßnahmen zur Sicherung des eigenen Netzwerks einzuleiten. Die Informationen über die Clients in der Reichweite des eigenen Netzwerks werden automatisch in den internen Tabellen der Access Points gespeichert. Mit der Aktivierung des **Background Scans** werden auch die benachbarten Access Points erfasst und in der Scan-Tabelle gespeichert. Lesen Sie dazu auch das Kapitel *Background Scan für Access Points aktivieren* auf Seite 291.

Mit dem WLANmonitor lassen sich diese Informationen sehr komfortabel auswerten, indem das Programm solche Access Points und Clients in Kategorien wie z. B. 'Bekannt', 'Unbekannt' oder 'Rogue' einteilt.

3.3.3.1 Die Gruppe "Rogue AP Detection"

Für die Organisation der Rogue Access Points nutzt WLANmonitor die folgenden vordefinierten (Unter-)Gruppen:

- **Alle APs**: Enthält die Übersicht der APs aller gescannten WLANs und stellt damit die Obermenge aller nachfolgenden Gruppen dar. Die APs sind entsprechend ihrer Gruppenzugehörigkeit eingefärbt.
- **Neue APs**: Enthält neue unbekannte und unkonfigurierte WLANs. Die zugehörigen APs sind gelb eingefärbt.
- **Rogue APs**: Enthält WLANs, die als Rogue erkannt wurden und dringend zu beobachten sind. Die zugehörigen APs sind rot eingefärbt.
- **Unbekannte APs**: Enthält WLANs, bei denen weitere Untersuchungen notwendig sind. Die zugehörigen APs sind grau eingefärbt.
- **Bekannte APs**: Enthält WLANs, welche keine Gefahr darstellen. Die zugehörigen APs sind grau eingefärbt.
- **Eigene APs**: Enthält neue eigene WLANs von APs, die der WLANmonitor beobachtet. Die zugehörigen APs sind grün eingefärbt.



Wenn sich bei einem AP ein Parameter ändert (z. B. die Sicherheitseinstellung), dann wird er wieder als neu gefundener AP angezeigt.

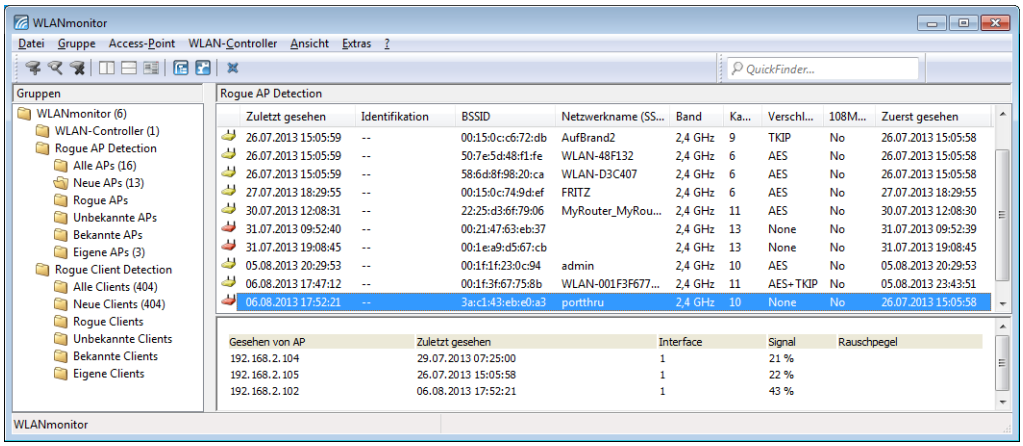
Innerhalb der einzelnen Gruppen zeigt WLANmonitor die folgenden Informationen zu den Rogue APs an:

- Zeitpunkt der ersten und letzten Erkennung
- Name des APs (Identifikation)
- MAC-Adresse des AP für dieses WLAN (BSSID)
- Bezeichnung des WLANss (SSID)
- Das verwendete Frequenzband
- Der verwendete Funkkanal
- Für die Funkverbindung verwendetes Verschlüsselungsverfahren
- Verwendung des 108 Mbps-Modus

Wenn Sie einen Listeneintrag anklicken, zeigt Ihnen WLANmonitor die folgenden Detailinformationen an:

- IP-Adressen der APs, die das betreffende WLAN gescannt haben
- Zeitpunkt der letzten Entdeckung bzw. des letzten Scans
- WLAN-Interface, auf dem der Scan durchgeführt wurde
- Signalstärke, mit welcher die APs das WLAN empfangen haben
- Rauschpegel

Sie haben die Möglichkeit, die gefundenen WLANs je nach Status in eine entsprechenden Gruppe verschieben. Innerhalb der einzelnen Gruppen legen Sie über das Kontextmenü (rechte Maustaste) eigene Gruppen an, mit Ausnahme der Gruppe **Alle APs**.



3.3.3.2 Die Gruppe "Rogue Client Detection"

Für die Organisation der Rogue Clients nutzt WLANmonitor die folgenden vordefinierten (Unter-)Gruppen:

- **Alle Clients**: Enthält die Übersicht aller gesehener Clients und stellt damit die Obermenge aller nachfolgenden Gruppen dar. Die Clients sind entsprechend ihrer Gruppenzugehörigkeit eingefärbt.
- **Neue Clients**: Enthält neue unbekannte Clients. Die zugehörigen Clients sind gelb eingefärbt.
- **Rogue Clients**: Enthält Clients, die als Rogue erkannt wurden und dringend zu beobachten sind. Die zugehörigen Clients sind rot eingefärbt.
- **Unbekannte Clients**: Enthält Clients, bei denen weitere Untersuchungen notwendig sind. Die zugehörigen Clients sind grau eingefärbt.
- **Bekannte Clients**: Enthält Clients, welche keine Gefahr darstellen. Die zugehörigen Clients sind grau eingefärbt.
- **Eigene Clients**: Enthält neue eigene Clients, die bei Access Points assoziiert sind, welche der WLANmonitor beobachtet. Die zugehörigen Clients sind grün eingefärbt.

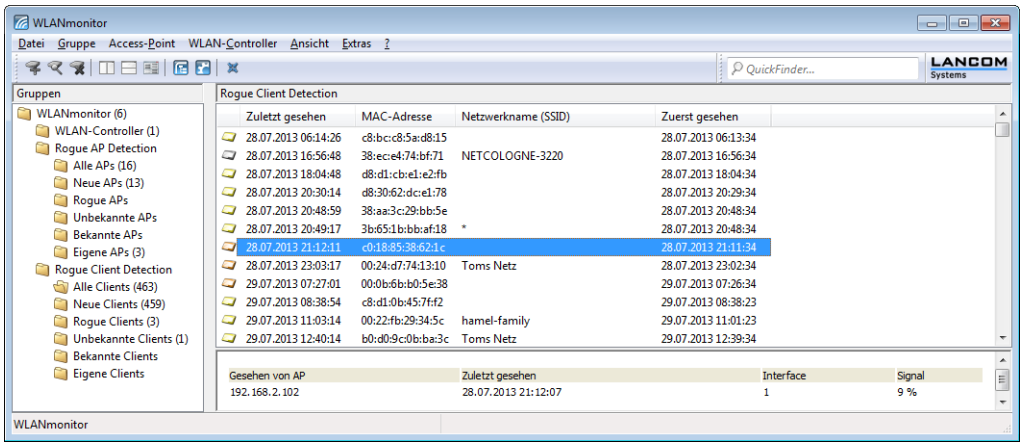
Innerhalb der einzelnen Gruppen zeigt WLANmonitor die folgenden Informationen zu den Rogue Clients an:

- Zeitpunkt der ersten und letzten Erkennung
- MAC-Adresse des Clients
- Bezeichnung des WLAN-Netzes (SSID)

Wenn Sie einen Listeneintrag anklicken, zeigt Ihnen WLANmonitor die folgenden Detailinformationen an:

- IP-Adressen der Access Points, die den betreffende Client gesehen haben
- Zeitpunkt der letzten Entdeckung
- WLAN-Interface, auf dem der Client entdeckt wurde
- Signalstärke, mit welcher die APs das WLAN-Netz empfangen haben

Sie können die gefundenen Clients je nach Status in eine entsprechenden Gruppe verschieben. Innerhalb der einzelnen Gruppen können Sie über das Kontextmenü (rechte Maustaste) eigene Gruppen anlegen, mit Ausnahme der Gruppe **Alle Clients**.



3.3.4 Die Menüstruktur im WLANmonitor

Über die Menüleiste verwalten Sie WLAN-Geräte und deren Konfigurationen, und passen sowohl das Aussehen als auch die Funktionsweise von WLANmonitor an.

3.3.4.1 Datei

Unter diesem Menüpunkt beenden Sie LANmonitor.

Beenden

Schließt und beendet WLANmonitor.

3.3.4.2 Gruppe

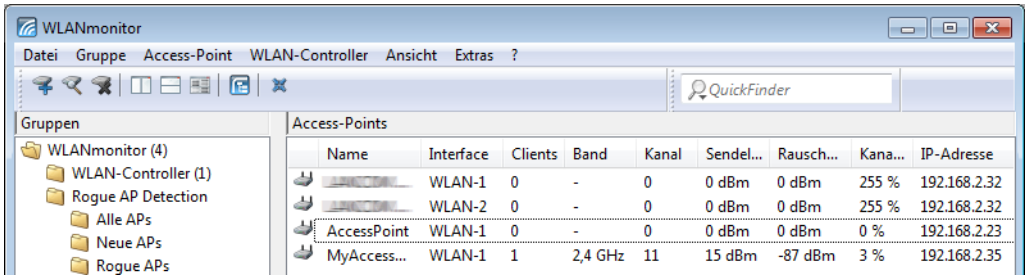
Die Bearbeitung von Gruppen umfasst die folgenden Funktionen:

- Gruppe hinzufügen
- Gruppe entfernen
- Gruppe umbenennen

WLANmonitor bietet Ihnen die Möglichkeit, alle verfügbaren Access Points unabhängig von ihren physikalischen Standorten anzuordnen. Das erleichtert den Überblick im Netzwerk und hilft bei der Lokalisierung von evtl. auftretenden Problemen. Zudem lassen sich WLAN-Informationen gruppenweise abrufen. Sie können Ihre Access Points z. B. nach Abteilungen, Standorten oder Ihrem Verwendungszweck (z. B. öffentlicher Hotspot) gruppieren.

In der linken Spalte des WLANmonitors (Gruppen-Baum) werden die Gruppen angezeigt. Von der obersten Gruppe 'WLANmonitor' ausgehend können Sie über den Menüpunkt **Datei** > **Gruppe** hinzufügen neue Untergruppen anlegen

und so eine Struktur aufbauen. Die bei der Suche gefundenen Access-Points befinden sich jeweils in der aktuell ausgewählten Gruppe im Gruppen-Baum.



Die bereits erkannten Access Points können Sie per Drag and Drop in die gewünschte Gruppe ziehen.

Um die Zuordnung von Access-Points und Clients zu erleichtern, können Sie ein Gerät mit der Maus markieren. Das jeweilige Pendant wird dann in den entsprechend verknüpften Listen ebenfalls markiert:

- Wenn in der Access-Point-Liste ein Access Point markiert wird, werden alle auf diesem Gerät eingeloggten Clients in der Client-Liste ebenfalls markiert.
- Wenn in der Client-Liste ein Client markiert wird, wird in der Access-Point-Liste der Access Point markiert, auf dem der gewählte Client eingeloggt ist.

Gruppe hinzufügen

Fügt eine Gruppe hinzu.

Gruppe entfernen

Entfernt eine Gruppe.

Gruppe umbenennen

Hier können Sie den Namen einer Gruppe ändern.

3.3.4.3 Access-Point

Unter diesem Menüpunkt verwalten Sie sämtliche Access Points.

Access-Point hinzufügen

Wählen Sie diesen Menüpunkt, um einen Access Point zur Liste hinzuzufügen, den WLANmonitor nicht automatisch erkannt hat. Die dazugehörigen Einstellungsmöglichkeiten sind mit denen von LANmonitor unter **Datei** > **Gerät hinzufügen** > **Allgemein** identisch (siehe *Allgemein* auf Seite 209).

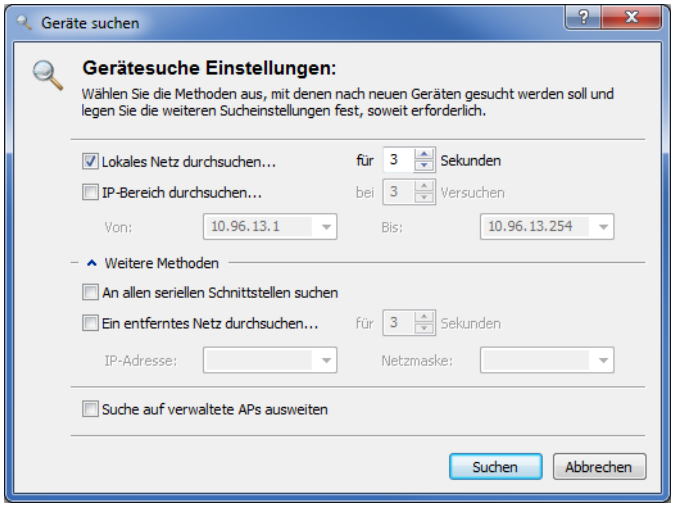
Wenn Sie Benutzernamen und Passwort dauerhaft speichern, erhält jeder Nutzer Zugang zu dem Gerät, der auch WLANmonitor ausführen darf.

Access Point entfernen

Entfernt den markierten Access Point aus der Liste.

Access Point suchen

Über diesen Menüpunkt starten Sie die automatische Suche nach verfügbaren Access Points im Netz.



Wählen Sie aus, wo nach Geräten gesucht werden soll:

- Im lokalen Netz
- In einem entfernten Netz

  Wenn Sie ein entferntes Netz durchsuchen wollen, müssen Sie die Adresse des Netzwerkes und die zugehörige Netzmaske angeben.

- Sie können die Suche bei Bedarf auch auf verwaltete Access Points (APs) ausweiten.

Klicken Sie auf **Suchen**, um die Suche zu starten. Die gefundenen Geräte werden automatisch der Liste hinzugefügt.

Wenn ein Gerät gefunden wird, das bereits in der Liste vorhanden ist, wird es nicht ein zweites Mal der Liste hinzugefügt. Daher kann es sein, dass weniger Geräte neu hinzukommen, als während des Suchvorgangs gemeldet werden.

Alle Access Points aktualisieren

Aktualisiert die Liste aller Access Points.

Aktualisieren

Aktualisiert die Anzeige des markierten Access Points.

Eigenschaften

Hier können Sie sich die Eigenschaften des ausgewählten Access Points anzeigen lassen. Die dazugehörigen Einstellungsmöglichkeiten sind mit denen von LANmonitor unter **Datei** > **Gerät hinzufügen** > **Allgemein** identisch (siehe *Allgemein* auf Seite 209). Zudem erhalten Sie hier Informationen zum Gerät und zum Hersteller.

Wenn Sie Benutzernamen und Passwort dauerhaft speichern, erhält jeder Nutzer Zugang zu dem Gerät, der auch WLANmonitor ausführen darf.

3.3.4.4 WLAN-Controller

Unter diesem Menüpunkt verwalten Sie die WLAN-Controller Ihres Netzes.

WLAN-Controller hinzufügen

Klicken Sie unter **Gruppen** auf den Ordner **WLAN-Controller** und wählen Sie dann in der Menüleiste den Menüpunkt **WLAN-Controller hinzufügen**, um einen WLAN-Controller zur Liste hinzuzufügen, den WLANmonitor nicht automatisch erkannt hat. Die dazugehörigen Einstellungsmöglichkeiten sind mit denen von LANmonitor unter **Datei** > **Gerät hinzufügen** > **Allgemein** identisch (siehe *Allgemein* auf Seite 209).

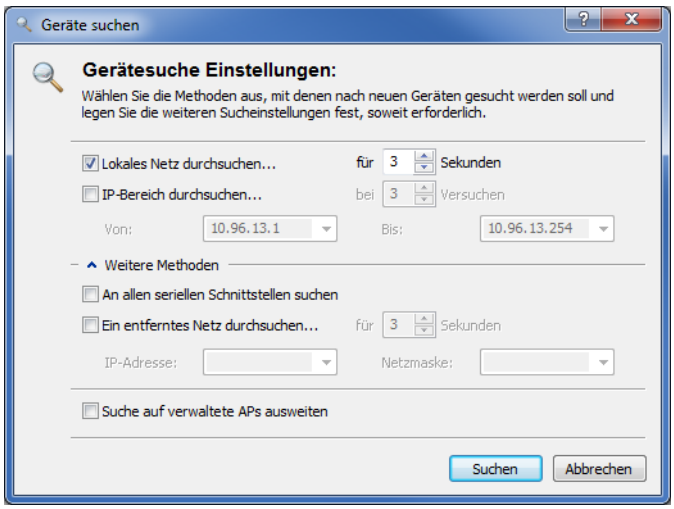
Wenn Sie Benutzernamen und Passwort dauerhaft speichern, erhält jeder Nutzer Zugang zu dem Gerät, der auch WLANmonitor ausführen darf.

WLAN-Controller entfernen

Entfernt den markierten WLAN-Controller.

WLAN-Controller suchen

Über diesen Menüpunkt starten Sie die automatische Suche nach verfügbaren WLAN-Controllern im Netz.



Wählen Sie aus, wo nach Geräten gesucht werden soll:

- Im lokalen Netz
- In einem entfernten Netz

  Wenn Sie ein entferntes Netz durchsuchen wollen, müssen Sie die Adresse des Netzwerkes und die zugehörige Netzmaske angeben.

- Sie können die Suche bei Bedarf auch auf verwaltete Access Points (APs) ausweiten.

Klicken Sie auf **Suchen**, um die Suche zu starten. Die gefundenen Geräte werden automatisch der Liste hinzugefügt.

Wenn ein Gerät gefunden wird, das bereits in der Liste vorhanden ist, wird es nicht ein zweites Mal der Liste hinzugefügt. Daher kann es sein, dass weniger Geräte neu hinzukommen, als während des Suchvorgangs gemeldet werden.

Alle WLAN-Controller aktualisieren

Aktualisiert die Liste aller WLAN-Controller.

Aktualisieren

Aktualisiert die Anzeige des markierten WLAN-Controllers.

Eigenschaften

Hier können Sie sich die Eigenschaften des ausgewählten WLAN-Controllers anzeigen lassen. Die dazugehörigen Einstellungsmöglichkeiten sind mit denen von LANmonitor unter **Datei** > **Gerät hinzufügen** > **Allgemein** identisch (siehe *Allgemein* auf Seite 209). Zudem erhalten Sie hier Informationen zum Gerät und zum Hersteller.

Wenn Sie Benutzernamen und Passwort dauerhaft speichern, erhält jeder Nutzer Zugang zu dem Gerät, der auch WLANmonitor ausführen darf.

3.3.4.5 Ansicht

Unter diesem Menüpunkt passen Sie das Verhalten der WLANmonitor-Bedienoberfläche an.

Symbol im Systray anzeigen

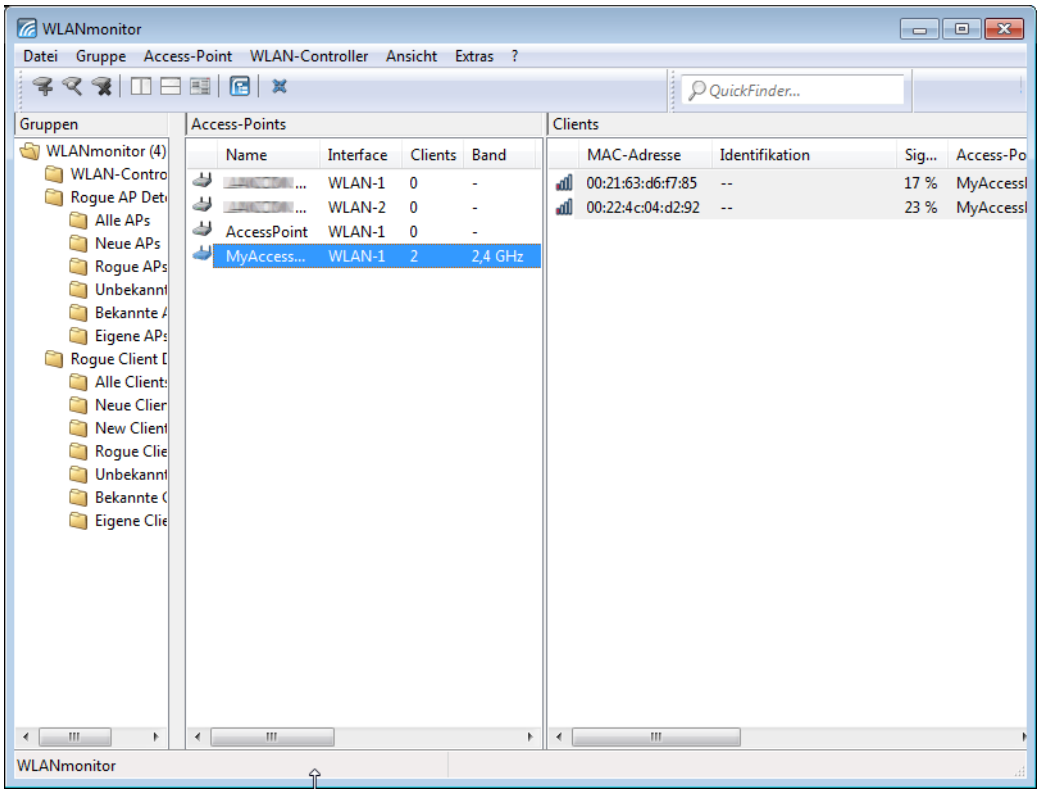
Zeigt das Symbol im Systray an.

WLANmonitor in den Systray minimieren

Wenn Sie diese Einstellung aktivieren, wird WLANmonitor beim Minimieren im Systray anstelle der Taskleiste abgelegt.

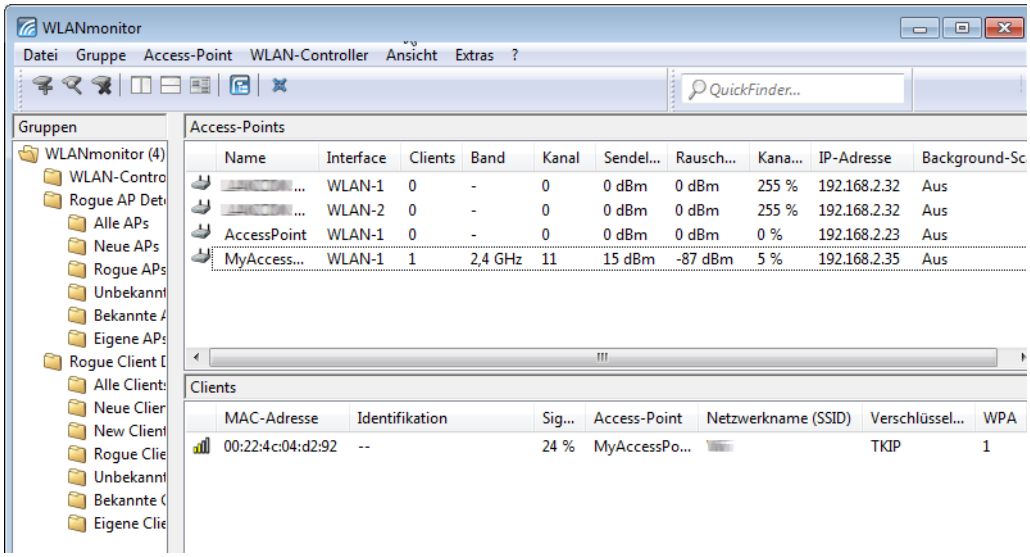
Fenster vertikal ausrichten

Richtet das Fenster vertikal aus, d. h. die Listen für Access Points und Clients werden nebeneinander dargestellt.



Fenster horizontal ausrichten

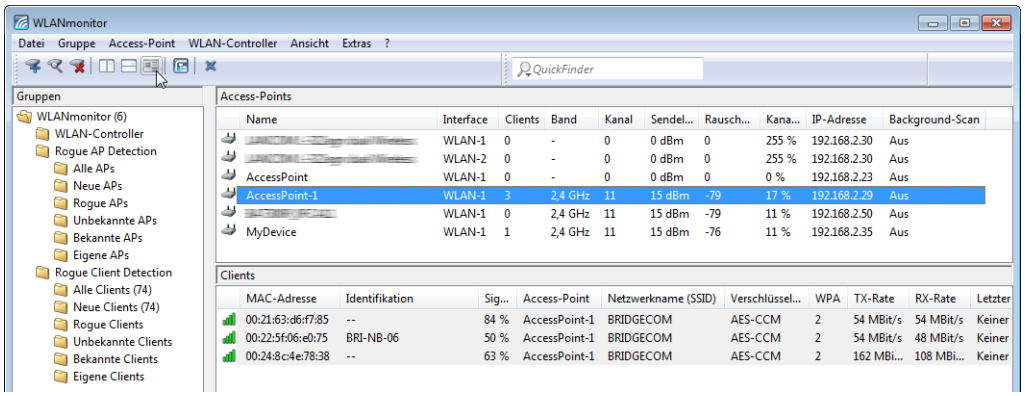
Richtet das Fenster horizontal aus, d. h. die Listen für Access Points und Clients werden untereinander dargestellt.



Zeilen markieren/ filtern

Mit dieser Option filtern Sie die Liste der angezeigten Access Points oder Clients.

- Markieren Sie eine Access Point und rufen Sie die Option **Ansicht** > **Zeilen markieren/Filtern** auf. Die Liste der Clients zeigt dann nur noch die Clients, die beim gewählten Access Point angemeldet sind.
- Markieren Sie eine Client und rufen Sie die Option **Ansicht** > **Zeilen markieren/Filtern** auf. Die Liste der Access Points zeigt dann nur noch den Access Point, bei dem der gewählte Client angemeldet ist.



Symbolleiste

Blendet die Symbolleiste aus bzw. ein. Lesen Sie hierzu auch *Die Symbolleiste im LANmonitor* auf Seite 271.

Statusleiste

Blendet die Statusleiste aus bzw. ein.

3.3.4.6 Extras

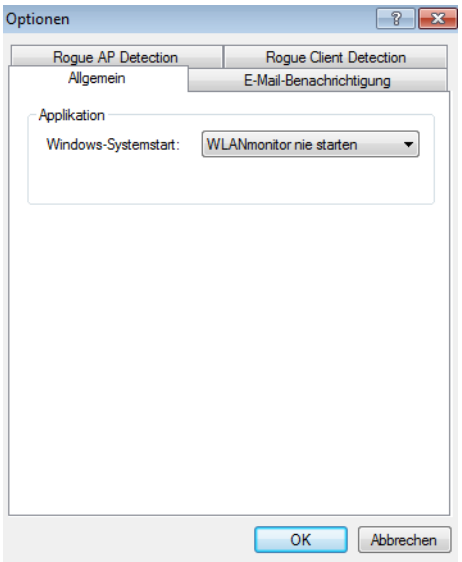
Unter diesem Menüpunkt starten Sie weitere Bestandteile der LANtools und konfigurieren z. B. das Verhalten von WLANmonitor bei Entdecken unbekannter oder unkonfigurierter Access Points.

Optionen

Unter diesem Menüpunkt nehmen Sie die programmbezogenen Einstellungen für WLANmonitor vor.

Allgemein

In diesem Dialog nehmen Sie die allgemeinen Einstellungen zum Programm vor.



Windows-Systemstart

WLANmonitor kann beim Start des Betriebssystems automatisch geladen werden. Folgende **Windows-Systemstart**-Arten stehen Ihnen zur Verfügung:

- **WLANmonitor nie starten**

  Die Anwendung startet nicht automatisch mit dem Betriebssystem, sondern muss manuell gestartet werden.

- **WLANmonitor immer starten**

  Die Anwendung startet immer automatisch nach dem erfolgreichen Start des Betriebssystems.

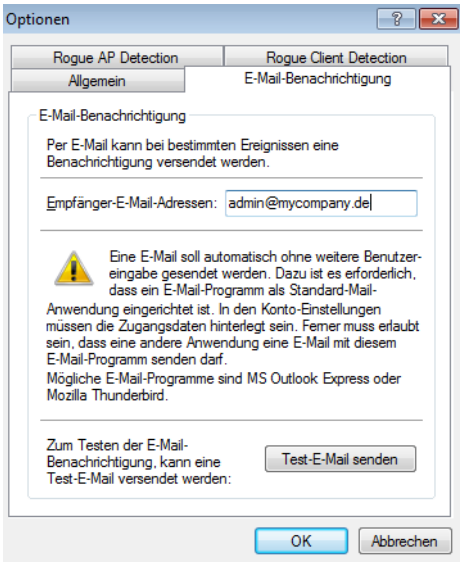
- **WLANmonitor wie zuvor starten**

  Die Anwendung startet in dem Zustand, in dem Sie sich beim Herunterfahren des Betriebssystems befand. War die Anwendung aktiv, wird sie wieder gestartet; war sie nicht aktiv, wird sie auch nicht automatisch gestartet.

Beim Wechsel auf eine Einstellung, die ein automatisches Starten der Anwendung ermöglicht, wird ein Eintrag in der Registry des Betriebssystems vorgenommen. Firewall-Applikationen auf dem Rechner oder die Betriebssysteme selbst können diesen Eintrag ggf. als Angriff deuten und eine Warnung ausgeben bzw. den Eintrag verhindern. Um das gewünschte Startverhalten zu ermöglichen, ignorieren Sie diese Warnungen bzw. lassen Sie die durchzuführenden Aktionen zu.

E-Mail-Benachrichtigung

In diesem Dialog nehmen Sie Einstellungen zur Alarmierungsfunktion im WLANmonitor vor.



Der WLANmonitor kann den Administrator automatisch per E-Mail informieren, wenn ein unbekannter oder unkonfigurierter Access Point entdeckt wird. Aktivieren Sie diese Option, wenn der WLANmonitor unbekannte oder unkonfigurierte Access Points per E-Mail melden soll.

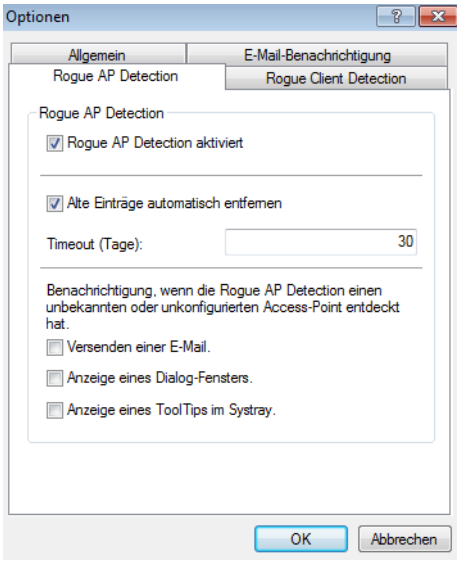
- **Empfänger-E-Mail-Adressen**: Geben Sie hier die E-Mail-Adresse(n) des Administrators an, der über die Rogue AP Detection informiert werden soll. Mehrere E-Mail-Adressen werden durch Kommata getrennt.

Für die Alarmierung per E-Mail muss auf dem Rechner, auf dem der WLANmonitor läuft, ein Mail-Client (z. B. MS Outlook Express oder Mozilla Thunderbird) als Standard-Mail-Client eingerichtet sein, der den automatischen Mail-Versand erlaubt.

- **Test-E-Mail senden**: Manche Mail-Clients erfordern vor dem Versand durch Dritt-Anwendungen eine Bestätigung durch den Benutzer. Testen Sie die Alarmierungsfunktion mit dieser Schaltfläche.

Rogue AP Detection

In diesem Dialog nehmen Sie Einstellungen zur "Rogue AP Detection" vor. Weitere Informationen zu dieser Funktion finden Sie im Kapitel *Rogue-Detection-Funktion* auf Seite 278.



Der Dialog bietet Ihnen folgende Einstellungsmöglichkeiten:

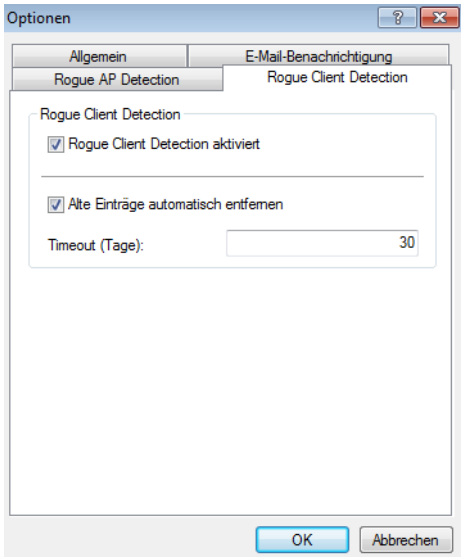
- **Rogue AP Detection aktiviert**: Aktiviert die automatische Suche nach Rogue Access Points.
- **Alte Einträge automatisch entfernen**: Wenn aktiviert, entfernt WLANmonitor automatisch Einträge zu Access Points aus den Gruppen, deren Sichtung länger zurückliegt als die unter **Timeout** angegebenen Tage.

Zudem haben Sie die Möglichkeit, festzulegen, auf welche Art und Weise WLANmonitor Sie bei Entdecken eines unbekannten oder unkonfigurierten Access Points benachrichtigt.

- **Versenden einer E-Mail**: Versendet eine Mitteilung an die unter **E-Mail-Benachrichtigung** hinterlegte(n) Empfänger-Adresse(n).
- **Anzeige eines Dialog-Fensters**: Öffnet ein Popup-Fenster.
- **Anzeige eines ToolTips im Systray**: Zeigt einen ToolTip im Systray an.

Rogue Client Detection

In diesem Dialog nehmen Sie Einstellungen zur "Rogue Client Detection" vor. Weitere Informationen zu dieser Funktion finden Sie im Kapitel *Rogue-Detection-Funktion* auf Seite 278.



Der Dialog bietet Ihnen folgende Einstellungsmöglichkeiten:

- **Rogue Client Detection aktiviert**: Aktiviert die automatische Suche nach Rogue Client.
- **Alte Einträge automatisch entfernen**: Wenn aktiviert, entfernt WLANmonitor automatisch Einträge zu Access Points aus den Gruppen, deren Sichtung länger zurückliegt als die unter **Timeout** angegebenen Tage.

LANmonitor starten

Startet LANmonitor. Mehr Informationen dazu erhalten Sie im Kapitel *LANmonitor – Geräte im LAN überwachen* auf Seite 250.

LANconfig starten

Startet LANconfig. Mehr Informationen dazu erhalten Sie im Kapitel *LANconfig – Geräte konfigurieren* auf Seite 174.

3.3.4.7 Hilfe

Unter diesem Menüpunkt finden Sie weitere Hilfe zum Programm und lassen sich Informationen zur Software anzeigen.

Hilfethemen

Über diesen Menüpunkt gelangen Sie zu den Hilfethemen. Alternativ können Sie auch F1 drücken.

Info

Unter diesem Menüpunkt werden Ihnen die Version und das Builddatum der Software angezeigt.

3.3.5 Die Symbolleiste im WLANmonitor



Die Symbolleiste im WLANmonitor beinhaltet die folgenden Funktionen:

- Gerät hinzufügen

- Geräte suchen
- Gerät entfernen
- Fenster vertikal ausrichten
- Fenster horizontal ausrichten
- Zeilen markieren/ filtern
- LANmonitor starten
- Fenster in den Systray minimieren
- QuickFinder

Unter **Ansicht** > **Symbolleiste** blenden Sie die Symbolleiste ein- oder aus.

3.3.6 Das Kontextmenü im WLANmonitor

Wenn Sie mit der rechten Maustaste auf eine Gerät im WLANmonitor klicken, dann öffnet sich das Kontextmenü.

Der Inhalt des Kontextmenüs hängt vom Typ des gewählten Gerätes ab: Im Falle eines markierten Access Points gleicht es dem Menü **Access Point**, im Falle eines markierten WLAN-Controllers dem Menü **WLAN-Controller**.

3.3.7 WLANmonitor Tastaturbefehle

Alt+F4	Beenden
Einfg	Gruppe hinzufügen
Entf	Gruppe entfernen
F2	Gruppe umbenennen
Einfg	Access Point hinzufügen
Entf	Access Point entfernen
F3	Access-Points suchen
F5	Alle Access-Points aktualisieren
Strg+F5	Aktualisieren
Space	Access Point > Optionen
Einfg	WLAN-Controller hinzufügen
Entf	WLAN-Controller entfernen
F3	WLAN-Controller suchen
Space	WLAN-Controller > Optionen
F7	Extras > Optionen
F1	Hilfethemen

3.3.8 Anwendungskonzepte für den WLANmonitor

In diesem Abschnitt finden Sie verschiedene Anwendungskonzepte für WLANmonitor.

3.3.8.1 Background Scan für Access Points aktivieren

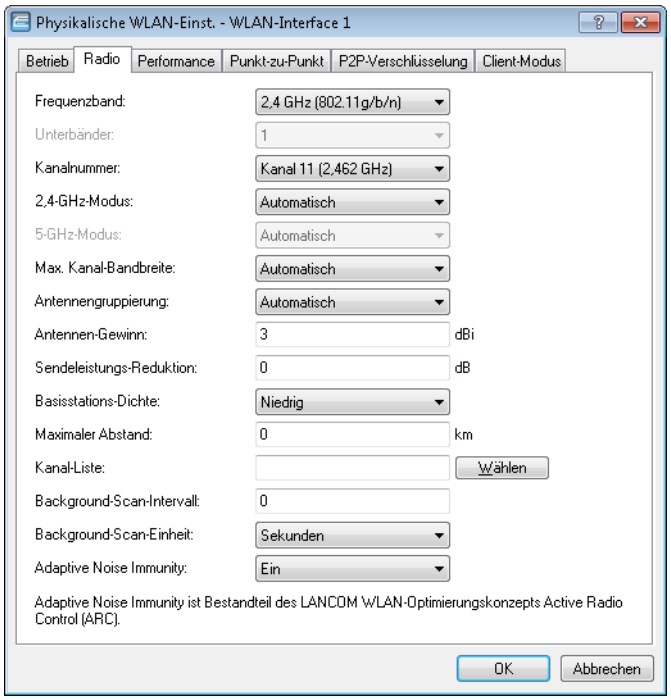
Zur Erkennung anderer Access Points in der eigenen Funkreichweite können Acess Points und Wireless Router die empfangenen Beacons (Management-Frames) aufzeichnen und in der Scan-Tabelle speichern. Da diese Aufzeichnung im Hintergrund neben der 'normalen' Funktätigkeit der Access Points abläuft, wird diese Funktion auch als "Background Scan" bezeichnet. Für Wireless-Router im Access Point-Modus wird die Background-Scan-Funktion üblicherweise zur

Rogue-AP-Detection eingesetzt. Ohne die Aktivierung des Background Scans ist z. B. die Rogue Detection im WLANmonitor auf die Erkennung von Rogue Clients beschränkt.

Zur Konfiguration des Background Scans definieren Sie eine Zeit, innerhalb der alle verfügbaren WLAN-Kanäle einmal auf die empfangenen Beacons hin gescannt werden. Das nachfolgende Tutorial beschreibt, wie Sie diese Zeit setzen.

1. Starten Sie LANconfig und öffnen Sie die manuelle Konfiguration für Ihr Gerät.
2. Öffnen Sie den Dialog **Wireless-LAN** > **Allgemein** und wählen Sie unter **Physikalische WLAN-Einst.** das WLAN-Interface, für das die Background Scanning aktivieren wollen.
3. Wechseln Sie im sich öffnenden Dialogfenster zum Reiter **Radio**.
4. Wählen Sie aus der Auswahlliste **Background-Scan-Einheit** eine Zeiteinheit aus und geben Sie im Eingabefeld **Background-Scan-Intervall** eine dazugehörige Dauer ein.

   Das Scan-Intervall sollte der Zeitspanne entsprechen, innerhalb derer unbefugte Access Points erkannt werden sollen, z. B. `3600 Sekunden`. Der kleinste sinnvolle Wert sowohl im 2,4-GHz- als auch 5-GHz-Band beträgt `260 Sekunden`. Dieser Wert führt bei möglichen 13 Kanälen dazu, dass alle 20 Sekunden ein weiterer Kanal gescannt wird (Intervall / Anzahl Kanäle).



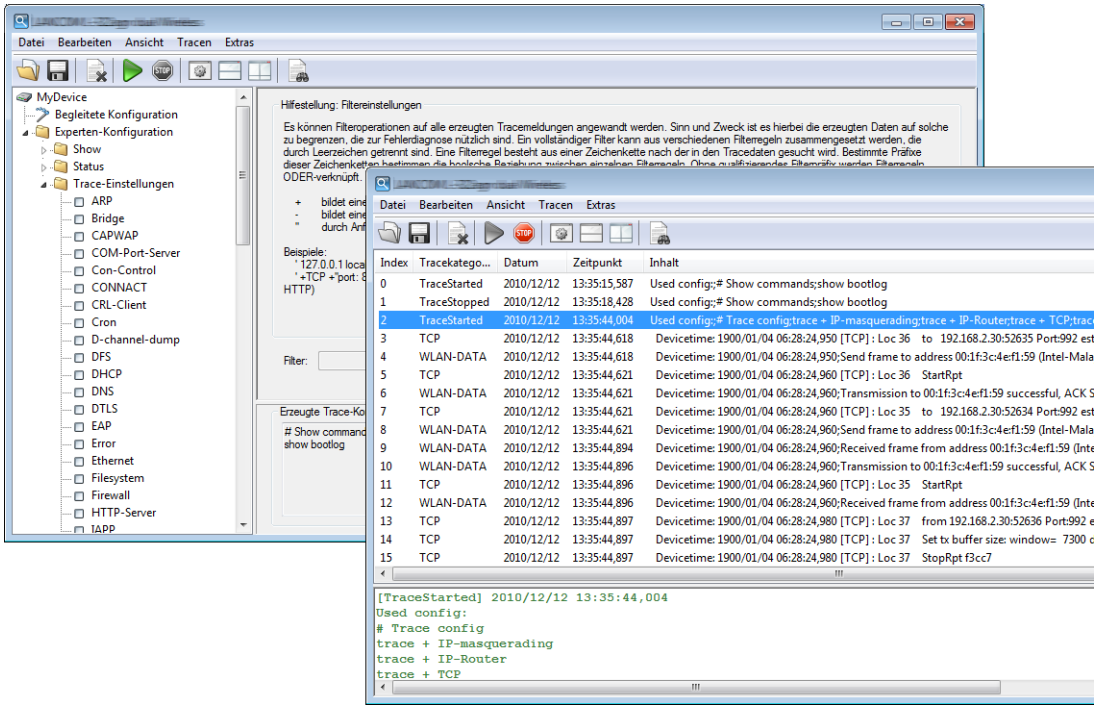
5. Schließen Sie alle Dialoge und laden Sie die Konfiguration auf Ihr Gerät zurück.

Fertig! Fortan sucht Ihr WLAN-Gerät innerhalb des angegebenen Scan-Intervalls zyklisch die aktuell ungenutzen Frequenzen des aktiven Bandes nach erreichbaren Access Points ab.

3.4 LANtracer – Tracen mit LANconfig und LANmonitor

Mit der Trace-Funktion in LANconfig und LANmonitor können Sie über die normalen Trace-Funktionen hinaus, wie sie von der Konsolen-Oberfläche bekannt sind, weitere Funktionen nutzen, die eine Erstellung und Auswertung der Traces erleichtern. So lässt sich z. B. die aktuelle Trace-Konfiguration, mit der die benötigten Trace-Befehle aktiviert werden, in einer Konfigurationsdatei speichern. Ein erfahrener Service-Techniker kann eine solche Trace-Konfiguration vorbereiten und einem weniger erfahrenen Anwender zur Verfügung stellen, der damit die gewünschte Trace-Ausgabe eines Gerätes

erzeugt. Auch Trace-Ergebnisse lassen sich komfortabel in einer Datei speichern, um sie an den Techniker zur Auswertung zurückzugeben.



3.4.1 LANtracer starten

Die Ausgabe von Traces kann sehr komfortabel über LANconfig oder LANmonitor vorgenommen werden. Um das Trace-Fenster für ein Gerät zu öffnen, klicken Sie mit der rechten Maustaste auf den Eintrag des Gerätes und wählen im Kontext-Menü den Eintrag **Trace-Ausgabe erstellen**.

Zur Abfrage von Traces über LANconfig oder LANmonitor muss ein (bestenfalls SSL-verschlüsselter) Telnet-Zugriff auf das Gerät erlaubt sein. Beim Starten des Trace-Dialogs versuchen LANconfig oder LANmonitor, zunächst eine SSL-verschlüsselte Telnet-Verbindung zum Gerät aufzubauen. Falls das Gerät keine SSL-Verbindungen unterstützt, wechseln LANconfig oder LANmonitor automatisch auf unverschlüsseltes Telnet. Wenn der Konfigurationszugriff auf das Gerät passwortgeschützt ist, sind zudem die Zugangsdaten für einen Administrator mit Trace-Rechten erforderlich.

Um nachfolgende Analysen durch detaillierte Trace-Daten zu vereinfachen, können Sie den Assistenten für die **Begleitete Konfiguration** starten. Der Assistent führt Sie durch mehrere Dialoge, in denen Sie bequem Trace-Parameter zur Analyse bestimmter Probleme auswählen. Nach Abschluss der Eingaben aktiviert der Assistent automatische die entsprechende Trace-Konfiguration.

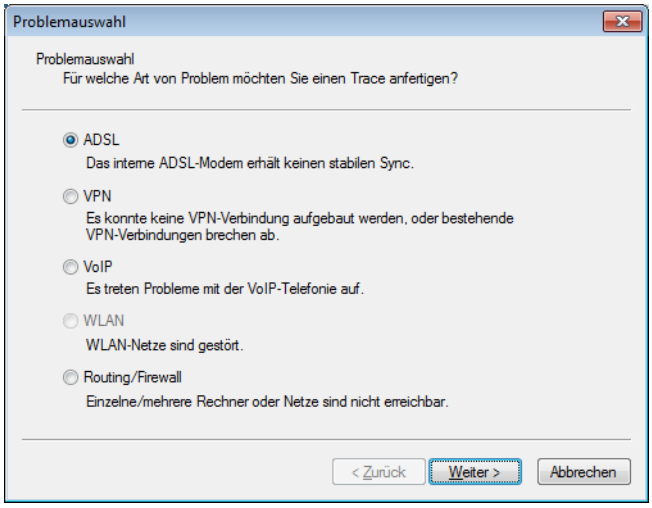
3.4.2 Arbeiten mit LANtracer

Das nachfolgende Kapitel beschreibt allgemein, wie Sie bestimmte Funktionalitäten von LANtracer für die Ausgabe und Sicherung von Traces nutzen.

3.4.2.1 Begleitete Konfiguration der Trace-Ausgaben

Als Alternative zur Experten-Konfiguration der Trace-Ausgaben bietet LANtracer Ihnen auch die Möglichkeit einer begleiteten (assistierten) Konfiguration. Dieser Assistent vereinfacht die Erstellung von Trace-Ausgaben, indem er Ihnen eine Auswahl möglicher Probleme anzeigt, für die Sie Diagnose-Informationen benötigen. Der Assistent setzt daraufhin für Sie die notwendigen Parameter bzw. Einstellungen in der Experten-Konfiguration.

Zum Starten des Assistenten klicken Sie im linken Fensterteil von LANtracer auf **Begleitete Konfiguration** > **Assistent starten** und navigieren weiter zur **Problemauswahl**.



3.4.2.2 Experten-Konfiguration der Trace-Ausgaben

Über die Einstellungen des Assistenten **Begleitete Konfiguration** hinaus können Sie – mit Hilfe der Experten-Konfiguration – die Traces und weitere Anzeigen genauer einstellen. Die Experten-Konfiguration unterteilt sich in drei Bereiche: ***Show***, ***Status*** und ***Trace-Einstellungen***.

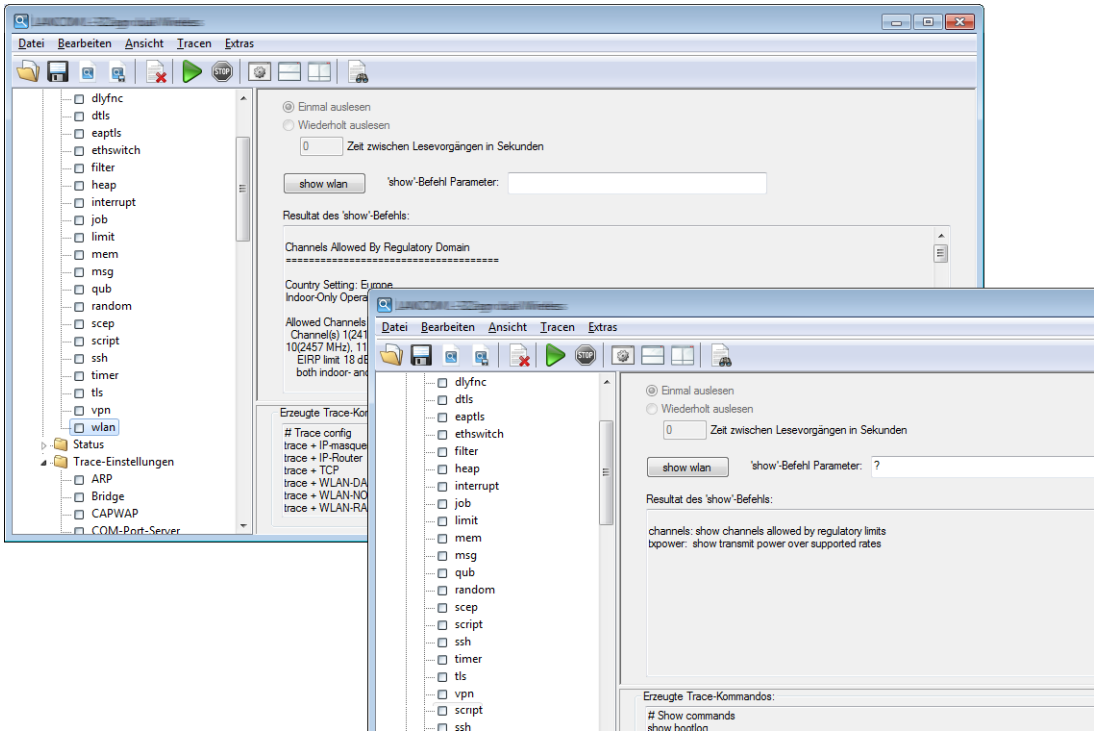
Show

Für jeden Gerätetyp können Sie bestimmte Informationen mit einem Show-Kommando aufrufen – üblicherweise werden die Show-Kommandos auf der Konsole angewendet. In der Experten-Konfiguration des Traces kann der Aufruf dieser Show-Kommandos sehr bequem über die grafische Windows-Oberfläche erfolgen.

- Klicken Sie im linken Bereich des Trace-Dialogs auf den Namen eines Show-Kommandos (z. B. **Show** > **wlan**) und dann den show-Button (z. B. **show wlan**), um die aktuelle Ausgabe des Show-Kommandos aufzurufen.
- Je nach gewähltem Eintrag können bzw. müssen noch ergänzende Parameter angegeben werden. Um eine Übersicht der möglichen Parameter zu erhalten, geben Sie in das Eingabefeld ein Fragezeichen ('?') ein und klicken den show-Button.

Um die Ausgabe eines Show-Kommandos in die Trace-Daten zu übernehmen, klicken Sie auf das entsprechende Kontrollkästchen vor dessen Namen. Für jedes aktivierte Show-Kommando ist separat einstellbar, ob es nur einmal beim Start des Traces oder in regelmäßigen Intervallen (in Sekunden) ausgeführt wird.

Die Einstellungen der Show-Kommandos werden zusammen mit den eigentlichen Trace-Einstellungen in der Trace-Konfiguration gespeichert.



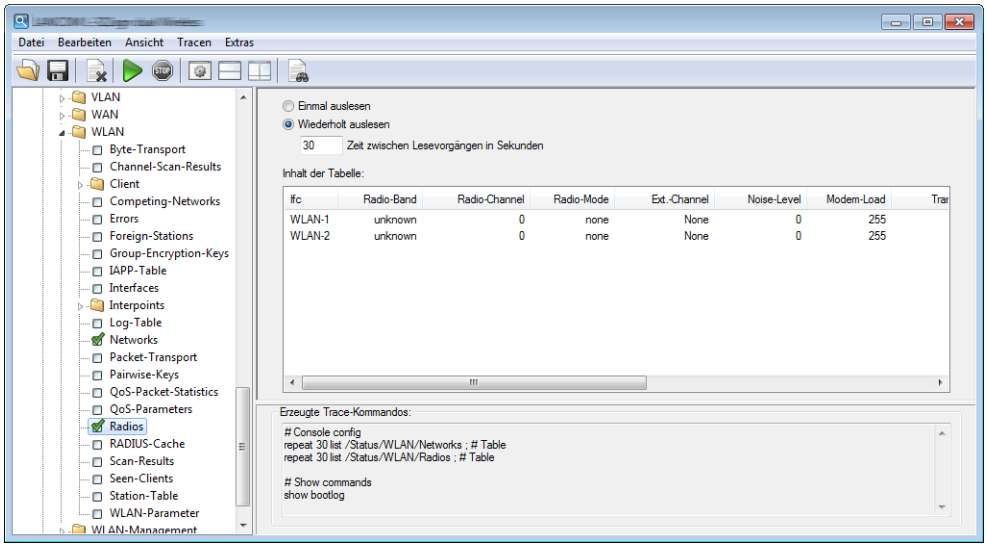
Status

Über die Konsole oder über WEBconfig können Sie umfangreiche Statusinformationen und Statistiken über ein Gerät abfragen. Alle verfügbaren Status-Informationen lassen sich aber auch über den Trace-Dialog einsehen.

› Klicken Sie im linken Bereich des Trace-Dialogs auf den Namen eines Status-Eintrags, um den aktuellen Inhalt der Tabelle bzw. des Wertes anzuzeigen.

Um die Ausgabe des Status-Eintrags in die Trace-Daten zu übernehmen, klicken Sie auf das entsprechende Kontrollkästchen vor dessen Namen. Für jeden aktivierten Status-Eintrag ist separat einstellbar, ob er nur einmal beim Start des Traces oder in regelmäßigen Intervallen (in Sekunden) ausgelesen wird.

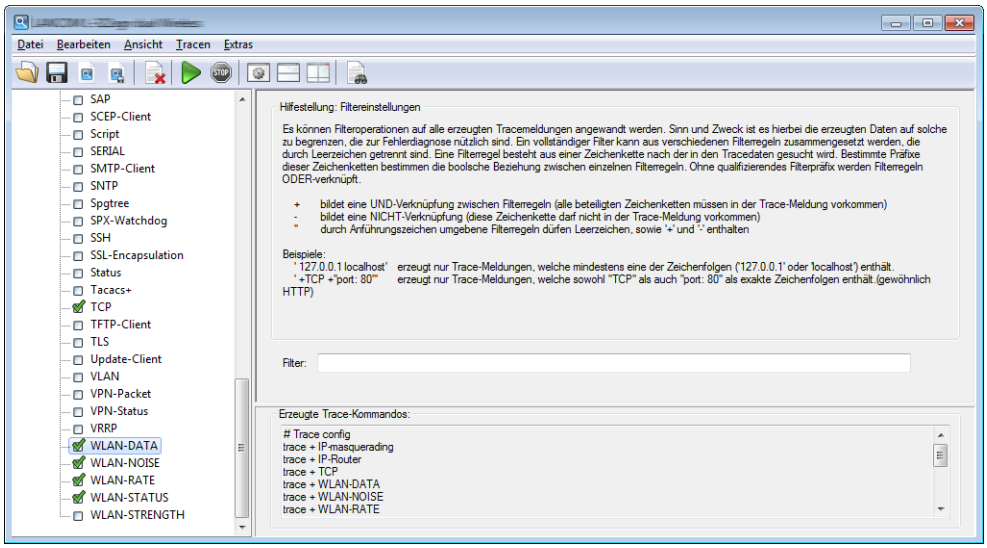
Die Einstellungen der Status-Informationen werden zusammen mit den eigentlichen Trace-Einstellungen in der Trace-Konfiguration gespeichert. Äquivalent dazu wird die Ausgabe der Status-Informationen zusammen mit den eigentlichen Trace-Daten gespeichert.



Trace-Einstellungen

Im Bereich der Trace-Einstellungen können Sie jene Traces aktivieren, die für das aktuelle Gerät ausgegeben werden sollen. Um die Trace-Kommandos in die Trace-Ergebnisse zu übernehmen, klicken Sie auf das entsprechende Kontrollkästchen vor dessen Namen.

Zu jedem Trace können Sie außerdem einen Filter eingeben. Um z. B. nur die IP-Adresse einer bestimmten Workstation anzuzeigen, geben Sie die entsprechende IP-Adresse als Filter des IP-Router-Traces ein. Um mehr über die Filterfunktion zu erfahren, lesen Sie das Kapitel *Trace-Ausgabe filtern* auf Seite 296.



3.4.2.3 Trace-Ausgabe filtern

Die Ausgabe von Traces an der Kommadozeile oder im Trace-Dialog der LANtools ist in vielen Fällen sehr umfangreich, weil der Trace in kurzer zeitlicher Abfolge Informationen aus dem Gerät empfängt. Um die Ausgabe der Traces übersichtlicher zu gestalten, können Sie geeignete Filter anwenden. Die Filter basieren auf einer Suchfunktion, welche die Trace-Ausgaben nach relevanten Informationen untersucht und nur die gewünschten Aspekte darstellt.

Im folgenden Beispiel aktiviert der Administrator einen einfachen IP-Router-Trace auf einem Gerät mit drei Internetanbindungen und verschickt Pings an verschiedene Ziele. Die ungefilterte Trace-Ausgabe zeigt alle Pakete, die der IP-Router des Gerätes verarbeitet:

```
root@MyDevice:/
> trace # ip-router
IP-Router ON

root@MyDevice:/

>[IP-Router] 2010/12/20 17:11:06,430
IP-Router Rx (LAN-1, INTRANET3, RtgTag: 3):
DstIP: 4.4.4.1, SrcIP: 192.168.3.100, Len: 84, DSCP/TOS: 0x00
Prot.: ICMP (1), echo request, id: 0x0015, seq: 0x1cde
Route: WAN Tx (INTERNET3)

[IP-Router] 2010/12/20 17:11:06,430
IP-Router Rx (LAN-1, INTRANET1, RtgTag: 1):
DstIP: 11.11.11.1, SrcIP: 192.168.1.100, Len: 84, DSCP/TOS: 0x00
Prot.: ICMP (1), echo request, id: 0x0016, seq: 0x1ccf
Route: WAN Tx (INTERNET1)

[IP-Router] 2010/12/20 17:11:06,430
IP-Router Rx (INTERNET1, RtgTag: 1):
DstIP: 192.168.1.100, SrcIP: 11.11.11.1, Len: 84, DSCP/TOS: 0x00
Prot.: ICMP (1), echo reply, id: 0x0016, seq: 0x1ccf
Route: LAN-1 Tx (INTRANET1):

[IP-Router] 2010/12/20 17:11:06,430
IP-Router Rx (INTERNET3, RtgTag: 3):
DstIP: 192.168.3.100, SrcIP: 4.4.4.1, Len: 84, DSCP/TOS: 0x00
Prot.: ICMP (1), echo reply, id: 0x0015, seq: 0x1cde
Route: LAN-1 Tx (INTRANET3):

[IP-Router] 2010/12/20 17:11:06,600
IP-Router Rx (LAN-1, INTRANET2, RtgTag: 2):
DstIP: 3.3.3.1, SrcIP: 192.168.2.100, Len: 84, DSCP/TOS: 0x00
Prot.: ICMP (1), echo request, id: 0x0014, seq: 0x1cea
Route: WAN Tx (INTERNET2)

[IP-Router] 2010/12/20 17:11:06,600
IP-Router Rx (INTERNET2, RtgTag: 2):
DstIP: 192.168.2.100, SrcIP: 3.3.3.1, Len: 84, DSCP/TOS: 0x00
Prot.: ICMP (1), echo reply, id: 0x0014, seq: 0x1cea
Route: LAN-1 Tx (INTRANET2):

[IP-Router] 2010/12/20 17:11:07,430
IP-Router Rx (LAN-1, INTRANET1, RtgTag: 1):
DstIP: 11.11.11.1, SrcIP: 192.168.1.100, Len: 84, DSCP/TOS: 0x00
Prot.: ICMP (1), echo request, id: 0x0016, seq: 0x1cd0
Route: WAN Tx (INTERNET1)

[IP-Router] 2010/12/20 17:11:07,430
IP-Router Rx (LAN-1, INTRANET3, RtgTag: 3):
DstIP: 4.4.4.1, SrcIP: 192.168.3.100, Len: 84, DSCP/TOS: 0x00
Prot.: ICMP (1), echo request, id: 0x0015, seq: 0x1cdf
Route: WAN Tx (INTERNET3)

[IP-Router] 2010/12/20 17:11:07,430
IP-Router Rx (INTERNET1, RtgTag: 1):
DstIP: 192.168.1.100, SrcIP: 11.11.11.1, Len: 84, DSCP/TOS: 0x00
Prot.: ICMP (1), echo reply, id: 0x0016, seq: 0x1cd0
Route: LAN-1 Tx (INTRANET1):

[IP-Router] 2010/12/20 17:11:07,430
IP-Router Rx (INTERNET3, RtgTag: 3):
DstIP: 192.168.3.100, SrcIP: 4.4.4.1, Len: 84, DSCP/TOS: 0x00
Prot.: ICMP (1), echo reply, id: 0x0015, seq: 0x1cdf
Route: LAN-1 Tx (INTRANET3):

[IP-Router] 2010/12/20 17:11:07,600
IP-Router Rx (LAN-1, INTRANET2, RtgTag: 2):
DstIP: 3.3.3.1, SrcIP: 192.168.2.100, Len: 84, DSCP/TOS: 0x00
Prot.: ICMP (1), echo request, id: 0x0014, seq: 0x1ceb
Route: WAN Tx (INTERNET2)

[IP-Router] 2010/12/20 17:11:07,600
IP-Router Rx (INTERNET2, RtgTag: 2):
```

```
DstIP: 192.168.2.100, SrcIP: 3.3.3.1, Len: 84, DSCP/TOS: 0x00
Prot.: ICMP (1), echo reply, id: 0x0014, seq: 0x1ceb
Route: LAN-1 Tx (INTRANET2):
```

Die Ausgabe von nur 2 Sekunden reicht schon aus, um eine recht große Menge an Daten zu erzeugen. Um die Ausgabe übersichtlicher zu gestalten, fügen Sie nach dem Trace-Kommando einen Filter an. Die Filter beginnen mit dem @-Zeichen und geben ein Suchkriterium an. In diesem Beispiel reduzieren Sie den Filter auf alle Ausgaben, in denen das Suchkriterium "Internet1" vorkommt, um nur die Pakete dieser Gegenstelle auszugeben.

Die Filter unterscheiden nicht zwischen Groß- und Kleinschreibung.

```
root@MyDevice:/
> trace # ip-router @ INTERNET1

IP-Router ON @ INTERNET1

[IP-Router] 2010/12/20 17:11:50,430
IP-Router Rx (LAN-1, INTRANET1, RtgTag: 1):
DstIP: 11.11.11.1, SrcIP: 192.168.1.100, Len: 84, DSCP/TOS: 0x00
Prot.: ICMP (1), echo request, id: 0x0016, seq: 0x1cfb
Route: WAN Tx (INTERNET1)

[IP-Router] 2010/12/20 17:11:50,430
IP-Router Rx (INTERNET1, RtgTag: 1):
DstIP: 192.168.1.100, SrcIP: 11.11.11.1, Len: 84, DSCP/TOS: 0x00
Prot.: ICMP (1), echo reply, id: 0x0016, seq: 0x1cfb
Route: LAN-1 Tx (INTRANET1):

[IP-Router] 2010/12/20 17:11:51,430
IP-Router Rx (LAN-1, INTRANET1, RtgTag: 1):
DstIP: 11.11.11.1, SrcIP: 192.168.1.100, Len: 84, DSCP/TOS: 0x00
Prot.: ICMP (1), echo request, id: 0x0016, seq: 0x1cfc
Route: WAN Tx (INTERNET1)

[IP-Router] 2010/12/20 17:11:51,430
IP-Router Rx (INTERNET1, RtgTag: 1):
DstIP: 192.168.1.100, SrcIP: 11.11.11.1, Len: 84, DSCP/TOS: 0x00
Prot.: ICMP (1), echo reply, id: 0x0016, seq: 0x1cfc
Route: LAN-1 Tx (INTRANET1):
```

Wieder beträgt der Zeitrahmen des Traces zwei Sekunden, die Menge an Daten wurde aber schon deutlich reduziert. Lediglich die Daten zur Gegenstelle "INTERNET1" werden angezeigt. Es können aber auch noch weitere Filterkriterien angegeben werden indem einfach ein Leerzeichen zwischen dem ersten und zweiten Kriterium gesetzt werden. Zusätzlich zum Leerzeichen können sowohl "+" als auch "-" als Operatoren verwendet werden. Hierbei gilt, bei einem "+" müssen beide Kriterien erfüllt sein, bei einem "-" darf das Kriterium nicht erfüllt sein und bei einem Leerzeichen muss eines der verknüpften Kriterien erfüllt sein. Die Möglichkeit Strings, die Operatoren enthalten auch als Filter zu nutzen wird durch Anführungszeichen umgesetzt.

Wenn Sie mehrere Suchbegriffe verwenden möchten, trennen Sie die einzelnen Begriffe durch die folgenden Operatoren:

- Leerzeichen: Ein Leerzeichen vor einem Suchbegriff stellt eine logische ODER-Verknüpfung dar. Die Trace-Ausgabe wird nur dann angezeigt, wenn sie eine der so markierten Zeichenketten enthält.
- +: Ein Pluszeichen vor einem Suchbegriff stellt eine logische UND-Verknüpfung dar. Die Trace-Ausgabe wird nur dann angezeigt, wenn sie alle der so markierten Zeichenketten enthält.
- -: Ein Minuszeichen vor einem Suchbegriff stellt eine logische NICHT-Verknüpfung dar. Die Trace-Ausgabe wird nur dann angezeigt, wenn sie keine der so markierten Zeichenketten enthält.

```
root@MyDevice:/
> trace # ip-router @ INTERNET1 -"echo request"

IP-Router ON @ INTERNET1 -"echo request"

[IP-Router] 2010/12/20 17:12:06,430
IP-Router Rx (INTERNET1, RtgTag: 1):
DstIP: 192.168.1.100, SrcIP: 11.11.11.1, Len: 84, DSCP/TOS: 0x00
Prot.: ICMP (1), echo reply, id: 0x0016, seq: 0x1d0b
Route: LAN-1 Tx (INTRANET1):

[IP-Router] 2010/12/20 17:12:07,430
IP-Router Rx (INTERNET1, RtgTag: 1):
DstIP: 192.168.1.100, SrcIP: 11.11.11.1, Len: 84, DSCP/TOS: 0x00
```

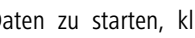
```
Prot.: ICMP (1), echo reply, id: 0x0016, seq: 0x1d0c
Route: LAN-1 Tx (INTRANET1):
```

Jetzt zeigt der Trace nur noch die Einträge an, welche die Gegenstelle 'INTERNET1' enthalten, die aber **nicht** die Zeichenkette 'echo request' enthalten. So reduzieren Sie die Anzeige auf die Antworten eines Pings, die von der entsprechenden Gegenstelle stammen.

Sie können zeitgleich mehrere Traces verwenden und nach unterschiedlichen Kriterien filtern. Im folgenden Beispiel läuft neben dem IP-Router Trace auch ein Ethernet Trace, um sich das zum Ping zugehörige Paket auf dem Ethernet anzuschauen.

```
root@MyDevice:/
> trace # ip-router @ INTERNET1 +"echo reply"
IP-Router ON @ INTERNET1 +"echo reply"

root@MyDevice:/
> trace # eth @ ICMP +"echo reply"
Ethernet ON @ icmp +"echo reply"

[IP-Router] 2010/12/21 14:17:21,000
IP-Router Rx (INTERNET1, RtgTag: 1):
DstIP: 192.168.1.100, SrcIP: 11.11.11.1, Len: 84, DSCP/TOS: 0x00
Prot.: ICMP (1), echo reply, id: 0x0002, seq: 0x2654
Route: LAN-1 Tx (INTRANET1):

[Ethernet] 2010/12/21 14:17:21,000
Sent 98 byte Ethernet packet via LAN-1:
HW Switch Port : ETH-1
-->IEEE 802.3 Header
Dest : 00:a0:57:12:a9:21 (LANCOM 12:a9:21)
Source : 00:a0:57:12:f7:81 (LANCOM 12:f7:81)
Type : IPv4
-->IPv4 Header
Version : 4
Header Length : 20
Type of service : (0x00) Precedence 0
Total length : 84
ID : 18080
Fragment : Offset 0
TTL : 59
Protocol : ICMP
Checksum : 24817 (OK)
Src Address : 11.11.11.1
Dest Address : 192.168.1.100
-->ICMP Header
Msg : echo reply
Checksum : 18796 (OK)
Body : 00 00 00 02 00 00 26 54 ......
 7e c9 6d 8c 00 00 00 00 ~.m.....
 00 01 02 03 04 05 06 07 ........
 08 09 0a 0b 0c 0d 0e 0f ........
 10 11 12 13 14 15 16 17 ........
 18 19 1a 1b 1c 1d 1e 1f ........
 20 21 22 23 24 25 26 27 !"#$%
```

3.4.2.4 Anzeige der Trace-Ergebnisse

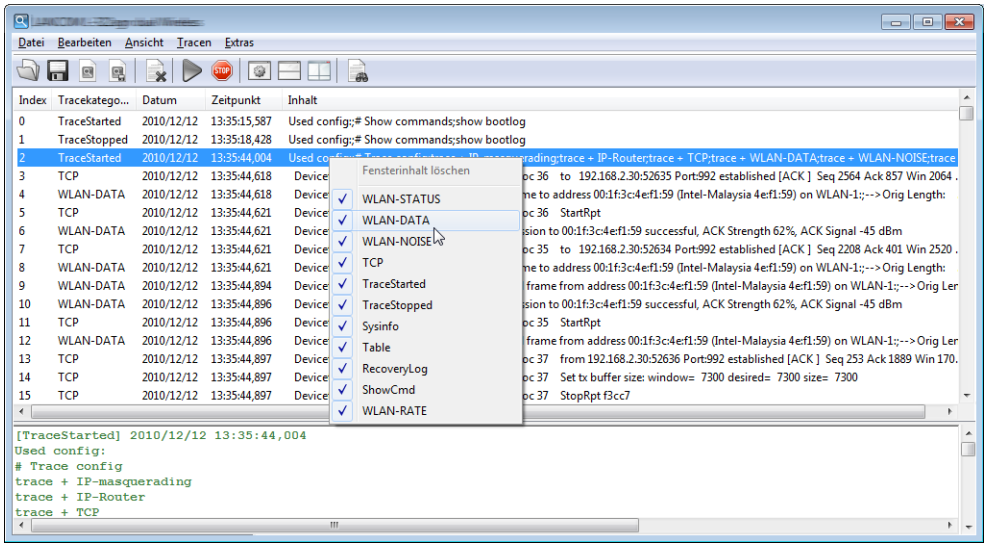
Um die Ausgabe der Trace-Daten zu starten, klicken Sie auf den Start-Button () und wechseln so von der Konfigurationsansicht in die Ergebnisansicht von LANtracer. In dieser Ansicht werden die laufenden Trace-Ausgaben angezeigt:

- Der obere Bereich listet die Ergebnisse für die ausgeführten Trace-Kommandos chronologisch in jeweils einer Zeile auf.
- Der untere Bereich stellt die Ergebnisse für das im oberen Bereich ausgewählte Trace-Kommando ausführlich dar. Hier sind alle aktiven Trace-, Status- und Show-Einträge mit den jeweiligen Filtern und Parametern aufgelistet. Die Ausgabe erfolgt mehrzeilig, da die Ergebnisse für ein einzelnes Trace-Kommando sehr umfangreich sein können.

Mit einem rechten Mausklick auf ein Trace-Ereignis öffnen Sie das Kontextmenü, über das Sie die einzelnen Trace-Kategorien ein- oder ausblenden können, um die angezeigten Ergebnisse grob zu filtern.

Die Trace-Daten werden erfasst, solange die Trace-Ausgabe aktiv ist. Um eine Überlastung des Arbeitsspeichers auf der Workstation mit LANconfig oder LANmonitor zu vermeiden, werden die Trace-Daten automatisch in eine

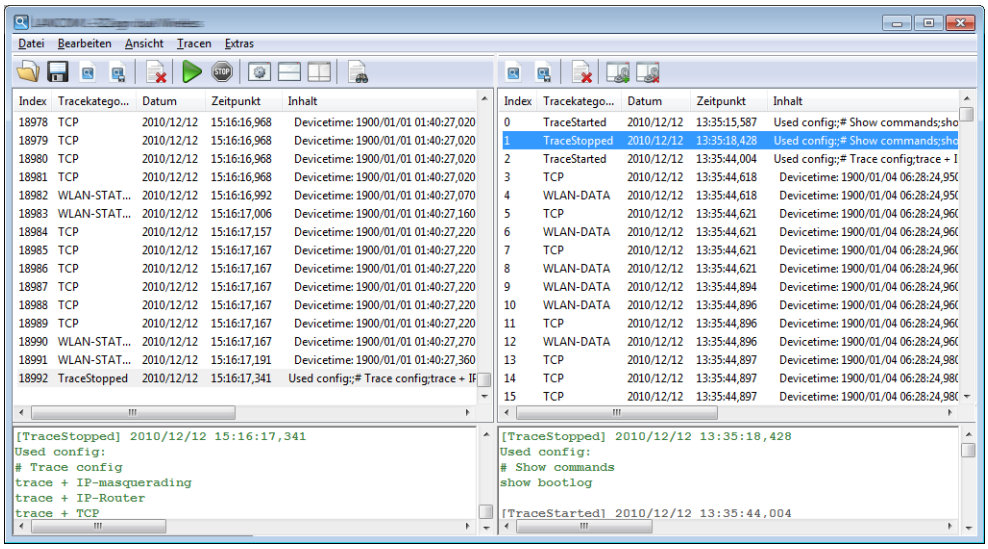
Backup-Datei gespeichert. Die zeitlichen Intervalle und die maximale Größe einer Sicherungsdatei stellen Sie im LANtracer unter **Extras** > **Sonstige Einstellungen** > **Traceeinstellungen** ein.



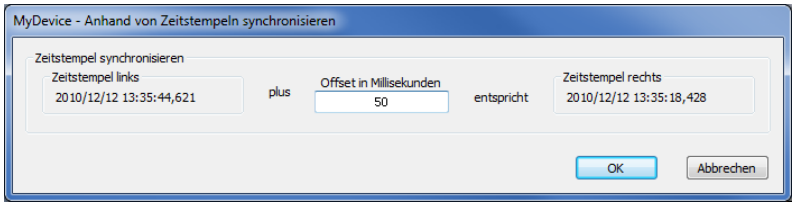
Trace-Daten vergleichen

Um die Ergebnisse eines Traces mit anderen (in einer Backup abgespeicherten) Tracedaten zu vergleichen, können Sie in der geteilten Trace-Ansicht zwei Traces nebeneinander darstellen.

1. Stoppen Sie dazu den aktuell laufenden Trace und wählen Sie im Menü **Ansicht** > **Trace-Erg. Doppelansicht**.
2. Laden Sie in den noch leeren Ansichtsbereich die Datei mit den aktuell oder zu einem früheren Zeitpunkt erfassten Trace-Daten.

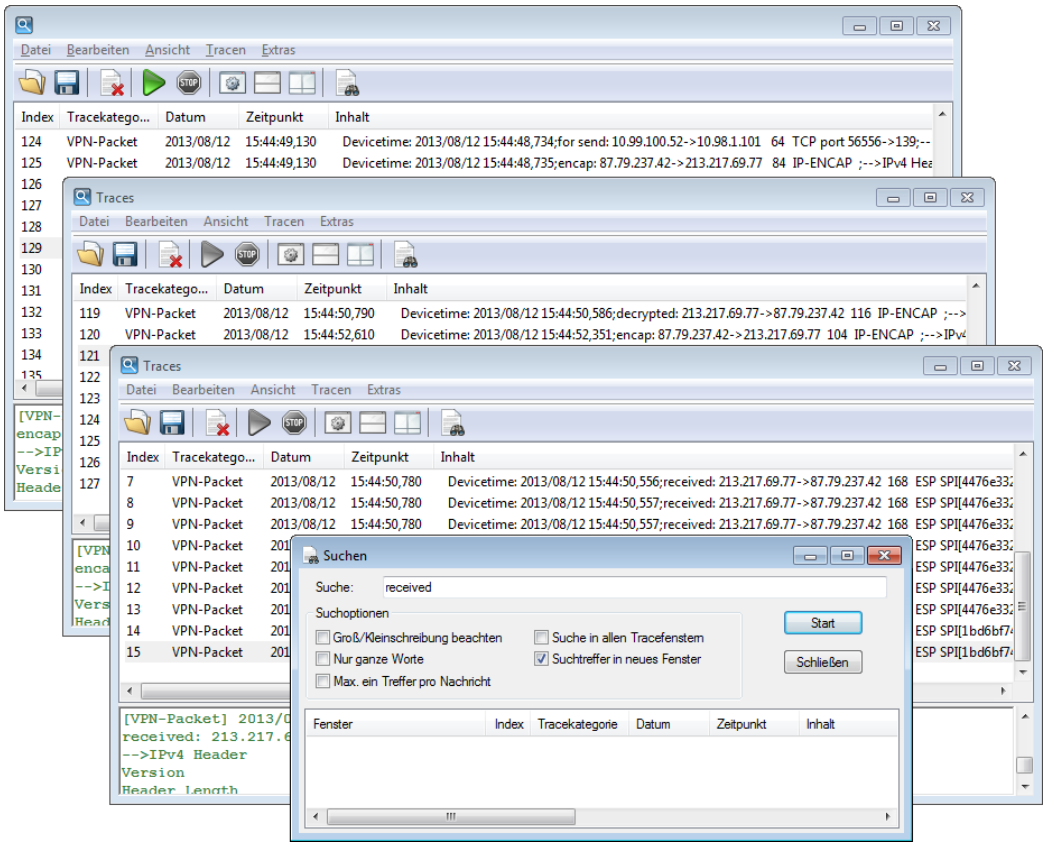


3. Starten Sie die Synchronisation der beiden Traces anhand des Zeitstempels mit der Schaltfläche . Geben Sie im folgenden Fenster einen geeigneten Wert für den Offset in Millisekunden ein und starten Sie die Synchronisation.



3.4.2.5 Mehrstufige Suche

Sie haben die Möglichkeit, durch intelligentes Verschachteln von Suchanfragen eine mehrstufige (kaskadierte) Suche innerhalb der Trace-Ergebnisse durchzuführen. Aktivieren Sie dazu *vor* dem Beginn der ersten Suche die Option **Suchtreffer in neues Fenster** und lassen Sie die Option für alle weiteren Suchanfragen aktiviert. Suchen Sie anschließend sukzessiv nach verschiedenen Schlüsselbegriffen im jeweils der zuletzt geöffneten Fester, um die Trefferliste immer weiter zu verfeinern.



Um eine Suchanfrage wieder zu verallgemeinern bzw. einen Suchschritt zurückzugehen, schließen Sie einfach die jeweils zuletzt geöffnete Ergebnisansicht und kehren so zur vorangehenden Ergebnisansicht zurück.

Mehr zu den Einstellungsmöglichkeiten im **Suchen**-Dialog finden Sie im Kapitel *Suchen* auf Seite 303.

3.4.2.6 Backup-Einstellungen für die Traces

Beim Starten eines Traces über LANconfig oder LANmonitor wird automatisch eine Backup-Datei mit den aktuellen Trace-Daten gespeichert. Mehr zu den entsprechenden Einstellungsmöglichkeiten finden Sie im Abschnitt *Traceeinstellungen* auf Seite 305.

3.4.2.7 Sichern und Wiederherstellen der Trace-Daten

Auch die eigentlichen Trace-Daten können Sie zur späteren Bearbeitung oder Weitergabe an einen anderen Benutzer über **Datei** > **Tracedaten/Support-Konfigurationsdatei speichern** auf einen Datenträger schreiben und über **Datei** > **Tracedaten laden** wieder öffnen.

Alternativ können Sie auch die Schaltflächen  zum Laden und  zum Speichern der Trace-Daten verwenden.

3.4.2.8 Sichern und Wiederherstellen der Trace-Konfiguration

Zur späteren Wiederverwendung oder Weitergabe an einen anderen Benutzer können Sie die komplette Konfiguration der Trace-Ausgabe über **Datei** > **Tracekonfiguration speichern** auf einen Datenträger schreiben und später mit **Datei** > **Tracekonfiguration laden** wieder öffnen.

Trace-Konfigurationen selbst sind geräteunspezifisch, lassen sich prinzipiell also in Kombination mit jedem Gerät verwenden. Nicht importierbare – weil auf dem Zielgerät nicht vorhandene Optionen, Status-Werte oder Show-Befehle – werden beim Ladevorgang übersprungen. LANtracer gibt Ihnen allerdings eine Warnmeldung aus, welche die vom Zielgerät nicht unterstützten Bestandteile einer Tracekonfiguration auflistet.

3.4.2.9 Konfigurationsdatei für den Support ausspielen

LANtracer bietet Ihnen die Möglichkeit, eine spezielle Konfigurationsdatei zu erstellen, um Sie zur Fehlerdiagnose oder weiteren Unterstützung an den Support weiterzugeben. Diese Datei beinhaltet die aktuelle Konfiguration sowie zusätzliche Informationen zum Gerät, welche den Support-Mitarbeitern die Fehlersuche ggf. erleichtern.

Falls Sie bestimmte Informationen nicht weitergeben möchten, bietet Ihnen LANtracer die Option, sicherheitsrelevante Informationen beim Speichern auszublenden. Mehr zu den entsprechenden Einstellungsmöglichkeiten finden Sie im Abschnitt *Support-Konfigurationsdatei* auf Seite 305.

3.4.3 Die Menüstruktur im LANtracer

Über die Menüleiste laden und speichern Sie Trace-Konfigurationen und -Daten, starten und stoppen Traces, und passen sowohl das Aussehen als auch die Funktionsweise von LANtracer an.

3.4.3.1 Datei

Unter diesem Menüpunkt speichern und laden Sie Trace-Konfigurationen/-Daten und beenden LANtracer.

Tracedaten laden

Über diesem Menüpunkt laden Sie die in einer *.lct-Datei abgespeicherten Trace-Daten in die Ergebnisansicht.

Tracedaten/Support-Konfigurationsdatei speichern

Über diesem Menüpunkt speichern Sie nach einem Trace die aufgezeichneten Trace-Daten in eine *.lct-Datei. Parallel dazu wird in das selbe Verzeichnis eine Support-Konfigurationsdatei abgelegt. Diese Datei ist mit der im Abschnitt *Support-Konfigurationsdatei speichern* auf Seite 303 beschriebenen Datei identisch.

Tracekonfiguration laden

Über diesem Menüpunkt laden Sie die in einer *.lcg-Datei abgespeicherte Trace-Konfiguration in die Konfigurationsansicht.

Trace-Konfigurationen selbst sind geräteunspezifisch, lassen sich prinzipiell also in Kombination mit jedem Gerät verwenden. Nicht importierbare – weil auf dem Zielgerät nicht vorhandene Optionen, Status-Werte oder Show-Befehle – werden beim Ladevorgang übersprungen. LANtracer gibt Ihnen allerdings eine Warnmeldung aus, welche die vom Zielgerät nicht unterstützten Bestandteile einer Tracekonfiguration auflistet.

Tracekonfiguration speichern

Über diesem Menüpunkt speichern Sie die in der Konfigurationsansicht getätigten Einstellungen in eine geräteunabhängige *.lcg-Datei.

Tracedaten importieren

Über diesem Menüpunkt importieren Sie die in einer *.lct-Datei abgespeicherten Trace-Daten in die Ergebnisansicht. Auf diese Weise haben Sie die Möglichkeit, Tracedaten grafisch aufzubereiten, die Sie über die Konsole (z. B. mit Telnet oder PuTTy) erstellt haben.

Support-Konfigurationsdatei speichern

Über diesem Menüpunkt speichern Sie die in der Konfigurationsansicht getätigten Einstellungen in eine gerätespezifische *.spf-Datei.

Eine Support-Konfigurationsdatei beeinhaltet die aktuelle Konfiguration und zusätzliche Informationen über das Gerät. Da diese Datei für den technischen Support bestimmt ist und somit Ihre Hände verlässt, können Sie in den *Einstellungen für die Support-Konfigurationsdatei* bei Bedarf sensible Bereiche der Konfiguration ausblenden.

Schließen

Schließt und beendet LANtracer.

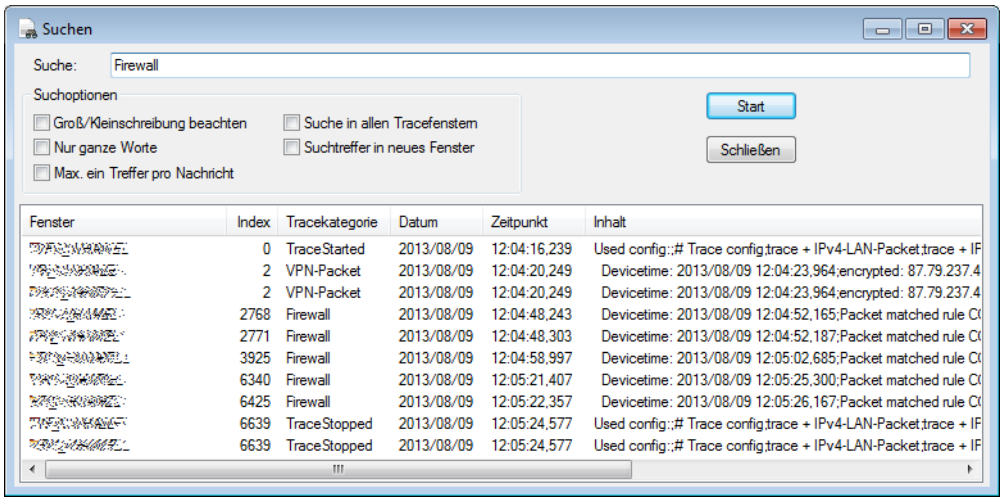
3.4.3.2 Bearbeiten

Unter diesem Menüpunkt durchsuchen oder löschen Sie die angezeigten Traces.

Suchen

Über diesem Menüpunkt öffnen Sie den Such-Dialog, der es Ihnen ermöglicht, die aufgezeigneten oder geladenen Trace-Daten gezielt nach bestimmten Begriffen zu durchsuchen. Sofern Sie keine weiteren Suchoptionen ausgewählt haben, führt die Funktion anhand des eingegeben Suchbegriffs eine Wildcard-Suche in allen existierenden Spalten durch; d. h. im Ergebnisfenster werden alle Treffer gelistet, die den eingegebenen Suchbegriff enthalten.

Um also gezielt nach Trace-Einträgen zu einer bestimmten Rubrik oder mit einem bestimmten Datum zu suchen, geben Sie z. B. `Firewall` oder `2013/08/09` ein und klicken **Start**.



Ferner haben Sie die Möglichkeit, folgende Suchoptionen zur Begrenzung der Suche zu aktivieren:

- **Groß/Kleinschreibung beachten**: Aktiviert die case-sensitive Suche.

- **Nur ganze Worte**: Aktiviert die Suche nach ganzen Wörtern bzw. deaktiviert die Suche nach Teil-Strings. In diesem Fall zeigt die Suche nach z. B. `VPN` nur Einträge an, in denen der Begriff als solcher vorkommt. Begriffe wie `VPN-Packet` fallen nicht ins Suchmuster.
- **Max. ein Treffer pro Nachricht**: Fasst mehrere Treffer zu einem Begriff innerhalb eines Trace-Eintrags zu einem einzigen Suchtreffer zusammen.
- **Suche in allen Tracefenstern**: Weitet die Suche auf alle geöffneten Ergebnisansichten aus. Andernfalls bleibt die Suche auf jene Ergebnisansicht beschränkt, auf die sie sich zuletzt bezog. Lesen Sie dazu auch das Kapitel *Mehrstufige Suche* auf Seite 301.
- **Suchtreffer in neues Fenster**: Zeigt die gefundenen Treffer in einer neuen Ergebnisansicht an.

Fensterinhalt löschen

Über diesem Menüpunkt löschen Sie die in der aktuellen Ergebnisansicht angezeigten Trace-Daten.

3.4.3.3 Ansicht

Unter diesem Menüpunkt passen Sie das Verhalten der LANtracer-Bedienoberfläche an.

Trace-Ergebnisse

Wechselt in den Modus zur Anzeige der Trace-Ergebnisse

Trace-Erg. Doppelansicht

Wechselt in den Modus zur geteilten Anzeige der Trace-Ergebnisse in zwei parallelen Fenstern (Doppelansicht).

Konfiguration

Wechselt in den Modus zur Konfiguration der Trace-Ausgabe.

3.4.3.4 Tracen

Unter diesem Menüpunkt starten und stoppen Sie die Trace-Ausgabe.

Trace starten

Über diesen Menüpunkt starten Sie die Trace-Ausgabe.

Trace starten

Über diesen Menüpunkt stoppen Sie die Trace-Ausgabe.

3.4.3.5 Extras

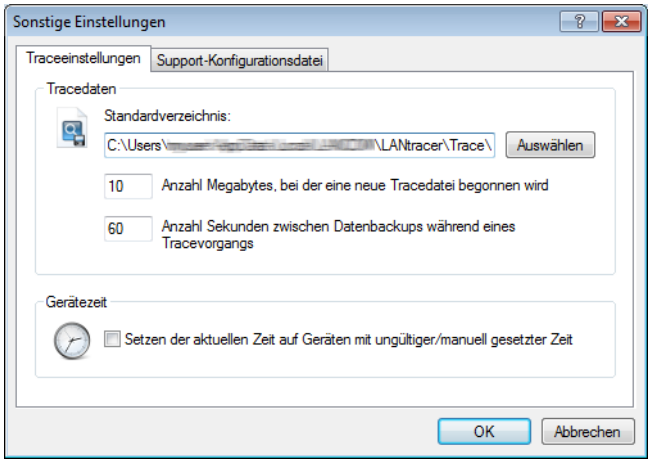
Unter diesem Menüpunkt finden Sie die programmbezogenen Einstellungsmöglichkeiten für LANtracer, z. B. zur automatischen Protokollierung der Trace-Ausgabe oder zur Definition der Support-Konfigurationsdatei.

Sonstige Einstellungen

Unter diesem Menüpunkt nehmen Sie die programmbezogenen Einstellungen für LANtracer vor.

Traceeinstellungen

Unter diesem Menüpunkt nehmen Sie die Einstellungen zu den Tracedaten und zur Gerätezeit vor.



Tracedaten

Beim Starten eines Traces über LANconfig oder LANmonitor wird automatisch eine Backup-Datei mit den aktuellen Trace-Daten gespeichert. Die Einstellungen für das Trace-Backup nehmen Sie im Abschnitt **Tracedaten** vor. Geben Sie

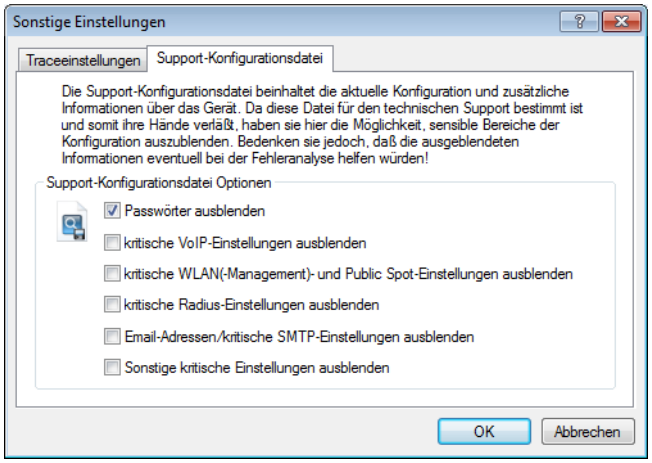
- … die maximale Größe einer Trace-Backup-Datei (in Megabyte) an. Wenn diese Größe mit einem aktiven Trace erreicht wird, wird automatisch eine weitere Trace-Backup-Datei angelegt. eine Ausgabegröße (in Megabyte) an, ab der LANtracer automatisch eine Trace-Datei erzeugt.
- … ein Intervall (in Sekunden) an, in dem LANtracer die Trace-Ausgabe in die erzeugte Datei speichert.
- … ein Verzeichnis an, in welchem LANtracer die Trace-Dateien standardmäßig ablegt.

Gerätezeit

Um eine zeitlich genaue Trace-Ausgabe zu erhalten, kann LANtracer außerdem vor einem Trace die Gerätezeit auf Gültigkeit prüfen und bei Geräten mit ungültiger/manuell gesetzter Zeit automatisch korrigieren, wenn Sie die betreffende Option aktivieren.

Support-Konfigurationsdatei

Unter diesem Menüpunkt legen Sie fest, welche Inhalte beim Speichern einer Support-Konfigurationsdatei automatisch entfernt werden. Die hierbei erstellte Support-Datei enthält alle Informationen im Klartext. Sie können die Datei daher in einem Editor öffnen und auf ggf. noch vorhandene sensible Einträge prüfen.



Bedenken Sie, dass das Ausblenden von sensiblen Bereichen der Konfiguration die Fehleranalyse durch den Support erschweren kann.

3.4.4 Die Symbolleiste im LANtracer

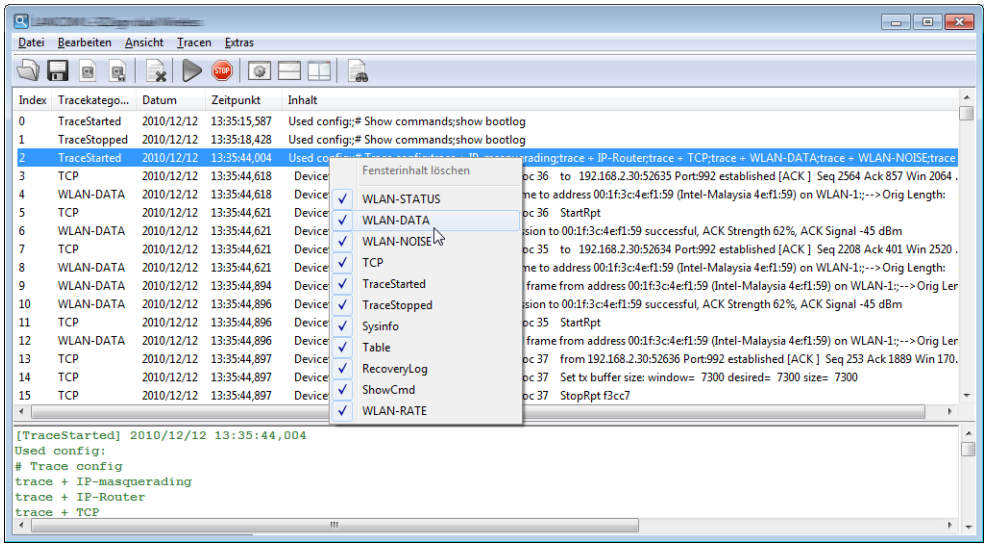
Das Trace-Modul bietet die folgenden Schaltflächen zur Bedienung:

Tabelle 21: Bedeutung der Symbole

	Lädt eine Datei mit Trace-Daten
	Speichert die aktuellen Trace-Daten, um diese an einen Anwender weiterzugeben.
	Löscht die aktuelle Anzeige der Trace-Ergebnisse
	Startet die Ausgabe der Trace-Ergebnisse gemäß der aktuellen Konfiguration und wechselt automatisch in den Anzeige-Modus der Trace-Ergebnisse. Solange die Ausgabe der Trace-Ergebnisse läuft, sind alle anderen Schaltflächen deaktiviert.
	Hält die Ausgabe der Trace-Ergebnisse an
	Wechselt in den Modus zur Konfiguration der Trace-Ausgabe
	Wechselt in den Modus zur Anzeige der Trace-Ergebnisse
	Wechselt in den Modus zur geteilten Anzeige der Trace-Ergebnisse in zwei parallelen Fenstern (Doppelansicht)
	Startet die Synchronisation der beiden Traces in der geteilten Anzeige anhand des Zeitstempels
	Beendet die Synchronisation der beiden Traces in der geteilten Anzeige
	Öffnet das Fenster zur Suche in den Trace-Ergebnissen

3.4.5 Das Kontextmenü in LANtracer

Das Kontextmenü ist nur in der Ergebnisansicht verfügbar. Darin haben Sie die Möglichkeit, einzelne Trace-Kategorien auszublenden und so die angezeigten Ergebnisse grob zu filtern, oder den Fensterinhalt komplett zu leeren.



3.4.6 LANtracer Tastaturbefehle

Alt+L	Tracedaten laden
Alt+I	Tracedaten importieren
Alt+S	Tracedaten/Support-Konfigurationsdatei speichern
Strg+L	Tracekonfiguration laden
Strg+S	Tracekonfiguration speichern
Strg+F	Öffnet das Fenster zur Suche in den Trace-Ergebnissen
Alt+D	Löscht die aktuelle Anzeige der Trace-Ergebnisse
Strg+R	Wechselt in den Modus zur Anzeige der Trace-Ergebnisse
Strg+T	Wechselt in den Modus zur geteilten Anzeige der Trace-Ergebnisse in zwei parallelen Fenstern (Doppelansicht)
Strg+K	Wechselt in den Modus zur Konfiguration der Trace-Ausgabe
Leertaste, Enter	Makiert Auswahlkästchen in der Experten-Konfiguration
Alt+C	Schließt LANtracer

4 Diagnose

4.1 Trace-Ausgaben

Zur Kontrolle der internen Abläufe im Router während oder nach der Konfiguration bieten sich die Trace-Ausgaben an. Durch einen solchen Trace werden z. B. die einzelnen Schritte bei der Verhandlung des PPPs angezeigt. Erfahrene Anwender können durch die Interpretation dieser Ausgaben evtl. Fehler beim Verbindungsaufbau aufspüren. Besonders positiv: Die aufzuspürenden Fehler können sowohl in der Konfiguration eigener Router als auch bei der Gegenseite zu finden sein.

Die Trace-Ausgaben sind leicht zeitverzögert zum tatsächlichen Ereignis, jedoch immer in der richtigen Reihenfolge. Das stört im Regelfall die Interpretation der Anzeigen nicht, sollte aber bei genaueren Analysen berücksichtigt werden.

4.1.1 So starten Sie einen Trace

Trace-Ausgaben starten Sie in einer Konsolen-Sitzung. Stellen Sie zunächst eine Konsolen-Verbindung zu Ihrem Gerät her. Der Trace-Aufruf erfolgt dann mit dieser Syntax:

```
> trace [Schlüssel] [Parameter]
```

Der Befehl Trace, der Schlüssel, die Parameter und die Kombinationsbefehle werden jeweils durch Leerzeichen voneinander getrennt.

4.1.2 Übersicht der Schlüssel

Dieser Schlüssel …	… ruft in Verbindung mit Trace die folgende Reaktion hervor:
?	zeigt einen Hilfetext an
+	schaltet eine Trace-Ausgabe ein
-	schaltet eine Trace-Ausgabe aus
#	schaltet zwischen den verschiedenen Trace-Ausgaben um (Toggle)
kein Schlüssel	zeigt den aktuellen Zustand des Traces an

4.1.3 Übersicht der Parameter im trace-Befehl

Die jeweils für ein bestimmtes Modell verfügbaren Traces können über die Eingabe von `trace` ohne Argumente auf der Konsole angezeigt werden.

Tabelle 22: Übersicht einiger durchführbarer Traces

Dieser Parameter ...	... ruft beim Trace die folgende Anzeige hervor:
`Status`	Status-Meldungen der Verbindungen
`Fehler`	Fehler-Meldungen der Verbindungen
`ACME`	Automatic Certificate Management Environment (ACME) Client

Dieser Parameter ...	... ruft beim Trace die folgende Anzeige hervor:
ADSL	ADSL-Verbindungsstatus
ARP	Address Resolution Protocol
ATM-Cell	ATM-Paketebene
ATM-Error	ATM-Fehler
Bridge	Informationen über die WLAN-Bridge
Connact	Meldungen aus dem Aktivitätsprotokoll
Cron	Aktivitäten der Zeitautomatik (Cron-Tabelle)
D-Kanal-Dump	Trace des D-Kanals des angeschlossenen ISDN-Busses
DFS	Trace zur Dynamic Frequency Selection, der automatischen Kanalwahl im 5-GHz-WLAN-Band
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Service Protocol
EAP	Trace zum EAP, dem bei WPA/802.11i und 802.1X verwendeten Protokoll zur Schlüsselaushandlung
Ethernet	Informationen über die Ethernet-Schnittstellen
Firewall	Zeigt die Aktionen der Firewall
FW-DNS	Änderungen an der Firewall-Datenbank der DNS-Ziele: › Wenn ein DNS-Paket eintrifft, werden das Paket und die betroffenen Wildcardausdrücke und Ziele ausgegeben. › Wenn die TTL (Time-to-Live – Lebensdauer) eines Eintrags abläuft, dann werden dieser Datensatz und die betroffenen Wildcardausdrücke und Ziele ausgegeben. › Wenn eine der beiden Firewalls ein DNS-Ziel registriert oder deregistriert, weil sich ihre Konfiguration geändert hat. › Wenn sich die Tabellen **Setup** > **Firewall** > **DNS-Ziele** oder **Setup** > **Firewall** > **DNS-Ziel-Liste** ändern.
GRE	Meldungen zu GRE-Tunneln
hnat	Informationen zum Hardware-NAT
IAPP	Trace zum Inter Access Point Protocol, zeigt Informationen über das WLAN-Roaming.
ICMP	Internet Control Message Protocol
IGMP	Informationen über das Internet Group Management Protocol
IP-Masquerading	Vorgänge im Masquerading-Modul
IPv6-Config	Informationen über die IPv6-Konfiguration
IPv6-Firewall	Ereignisse der IPv6-Firewall
IPv6-Interfaces	Informationen der IPv6-Schnittstellen
IPv6-LAN-Packet	Datenpakete über die IPv6-LAN-Verbindung
IPv6-Router	Informationen über das IPv6-Routing

Dieser Parameter ...	... ruft beim Trace die folgende Anzeige hervor:
IPv6-WAN-Packet	Datenpakete über die IPv6-WAN-Verbindung
L2TP	L2TPv2 / v3-Protokoll
LANAUTH	LAN-Authentifizierung (z. B. Public Spot)
Load-Balancer	Informationen zum Load-Balancing
Mail-Client	E-Mail-Verarbeitung des integrierten Mail-Clients
VPN-Mesh	Trace für *LANCOM Advanced Mesh VPN (AMVPN)* auf Seite 893.
NETFLOW-Common	Mehr Informationen zu NetFlow / IPFIX finden Sie unter *Netflow / IPFIX* auf Seite 1678.
NETFLOW-Error	
NETFLOW-Export	
NETFLOW-Metering	
NTP	Timeserver Trace
Paket-Dump	Anzeige der ersten 64 Bytes eines Pakets in hexadezimaler Darstellung
PPP	Verhandlung des PPP-Protokolls
RADIUS	RADIUS-Trace
RIP	IP Routing Information Protocol
Script	Script-Verhandlung
Serial	Informationen über den Zustand der seriellen Schnittstelle
SIP-Packet	SIP-Informationen, die zwischen einem VoIP Router und einem SIP-Provider bzw. einer übergeordneten SIP-TK-Anlage ausgetauscht werden
SMTP-Client	E-Mail-Verarbeitung des integrierten Mail-Clients
SNTP	Simple Network Time Protokoll
Spgtree	Informationen zum Spanning Tree Protokoll
USB	Informationen über den Zustand der USB-Schnittstelle
VLAN	Informationen über virtuelle Netzwerke
VPN-Packet	IPSec und IKE Pakete
VPN-Status	IPSec und IKE Verhandlungen
VRRP	Informationen über das Virtual Router Redundancy Protocol
WLAN	Informationen über die Aktivitäten in den Funknetzwerken
WLAN-ACL	Status-Meldungen über MAC-Filterregeln. Die Anzeige ist abhängig von der Konfiguration des WLAN-Data-Trace. Ist dort eine MAC-Adresse vorgegeben, zeigt der Trace nur die Filterergebnisse an, die diese spezielle MAC-Adresse betreffen.
XML-Interface-PbSpot	Meldungen des Public-Spot-XML-Interfaces

4.1.3.1 Erweiterte WLAN-Traces

Zur Unterstützung einer besseren Diagnose im WLAN-Bereich lassen sich unter **Setup** > **WLAN** einige Trace-Parameter gezielt anpassen.

Trace-Daten-Pakete

Die Ausgabe der Tracemeldungen lässt sich auf bestimmte Datenpakete eingrenzen.

Mögliche Werte:

normal

NULL

andere

Default:

normal

NULL

andere

Trace-MAC

Für den WLAN-Data-Trace lässt sich die Ausgabe von Tracemeldungen auf einen bestimmten Client mit der hier eingetragenen WLAN-MAC-Adresse einstellen.

Mögliche Werte:

max. 12 hexadezimale Zeichen aus

0123456789abcdef

Default:

000000000000

Besondere Werte:

000000000000: Deaktiviert diese Funktion und gibt die Tracemeldungen von allen Clients aus.

Dieser Filter wirkt für die Traces WLAN-DATA, WLAN-STRENGTH und WLAN-AGGREGATION, jedoch nicht für WLAN-STATUS.

Trace-Mgmt-Packete

Mit dieser Auswahl lässt sich einstellen, welche Klassen von Management-Frames im WLAN-DATA-Trace auftauchen sollen.

Mögliche Werte:

Assoziierung: (Re)Association Request/Response, Disassociate

Authentisierung: Authentication, Deauthentication

Probes: Probe Request, Probe Response

Action

Beacon

Andere: alle restlichen Management-Frametypen

Default:

Assoziierung

Authentisierung

Probes

Action

Andere

Trace-Pakete

Ähnlich wie bei der Trace-MAC und der Trace-Stufe lassen sich die Ausgaben im WLAN-DATA-Traces anhand des Typs der empfangenen bzw. gesendeten Pakete einschränken, z. B. Management (Authenticate, Association, Action, Probe-Request/Response), Control (z. B. Powersave-Poll), EAPOL (802.1X-Verhandlung, WPA-Key-Handshake).

Mögliche Werte:

Management

Control

Daten

EAPOL

Alle

Default:

Alle

Trace-Stufe

Für den WLAN-Data-Trace lässt sich die Ausgabe von Tracemeldungen auf einen bestimmten Inhalt beschränken. Der hier eingetragene Wert schränkt die Pakete im WLAN-DATA-Trace bis zur entsprechenden Stufe ein.

Mögliche Werte:

0 bis 255

Besondere Werte:

0: nur die Meldung, dass ein Paket überhaupt empfangen/gesendet wurde

1: zusätzlich die physikalischen Parameter der Pakete (Datenrate, Signalstärke etc.)

2: zusätzlich der MAC-Header

3: zusätzlich der Layer3-Header (z. B. IP)

4: zusätzlich der Layer4-Header (TCP, UDP...)

5: zusätzlich die TCP/UDP-Payload

255: keine Beschränkung des Inhalts. Der Trace gibt die kompletten Pakete aus.

Default:

255

4.1.4 Kombinationsbefehle

Dieser Kombinations-Befehl …	… ruft beim Trace die folgende Anzeige hervor:
Display	Status- und Error-Ausgaben
Protocol	PPP- und Script-Ausgaben
TCP-IP	IP-Routing-, IP-RIP-, ICMP- und ARP-Ausgaben

Die angehängten Parameter werden dabei von links nach rechts abgearbeitet. Dadurch kann ein zunächst aufgerufener Parameter anschließend auch wieder eingeschränkt werden.

4.1.5 Filter für Traces

Manche Traces wie der IP-Router-Trace oder die VPN-Traces erzeugen eine große Anzahl von Ausgaben. Damit wird die Ausgabe schnell unübersichtlich. Mit den Trace-Filtern haben Sie die Möglichkeit, nur die für Sie wichtigen Informationen aus den gesamten Traces herauszufiltern.

Zum Einschalten eines Trace-Filters wird das Trace-Kommando um den Parameter „@“ erweitert, der die folgende Filterbeschreibung einleitet. In der Filterbeschreibung gelten folgende Operatoren:

Operator	Beschreibung
(Leerzeichen)	ODER-Verknüpfung: Der Filter passt dann, wenn einer der Operanden in der Trace-Ausgabe vorkommt
+	UND-Verknüpfung: Der Filter passt dann, wenn der Operand in der Trace-Ausgabe vorkommt
-	Nicht-Verknüpfung: Der Filter passt dann, wenn der Operand nicht in der Trace-Ausgabe vorkommt
"	die Ausgabe muss exakt dem Suchmuster entsprechen

Als Operanden können beliebige Zeichenketten eingetragen werden, z. B. die Namen von Gegenstellen, Protokollen oder Ports. Der Trace-Filter verarbeitet diese Angaben dann nach den Regeln der verwendeten Operatoren so wie z. B. die Suchmaschinen im Internet.

4.1.6 Beispiele für die Traces

Dieser Schlüssel …	… ruft in Verbindung mit Trace die folgende Reaktion hervor:
trace	zeigt alle Protokolle an, die während der Konfiguration Ausgaben erzeugen können, und den Zustand der jeweiligen Ausgaben (ON oder OFF)
trace + protocol display	schaltet die Ausgabe aller Verbindungsprotokolle und der Status- und Fehlermeldungen ein
trace - icmp	schaltet alle Trace-Ausgaben mit Ausnahme des ICMP-Protokolls ein
trace ppp	zeigt den Zustand des PPPs an
trace + ip-router @ GEGENSTELLE-A GEGENSTELLE-B	schaltet die Ausgaben des IP-Routers an für alle Ausgaben, die sich auf die Gegenstellen A oder B beziehen
trace + ip-router @ GEGENSTELLE-A GEGENSTELLE-B -ICMP	schaltet die Ausgaben des IP-Routers an für alle Ausgaben, die sich auf die Gegenstellen A oder B beziehen, die nicht ICMP verwenden
trace + ip-router @ GEGENSTELLE-A GEGENSTELLE-B +ICMP	schaltet die Ausgaben des IP-Routers an für alle Ausgaben, die sich auf die Gegenstellen A oder B beziehen und die ICMP verwenden
trace + ip-router @+TCP +"port: 80"	schaltet die Ausgaben des IP-Routers an für alle Ausgaben, die TCP/IP und den Port 80 verwenden. “port: 80” steht in Anführungszeichen, um auch das Leerzeichen als Teil der Zeichenkette einzubeziehen.

4.1.7 Traces aufzeichnen

Um einen Trace komfortabel mit einem Windows-System aufzuzeichnen (z. B. als Unterstützung für den Support), empfehlen wir Ihnen folgende Vorgehensweise:

Öffnen Sie ein Terminal-Programm, z.B. HyperTerminal. Als Name geben Sie einen beliebigen Namen ein.

Ab Windows Vista ist HyperTerminal nicht mehr Bestandteil des Betriebssystems, aber man kann im Internet diverse ähnlich funktionierende und frei erhältliche Programme herunterladen.



Wählen Sie im Fenster 'Verbinden mit' im Pulldown-Menü 'Verbindung herstellen über' den Eintrag 'TCP/IP'. Geben Sie anschließend als 'Hostadresse' die lokale/öffentliche IP-Adresse oder den FQDN des Gerätes ein. Nach der Bestätigung erscheint im HyperTerminal eine Login Aufforderung. Geben Sie nun das Konfigurationspasswort ein.

Zum Aufzeichnen des Traces klicken Sie in der Menüleiste auf **Übertragen** / **Text aufzeichnen**. Geben Sie den Pfad an, in dem die Textdatei gespeichert werden soll. Wechseln Sie nun wieder in das Dialogfenster und geben den entsprechenden Trace-Befehl ein.

Um den Trace wieder zu stoppen, klicken Sie im HyperTerminal in der oberen Menüleiste auf **Übertragen** / **Text aufzeichnen beenden**.

4.1.8 Tracen auf ein angeschlossenes USB-Laufwerk

Es ist möglich, Traces auf ein angeschlossenes USB-Laufwerk, z. B. einen USB-Stick, im Hintergrund zu speichern. Eine aktive Konsolensitzung ist dazu nicht erforderlich, da die Aufzeichnung im Hintergrund durchgeführt wird.

Auf die Datei kann nach Abschluss der Aufzeichnung zugegriffen werden, in dem der USB-Stick an einen Computer angeschlossen wird. Alternativ kann remote per SCP auf das Gerät auf das Verzeichnis /usb/ zugegriffen werden.

Das USB-Laufwerk muss dazu FAT32-formatiert sein. Das Gerät schreibt so lange auf den USB-Stick, bis dieser voll ist, danach stoppt die Aufzeichnung.

Es ist nicht möglich, eine Datei auf den internen Flash des Geräts zu schreiben oder von dort zu laden.

Ein ICMP-Trace auf der Konsole wird z. B. wie folgt auf ein USB-Laufwerk umgeleitet:

```
Trace # ICMP > /usb/file.lct
```

Der ICMP-Trace wird wie folgt gestoppt:

`Trace # ICMP > /usb/file.lct` bzw. `Trace - all > /usb/file.lct`

Das Show-Kommando „show trace-file“ zeigt aktive Trace-Sitzungen auf USB an.

Ein `Trace - all` beendet nicht die laufenden Sitzungen, die auf USB augfezeichnet werden, sondern nur die aktiven Traces der aktiven Konsolensitzung.

```
root@lc1900ef-aa:/
> tr # icmp >/usb/my
```

```
created trace session for '/usb/my.lct'
/usb/my.lct:
ICMP                        ON

root@lc1900ef-aa:/
> show trace-file

/usb/my.lct:
  ICMP                  ON

root@lc1900ef-aa:/
> tr # tcp >/usb/my
/usb/my.lct:
TCP                         ON

root@lc1900ef-aa:/
> show trace-file

/usb/my.lct:
  ICMP                  ON
  TCP                   ON

root@lc1900ef-aa:/
> tr - all >/usb/my
/usb/my.lct:
remove trace session for '/usb/my.lct'
```

4.2 Tracen mit dem LANmonitor

Informationen zu diesem Thema finden Sie im Kapitel *LANtracer – Tracen mit LANconfig und LANmonitor* auf Seite 292.

4.3 Datenpakete aufzeichnen und analysieren

Sie haben mit LCOS zwei Möglichkeiten, Datenpakete zwecks Analyse von Störungen oder Problemen aufzuzeichnen.

Zum einen besteht die Möglichkeit, über ein Kommandozeilen-Tool den Befehl **lcoscap** auszuführen. Dieser Befehl aktiviert die Aufzeichnung der Pakete und schreibt die Ergebnisse in eine Datei, die Sie mit einem Tool wie „Wireshark" öffnen und analysieren können.

Zum anderen können Sie die deutlich komfortablere Methode über WEBconfig nutzen. Hierbei können Sie unterschiedliche Parameter definieren und auf diese Weise Datenpakete ausgewählter Schnittstellen aufzeichnen, um Sie für eine anschließende Analyse in eine Ergebnisdatei zu schreiben.

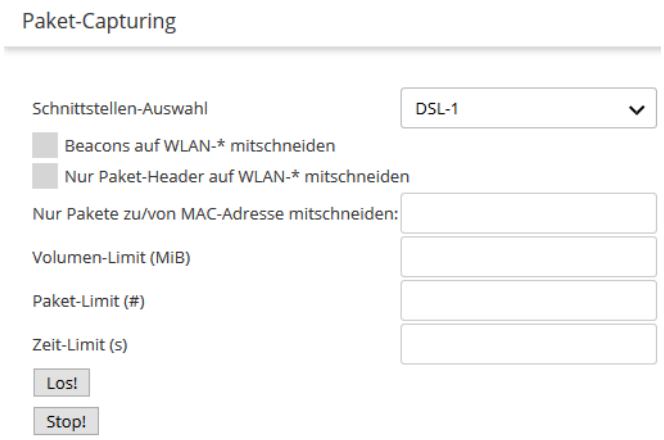
Diese Methode bietet Ihnen mehrere Vorteile:

- Sie sind auf keine spezielle Software angewiesen, da Sie Webconfig auf beliebigen Web-Browsern ausführen können.
- Die Eingabe von Kommandozeilenbefehlen entfällt. Stattdessen stehen Ihnen komfortable Menü-Elemente zur Verfügung.
- Wenn Sie WEBconfig über HTTPS betreiben, ist die Vertraulichkeit und Sicherheit des aufgezeichneten Datenverkehrs gewährleistet.

Der LCOScap-Client kann sich somit sowohl über IPv4 als auch über IPv6 mit dem Gerät verbinden.

4.3.1 Capture-Daten via Paket-Capturing erstellen

Der Dialog **Extras** > **Paket-Capturing** im WEBConfig bietet Ihnen eine einfache Möglichkeit, Datenpakete von unterschiedlichen Schnittstellen aufzuzeichnen und anschließend mit einer geeigneten Software (z. B. Wireshark) zu analysieren.



Für die Spezifizierung der Ausgabe-Datei stehen Ihnen folgende allgemeine Menüpunkte zur Verfügung:

Schnittstellen-Auswahl

Mit diesem Auswahlmenü bestimmen Sie die Schnittstelle, deren Datenpakete aufgezeichnet werden.

Beacons auf WLAN-* mitschneiden

Aktivieren Sie diese Option, um neben den Datenpaketen auch die Beacon-Informationen aufzuzeichnen, wenn die ausgewählte Schnittstelle eine WLAN-Schnittstelle ist.

Nur Paket-Header auf WLAN-* mitschneiden

Aktivieren Sie diese Option, um die Aufzeichnung der Datenpakete auf den Paket-Header zu beschränken, wenn die ausgewählte Schnittstelle eine WLAN-Schnittstelle ist.

Nur Pakete zu/von MAC-Adresse mitschneiden

Wenn Sie nur Datenpakete einer bestimmten physikalischen Adresse innerhalb der ausgewählten Schnittstelle aufzeichnen wollen, können Sie diese hier festlegen.

Volumen-Limit (MiB)

Geben Sie hier das maximale Volumen der aufgezeichneten Pakete in Mebibytes an.

Paket-Limit (#)

Hier können Sie eine maximale Anzahl aufzuzeichnender Pakete festlegen.

Zeit-Limit (s)

Geben Sie hier eine maximale Zeit in Sekunden an, nach welcher die Aufzeichnung endet.

Nach dem Festlegen der Parameter und einem Klick auf **Los!** erzeugen Sie eine extern zu speichernde Datei, die Sie z. B. mit Wireshark öffnen können. Nach einiger Zeit – abhängig von der Verbindungsgeschwindigkeit – öffnet sich ein Dialog, der Sie zum Speichern der erzeugten Datei auffordert. Sie können die Datei mit der Endung *.cap jetzt lokal speichern. Standardmäßig erhält die Datei einen Namen, welcher die Bezeichnung und die zugehörige Schnittstelle des Gerätes enthält, dessen Datenpakete Sie aufgezeichnet haben (z. B. MyDevice-LAN-2.cap). Sie können den voreingestellten Dateinamen jedoch während des Speichervorgangs oder auch nachträglich ändern.

Eine laufende Aufzeichnung lässt sich jederzeit durch einen Klick auf **Stop!** beenden. Dies ist beispielsweise dann sinnvoll, um zunächst eingegebene Parameter zu korrigieren bzw. anzupassen.

Wenn Sie Aufzeichnung ohne Angabe von Limits starten, zeichnet das Gerät die Pakete solange auf, bis Sie den Vorgang mit einem Klick auf **Stop** manuell beenden!

Flexibles WLAN Capture-Format

Ihnen stehen für das Paket-Capturing im WLAN verschiedene Formate zur Auswahl, unter denen das Gerät die aufgezeichnete Paketdaten speichern kann (Konsole: **Setup** > **WLAN** > **Paket-Capture**).

4.3.2 Capture-Daten via LCOSCAP erstellen

Mit „LCOSCAP" haben Sie die Möglichkeit, den Datenverkehr aufzuzeichnen und in einem Wireshark kompatiblen Format abzuspeichern. Sie bedienen „LCOSCAP" über die Kommandozeile, indem Sie die entsprechenden Parameter anhängen.

Sie steuern LCOSCAP über die folgenden Parameter:

-o

Zieldatei, welche den Mitschnitt enthält.

-p

Passwort des Gerätes, auf dem LCOSCAP den Datenverkehr aufnimmt.

-i

Interface des Gerätes, dessen Daten LCOSCAP erfasst.

Wenn sie den Parameter -i auslassen, gibt LCOSCAP die Interface-Liste des Gerätes aus.

-b

Schalter, der die Beacons des Datenverkehrs mit einbezieht (ausschließlich für WLAN).

-h

Schalter, der die 802.11-Header mit einbezieht, allerdings ohne Payload (ausschließlich für WLAN).

-l

Gibt die maximale Größe der Capture-Datei an. Tritt der angegebene Wert ein, erzeugt LCOSCAP eine neue Datei. Die erstellten Dateien erhalten fortlaufende Nummern.

-n

Gibt die Anzahl der Dateien an, die LCOSCAP erzeugt. Wenn die maximale Anzahl der Dateien eintritt, überschreibt LCOSCAP die 1. Datei.

--h

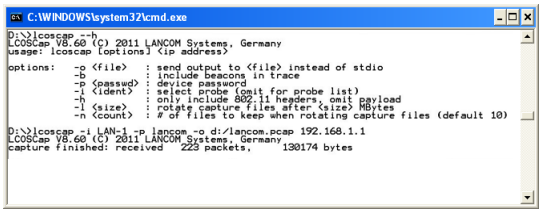
Mit `LCOSCAP --h` rufen Sie die LCOSCAP-Hilfe auf.

Um den Datenverkehr eines Gerätes aufzuzeichnen, geben Sie folgenden Befehl ein:

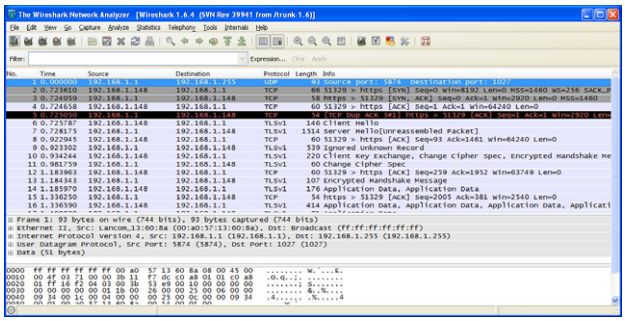
```
LCOSCAP -i LAN-1 -p lancom -o d:/lancom.pcap 192.168.1.1
```

- Das Gerät besitzt in diesem Beispiel die IP-Adresse "192.168.1.1".
- Das Passwort lautet "lancom".
- Sie zeichnen den Datenverkehr am Interface "LAN-1" auf.
- Speicherort und Name der Datei lauten `d:/lancom.pcap`

Mit der Tastenkombination **Strg + C** stoppen Sie die Aufzeichnung



Zur Analyse öffnen Sie die von LCOSCAP erzeugte Datei mit "Wireshark".



4.3.3 Capture Daten via RPCap erstellen

Mit der im LCOS integrierten RPCap-Schnittstelle haben Sie die Möglichkeit, anhand des Paketanalyse-Tools „Wireshark" Paketmitschnitte von einem beliebigen Interface eines LANCOM Routers zu erzeugen.

Gegenüber einem Mitschnitt durch LCOSCap ist es bei den mit RPCap aufgezeichneten Paketen möglich, diese noch während der Aufzeichnung zu untersuchen und ggf. Capture-Filter zu erstellen.

Bitte beachten Sie, dass eine laufende Wireshark-Instanz auf dem PC deutlich mehr Ressourcen verbraucht als eine LCOSCap-Instanz. Für langfristige Aufzeichnungen wird daher empfohlen, LCOSCap zu verwenden.

Um Paketmitschnitte mittels RPCap zu erstellen, sind folgende Voraussetzungen erforderlich:

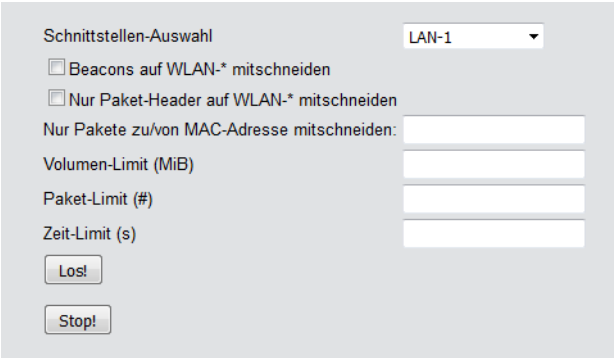
- aktuelle Wireshark-Version und WinPcap-Version unter Microsoft Windows
- LCOS ab Version 8.80
- IP-Konnektivität zwischen dem Wireshark ausführenden PC und dem zu untersuchenden Router

4.3.3.1 Paketmitschnitte mit WEBconfig aktivieren

Um Paketmitschnitte über WEBconfig zu aktivieren, gehen Sie wie folgt vor:

1. Öffnen Sie die Konfiguration des Routers in WEBconfig und wechseln Sie in das Menü **Extras** > **Paket-Capturing**.
2. Wählen Sie die Schnittstelle aus, auf welcher Sie den Paketmitschnitt durchführen möchten (z. B. LAN-1).

3. Klicken Sie auf die Schaltfläche **Los!** um den Mitschnitt zu starten.

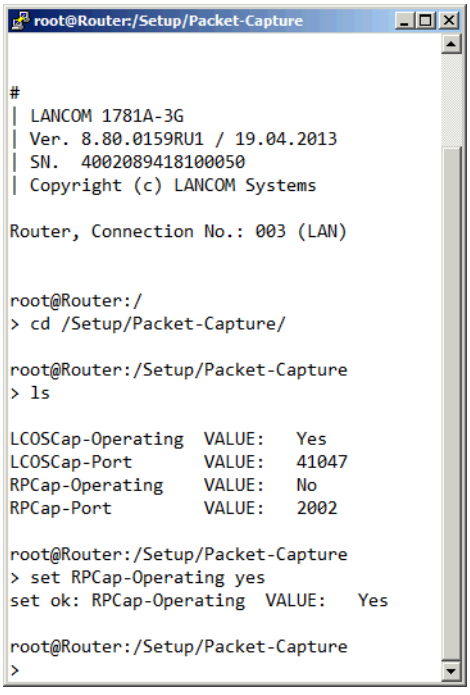


Die Datenpakete werden nun auf der ausgewählten Schnittstelle mitgeschnitten. Um die Aufzeichnung zu beenden, klicken Sie auf die Schaltfläche **Stop!**.

4.3.3.2 Paketmitschnitte über die Konsole aktivieren

Um Paketmitschnitte über die Konsole zu aktivieren, gehen Sie wie folgt vor:

1. Starten Sie eine Konsolen-Sitzung auf dem Router, von dem der Mitschnitt erzeugt werden soll.
2. Wechseln Sie in den Pfad `/Setup/Packet-Capture`.
3. Aktivieren Sie die RPCap-Schnittstelle mit dem Befehl `set RPCap-Operating yes`.



Die Datenpakete werden nun auf der ausgewählten Schnittstelle mitgeschnitten. Indem Sie den Befehl `set RPCap-Operating no` eingeben, deaktivieren Sie den Mitschnitt.

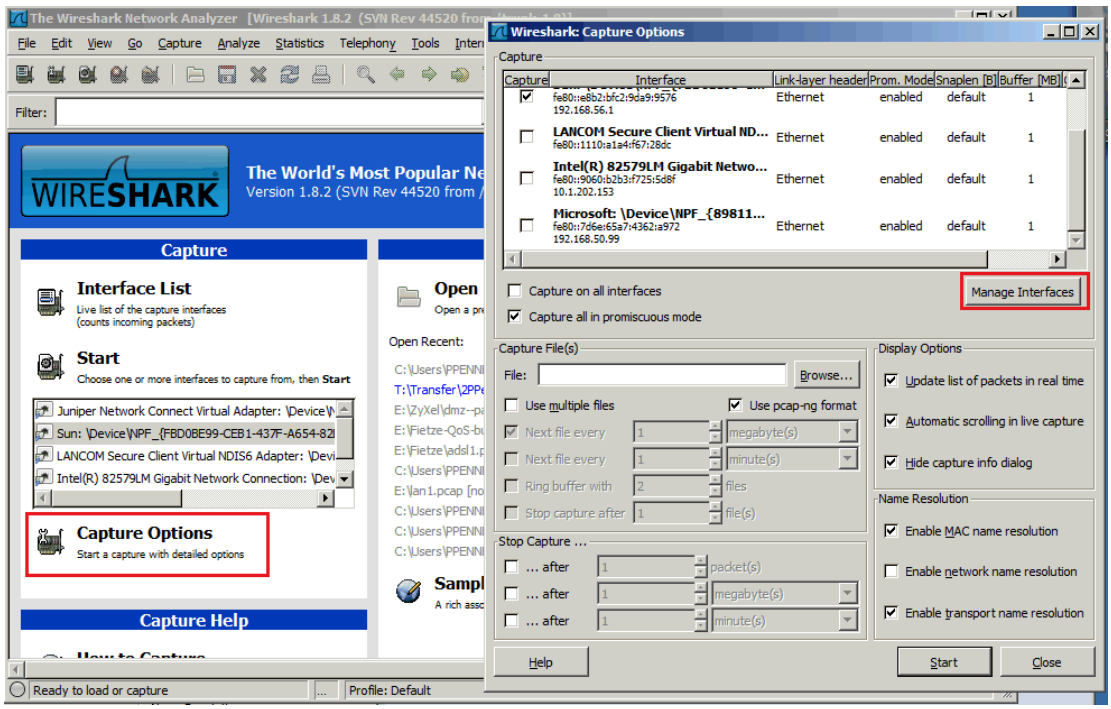
4.3.3.3 Paketmitschnitte mit Wireshark analysieren

Um Paketmitschnitte mit dem Paketanalyse-Tools „Wireshark“ zu analysieren, gehen Sie wie folgt vor:

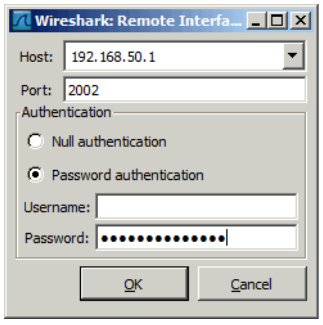
1. Starten Sie Wireshark.

Beachten Sie bitte, dass die RPCap-Schnittstelle nur sinnvoll mit der Windows-Version von Wireshark verwendet werden kann, da nur der für Windows verfügbare und in Wireshark beinhaltete WinPcap-Treiber RPCap unterstützt.

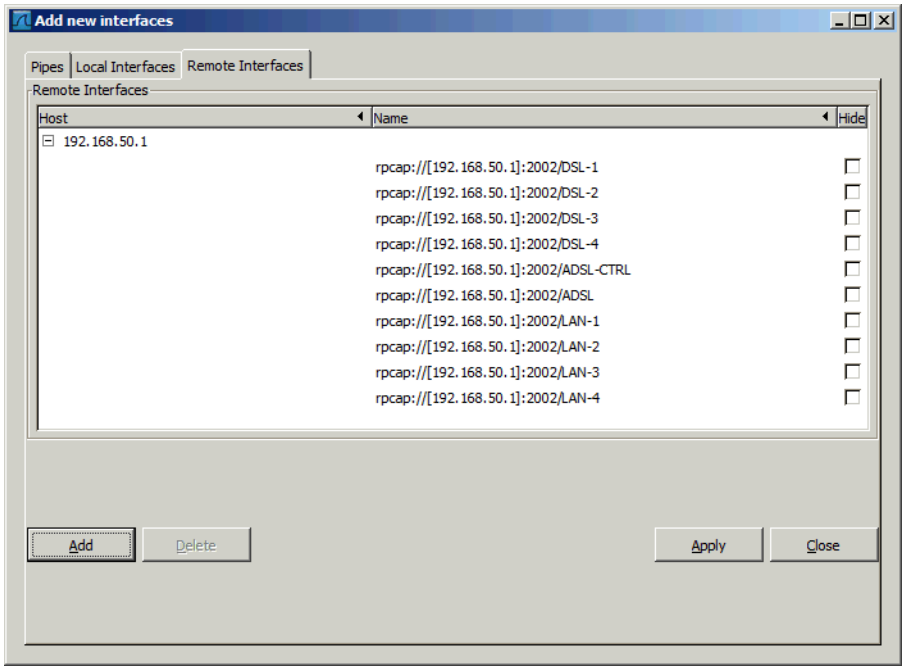
2. Wählen Sie auf dem Startbilschirm **Capture Options** aus. Klicken Sie im darauf erscheinenden Fenster auf die Schaltfläche **Manage Interfaces**.



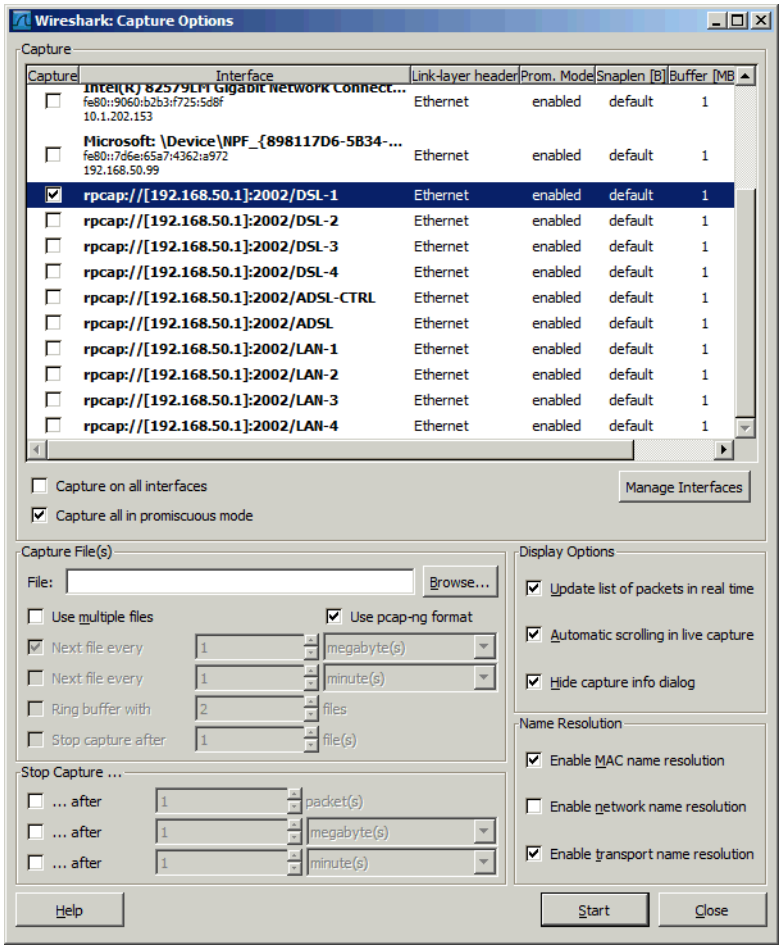
3. Wählen Sie im folgenden Fenster den Reiter **Remote Interfaces** und fügen Sie Ihren Router hinzu. Das Feld **Username** kann leer bleiben, als Password verwenden Sie das **Hauptgerätepasswort des Routers**.



4. Alle zur Aufzeichnung verwendbaren Schnittstellen des Routers werden nun aufgelistet. Bestätigen Sie den Dialog mit einem Klick auf die Schaltflächen **Apply** und **Close**.



5. Wählen Sie in den **Capture Options** aus, welche Schnittstellen erfasst werden sollen. Klicken Sie anschließend auf die Schaltfläche **Start**.



Die durchlaufenden Pakete der ausgewählten Schnittstellen werden nun mitgeschnitten.

4.3.4 Capture-Daten auf ein USB-Laufwerk ausgeben

Sie können Wireshark-Captures im Hintergrund vom Router auf ein angeschlossenes USB-Laufwerk, z. B. einen USB-Stick schreiben lassen. Eine aktive Management-Session vom Computer auf das Gerät ist dazu nicht erforderlich.

Auf die Datei kann nach Abschluss der Aufzeichnung zugegriffen werden, indem der USB-Stick an einen Computer angeschlossen wird. Alternativ kann remote per SCP auf das Gerät auf das Verzeichnis /usb/ zugegriffen werden.

Das USB-Laufwerk muss dazu FAT32-formatiert sein. Das Gerät schreibt so lange auf den USB-Stick, bis dieser voll ist, danach stoppt die Aufzeichnung.

Es ist nicht möglich, eine Datei auf den internen Flash des Geräts zu schreiben oder von dort zu laden.

Den Dateinamen und alle weiteren notwendigen Angaben machen Sie über die Kommandozeile in der Tabelle **Setup** > **Paket-Capture** > **Capturing-auf-Datei** > **Dateien**. Näheres zu den Werten finden sie in der Menüreferenz.

4.4 Das SYSLOG-Modul

Mit dem SYSLOG-Modul besteht die Möglichkeit, Zugriffe auf das Gerät protokollieren zu lassen. Diese Funktion ist insbesondere für Systemadministratoren interessant, da sie die Möglichkeit bietet, eine lückenlose Historie aller Aktivitäten aufzeichnen zu lassen.

Um die SYSLOG-Nachrichten empfangen zu können, benötigen Sie einen entsprechenden SYSLOG-Client bzw. -Dämon. Unter UNIX / Linux erfolgt die Protokollierung durch den in der Regel standardmäßig eingerichteten SYSLOG-Dämon. Dieser meldet sich entweder direkt über die Konsole oder schreibt das Protokoll in eine entsprechende SYSLOG-Datei.

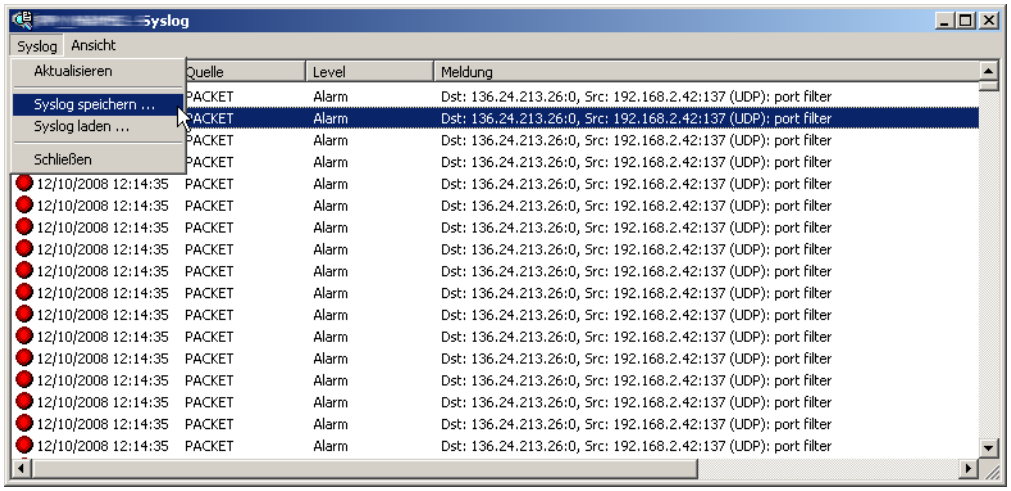
Unter Linux wird in der Datei `/etc/syslog.conf` angegeben, welche Facilities (Dienst oder die Komponente, welche die Nachricht ausgelöst hat) in welche Logdatei geschrieben werden sollen. Überprüfen Sie in der Konfiguration des Dämons, ob auf Netzwerkverbindungen explizit gehört wird.

Windows stellt keine entsprechende Systemfunktion bereit. Sie benötigen spezielle Software, die die Funktion eines SYSLOG-Dämons erfüllt.

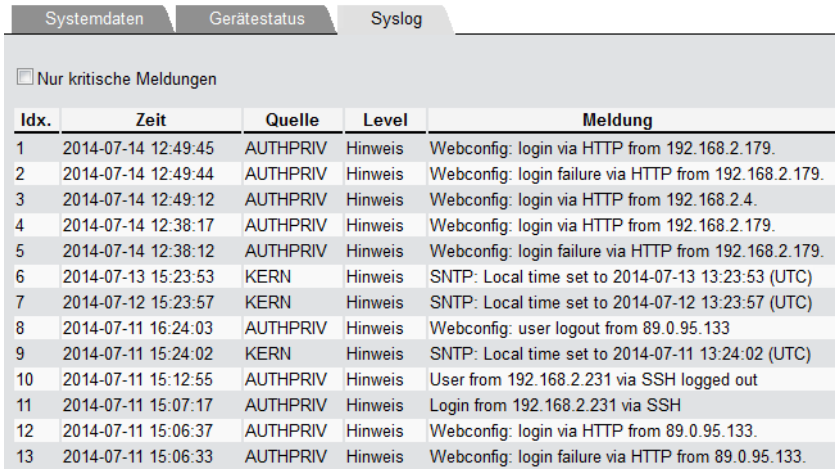
Als Erweiterung zur Ausgabe der SYSLOG-Informationen über einen entsprechenden SYSLOG-Client werden je nach Speicherausstattung des Gerätes zwischen 100 und 23.000 SYSLOG-Meldungen im RAM gespeichert. Diese internen SYSLOGs können an verschiedenen Stellen eingesehen werden:

- In der Statistik der Geräte auf der Kommandozeite
- In WEBconfig unter /Systeminformation/Syslog
- In LANmonitor haben Sie zusätzlich die Möglichkeit, das Syslog aus dem Gerät zu exportieren und in einer Datei zu speichern. Klicken Sie dazu mit der rechten Maustaste auf den Namen des Gerätes und wählen Sie im Kontextmenü den Eintrag **Syslog anzeigen**. Die Ansicht ist jeweils ein aktueller Schnappschuss. Mit **Aktualisieren** wird eine Kopie des derzeitigen SYSLOGs vom Gerät exportiert und in der Ansicht dargestellt. **Syslog speichern** speichert die aktuelle Anzeige in eine Datei. Gespeicherte SYSLOGs können mit **Syslog laden** wieder zur Ansicht geöffnet werden.

Die SYSLOG-Meldungen werden nur dann in den geräteinternen Speicher geschrieben, wenn das Gerät als SYSLOG-Client mit der Loopback-Adresse 127.0.0.1 eingetragen wurde oder die bootpersistente Speicherung aktiviert wurde. Siehe *SYSLOG, Eventlog und Bootlog bootpersistent*.



Alternativ können Sie die aktuellen SYSLOG-Meldungen auf der Startseite von WEBconfig auf der Registerkarte **Syslog** einsehen:



Idx.	Zeit	Quelle	Level	Meldung
1	2014-07-14 12:49:45	AUTHPRIV	Hinweis	Webconfig: login via HTTP from 192.168.2.179.
2	2014-07-14 12:49:44	AUTHPRIV	Hinweis	Webconfig: login failure via HTTP from 192.168.2.179.
3	2014-07-14 12:49:12	AUTHPRIV	Hinweis	Webconfig: login via HTTP from 192.168.2.4.
4	2014-07-14 12:38:17	AUTHPRIV	Hinweis	Webconfig: login via HTTP from 192.168.2.179.
5	2014-07-14 12:38:12	AUTHPRIV	Hinweis	Webconfig: login failure via HTTP from 192.168.2.179.
6	2014-07-13 15:23:53	KERN	Hinweis	SNTP: Local time set to 2014-07-13 13:23:53 (UTC)
7	2014-07-12 15:23:57	KERN	Hinweis	SNTP: Local time set to 2014-07-12 13:23:57 (UTC)
8	2014-07-11 16:24:03	AUTHPRIV	Hinweis	Webconfig: user logout from 89.0.95.133
9	2014-07-11 15:24:02	KERN	Hinweis	SNTP: Local time set to 2014-07-11 13:24:02 (UTC)
10	2014-07-11 15:12:55	AUTHPRIV	Hinweis	User from 192.168.2.231 via SSH logged out
11	2014-07-11 15:07:17	AUTHPRIV	Hinweis	Login from 192.168.2.231 via SSH
12	2014-07-11 15:06:37	AUTHPRIV	Hinweis	Webconfig: login via HTTP from 89.0.95.133.
13	2014-07-11 15:06:33	AUTHPRIV	Hinweis	Webconfig: login failure via HTTP from 89.0.95.133.

4.4.1 Aufbau der SYSLOG-Nachrichten

Die SYSLOG-Nachrichten bestehen aus drei Teilen:

- Priorität
- Header
- Inhalt

4.4.1.1 Priorität

Die Priorität einer SYSLOG-Meldung enthält Informationen über die Severity (den Schweregrad bzw. die Bedeutung einer Meldung) und die Facility (Dienst oder die Komponente, welche die Nachricht ausgelöst hat).

Die im SYSLOG ursprünglich definierten acht Severity-Stufen sind im Gerät auf fünf Stufen reduziert. Die nachfolgende Tabelle zeigt die Zuordnung zwischen dem Alarmlevel, Bedeutung und SYSLOG-Severities.

Priorität	Bedeutung	SYSLOG-Severity
Alarm	Hierunter werden alle Meldungen zusammengefasst, die der erhöhten Aufmerksamkeit des Administrators bedürfen.	PANIC, ALERT, CRIT
Fehler	Auf diesem Level werden alle Fehlermeldungen übermittelt, die auch im Normalbetrieb auftreten können, ohne dass ein Eingriff des Administrators notwendig wird (z. B. Verbindungsfehler).	ERROR
Warning	Dieser Level übermittelt Fehlermeldungen, die den ordnungsgemäßen Betrieb des Geräts nicht beeinträchtigen.	WARNING
Information	Auf diesem Level werden alle Nachrichten übermittelt, die rein informellen Charakter haben (z. B. Accounting-Informationen).	NOTICE, INFORM
Debug	Übertragung aller Debug-Meldungen. Debug-Meldungen erzeugen ein erhebliches Datenvolumen und beeinträchtigen den ordnungsgemäßen Betrieb des Geräts. Sie sollten daher im Regelbetrieb ausgeschaltet sein und nur zur Fehlersuche verwendet werden.	DEBUG

Die folgende Tabelle gibt eine Übersicht über die Bedeutung aller internen Nachrichtenquellen, die Sie im Gerät einstellen können. Zusätzlich gibt Ihnen die letzte Spalte der Tabelle die standardmäßige Zuordnung zwischen den internen Quellen des Geräts und den SYSLOG-Facilities an. Diese Zuordnung kann bei Bedarf verändert werden.

Quelle	Bedeutung	Facility
System	Systemmeldungen (Bootvorgänge, Timersystem etc.)	KERNEL

Quelle	Bedeutung	Facility
Logins	Meldungen sowohl über den erfolgreichen Verbindungsauf- und -abbau als auch über Login und Logout eines Users während der PPP-Verhandlung sowie dabei auftretende Fehler	AUTH
Systemzeit	Meldungen über Änderungen der Systemzeit	CRON
Konsolen-Logins	Meldungen über Konsolen-Logins (Telnet, Outband, etc), Logouts und dabei auftretende Fehler	AUTHPRIV
Verbindungen	Meldungen über auftretende Fehler beim Verbindungsauf- und -abbau (Display-Trace)	LOCAL0
Accounting	Accounting-Informationen nach dem Abbau einer Verbindung (User, Onlinezeit, Transfervolumen)	LOCAL1
Verwaltung	Meldungen über Konfigurationsänderungen, remote ausgeführte Kommandos etc.	LOCAL2
Router	Regelmäßige Statistiken über die am häufigsten genutzten Dienste (nach Portnummern aufgeschlüsselt) sowie Meldungen über gefilterte Pakete, Routing-Fehler etc.	LOCAL3

4.4.1.2 Header

Der Header beinhaltet den Namen oder die IP-Adresse des Gerätes, von dem die SYSLOG-Nachricht empfangen wurde. Für die Auswertung der Nachrichten ist auch die zeitliche Abfolge sehr wichtig. Um die zeitliche Konsistenz der Meldungen nicht durch unterschiedliche Gerätezeiten zu stören, wird die Zeitinformation erst beim SYSLOG-Client in die Nachrichten eingefügt.

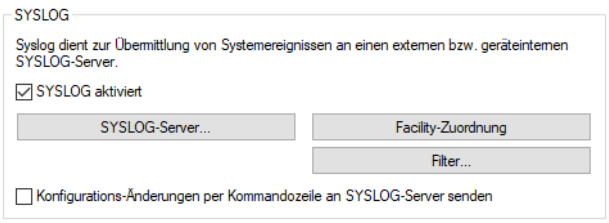
Für die Auswertung der SYSLOG-Meldungen im internen Speicher müssen die Geräte über eine gültige Zeitinformation verfügen.

4.4.1.3 Inhalt

Der eigentliche Inhalt der SYSLOG-Meldungen beschreibt das Ereignis, also z. B. einen Login-Vorgang, den Aufbau einer WAN-Verbindung oder die Aktivität der Firewall.

4.4.2 SYSLOG konfigurieren

In LANconfig konfigurieren Sie SYSLOG unter **Meldungen/Monitoring** > **Protokolle** im Abschnitt **SYSLOG**.



SYSLOG aktiviert

Aktivieren Sie das SYSLOG-Protokoll.

Konfigurations-Änderungen per Kommandozeile an SYSLOG-Server senden

Über das Kommandozeilen-Interface vorgenommene Konfigurations-Änderungen werden per SYSLOG an die eingerichteten Server gesendet.

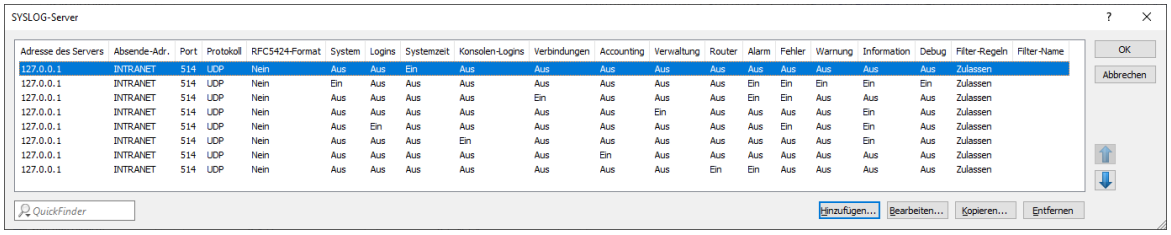
Diese Protokollierung umfasst ausschließlich die an der Konsole ausgeführten Befehle. Konfigurationsänderungen und Aktionen über LANconfig oder Webconfig sind davon nicht erfasst.

4.4.2.1 SYSLOG-Server

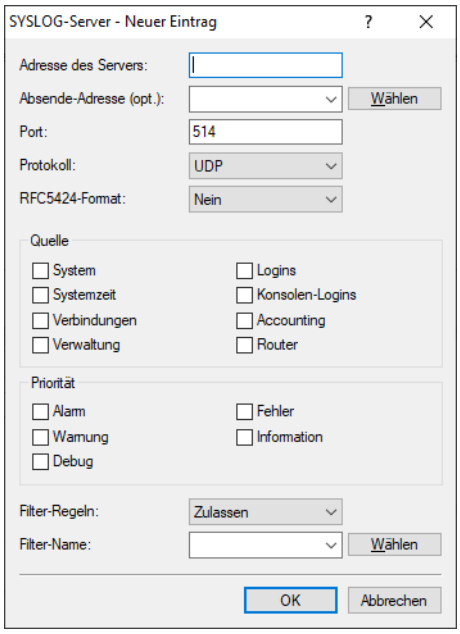
In LANconfig konfigurieren Sie die Einstellungen zum SYSLOG-Server unter **Meldungen/Monitoring** > **Protokolle** > **SYSLOG** über **SYSLOG-Server**.

Klicken Sie auf **SYSLOG-Server**, um die vorhandenen SYSLOG-Einträge anzuzeigen.

Die Tabelle der SYSLOG-Einträge ist im Auslieferungszustand mit sinnvollen Einstellungen vorbelegt, um wichtige Ereignisse für die Diagnose im internen SYSLOG-Speicher abzulegen. Diese Einstellungen entsprechen den Vorgaben aus der UNIX-Welt, aus der SYSLOG ursprünglich kommt. Der folgende Screenshot zeigt diese vordefinierten SYSLOG-Einträge unter LANconfig:



Klicken Sie auf **Hinzufügen** bzw. markieren Sie einen Eintrag und klicken Sie auf **Bearbeiten**.



Adresse des Servers

Legen Sie die IP-Adresse des SYSLOG-Servers fest. Die Angabe ist möglich in Form einer IPv4- / IPv6-Adresse oder eines Hostnamens.

Absende-Adresse (opt.)

Konfigurieren Sie optional eine Absende-Adresse, die der SYSLOG-Client statt der ansonsten automatisch für die Zieladresse gewählten Absende-Adresse verwendet. Falls Sie z. B. Loopback-Adressen konfiguriert haben, können Sie diese hier als Absende-Adresse angeben.

Port

Definiert die Portnummer (z. B. 514 für TCP / UDP).

Protokoll

Definiert das verwendete Protokoll. Mögliche Werte:

UDP

User Datagram Protocol

TCP

Transmission Control Protocol

TLS

Der Syslog-Client unterstützt drei Szenarien im TLS-Modus:

1. Der Syslog-Client akzeptiert alle TLS-Server-Zertifikate des Syslog-Servers. Dazu wird im Router kein vertrauenswürdiges CA-Zertifikat hinterlegt.
2. Der Syslog-Client akzeptiert nur Server-Zertifikate, die von einer vertrauenswürdigen CA signiert wurden. Dazu muss das CA-Zertifikat in den entsprechenden Zertifikatsslot des Routers hochgeladen werden.
3. Der Syslog-Client authentifiziert sich mit einem TLS-Client-Zertifikat beim Syslog-Server und der Syslog-Server authentifiziert sich mit seinem CA-Zertifikat. Dazu muss sowohl das TLS-Client-Zertifikat für den Router und das CA-Zertifikat in den entsprechenden Zertifikatsslot des Routers hochgeladen werden, z. B. in einem Container als PKCS#12-Datei.

Zertifikate für Syslog können entweder über die WEBconfig oder per LANconfig in das Gerät geladen werden.

- **LANconfig**:**Rechtsklick auf das Gerät** > **Konfigurationsverwaltung** > **Zertifikat oder Datei hochladen**
  - **Syslog - Container als PKCS12-Datei** oder
  - **Syslog - Root CA Zertifikat**
- **WEBconfig**: **Extras** > **Dateimanagement** > **Zertifikat oder Datei hochladen** > **Dateityp**
  - **Syslog - Container als PKCS12-Datei** oder
  - **Syslog - Root CA Zertifikat**

RFC5424-Format

Definiert, ob der Syslog-Client Nachrichten im RFC5424-Format an den Syslog-Server senden soll.

Quelle

Die folgende Tabelle gibt eine Übersicht über die Bedeutung aller Nachrichtenquellen, die Sie im Gerät einstellen können. Zusätzlich gibt Ihnen die letzte Spalte der Tabelle die Zuordnung zwischen den internen Quellen des Geräts und den SYSLOG-Facilities an.

Quelle	Bedeutung	Facility
System	Systemmeldungen (Bootvorgänge, Timersystem etc.)	KERNEL
Logins	Meldungen über Login und Logout eines Users während der PPP-Verhandlung sowie dabei auftretende Fehler	AUTH
Systemzeit	Meldungen über Änderungen der Systemzeit	CRON
Konsolen-Logins	Meldungen über Konsolen-Logins (Telnet, Outband, etc), Logouts und dabei auftretende Fehler	AUTHPRIV
Verbindungen	Meldungen über den Verbindungsauf- und -abbau sowie dabei auftretende Fehler (Display-Trace)	LOCAL0
Accounting	Accounting-Informationen nach dem Abbau einer Verbindung (User, Onlinezeit, Transfervolumen)	LOCAL1
Verwaltung	Meldungen über Konfigurationsänderungen, remote ausgeführte Kommandos etc.	LOCAL2
Router	Regelmäßige Statistiken über die am häufigsten genutzten Dienste (nach Portnummern aufgeschlüsselt) sowie Meldungen über gefilterte Pakete, Routing-Fehler etc.	LOCAL3

Priorität

Die im SYSLOG ursprünglich definierten acht Prioritätsstufen sind im Gerät auf fünf Stufen reduziert. Die nachfolgende Tabelle zeigt die Zuordnung zwischen Alarmlevel, Bedeutung und SYSLOG-Prioritäten.

Priorität	Bedeutung	SYSLOG-Priorität
Alarm	Hierunter werden alle Meldungen zusammengefasst, die der erhöhten Aufmerksamkeit des Administrators bedürfen.	PANIC, ALERT, CRIT
Fehler	Auf diesem Level werden alle Fehlermeldungen übermittelt, die auch im Normalbetrieb auftreten können, ohne dass ein Eingriff des Administrators notwendig wird (z. B. Verbindungsfehler).	ERROR
Warnung	Dieser Level übermittelt Fehlermeldungen, die den ordnungsgemäßen Betrieb des Geräts nicht beeinträchtigen.	WARNING
Information	Auf diesem Level werden alle Nachrichten übermittelt, die rein informellen Charakter haben (z. B. Accounting-Informationen).	NOTICE, INFORM
Debug	Übertragung aller Debug-Meldungen. Debug-Meldungen erzeugen ein erhebliches Datenvolumen und beeinträchtigen den ordnungsgemäßen Betrieb des Geräts. Sie sollten daher im Regelbetrieb ausgeschaltet sein und nur zur Fehlersuche verwendet werden.	DEBUG

Filter-Regeln

Werden die Syslog-Meldungen an einen oder mehrere Server übertragen, indem Einstellungen für den Empfang bestimmter Meldungen konfiguriert wurden, so werden alle konfigurierten Meldungen mit der konfigurierten Quelle und Priorität an die Server übertragen. Mitunter ist es jedoch wünschenswert, bestimmte Meldungen für die Server auszufiltern, nur bestimmte Meldungen überhaupt zu schicken oder auch deren Quelle und Priorität zu verändern, falls sie im Serverlog eine andere Gewichtung erhalten sollen. Der Syslog-Filter erlaubt es, Meldungen in Abhängigkeit von Quelle, Priorität und / oder Meldungstext zu filtern. Dabei stellen Sie hier ein, ob die Meldungen, die über den im folgenden Feld eingestellten Filter bestimmt werden, zugelassen oder abgelehnt werden.

Filter-Name

Wählen Sie einen der konfigurierten Filter aus.

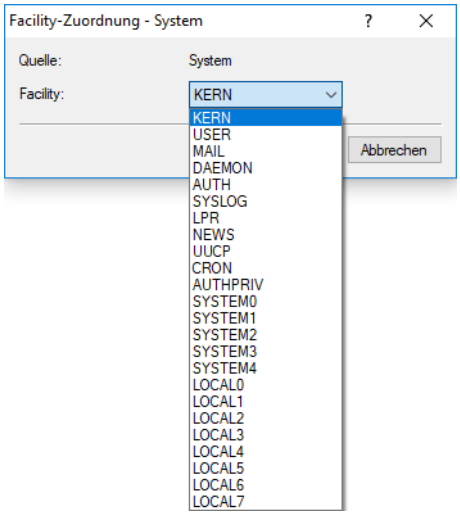
Wenn Sie alle Parameter definiert haben, bestätigen Sie die Eingaben mit **OK**. In der SYSLOG-Tabelle erscheint der SYSLOG-Client mit seinen Parametern.

4.4.2.2 SYSLOG-Facilities zuordnen

Das SYSLOG-Protokoll verwendet bestimmte Bezeichnungen für die Quellen der Nachrichten, die so genannten Facilities. Jede interne Quelle der Geräte, die eine SYSLOG-Nachricht erzeugen kann, muss daher einer SYSLOG-Facility zugeordnet sein.

Die standardmäßige Zuordnung ist bei Bedarf veränderbar. So lassen sich z. B. alle SYSLOG-Meldungen eines Geräts mit einer bestimmten Facility (Local7) versenden. Mit der entsprechenden Konfiguration des SYSLOG-Clients können Sie so alle Meldungen in einer gemeinsamen Log-Datei sammeln.

Über **Meldungen/Monitoring** > **Protokolle** lassen sich im Abschnitt **SYSLOG** unter **Facility-Zuordnung** die internen Quellen den entsprechenden SYSLOG-Facilities zuordnen.



Hier können Sie alle Meldungen vom Gerät einer Facility zuordnen und dadurch können diese vom SYSLOG-Client ohne zusätzlichen Aufwand in eine spezielle Log-Datei geschrieben werden.

Alle Facilities werden auf 'local7' gesetzt. Unter Linux werden nun in der Datei `/etc/syslog.conf` durch den Eintrag

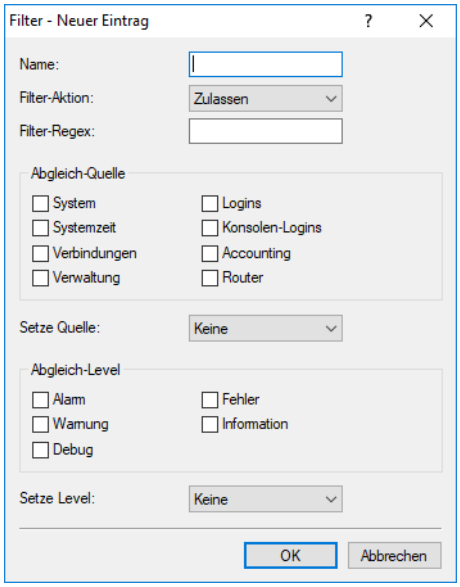
```
local7.* /var/log/lancom.log
```

alle Ausgaben des Geräts in die Datei `/var/log/lancom.log` geschrieben.

4.4.2.3 Filter

Werden die Syslog-Meldungen an einen oder mehrere Server übertragen, indem Einstellungen für den Empfang bestimmter Meldungen konfiguriert wurden, so werden alle konfigurierten Meldungen mit der konfigurierten Quelle und Priorität an die Server übertragen. Mitunter ist es jedoch wünschenswert, bestimmte Meldungen für die Server auszufiltern, nur bestimmte Meldungen überhaupt zu schicken oder auch deren Quelle und Priorität zu verändern, falls sie im Serverlog eine andere Gewichtung erhalten sollen. Der Syslog-Filter erlaubt es, Meldungen in Abhängigkeit von Quelle, Priorität und / oder Meldungstext zu filtern. Konfigurieren Sie hier diese Filter, die Sie dann bei Einträgen des SYSLOG-Servers verwenden können.

In LANconfig konfigurieren Sie die Filtereinstellungen zum SYSLOG-Server unter **Meldungen/Monitoring** > **Protokolle** > **SYSLOG** über **Filter**.



Name

Geben Sie diesem Filter einen aussagekräftigen Namen. Es können mehrere Regeln mit demselben Filter-Namen angelegt werden. Diese werden dann in der Reihenfolge, in der sie in der Filter-Tabelle angelegt werden, beim Versenden der Nachrichten geprüft. Trifft keine Regel in dieser Filterkette zu, wird die Nachricht gemäß der in der Server-Tabelle eingetragenen Default-Policy für den Server versendet oder verworfen.

Filter-Aktion

Aktion, falls die Regel zutrifft; „Zulassen" erlaubt das Versenden der Meldung an den Server, „Ablehnen" verwirft die Meldung.

Filter-Regex

Regulärer Ausdruck in Perl-Syntax (siehe z. B. *Regular expressions in Perl*), auf den der Meldungstext zutreffen muss. Ein leerer String bedeutet, dass der Meldungstext nicht betrachtet wird und daher alle Meldungstexte zutreffen.

Abgleich-Quelle

Quelle der Meldung, für die diese Regel gilt. Der Wert „keine" steht für eine beliebige Quelle.

Setze Quelle

Neue Quelle der Meldung, falls die Regel zutrifft. Der Wert „Keine" bedeutet, dass die Quelle nicht verändert wird.

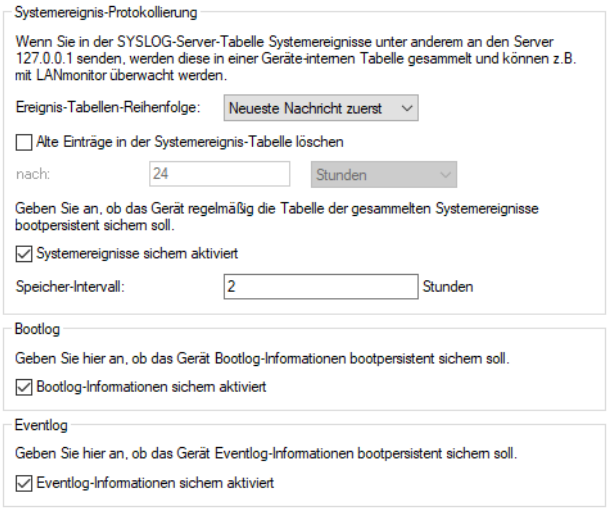
Abgleich-Level

Priorität der Meldung, für die diese Regel gilt. Der Wert „keine" steht für eine beliebige Priorität.

Setze Level

Neue Priorität der Meldung, falls die Regel zutrifft. Der Wert „Keine" bedeutet, dass die Priorität nicht verändert wird.

4.4.2.4 Systemereignis-Protokollierung



Speicherfrist von Systemereignissen festlegen

Unter **Meldungen/Monitoring** > **Systemereignisse** > **Systemereignis-Protokollierung** bestimmen Sie, für wie lange das Gerät Systemereignisse speichert. Markieren Sie dazu die Option **Alte Einträge in der Systemereignis-Tabelle löschen** und defnieren Sie eine Zeit (0-9999) in Stunden, Tagen oder Monaten.

Ein Monat entspricht hierbei 30 Tagen.

SYSLOG, Eventlog und Bootlog bootpersistent

Die Einstellungen für das bootpersistente Speichern von SYSLOG-, Eventlog- und Bootlog-Nachrichten finden Sie (sofern für Ihr Gerät verfügbar) unter **Meldungen/Monitoring** > **Systemereignisse** Aktivieren Sie dazu die folgenden Optionen:

- SYSLOG: **Systemereignisse sichern aktiviert**

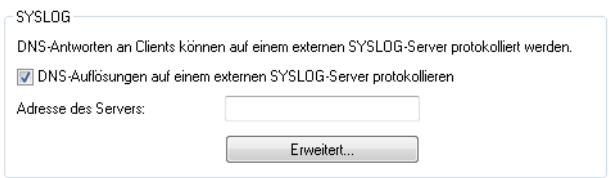
  Über den Eintrag **Speicher-Intervall** geben Sie die Zeitspanne in Stunden an, nach der die SYSLOG-Systemereignisse bootpersistent gesichert werden.
- Bootlog: **Bootlog-Informationen sichern aktiviert**
- Eventlog: **Eventlog-Informationen sichern aktiviert**

4.4.2.5 DNS-Anfragen und -Antworten an externen Syslog-Servern dokumentieren

Der DNS-Server in LANCOM Geräten löst DNS-Anfragen von Clients auf. Eine Übersicht darüber, welche Clients welche Namen angefragt und welche Antworten sie erhalten haben, steht im Syslog zur Verfügung.

Das Syslog des Routers / Access Points selbst kann nicht genutzt werden. Es ist daher erforderlich, einen externen Syslog-Server einzutragen.

Die Konfiguration des DNS-Loggings erfolgt im LANconfig unter **DNS** > **Allgemein** im Abschnitt **SYSLOG**.



DNS-Auflösungen auf einem externen SYSLOG-Server protokollieren

Markieren Sie diese Option, um das DNS-Logging zu aktivieren.

Diese Option ist unabhängig von der Einstellung im Syslog-Modul. Auch bei aktiviertem DNS-Logging und deaktiviertem Syslog-Modul (Einstellung unter **Meldungen** > **Allgemein** im Abschnitt **SYSLOG**) erfolgt das DNS-Logging.

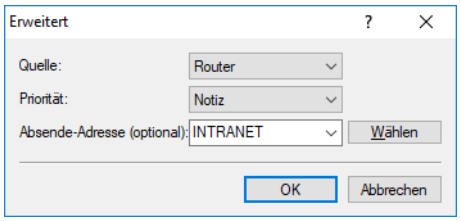
Die entsprechende SYSLOG-Meldung hat den folgenden Aufbau:

```
PACKET_INFO: DNS for <IP-Address>, TID {Hostname}: Resource-Record
```

Adresse des Servers

Enthält die IP-Adresse oder den DNS-Namen des zu nutzenden SYSLOG-Servers.

Die Einstellungen hinter der Schaltfläche **Erweitert** beeinflussen die Inhalte der SYSLOG-Meldungen.



Quelle

Enthält die Log-Quelle, die in den SYSLOG-Meldungen erscheint.

Priorität

Enthält den Log-Level, der in den SYSLOG-Meldungen erscheint.

Absende-Adresse (optional)

Enthält die Absende-Adresse, die in den SYSLOG-Meldungen erscheint.

4.4.3 Bedeutung von SYSLOG-Meldungen

4.4.3.1 Erweiterte Statusanzeige des Einbuchvorgangs ins Mobilfunknetz

Um Probleme bei der Verbindung in ein Mobilfunknetz schneller analysieren zu können, führen WWAN-fähige Router alle Einbuchvorgänge im SYSLOG auf. Somit kann der Anwender z. B. erkennen, ob und warum der Mobilfunkprovider eine Verbindung ablehnt.

Das Gerät erzeugt bei den folgenden Ereignissen je einen SYSLOG-Eintrag:

Status	Bedeutung	SYSLOG-Severity
WWAN: Currently not searching for network	Das Modem ist nicht eingebucht und sucht derzeit nicht nach einem Funknetz.	INFORM
WWAN: Searching for network	Das Modem ist nicht eingebucht und sucht nach einem Funknetz.	INFORM
WWAN: Registered to home network	Das Modem hat sich erfolgreich ins Funknetz seines Mobilfunkproviders eingebucht.	INFORM
WWAN: Registered to foreign network	Das Modem hat sich erfolgreich ins Funknetz eines Roaming-Partners seines Mobilfunkproviders eingebucht.	INFORM

Status	Bedeutung	SYSLOG-Severity
WWAN: Unknown registration	Initialwert. Das Modem hat noch keine Rückmeldung vom Funkmodul über den Einbuchungsstatus erhalten.	INFORM
WWAN: Network registration denied	Der Mobilfunkprovider hat die Einbuchung ins Funknetz abgelehnt.	ERROR
WWAN: Lost network registration	Das Modem hat die Verbindung zum eingebuchten Funknetz verloren.	NOTICE
WWAN: Failed to set network	Das Modem hat den Befehl zum Setzen des Netzwerks mit einer Fehlermeldung beantwortet. Dieser Fehler tritt z. B. auf, wenn das Netzwerk unerreichbar ist oder nicht existiert, oder ein Fehler im Gerät vorliegt.	ERROR
WWAN: Failed to set network mode	Das Modem hat den Befehl zum Setzen des Netzwerkmodus mit einer Fehlermeldung beantwortet. Dieser Fehler tritt z. B. auf, wenn das Netzwerk unerreichbar ist oder nicht existiert, oder ein Fehler im Gerät vorliegt.	ERROR
WWAN: Using modem '...'.	Zeigt das verwendete Modem an.	INFORM
WWAN: Modem is gone.	Modem ist nicht mehr verfügbar.	INFORM
WWAN: Resetting modem.	Re-Init durch Modem-Reset	WARNING
WWAN: Local disconnect.	D-Kanal-Disconnect	INFORM
WWAN: Local disconnect (Release).	D-Kanal-Release	INFORM
WWAN: Force 2G mode at ... dB.	Modem startet den 2G-Fallback	NOTICE
WWAN: Ending forced 2G mode.	Modem beendet den 2G-Fallback	INFO
WWAN: Forced 2G mode disabled.	Der 2G-Fallback-Modus ist deaktiviert.	INFO
WWAN: PIN missing in profile.	PIN fehlt im Profil.	ERROR
WWAN: PUK required.	Modem fordert PUK.	ERROR
WWAN: Invalid PIN.	Falsche PIN	ERROR
WWAN: Failed to set APN	Fehler beim Setzen des APN. Das Modem hat den Befehl zum Setzen eines APNs mit einer Fehlermeldung beantwortet. Dieser Fehler tritt z. B. auf, wenn das Netzwerk unerreichbar ist bzw. nicht existiert oder ein Fehler im Gerät vorliegt.	ERROR
WWAN: Using profile '...'.	Name des verwendeten Profils.	NOTICE
WWAN: Can not find profile '...'.	Profil nicht vorhanden.	ERROR
WWAN: Disonnected.	Physikalische Verbindung beendet.	INFORM
WWAN: Connected: '...'.	Das Modem hat eine Datenverbindung zum Netzwerk hergestellt und kann ab jetzt Daten über das Mobilfunk-Netzwerk übertragen.	INFORM
WWAN: Cell-ID is ..., Local Area Code is	Funkzellen-ID und Ländercode.	INFORM
WWAN: Current Network is '...'.	Netzwerk (Text)	INFORM
WWAN: Current Network is	Netzwerk (Nummer)	INFORM

Status	Bedeutung	SYSLOG-Severity
WWAN: Mode ..., Band '...'.	Anzeige von Netzwerk-Modus und Band	INFORM
WWAN: Mode ..., Band '...', Bandwith in MHz: ..., Channel (Rx/Tx): .../....	Anzeige von Netzwerk-Modus, Band, Bandbreite sowie Kanal (Empfangs- und Senderichtung).	INFORM
WWAN: Mode ..., Band '...', Channel (Rx/Tx): .../....	Anzeige von Netzwerk-Modus, Band sowie Kanal (Empfangs- und Senderichtung).	INFORM
WWAN: Max. Datarate (Ds/Us): .../....	Aktuelle QoS-Datenrate (Down- und Upstream)	INFORM
WWAN: Network mode is '...'.	Aktueller Modus. Mögliche Werte sind: › GPRS › EDGE › UMTS › HSPA › LTE	INFORM
WWAN: Signal strength is ... dBm.	Aktuelle Signalstärke	INFORM
WWAN: Using stored APN. APN: '...', PDP type:	Aktuell verwendeter Zugangspunkt im Netzwerk.	INFORM
WWAN: Setting new APN. APN: '...', PDP type:	Wechsel des Netzwerk-Zugangspunktes	INFORM
WWAN: Temperature is ...°C.	Aktuelle Modultemperatur	INFORM
WWAN: Temperature status: '...'.	Aktueller Temperaturstatus des Moduls. Mögliche Werte sind: › Normal › High Warning › High Critical › Low Critical	INFORM (Normal), WARNING (High Warning), CRITICAL (High Critical, Low Critical)
WWAN: Closing device: '...'.	Das Gerät, über das die Verbindung ins WAN läuft, fährt herunter.	INFORM
WWAN: Hangup: '...'.	Das Modem beendet die Netzwerk-Verbindung.	INFORM
WWAN: Error in modem init: '___'.	Bei der Initialisierung des Modems ist ein Fehler aufgetreten.	ERROR

4.4.3.2 Dokumentation von Ereignissen auf den xDSL-Schnittstellen

Das Gerät erzeugt bei den folgenden xDSL-Schnittstellen-Ereignissen je einen SYSLOG-Eintrag:

Status	Bedeutung	SYSLOG-Severity
xDSL: Booting modem: ...	Das Modem startet neu.	NOTICE
xDSL: Set up line to <Leitungsmodus>/<Leitungstyp>	Das xDSL-Modul baut die Verbindung mit dem angegebenen Modus und Typ auf. Folgende Werte sind möglich: › Leitungsmodus: Disabled, Auto sowie alle unter **Setup** > **Schnittstellen** > **ADSL-Interface bzw. VDSL-Interface** konfigurierbaren Modi. › Leitungstyp: POTS, ISDN	INFORM

Status	Bedeutung	SYSLOG-Severity
xDSL: Line is up. DS-Rate: ..., US-Rate: ..., DS-Margin: ..., US-Margin: ..., DS-Attn: ..., US-Attn: ..., Mode: ..., Profile:	Das Modem hat die Verbindung erfolgreich mit angegebenen Werten aufgebaut.	NOTICE
xDSL: Line data update. DS-Rate: ..., US-Rate: ..., DS-Margin: ..., US-Margin: ..., DS-Attn: ..., US-Attn: ..., Mode: ..., Profile: ...	Nach einer Synchronisation nehmen Modem und DSLAM eine Optimierung der xDSL-Verbindung vor. Dadurch können sich ggf. die Leitungswerte ändern. Nach einer Minute gibt das Modem die aktuellen Leitungswerte aus.	NOTICE
xDSL: Line data update.	Nach einer Synchronisation nehmen Modem und DSLAM eine Optimierung der xDSL-Verbindung vor. Nach einer Minute gibt das Modem diese Meldung aus, wenn sich die Leitungswerte nach der Synchronisation nicht geändert haben.	NOTICE
xDSL: Line disconnected due to	Die Verbindung ist aus dem angegebenem Grund abgebrochen. Folgende Werte sind möglich: › modem reboot › retrain › silence › high line error rate › protocol setting › line type setting › automode line type switch › modem timeout › VC parameter change	NOTICE
xDSL: SNR margin (dB, Down/Up): .../...	Der Wert zwischen notwendigem und gemessenem Signal-Rausch-Abstand (SNR) hat sich um mehr als 1dB geändert.	INFORM

4.5 Übersicht der Parameter im ping-Befehl

Das ping-Kommando an der Eingabeaufforderung einer Terminal-Verbindung sendet ein „ICMP Echo-Request"-Paket an die Zieladresse des zu überprüfenden Hosts. Wenn der Empfänger das Protokoll unterstützt und es nicht in der Firewall gefiltert wird, antwortet der angesprochene Host mit einem „ICMP Echo-Reply". Ist der Zielrechner nicht erreichbar, antwortet das letzte Gerät vor dem Host mit „Network unreachable" (Netzwerk nicht erreichbar) oder „Host unreachable" (Gegenstelle nicht erreichbar).

Die Syntax des ping-Kommandos lautet wie folgt:

```
ping [-46dfnoqrmb] [-s n] [-i n] [-c n] [-x x][-p <dscp>][-a ...] destination [%scope] [%scope@rtg-tag] [%%interface] [@rtg-tag]
```

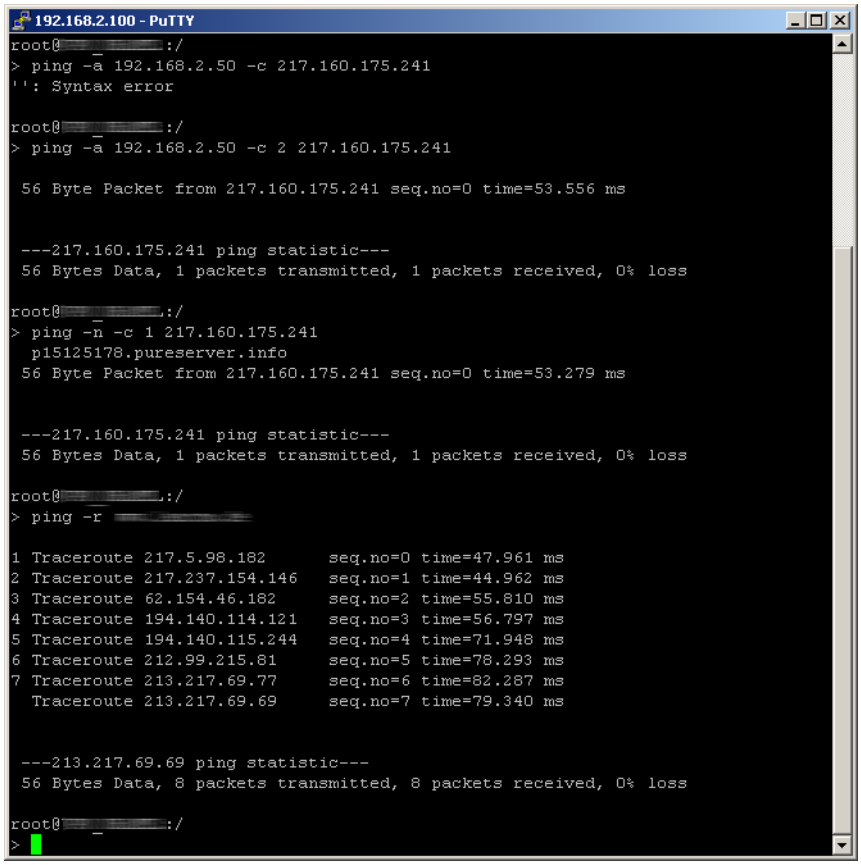
Die Bedeutung der optionalen Parameter können Sie der folgenden Tabelle entnehmen:

Tabelle 23: Übersicht aller optionalen Parameter im ping-Befehl

Parameter	Bedeutung
`-4`	Verwendung von IPv4 erzwingen

Parameter	Bedeutung
`-6`	Verwendung von IPv6 erzwingen
`-d`	Fragmentierung verbieten
`-f`	flood ping: Sendet eine große Anzahl von ping-Signalen in kurzer Zeit. Kann z. B. zum Testen der Netzwerkbandbreite genutzt werden. flood ping kann leicht als Denial-of-Service-Angriff (DoS) fehlinterpretiert werden.
`-n`	Liefert den Computernamen zu einer eingegebenen IP-Adresse zurück.
`-o`	Schickt nach einer Antwort sofort eine weitere Anfrage.
`-q`	ping-Kommando liefert keine Ausgaben auf der Konsole.
`-r`	Wechselt in den traceroute-Modus: Der Weg der Datenpakete zum Zielcomputer wird mit allen Zwischenstationen angezeigt.
`-m`	Wechselt in den tracepath-Modus zur Ermittlung der Pfad-MTU zu der angegebenen IP-Adresse.
`-b`	Nicht aufhören zu pingen, wenn ein PacketTooBig(DF) empfangen wird, damit man „Path MTU Discovery" hat.
`-s n`	Setze Größe der Pakete auf n Byte (max. 65500).
`-i n`	Zeit zwischen den einzelnen Paketen in Sekunden.
`-c n`	Sende n Ping-Signale.
`[-x x]`	Atomare Fragmente: (n)ever, (f)orce, (a)automatic
`[-p <dscp>]`	Verwende einen spezifischen DSCP-Wert für diesen Ping. DSCP (Differentiated Services Code Point) wird für QoS (Quality of Service) verwendet. Mögliche DSCP-Werte: BE/CS0, CS1, CS2, CS3, CS4, CS5, CS6, CS7, AF11, AF12, AF13, AF21, AF22, AF23, AF31, AF32, AF33, AF41, AF42, AF43, EF
`-a a.b.c.d`	Setzt die Absenderadresse des Pings (Standard: IP-Adresse des Gerätes)
`-a <name>`	Verwendet ein benanntes Netzwerk, Interface oder Loopback-Adresse als Absendeadresse
`-l <Load-Balancer-Policy>`	Wenn das Ping-Ziel über einen Load Balancer erreichbar ist, wird beim Versand der Pings anhand der Policy eine Load-Balancer-Entscheidung getroffen. Mögliche Werte sind Default, Traffic, Bandwidth, Round-Robin, Most-Used sowie alle definierten Dynamic-Path-Selection-Policies. Die Angabe einer ungültigen Policy sorgt dafür, dass keine Pings versendet werden können Es ist nicht möglich, diese Kommandozeilen-Option zusammen mit der Angabe eines Scopes oder einer Interface-Bindung in der Destination zu verwenden.
`-6 <IPv6-Address>%<Scope>`	Führt ein Ping-Kommando über das mit <Scope> bestimmte Interface auf die Link-Lokale-Adresse aus. Der Parameter-Bereich ist bei IPv6 von zentraler Bedeutung: Da ein IPv6-Gerät sich mit mehreren Schnittstellen (logisch oder physikalisch) pro Schnittstelle eine Link-Lokale-Adresse (fe80::/10) teilt, müssen Sie beim Ping auf eine Link-Lokale-Adresse immer den Bereich (Scope) angeben. Nur so kann das Ping-Kommando die Schnittstelle bestimmen, über die es das Paket senden soll. Den Namen der Schnittstelle trennen Sie durch ein Prozentzeichen (%) von der IPv6-Adresse. **Beispiele:**

Parameter	Bedeutung
	› `ping -6 fe80::1%INTRANET` Ping auf die Link-Lokale-Adresse „fe80::1“, die über die Schnittstelle bzw. das Netz „INTRANET“ zu erreichen ist. › `ping -6 2001:db8::1` Ping auf die globale IPv6-Adresse „2001:db8::1“.
`destination`	Adresse oder Hostname des Zielcomputers.
`%scope`	Name des Interfaces über welches das Paket bei der Verwendung von Link-Lokalen-Adressen als Ziel versendet werden soll.
`%scope@rtg-tag`	Name des Interfaces über welches das Paket bei der Verwendung von Link-Lokalen-Adressen als Ziel versendet werden soll mit zusätzlicher Angabe des Routing-Tags.
`%%interface`	Name des Ziel-Interfaces. Das Paket wird direkt und ohne Berücksichtigung der Routing-Tabelle an das Interface gesendet.
`@rtg-tag`	Routing-Tag, das zum Senden des Pakets verwendet werden soll.
`stop /<RETURN>`	Die Eingabe von `stop` oder das Drücken der RETURN-Taste beenden das Ping-Kommando.

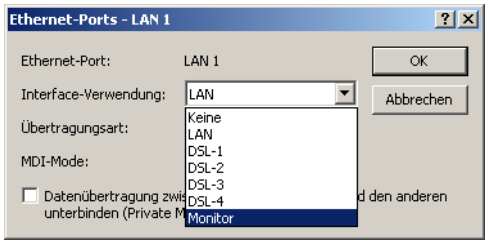


4.6 Monitor-Modus am Switch

Die über den Switch der Geräte übertragenen Daten werden zielgerichtet nur auf den Port aufgelegt, an dem der entsprechende Zielrechner angeschlossen ist. An den anderen Ports sind diese Verbindungen daher nicht sichtbar.

Um den Datenverkehr zwischen den einzelnen Ports mithören zu können, können die Ports in den Monitor-Modus geschaltet werden. In diesem Zustand werden auf diesen Ports alle Daten ausgegeben, die zwischen Stationen im LAN und WAN über den Switch des Gerätes ausgetauscht werden.

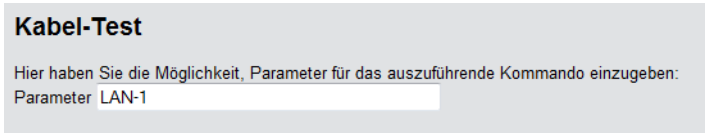
Bei der Konfiguration mit LANconfig öffnen Sie die Ethernet-Switch-Einstellungen unter **Interfaces** > **LAN** mit der Schaltfläche **Ethernet-Ports**.



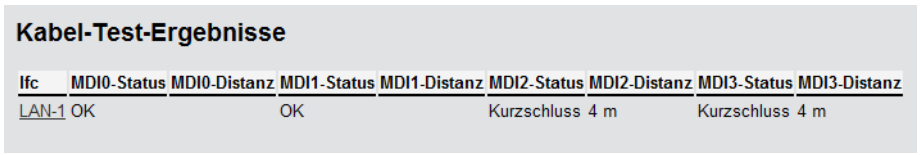
4.7 Kabel-Test

Werden auf Ihren LAN- oder WAN-Verbindungen gar keine Daten übertragen, obwohl die Konfiguration der Geräte keine erkennbaren Fehler aufweist, liegt möglicherweise ein Defekt in der Verkabelung vor.

Mit dem Kabel-Test können Sie aus dem Gerät heraus die Verkabelung testen. Wechseln Sie dazu unter WEBconfig in den Menüpunkt **Extras** > **LCOS-Menübaum** > **Status** > **LAN** > **Kabel-Test**. Geben Sie dort die Bezeichnung des Interfaces ein, das Sie testen wollen (z. B. "DSL1" oder "LAN-1"). Achten Sie dabei auf die genaue Schreibweise der Interfaces. Mit einem Klick auf die Schaltfläche **Ausführen** starten Sie den Test für das eingetragene Interface.



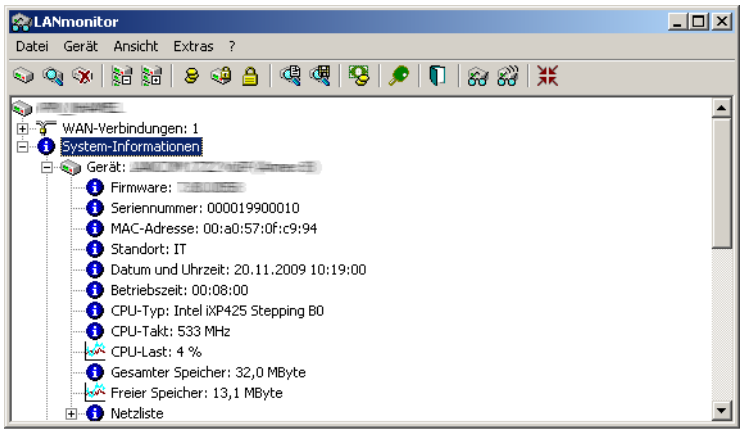
Wechseln Sie anschließend in den Menüpunkt **Extras** > **LCOS-Menübaum** > **Status** > **LAN** > **Kabel-Test-Ergebnisse**. In der Liste sehen Sie die Ergebnisse, die der Kabel-Test für die einzelnen Interfaces ergeben hat.



4.8 Mittelwert der CPU-Lastanzeige

4.8.1 Einleitung

Die aktuelle CPU-Last der Geräte wird über verschiedene Ausgabemöglichkeiten angezeigt (LANmonitor, über WEBconfig oder CLI im Status-Bereich, bei einigen Modellen im Display).



4.8.2 Konfiguration

Je nach Bedarf können Sie einstellen, über welchen Zeitraum die angezeigte CPU-Last gemittelt werden soll.

Konsole: **Setup** > **Config**

CPU-Last-Intervall

Hier können Sie die den Zeitraum zur Mittelung der CPU-Lastanzeige auswählen. Die Anzeige der CPU-Last im LANmonitor, im Status-Bereich, im Display (sofern vorhanden) sowie in evtl. genutzten SNMP-Tools basiert auf dem hier eingestellten Mittelungszeitraum. Im Status-Bereich unter WEBconfig oder CLI werden zusätzlich die CPU-Lastwerte für alle vier möglichen Mittelungszeiträume angezeigt.

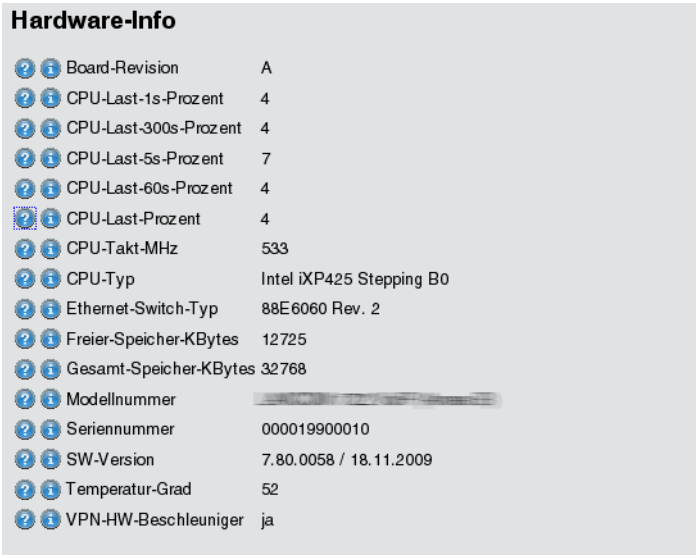
Mögliche Werte:

- 1, 5, 60 oder 300 Sekunden.

Default:

- 60 Sekunden.

Die defaultmäßige Mittelung über 60 Sekunden ist in der HOST-RESOURCES-MIB vorgeschrieben, die von gängigen SNMP-Tools zur Anzeige der CPU-Last in einem Tacho-Display verwendet wird. Bitte beachten Sie diese Vorgabe bei der Anpassung des CPU-Last-Intervalls.



4.9 Versand von Anhängen mit dem mailto-Kommando

Mit dem mailto-Kommando in den Einträgen der Aktionstabelle oder Cron-Tabelle können bei bestimmten Ereignissen automatisch E-Mails mit Informationen über den Zustand der Geräte verschickt werden.

Mit der Erweiterung um Anhänge in den E-Mails können vor dem Versand der Mail beliebige Konsolen-Befehle auf dem Gerät ausgeführt werden, deren Ergebnisse dann als Anhang mit der Mail verschickt werden. So lassen sich auch Inhalte von Tabellen oder Menüs (z. B. umfangreiche Statusmeldungen) per Mail versenden.

› Aktion (Aktionstabelle) oder Befehl (Cron-Tabelle) (max. 250 Zeichen)

Hier beschreiben Sie die Aktion, die beim Zustandswechsel der WAN-Verbindung bzw. beim Erreichen der definierten Zeit ausgeführt werden soll. In jedem Eintrag darf nur eine Aktion ausgeführt werden.

Mögliche Werte für die Aktionen (maximal 250 Zeichen):

› mailto: – Mit diesem Prefix lösen Sie den Versand einer E-Mail aus.

Mögliche Variablen zur Erweiterung der Aktionen:

› attach=`Konsolen-Befehl`

Als Konsolen-Befehl können beliebige Befehle auf der Konsole genutzt werden, die zu einer sinnvollen Ausgabe von Informationen führen. Der Konsolen-Befehl wird in Backquotes (auch bekannt als Backticks) eingefasst. Dieses Zeichen wird mit Hilfe der Taste für den „Accent Grave" erzeugt.

Die Ausgabe des Konsolenbefehls wird in eine Text-Datei geschrieben und an die Mail angehängt. Vor die Ausgaben wird in den angehängten Text automatisch das Kommando und ein Zeit / Datumsstempel eingesetzt.

Default:

› leer

Beispiele:

Mit der folgenden Aktion können Sie den ADSL-Status per E-Mail versenden:

```
mailto:admin@mycompany.de?subject=ADSL-Status?attach=`dir /status/adsl`
```

Mit einer Aktion können auch durchaus mehrere Konsolenbefehle verschickt werden:

```
mailto:admin@mycompany.de?subject=Statusmeldungen?attach=`dir /status/adsl`?attach=`dir /status/config`
```

Die angehängten Texte werden als 'cmd1.txt', 'cmd2.txt' usw. bezeichnet.

4.10 Erweiterung der Sysinfo

Um Änderungen der Konfiguration feststellen und den Zeitpunkt einer Änderung nachvollziehen zu können, enthält Sysinfo im Feld CONFIG_STATUS zusätzliche Einträge.

Die Geräte speichern den Wert CONFIG_STATUS bei jeder Änderung der Konfiguration (per Konsole, per SNMP oder durch das Laden von Skripten oder kompletten Konfigurationen). Der Wert CONFIG_STATUS besteht aus den folgenden Komponenten:

- Hash-Wert der Gerätekonfiguration als eindeutiges Merkmal eines Konfigurationsstandes.
- Zeitstempel der letzten Konfigurationsänderung im Format HHMMSSddmmyyyy auf Basis der koordinierten Weltzeit UTC. Der Bezug auf UTC garantiert eindeutige Werte ohne Einfluss von Standort oder Sommerzeiteinstellung.
- Zähler für die Konfigurationsänderungen, fortlaufend.

Das Feld CONFIG_STATUS enthält neben einem Wert für Statusschalter der Konfiguration und einem Wert für den Status zum Flashen der Konfiguration die zusätzlichen Komponenten in der Form <Hash>.<Datum>.<Zähler>.

Sie können die Änderungen an der Konfiguration sowohl in entsprechenden Dateien oder Skripten (z. B. mit LANtools) als auch auf den Geräten direkt vornehmen (Konsole oder WEBconfig). Der Weg der Konfigurationsänderung hat dabei teilweise Einfluss auf den Inhalt des CONFIG_STATUS.

Hash-Wert der Gerätekonfiguration

Nur LCOS – das Betriebssystem der Geräte – kann den Hash-Wert berechnen. Der Hash-Wert ist für jeden Konfigurationsstand unterschiedlich, ein veränderter Hash-Wert auf einem Gerät zeigt so eine geänderte Konfiguration an.

LCOS speichert den berechneten Hash-Wert während des Flash-Vorgangs in das Gerät.

Zeitstempel der letzten Konfigurationsänderung

Sowohl LCOS als auch die LANtools können den Zeitstempel setzen, sofern sie über eine gültige Uhrzeit verfügen.

Sofern der gewählte Konfigurationsweg nicht über eine gültige Uhrzeit verfügt, setzt das Gerät den Zeitstempel auf den Wert '00:00:00 0000-00-00'.

Zähler für die Konfigurationsänderungen

Bei der Auslieferung der Geräte enthält der Zähler für die Konfigurationsänderungen den Wert '0'. Danach erhöht jede Konfigurationsänderung diesen Wert um 1. Der Zähler für die Konfigurationsänderungen erlaubt die Ermittlung der aktuellen Konfigurationsversion auch dann, wenn bei der Konfiguration keine gültige Uhrzeit verfügbar war und der Zeitstempel daher den Wert '00:00:00 0000-00-00' enthält.

Ein Konfigurationszähler mit dem Wert '0' nach einer Änderung der Konfiguration deutet auf einen Fehler beim Lesen oder Schreiben des Zählers im Flash hin.

Anzeige des CONFIG_STATUS

Geben Sie zur Anzeige des Wertes CONFIG_STATUS an der Konsole des Gerätes den Befehl `sysinfo` ein.

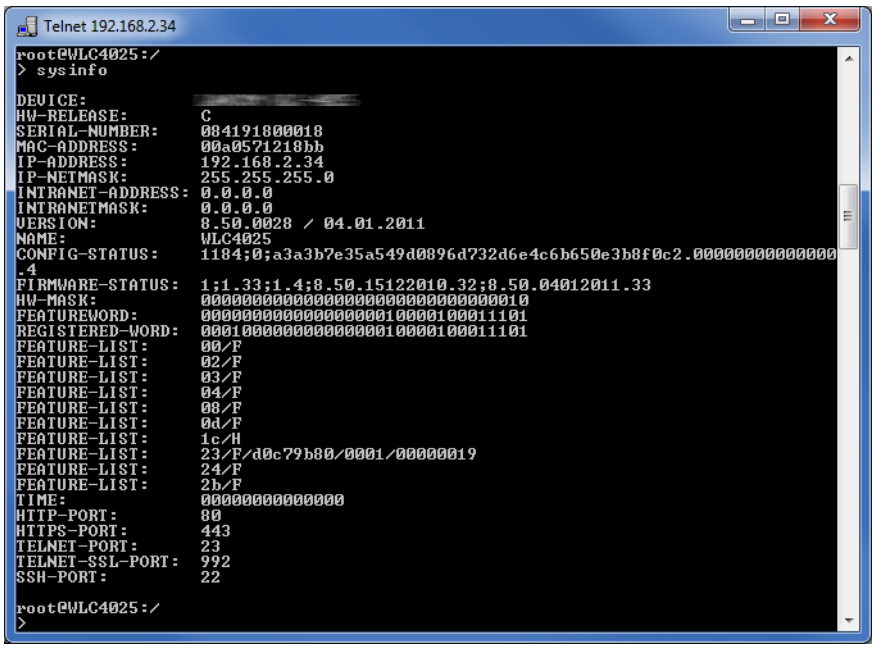


Abbildung 1: Anzeige der Systeminformationen auf der Konsole

4.10.1 Ausgabe zusätzlicher Ports im SYSINFO an der Konsole

Ab LCOS-Version 9.00 überträgt der Befehl `sysinfo` auch die Nummern der folgenden Ports:

- HTTP
- HTTPS
- TELNET
- TELNET-SSL
- SSH
- SNMP
- TFTP

4.10.2 Ausgabe des Konfigurations-Datums

Ab LCOS-Version 9.10 haben Sie die Möglichkeit, über `status/config/config-date` das Datum und die Uhrzeit der Geräte-Konfiguration auszulesen.

SNMP-ID: 1.11.20

```
root@LANCOM_1781AW:/Status/Config
> ls

LAN-Active-Connections      INFO:    1
LAN-Total-Connections       INFO:    7
WAN-Active-Connections      INFO:    0
WAN-Total-Connections       INFO:    0
Outband-Active-Connections  INFO:    0
Outband-total-Connections   INFO:    0
Outband-Bitrate             INFO:    115200
Login-Errors                INFO:    0
Login-Locks                 INFO:    0
Login-Rejects               INFO:    0
Start-Scan                  ACTION:
Scan-Results                TABINFO: 0 x [IP-Address,Rtg-tag,Name,..]
Features                    TABINFO: 7 x [Feature,Expires,State,Index,Count]
Anti-Theft-Protection       MENU:
Delete-Values               ACTION:
Event-Log                   TABINFO: 64 x [Idx.,System-time,Event,Access,..]
Config-Date                 INFO:    03/25/2014 06:47:12
Config-Hash                 INFO:    cbba4fc366a8ae2b71d35e1ce58ee8f496588cf9
Config-Version              INFO:    126
Script-Log                  TABINFO: 8+ x [Index,Time,Comment,Successful,..]
```

Die Werte werden im UTC-Format angezeigt.

4.10.3 Ausgabe des Konfigurations-Hashs

Ab LCOS-Version 9.10 haben Sie die Möglichkeit, über `status/config/config-hash` den Hash-Wert der Geräte-Konfiguration auszulesen.

SNMP-ID: 1.11.21

```
root@LANCOM_1781AW:/Status/Config
> ls

LAN-Active-Connections      INFO:    1
LAN-Total-Connections       INFO:    7
WAN-Active-Connections      INFO:    0
WAN-Total-Connections       INFO:    0
Outband-Active-Connections  INFO:    0
Outband-total-Connections   INFO:    0
Outband-Bitrate             INFO:    115200
Login-Errors                INFO:    0
Login-Locks                 INFO:    0
Login-Rejects               INFO:    0
Start-Scan                  ACTION:
Scan-Results                TABINFO: 0 x [IP-Address,Rtg-tag,Name,..]
Features                    TABINFO: 7 x [Feature,Expires,State,Index,Count]
Anti-Theft-Protection       MENU:
Delete-Values               ACTION:
Event-Log                   TABINFO: 64 x [Idx.,System-time,Event,Access,..]
Config-Date                 INFO:    03/25/2014 06:47:12
Config-Hash                 INFO:    cbba4fc366a8ae2b71d35e1ce58ee8f496588cf9
Config-Version              INFO:    126
Script-Log                  TABINFO: 8+ x [Index,Time,Comment,Successful,..]
```

Bei dem angezeigten Wert handelt es sich um einen SHA1-Hash.

4.10.4 Ausgabe der Konfigurations-Version

Ab LCOS-Version 9.10 haben Sie die Möglichkeit, über `status/config/config-version` die Versionsnummer der Geräte-Konfiguration auszulesen.

SNMP-ID: 1.11.22

```
root@LANCOM_1781AW:/Status/Config
> ls

LAN-Active-Connections      INFO:    1
LAN-Total-Connections       INFO:    7
WAN-Active-Connections      INFO:    0
WAN-Total-Connections       INFO:    0
Outband-Active-Connections  INFO:    0
Outband-total-Connections   INFO:    0
Outband-Bitrate             INFO:    115200
Login-Errors                INFO:    0
Login-Locks                 INFO:    0
Login-Rejects               INFO:    0
Start-Scan                  ACTION:
Scan-Results                TABINFO: 0 x [IP-Address,Rtg-tag,Name,..]
Features                    TABINFO: 7 x [Feature,Expires,State,Index,Count]
Anti-Theft-Protection       MENU:
Delete-Values               ACTION:
Event-Log                   TABINFO: 64 x [Idx.,System-time,Event,Access,..]
Config-Date                 INFO:    03/25/2014 06:47:12
Config-Hash                 INFO:    cbba4fc366a8ae2b71d35e1ce58ee8f496588cf9
Config-Version              INFO:    126
Script-Log                  TABINFO: 8+ x [Index,Time,Comment,Successful,..]
```

4.11 Bandbreiten-Messung mit iPerf

Die Messung der Netzwerkperformance ermittelt Werte wie Datendurchsatz, Verzögerung, Jitter und Fehlerraten einer Netzwerkverbindung. Die gemessenen Werte dienen u. a. der Netzwerkoptimierung, der Fehlererkennung und -beseitigung sowie der Beurteilung der Leistungsfähigkeit einer Netzwerkinfrastruktur.

Als freie Software zur Erzeugung und Auswertung von definierten Datenströmen auf bestimmten Verbindungen hat sich iPerf etabliert. Ein iPerf-Server-Daemon empfängt TCP- und UDP-Streams und misst den Datendurchsatz für die entsprechenden Anwendungen sowie Verzögerung, Jitter, Verlust und Neuanordnung von Datenpaketen bei UDP-Verbindungen.

Zur Bandbreitenmessung zwischen zwei Hosts startet man den iPerf-Server auf dem einen und den iPerf-Client auf dem anderen Gerät. Der iPerf-Client verbindet sich daraufhin mit dem iPerf-Server. Server und Client tauschen für eine bestimmte Zeit oder eine bestimmte Datenmenge Datenpakete untereinander aus und erzeugen darüber eine Statistik. Diese Statistik gibt Auskünft über die Qualität der Verbindung zwischen beiden Gegenstellen.

Bei der Messung der TCP-Verbindungsqualität sendet der iPerf-Client so schnell wie möglich komplett gefüllte TCP-Datenpakete. Die durchschnittliche Datenrate für den erfolgreichen Datentransfer („goodput“) ist das Ergebnis dessen, was der iPerf-Server fehlerfrei empfangen hat.

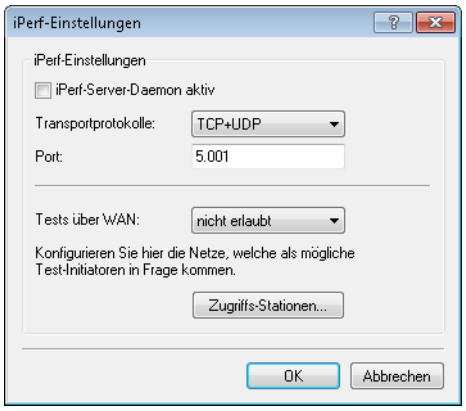
Bei der Messung der UDP-Verbindungsqualität überträgt der iPerf-Client Daten über eine definierte Bandbreite (standardmäßig 1 Mbit/s), allerdings ohne Fluss- oder Leistungskontrolle. Der „goodput“ orientiert sich an der maximalen Bandbreite, bei der der Übertragungspuffer des Clients dauerhaft und ohne den Verlust von Datenpaketen gefüllt ist.

LANCOM Geräte beinhalten eine iPerf2-kompatible Funktion zur Messung der Netzwerkperformance direkt zwischen den Netzwerkzugangspunkten (z. B. Router, VPN-Gateway, AP). Damit vereinfacht sich die Messung z. B. des Datendurchsatzes über WAN- oder WLAN-Point-to-Point-Verbindungen.

Sowohl die Messung zwischen zwei LANCOM Geräten als auch die Messung zwischen einem LANCOM Gerät und einer anderen iPerf2-Instanz ist möglich.

4.11.1 iPerf mit LANconfig einrichten

Mit LANconfig konfigurieren Sie iPerf unter **Meldungen** > **Allgemein** mit einem Klick auf **iPerf-Einstellungen**.



iPerf-Server-Daemon aktiv

Aktiviert bzw. deaktiviert den iPerf-Server-Daemon.

Statt den iPerf-Server an dieser Stelle dauerhaft einzurichten, besteht die Möglichkeit, über die Konsole via SSH-Verbindung für einen einzelnen Test auch nur einen temporären iPerf-Server zu starten.

Transportprotokolle

Bestimmen Sie hier, über welche Übertragungsprotokolle das Gerät die Bandbreite messen soll.

Port

Über diesen Port kommunizieren iPerf-Client und -Server (standardmäßig „5001“).

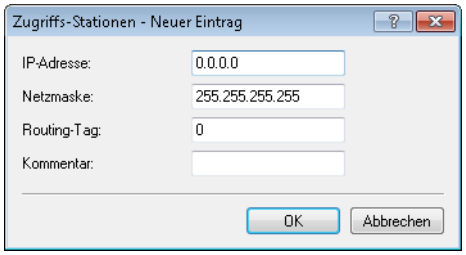
Tests über WAN

Bestimmen Sie, ob die Messung auch über eine WAN-Verbindung erfolgen darf.

Bei Messungen über WAN-Verbindungen können je nach Providervertrag zusätzliche Verbindungskosten entstehen.

Zugriffs-Stationen

Um den iPerf-Zugriff auf bestimmte Stationen zu begrenzen, tragen Sie deren Verbindungsdaten in diese Tabelle ein.



IP-Adresse

Geben Sie die IPv4-Adresse der entfernten Station ein.

Netzmaske

Geben Sie die Netzmaske für die entfernte Station ein.

Routing-Tag

Tragen Sie hier die das Routing-Tag ein, das die Verbindung zur entfernten Station definiert.

Kommentar

Geben Sie eine aussagekräftige Beschreibung für diesen Eintrag an.

4.11.2 Temporärer iPerf-Server und -Client

Bei der iPerf-Konfiguration über LANconfig ist die iPerf-Funktion dauerhaft aktiv. Es besteht die Möglichkeit, mit der Konsole über eine SSH-Verbindung einen temporären iPerf-Daemon zu starten, der nur für die Dauer eines Tests aktiv ist.

Starten Sie dazu ein Terminalprogramm (z. B. PuTTY) und öffnen Sie die Verbindung zum Gerät, auf dem Sie die iPerf-Funktion aktivieren möchten. Mit dem Konsolenbefehl `iperf` und den entsprechenden Optionsschaltern konfigurieren Sie den temporären iPerf-Daemon. Die folgenden Konsolenbeispiele erläutern einige Standardbefehle.



Mehr Informationen über die Optionsschalter bei `iperf` finden Sie im Abschnitt *Befehle für die Konsole*.

iPerf-Server im TCP-Modus starten

```
root@device:/Setup/Iperf/Server-Daemon
> iperf -s
[Iperf-TCP-Server|1526] Now listening on port 5001
```

Drücken Sie erneut die Enter-Taste oder schließen Sie das Konsolenfenster, um den iPerf-Server zu beenden.

iPerf-Server im UDP-Modus starten

```
root@device:/Setup/Iperf/Server-Daemon
> iperf -s -u
[Iperf-UDP-Server|1524] Now listening on port 5001
```

Drücken Sie erneut die Enter-Taste oder schließen Sie das Konsolenfenster, um den iPerf-Server zu beenden.

iPerf-Client im UDP-Modus starten

```
root@device:/Setup/Iperf/Server-Daemon
> iperf -u -c 172.16.30.23
WARN: Using default UPD bandwidth limitation of 1 MBit/s
WARN: Using default UDP payload length of 1472 bytes (for matching Ethernet MTU via IPv4)
[Iperf-UDP-Client|2100] Connecting to server...
[Iperf-UDP-Client|2100] Connection established to 172.16.30.23:5001

root@device:/
>
```

Drücken Sie die Enter-Taste, um den Test zu beenden.

```
[Iperf-UDP-Client|2100] Connection closed actively
[Iperf-UDP-Client|2100] Sent 1249728 bytes within 10s (10000ms) -> 0 Mbit/s (999 Kbit/s)
[Iperf-UDP-Client|2100] Server reports 1249728 bytes received within 9s (9985ms) -> 1 Mbit/s (1001
Kbit/s)
[Iperf-UDP-Client|2100] Server received 849 packets (0 lost / 0 out-of-order) with 62us jitter

root@device:/
>
```

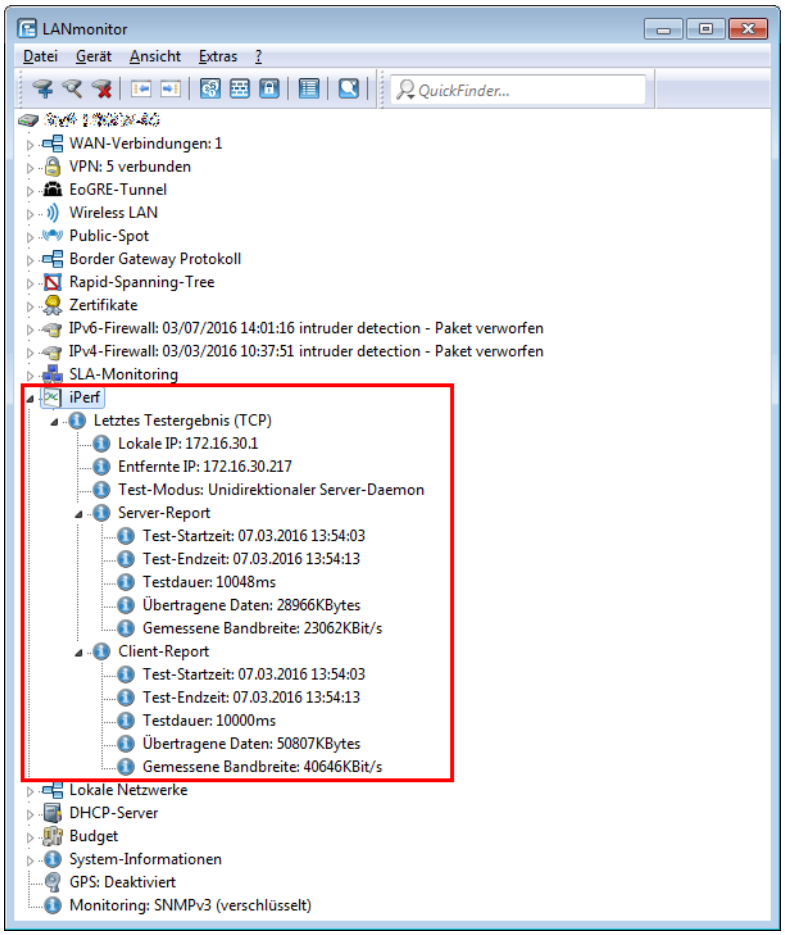
4.11.3 iPerf-Ergebnisse mit LANmonitor auswerten

LANCOM-Geräte beinhalten eine iPerf2-kompatible Funktion zur Messung der Netzwerkperformance direkt zwischen den Netzwerkzugangspunkten (z. B. Router, VPN-Gateway, AP). Damit vereinfacht sich die Messung z. B. des Datendurchsatzes über WAN- oder WLAN-Point-to-Point-Verbindungen.



Mehr Informationen zu iPerf finden Sie im Abschnitt *Bandbreiten-Messung mit iPerf*.

Das letzte iPerf-Testergebnis lässt sich auch im LANmonitor unter „iPerf“ anzeigen. Dabei ist es egal, ob das Gerät eine Verbindung gestartet hat oder sich von extern verbunden hat. Die Verbindungsart „Test-Modus“ zeigt den verwendeten Modus entsprechend an:



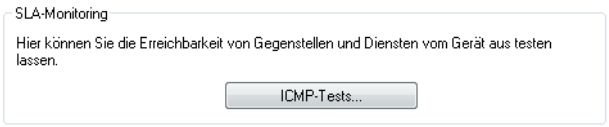
LANmonitor stellt dabei die im Gerät unter **Status** > **Iperf** > **Last-Results** gespeicherten Testergebnisse dar.

4.12 SLA-Monitoring

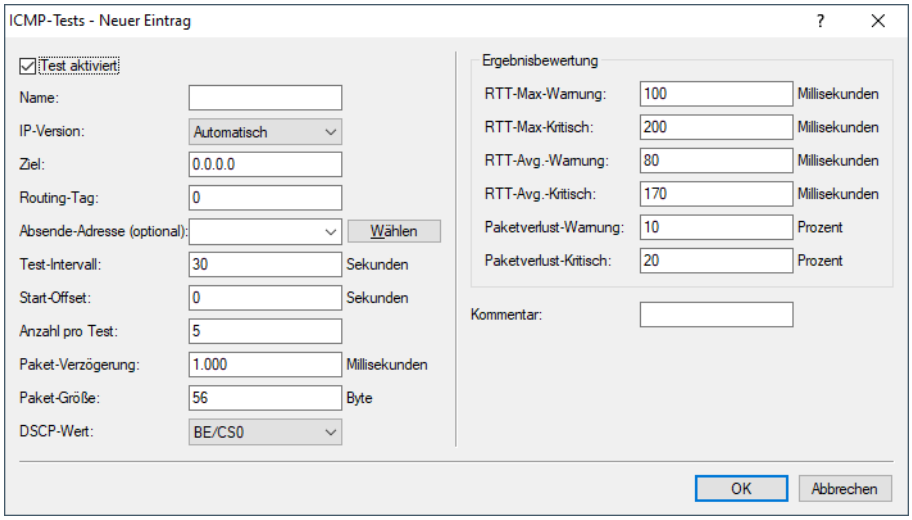
Das SLA-Monitoring überwacht die Verbindungen zu Gegenstellen innerhalb einer Netzwerkstruktur. Ping-Tests zu definierten Zielen geben Aufschluss über die Verfügbarkeit der Peers und zeigen Paketlaufzeiten sowie die Anzahl verlorener Datenpakete an. Sie haben die Möglichkeit, Warnungen bei der Überschreitung festgelegter Richtwerte zu definieren und über LANmonitor ausgeben zu lassen. Zudem wird die Historie vergangener Überprüfungen gespeichert, sodass Administratoren stets über die Qualität der Verbindungen informiert sind.

4.12.1 Konfiguration von SLA-Monitoring über LANconfig

Die Parameter zur Konfiguration des SLA-Monitors finden Sie bei LANconfig unter **Meldungen/Monitoring** > **Allgemein** im Abschnitt **SLA-Monitoring**.



Klicken Sie auf die Schaltfläche **ICMP-Tests**, um neue Abfragen hinzuzufügen und Richtwerte für die Verbindungstests zu definieren.



Test aktiviert

Bei aktivierter Checkbox verwendet das Gerät die definierten Einstellungen für den Verbindungstest.

Name

Name der Verbindung

IP-Version

Legt fest, ob IPv4 oder IPv6 verwendet wird.

Per Default ist die Einstellung "Automatisch" ausgewählt.

Ziel

Definiert das Ziel der Überprüfung (ICMP / PING Ziel).

Routing-Tag

Geben Sie ein Routing-Tag an, falls eine bestimmte Route verwendet werden soll.

Absende-Adresse (opt.)

Konfigurieren Sie optional eine Absende-Adresse, falls Sie ein bestimmtes Netzwerk als Absende-Schnittstelle verwenden möchten.

Test-Intervall

Definiert das Zeitintervall, in dem das Gerät ICMP Pakete verschickt (**Default: 30 Sekunden**).

Start-Offset

Legen Sie eine Verzögerungszeit für den Versand von ICMP-Paketen fest.

Anzahl pro Test

Gibt an, wie viele ICMP Pakete pro Durchlauf verschickt werden (**Default: 5**).

Paket-Verzögerung

Legen Sie eine Verzögerung für den Versand von Paketen fest.

Paket-Größe

Definiert die Paketgröße der ICMP Nachricht.

DSCP-Wert

Definiert den DSCP-Wert der ICMP-Nachricht. DSCP (Differentiated Services Code Point) wird für QoS (Quality of Service) verwendet. Mögliche Werte: BE/CS0, CS1, CS2, CS3, CS4, CS5, CS6, CS7, AF11, AF12, AF13, AF21, AF22, AF23, AF31, AF32, AF33, AF41, AF42, AF43, EF

Ergebnisbewertung

In diesem Abschnitt definieren Sie Grenzwerte für die Paketbehandlung.

RTT-Max-Warnung

Definieren Sie eine maximale Paketumlaufzeit (**R**ound **T**rip **T**ime). Sollte eines der ICMP-Pakete eine längere Umlaufzeit als die hier festgelegte benötigen, wird eine Warnmeldung generiert.

RTT-Max-Kritisch

Definieren Sie eine maximale Paketumlaufzeit, nach der eine Fehlermeldung generiert wird, falls eines der ICMP-Pakete eine längere Umlaufzeit als die hier festgelegte benötigt.

RTT-Avg.-Warnung

Definieren Sie eine durchschnittliche Paketumlaufzeit. Sollte die durchschnittliche Anzahl der ICMP-Pakete eine längere Umlaufzeit als die hier festgelegte benötigen, wird eine Warnmeldung generiert.

RTT-Avg.-Kritisch

Definieren Sie eine durchschnittliche Paketumlaufzeit. Sollte die durchschnittliche Anzahl der ICMP-Pakete eine längere Umlaufzeit als die hier festgelegte benötigen, wird eine Fehlermeldung generiert.

Paketverlust-Warnung

Wenn der Prozentsatz der verloren gegangenen Pakete diesen definierten Wert erreicht, wird eine entsprechende Warnmeldung generiert.

Paketverlust-Kritisch

Wenn der Prozentsatz der verloren gegangenen Pakete diesen definierten Wert erreicht, wird eine entsprechende Fehlermeldung generiert.

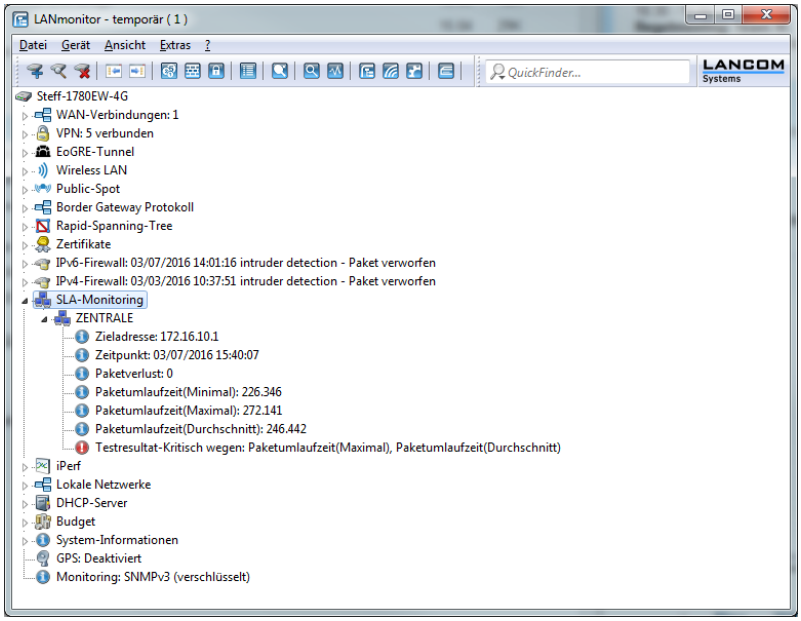
Kommentar

Geben Sie eine aussagekräftige Beschreibung für diesen Eintrag an.

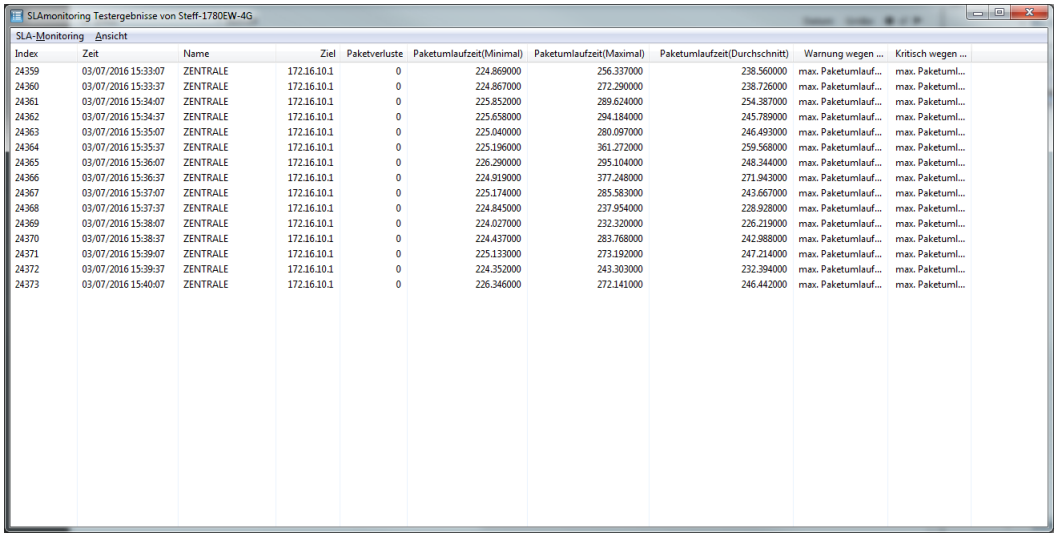
4.12.2 Anzeigen der SLA-Monitoring Ergebnisse in LANmonitor

In LANmonitor sind die Ergebnisse der konfigurierten Tests unter **SLA-Monitoring** ersichtlich.

Angezeigt werden die zuletzt gesammelten Informationen des Verbindungstests.



Sie haben zudem die Möglichkeit, sich die Historie der Verbindungsprüfungen anzeigen zu lassen. Klicken Sie dazu mit der rechten Maustaste auf den Eintrag **SLA-Monitoring**. Wählen Sie im folgenden Dialog den Eintrag **SLA-Monitoring Historie** aus.



Index	Zeit	Name	Ziel	Paketverluste	Paketumlaufzeit(Minimal)	Paketumlaufzeit(Maximal)	Paketumlaufzeit(Durchschnitt)	Warnung wegen ...	Kritisch wegen ...
24359	03/07/2016 15:33:07	ZENTRALE	172.16.10.1	0	224.869000	256.337000	238.560000	max. Paketumlauf...	max. Paketuml...
24360	03/07/2016 15:33:37	ZENTRALE	172.16.10.1	0	224.867000	272.290000	238.726000	max. Paketumlauf...	max. Paketuml...
24361	03/07/2016 15:34:07	ZENTRALE	172.16.10.1	0	225.852000	289.624000	254.387000	max. Paketumlauf...	max. Paketuml...
24362	03/07/2016 15:34:37	ZENTRALE	172.16.10.1	0	225.658000	294.184000	245.789000	max. Paketumlauf...	max. Paketuml...
24363	03/07/2016 15:35:07	ZENTRALE	172.16.10.1	0	225.040000	280.097000	246.493000	max. Paketumlauf...	max. Paketuml...
24364	03/07/2016 15:35:37	ZENTRALE	172.16.10.1	0	225.196000	361.272000	259.568000	max. Paketumlauf...	max. Paketuml...
24365	03/07/2016 15:36:07	ZENTRALE	172.16.10.1	0	226.290000	295.104000	248.344000	max. Paketumlauf...	max. Paketuml...
24366	03/07/2016 15:36:37	ZENTRALE	172.16.10.1	0	224.919000	377.248000	271.943000	max. Paketumlauf...	max. Paketuml...
24367	03/07/2016 15:37:07	ZENTRALE	172.16.10.1	0	225.174000	285.583000	243.667000	max. Paketumlauf...	max. Paketuml...
24368	03/07/2016 15:37:37	ZENTRALE	172.16.10.1	0	224.845000	237.954000	228.928000	max. Paketumlauf...	max. Paketuml...
24369	03/07/2016 15:38:07	ZENTRALE	172.16.10.1	0	224.027000	232.320000	226.219000	max. Paketumlauf...	max. Paketuml...
24370	03/07/2016 15:38:37	ZENTRALE	172.16.10.1	0	224.437000	283.768000	242.988000	max. Paketumlauf...	max. Paketuml...
24371	03/07/2016 15:39:07	ZENTRALE	172.16.10.1	0	225.133000	273.192000	247.214000	max. Paketumlauf...	max. Paketuml...
24372	03/07/2016 15:39:37	ZENTRALE	172.16.10.1	0	224.352000	243.303000	232.394000	max. Paketumlauf...	max. Paketuml...
24373	03/07/2016 15:40:07	ZENTRALE	172.16.10.1	0	226.346000	272.141000	246.442000	max. Paketumlauf...	max. Paketuml...

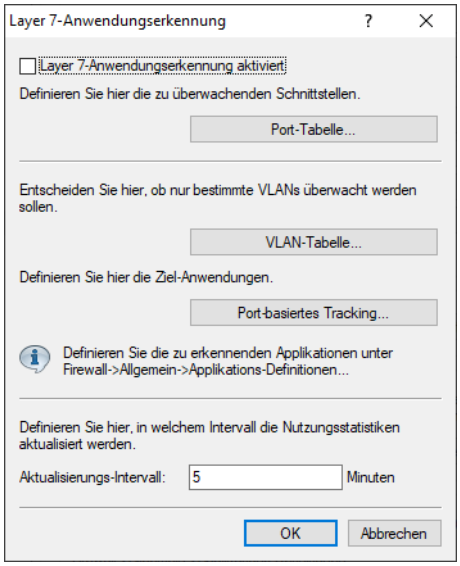
4.13 Layer-7-Anwendungserkennung

Mit Hilfe der Layer-7-Anwendungserkennung haben Sie die Möglichkeit, Dienste in Ihrem Netzwerk zu identifizieren, auf die besonders häufig zugegriffen wird und somit viel Bandbreite beanspruchen. Diese Funktion ermöglicht es Ihnen zudem, denjenigen Client aus dem vorhandenen Clientpool zu isolieren, der diese(n) Dienst(e) intensiv nutzt und den gesamten Traffic des betreffenden Benutzers einzusehen.

Um diese Funktion nutzen zu können ist es erforderlich, die Layer-7-Anwendungserkennung zu aktivieren. Diese ist per Default nicht aktiv.

Die Anwendungserkennung analysiert ein- und ausgehende Verbindungen aller Schnittstellen, die für eine Überwachung definiert wurden und speichert die Statistik der konfigurierten Anwendungen. Ab LCOS-Version 10.12 erfasst die Layer-7-Anwendungserkennung auch separat *IPv4- und IPv6-Traffic*.

Aktivieren und konfigurieren Sie die Layer-7-Anwendungserkennung mit LANconfig unter **Firewall/QoS** > **Allgemein** > **Layer-7-Anwendungserkennung**.



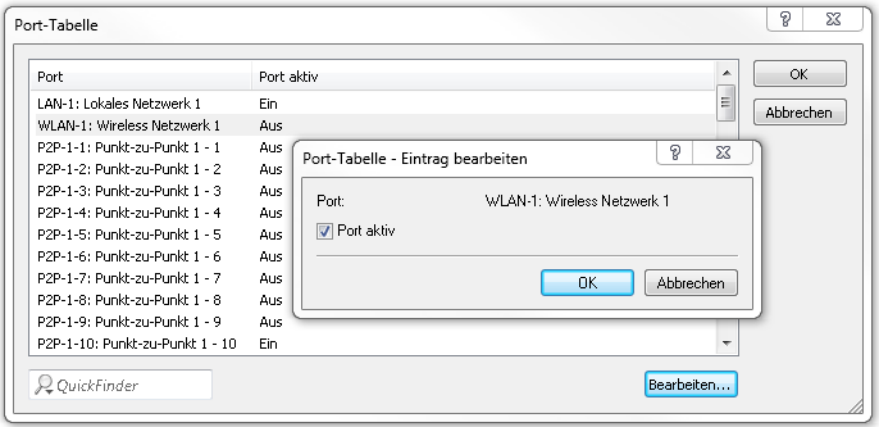
In diesem Abschnitt bestimmen Sie folgende Parameter:

Layer-7-Anwendungserkennung aktiviert

Aktivieren oder deaktivieren Sie die Layer-7-Anwendungserkennung.

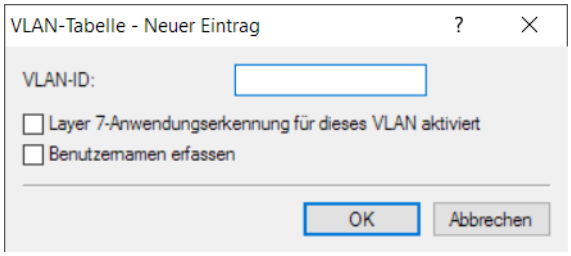
Port-Tabelle

Legen Sie hier fest, welche Verbindungen mit der Layer-7-Anwendungserkennung überwacht werden sollen. Aktivieren oder deaktivieren Sie dazu die zur Verfügung stehenden Ports.



VLAN-Tabelle

Geben Sie hier die zu überwachenden VLAN-IDs an und legen Sie fest, in welchem Umfang die Layer-7-Anwendungserkennung Traffic-Informationen erfasst.

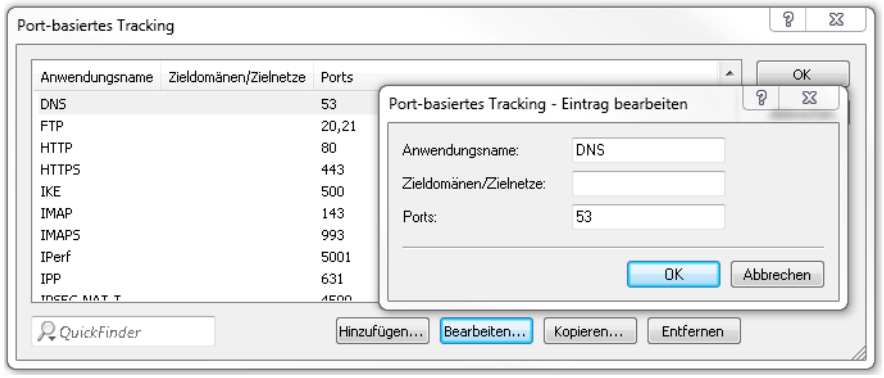


- **Layer 7-Anwendungserkennung für dieses VLAN aktiviert**: Das Gerät erfasst allgemeine bzw. applikationsspezifische Daten.
- **Benutzernamen erfassen:** Das Gerät erfasst in dem angegebenen VLAN benutzerspezifische Daten (Benutzer- oder Client-Name sowie MAC-Adresse).

Damit die Layer-7-Anwendungserkennung im VLAN aktiv ist, muss das Gerät zumindest applikationsspezifischen Daten erfassen.

Port-basiertes Tracking

Wählen Sie hier die Anwendungen aus, die überwacht werden sollen. Sie haben dabei die Möglichkeit, aus Default-Anwendungen zu wählen oder eigene Anwendungen zu definieren. Geben Sie zusätzlich die Zieldomänen oder die Zielnetze der Anwendung an. Erweitern Sie die Liste nach Ihren Bedürfnissen.



Geben Sie mehrere Zieldomänen, Zielnetze oder Ports mittels einer kommaseparierten Liste in CIDR-Notation (Classless Inter-Domain Routing) an. Dabei haben Sie die Möglichkeit, IPv4- oder IPv6-Zielnetze verwenden.

Aktualisierungs-Intervall

Geben Sie einen Wert in Minuten an, nach dessen Ablauf die Nutzungsstatistik aktualisiert wird.

Baut ein Client eine Verbindung über eine überwachte Schnittstelle auf, beginnt die Anwendungserkennung mit der Analyse und Aufzeichnung des Traffic-Volumens.

Die Aufzeichnung und die daraus resultierende Nutzungsstatistik ist abhängig von der für diese Verbindung definierten Konfiguration.

Die Layer-7-Anwendungserkennung beobachtet den Ziel-Port einer Anwendung. Wird eine Verbindung über Port 80 oder 443 (HTTP oder HTTPS) erkannt, erfolgt eine weitere Analyse des Verbindungsaufbaus. Weicht der Ziel-Port davon ab, erfolgt die Zuordnung der Verbindung Port-abhängig über die in der Liste "Port-basiertes Tracking" festgelegten Anwendungen.

Die zu erkennenden Applikationen definieren Sie unter **Konfiguration** > **Firewall/QoS** > **Allgemein** > **Applikations-Definitionen**. Siehe *Applikationsdefinitionen für die Layer-7-Erkennung und die Layer-7-Applikationskontrolle* auf Seite 661.

Bei einem erkannten HTTP/HTTPS-Aufbau wird diese Verbindung tiefer analysiert. Dazu extrahiert die Anwendungserkennung bei HTTP-Verbindungen den Ziel-Host aus der Ziel-URL des HTTP GET Requests.

Es wird nur der Host-Anteil verwendet, weitere URL-Bestandteile werden abgeschnitten

Wird eine HTTPS-Verbindung erkannt, versucht die Layer-7-Anwendungserkennung den Ziel-Host durch Informationen in folgender Reihenfolge zu identifizieren:

- Server Name Indication aus dem TLS Client Hello
- Common Name aus dem übermittelten TLS-Server-Zertifikat
- Reverse DNS Request auf die Server-IP-Adresse

Sowohl bei Verbindungen über HTTP als auch über HTTPS wird der ermittelte Ziel-Hostname mit der Liste "HTTP/HTTPS-Tracking" abgeglichen. Diese Liste enthält die am weitesten verbreiteten Web-Dienste/Anwendungen inklusive der Bestandteile ihrer Hostnamen.

Sollte der aufgerufene Dienst oder die gewählte Verbindung nicht in der Liste enthalten und deshalb eine Zuordnung nicht möglich sein, erfolgt eine Port-basierte Zuordnung zu dem generellen Dienst HTTP oder HTTPS.

Für diese Zuordnung ist es erforderlich, dass die HTTP- und HTTP-Einträge in der Liste für "Port-basiertes Tracking" enthalten sind.

Ist der Ziel-Dienst für jede über eine überwachte Schnittstelle geführte Verbindung bekannt, ist es gemeinsam mit dem verbindungsherstellenden Client möglich, die Verbindung zu tracken und so zu ermitteln, welcher Client wie viel Traffic von / zu einem Dienst verursacht hat.

Die ermittelten Werte finden Sie in den zugehörigen Tabellen im LCOS-Menübaum unter **Status** > **Layer-7-App-Erkennung**.

Sie haben die Möglichkeit, die Layer-7-Anwendungserkennung zentral oder dezentral in Ihrem Netzwerk einzusetzen. Beide Varianten verhindern, dass Traffic mehrfach gelistet wird:

Zentraler Einsatz

Die Layer-7-Anwendungserkennung wird auf einem zentralen Router im LAN aktiviert, auf allen anderen LANCOM Geräten ist sie deaktiviert.

Dezentraler Einsatz

Die Layer-7-Anwendungserkennung wird nur auf den letzten Bridges im LAN aktiviert, z. B. Access Points oder LANCOM Router, an deren LAN-Schnittstellen die Clients direkt angeschlossen sind.

Um verfälschte Ergebnisse zu verhindern, achten Sie bitte darauf, dass der Traffic nur genau ein Gerät oder eine Bridge mit aktiver Layer-7-Anwendungserkennung durchläuft.

4.13.1 IPv4- / IPv6-Traffic-Accounting

Die Layer-7-Anwendungserkennung erfasst auch separat IPv4- und IPv6-Traffic.

Ein gesondertes Einschalten dieses Features ist nicht erforderlich. Bei aktiver Layer-7-Anwendererkennung werden automatisch sowohl IPv4- als auch IPv6-Anwendungen separat aufgelöst.

Die Layer-7-Anwendungserkennung erfasst, zusätzlich zur ihrer Kernaufgabe, das Protokoll des über die entsprechende Schnittstelle übertragenen Traffics.

Für die Darstellung dient folgende Statustabelle:

```
root@LN-1700Esc:/Status/Layer-7-App-Detection/Total-Traffic-per-Protocol
> ls -a
```

```
[1.3.6.1.4.1.2356.11][1.95.8]
Protocol-Name   Tx-KBytes  Rx-KBytes  Tx-KBytes-Curr.-Day  Rx-KBytes-Curr.-Day
[1]             [2]        [3]        [4]                  [5]
===============-------------------------------------------------------------
IPv4             522        259        522                  259
IPv6             2696       18         2696                 18
```

Der eingehende (RX) und der ausgehende (TX) Traffic werden zwischen IPv4 und IPv6 unterschieden und in KBytes gemessen aufgelistet.

5 Sicherheit

Sie mögen es sicher nicht, wenn Außenstehende die Daten auf Ihren Rechnern einsehen oder verändern können. Darüber hinaus sollten Sie die Konfigurationseinstellungen Ihrer Geräte vor unbefugten Änderungen schützen. Dieses Kapitel widmet sich daher einem sehr wichtigen Thema: der Sicherheit. Die Beschreibung der Sicherheitseinstellungen ist in folgende Abschnitte unterteilt:

- Schutz für die Konfiguration
  - Passwortschutz
  - Login-Sperre
  - Zugangskontrolle

Zum Ende des Kapitels finden Sie die wichtigsten Sicherheitseinstellungen in Form einer Checkliste. Damit Sie ganz sicher sein können, dass Ihr Gerät bestens abgesichert ist.

Zur Sicherheit der Daten tragen auch noch einige weitere Funktionen des LCOS bei, die in separaten Kapiteln beschrieben sind:

- *Firewall*
- *Router-Funktionen*
- *VLAN*

5.1 Schutz für die Konfiguration

Mit der Konfiguration des Gerätes legen Sie eine Reihe von wichtigen Parametern für den Datenaustausch fest: Die Sicherheit des eigenen Netzes, die Kontrolle der Kosten und die Berechtigung einzelner Netzteilnehmer gehören z. B. dazu.

Die von Ihnen einmal eingestellten Parameter sollen natürlich nicht durch Unbefugte verändert werden. Daher bietet das Gerät die Möglichkeit, die Konfiguration mit verschiedenen Mitteln zu schützen.

5.1.1 Passwortschutz

Die einfachste Möglichkeit zum Schutz der Konfiguration ist die Vereinbarung eines Passworts.

Solange Sie kein Passwort vereinbart haben, kann jeder die Konfiguration des Gerätes verändern. Beispielsweise könnten Ihre Internetzugangsdaten eingesehen werden, oder der Router so umkonfiguriert werden, dass alle Schutzmechanismen außer Kraft gesetzt werden.

Unter anderem wird ein nicht gesetztes Passwort auf allen Geräten durch eine blinkende Power-LED signalisiert, sofern ein Konfigurationszugriff über WAN oder WLAN möglich ist.

5.1.1.1 Tipps für den richtigen Umgang mit Passwörtern

Für den Umgang mit Passwörtern möchten wir Ihnen an dieser Stelle einige Tipps ans Herz legen:

- **Halten Sie ein Passwort so geheim wie möglich.**

  Notieren Sie niemals ein Passwort. Beliebt aber völlig ungeeignet sind beispielsweise: Notizbücher, Brieftaschen und Textdateien im Computer. Es klingt trivial, kann aber nicht häufig genug wiederholt werden: verraten Sie Ihr Passwort nicht weiter. Die sichersten Systeme kapitulieren vor der Geschwätzigkeit.

- **Passwörter nur sicher übertragen.**

  Ein gewähltes Passwort muss der Gegenseite mitgeteilt werden. Wählen Sie dazu ein möglichst sicheres Verfahren. Meiden Sie: Ungeschütztes E-Mail, Brief, Fax. Besser ist die persönliche Übermittlung unter vier Augen. Die höchste Sicherheit erreichen Sie, wenn Sie das Passwort auf beiden Seiten persönlich eingeben.

- **Wählen Sie ein sicheres Passwort.**

  Verwenden Sie zufällige Buchstaben- und Ziffernfolgen. Passwörter aus dem allgemeinen Sprachgebrauch sind unsicher. Auch Sonderzeichen wie '&"?#-*+_:;,!°' erschweren es Angreifern, Ihr Passwort zu erraten und erhöhen so die Sicherheit des Passworts.

  Groß- und Kleinschreibung werden beim Passwort für die Konfiguration unterschieden.

- **Verwenden Sie ein Passwort niemals doppelt.**

  Wenn Sie dasselbe Passwort für mehrere Zwecke verwenden, mindern Sie seine Sicherheitswirkung. Wenn eine Gegenseite unsicher wird, gefährden Sie mit einem Schlag auch alle anderen Verbindungen, für die Sie dieses Passwort verwenden.

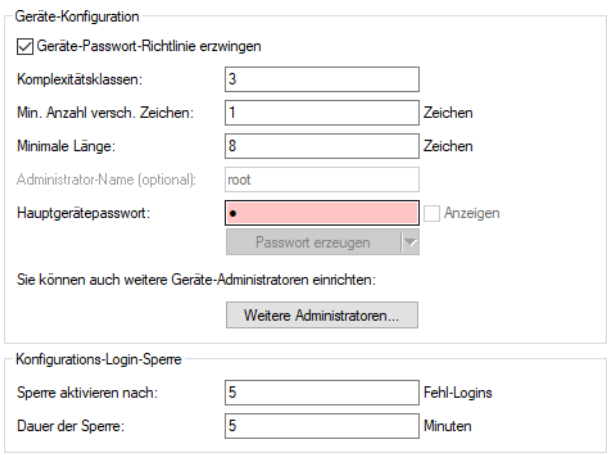
- **Wechseln Sie das Passwort sofort bei Verdacht.**

  Wenn ein Mitarbeiter mit Zugriff auf ein Passwort Ihr Unternehmen verlässt, wird es höchste Zeit, dieses Passwort zu wechseln. Ein Passwort sollte auch immer dann gewechselt werden, wenn der geringste Verdacht einer undichten Stelle auftritt.

Wenn Sie diese einfachen Regeln einhalten, erreichen Sie ein hohes Maß an Sicherheit.

5.1.1.2 Eingabe des Passwortes

Das Feld zur Eingabe des Passworts finden Sie in LANconfig im Konfigurationsbereich **Management** > **Admin** > **Geräte-Konfiguration** > **Hauptgerätepasswort**. In einer Konsolensitzung setzen oder ändern Sie das Passwort mit dem Befehl `passwd`. Die maximale Länge des Hauptgerätepassworts beträgt 128 Zeichen.



Die Option **Anzeigen** ist nur verfügbar, wenn das Gerät die Passwörter zusätzlich so ablegt, dass es diese wiederherstellen kann. Über den Wert **Setup** > **Config** > **Passwoerter** > **Klartext-behalten** können Sie dies anpassen.

Der Schalter **Geräte-Passwort-Richtlinie erzwingen** legt die folgenden Richtlinien für das Hauptgeräte- und die Administrator-Passwörter fest:

Komplexitätsklassen

Konfigurieren Sie hier die notwendige Anzahl an unterschiedlichen Komplexitätsklassen für Passwörter. Komplexitätsklassen sind Klein- bzw. Großbuchstaben, Zahlen und Sonderzeichen. Bei einer Einstellung von 2 müsste das Passwort somit Zeichen aus mindestens zweien dieser Komplexitätsklassen enthalten.

Minimale Anzahl verschiedener Zeichen

Konfigurieren Sie hier die notwendige Anzahl an unterschiedlichen Zeichen für Passwörter.

Minimale Länge

Konfigurieren Sie hier die minimale Anzahl an Zeichen für Passwörter.

Beachten Sie bitte, dass sich die Aktivierung dieser Funktion nicht auf aktuelle Passwörter auswirkt. Nur bei Änderungen der Passwörter werden diese auf ihre Richtlinienkonformität überprüft.

Sobald in der Konfiguration des Gerätes ein Passwort für den „root"-Administrator gesetzt ist, erscheint beim Aufruf von WEBconfig auf der Startseite die Schaltfläche Login, mit dem das Fenster zur Anmeldung eingeblendet wird. Nach Eingabe von korrektem Benutzernamen und Passwort erscheint das Hauptmenü der WEBconfig.

Im Bereich **Konfigurations-Login-Sperre** können Sie den Zugriff auf die Konfiguration nach einer einstellbaren Anzahl am fehlerhaften Login-Versuchen für einige Minuten sperren. Dies ist eine wichtige Hilfe gegen Brute-Force-Attacken auf die Zugangsdaten. Bei einem Brute-Force-Angriff versucht ein unberechtigter Benutzer, ein Passwort zu knacken, und so Zugang zu einem Netzwerk, einem Rechner oder einem anderen Gerät zu erlangen. Dazu spielt z. B. ein Rechner automatisch alle möglichen Kombinationen aus Buchstaben und Zahlen durch, bis das richtige Passwort gefunden wurde. Zum Schutz gegen solche Versuche kann die maximal zulässige Anzahl von fehlerhaften Login-Versuchen eingegeben werden. Wird diese Grenze erreicht, wird der Zugang für eine bestimmte Zeit gesperrt. Die Login-Sperre greift immer nur für die genutzte Zugangsmöglichkeit. Die anderen Zugangsmöglichkeiten können weiterhin genutzt werden.

Technisch bedingt können SSH und Telnet immer nur gemeinsam gesperrt und entsperrt werden.

5.1.1.3 Den SNMP-Zugang schützen

Im gleichen Zug sollten Sie auch den SNMP-Lesezugriff mit Passwort schützen. Für SNMP wird das allgemeine Konfigurations-Passwort verwendet. Mehr Informationen hierzu finden Sie unter *SNMPv3-Zugriffseinstellungen für Administratoren*

5.1.2 Weitere Administratoren mit eingeschränkten Rechten

Nicht für jede Konfigurationstätigkeit benötigen Sie einen Administrator mit allen Rechten. Als Root-Administrator können sie unter **Konfiguration** > **Management** > **Admin** > **Weitere Administratoren** Administratoren mit eingeschränkten Rechten anlegen. Somit muss das Hauptgerätepasswort nicht jedem Administrator bekannt sein. Näheres hierzu unter *Rechteverwaltung für verschiedene Administratoren* auf Seite 109.

5.1.3 Die Login-Sperre

Die Konfiguration im Gerät ist durch eine Login-Sperre gegen „Brute-Force-Angriffe" geschützt. Bei einem Brute-Force-Angriff versucht ein unberechtigter Benutzer, ein Passwort zu knacken, und so Zugang zu einem Netzwerk, einem Rechner oder einem anderen Gerät zu erlangen. Dazu spielt z. B. ein Rechner automatisch alle möglichen Kombinationen aus Buchstaben und Zahlen durch, bis das richtige Passwort gefunden wurde.

Zum Schutz gegen solche Versuche kann die maximal zulässige Anzahl von fehlerhaften Login-Versuchen eingegeben werden. Wird diese Grenze erreicht, wird der Zugang für eine bestimmte Zeit gesperrt.

Die Login-Sperre greift immer nur für die genutzte Zugangsmöglichkeit. Die anderen Zugangsmöglichkeiten können weiterhin genutzt werden.

Technisch bedingt können SSH und Telnet immer nur gemeinsam gesperrt und entsperrt werden.

Zur Konfiguration der Login-Sperre stehen in den Konfigurationstools folgende Einträge zur Verfügung:

- Sperre aktivieren nach (`Anzahl Login-Fehler`)
- Dauer der Sperre (`Sperr-Minuten`)

LANconfig: Management / Admin

Wenn Sie im Feld **Sperre aktivieren nach** den Wert „0" eintragen, wird die Login-Sperre deaktiviert.

WEBconfig: LCOS-Menübaum / Setup / Config

Erfolgt die Anmeldung über RADIUS oder TACACS, bleibt die Login-Sperre ohne Funktionalität.

5.1.4 Einschränkung der Zugriffsrechte auf die Konfiguration

Der Zugriff auf die internen Funktionen kann wie folgt nach Interfaces getrennt konfiguriert werden:

- LAN
- Wireless LAN (WLAN)
- WAN (z. B. DSL oder ADSL)

Bei den Netzwerk-Konfigurationszugriffen können weitere Einschränkungen vorgenommen werden, z. B. dass nur die Konfiguration von bestimmten IP-Adressen vorgenommen werden darf. Ferner sind die folgenden internen Funktionen getrennt schaltbar:

- LANconfig (TFTP)
- WEBconfig (HTTP, HTTPS)
- SNMP
- Terminal/Telnet

Bei Geräten mit VPN-Unterstützung kann die Nutzung der einzelnen internen Funktionen über WAN-Interfaces auch nur auf VPN-Verbindungen beschränkt werden.

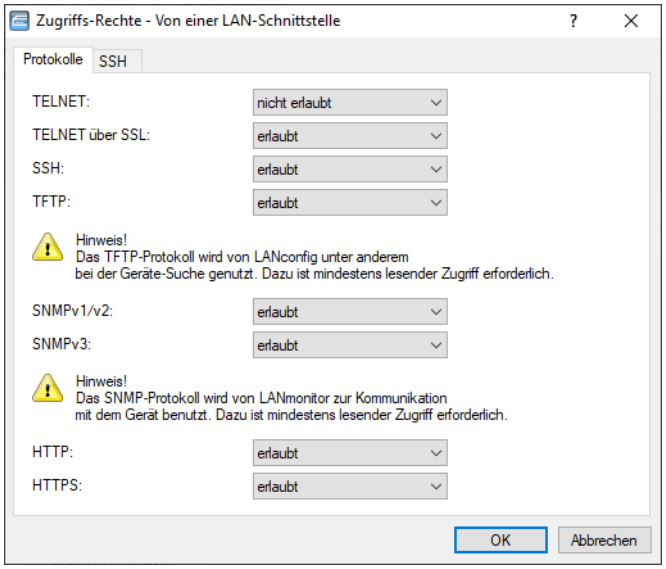
5.1.4.1 Den Netzwerk-Konfigurationszugriff einschränken

Den Zugriff auf die internen Funktionen steuern Sie – getrennt für Zugriffe aus dem lokalen Netz, aus entfernten Netzen oder aus Wireless LANs – für alle Konfigurationsdienste separat.

Dabei ist es möglich, den Konfigurationszugriff generell zu erlauben oder zu verbieten, als reinen Lesezugriff oder – falls Ihr Modell mit VPN ausgerüstet ist – auch nur über VPN zu erlauben.

Die Konfigurationsdialoge im LANconfig mit den Zugriffsrechten vom lokalen Netz (LAN), über das WLAN oder über entfernte Netze (WAN) öffnen Sie unter **Management** > **Admin** im Bereich **Gerätezugriff** mit der Schaltfläche

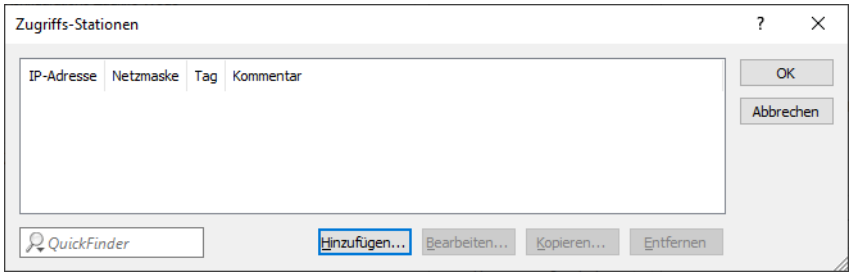
Zugriffseinstellungen. Wählen Sie anschließend nach einem Klick auf **Konfigurations-Zugriffs-Wege** > **Zugriffs-Rechte** die entsprechende Schnittstelle aus:



Wenn Sie den Netzwerkzugriff auf den Router über das WAN ganz sperren wollen, stellen Sie den Konfigurationszugriff von einer WAN-Schnittstelle für alle Methoden auf „nicht erlaubt“.

5.1.4.2 Einschränkung des Netzwerk-Konfigurationszugriffs auf bestimmte IP-Adressen

Sie haben die Möglichkeit, über eine spezielle Filterliste den Zugriff auf die internen Funktionen eines Gerätes auf bestimmte IP-Adressen einzuschränken. Sie erreichen den Konfigurationsdialog mit den Zugriffsadressen in LANconfig über die Tabelle **Zugriffs-Stationen** im Dialog **Management** > **Admin** > **Gerätezugriff** > **Zugriffseinstellungen** > **Konfigurations-Zugriffs-Wege**.

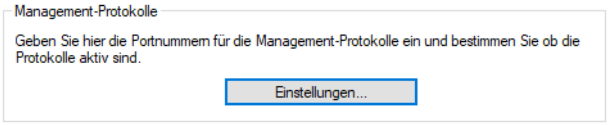


Standardmäßig enthält diese Tabelle keine Einträge. Sie sind also damit in der Lage, über eine beliebige IP-Adresse auf Ihr Gerät zuzugreifen. Mit dem ersten Eintrag einer IP-Adresse sowie der zugehörigen Netzmaske aktivieren Sie den Filter. Danach sind ausschließlich die in diesem Eintrag enthaltenen IP-Adressen dazu berechtigt, die internen Gerätefunktionen zu nutzen. Über zusätzliche Einträge lässt sich der Kreis der Berechtigten erweitern. Die Filter-Einträge können sowohl einzelne Rechner als auch ganze Netze umfassen.

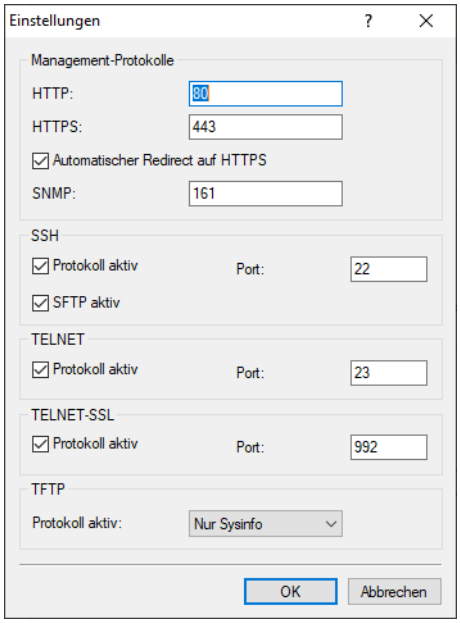
5.1.5 Management-Protokolle

Über die Management-Protokolle definieren Sie die Protokolle und deren Ports, die grundsätzlich für die Konfiguration aktiv sein sollen. Die entsprechenden Einstellungen finden Sie in LANconfig unter **Management** > **Admin** >

Management-Protokolle Die Verwendung des jeweiligen Protokolls auf bestimmten Schnittstellen lässt sich ebenfalls einstellen. Näheres hierzu unter *Einschränkung der Zugriffsrechte auf die Konfiguration* auf Seite 358.



Nach einem Klick auf **Einstellungen** können Sie die folgenden Protokolle aktivieren und den jeweils verwendeten Port konfigurieren:



HTTP / HTTPS

Zugriff per WEBconfig.

Automatischer Redirect auf HTTPS

Falls per HTTP auf die WEBconfig zugegriffen wird, dann kann hier automatisch auf eine verschlüsselte HTTPS-Verbindung umgeschaltet werden. Dadurch werden sensitive Daten wie z. B. das Passwort beim Login oder die Konfiguration durch die verschlüsselte Verbindung geschützt.

SNMP

Das SNMP-Protokoll ist auf dem angegebenen Port aktiv.

SSH

Zugriff auf die Konsole über SSH. Zusätzlich kann hier das Protokoll SFTP ein- bzw ausgeschaltet werden.

TELNET

Zugriff auf die Konsole über TELNET.

TELNET-SSL

Zugriff auf die Konsole über TELNET-SSL.

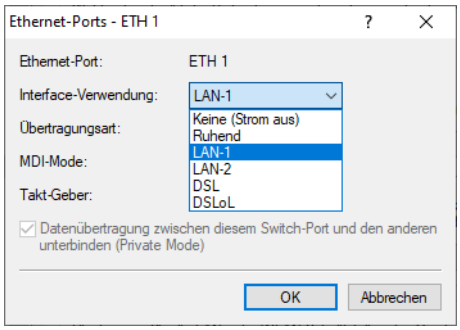
TFTP

Zugriff über TFTP. Das Trivial File Transfer Protocol (TFTP) ist eine einfachere Variante des File Transfer Protokolls (FTP). Im Gegensatz zu FTP ist mit TFTP lediglich das Lesen oder Schreiben von Dateien über UDP möglich. Die Einstellung **Nur Sysinfo** lässt den Port zwar offen, aber das Gerät antwortet nur auf einen Sysinfo-Request. Dadurch wird es in LANconfig angezeigt und insbesondere bei einer Suche nach Geräten gefunden. Es lässt

sich aber keine Konfiguration zum Gerät hochladen. Da dieses Protokoll unverschlüsselt überträgt könnten sonst evtl. sensitive Daten im Netzwerk mitgelesen werden.

5.1.6 Abschalten von Ethernet-Schnittstellen

Die Ethernet-Schnittstellen von öffentlich zugänglichen Geräten können ggf. von unbefugten Anwendern genutzt werden, um physikalischen Zugang zu einem Netzwerk zu erhalten. Um diesen Versuch zu verhindern, können die Ethernet-Schnittstellen der Geräte ausgeschaltet werden.



LANconfig: **Schnittstellen** > **LAN** > **Ethernet-Switch-Einstellungen** > **Ethernet-Ports**

Interface-Verwendung

Wählen Sie hier aus, wie diese Schnittstelle verwendet werden soll.

Mögliche Werte:

Keine (Strom aus)

Die Schnittstelle ist deaktiviert.

Ruhend

Die Schnittstelle ist keiner Verwendung zugeordnet, sie ist allerdings physikalisch aktiv.

LAN-1 bis LAN-n

Die Schnittstelle ist einem logischen LAN zugeordnet.

DSL-1 bis DSL-n

Die Schnittstelle ist einem DSL-Interface zugeordnet.

DSLoL

Eine IPv4-Maskierung („NAT“) ist nur über eine WAN-Verbindung möglich. Wenn man in Richtung eines LAN- oder WLAN-Interface maskieren will, dann muss das entsprechende LAN- oder WLAN-Interface als DSL-Port deklariert werden, so dass dieser für den Aufbau einer WAN-Verbindung (typischerweise IPoE oder DHCPoE) verwendet werden kann.

Monitor

Der Port ist ein Monitor-Port, d. h. es wird alles, was auf den anderen Ports empfangen wird, auf diesem Port wieder ausgegeben. Damit kann an diesem Port z. B. ein Paket-Sniffer (wie Wireshark / Ethereal) angeschlossen werden.

Default: Abhängig von der jeweiligen Schnittstelle bzw. dem spezifischen Hardware-Modell.

5.2 Standortverifikation über GPS

Nach einem Diebstahl kann ein Gerät theoretisch von Unbefugten an einem anderen Ort betrieben werden. Auch bei einer passwortgeschützten Geräte-Konfiguration könnten so die im Gerät konfigurierten RAS-Zugänge, LAN-Kopplungen oder VPN-Verbindungen unerlaubt genutzt werden, ein Dieb könnte sich Zugang zu geschützten Netzwerken verschaffen.

Der Betrieb des Gerätes kann jedoch mit verschiedenen Mitteln so geschützt werden, dass es nach dem Wiedereinschalten oder beim Einschalten an einem anderen Ort nicht mehr verwendet werden kann.

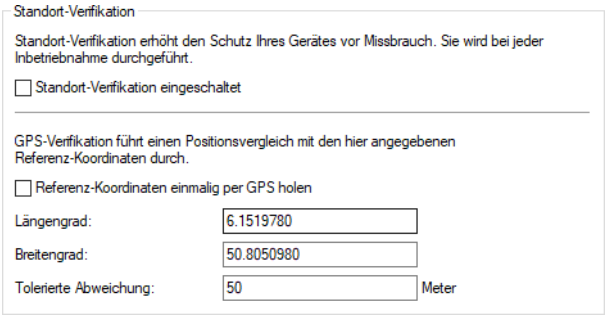
5.2.1 GPS-Standortverifikation

Für die GPS-Standortverifikation können Sie im Gerät eine erlaubte geografische Position definieren. Nach dem Einschalten aktiviert das Gerät bei Bedarf automatisch das GPS-Modul und prüft, ob es sich an der „richtigen" Position befindet – nur bei einer positiven Prüfung wird das Router-Modul eingeschaltet. Nach Abschluss der Standortverifikation wird das GPS-Modul automatisch wieder deaktiviert, sofern es nicht manuell eingeschaltet ist.

5.2.2 Konfiguration der Standortverifikation

Die Parameter für die Standortverifikation finden Sie im LANconfig unter **Management** > **Standort**.

Unter **Management** > **Erweitert** > **GPS-Modul** können Sie das GPS-Modul unabhängig von der Standortverifikation einschalten, um z. B. die aktuellen Standortkoordinaten mit LANmonitor zu überwachen.

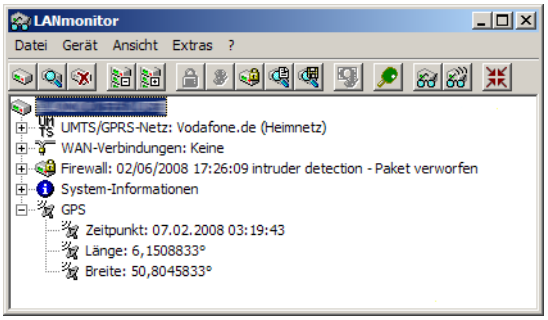


- Mit der Option **Standortverifikation eingeschaltet** aktivieren Sie die Standortverifikation.
- Wählen Sie die Methode für die Standort-Überprüfung:
  - 'GPS-Verifikation' für die Überprüfung über die Geo-Koordinaten.

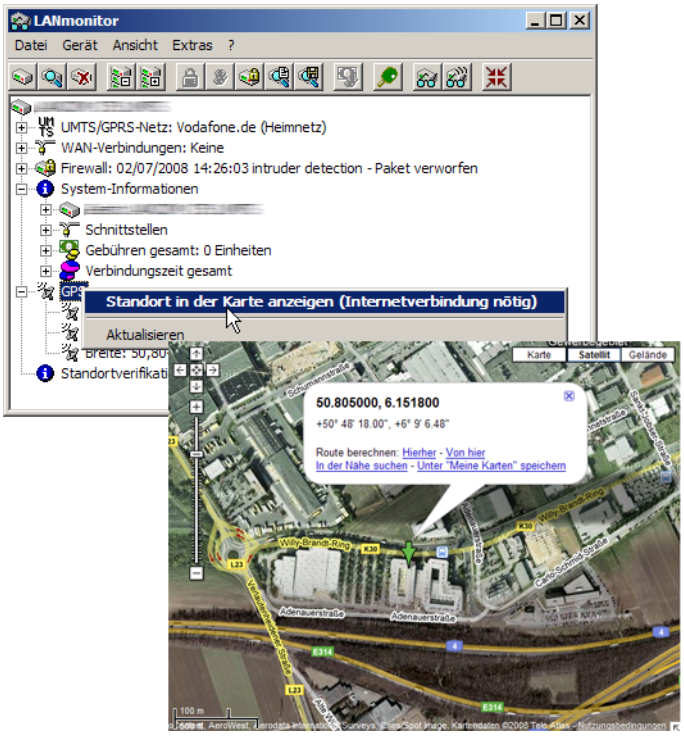
  Für die Standort-Überprüfung über GPS muss eine entsprechende GPS-Antenne an den AUX-Anschluss des Gerätes angeschlossen werden. Zusätzlich muss eine SIM-Karte für den Mobilfunkbetrieb eingelegt werden und das Gerät muss in ein Mobilfunknetz eingebucht sein.
- Tragen Sie für die Standort-Überprüfung über 'Selbst-Anruf' oder 'Rufweiterleitungs-Überprüfung' als 'Ziel-Rufnummer' ein, auf welche Telefonnummer geprüft werden soll.
- Tragen Sie für die Standort-Überprüfung über GPS die Parameter für die GPS-Prüfung ein:
  - Längen- und Breitengrad
  - Abweichung von der erlaubten Position in Metern

  Die Geo-Koordinaten für den aktuellen Standort kann das Gerät selbst ermitteln, indem Sie den Schalter **Referenz-Koordinaten einmalig per GPS holen** aktivieren. Nach dem Rückschreiben der Konfiguration in das Gerät werden automatisch die aktuellen Längen- und Breitengrade eingetragen, wenn die Standortverifikation aktiv ist und gültige GPS-Daten vorliegen. Anschließend wird diese Option selbsttätig wieder deaktiviert.

Alternativ können Sie die Geo-Koordinaten für beliebige Standorte über Tools wie z. B. Google Maps ermitteln.

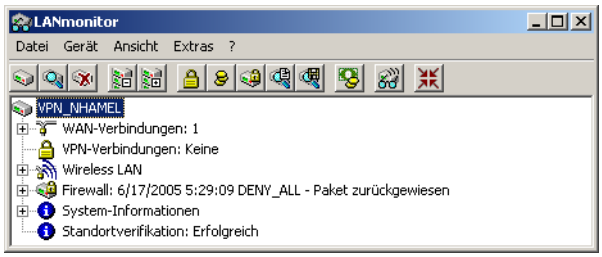


Wenn im LANmonitor die aktuellen Geo-Koordinaten angezeigt werden, können Sie mit einem rechten Mausklick auf den Eintrag 'GPS' den aktuellen Standort in der Satelliten-Ansicht von Google Maps aufrufen.

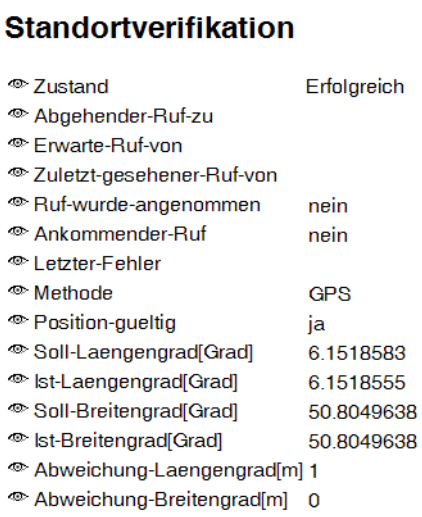


5.2.2.1 Statusabfrage der Standortverifikation

Der Status der Standortverifikation kann über den LANmonitor eingesehen werden:



Mit WEBconfig (**LCOS-Menübaum** / **Status** / **Config** / **Standortverifikation**) oder CLI (`Status/Config/Standortverifikation`) können Sie den Status der Standortverifikation einsehen:



Erst wenn die Standortverifikation im Zustand 'Erfolgreich' ist, kann der Router Daten über die WAN-Interfaces übertragen.

› Eine Standortverifikation über GPS ist dann erfolgreich, wenn die GPS-Position gültig ist und innerhalb der zulässigen Abweichung mit der Soll-Position übereinstimmt.

5.3 Speicherung von Passwort-Formularfeldern im Browser verhindern

Eingabe-Dialoge auf Webseiten bieten den Webbrowsern die Möglichkeit, eingegebene Passwörter zu speichern, um sie bei einem erneuten Seitenaufruf komfortabel abzurufen. Diese Funktion der Webbrowser erleichtert Schadsoftware das Auslesen der vertraulichen Formulardaten.

Um die manuelle Eingabe des Login-Passwortes bei jedem erneuten Seitenaufruf zu erzwingen, deaktivieren Sie im WEBconfig unter **Setup** > **HTTP** > **Verhindere-Passwort-Vervollstaendigung** die Speicherung von Formularfeld-Inhalten mit der Einstellung „Ja“.

5.4 Die Sicherheits-Checkliste

In der folgenden Checkliste finden Sie alle wichtigen Sicherheitseinstellungen im Überblick. Die meisten Punkte dieser Checkliste sind in einfachen Konfigurationen unbedenklich. In solchen Fällen reichen die Sicherheitseinstellungen aus, die während der Grundkonfiguration oder mit dem Sicherheits-Assistenten gesetzt werden.

Haben Sie das Funknetzwerk durch Verschlüsselung und Zugangskontrolllisten abgesichert?

Mit Hilfe von 802.11i, WPA oder WEP verschlüsseln Sie die Daten im Funknetzwerk mit verschiedenen Verschlüsselungsmethoden wie AES, TKIP oder WEP. LANCOM empfiehlt die stärkste mögliche Verschlüsselung mit 802.11i und AES. Wenn der eingesetzte WLAN-Client Adapter diese nicht unterstützt, nutzen Sie TKIP oder zumindest WEP. Stellen Sie sicher, dass in Ihrem Gerät bei aktivierter Verschlüsselungs-Funktion mindestens eine Passphrase oder ein WEP-Schlüssel eingetragen und zur Verwendung ausgewählt ist.

LANCOM rät aus Sicherheitsgründen von der Verwendung von WEP ab! Setzen Sie WEP nur in begründeten Ausnahmefällen ein und ergänzen Sie die WEP-Verschlüsselung nach Möglichkeit mit anderen Schutzmechanismen!

Zur Kontrolle der Einstellungen wählen Sie in LANconfig unter **Wireless LAN** > **Verschlüsselung** > **WLAN-Verschlüsselungs-Einstellungen** die Verschlüsselungseinstellungen für die logischen WLAN-Schnittstellen aus.

Mit der Access Control List (ACL) gewähren oder untersagen Sie einzelnen Funk-LAN-Clients den Zugriff auf Ihr Funk-LAN. Die Festlegung erfolgt anhand der fest programmierten MAC-Adressen der Funk-Netzwerkkarten. Zur Konfiguration der Access Control List öffnen Sie in LANconfig die **Stationsregeln** unter **Wireless-LAN** > **Stationen/LEPS** > **LEPS-MAC**.

Mit der LANCOM Enhanced Passphrase Security MAC (LEPS-MAC) ordnen Sie jeder MAC-Adresse in einer zusätzlichen Spalte der ACL eine individuelle Passphrase zu – eine beliebige Folge aus 8 bis 64 ASCII-Zeichen. Nur die Verbindung von Passphrase und MAC-Adresse erlaubt die Anmeldung am Access Point und die anschließende Verschlüsselung per IEEE 802.11i oder WPA2. Siehe auch *Konfiguration* auf Seite 971.

Die Zugangskontrolle findet gestaffelt statt. Zuerst wird nach einem LEPS-MAC-Eintrag gesucht. Falls es den nicht gibt, dann wird bei LEPS-U nach einem passenden Eintrag gesucht. Als letztes wird die für ein WLAN unter **Wireless-LAN** > **Verschlüsselung** > **WLAN-Verschlüsselungs-Einstellungen** eingestellte Passphrase überprüft.

Bei Verwendung von LEPS-U und / oder LEPS-MAC sollten Sie diese Passphrase geheim halten und am Besten nicht verwendet. Falls Sie einen Benutzer bzw. MAC-Adresse entfernen, dann soll dieser auch keinen Zugang über die WLAN-Passphrase erhalten.

Haben Sie ein Passwort für die Konfiguration vergeben?

Die einfachste Möglichkeit zum Schutz der Konfiguration ist die Vereinbarung eines Passworts. Solange Sie kein Passwort vereinbart haben, kann jeder die Konfiguration des Gerätes verändern. Das Feld zur Eingabe des Passworts finden Sie in LANconfig unter **Management** > **Admin**. Es ist insbesondere dann unerlässlich, ein Passwort zur Konfiguration zu vergeben, wenn Sie die Fernkonfiguration erlauben wollen!

Haben Sie die Fernkonfiguration zugelassen?

Wenn Sie die Fernkonfiguration nicht benötigen, so schalten Sie sie ab. Wenn Sie die Fernkonfiguration benötigen, so vergeben Sie unbedingt einen Passwortschutz für die Konfiguration. Das Feld zur Abschaltung der Fernkonfiguration finden Sie in LANconfig unter **Management** > **Admin** > **Gerätezugriff** > **Zugriffseinstellungen**. Wählen Sie hier im Abschnitt **Konfigurations-Zugriffs-Wege Zugriffs-Rechte** > **Von einer WAN-Schnittstelle** für alle Protokolle die Option **nicht erlaubt**. Zudem haben Sie die Möglichkeit, den HTTP-Port für die Web Server Dienste zu sperren. Wählen Sie hierfür im Abschnitt **Zugriff auf Web-Server-Dienste** unter **Zugriffs-Rechte** > **Von einer WAN-Schnittstelle** die Option **Deaktiviert**.

Haben Sie die Konfiguration vom Funk-Netzwerk aus zugelassen?

Wenn Sie die Konfiguration vom Funk-Netzwerk aus nicht benötigen, so schalten Sie sie ab. Das Feld zur Abschaltung der Konfiguration vom Funk-Netzwerk aus finden Sie ebenfalls in LANconfig unter **Management** > **Admin** > **Gerätezugriff** > **Zugriffseinstellungen**. Wählen Sie hier im Abschnitt **Konfigurations-Zugriffs-Wege Zugriffs-Rechte** > **Von einer WLAN-Schnittstelle** für alle Protokolle die Option **nicht erlaubt**. Zudem haben Sie die Möglichkeit, den HTTP-Port für die Web Server Dienste zu sperren. Wählen Sie hierfür im Abschnitt **Zugriff auf Web-Server-Dienste** unter **Zugriffs-Rechte** > **Von einer WLAN-Schnittstelle** die Option **Deaktiviert**.

Haben Sie die SNMP-Konfiguration mit einem Passwort versehen?

Schützen Sie auch die SNMP-Konfiguration mit einem Passwort. Das Feld zum Schutz der SNMP-Konfiguration mit einem Passwort finden Sie ebenfalls in LANconfig unter **Management** > **Admin**.

Haben Sie die Firewall aktiviert?

Die Stateful-Inspection Firewall der Geräte sorgt dafür, dass Ihr lokales Netzwerk von außen nicht angegriffen werden kann, wenn Ihr WLAN-Controller als Public Spot eingesetzt wird. Die Firewall können Sie in LANconfig unter **Firewall/Qos** > **Allgemein** einschalten.

Beachten Sie, dass alle Sicherheitsaspekte der Firewall (inkl. IP-Masquerading, Port-Filter und Zugriffs-Liste) nur für Datenverbindungen aktiv sind, die über den IP-Router geführt werden. Direkte Datenverbindungen über die Bridge werden nicht von der Firewall geschützt!

Verwenden Sie eine „Deny-All" Firewall-Strategie?

Für maximale Sicherheit und Kontrolle unterbinden Sie zunächst jeglichen Datentransfer durch die Firewall. Nur die Verbindungen, die explizit gestattet sein sollen, sind in die Firewall einzutragen. Damit wird „Trojanern" und bestimmten E-Mail-Viren der Kommunikations-Rückweg entzogen. Die Firewall-Regeln finden Sie in LANconfig unter **Firewall/QoS** > **IPv4-Regeln** > **Regeln** und **Firewall/QoS** > **IPv6-Regeln** > **IPv6-Inbound-Regeln** oder **Firewall/QoS** > **IPv6-Regeln** > **IPv6-Forwarding-Regeln**.

Die Stateful-Inspection Firewall der Geräte sorgt dafür, dass Ihr lokales Netzwerk von außen nicht angegriffen werden kann, wenn Ihr WLAN-Controller als Public Spot eingesetzt wird. Die Firewall können Sie in LANconfig unter **Firewall/Qos** > **Allgemein** einschalten.

Beachten Sie, dass alle Sicherheitsaspekte der Firewall (inkl. IP-Masquerading, Port-Filter und Zugriffs-Liste) nur für Datenverbindungen aktiv sind, die über den IP-Router geführt werden. Direkte Datenverbindungen über die Bridge werden nicht von der Firewall geschützt!

Haben Sie IP-Masquerading aktiviert?

„IP-Masquerading" heißt das Versteck für alle lokalen Rechner beim Zugang ins Internet. Dabei wird nur das Router-Modul des Geräts mit seiner IP-Adresse im Internet bekannt gemacht. Die IP-Adresse kann fest vergeben sein oder vom Provider dynamisch zugewiesen werden. Die Rechner im LAN nutzen den Router dann als Gateway und können selbst nicht erkannt werden. Der Router trennt Internet und Intranet wie eine Wand. Die Verwendung von IP-Masquerading wird für jede Route in der Routing-Tabelle einzeln festgelegt. Die Routing-Tabellen für IPv4 und IPv6 finden Sie in LANconfig unter **IP-Router** > **Routing**.

Haben Sie kritische Ports über Filter geschlossen?

Die Firewall-Filter des Geräts bieten Filterfunktionen für einzelne Rechner oder ganze Netze. Es ist möglich, Quell- und Ziel-Filter für einzelne Ports oder auch Portbereiche aufzusetzen. Zudem können einzelne Protokolle oder beliebige Protokollkombinationen (ICMP) gefiltert werden. Besonders komfortabel ist die Einrichtung der Filter mit Hilfe von LANconfig. Unter **Firewall/QoS** > **IPv4-Regeln** > **Regeln** und **Firewall/QoS** > **IPv6-Regeln** > **IPv6-Inbound-Regeln** oder **Firewall/QoS** > **IPv6-Regeln** > **IPv6-Forwarding-Regeln** können Sie Filterregeln definieren und verändern.

Haben Sie bestimmte Stationen von dem Zugriff auf das Gerät ausgeschlossen?

Mit einer speziellen Filter-Liste kann der Zugriff auf die internen Funktionen der Geräte über TCP/IP eingeschränkt werden. Mit den internen Funktionen werden hierbei Konfigurationssitzungen über LANconfig, WEBconfig, Telnet oder TFTP bezeichnet. Standardmäßig enthält diese Tabelle keine Einträge, damit kann also von Rechnern mit beliebigen IP-Adressen aus über TCP/IP mit TFTP ein Zugriff auf das Gerät gestartet werden. Mit dem ersten Eintrag einer IP-Adresse sowie der zugehörigen Netzmaske wird der Filter aktiviert, und nur noch die in diesem Eintrag enthaltenen IP-Adressen sind berechtigt, die internen Funktionen zu nutzen. Mit weiteren Einträgen kann der Kreis der Berechtigten erweitert werden. Die Filter-Einträge können sowohl einzelne Rechner als auch ganze Netze bezeichnen. Die Zugangsliste finden Sie in LANconfig unter **Firewall/QoS** > **IPv4-Regeln** und **Firewall/QoS** > **IPv6-Regeln**.

Lagern Sie Ihre abgespeicherte Konfiguration an einem sicheren Ort?

Schützen Sie abgespeicherte Konfigurationen an einem sicheren Ort vor unberechtigtem Zugriff. Eine abgespeicherte Konfiguration könnte sonst von einer unberechtigten Person in ein anderes Gerät geladen werden, wodurch z. B. Ihre Internet-Zugänge auf Ihre Kosten benutzt werden können.

Haben Sie für besonders sensiblen Datenaustausch auf dem Funknetzwerk die Funktionen von IEEE 802.1X eingerichtet?

Wenn Sie auf Ihrem Funk-LAN besonders sensible Daten austauschen, können Sie zur weiteren Absicherung die IEEE-802.1X-Technologie verwenden. Die IEEE-802.1X-Einstellungen konfigurieren Sie in LANconfig unter **Wireless-LAN** > **802.1X**.

Haben Sie die Möglichkeiten zum Schutz der WAN-Zugänge bei einem Diebstahl des Gerätes aktiviert?

Nach einem Diebstahl kann ein Gerät theoretisch von Unbefugten an einem anderen Ort betrieben werden. Auch bei einer passwortgeschützten Geräte-Konfiguration könnten so die im Gerät konfigurierten RAS-Zugänge, LAN-Kopplungen oder VPN-Verbindungen unerlaubt genutzt werden, ein Dieb könnte sich Zugang zu geschützten Netzwerken verschaffen.

Der Betrieb des Gerätes kann jedoch mit verschiedenen Mitteln so geschützt werden, dass es nach dem Wiedereinschalten oder beim Einschalten an einem anderen Ort nicht mehr verwendet werden kann.

Für die GPS-Standortverifikation können Sie im Gerät eine erlaubte geografische Position definieren. Nach dem Einschalten prüft das Gerät, ob es sich an der „richtigen" Position befindet – nur bei einer positiven Prüfung wird das Router-Modul eingeschaltet.

Mit den Funktionen des Scripting kann die gesamte Konfiguration des Gerätes nur im RAM gespeichert werden, der beim Booten des Gerätes gelöscht wird. Die Konfiguration wird dabei gezielt nicht in den bootresistenten Flash-Speicher geschrieben. Mit dem Trennen von der Stromversorgung und dem Aufstellen an einem anderen Ort wird damit die gesamte Konfiguration des Gerätes gelöscht.

Haben Sie die Speicherung der Konfigurationsdaten Ihren Sicherheitsanforderungen angepasst?

Mit der Funktion des „Autarken Weiterbetriebs" wird die Konfiguration für ein WLAN-Interface, das von einem WLAN-Controller verwaltet wird, nur für eine bestimmte Zeit im Flash bzw. ausschließlich im RAM gespeichert. Die Konfiguration des Geräts wird gelöscht, wenn der Kontakt zum WLAN-Controller oder die Stromversorgung länger als die eingestellte Zeit unterbrochen wird.

Haben Sie den Reset-Taster gegen das unbeabsichtigte Zurücksetzen der Konfiguration gesichert?

Manche Geräte können nicht unter Verschluss aufgestellt werden. Hier besteht die Gefahr, dass die Konfiguration versehentlich gelöscht wird, wenn ein Mitarbeiter den Reset-Taster zu lange gedrückt hält. Mit einer entsprechenden Einstellung kann das Verhalten des Reset-Buttons gesteuert werden, der Reset-Taster wird dann entweder ignoriert oder es wird nur ein Neustart ausgelöst, unabhängig von der gedrückten Dauer.

6 Routing und WAN-Verbindungen

Dieses Kapitel beschreibt die wichtigsten Protokolle und Konfigurationseinträge, die bei WAN-Verbindungen eine Rolle spielen. Es zeigt auch Wege auf, WAN-Verbindungen zu optimieren.

6.1 Allgemeines über WAN-Verbindungen

WAN-Verbindungen werden für folgende Anwendungen verwendet.

- Internet-Zugang
- LAN-LAN-Kopplung
- Remote Access

6.1.1 Brücken für Standard-Protokolle

WAN-Verbindungen unterscheiden sich von direkten Verbindungen dadurch, dass die Daten im WAN über standardisierte Netzwerk-Protokolle übertragen werden, die auch im LAN Anwendung finden. Direkte Verbindungen arbeiten hingegen mit proprietären Verfahren, die speziell für Punkt-zu-Punkt-Verbindungen entwickelt worden sind.

Über WAN-Verbindungen wird ein LAN erweitert, bei direkten Verbindungen erhält nur ein einzelner PC eine Verbindung zu einem anderen PC. WAN-Verbindungen bilden gewissermaßen Brücken für die Kommunikation zwischen Netzwerken (bzw. für die Anbindung einzelner Rechner an ein LAN).

6.1.1.1 Welche Protokolle werden auf WAN-Verbindungen eingesetzt?

Auf WAN-Verbindungen über den Highspeed-Anschluss (z. B. DSL-Verbindungen) werden Pakete nach dem IP-Standard übertragen.

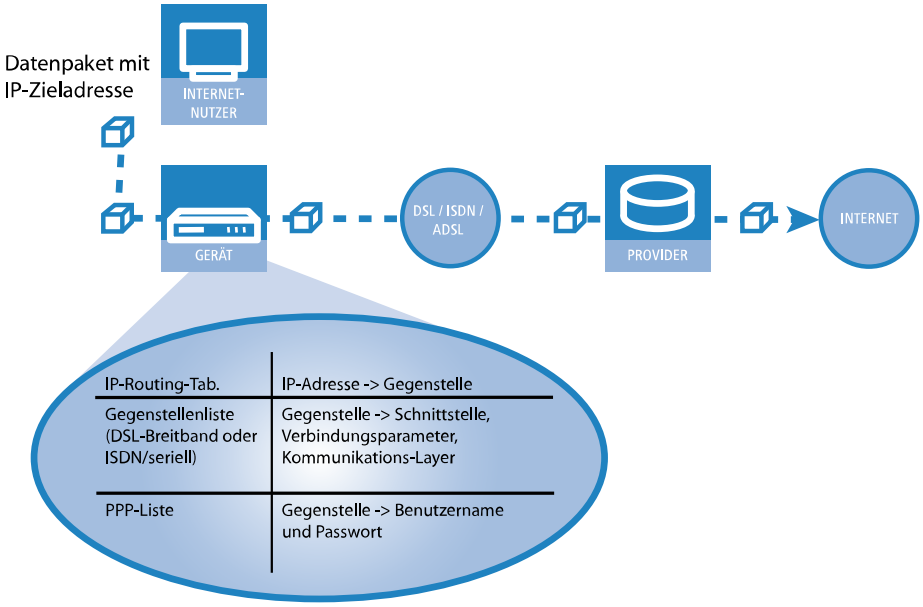
6.1.1.2 Die enge Zusammenarbeit mit den Router-Modulen

Charakteristisch für WAN-Verbindungen ist die enge Zusammenarbeit mit den Router-Modulen im Gerät. Die Router-Module (IP) sorgen für die Verbindung von LAN und WAN. Sie bedienen sich der WAN-Module, um Anfragen von PCs aus dem LAN nach externen Ressourcen zu erfüllen.

6.1.2 Was passiert bei einer Anfrage aus dem LAN?

Die Routermodule ermitteln zunächst nur, zu welcher Gegenstelle ein Datenpaket übertragen werden soll. Damit die entsprechende Verbindung ausgewählt und ggf. aufgebaut werden kann, müssen verschiedene Parameter für alle notwendigen Verbindungen vereinbart werden. Diese Parameter sind in unterschiedlichen Listen abgelegt, deren Zusammenspiel die richtigen Verbindungen erlaubt.

Wir wollen diesen Ablauf an einem vereinfachten Beispiel verdeutlichen. Dabei gehen wir davon aus, dass die IP-Adresse des gesuchten Rechners im Internet bekannt ist.



1. **Auswahl der richtigen Route**

   Ein Datenpaket aus einem Rechner findet den Weg ins Internet in erster Linie über die IP-Adresse des Empfängers. Mit dieser Adresse schickt der Rechner das Paket los über das LAN zum Router. Der Router ermittelt in seiner IP-Routing-Tabelle die Gegenstelle, über die die Ziel-IP-Adresse erreichbar ist, z. B. 'Provider'.

2. **Verbindungsdaten für die Gegenstelle**

   Mit diesem Namen prüft der Router dann die Gegenstellenliste und findet die notwendigen Verbindungsdaten für den Provider. Zu diesen Verbindungsdaten gehören z. B die WAN-Schnittstelle (DSL) über die der Provider angewählt wird oder auch Protokollinformationen. Außerdem erhält der Router aus der PPP-Liste Benutzernamen und Passwort, die für die Anmeldung notwendig sind.

3. **Aufbau der WAN-Verbindung**

   Der Router kann dann eine Verbindung über eine WAN-Schnittstelle zum Provider aufbauen. Er authentifiziert sich mit Benutzernamen und Passwort.

4. **Weitergabe des Datenpaketes**

   Sobald die Verbindung hergestellt ist, kann der Router das Datenpaket ins Internet weitergeben.

6.2 IP-Routing

Ein IP-Router arbeitet zwischen Netzen, die TCP/IP als Netzwerk-Protokoll verwenden. Dabei werden nur Daten übertragen, deren Zieladressen in der Routing-Tabelle eingetragen sind. In diesem Abschnitt erfahren Sie, wie die IP-Routing-Tabelle in einem Router von LANCOM aufgebaut ist und mit welchen weiteren Funktionen das IP-Routing unterstützt wird.

6.2.1 Informationen zum Routingverhalten

In LCOS wird das Routing über die **FIB** (**F**orwarding**I**nformation **B**ase) realisiert.

Zusätzlich gibt es noch die **RIB** (**R**oute **I**nformation **B**ase), welche für die Priorisierung von Routen aus unterschiedlichen Quellen zuständig ist, die das gleiche Ziel-Netzwerk und das gleiche Routing-Tag haben. Die Priorisierung erfolgt dabei anhand der **Administrativen Distanz**.

Die **FIB** setzt sich aus den folgenden Quellen zusammen:

- **Automatisch erstellte Quellen:**
  - **Dynamische Routing-Protokolle** (**RIP**, **BGP**, **LISP**, **OSPF**)
  - **DHCP**
  - **IPv6-Auto-Config**
- **Manuell erstellte Quellen:**
  - **Routing-Tabelle** (IPv4-Routing-Tabelle bzw. IPv6-Routing-Tabelle)
  - **LAN-Interface** (IPv4- bzw. IPv6-Netzwerk)
  - **WAN-Interface** (IPv4- bzw. IPv6-Internet- und VPN-Verbindung)
  - **WAN-Tag-Tabelle** (nur IPv4)
  - **Loopback-Adressen**

Es wird für jedes Routing-Tag eine eigene Tabelle in der **FIB** erstellt.

6.2.1.1 Allgemeine Regeln

Für jedes vergebene Routing-Tag muss eine Route in der **FIB** mit diesem Tag existieren, damit die Kommunikation möglich ist. Es erfolgt **kein Rückfall auf eine Route mit Routing-Tag 0**.

Eine Tabelle mit Tag 0 existiert immer, diese kann aber leer sein.

6.2.1.2 Spezifische Regeln

Die folgenden spezifischen Regeln werden beim Hinzufügen von Einträgen in die **FIB** der Reihe nach durchlaufen:

Regel 1: Routen mit gleichem Ziel

Routen-Kollisionen sind nach Möglichkeit zu vermeiden.

1. **Ergänzen einer Route bei bereits vorhandener Route mit gleichem Ziel und unterschiedlichen Routing-Tags**

   Soll ein **Routing-Eintrag in die FIB eingetragen** werden und eine weitere **Route mit dem gleichen Ziel und einem anderen Routing-Tag ist schon vorhanden**, dann wird die **vorhandene Route in der Tabelle mit dem neu hinzugekommenen Routing-Tag überschrieben.**

   Beispiel:

   - Das Netzwerk INTRANET (192.168.1.0/24) ist auf dem Router eingerichtet.
   - In der IPv4-Routing-Tabelle ist bereits ein Routing-Eintrag mit dem Ziel 192.168.45.0/24 und dem Routing-Tag 0 vorhanden, welcher auf die Internet-Gegenstelle INTERNET-DEFAULT (DHCPoE) verweist. Da es sich um einen Routing-Eintrag für eine WAN-Verbindung mit Routing-Tag 0 handelt (siehe **Regel 5)**), wird diese Route auch in allen anderen Routing-Tabellen eingetragen.

```
Rtg-Tag 0

 Prefix            Next-Hop        Interface                ID        Masquerading Redistribution Type (Distance)
 ------------------------------------------------------------------------------------------------------------------------
 0.0.0.0/0         192.168.45.254  INTERNET-DEFAULT         3         on           Redistribute   Static (5)
 10.0.0.0/24       192.168.1.253   INTRANET                 10        no           Down           Static Ifc Down (255)
 127.0.0.0/8       0.0.0.0         #Loopback                1         no           Never          Loopback (0)
 127.0.0.1/32      0.0.0.0         #Loopback                1         no           Never          Loopback (0)
 192.168.1.0/24    0.0.0.0         INTRANET                 10        no           Down           Connected LAN (2)
 192.168.1.254/32  0.0.0.0         #Loopback                1         no           Redistribute   Local LAN (0)
 192.168.45.0/24   0.0.0.0         INTERNET-DEFAULT         3         on           Redistribute   Connected WAN (2)
 192.168.45.139/32 0.0.0.0         #Loopback                1         no           Redistribute   Local WAN (0)
 192.168.45.254/32 0.0.0.0         INTERNET-DEFAULT         3         on           Redistribute   DHCP (15)

Rtg-Tag 5

 Prefix            Next-Hop        Interface                ID        Masquerading Redistribution Type (Distance)
 ------------------------------------------------------------------------------------------------------------------------
 0.0.0.0/0         192.168.45.254  INTERNET-DEFAULT         3         on           Redistribute   Static (5)
 10.0.0.0/24       192.168.1.253   INTRANET                 10        no           Down           Static Ifc Down (255)
 127.0.0.0/8       0.0.0.0         #Loopback                1         no           Never          Loopback (0)
 127.0.0.1/32      0.0.0.0         #Loopback                1         no           Never          Loopback (0)
 192.168.45.0/24   0.0.0.0         INTERNET-DEFAULT         3         on           Redistribute   Connected WAN (2)
 192.168.45.139/32 0.0.0.0         #Loopback                1         no           Redistribute   Local WAN (0)
 192.168.45.254/32 0.0.0.0         INTERNET-DEFAULT         3         on           Redistribute   DHCP (15)
```

- In der IPv4-Routing-Tabelle wird ein weiterer Eintrag für das Ziel 192.168.45.0/24 mit dem Routing-Tag 5 hinzugefügt, welcher auf die Internet-Gegenstelle INTERNET-DEFAULT verweist.
  - Die statische Route mit Routing-Tag 5 überschreibt in der Tabelle mit dem Tag 5 die DHCPoE-Route.

```
Rtg-Tag 0

 Prefix            Next-Hop        Interface                ID        Masquerading Redistribution Type (Distance)
 ------------------------------------------------------------------------------------------------------------------------
 0.0.0.0/0         192.168.45.254  INTERNET-DEFAULT         3         on           Redistribute   Static (5)
 10.0.0.0/24       192.168.1.253   INTRANET                 10        no           Down           Static Ifc Down (255)
 127.0.0.0/8       0.0.0.0         #Loopback                1         no           Never          Loopback (0)
 127.0.0.1/32      0.0.0.0         #Loopback                1         no           Never          Loopback (0)
 192.168.1.0/24    0.0.0.0         INTRANET                 10        no           Down           Connected LAN (2)
 192.168.1.254/32  0.0.0.0         #Loopback                1         no           Redistribute   Local LAN (0)
 192.168.45.0/24   0.0.0.0         INTERNET-DEFAULT         3         on           Redistribute   Connected WAN (2)
 192.168.45.139/32 0.0.0.0         #Loopback                1         no           Redistribute   Local WAN (0)
 192.168.45.254/32 0.0.0.0         INTERNET-DEFAULT         3         on           Redistribute   DHCP (15)

Rtg-Tag 5

 Prefix            Next-Hop        Interface                ID        Masquerading Redistribution Type (Distance)
 ------------------------------------------------------------------------------------------------------------------------
 0.0.0.0/0         192.168.45.254  INTERNET-DEFAULT         3         on           Redistribute   Static (5)
 10.0.0.0/24       192.168.1.253   INTRANET                 10        no           Down           Static Ifc Down (255)
 127.0.0.0/8       0.0.0.0         #Loopback                1         no           Never          Loopback (0)
 127.0.0.1/32      0.0.0.0         #Loopback                1         no           Never          Loopback (0)
 192.168.45.0/24   0.0.0.0         INTERNET-DEFAULT         3         on           Redistribute   Static (5)
 192.168.45.139/32 0.0.0.0         #Loopback                1         no           Redistribute   Local WAN (0)
 192.168.45.254/32 0.0.0.0         INTERNET-DEFAULT         3         on           Redistribute   DHCP (15)
```

2. **Ergänzen mehrerer Routen mit gleichem Ziel sowie unterschiedlichen und in der FIB unbekannten Routing-Tags**

   Sollen **mehrere Routen mit dem gleichen Ziel sowie unterschiedlichen Routing-Tags in die FIB eingetragen** werden und das **Routing-Tag der Routen ist noch nicht in der FIB bekannt**, wird die **Route in alle Tabellen kopiert, die diese Route noch nicht kennen.**

   Beispiel 1:

   - Neben dem Netzwerk INTRANET (192.168.45.0/24) sind zwei DMZ-Netzwerke éingerichtet (DMZ1 mit 192.168.10.0/24 und DMZ2 mit 192.168.20.0/24).
   - In der IPv4-Routing-Tabelle ist bereits ein Routing-Eintrag für das Ziel 10.0.0.0/24 mit dem Routing-Tag 5 vorhanden, sodass es in der FIB eine Tabelle für das Routing-Tag 5 gibt.

```
Rtg-Tag 0

 Prefix            Next-Hop        Interface                ID        Masquerading Redistribution Type (Distance)
 ------------------------------------------------------------------------------------------------------------------
 0.0.0.0/0         0.0.0.0         INTERNET-DEFAULT         3         on           Down           Static Ifc Down (255)
 10.0.0.0/24       192.168.45.254  INTRANET                 4         no           Redistribute   Static (5)
 127.0.0.0/8       0.0.0.0         #Loopback                1         no           Never          Loopback (0)
 127.0.0.1/32      0.0.0.0         #Loopback                1         no           Never          Loopback (0)
 192.168.10.0/24   0.0.0.0         DMZ1                     7         no           Redistribute   Connected LAN (2)
 192.168.10.254/32 0.0.0.0         #Loopback                1         no           Redistribute   Local LAN (0)
 192.168.20.0/24   0.0.0.0         DMZ2                     8         no           Redistribute   Connected LAN (2)
 192.168.20.254/32 0.0.0.0         #Loopback                1         no           Redistribute   Local LAN (0)
 192.168.45.0/24   0.0.0.0         INTRANET                 4         no           Redistribute   Connected LAN (2)
 192.168.45.100/32 0.0.0.0         #Loopback                1         no           Redistribute   Local LAN (0)

Rtg-Tag 5

 Prefix            Next-Hop        Interface                ID        Masquerading Redistribution Type (Distance)
 ------------------------------------------------------------------------------------------------------------------
 0.0.0.0/0         0.0.0.0         INTERNET-DEFAULT         3         on           Down           Static Ifc Down (255)
 10.0.0.0/24       192.168.45.254  INTRANET                 4         no           Redistribute   Static (5)
 127.0.0.0/8       0.0.0.0         #Loopback                1         no           Never          Loopback (0)
 127.0.0.1/32      0.0.0.0         #Loopback                1         no           Never          Loopback (0)
 192.168.10.0/24   0.0.0.0         DMZ1                     7         no           Redistribute   Connected LAN (2)
 192.168.10.254/32 0.0.0.0         #Loopback                1         no           Redistribute   Local LAN (0)
 192.168.20.0/24   0.0.0.0         DMZ2                     8         no           Redistribute   Connected LAN (2)
 192.168.20.254/32 0.0.0.0         #Loopback                1         no           Redistribute   Local LAN (0)
```

- In der IPv4-Routing-Tabelle werden zwei Routen mit dem Ziel 192.168.1.0/24 für die Routing-Tags 1 und 2 hinzugefügt, die als Next-Hop jeweils auf eine IP-Adresse in einer der DMZ-Netzwerke verweisen (Routing-Tag 1 auf die IP-Adresse 192.168.10.253 in der DMZ1 und Routing-Tag 2 auf die IP-Adresse 192.168.20.253 in der DMZ2).
  - Die Route für das Interface DMZ1 wird in der FIB sowohl in die Tabelle mit dem Tag 0 als auch in die Tabelle für das Tag 5 eingetragen.

```
Rtg-Tag 0

 Prefix            Next-Hop        Interface                ID        Masquerading Redistribution Type (Distance)
 ------------------------------------------------------------------------------------------------------------------
 0.0.0.0/0         0.0.0.0         INTERNET-DEFAULT         3         on           Down           Static Ifc Down (255)
 10.0.0.0/24       192.168.45.254  INTRANET                 4         no           Redistribute   Static (5)
 127.0.0.0/8       0.0.0.0         #Loopback                1         no           Never          Loopback (0)
 127.0.0.1/32      0.0.0.0         #Loopback                1         no           Never          Loopback (0)
 192.168.1.0/24    192.168.10.253  DMZ1                     11        no           Redistribute   Static (5)
 192.168.10.0/24   0.0.0.0         DMZ1                     11        no           Redistribute   Connected LAN (2)
 192.168.10.254/32 0.0.0.0         #Loopback                1         no           Redistribute   Local LAN (0)
 192.168.20.0/24   0.0.0.0         DMZ2                     12        no           Redistribute   Connected LAN (2)
 192.168.20.254/32 0.0.0.0         #Loopback                1         no           Redistribute   Local LAN (0)
 192.168.45.0/24   0.0.0.0         INTRANET                 4         no           Redistribute   Connected LAN (2)
 192.168.45.100/32 0.0.0.0         #Loopback                1         no           Redistribute   Local LAN (0)

Rtg-Tag 1

 Prefix            Next-Hop        Interface                ID        Masquerading Redistribution Type (Distance)
 ------------------------------------------------------------------------------------------------------------------
 0.0.0.0/0         0.0.0.0         INTERNET-DEFAULT         3         on           Down           Static Ifc Down (255)
 127.0.0.0/8       0.0.0.0         #Loopback                1         no           Never          Loopback (0)
 127.0.0.1/32      0.0.0.0         #Loopback                1         no           Never          Loopback (0)
 192.168.1.0/24    192.168.10.253  DMZ1                     11        no           Redistribute   Static (5)
 192.168.10.0/24   0.0.0.0         DMZ1                     11        no           Redistribute   Connected LAN (2)
 192.168.10.254/32 0.0.0.0         #Loopback                1         no           Redistribute   Local LAN (0)
 192.168.20.0/24   0.0.0.0         DMZ2                     12        no           Redistribute   Connected LAN (2)
 192.168.20.254/32 0.0.0.0         #Loopback                1         no           Redistribute   Local LAN (0)

Rtg-Tag 2

 Prefix            Next-Hop        Interface                ID        Masquerading Redistribution Type (Distance)
 ------------------------------------------------------------------------------------------------------------------
 0.0.0.0/0         0.0.0.0         INTERNET-DEFAULT         3         on           Down           Static Ifc Down (255)
 127.0.0.0/8       0.0.0.0         #Loopback                1         no           Never          Loopback (0)
 127.0.0.1/32      0.0.0.0         #Loopback                1         no           Never          Loopback (0)
 192.168.1.0/24    192.168.20.253  DMZ2                     12        no           Redistribute   Static (5)
 192.168.10.0/24   0.0.0.0         DMZ1                     11        no           Redistribute   Connected LAN (2)
 192.168.10.254/32 0.0.0.0         #Loopback                1         no           Redistribute   Local LAN (0)
 192.168.20.0/24   0.0.0.0         DMZ2                     12        no           Redistribute   Connected LAN (2)
 192.168.20.254/32 0.0.0.0         #Loopback                1         no           Redistribute   Local LAN (0)

Rtg-Tag 5

 Prefix            Next-Hop        Interface                ID        Masquerading Redistribution Type (Distance)
 ------------------------------------------------------------------------------------------------------------------
 0.0.0.0/0         0.0.0.0         INTERNET-DEFAULT         3         on           Down           Static Ifc Down (255)
 10.0.0.0/24       192.168.45.254  INTRANET                 4         no           Redistribute   Static (5)
 127.0.0.0/8       0.0.0.0         #Loopback                1         no           Never          Loopback (0)
 127.0.0.1/32      0.0.0.0         #Loopback                1         no           Never          Loopback (0)
 192.168.1.0/24    192.168.10.253  DMZ1                     11        no           Redistribute   Static (5)
 192.168.10.0/24   0.0.0.0         DMZ1                     11        no           Redistribute   Connected LAN (2)
 192.168.10.254/32 0.0.0.0         #Loopback                1         no           Redistribute   Local LAN (0)
 192.168.20.0/24   0.0.0.0         DMZ2                     12        no           Redistribute   Connected LAN (2)
 192.168.20.254/32 0.0.0.0         #Loopback                1         no           Redistribute   Local LAN (0)
```

Beispiel 2:

- Neben dem Netzwerk INTRANET (192.168.45.0/24) mit dem Tag 0 ist eine DMZ (192.168.10.0/24) mit dem Tag 0 auf dem Router eingerichtet und somit sind auch beide in der FIB in der Tabelle für das Routing-Tag 0 vorhanden.
- In der IPv4-Routing-Tabelle ist bereits ein Routing-Eintrag für das Ziel 10.0.0.0/24 mit dem Routing-Tag 5 vorhanden, sodass es in der FIB eine Tabelle für das Routing-Tag 5 gibt.

```
Rtg-Tag 0

 Prefix            Next-Hop        Interface                ID        Masquerading Redistribution Type (Distance)
 ------------------------------------------------------------------------------------------------------------------------
 0.0.0.0/0         0.0.0.0         INTERNET-DEFAULT         3         on           Down           Static Ifc Down (255)
 10.0.0.0/24       192.168.45.254  INTRANET                 4         no           Redistribute   Static (5)
 127.0.0.0/8       0.0.0.0         #Loopback                1         no           Never          Loopback (0)
 127.0.0.1/32      0.0.0.0         #Loopback                1         no           Never          Loopback (0)
 192.168.10.0/24   0.0.0.0         DMZ                      9         no           Redistribute   Connected LAN (2)
 192.168.10.254/32 0.0.0.0         #Loopback                1         no           Redistribute   Local LAN (0)
 192.168.45.0/24   0.0.0.0         INTRANET                 4         no           Redistribute   Connected LAN (2)
 192.168.45.100/32 0.0.0.0         #Loopback                1         no           Redistribute   Local LAN (0)

Rtg-Tag 5

 Prefix            Next-Hop        Interface                ID        Masquerading Redistribution Type (Distance)
 ------------------------------------------------------------------------------------------------------------------------
 0.0.0.0/0         0.0.0.0         INTERNET-DEFAULT         3         on           Down           Static Ifc Down (255)
 10.0.0.0/24       192.168.45.254  INTRANET                 4         no           Redistribute   Static (5)
 127.0.0.0/8       0.0.0.0         #Loopback                1         no           Never          Loopback (0)
 127.0.0.1/32      0.0.0.0         #Loopback                1         no           Never          Loopback (0)
 192.168.10.0/24   0.0.0.0         DMZ                      9         no           Redistribute   Connected LAN (2)
 192.168.10.254/32 0.0.0.0         #Loopback                1         no           Redistribute   Local LAN (0)
```

- In der IPv4-Routing-Tabelle wird eine Route mit dem Ziel 192.168.45.0/24 und dem Tag 1 hinzugefügt, welche als Next-Hop auf die IP-Adresse 192.168.10.253 in der DMZ verweist.
  - Die Route für die DMZ wird in der FIB in die Tabelle mit dem Tag 5 eingetragen aber nicht in die Tabelle mit dem Tag 0, da bereits ein Eintrag mit dem Tag 0 existiert (INTRANET) und der vorhandene Eintrag bevorzugt wird.

```
Rtg-Tag 0

 Prefix            Next-Hop        Interface                ID        Masquerading Redistribution Type (Distance)
 ------------------------------------------------------------------------------------------------------------------------
 0.0.0.0/0         0.0.0.0         INTERNET-DEFAULT         3         on           Down           Static Ifc Down (255)
 10.0.0.0/24       192.168.45.254  INTRANET                 4         no           Redistribute   Static (5)
 127.0.0.0/8       0.0.0.0         #Loopback                1         no           Never          Loopback (0)
 127.0.0.1/32      0.0.0.0         #Loopback                1         no           Never          Loopback (0)
 192.168.10.0/24   0.0.0.0         DMZ                      13        no           Redistribute   Connected LAN (2)
 192.168.10.254/32 0.0.0.0         #Loopback                1         no           Redistribute   Local LAN (0)
 192.168.45.0/24   0.0.0.0         INTRANET                 4         no           Redistribute   Connected LAN (2)
 192.168.45.100/32 0.0.0.0         #Loopback                1         no           Redistribute   Local LAN (0)

Rtg-Tag 1

 Prefix            Next-Hop        Interface                ID        Masquerading Redistribution Type (Distance)
 ------------------------------------------------------------------------------------------------------------------------
 0.0.0.0/0         0.0.0.0         INTERNET-DEFAULT         3         on           Down           Static Ifc Down (255)
 127.0.0.0/8       0.0.0.0         #Loopback                1         no           Never          Loopback (0)
 127.0.0.1/32      0.0.0.0         #Loopback                1         no           Never          Loopback (0)
 192.168.10.0/24   0.0.0.0         DMZ                      13        no           Redistribute   Connected LAN (2)
 192.168.10.254/32 0.0.0.0         #Loopback                1         no           Redistribute   Local LAN (0)
 192.168.45.0/24   192.168.10.253  DMZ                      13        no           Redistribute   Static (5)

Rtg-Tag 5

 Prefix            Next-Hop        Interface                ID        Masquerading Redistribution Type (Distance)
 ------------------------------------------------------------------------------------------------------------------------
 0.0.0.0/0         0.0.0.0         INTERNET-DEFAULT         3         on           Down           Static Ifc Down (255)
 10.0.0.0/24       192.168.45.254  INTRANET                 4         no           Redistribute   Static (5)
 127.0.0.0/8       0.0.0.0         #Loopback                1         no           Never          Loopback (0)
 127.0.0.1/32      0.0.0.0         #Loopback                1         no           Never          Loopback (0)
 192.168.10.0/24   0.0.0.0         DMZ                      13        no           Redistribute   Connected LAN (2)
 192.168.10.254/32 0.0.0.0         #Loopback                1         no           Redistribute   Local LAN (0)
 192.168.45.0/24   192.168.10.253  DMZ                      13        no           Redistribute   Static (5)
```

3. **Ergänzen mehrerer Routen mit gleichem Ziel sowie unterschiedlichen Routing-Tags und Einfügen der Route in der FIB in die Tabelle mit dem Tag 0**

   Werden **mehrere Routen mit dem gleichen Ziel sowie unterschiedlichen Routing-Tags hinzugefügt**, wird die **Route mit dem niedrigeren Tag in die Tabelle mit dem Tag 0 hinzugefügt**, es sei denn es gibt dort bereits eine Route mit dem Tag 0.

   Beispiel:

- Im Router ist das Netzwerk INTRANET (192.168.45.0/24) eingerichtet.

```
Rtg-Tag 0

 Prefix             Next-Hop        Interface                ID        Masquerading Redistribution Type (Distance)
 ------------------------------------------------------------------------------------------------------------------------
 0.0.0.0/0          0.0.0.0         INTERNET-DEFAULT         3         on           Down           Static Ifc Down (255)
 127.0.0.0/8        0.0.0.0         #Loopback                1         no           Never          Loopback (0)
 127.0.0.1/32       0.0.0.0         #Loopback                1         no           Never          Loopback (0)
 192.168.45.0/24    0.0.0.0         INTRANET                 4         no           Redistribute   Connected LAN (2)
 192.168.45.100/32  0.0.0.0         #Loopback                1         no           Redistribute   Local LAN (0)
```

- In der IPv4-Routing-Tabelle werden zwei Routen mit dem Ziel 192.168.1.0/24 und den Routing-Tags 2 und 5 hinzugefügt, welche als Next-Hop jeweils auf eine IP-Adresse aus dem Netzwerk INTRANET verweisen (Tag 2 auf 192.168.45.253 und Tag 5 auf 192.168.45.254).
  - Die Route mit dem Tag 2 wird in die Tabelle mit dem Tag 0 übernommen.

```
Rtg-Tag 0

 Prefix             Next-Hop        Interface                ID        Masquerading Redistribution Type (Distance)
 ------------------------------------------------------------------------------------------------------------------------
 0.0.0.0/0          0.0.0.0         INTERNET-DEFAULT         3         on           Down           Static Ifc Down (255)
 127.0.0.0/8        0.0.0.0         #Loopback                1         no           Never          Loopback (0)
 127.0.0.1/32       0.0.0.0         #Loopback                1         no           Never          Loopback (0)
 192.168.1.0/24     192.168.45.253  INTRANET                 4         no           Redistribute   Static (5)
 192.168.45.0/24    0.0.0.0         INTRANET                 4         no           Redistribute   Connected LAN (2)
 192.168.45.100/32  0.0.0.0         #Loopback                1         no           Redistribute   Local LAN (0)

Rtg-Tag 2

 Prefix             Next-Hop        Interface                ID        Masquerading Redistribution Type (Distance)
 ------------------------------------------------------------------------------------------------------------------------
 0.0.0.0/0          0.0.0.0         INTERNET-DEFAULT         3         on           Down           Static Ifc Down (255)
 127.0.0.0/8        0.0.0.0         #Loopback                1         no           Never          Loopback (0)
 127.0.0.1/32       0.0.0.0         #Loopback                1         no           Never          Loopback (0)
 192.168.1.0/24     192.168.45.253  INTRANET                 4         no           Redistribute   Static (5)

Rtg-Tag 5

 Prefix             Next-Hop        Interface                ID        Masquerading Redistribution Type (Distance)
 ------------------------------------------------------------------------------------------------------------------------
 0.0.0.0/0          0.0.0.0         INTERNET-DEFAULT         3         on           Down           Static Ifc Down (255)
 127.0.0.0/8        0.0.0.0         #Loopback                1         no           Never          Loopback (0)
 127.0.0.1/32       0.0.0.0         #Loopback                1         no           Never          Loopback (0)
 192.168.1.0/24     192.168.45.254  INTRANET                 4         no           Redistribute   Static (5)
```

4. **Abweichende Regelung für Routen mit dem Interface DMZ**

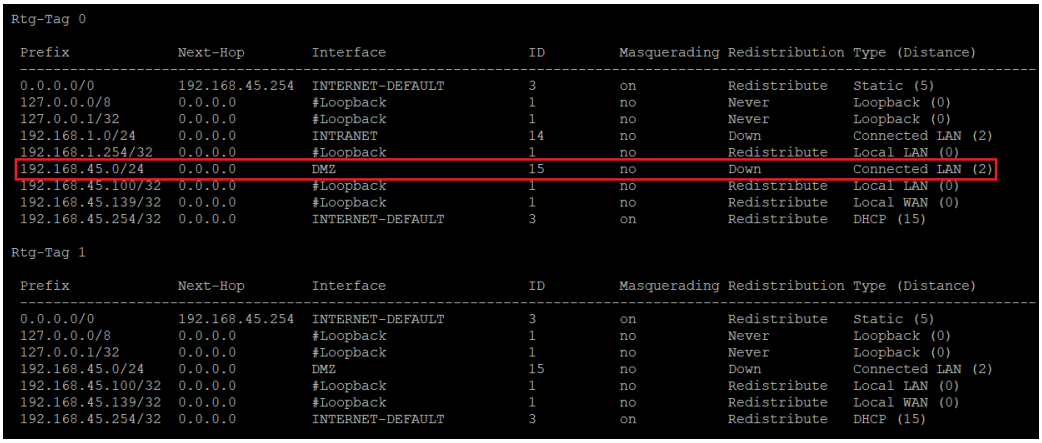
   Abweichend hiervon können **Routen mit dem Interface DMZ, welche aus einem anderen Tag kommen, Routen mit dem Typ Connected WAN in dem ursprünglichen Tag der Connected WAN Route verdrängen, sofern sie dasselbe Ziel-Netzwerk haben**.

   Beispiel:

   - Im Router ist das Netzwerk INTRANET (192.168.1.0/24) eingerichtet.
   - Ein Routing-Eintrag für das Ziel 192.168.45.0/24 mit dem Tag 0 ist bereits vorhanden. Es handelt sich dabei um eine separate Route einer DHCPoE-Verbindung (Connected WAN).

```
Rtg-Tag 0

 Prefix             Next-Hop        Interface                ID        Masquerading Redistribution Type (Distance)
 ------------------------------------------------------------------------------------------------------------------------
 0.0.0.0/0          192.168.45.254  INTERNET-DEFAULT         3         on           Redistribute   Static (5)
 127.0.0.0/8        0.0.0.0         #Loopback                1         no           Never          Loopback (0)
 127.0.0.1/32       0.0.0.0         #Loopback                1         no           Never          Loopback (0)
 192.168.1.0/24     0.0.0.0         INTRANET                 14        no           Down           Connected LAN (2)
 192.168.1.254/32   0.0.0.0         #Loopback                1         no           Redistribute   Local LAN (0)
 192.168.45.0/24    0.0.0.0         INTERNET-DEFAULT         3         on           Redistribute   Connected WAN (2)
 192.168.45.139/32  0.0.0.0         #Loopback                1         no           Redistribute   Local WAN (0)
 192.168.45.254/32  0.0.0.0         INTERNET-DEFAULT         3         on           Redistribute   DHCP (15)
```

   - Es wird eine DMZ (192.168.45.0/24) mit dem Tag 1 erstellt.
     - Die ursprüngliche Route des Typs Connected WAN wird durch die Route der DMZ überschrieben.



```
Rtg-Tag 0

 Prefix            Next-Hop        Interface               ID        Masquerading Redistribution Type (Distance)
 ------------------------------------------------------------------------------------------------------------------------
 0.0.0.0/0         192.168.45.254  INTERNET-DEFAULT        3         on           Redistribute   Static (5)
 127.0.0.0/8       0.0.0.0         #Loopback               1         no           Never          Loopback (0)
 127.0.0.1/32      0.0.0.0         #Loopback               1         no           Never          Loopback (0)
 192.168.1.0/24    0.0.0.0         INTRANET                14        no           Down           Connected LAN (2)
 192.168.1.254/32  0.0.0.0         #Loopback               1         no           Redistribute   Local LAN (0)
 192.168.45.0/24   0.0.0.0         DMZ                     15        no           Down           Connected LAN (2)
 192.168.45.100/32 0.0.0.0         #Loopback               1         no           Redistribute   Local LAN (0)
 192.168.45.139/32 0.0.0.0         #Loopback               1         no           Redistribute   Local WAN (0)
 192.168.45.254/32 0.0.0.0         INTERNET-DEFAULT        3         on           Redistribute   DHCP (15)

Rtg-Tag 1

 Prefix            Next-Hop        Interface               ID        Masquerading Redistribution Type (Distance)
 ------------------------------------------------------------------------------------------------------------------------
 0.0.0.0/0         192.168.45.254  INTERNET-DEFAULT        3         on           Redistribute   Static (5)
 127.0.0.0/8       0.0.0.0         #Loopback               1         no           Never          Loopback (0)
 127.0.0.1/32      0.0.0.0         #Loopback               1         no           Never          Loopback (0)
 192.168.45.0/24   0.0.0.0         DMZ                     15        no           Down           Connected LAN (2)
 192.168.45.100/32 0.0.0.0         #Loopback               1         no           Redistribute   Local LAN (0)
 192.168.45.139/32 0.0.0.0         #Loopback               1         no           Redistribute   Local WAN (0)
 192.168.45.254/32 0.0.0.0         INTERNET-DEFAULT        3         on           Redistribute   DHCP (15)
```

Regel 2: Dynamische Routing-Protokolle

Handelt es sich bei der **Quelle der Route um ein dynamisches Routingprotokoll** (**eBGP**, **iBGP**, **OSPF**, **RIP**, **LISP**), wird die **Route in der FIB nur in die Tabelle eingefügt, deren Routing-Tag übergeben wurde**

Regel 3: Konfiguration einer Loopback-Adresse

- Wird ein **Routing-Tag 0** eingetragen, wird die **Route in der FIB in alle Tabellen eingefügt**.
- Wird ein **Routing-Tag ungleich 0** eingetragen, wird die **Route in der FIB in die Tabelle mit dem vergebenen Routing-Tag** und **zusätzlich in die Tabelle mit dem Routing-Tag 0 eingefügt**.

Regel 4: Routen mit dem Ziel DMZ sind aus allen Netzwerken erreichbar

Routen mit dem Ziel DMZ (etwa ein **IP-Netzwerk mit dem Typ DMZ**) können über ein beliebiges Routing-Tag angesprochen werden, da für die **DMZ** automatisch ein Eintrag in der **FIB** für jedes im Router konfigurierte Routing-Tag erstellt wird.

Regel 5: Routen mit einem Ziel im WAN und Behandlung statischer Routen

- Handelt es sich um eine **Route mit Routing-Tag 0** mit einem **Zielinterface des Typs WAN** (Internet-Gegenstelle) **oder** es wird eine **statische Route mit Routing-Tag 0** konfiguriert (in der IPv4- / IPv6-Routing-Tabelle), wird die **Route in der FIB in alle Tabellen eingefügt**.
- Handelt es sich um eine **Route mit einem Tag ungleich 0**, wird die **Route in der FIB mit dem konfigurierten Tag eingefügt**.

Regel 6: Routen mit einem Ziel im LAN

- Wird eine **Route mit einem Ziel im LAN** (etwa ein **IPv4- / IPv6-Netzwerk**) **mit Routing-Tag 0** eingetragen, wird die **Route in der FIB lediglich in die Tabelle mit dem Routing-Tag 0 eingefügt**.
- Wird eine **Route mit einem Ziel im LAN** (etwa ein **IPv4- / IPv6-Netzwerk**) **mit einem Routing-Tag ungleich 0** eingetragen, wird die **Route in der FIB in die Tabelle mit dem vergebenen Routing-Tag** und **zusätzlich in die Tabelle mit dem Routing-Tag 0 eingefügt**.

Regel 7: Verhalten bei nicht bereits aufgeführtem Fall

Wenn keine der oben genannten Regeln zutrifft, wird die **Route in der FIB nur in die Tabelle mit dem übertragenen Routing-Tag der Route eingefügt**.

Wird ein **Routing-Eintrag aus der FIB entfernt**, wird nach einem **gleichwertigen Ersatz gesucht, der den in Regel 1 – 7 beschriebenen Regeln genügt**. Existiert in der **FIB kein Routing-Eintrag mehr für ein bestimmtes Routing-Tag**, wird die **zugehörige Tabelle gelöscht**.

6.2.1.3 Weitere Beispiele

SIP-Leitung mit Routing-Tag 10

1. Einer **SIP-Leitung** wird das **Routing-Tag 10** zugewiesen. Es gibt ein **IP-Netzwerk** namens **INTRANET** mit dem **Schnittstellen-Tag 0** und eine **Default-Route** namens **INTERNET** mit dem **Routing-Tag 0**.

   › In diesem Fall **kann die SIP-Leitung nicht registriert werden**, da das **Routing-Tag 10 in keiner der Tabellen vorhanden** ist.

2. Einer **SIP-Leitung** wird das **Routing-Tag 10** zugewiesen. Es gibt ein **IP-Netzwerk** namens **INTRANET** mit dem **Schnittstellen-Tag 10** und eine **Default-Route** namens **INTERNET** mit dem **Routing-Tag 0**.

   › In diesem Fall **kann die SIP-Leitung registriert werden**, da das **Routing-Tag 10 in dem IP-Netzwerk INTRANET vorhanden** ist.

3. Einer **SIP-Leitung** wird das **Routing-Tag 10** zugewiesen. Es gibt ein **IP-Netzwerk** namens **INTRANET** mit dem **Schnittstellen-Tag 0** und eine **Default-Route** namens **INTERNET** mit dem **Routing-Tag 10**.

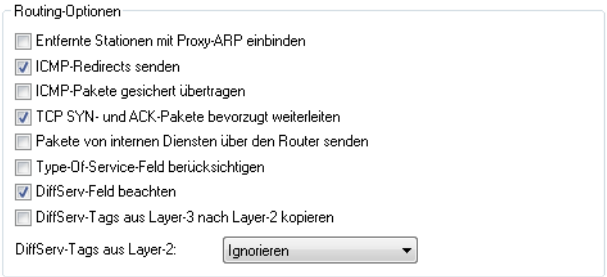
   › In diesem Fall **kann die SIP-Leitung registriert werden**, da das **Routing-Tag 10 in der DEFAULT-Route INTERNET vorhanden** ist.

Sonderfall: WAN-Tag-Tabelle

Soll ein **Portforwarding** bzw. eine **VPN-Einwahl** auf eine Internet-Verbindung mit einem **von 0 abweichenden Routing-Tag** erfolgen und das **Weiterleitungsziel hat das Tag 0**, muss in der **WAN-Tag-Tabelle** ein **Eintrag für die Internet-Verbindung** mit dem **gleichen Routing-Tag** (in diesem Beispiel das **Tag 1**) hinterlegt werden, damit die Antwort-Pakete über diese Internet-Verbindung geleitet werden. Ansonsten werden die **Antwort-Pakete über die Internet-Verbindung mit dem Routing-Tag 0** gesendet. Weiterhin muss eine **Firewall-Regel mit dem Routing-Tag 65535** erstellt werden, welche das per **WAN-Tag-Tabelle** gesetzte Tag wieder entfernt. Anderenfalls wird das für das lokale Netzwerk bestimmte Paket wieder über eine passende Route versendet (etwa die Internet-Verbindung).

6.2.2 Routing-Optionen

In LANconfig konfigurieren Sie die allgemeinen Routing-Optionen unter **IP-Router** > **Allgemein**.



Entfernte Stationen mit Proxy-ARP einbinden

Hier aktivieren bzw. deaktivieren Sie den Proxy-ARP-Mechanismus. Mit Proxy-ARP binden Sie entfernte Rechner in Ihr lokales Netz so ein, als befänden sie sich in Ihrem lokalen Netz.

ICMP-Redirects senden

Sie kennen das folgende Verhalten der Arbeitsplatzrechner in einem lokalen Netz: Möchte der Rechner ein Datenpaket an eine IP-Adresse senden, die nicht in seinem eigenen LAN liegt, sucht er nach einem Router,

der ihm weiterhelfen kann. Dieser Router wird normalerweise dem Betriebssystem durch den Eintrag als Standard-Router oder Standard-Gateway bekanntgegeben. Gibt es in einem Netz mehrere Router, so kann oft nur ein Standard-Router eingetragen werden, der alle dem Arbeitsplatzrechner unbekannten IP-Adressen erreichen können soll. Manchmal kann dieser Standard-Router jedoch nicht selbst das Zielnetz erreichen, er kennt aber einen anderen Router, der zu diesem Ziel findet.

Standardmäßig schickt der Router dem Rechner eine Antwort mit der Adresse des Routers, der die Route ins Ziel-Netz kennt (diese Antwort nennt man „ICMP-Redirect"). Der Arbeitsplatzrechner übernimmt daraufhin diese Adresse und schickt das Datenpaket sofort an den anderen Router.

Manche Rechner können mit den ICMP-Redirects leider nichts anfangen. Um die Datenpakete trotzdem zustellen zu können, verwenden Sie das lokale Routing. Dadurch weisen Sie den Router in Ihrem Gerät an, das Datenpaket selbst zum anderen, zuständigen Router zu senden. Außerdem sendet er dann keine ICMP-Redirects mehr an die Clients.



Lokales Routing kann im Einzelfall sehr hilfreich sein, sollte aber auch nur im Einzelfall verwendet werden. Denn lokales Routing führt zu einer Verdoppelung aller Datenpakete zum gewünschten Zielnetz. Die Daten werden erst zum Standard-Router und von diesem erneut zum eigentlich zuständigen Router im lokalen Netz geschickt.

Mit dieser Option bestimmen Sie, ob das Gerät ICMP-Redirects versenden soll.

ICMP-Pakete gesichert übertragen

Bestimmen Sie hier, ob das Gerät die ICMP-Redirects gesichert übertragen soll.

TCP SYN- und ACK-Pakete bevorzugt weiterleiten

Das SYN/ACK-Speedup-Verfahren dient der Beschleunigung des IP-Datenverkehrs. Beim SYN/ACK-Speedup werden IP-Kontrollzeichen (`SYN` für Synchronisation und `ACK` für Acknowledge) innerhalb des Sendebuffers gegenüber einfachen Datenpaketen bevorzugt behandelt. Dadurch wird die Situation vermieden, dass Kontrollzeichen länger in der Sende-Warteschlange hängen bleiben und die Gegenstelle deshalb aufhört, Daten zu senden.

Der größte Effekt tritt beim SYN/ACK-Speedup bei schnellen Anschlüssen (z. B. ADSL) ein, wenn gleichzeitig in beiden Richtungen mit hoher Geschwindigkeit Datenmengen übertragen werden.

Werkseitig ist der SYN/ACK-Speedup eingeschaltet.

Durch die bevorzugte Behandlung einzelner Pakete wird die ursprüngliche Paketreihenfolge geändert. Obwohl TCP/IP keine bestimmte Paketreihenfolge gewährleistet, kann es in einzelnen Anwendungen zu Problemen kommen. Das betrifft nur Anwendungen, die abweichend vom Protokollstandard eine bestimmte Paketreihenfolge voraussetzen. Für diesen Fall deaktivieren Sie den SYN/ACK-Speedup.

Pakete von internen Diensten über den Router senden

Lokale Dienste arbeiten standardmäßig immer am Router vorbei. Dabei werden Antwortpakete immer direkt an die MAC-Adresse zurückgeschickt, von der die Anfrage kam. Selektieren Sie diese Option, um Pakete von internen Diensten über den Router zu senden. Die Pakete werden dann nicht direkt an die MAC-Adresse des Absenders, sondern über den Router an den Absender zurückgeschickt (vorausgesetzt eine entsprechende Route ist dafür konfiguriert).

Type-of-Service-Feld berücksichtigen

Wenn Sie „Type-Of-Service" gewählt haben, wertet der Router bestimmte Optionen in IP-Paketen aus, die angeben, ob die Pakete besonders schnell oder gesichert übertragen werden sollen.

DiffServ-Feld beachten

Wenn der Router das DiffServ-Feld in IP-Paketen beachtet, dann benutzt er die standardisierten DSCPs (DiffServ Codepoints) `AFxx` (Assured Forwarding) zur gesicherten Übertragung und `EF` (Expedited Forwarding) zur bevorzugten Übertragung. Alle abweichend gekennzeichneten IP-Pakete werden normal übertragen. Standardmäßig ist diese Option aktiviert.

Diese Option ist nicht gleichzeitig mit ToS nutzbar, da das DiffServ-Feld innerhalb eines IP- Paketes das ToS-Feld ersetzt.

Mehr Informationen zu DiffServ erhalten Sie im Kapitel *Quality-of-Service*.

DiffServ-Tags aus Layer-3 nach Layer-2 kopieren

Die Einstellung für das Layer3-Layer2-Tagging regelt das Verhalten beim Senden eines Datenpakets. Wenn diese Option aktiviert ist, werden VLAN-Tags mit Prioritäts-Bits erzeugt, die aus der Precedence des DSCP stammen, wenn der Empfänger mindestens ein getaggtes Paket verschickt hat.

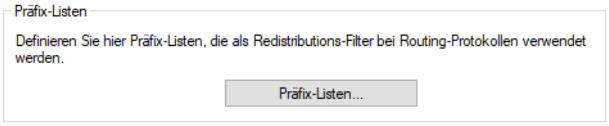
DiffServ-Tags aus Layer-2

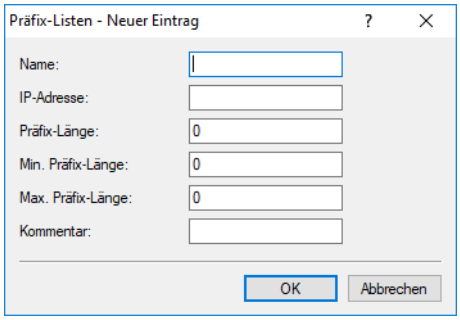
Die Einstellung für das Layer2-Layer3-Tagging regelt das Verhalten beim Empfangen eines Datenpakets:

- **Ignorieren**: VLAN-Tags werden ignoriert.
- **Nach Layer-3 kopieren**: Prioritäts-Bits im VLAN-Tag werden immer in die Precedence des DSCP kopiert.
- **Automatisch kopieren**: Prioritäts-Bits im VLAN-Tag werden nur dann in die Precedence des DSCP kopiert, wenn diese „000" ist.

6.2.3 Präfix-Listen

Mit Hilfe von Filterlisten für die Redistribution bei BGP, LISP und OSPF können bestimmte Präfixe für die Redistribution erlaubt oder verweigert werden. Dazu legen Sie die Präfix-Filterliste unter **IP-Router** > **Allgemein** > **Präfix-Listen** an.





Name

Geben Sie hier diesem Eintrag einen Namen. Präfixe, die zu einer Liste gehören sollen, werden über den gleichen Namen referenziert, z. B. Liste1.

IP-Adresse

Geben Sie hier die IPv4- oder IPv6-Adresse des Netzwerkes an.

Präfix-Länge

Enthält die Netzmaske oder Präfix-Länge des Netzwerkes. Dieser Eintrag legt fest, wie viele höchstwertige Bits (Most Significant Bit, MSB) der IP-Adresse für eine Übereinstimmung notwendig sind. Die Präfix-Länge muss für eine Übereinstimmung diesem Wert exakt entsprechen, wenn nicht für **Min. Präfix-Länge** und **Max. Präfix-Länge** andere Werte vorgegeben sind.

Beim Wert „0" stimmt das Präfix für diese Regel dann überein, wenn es aus derselben IP-Adressfamilie stammt, die unter **IP-Adresse** vorgegeben ist.

Min. Präfix-Länge

Geben Sie hier die minimale Präfix-Länge an, die das Präfix für eine Übereinstimmung aufweisen darf.

Max. Präfix-Länge

Geben Sie hier die maximale Präfix-Länge an, die das Präfix für eine Übereinstimmung aufweisen darf.

Kommentar

Kommentar zu diesem Eintrag.

Verwendung der Präfix-Listen bei BGP

Diese **Präfix-Listen** können Sie dann bei den IPv4- und IPv6-Adressfamilien des BGP-Protokolls referenzieren sowie definieren, ob diese Präfix-Listen erlaubt oder abgelehnt werden sollen.

Verwendung der Präfix-Listen bei LISP

Mit diesen **Präfix-Listen** können Sie dann für die Redistribution bei LISP bestimmte Präfixe für die Routen-Redistribution erlauben oder verweigern. Verwenden Sie die hier defintierten Präfixe für die Redistribution von statischen Routen, BGP, OSPF und verbundenen Routen.

Verwendung der Präfix-Listen bei OSPF

Mit diesen **Präfix-Listen** können Sie dann für die Redistribution bei OSPF bestimmte Präfixe für die Routen-Redistribution erlauben oder verweigern. Verwenden Sie die hier defintierten Präfixe für die Redistribution von statischen Routen, BGP und verbundenen Routen.

6.2.4 Die Routing-Tabelle

In der Routing-Tabelle wird definiert, an welche Gegenstelle – also an welchen anderen Router oder Rechner – der Router Daten für bestimmte IP-Adressen oder IP-Adress-Bereiche schicken soll. So ein Eintrag heißt auch „Route", weil damit der Weg der Datenpakete beschrieben wird. Da Sie diese Einträge selbst vornehmen und sie solange unverändert bleiben, bis Sie selbst sie wieder ändern oder löschen, heißt dieses Verfahren auch „statisches Routing". Im Gegensatz dazu gibt es natürlich auch ein „dynamisches Routing". Dabei tauschen die Router selbstständig untereinander Informationen über die Routen aus und erneuern diese fortlaufend. Dynamische Routing-Protokolle sind beispielsweise RIP, OSPF, BGP oder LISP. Wenn dynamische Routing-Protokolle aktiviert sind, beachtet der Router die statischen Routing-Einträge sowie die dynamischen Routing-Informationen.

Die statischen Unicast-Routen für IPv4 und IPv6 werden jeweils in getrennten Tabellen konfiguriert. Multicast-Routen werden über IGMP / MLD, PIM und die Tabellen für statische Multicast-Routen konfiguriert.

Außerdem sagen Sie dem Router in der statischen IPv4-Routing-Tabelle, wie weit der Weg über diese Route ist, damit im Zusammenspiel mit RIP bei mehreren Routen zum gleichen Ziel der günstigste Weg ausgewählt werden kann. Die Grundeinstellung für die RIP-Distanz zu einem anderen Router ist 0, d. h., der Router ist direkt erreichbar. Alle lokal erreichbaren Geräte, also weitere Router im eigenen LAN oder Arbeitsplatzrechner, die über Proxy-ARP angeschlossen sind, werden mit der Distanz 0 eingetragen. Mit dem gezielten Eintrag einer höheren RIP-Distanz (bis 14) wird die „Qualität" dieser Route herabgesetzt. Solche „schlechteren" Routen sollen nur dann verwendet werden, wenn keine andere Route zu der entsprechenden Gegenstelle gefunden werden kann.

6.2.4.1 Administrative Distanz

Über die administrative Distanz ist es möglich mehrere gleiche statische Routen bzw. Präfixe zu unterschiedlichen Gegenstellen zu konfigurieren. Die Route mit der geringsten administrativen Distanz ist die bevorzugt aktive Route. Über diesen Mechanismus lassen sich beispielsweise einfache Backup-Mechanismen konfigurieren.

Die Manipulation der administrativen Distanz für Routen von dynamischen Routen erfolgt bei dem jeweiligen dynamischen Routing-Protokoll.

Beispiel 1: Es sollen zwei VPN-Tunnel mit Route 192.168.2.0/24 konfiguriert werden. Der zweite VPN-Tunnel soll als „Always-On" Backup für den ersten VPN-Tunnel konfiguriert werden.

Für den ersten Tunnel wird das Präfix 192.168.2.0/24 auf die Gegenstellen VPN-1 mit einer administrativen Distanz von 10 eingerichtet, für den zweiten Tunnel wird das Präfix 192.168.2.0/24 auf die Gegenstellen VPN-2 mit einer administrativen Distanz von 20 eingerichtet. Beide VPN-Tunnel werden aufgebaut, aber nur für den ersten VPN-Tunnel wird die Route aktiv, da diese die bessere / niedrigere administrative Distanz hat. Ist der erste VPN-Tunnel nicht verbunden, so setzt das Betriebssystem diese Route auf die administrative Distanz von 255 (Interface Down), womit die Route über den zweiten Tunnel automatisch aktiv wird.

Beispiel 2: Es existiert eine statische Route für 192.168.1.0/24 zur Gegenstellen VPN-Tunnel1. Wird das gleiche Präfix 192.168.1.0/24 nun über BGP empfangen, so hat die statische Route im Default eine bessere / niedrigere administrative Distanz, so dass diese verwendet wird und nicht die Route über BGP.

Setzt man nun die administrative Distanz der statischen Route auf den Wert 210, so wird die über BGP gelernte Route bevorzugt und aktiv, da (e)BGP eine administrative Distanz von 20 bzw. 200 (iBGP) hat. Somit dient die statische Route als Backup für die dynamische BGP-Route.

Diese Funktion ersetzt nicht die Funktion der Backup-Tabelle, sondern stellt eine andere Art von „Backup" zur Verfügung. Bei Verwendung der Backup-Tabelle ist immer nur eine Verbindung aktiv. Im Backup-Fall wird versucht die Backup-Verbindung zu aktivieren. Wenn die Backup-Verbindung aktiv ist, wird versucht, im Hintergrund die primäre Verbindung wieder aufzubauen und im Erfolgsfall wieder umzuschalten. Die Backup-Strategie über die administrative Distanz geht davon aus, dass alle Gegenstellen immer aufgebaut sind. Dies ist in bestimmten Szenarien, z. B. Backup über Mobilfunk nicht immer gewünscht und die Backup-Tabelle ist dann die bevorzugte Wahl.



Die Backup-Funktion über die Backuptabelle und ein Backup über administrative Distanzen schließen sich gegenseitig aus.

Der Wert 0 hat eine Sonderfunktion und ist intern der niedrigste Wert, der für eigene Adressen des Gerätes reserviert ist (also für die Quellen Loopback, Local LAN, Local WAN, Broadcast, VRRP).

In der Konfiguration hat 0 die Sonderrolle, dass eine Route, die mit dieser administrativen Distanz markiert ist, der Default-Wert für die Routenquelle zugewiesen wird. Dieser ist in `show admin-distance` zu sehen.

Der Wert 255 hat die Sonderfunktion für den Zustand „Route deaktiviert" bzw. „Interface down".

Wenn administrative Distanzen für die Priorisierung von Routen in der Konfiguration verwendet werden sollen, müssen Werte von 1-254 verwendet werden. Die Werte 0 und 255 haben eine Sonderfunktion.

Das Kommando `show ipv4-static-routes` bzw. `show ipv6-static-routes` zeigt alle aktiven und inaktiven statischen Routen an. Die gültigen administrativen Distanzen für die entsprechenden Routen-Quellen sind auf der Konsole über das Kommando `show admin-distance` abrufbar.

Die wichtigsten administrativen Distanzen sind:

Tabelle 24: Administrative Distanzen

Art der Route	Administrative Distanz
Eigene Adressen des Geräts, Automatischer Default	0
Statische Routen	5
VPN	15
eBGP	20
OSPF	110
RIP	120
iBGP	200
LISP	240

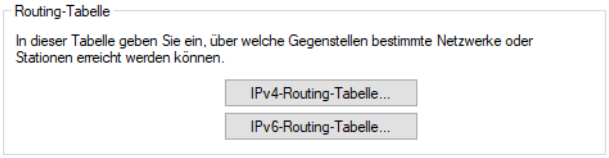
Art der Route	Administrative Distanz
Interface Down	255

Statische Routen sind definiert als Routen, die in der IPv4- bzw. IPv6-Routing-Tabelle vom Benutzer konfiguriert werden.

VPN-Routen sind definiert als Routen, die vom VPN automatische in die Routing-Tabelle eingetragen werden, z. B. durch IKEv2-Routing.

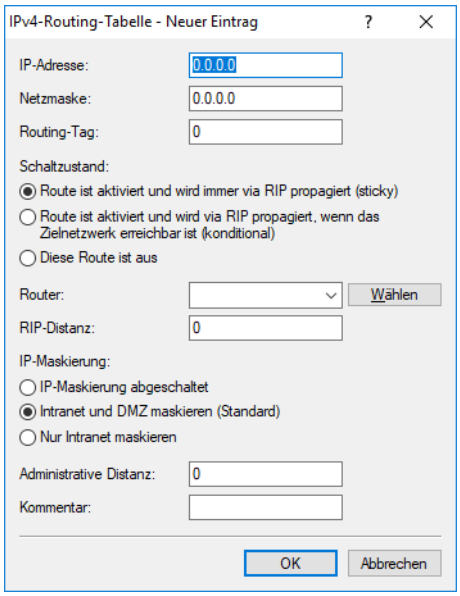
6.2.4.2 Routing-Tabellen für IPv4 / IPv6

Statische Routing-Einträge werden für IPv4 und IPv6 in getrennten Tabellen konfiguriert. Die Tabellen finden Sie in LANconfig unter **IP-Router** > **Routing** > **Routing-Tabelle**.



IPv4

Die Routing-Tabelle für das statische Routing von IPv4-Paketen finden Sie unter **IP-Router** > **Routing** > **Routing-Tabelle** > **IPv4-Routing-Tabelle**.



IP-Adresse / Netzmaske

Das ist die Adresse des Zielnetzes, zu dem Datenpakete geschickt werden können, mit der zugehörigen Netzmaske. Mit der Netzmaske und der Ziel-IP-Adresse aus den ankommenden Datenpaketen prüft der Router, ob das Paket in das Zielnetz gehört.

Die Route mit der IP-Adresse '255.255.255.255' und der Netzmaske '0.0.0.0' ist die Default-Route. Alle Datenpakete, die nicht durch andere Routing-Einträge geroutet werden können, werden über diese Route übertragen.

Routing-Tag

Mit dem Routing-Tag kann die Auswahl der Zielroute genauer gesteuert werden. Die so markierte Route ist nur aktiv für Pakete mit dem gleichen Tag. Dabei wird für die Auswahl der Route nicht nur die Ziel-IP-Adresse,

sondern auch weitere Informationen ausgewertet, die den Datenpaketen über die Firewall zugefügt werden (siehe *Policy-based Routing* auf Seite 385). Detaillierte Informationen zum Routingverhalten in LCOS erhalten Sie im Kapitel *Informationen zum Routingverhalten* auf Seite 369.

Schaltzustand

Bestimmen Sie hier den Schaltzustand. Die Route kann aktiviert werden und entweder immer via RIP propagiert oder nur dann via RIP propagiert werden, wenn das Zielnetzwerk erreichbar ist.

Router

An diese Gegenstelle bzw. IPv4-Adresse überträgt der Router die zur IP-Adresse und Netzmaske passenden Datenpakete.

- Ist die Gegenstelle ein Router in einem anderen Netz oder ein einzelner Arbeitsplatzrechner, dann steht hier der Name der Gegenstelle.
- Kann der eigene Router die Gegenstelle nicht selbst erreichen, steht hier die IP-Adresse eines anderen Routers im LAN, der den Weg ins Zielnetz kennt.
- Falls der Router bzw. Next-Hop in einem anderem Routing-Kontext aufgelöst werden soll, dann kann die Syntax 'IP-Adresse@Tag' verwendet werden.

  Dies ist beispielsweise der Fall, wenn eine statische Route mit einem Tag angelegt wurde, bei welcher dieses Tag nur durch eine Firewallregel zugewiesen werden kann.

  Beispiel: Soll der Router 192.168.1.1 im Routing Kontext 1 aufgelöst werden, so lautet die Eingabe '192.168.1.1@1'.

Routen mit dem Eintrag '0.0.0.0' für Router bezeichnen Ausschluss- bzw. Sperr-Routen. Datenpakete für diese „Null-Routen“ werden verworfen und nicht weitergeleitet. Damit werden z. B. die im Internet verbotenen Routen (private Adressräume nach RFC 1918, z. B. '10.0.0.0/8') von der Übertragung ausgeschlossen.

Wird als Gegenstelle eine IP-Adresse eingetragen, handelt es sich dabei um einen lokal erreichbaren Router, der für die Übertragung der entsprechenden Datenpakete zuständig ist.

RIP-Distanz

Anzahl der zwischen dem eigenen und dem Ziel liegenden Router. Dieser Wert wird bei Weitverkehrsverbindungen oft auch mit den Kosten der Übertragung gleichgesetzt und zur Unterscheidung zwischen preiswerten und teuren Übertragungswegen genutzt. Die eingetragenen Distanzwerte werden wie folgt propagiert:

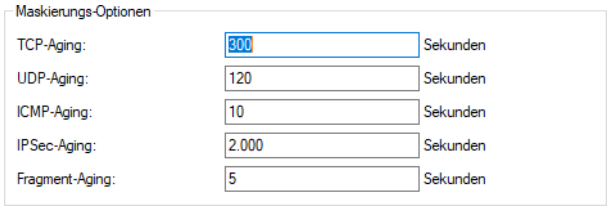
- Während eine Verbindung zu einem Zielnetz existiert, werden alle über diese Verbindung erreichbaren Netze mit einer Distanz von 1 propagiert.
- Alle nicht verbundenen Netze werden mit der Distanz propagiert, die in der Routing-Tabelle eingetragen ist (mindestens jedoch mit einer Distanz von 2), solange noch ein freier Übertragungskanal verfügbar ist.
- Ist kein Kanal mehr frei, so werden die verbleibenden Netze mit einer Distanz von 16 (unreachable) propagiert.
- Eine Ausnahme bilden die Gegenstellen, die über Proxy-ARP angeschlossen sind. Diese „Proxy-Hosts“ werden gar nicht propagiert.

IP-Maskierung

Mit dieser Option in der Routing-Tabelle informieren Sie den Router darüber, welche IP-Adresse er bei der Weitergabe der Pakete verwenden soll.

Weitere Informationen finden Sie im Abschnitt *IP-Masquerading* auf Seite 419.

Die Optionen zum maximalen Alter der verschiedenen Arten von Paketen finden Sie unter **IP-Router** > **Maskierung** > **Maskierungs-Optionen**.



TCP-Aging

Die Connection-List hält offene Sitzungen von TCP-Paketen für jegliche Kommunikation nach, welche über den Router läuft, damit diese während der Kommunikation zugeordnet werden können. Üblicherweise wird eine TCP-Verbindung nach abgeschlossener Kommunikation abgebaut. In einigen Fällen kommt es aber vor, dass TCP-Verbindungen vom Initiator oder Responder nicht wieder abgebaut werden. Damit die Connection-List sich nicht immer weiter füllt und die Performance dadurch sinkt, werden TCP-Verbindungen nach Ablauf dieses Timers automatisch abgebaut.

Geben Sie hier eine Zeit in Sekunden an, nach welcher der zugehörige Eintrag einer TCP-Verbindung bei Inaktivität in der Maskierungs-Tabelle entfernt werden soll.

UDP-Aging

Geben Sie hier an, nach welcher Zeit der Inaktivität einer UDP-Verbindung der entsprechende Eintrag in der Maskierungs-Tabelle entfernt werden soll.

ICMP-Aging

Geben Sie hier an, nach welcher Zeit der Inaktivität einer ICMP-Verbindung der entsprechende Eintrag in der Maskierungs-Tabelle entfernt werden soll.

IPSec-Aging

Geben Sie hier die Default-Lebenszeit für Einträge in der IPSec-Maskierungstabelle in Sekunden an.

Fragment-Aging

Wenn ein IP-Paket nicht vollständig demaskiert werden kann, weil nicht alle Fragmente empfangen wurden, dann werden die unvollständigen Fragmente nach der hier eingestellten Zeit verworfen.

Administrative Distanz

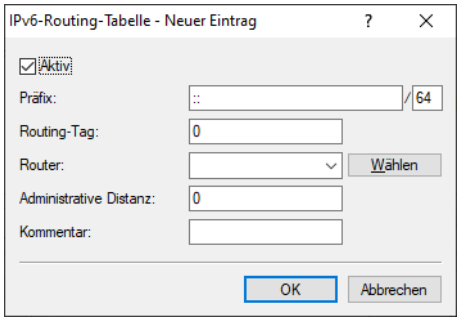
Administrative Distanz für diese Route. Default ist 0 (wird automatisch vom Betriebssystem vergeben). Über den Parameter administrative Distanz ist es möglich mehrere gleiche Routen bzw. Präfixe zu unterschiedlichen Gegenstellen zu konfigurieren. Die Route mit der geringsten administrativen Distanz ist die bevorzugt aktive Route. Siehe *Administrative Distanz* auf Seite 379.

Kommentar

Vergeben Sie optional einen sinnvollen Kommentar als Beschreibung.

IPv6

Die Routing-Tabelle für das statische Routing von IPv6-Paketen finden Sie unter **IP-Router** > **Routing** > **Routing-Tabelle** > **IPv6-Routing-Tabelle**.



Aktiv

Aktiviert bzw. deaktiviert diesen Eintrag in der Routing-Tabelle.

Präfix

Tragen Sie hier als Präfix inkl. Präfixlänge den Netzbereich ein, dessen Daten die aktuelle Gegenstelle erhalten soll, z. B. 2001:db8::/32. Der Wert ::/0 bezeichnet die Default-Route.

Routing-Tag

Mit dem Routing-Tag kann die Auswahl der Zielroute genauer gesteuert werden. Die so markierte Route ist nur aktiv für Pakete mit dem gleichen Tag. Die Datenpakete erhalten das Routing-Tag entweder über die Firewall (siehe *Policy-based Routing* auf Seite 385) oder anhand der verwendeten LAN- oder WAN-Schnittstelle. Detaillierte Informationen zum Routingverhalten in LCOS erhalten Sie im Kapitel *Informationen zum Routingverhalten* auf Seite 369.

Router

Wählen Sie hier das Ziel bzw. die Gegenstelle für diese Route aus. Geben Sie dazu eine der folgenden Optionen an:

- einen Interface-Namen
- eine IPv6-Adresse (z. B. 2001:db8::1)
- einen um eine Link-lokale Adresse erweiterten Interface-Namen (z. B. fe80::1%INTERNET)
- eine IPv6-Adresse mit TAG (z. B. 2001:db8::1@1), falls der Router bzw. Next-Hop in einem anderem Routing-Kontext aufgelöst werden soll.

  Dies ist beispielsweise der Fall, wenn eine statische Route mit einem Tag angelegt wurde, bei welcher dieses Tag nur durch eine Firewallregel zugewiesen werden kann.

  Beispiel: Soll der Router 2001:db8::1 im Routing Kontext 1 aufgelöst werden, so lautet die Eingabe '2001:db8::1@1'

Routen mit dem Eintrag „::“ für Router bezeichnen Ausschluss- bzw. Sperr-Routen. Datenpakete für diese „Null-Routen“ werden verworfen und nicht weitergeleitet. Damit werden z. B. die im Internet verbotenen Routen (private Adressräume, z. B. Unique Local Adressen 'fc00::/7' nach RFC 4193) von der Übertragung ausgeschlossen.

Administrative Distanz

Definieren Sie hier die administrative Distanz dieser Route. Über diesen Parameter ist es möglich mehrere gleiche Routen bzw. Präfixe zu unterschiedlichen Gegenstellen zu konfigurieren. Die Route mit der geringsten administrativen Distanz ist die bevorzugt aktive Route. Der Default ist 0, d. h. der Wert wird automatisch vom Betriebssystem vergeben. Siehe *Administrative Distanz* auf Seite 379.

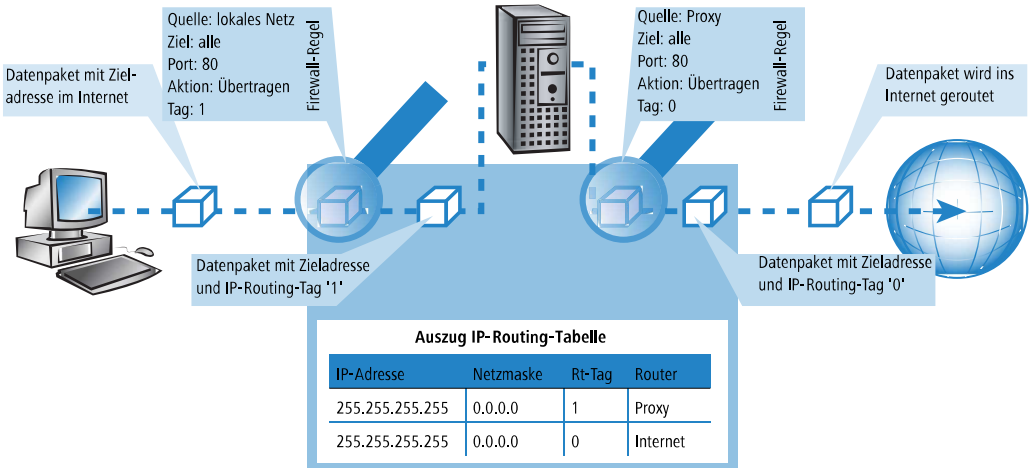
Kommentar

Vergeben Sie optional einen sinnvollen Kommentar als Beschreibung.

6.2.5 Policy-based Routing

Beim Policy-based Routing wird die Zielroute (also die Gegenstelle, über die die Daten übertragen werden), nicht ausschließlich anhand der Ziel-IP-Adressen ausgewählt. Weitere Informationen wie z. B. der verwendete Dienst oder das verwendete Protokoll sowie Adressen von Absender oder Ziel der Datenpakete können für die Auswahl der Zielroute genutzt werden. Mit Hilfe von Policy-based Routing ist eine deutlich feinere Steuerung des Routing-Verhaltens möglich, z. B. in folgenden Anwendungsszenarien:

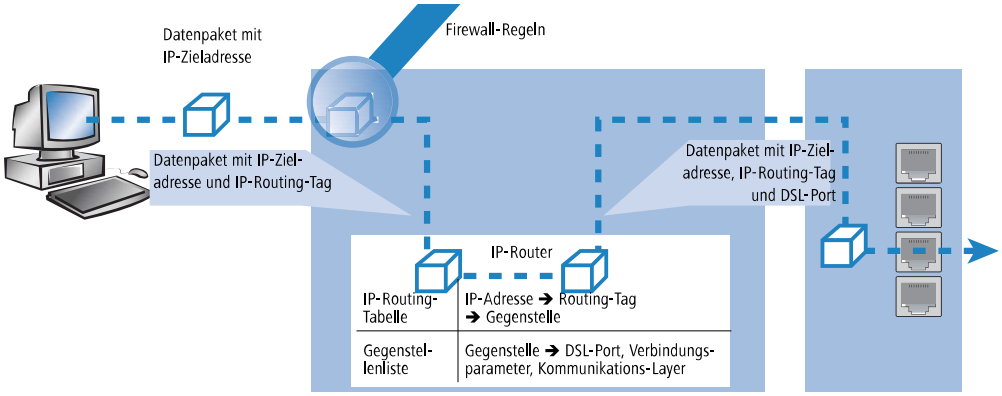
- Der gesamte Internetverkehr eines LANs wird über einen Proxy umgeleitet, ohne das Eintragen der Proxy-Adresse in den Browsern. Das Routing über den Proxy läuft unbemerkt für die Anwender ab, man spricht daher hier auch von einem „transparenten" Proxy.



- Beim Load-Balancing wird der Datenverkehr für bestimmte Protokolle über einen bestimmten DSL-Port mit einem zusätzlichen externen ADSL-Modem geleitet.
- Ein Server im lokalen Netz, der über eine feste IP-Adresse aus dem WAN erreichbar sein sollte, wird über ein bestimmtes WAN-Interface geroutet.
- Der VPN-Verkehr wird mit dem Routing-Tag '0' durch einen VPN-Tunnel mit dynamischen Endpunkten geleitet, der restliche Internetverkehr der Firma wird mit einem entsprechenden Routing-Tag auf eine andere Firewall umgeleitet.

Um die Kanalauswahl aufgrund anderer Informationen als nur der Ziel-IP-Adresse zu entscheiden, werden geeignete Einträge in der Firewall angelegt. Den Firewall-Einträgen wird dabei ein spezielles „Routing-Tag" zugefügt, mit dem über die Routing-Tabelle die gewünschte Kanalauswahl gesteuert werden kann. So wird z. B. über eine Regel dem gesamten Datenverkehr einer lokalen Rechnergruppe (entsprechend dem IP-Adress-Bereich) das Routing-Tag '2' angehängt. Alternativ definieren gezielt einige Protokolle ein anderes Routing-Tag.

Die Zeichnung zeigt die Anwendung des Policy-based Routing beim Load-Balancing:



- Beim Aufbau der Verbindungen prüft zunächst die Firewall, ob die anstehenden Pakete zu einer Regel passen, in der ein Routing-Tag enthalten ist. Das Routing-Tag wird in das Datenpaket eingetragen.
- Mit dem gefundenen Routing-Tag und der Ziel-IP-Adresse kann in der IP-Routing-Tabelle die passende Gegenstelle gefunden werden. Dazu wird die IP-Routing-Tabelle wie üblich von oben nach unten durchgearbeitet.
- Wird ein übereinstimmender Eintrag für das Netzwerk gefunden, wird im zweiten Schritt das Routing-Tag geprüft. Mit dem passenden Routing-Tag kann so die gewünschte Gegenstelle gefunden werden. Über die Gegenstelle kann das Gerät beim Load-Balancing aus der Gegenstellenliste den richtigen DSL-Port ermitteln.

  Wenn das Routing-Tag den Wert „0“ hat (Default), dann gilt der Routing-Eintrag für alle Pakete.

- Interne Dienste verwenden implizit immer das Default-Tag. Wenn der Anwender z. B. die Default-Route durch einen VPN-Tunnel leiten will, der einen dynamischen Tunnelendpunkt hat, so nutzt das VPN-Modul standardmäßig die Default-Route mit dem Routing-Tag „0“.

  Um die Default-Route dennoch durch den VPN-Tunnel zu führen, legen Sie eine zweite Default-Route mit dem Routing-Tag „1“ und der VPN-Gegenstelle als Router-Namen an. Mit einer passenden Firewall-Regel übertragen Sie alle Dienste von allen Quell-Stationen zu allen Ziel-Stationen mit dem Routing-Tag „1“.

- Routing-Tags und RIP: Das Routing-Tag wird auch in RIP-Paketen versendet und beim Empfang ausgewertet, damit z. B. die geänderten Distanzen in den richtigen Routen geändert werden können.

6.2.5.1 Routing-Tags für VPN- und PPTP-Verbindungen

Routing-Tags werden im Gerät genutzt, um neben der IP-Adresse weitere Kriterien zur Auswahl der Zielroute auswerten zu können. Normalerweise werden die Routing-Tags den Datenpaketen über spezielle Regeln der Firewall hinzugefügt. In manchen Fällen ist es aber erwünscht, die Routing-Tags auf direkterem Wege zuzuweisen.

- Routing-Tags bei VPN-Verbindungen

In der VPN-Namenliste kann für jede VPN-Verbindung das Routing-Tag angegeben werden, das verwendet werden soll, um die Route zum Remote Gateway zu ermitteln (Default '0').

Zusätzlich kann in der Gateway-Tabelle jedem Gateway ein spezifisches Routing-Tag zugeordnet werden. Das Tag 0 hat in dieser Tabelle eine Sonderfunktion: Wenn bei einem Gateway das Tag 0 gesetzt ist, dann wird das Tag aus der VPN-Namenliste-Tabelle verwendet.

Die Einstellungen für die VPN-Routing-Tags finden Sie unter Setup/VPN/VPN-Peers bzw. Setup/VPN/Additional-Gateways sowie unter LANconfig im Konfigurationsbereich 'VPN' auf der Registerkarte 'Allgemein' in der 'Verbindungsliste' und in der Liste 'Weitere entfernte Gateways'.

- Routing-Tags bei PPTP-Verbindungen

In der PPTP-Tabelle kann zusätzlich zur IP-Adresse des PPTP-Servers ein Routing-Tag angegeben werden. Mit Hilfe dieses Routing-Tags können z. B. mehrere DSL-Modems, die eine einheitliche IP-Adresse verwenden, an verschiedenen DSL-Ports betrieben werden.

Peer	IP-Address	Rtg-tag	Port	SH-Time
PEER01	10.0.0.138	1	1723	9999
PEER02	10.0.0.138	2	1723	9999

In der IP-Routing-Tabelle sind dazu zwei passend getaggte Routen nötig:

IP-Adresse	IP-Netzmaske	Rtg-tag	Peer-oder-IP	Distanz	Maskierung
10.0.0.138	255.255.255.255	2	PEER02-PPTP	0	Nein
10.0.0.138	255.255.255.255	1	PEER01-PPTP	0	Nein
192.168.0.0	255.255.0.0	0	0.0.0.0	0	Nein
172.16.0.0	255.240.0.0	0	0.0.0.0	0	Nein
10.0.0.0	255.0.0.0	0	0.0.0.0	0	Nein
224.0.0.0	224.0.0.0	0	0.0.0.0	0	Nein
255.255.255.255	0.0.0.0	0	PEER-LB	0	Ja

Mit diesen Einstellungen und dem entsprechenden Eintrag in der Load-Balancing-Tabelle kann z. B. ein Load-Balancing realisiert werden, dass auch in Österreich verwendet werden kann.

Peer	Bundle-Peer-1	Bundle-Peer-2	Bundle-Peer-3
PEER-LB	PEER01	PEER02	

6.2.6 Dynamisches Routing mit IP-RIP

Neben der statischen Routing-Tabelle verfügen Router von LANCOM auch über eine dynamische Routing-Tabelle. Diese Tabelle füllt der Anwender im Gegensatz zu der statischen nicht aus, das erledigt der Router selbst. Dazu nutzt er das Routing Information Protocol (RIP). Über dieses Protokoll tauschen alle Geräte, die RIP beherrschen, Informationen über die erreichbaren Routen aus.

6.2.6.1 Welche Informationen werden über IP-RIP propagiert?

Ein Router teilt in den IP-RIP-Informationen den anderen Routern im Netz die Routen mit, die er in seiner eigenen Tabelle findet. Nicht berücksichtigt werden dabei die folgenden Einträge:

- Routen, die mit der Router-Einstellung '0.0.0.0' verworfen werden.
- Routen, die auf andere Router im lokalen Netz lauten.
- Routen, die einzelne Rechner über Proxy-ARP an das LAN anbinden.

Die Einträge in der statischen Routing-Tabelle werden zwar von Hand gesetzt, trotzdem ändern sich diese Informationen je nach Verbindungssituation der Router und damit auch die versendeten RIP-Pakete.

- Solange der Router eine Verbindung zu einer Gegenstelle aufgebaut hat, gibt er alle über diese Route erreichbaren Netze in den RIPs mit der Distanz '1' weiter. Damit werden andere Router im LAN darüber informiert, dass hier bei diesem Router eine bestehende Verbindung zu dieser Gegenstelle genutzt werden kann. So kann zusätzlicher Verbindungsaufbau von Routern mit Wählverbindungen verhindert und ggf. Verbindungskosten reduziert werden.
- Wenn darüber hinaus in diesem Router keine weitere Verbindung zu einer anderen Gegenstelle aufgebaut werden kann, werden alle anderen Routen mit der Distanz '16' im RIP weitergemeldet. Die '16' steht dabei für „Im Moment ist diese Route nicht erreichbar“.

6.2.6.2 Welche Informationen entnimmt der Router aus empfangenen IP-RIP-Paketen?

Wenn der Router IP-RIP-Pakete empfängt, baut er sie in seine dynamische IP-Routing-Tabelle ein, und die sieht etwa so aus:

IP-Adresse	IP-Netzmaske	Zeit	Distanz	Router
192.168.120.0	255.255.255.0	1	2	192.168.110.1
192.168.130.0	255.255.255.0	5	3	192.168.110.2
192.168.140.0	255.255.255.0	1	5	192.168.110.3

6.2.6.3 Was bedeuten die Einträge?

IP-Adresse und Netzmaske bezeichnen das Ziel-Netz, die Distanz gibt die Anzahl der zwischen Sender und Empfänger liegenden Router an, die letzte Spalte zeigt an, welcher Router diese Route bekannt gemacht hat. Mit der 'Zeit' zeigt die dynamische Tabelle an, wie alt die entsprechende Route ist. Der Wert in dieser Spalte gilt als Multiplikator für das Intervall, in dem die RIP-Pakete eintreffen, eine '1' steht also für etwa 30 Sekunden, eine '5' für etwa 2,5 Minuten usw. Wenn eine Information über eine Route neu eintrifft, gilt diese Route natürlich als direkt erreichbar und erhält die Zeit '1'. Nach Ablauf der entsprechenden Zeit wird der Wert in dieser Spalte automatisch erhöht. Nach 3,5 Minuten wird die Distanz auf '16' gesetzt (Route nicht erreichbar), nach 5,5 Minuten wird die Route gelöscht.

Wenn der Router nun ein IP-RIP-Paket empfängt, muss er entscheiden, ob er die darin enthaltenen Routen in seine dynamische Tabelle aufnehmen soll oder nicht. Dazu geht er wie folgt vor:

- Die Route ist in der Tabelle noch gar nicht vorhanden, dann wird sie aufgenommen (sofern Platz in der Tabelle ist).
- Die Route ist in der Tabelle vorhanden mit der Zeit von '5' oder '6'. Die neue Route wird dann verwendet, wenn sie die gleiche oder eine bessere Distanz aufweist.
- Die Route ist in der Tabelle vorhanden mit der Zeit von '7' bis '10', hat also die Distanz '16'. Die neue Route wird auf jeden Fall verwendet.
- Die Route ist in der Tabelle vorhanden. Die neue Route kommt von dem gleichen Router, der auch diese Route bekannt gegeben hat, hat aber eine schlechtere Distanz als der bisherige Eintrag. Wenn ein Gerät so die Verschlechterung seiner eigenen statischen Routing-Tabelle bekannt macht (z. B. durch den Abbau einer Verbindung steigt die Distanz von '1' auf '2', siehe unten), dann glaubt der Router ihm das und nimmt den schlechteren Eintrag in seine dynamische Tabelle auf.

RIP-Pakete aus dem WAN werden nicht beachtet und sofort verworfen! RIP-Pakete aus dem LAN werden ausgewertet und nicht im LAN weitergeleitet!

6.2.6.4 Zusammenspiel: statische und dynamische Tabelle

Aus der statischen und der dynamischen Tabelle stellt der Router die eigentliche IP-Routing-Tabelle zusammen, mit der er den Weg für die Datenpakete bestimmt. Dabei nimmt er zu den Routen aus der eigenen statischen Tabelle die Routen aus der dynamischen Tabelle auf, die er selber nicht kennt oder die eine kürzere Distanz aufweisen als die eigene (statische) Route.

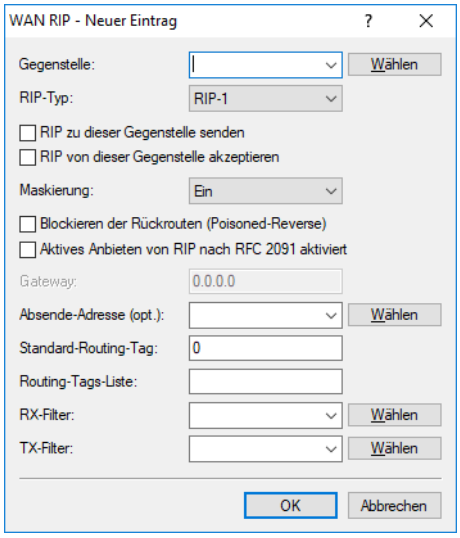
6.2.6.5 Skalierung durch IP-RIP

Verwenden Sie mehrere Router in einem lokalen Netz mit IP-RIP, können Sie die Router im lokalen Netz nach außen hin als einen einzigen großen Router darstellen. Dieses Vorgehen nennt man auch „Skalierung“. Durch den regen Informationsaustausch der Router untereinander steht so ein Router mit prinzipiell beliebig vielen Übertragungswegen zur Verfügung.

6.2.6.6 Konfiguration der IP-RIP-Funktion

Um die über RIP gelernten und statisch definierten Routen auch über das WAN bekannt zu machen oder Routen aus dem WAN zu lernen, können die entsprechenden Gegenstellen in der WAN-RIP-Tabelle eingetragen werden.

LANconfig: **Routing Protokolle** > **RIP** > **RIP-Optionen** > **WAN RIP**



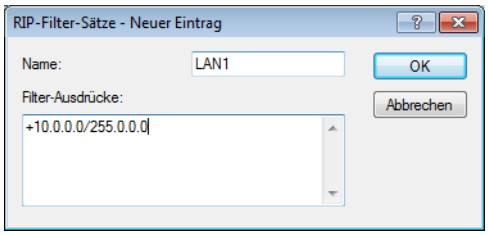
Konsole: **Setup** > **IP-Router** > **RIP** > **WAN-Tabelle**

RIP-fähige Router versenden die RIP-Pakete ungefähr alle 30 Sekunden. Der Router ist nur dann auf das Versenden und Empfangen von RIPs eingestellt, wenn er eine eindeutige IP-Adresse hat. In der Grundeinstellung mit der IP-Adresse xxx.xxx.xxx.254 ist das IP-RIP-Modul ausgeschaltet.

6.2.6.7 RIP-Filter

Über RIP gelernte Routen können durch die Einstellungen bei LAN- und WAN-RIP nach dem Routing-Tag gefiltert werden. Um die Routen zusätzlich über die Angabe von Netzadressen zu filtern (z. B. „Lerne nur Routen, die im Netz 192.168.0.0/255.255.0.0 liegen“), werden in einer zentralen Tabelle zunächst die Filter definiert, die dann von Einträgen in der LAN- und WAN-RIP-Tabelle genutzt werden können.

LANconfig: **Routing-Protokolle** > **RIP** > **RIP-Filter-Sätze**

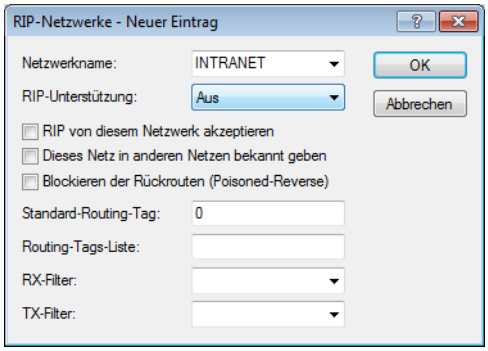


Konsole: **Setup** > **IP-Router** > **RIP** > **Filter**

6.2.6.8 RIP für Netzwerke getrennt einstellen

Meistens ist es nicht erwünscht, dass die lokale Netzstruktur über RIP in die DMZ propagiert wird. Außerdem ist es zwar manchmal erwünscht, in ein Netzwerk die bekannten Routen zwar zu propagieren, von dort aber keine Routen zu lernen (wie z. B. auch im WAN). Der RIP-Funktionalität kann daher für jedes Netzwerk getrennt eingestellt werden

LANconfig: **Routing-Protokolle** > **RIP** > **RIP-Netzwerke**



Konsole: **Setup** > **IP-Router** > **RIP** > **LAN-Tabelle**

6.2.6.9 Timereinstellungen

Das Routing Information Protocol (RIP) versendet regelmäßige Update-Nachrichten an die benachbarten Router mit Informationen über die erreichbaren Netzwerke und die zugehörigen Metriken (Hops). RIP verwendet verschiedene Timer, um den Austausch der Routing-Informationen zeitlich zu steuern.

Konsole: **Setup** > **IP-Router** > **RIP** > **Parameter**

6.2.6.10 Triggered Update im LAN

Bei einem Triggered Update werden Änderungen in den Metriken sofort an die benachbarten Router gemeldet, nicht erst beim nächsten regelmäßigen Update. Damit es bei Fehlkonfigurationen im Netzwerk nicht zu massenhaften Update-Nachrichten kommt, wird eine so genannte Update-Verzögerung (Update-Delay) definiert.

› Update-Delay

Die Update-Verzögerung startet, sobald die Routing-Tabelle bzw. Teile davon propagiert wurden. Solange dieses Verzögerung läuft, werden neue Routing-Informationen zwar angenommen und in die Tabelle eingetragen, aber nicht sofort weitergeleitet. Der Router meldet die aktuellen Einträge erst nach Ablauf der Verzögerung aktiv weiter.

Der hier konfigurierte Wert gibt die Obergrenze der Verzögerung an – die tatsächliche Verzögerung wird immer zufällig ermittelt und liegt zwischen einer Sekunde und dem hier angegebenen Wert.

6.2.6.11 Triggered Update im WAN

Anders als im LAN sind auf WAN-Strecken regelmäßige Updates alle 30 Sekunden ggf. unerwünscht, weil die Bandbreite beschränkt ist. Daher können nach RFC 2091 alle Routen im WAN nur noch einmal beim Verbindungsaufbau übertragen werden, danach nur noch Updates.

Da in diesem Fall die Updates explizit angefragt werden, können keine Broadcasts oder Multicasts für die Zustellung der RIP-Nachrichten verwendet werden. Stattdessen muss im Filialgerät die IP-Adresse des nächsten erreichbaren Routers in der Zentrale statisch konfiguriert werden. Der Zentralrouter kann sich aufgrund der Anfragen merken, von welchen Filialroutern er Update-Requests empfangen hat, um etwaige Routenänderungen über passende Messages direkt an das Filialgerät zu senden.

Zur Konfiguration des triggered Update im WAN wird die WAN-RIP-Tabelle erweitert.

6.2.6.12 Poisoned Reverse

Poisoned Reverse dient dazu, Routing-Schleifen zu verhindern. Dazu wird an den Router, der die beste Route zu einem Netz propagiert hat, dieses Netz auf dem zugehörigen Interface als unerreichbar zurückpropagiert.

Gerade auf WAN-Strecken hat dies aber einen entscheidenden Nachteil: Hier werden von der Zentrale sehr viele Routen gesendet, die dann als nicht erreichbar zurückpropagiert werden und so gegebenenfalls die verfügbare Bandbreite belasten. Daher kann die Verwendung von Poisoned Reverse auf jedem Interface (LAN/WAN) manuell aktiviert werden.

Zur Konfiguration der Poisoned Reverse werden LAN- und WAN-RIP-Tabelle erweitert.

6.2.6.13 Statische Routen, die immer propagiert werden

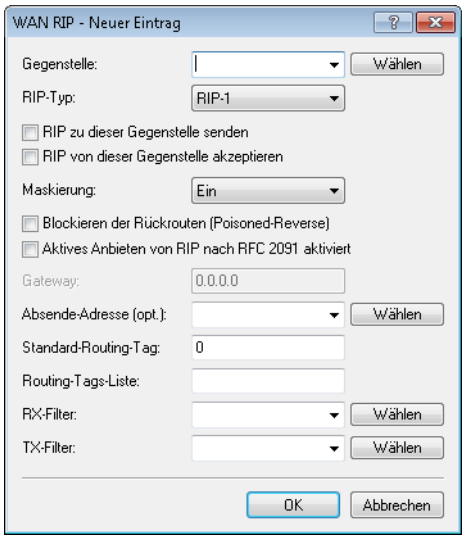
Neben den dynamischen Routen propagiert ein Router über RIP auch die statisch konfigurierten Routen. Dabei sind manche der statischen Routen nicht immer erreichbar, z. B. weil eine notwendige Internetverbindung oder ein Wählzugang temporär nicht verfügbar sind.

Mit der Angabe der „Aktivität" in der Routingtabelle kann für eine statische Route definiert werden, ob sie immer propagiert werden soll oder nur dann, wenn die Route auch tatsächlich erreichbar ist.

Konsole: **Setup** > **IP-Router** > **IP-Routing-Tabelle**

6.2.7 WAN-RIP

Um die über RIP gelernten Routen auch über das WAN bekannt zu machen, können die entsprechenden Gegenstellen unter **IP-Router** > **Allgemein** > **WAN-RIP** in der WAN-RIP-Tabelle eingetragen werden.



Die WAN-RIP-Tabelle enthält folgende Werte:

Peer

Enthält den Namen der Gegenstelle.

RIP-Typ

Gibt an, mit welcher RIP-Version die lokalen Routen propagiert werden.

RIP zu dieser Gegenstelle senden

Stellen Sie ein, ob RIP auf dem WAN Routen propagiert. Dazu muss gleichzeitig der RIP-Typ gesetzt sein.

RIP von dieser Gegenstelle akzeptieren

Stellen Sie ein, ob RIP aus dem WAN akzeptiert wird. Dazu muss gleichzeitig der RIP-Typ gesetzt sein.

Bitte beachten Sie, dass WAN-seitiges RIP ein potenzielles Sicherheits-Risiko darstellt.

Maskierung

Geben Sie an, ob und wie das Gerät auf der Strecke maskiert. Durch diesen Eintrag ist es möglich, das WAN-RIP auch mit einer leeren Routing-Tabelle zu starten. Es sind folgende Werte möglich:

- **Auto**: Der Maskierungstyp wird aus der Routing-Tabelle entnommen (Wert: 0). Existiert für die Gegenstelle kein Routing-Eintrag, so wird nicht maskiert.
- **An**: Alle Verbindungen werden maskiert (Wert: 1).
- **Intranet**: Verbindungen aus dem Intranet werden maskiert, Verbindungen aus der DMZ gehen transparent hindurch (Wert: 2).

Blockieren der Rückrufrouten (Poisoned-Reverse)

Beim Blockieren der Rückrouten (Poisoned-Reverse) werden alle über diese Schnittstelle gelernten/empfangenen Routen als „nicht erreichbar" gekennzeichnet und zurückgesendet, indem die Anzahl der Hops direkt auf 16 (bzw. die maximale Anzahl) gesetzt wird.

Aktives Anbieten von RIP nach RFC 2091 aktiviert

Das Gerät unterstützt grundsätzlich RIP nach RFC 2091.

Die Einstellung „RFC 2091 anbieten" ist nur für den aktiven Verbindungsaufbau relevant. Bei passiven Verbindungen wird für jede Gegenstelle die RIP-Version genommen, die die Gegenstelle anbietet – unabhängig von der Stellung dieses Schalters.

Bei aktiven Verbindungsaufbauten gibt es zudem bei aktiviertem Anbieten von RIP nach RFC-2091 einen Rückfall auf „normales" RIP nach RFC 2453: Wenn die Gegenstelle nach 10 Wiederholungen des ersten Pakets nicht geantwortet hat, wird zurückgeschaltet (10 Wiederholungen dauern ca. 30 Sekunden).

Als Gateway wird die IP-Adresse des RIP-Partners auf der anderen Seite der WAN-Strecke eingetragen. Hier kann 0.0.0.0 eingetragen werden, wenn auf der WAN-Strecke eine PPP-Verhandlung läuft und dabei die IP-Adresse der Gegenseite übermittelt wird.

In einem Zentral-Gateway kann die Einstellung „RFC 2091" immer aus und der Eintrag "Gateway" immer auf 0.0.0.0 stehen, da das Zentral-Gateway immer die Vorgabe des Filial-Gateway berücksichtigt.

Gateway

Tragen Sie die IP-Adresse des RIP-Partners ein.

Absende-Adresse (opt.)

Hier können Sie optional eine Absendeadresse konfigurieren, die statt der ansonsten automatisch für die Zieladresse gewählten Absendeadresse verwendet wird.

Falls Sie z. B. Loopback-Adressen konfiguriert haben, können Sie diese hier als Absendeadresse angeben. Als Adresse werden verschiedene Eingabeformen akzeptiert:

- Name des IP-Netzwerks (ARF-Netz), dessen Adresse eingesetzt werden soll.
- „INT" für die Adresse des ersten Intranets.
- „DMZ" für die Adresse der ersten DMZ (Achtung: wenn es eine Schnittstelle Namens „DMZ" gibt, dann wird deren Adresse genommen).
- LB0…LBF für eine der 16 Loopback-Adressen oder deren Name.
- Desweiteren kann eine beliebige IP-Adresse in der Form x.x.x.x angegeben werden.

Sofern die hier eingestellte Absendeadresse eine Loopback-Adresse ist, wird diese auch auf maskiert arbeitenden Gegenstellen unmaskiert verwendet.

Standard-Routing-Tag

Gibt das für die WAN-Verbindung geltende „Standard-Routing-Tag". Alle ungetaggten Routen taggt das Gerät beim Versenden im WAN mit diesem Tag.

Routing-Tags-Liste

In dieser Liste steht eine kommaseparierte Liste der Tags, die das Gerät auf dem Interface akzeptiert. Wenn diese Liste leer ist, akzeptiert das Gerät alle Tags. Steht mindestens ein Tag in der Liste, dann akzeptiert das

Gerät nur die Tags in dieser Liste. Ebenso propagiert das Gerät beim Senden von getaggten Routen auf das WAN nur Routen mit erlaubten Tags.

Alle vom WAN gelernten Routen behandelt das Gerät intern als ungetaggte Routen und propagiert diese über das LAN mit dem Default-Tag (0). Über das WAN hingegen propagiert es die Routen mit dem Tag, mit dem es sie auch gelernt hat.

RX-Filter

Geben Sie hier beim Empfang (RX) von RIP-Paketen die anzuwendenden Filter an.

Definieren Sie die Filter zuerst in der RIP-Filterliste, um sie hier verwenden zu können.

TX-Filter

Geben Sie hier beim Senden (TX) von RIP-Paketen die anzuwendenden Filter an.

Definieren Sie die Filter zuerst in der RIP-Filterliste, um sie hier verwenden zu können.

6.2.8 SYN/ACK-Speedup

Das SYN/ACK-Speedup-Verfahren dient der Beschleunigung des IP-Datenverkehrs. Beim SYN/ACK-Speedup werden IP-Kontrollzeichen (SYN für Synchronisation und ACK für Acknowledge) innerhalb des Sendebuffers gegenüber einfachen Datenpaketen bevorzugt behandelt. Dadurch wird die Situation vermieden, dass Kontrollzeichen länger in der Sendeschlange hängen bleiben und die Gegenstelle deshalb aufhört, Daten zu senden.

Der größte Effekt tritt beim SYN/ACK-Speedup bei schnellen Anschlüssen (z. B. ADSL) ein, wenn gleichzeitig in beiden Richtungen mit hoher Geschwindigkeit Datenmengen übertragen werden.

Werkseitig ist der SYN/ACK-Speedup eingeschaltet.

6.2.8.1 Ausschalten in Problemfällen

Durch die bevorzugte Behandlung einzelner Pakete wird die ursprüngliche Paketreihenfolge geändert. Obwohl TCP/IP keine bestimmte Paketreihenfolge gewährleistet, kann es in einzelnen Anwendungen zu Problemen kommen. Das betrifft nur Anwendungen, die abweichend vom Protokollstandard eine bestimmte Paketreihenfolge voraussetzen. Für diesen Fall kann der SYN/ACK-Speedup ausgeschaltet werden:

LANconfig: **IP-Router** > **Allgemein** > **TCP SYN- und ACK-Pakete bevorzugt weiterleiten**

6.3 Advanced Routing and Forwarding (ARF)

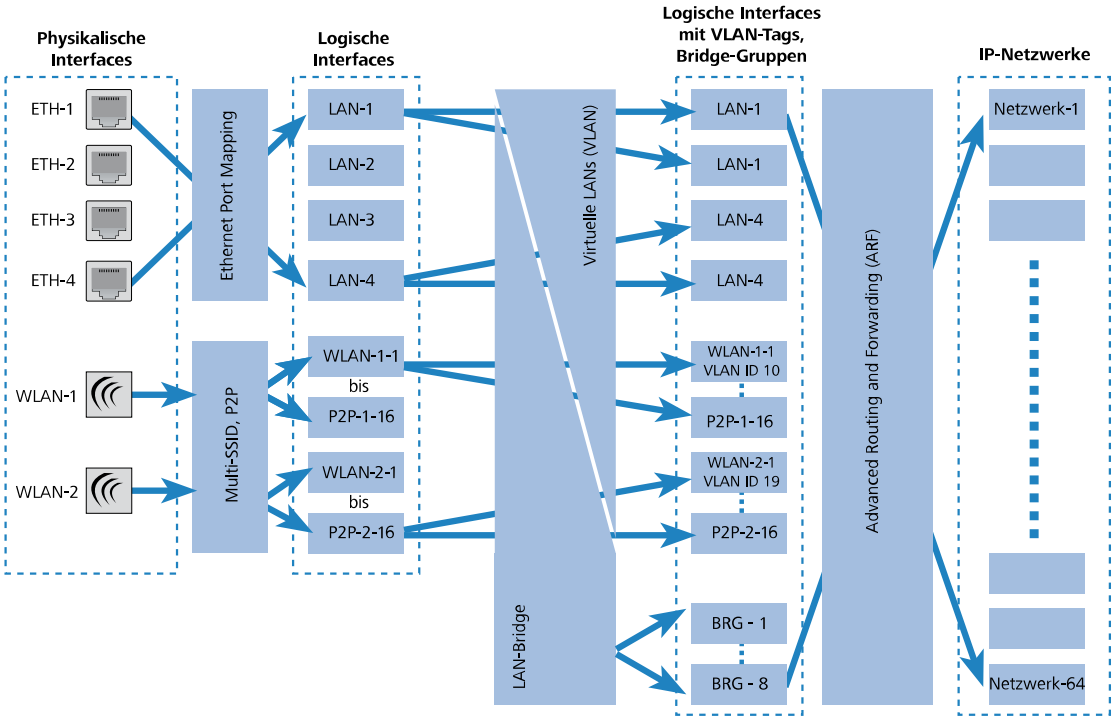
6.3.1 Einleitung

In einfachen Anwendungsfällen verwaltet ein Gerät lediglich zwei lokale Netzwerke: das Intranet und die DMZ. In einer komplexeren Umgebung ist es jedoch oft wünschenwert, mehr als ein Intranet und eine DMZ mit einem Gerät zu realisieren, um auf diese Weise z. B. mehreren IP-Netzen über ein zentrales Gerät den Zugang zum Internet zu ermöglichen. Aktuelle Geräte unterstützen je nach Modell bis zu 64 verschiedene IP-Netzwerke.

Bei der Realisierung von mehreren IP-Netzwerken sind mehrere Szenarien möglich:

- Ein Netzwerk je Interface.
- Mehrere Netzwerke je Interface.
- Mehrere VLANs je Interface, auf jedem VLAN ein oder mehrere Netzwerke (das entspricht einer Kombination aus den ersten beiden Szenarien).

Um diese Szenarien zu ermöglichen, stehen mit den Funktionen des Advanced Routing and Forwarding (ARF) sehr flexible Möglichkeiten zur Definition von IP-Netzwerken und der Zuordnung dieser Netzwerke zu den Interfaces bereit. Das untenstehende Diagramm verdeutlicht die Zuordnung von Netzwerken zu Interfaces auf verschiedenen Ebenen. Die dabei verwendeten Konfigurationsmöglichkeiten werden in den folgenden Kapiteln vorgestellt.



So verläuft die Zuordnung von IP-Netzwerken zu Interfaces:

- Je nach Modell haben die Geräte eine unterschiedliche Anzahl von physikalischen Interfaces, also Ethernet-Ports oder WLAN-Module. Diesen zugeordnet sind die logischen Interfaces:
  - Für die Ethernet-Ports geschieht die Zuordnung durch das Ethernet Port Mapping.

    Die Anzahl der logischen LAN-Interfaces entspricht nicht bei allen Modellen der Anzahl der verfügbaren physikalischen Ethernet-Ports.
  - Für die WLAN-Module entstehen durch den Aufbau von Point-to-Point-Strecken (P2P) bzw. durch die Verwendung von Multi-SSID auf jedem physikalischen WLAN-Modul mehrere WLAN-Interfaces: bis zu 16 WLAN-Netze und bis zu 16 P2P-Strecken pro Modul.
- Diese logischen Interfaces werden im nächsten Schritt weiter spezifiziert bzw. gruppiert:
  - Bei Geräten mit VLAN-Unterstützung können für jedes logische Interface durch die Verwendung von VLAN-IDs mehrere VLANs definiert werden. Der Datenverkehr der verschiedenen VLANs läuft dann zwar ggf. über ein gemeinsames logisches Interface ab, wird aber durch die VLAN-ID streng von den anderen VLANs getrennt. Aus Sicht der Geräte stellen sich die VLANs also als separate Interfaces dar, aus einem einzelnen logischen Interface werden also für das Gerät mehrere logische Interfaces, die einzeln angesprochen werden können.
  - Bei Geräten mit WLAN-Modulen können die einzelnen logischen Interfaces zu Gruppen zusammengefasst werden. Dazu wird die LAN-Bridge verwendet, welche die Datenübertragung zwischen den LAN- und WLAN-Interfaces regelt. Durch die Zusammenfassung zu Bridge-Gruppen (BRG) können mehrere logische Interfaces gemeinsam angesprochen werden und wirken so für das Gerät wie ein einzelnes Interface – damit wird also das Gegenteil des VLAN-Verfahrens erreicht.
- Im letzten Schritt wird durch die Möglichkeiten des ARF eine Verbindung zwischen den logischen Interfaces mit VLAN-Tags und den Bridge-Gruppen einerseits sowie den IP-Netzwerken andererseits hergestellt. Ein IP-Netzwerk enthält daher in der Konfiguration den Verweis auf ein logisches Interface (ggf. mit VLAN-ID) oder eine Bridge-Gruppe.

Darüber hinaus kann für jedes IP-Netzwerk ein Schnittstellen-Tag festgelegt werden, mit dem ein IP-Netz auch ohne Firewall-Regel von anderen Netzen getrennt werden kann.

Gerade die zuletzt dargestellte Definition von Schnittstellen-Tags für IP-Netze stellt einen der bedeutenden Vorteile des Advanced Routing and Forwarding dar – mit Hilfe dieser Option werden „virtuelle Router" realisiert. Ein virtueller Router nutzt anhand des Schnittstellen-Tags für ein IP-Netz nur einen Teil der Routing-Tabelle und steuert so das Routing ganz speziell für dieses eine IP-Netzwerk. Auf diese Weise können in der Routing-Tabelle z. B. mehrere Default-Routen definiert werden, jeweils mit Routing-Tags versehen. Die virtuellen Router für die IP-Netze wählen anhand dieser Tags diejenige Default-Route aus, die für das jeweilige IP-Netz mit dem passenden Schnittstellen-Tag gilt. Die Separation der IP-Netzwerke über die virtuellen Router geht so weit, dass sogar mehrere IP-Netzwerke mit identischem Adresskreis problemlos parallel in einem Gerät betrieben werden können.

Ein Beispiel: In einem Bürogebäude sollen mehrere Firmen über ein zentrales Gerät an das Internet angebunden werden, dabei hat jede Firma einen eigenen Internetprovider. Alle Firmen wollen das oft verwendete IP-Netzwerk '10.0.0.0' mit Netzmaske '255.255.255.0' nutzen. Um diese Aufgabe zu realisieren, wird für jede Firma ein IP-Netz '10.0.0.0/255.255.255.0' mit einem eindeutigen Namen und einem eindeutigen Schnittstellen-Tag angelegt. In der Routing-Tabelle wird für jeden Internetprovider eine entsprechende Default-Route mit dem passenden Routing-Tag angelegt. Auf diese Weise können die Clients in den verschiedenen Firmennetzen mit den gleichen IP-Adressen über ihren jeweiligen Provider das Internet nutzen. Mit dem Einsatz von VLANs können die logischen Netzwerke auch auf demselben physikalischen Medium (Ethernet) voneinander getrennt werden.

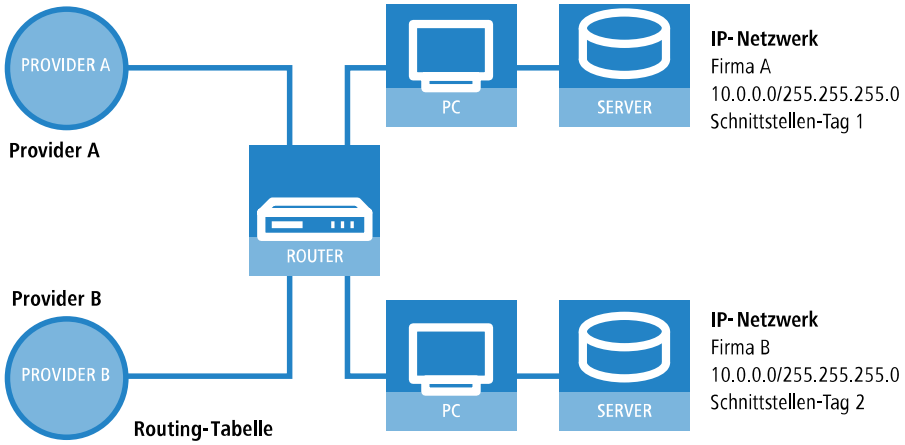
Unterschiede zwischen Routing-Tags und Schnittstellen-Tags

Routing-Tags, die über die Firewall zugewiesen werden, und die über IP-Netzwerke definierten Schnittstellen-Tags haben einiges gemeinsam, es gibt aber auch wichtige Unterschiede:

- Der Router wertet beide Tags gleich aus. Für die Pakete mit dem Schnittstellen-Tag '2' gelten also alle Routen mit Routing-Tag '2' in der Routing-Tabelle (und alle Routen mit Default-Routing-Tag '0'). Die gleichen Routen gelten auch für Pakete, denen die Firewall das Routing-Tag '2' zugewiesen hat.

  Das heißt, beim Routing wird das Schnittstellen-Tag wie ein Routing-Tag verwendet!

- Schnittstellen-Tags schränken aber darüber hinaus noch die Sichtbarkeit (oder Erreichbarkeit) der Netzwerke untereinander ein:
  - Grundsätzlich können sich nur Netzwerke mit gleichem Schnittstellen-Tag untereinander „sehen", also Verbindungen in das jeweils andere Netz aufbauen.
  - Netzwerke mit dem Schnittstellen-Tag '0' haben eine besondere Bedeutung – sie sind quasi Supervisor-Netze. Diese Netze können alle anderen Netze sehen, also Verbindungen in andere Netze aufbauen. Netze mit Schnittstellen-Tag ungleich '0' können hingegen keine Verbindungen in die Supervisor-Netze aufbauen.
  - Netzwerke vom Typ 'DMZ' sind unabhängig vom Schnittstellen-Tag für alle anderen Netzwerke sichtbar – das ist auch sinnvoll, da in der DMZ oft öffentlich zugängliche Server wie Webserver etc. stehen. Die DMZ-Netze selbst sehen aber nur die Netze mit gleichem Schnittstellen-Tag (und natürlich alle anderen DMZ-Netze).
  - Einen Sonderfall stellen Netze vom Typ 'DMZ' mit dem Schnittstellen-Tag '0' dar: diese Netze können als „Supervisor-Netz" selbst alle anderen Netze sehen, werden aber auch gleichzeitig von allen anderen Netze gesehen.



Routing-Tabelle

IP-Adresse	Netzmaske	Schnittstellen-Tag	Router
255.255.255.255	0.0.0.0	1	Provider A
255.255.255.255	0.0.0.0	2	Provider B

In Fällen, die keine eindeutige Zuordnung der IP-Adressen über die Schnittstellen-Tags erlauben, wird das Advanced Routing and Forwarding durch entsprechende Firewall-Regeln unterstützt. Das ist im vorgenannten Beispiel der Fall, wenn in jedem Netzwerk ein öffentlich erreichbarer Web- oder Mailserver steht, die ebenfalls die gleiche IP-Adresse verwenden.

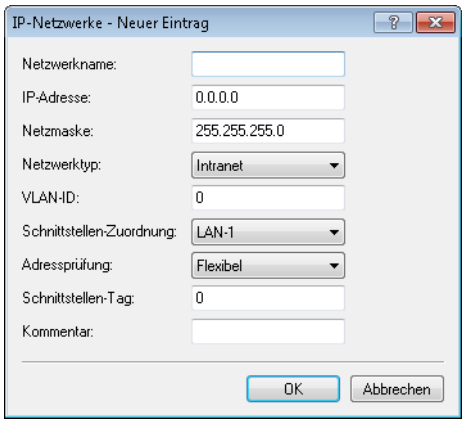
6.3.2 Definition von Netzwerken und Zuordnung von Interfaces

Bei der Definition eines Netzwerkes wird zunächst festgelegt, welcher IP-Adress-Kreis auf einem bestimmten lokalen Interface des Routers gültig sein soll. „Lokale Interfaces" sind dabei logische Interfaces, die einem physikalischen Ethernet- (LAN) oder Wireless-Port (WLAN) zugeordnet sind. Um die oben aufgeführten Szenarien zu realisieren, können durchaus mehrere Netzwerke auf einem Interface aktiv sein – umgekehrt kann ein Netzwerk auch auf mehreren Interfaces aktiv sein.

Die Netzwerke werden in einer Tabelle unter **IPv4** > **Allgemein** > **IP-Netzwerke** definiert. Neben der Definition des Adresskreises und der Interfacezuordnung wird darin auch ein eindeutiger Name für die Netzwerke festgelegt. Dieser Netzwerkname erlaubt es, die Netze in anderen Modulen (DHCP-Server, RIP, etc.) zu identifizieren und diese Dienste nur in bestimmten Netzen anbieten zu können.

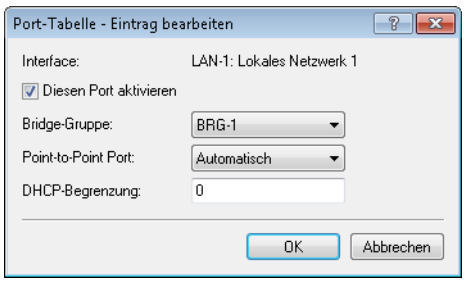
Der Netzwerk-Name darf nicht einem bereits verwendeten Gegenstellen-Namen entsprechen (etwa einer VPN-Verbindung). Die Kommunikation auf dem Netzwerk bzw. der Gegenstelle ist sonst nicht zuverlässig möglich.

Der Netzwerk-Name muss mindestens einen Buchstaben enthalten, da ansonsten in der Routing-Tabelle nicht zwischen IP-Adresse und Interface unterschieden werden kann.



6.3.3 Zuweisung von logischen Interfaces zu Bridge-Gruppen

Unter **Schnittstellen** > **LAN** > **LAN-Bridge** definieren Sie in der **Port-Tabelle** spezielle Eigenschaften der logischen Interfaces.



Diesen Port aktivieren

Mit dieser Option wird das logische Interface aktiviert oder deaktiviert.

Bridge-Gruppe

Ordnet das logische Interface einer Bridge-Gruppe zu und ermöglicht so das Bridging von/zu diesem logischen Interface über die LAN-Bridge. Durch die Zuordnung zu einer gemeinsamen Bridge-Gruppe können mehrere logische Interfaces gemeinsam angesprochen werden und wirken so für den Router wie ein einzelnes Interface – z. B. für die Nutzung im Zusammenhang mit Advanced Routing and Forwarding.

Wird das Interface über die Einstellung **keine** aus allen Bridge-Gruppen entfernt, so findet keine Übertragung über die LAN-Bridge zwischen LAN und WLAN statt (isolierter Modus). In dieser Einstellung ist eine Datenübertragung zwischen LAN und WLAN für dieses Interface nur über den Router möglich.

Voraussetzung für die Datenübertragung von/zu einem logischen interface über die LAN-Bridge ist die Deaktivierung des globalen „Isolierten Modus“, der für die gesamte LAN-Bridge gilt. Außerdem muss das logische Interface einer Bridge-Gruppe zugeordnet sein – in der Einstellung **keine** ist keine Übertragung über die LAN-Bridge möglich.

Point-to-Point Port

Dieser Wert beschreibt die in der IEEE 802.1D definierte „adminPointToPointMAC“-Einstellmöglichkeit. Standardmäßig wird die Point-to-Point-Einstellung der LAN-Schnittstelle automatisch aufgrund der Technologie und des momentanen Status hergeleitet. Es ist jedoch möglich, diese automatisch getroffene Festlegung zu revidieren, falls diese z. B. nicht brauchbar für die vorliegende Konfiguration erscheint.

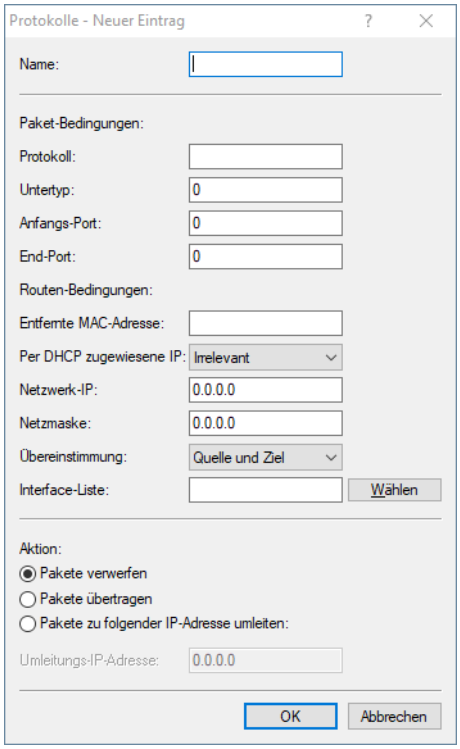
Schnittstellen im Point-to-Point-Modus haben besondere Fähigkeiten, die benutzt werden können, um z. B. im Rapid-Spanning-Tree Verfahren die Port-Status-Wechsel zu beschleunigen.

DHCP-Begrenzung

Anzahl der Clients, die über DHCP zugewiesen werden können. Bei Überschreiten des Limits wird der jeweils älteste Eintrag verworfen. Dies kann in Kombination mit der Protokoll-Filter-Tabelle genutzt werden, um den Zugang auf ein logisches Interface zu begrenzen.

6.3.4 Protokolle filtern

Mit dem Protokoll-Filter können Sie die Behandlung von bestimmten Datenpaketen bei der Übertragung zwischen Interfaces, z. B. aus dem WLAN ins LAN beeinflussen. Mit Hilfe von entsprechenden Regeln wird dabei festgelegt, welche Datenpakete erfasst werden sollen, für welche Interfaces der Filter gilt und welche Aktion mit den Datenpaketen ausgeführt werden soll.



LANconfig: **Schnittstellen** > **LAN** > **LAN-Bridge** > **Protokolle**

Konsole: **Setup** > **LAN-Bridge** > **Protokoll-Tabelle**

Ein Protokoll-Filter besteht ähnlich einer Firewall-Regel aus zwei Teilen:

- Die Paket-Bedingung definiert die Bedingungen, die zutreffen müssen, damit der Filter auf ein Paket angewendet werden muss.
- Die Aktion definiert, was mit dem Paket geschehen soll, wenn die Bedingung zutrifft.

Ein Paketfilter wird durch die folgenden Parameter beschrieben:

Name

Frei wählbarer Name für den Filtereintrag.

Protokoll

Protokoll, für das dieser Filter gelten soll. Wird als Protokoll eine '0' eingetragen, so gilt dieser Filter für **alle** Pakete.

Untertyp

Unterprotokoll, für das dieser Filter gelten soll. Wird als Unterprotokoll eine '0' eingetragen, so gilt dieser Filter für **alle** Pakete des eingetragenen Protokolls.

Anfangs-Port / End-Port

Portbereich, für den dieser Filter gelten soll. Wird für den Anfangs-Port eine '0' eingetragen, so gilt dieser Filter für **alle** Ports des entsprechenden Protokolls / Unterprotokolls. Wird für den End-Port eine '0' eingetragen, gilt der Anfangs-Port auch als End-Port.

Listen mit den offiziellen Protokoll- und Portnummern finden Sie im Internet unter www.iana.org.

Entfernte MAC-Adresse

Die MAC-Adresse des Clients, zu dem das Paket übertragen werden soll. Wird keine Ziel-MAC-Adresse eingetragen, so gilt dieser Filter für **alle** Pakete.

Per DHCP zugewiesene IP

Wird diese Option auf **Ja** oder **Nein** gesetzt, dann wird das DHCP-Tracking aktiviert. Dadurch wird geprüft, ob in der Tabelle **Status** > **LAN-Bridge** > **DHCP-Table** die Quell-MAC-Adresse eines Paketes eingetragen ist, dessen Netzwerk-Teilnehmer eine IP-Adresse per DHCP bezogen hat. Für eine Filterregel kann zusätzlich ein Netz spezifiziert werden. Wenn eine Regel allerdings diesen Parameter auf **Ja** eingestellt hat, wird ein eventuell angegebenes Netz ignoriert.

Mögliche Werte:

- **Ja**: Die Regel trifft zu, wenn die Quell-MAC-Adresse des Pakets in der Tabelle unter **Status** > **LAN-Bridge** > **DHCP-Table** als Adresse verzeichnet ist, die eine IP-Adresse per DHCP bezogen hat.
- **Nein**: Die Regel trifft zu, wenn dies nicht der Fall ist.
- **Irrelevant**: Die Quell-MAC-Adresse findet keine Beachtung.

Wenn das DHCP-Adress-Tracking aktiviert ist, werden die in der Regel evtl. eingetragenen IP-Adressen nicht beachtet.

Netzwerk-IP / Netzmaske

Die IP-Adresse des Netzwerks, für das dieser Filter gilt. Nur IP-Pakete, deren Quell- und Ziel-IP-Adressen in diesem Netzwerk liegen, werden von der Regel erfasst.

Wird kein Netzwerk eingetragen, so gilt dieser Filter für **alle** Pakete.

Übereinstimmung

Per Voreinstellung wird sowohl auf die Quell- als auch auf die Zieladresse geprüft. Hier können Sie festlegen, ob stattdessen nur auf die Quell- oder Zieladresse geprüft werden soll.

Interface-Liste

Liste der Schnittstellen, für die der Filter gilt.

Als Interfaces können alle LAN-Interfaces, DMZ-Interfaces, die logischen WLAN-Netze und die Point-to-Point-Strecken im WLAN eingetragen werden.

Die Interfaces werden z. B. in der Form 'LAN-1' für das erste LAN-Interface oder 'WLAN-2-3' für das dritte logische WLAN-Netz auf dem zweiten physikalischen WLAN-Interface oder 'P2P-1-2' für die zweite Point-to-Point-Strecke auf dem ersten physikalischen WLAN-Interface angegeben.

Gruppen von Interfaces können in der Form 'WLAN-1-1~WLAN-1-6' (logische WLANs 1 bis 6 auf dem ersten physikalischen WLAN-Interface) oder mit Wildcard als 'P2P-1-*' (alle P2P-Strecken auf dem ersten physikalischen Interface) angegeben werden.

Nur Filter-Regeln mit gültigen Einträgen in der Interface-Liste sind aktiv. Eine Regel ohne Angabe der Interfaces gilt nicht für alle, sondern wird ignoriert.

Aktion

Aktion, die für Datenpakete ausgeführt wird, die mit dieser Regel erfasst werden.

Umleitungs-IP-Adresse

Ziel-IP-Adresse für die Aktion 'Umleiten'

Bei einem Redirect wird die Ziel-IP-Adresse der Pakete durch die hier eingetragene Umleitungs-IP-Adresse ersetzt. Zusätzlich wird die Ziel-MAC-Adresse durch die MAC-Adresse ersetzt, die über ARP für die Umleite-IP-Adresse ermittelt wurde.

Wenn die Ziel-MAC-Adresse nicht über ARP ermittelt werden konnte, wird das Paket nicht umgeleitet, sondern verworfen.

Beispiel:

Name	DHCP-Src-MAC	Ziel-MAC-Adr.	Prot.	IP-Adresse	IP-Netzwerk	Untertyp	Anfangs-Port	End-Port	Interface-Liste	Aktion	Umleitungs-IP-Adresse
ARP	irrelevant	000000000000	0806	0.0.0.0	0.0.0.0	0	0	0	WLAN-1-2	Durchlassen	0.0.0.0
DHCP	irrelevant	000000000000	0800	0.0.0.0	0.0.0.0	17	67	68	WLAN-1-2	Durchlassen	0.0.0.0
TELNET	irrelevant	000000000000	0800	0.0.0.0	0.0.0.0	6	23	23	WLAN-1-2	Umleiten	192.168.11.5
ICMP	irrelevant	000000000000	0800	0.0.0.0	0.0.0.0	1	0	0	WLAN-1-2	Durchlassen	0.0.0.0
HTTP	irrelevant	000000000000	0800	0.0.0.0	0.0.0.0	6	80	80	WLAN-1-2	Umleiten	192.168.11.5

ARP, DHCP, ICMP werden durchgelassen, Telnet und HTTP werden umgleitet auf 192.168.11.5, alle anderen Pakete werden verworfen.

Solange für ein Interface keine Filter-Regeln definiert sind, werden alle Pakete von diesem Interface sowie alle Pakete für dieses Interface ohne Veränderung übertragen. Sobald für ein Interface eine Filter-Regel definiert wurde, werden alle Pakete, die über dieses Interface übertragen werden sollen, vor der Bearbeitung geprüft.

1. Im ersten Schritt werden aus den Paketen die zur Prüfung benötigten Informationen ausgelesen:
   - DHCP-Source-MAC
   - Ziel-MAC-Adresse des Paketes
   - Protokoll, z. B. IPv4, ARP
   - Subprotokoll, z. B. TCP, UDP oder ICMP für IPv4-Pakete, ARP Request oder ARP Response für ARP-Pakete
   - IP-Adresse und Netzmaske (Quelle und Ziel) für IPv4-Pakete
   - Quell- und Ziel-Port für IPv4-TCP- oder IPv4-UDP-Pakete

2. Diese Informationen werden im zweiten Schritt gegen die Angaben aus den Filter-Regeln geprüft. Dabei werden alle Regeln berücksichtigt, bei denen das Quell- **oder** das Ziel-Interface in der Interface-Liste enthalten sind. Die Prüfung der Regeln verhält sich für die einzelnen Werte wie folgt:
   - Für DHCP-Source-MAC, Protokoll und Unterprotokoll werden die aus den Paketen ausgelesenen Werte mit den Werten der Regel auf Übereinstimmung geprüft.
   - Bei IP-Adressen werden die Quell- **und** die Ziel-Adresse des Pakets daraufhin geprüft, ob sie in dem Bereich liegen, der durch die IP-Adresse und die Netzmaske der Regel gebildet wird.
   - Quell- und den Zielports werden daraufhin geprüft, ob sie im Bereich zwischen Anfangs- und End-Port liegen.

   Wenn keiner der spezifizierten (nicht durch Wildcards gefüllten) Werte der Regel mit den aus dem Paket ausgelesenen Werten übereinstimmt, wird die Regel als nicht zutreffend betrachtet und ausgelassen. Falls mehrere Regeln zutreffen,

wird die Aktion der Regel ausgeführt, die am genauesten zutrifft. Dabei gelten die Parameter als genauer, je weiter unten Sie in der Liste der Parameter stehen bzw. je weiter rechts sie in der Protokoll-Tabelle auftauchen.

Wenn für ein Interface Regeln definiert sind, bei einem Paket von bzw. für dieses Interface jedoch keine Übereinstimmung mit einer der Regeln gefunden werden kann, dann wird für das Paket die Default-Regel für das Interface verwendet. Die Default-Regel ist für jedes Interface mit der Aktion 'verwerfen' vorkonfiguriert, aber nicht sichtbar in der Protokoll-Tabelle. Um die Default-Regel für ein Interface zu modifizieren, wird eine Regel mit dem Namen 'default-drop' angelegt, die neben den entsprechenden Interface-Bezeichnungen nur Wildcards und die gewünschte Aktion enthält.

Die Prüfung der MAC-Adressen verhält sich bei Paketen, die über das entsprechende Interface verschickt werden, anders als bei eingehenden Paketen.

- Bei den ausgehenden Paketen wird die aus dem Paket ausgelesene Quell-MAC-Adresse gegen die in der Regel eingetragene Ziel-MAC-Adresse geprüft.
- Die aus dem Paket ausgelesene Ziel-MAC-Adresse wird daraufhin geprüft, ob sie in der Liste der aktuell aktiven DHCP-Clients enthalten sind.
- Regeln mit der Aktion 'Umleiten' werden ignoriert, wenn sie für ein Interface zutreffen, auf dem das Paket verschickt werden soll.

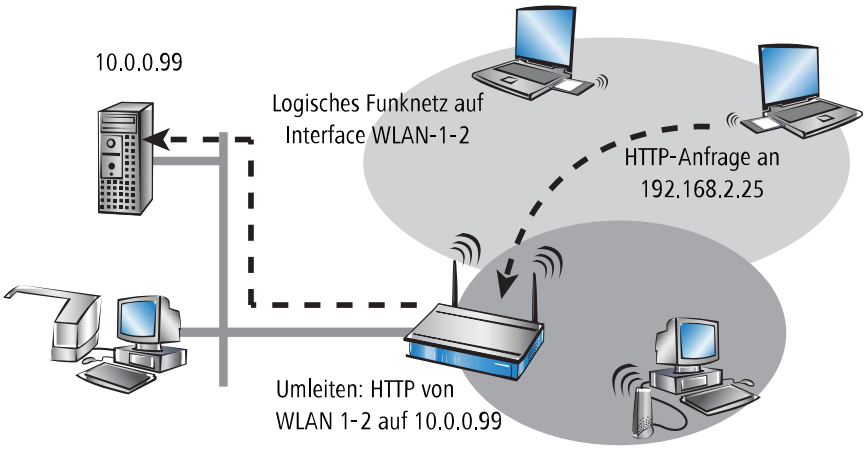
3. Im dritten Schritt wird die Aktion der zutreffenden Regel ausgeführt.

Mit der Aktion 'Umleiten' (Redirect) können IPv4-Pakete nicht nur übertragen oder verworfen werden, sondern gezielt zu einem bestimmten Ziel übermittelt werden. Dazu wird die Ziel-IP-Adresse des Pakets durch die in der Regel eingetragene Umleitungs-IP-Adresse ersetzt, die Ziel-MAC-Adresse des Pakets wird durch die per ARP ermittelte, zur Umleitungs-IP-Adresse gehörige MAC-Adresse ersetzt.

Damit die umgeleiteten Pakete auf dem „Rückweg“ auch wieder den richtigen Absender finden, werden in einer dynamischen Tabelle automatisch Filter-Regeln angelegt, die für die ausgehenden Pakete auf diesem Interface genutzt werden. Diese Tabelle kann unter `Status > LAN-Bridge-Statistiken > Verbindungs-Tabelle` eingesehen werden. Die Regeln in dieser Tabelle haben eine höhere Priorität als andere passende Regeln mit den Aktionen 'Übertragen' oder 'Verwerfen'.

Die Teilnehmer (Clients) in Funknetzwerken haben vor allem eine Eigenschaft oft gemeinsam: eine hohe Mobilität. Die Clients verbinden sich also nicht unbedingt immer mit dem gleichen AP, sondern wechseln den AP und das zugehörige LAN relativ häufig.

Die Redirect-Funktion hilft dabei, die Anwendungen von WLAN-Clients bei der Übertragung in das LAN automatisch immer auf den richtigen Zielrechner einzustellen. Wenn die Anfragen von WLAN-Clients über HTTP aus einem bestimmten logischen Funknetzwerk immer auf einen bestimmten Server im LAN umgeleitet werden sollen, wird für das entsprechende Protokoll ein Filtereintrag mit der Aktion 'Umleiten' für das gewünschte logische WLAN-Interface aufgestellt.



Alle Anfragen mit diesem Protokoll aus diesem logischen Funknetz werden dann automatisch umgeleitet auf den Zielserver im LAN. Bei der Rückübertragung der Datenpakete werden die entsprechenden Absenderadressen und Ports aufgrund der Einträge in der Verbindungsstatistik wieder eingesetzt, so dass ein störungsfreier Betrieb in beiden Richtungen möglich ist.

Mit dem DHCP-Adress-Tracking wird nachgehalten, welche Clients ihre IP-Adresse über DHCP erhalten haben. Die entsprechenden Informationen werden für ein Interface automatisch in einer Tabelle unter `Status > LAN-Bridge-Statistiken > DHCP-Tabelle` geführt. DHCP-Tracking wird auf einem Interface aktiviert, wenn für dieses Interface mindestens eine Regel definiert ist, bei denen 'DHCP-Source-MAC' auf 'Ja' steht.

Die Anzahl der Clients, die über DHCP mit einem Interface verbunden sein dürfen, kann in der Port-Tabelle unter `Setup > LAN-Bridge > Port-Daten` eingestellt werden. Mit dem Eintrag von '0' können sich beliebig viele Clients an diesem Interface über DHCP anmelden. Würde die maximale Anzahl der DHCP-Clients bei einem weiteren Anmeldeversuch überschritten, so wird der älteste Eintrag aus der Liste entfernt.

Bei der Prüfung der Datenpakete werden die in der Regel definierten IP-Adresse und die IP-Netzmaske nicht verwendet. Es wird also nicht geprüft, ob die Ziel-IP-Adresse des Paketes im vorgegebenen Bereich liegt. Stattdessen wird geprüft, ob die Quell-IP-Adresse des Pakets mit derjenigen IP-Adresse übereinstimmt, die dem Client per DHCP zugewiesen wurde. Die Verbindung der beiden IP-Adressen findet anhand der Quell-MAC-Adresse statt.

Mit dieser Prüfung können Clients geblockt werden, die zwar eine IP-Adresse via DHCP empfangen haben, dann aber (versehentlich oder bewusst) tatsächlich eine andere IP-Adresse verwenden. Eine Regel mit dem Parameter DHCP-Source-MAC = 'Ja' würde also nicht zutreffen, da die beiden Adressen nicht übereinstimmen. Stattdessen würde eine andere Regel oder die Default-Regel das Paket verarbeiten.

Damit DHCP-Tracking funktionieren kann, müssen mindestens zwei weitere Regeln für dieses Interface konfiguriert werden, die nicht auf DHCP-Tracking beruhen. Das ist erforderlich, da die erforderliche DHCP-Information erst am Ende der DHCP-Verhandlung ausgetauscht wird. Daher müssen die vorher zu übertragenden Pakete über Regeln zugelassen werden, die kein DHCP-Tracking verwenden. Dazu gehören normalerweise Pakete über TCP / UDP auf Port 67 und 68 und ARP-Pakete.

Ist DHCP-Tracking auf einem Interface aktiviert, so werden automatisch auf diesem Interface empfangene Pakete von DHCP-Servern verworfen.

6.3.5 Schnittstellen-Tags für Gegenstellen

Mit der Definition von Schnittstellen-Tags können im Rahmen des Advanced Routing and Forwarding (ARF) virtuelle Router genutzt werden, die nur einen Teil der gesamten Routing-Tabelle verwenden. Bei den aus dem WAN eingehenden Datenpaketen kann die Zuordnung der Schnittstellen-Tags auf unterschiedliche Weise geregelt werden:

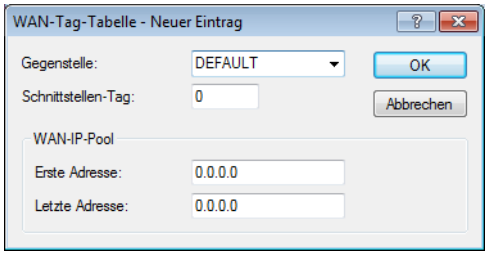
- mit Hilfe von entsprechenden Firewall-Regeln, die nur Datenpakete von bestimmten Gegenstellen, IP-Adressen oder Ports erfassen
- über eine explizite Zuordnung der Tags zu den Gegenstellen.

Mit der Zuordnung der Tags zu den Gegenstellen kann die Trennung der ARF-Netze auch für WAN-seitig empfangende Pakete komfortabel genutzt werden (die standardmäßig das Tag 0 erhalten). Ohne eine Zuordnung der Tags explizit über die Firewall zu steuern kann der virtuelle Router in Form des Schnittstellen-Tags direkt aus der Gegenstelle bzw. der Quellroute bestimmt werden. Ein- und ausgehende Kommunikation kann somit einfacher bidirektional in virtuelle Router unterteilt werden.

Die über die Tag-Tabelle ermittelten Schnittstellen-Tags können durch einen passenden Eintrag in der Firewall überschrieben werden.

6.3.5.1 Zuweisung von Schnittstellen-Tags über die Tag-Tabelle

LANconfig: **Kommunikation** > **Gegenstellen** > **WAN-Tag-Tabelle**



Mit dem Schnittstellen-Tag werden Gegenstellen einem eindeutigen ARF-Netz bzw. Tag zugeordnet. Diese Zuweisung muss manuell für jedes ARF-Netz erfolgen.

Ab LCOS 10.20 wird eine automatische WAN-Tag-Erzeugung nicht mehr unterstützt. Alle Gegenstellen müssen manuell zugeordnet werden.

6.3.6 Ermittlung des Routing-Tags für lokale Routen

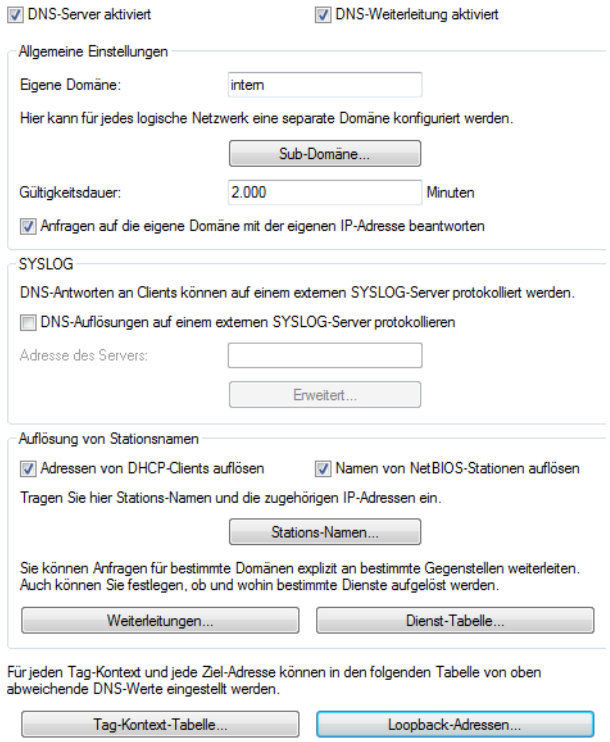
Mit der Definition von Schnittstellen-Tags können im Rahmen des Advanced Routing and Forwarding (ARF) virtuelle Router genutzt werden, die nur einen Teil der gesamten Routing-Tabelle verwenden. Für ein von einem anderen lokalen Router empfangenes Paket wird das Schnittstellen-Tag in den folgenden Schritten ermittelt:

1. Gibt es auf einem LAN-Interface / VLAN-Paar nur ein ARF-Netz, so wird dieses ausgewählt.
2. Gibt es mehrere ARF-Netze auf einem LAN-Descriptor / VLAN-Paar, so wird geschaut, ob die Quell-Adresse des Pakets lokal in einem der ARF-Netze ist. Dieses wird dann ausgewählt.
3. Scheitert dies, dann wird für die Quell-MAC-Adresse ein Revers-ARP-Lookup gemacht und so die Adresse des Next-Hops zur Quell-Adresse ermittelt. Ist die Adresse auflösbar, so wird geschaut, ob sie lokal in einem der ARF-Netze ist. Dieses wird dann ausgewählt.
4. Ist keine Auflösung möglich, so wird das erste ARF-Netz des LAN-Interface / VLAN-Paares ausgewählt.
5. Das ausgewählte ARF-Netz bestimmt das verwendete Schnittstellen-Tag.

6.3.7 Routing-Tags für DNS-Weiterleitung

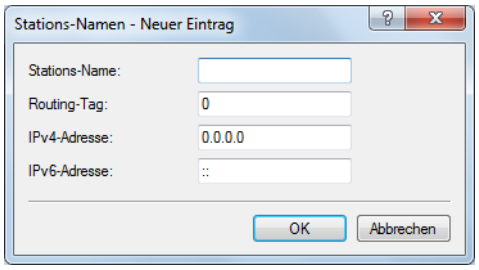
Bei der DNS-Weiterleitung sind mehrere voneinander unabhängige Forwarding-Definitionen (insbesondere allgemeine Wildcard-Definitionen mit „*“) durch die Kennzeichnung mit eindeutigen Routing-Tags möglich. Abhängig vom

Routing-Kontext des anfragenden Clients berücksichtigt der Router nur die passend gekennzeichneten Forwarding-Einträge sowie die allgemeinen, mit „0“ gekennzeichneten Einträge.



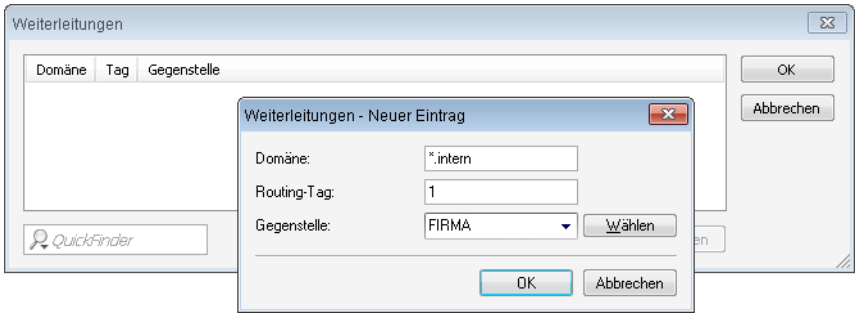
Stations-Namen

Unter **DNS** > **Allgemein** > **Stations-Namen** definieren Sie, welche Stations-Namen das Gerät wie und in welchem Tag-Kontext auflöst.



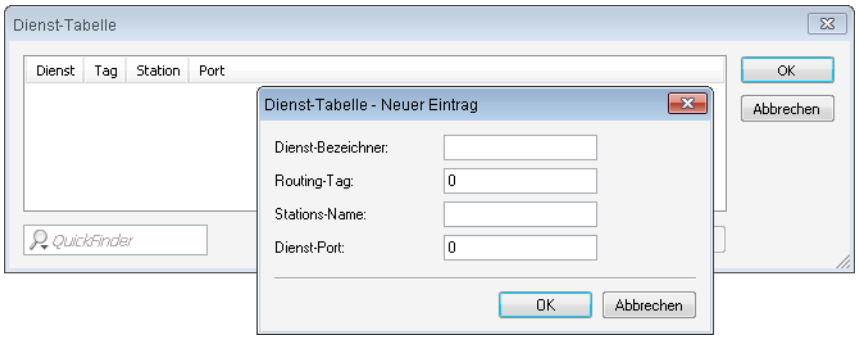
DNS-Weiterleitungen

Unter **DNS** > **Allgemein** > **Weiterleitungen** versehen Sie Weiterleitungsregeln mit Routing-Tags, so dass diese nur mit dem korrekten Routing-Tag zur Verfügung stehen.



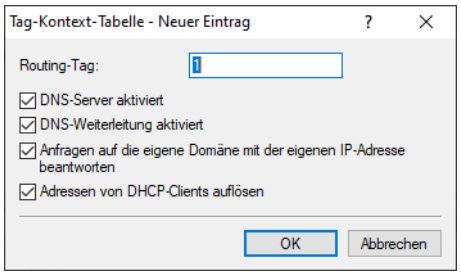
Dienst-Tabelle

Unter **DNS** > **Allgemein** > **Dienst-Tabelle** versehen Sie Dienste mit Routing-Tags, so dass diese nur mit dem korrekten Routing-Tag erreichbar sind.



Tag-Kontext-Tabelle

Im LANconfig lassen sich unter **DNS** > **Allgemein** > **Tag-Kontext-Tabelle** Tag-Kontexte definieren, die die globalen Einstellungen des DNS-Servers für bestimmte Schnittstellen- und Routing-Tags (Routing-Kontext) überschreiben:



Wenn ein Eintrag für einen Tag-Kontext existiert, dann gelten für diesen Kontext nur die DNS-Einstellungen in dieser Tabelle. Existiert hingegen kein Eintrag in dieser Tabelle, dann gelten die globalen Einstellungen des DNS-Servers.

Folgende Optionen sind je Tag-Kontext möglich:

Routing-Tag

Eindeutiges Schnittstellen- bzw. Routing-Tag im Bereich von 1-65535, dessen folgende Einstellungen die globalen Einstellungen des DNS-Servers überschreiben sollen.

DNS-Server aktiviert

Aktiviert den DNS-Server des Gerätes.

DNS-Weiterleitung aktiviert

Aktiviert DNS-Weiterleitungen für dieses Gerät.

Anfragen auf die eigene Domäne mit der eigenen IP-Adresse beantworten

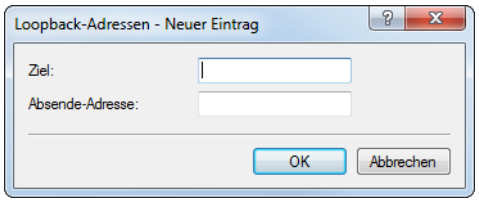
Wenn aktiviert, werden DNS-Anfragen betreffs der eigenen Domäne mit der IP-Adresse des Routers beantwortet.

Adressen von DHCP-Clients auflösen

Aktiviert die Auflösung von Stations-Namen, die über DHCP eine IP-Adresse angefordert haben.

Loopback-Adressen

Im LANconfig lassen sich unter **DNS** > **Allgemein** > **Loopback-Adressen** Loopback-Adressen für jede Gegenstelle hinterlegen. Somit gibt es dann eine einstellbare Absende-Adresse für DNS-Weiterleitungen. Jede Loopback-Adresse besteht aus genau einer Gegenstelle und Loopback-Adresse. Da pro Loopback-Adresse nur genau eine Gegenstelle eingetragen werden kann, müssen hier zwei Einträge erfolgen, falls in den DNS-Weiterleitungen für eine Domain zwei Gegenstellen konfiguriert wurden.



Folgende Optionen sind je Loopback-Adresse möglich:

Ziel

Die Gegenstelle für eine Loopback-Adresse. Dies ist entweder ein Interface-Name, eine IPv4- oder IPv6-Adresse. Nach einem „@" kann ein Routing-Tag hinzugefügt werden. Die Gegenstelle muss genauso auch in der Tabelle DNS-Weiterleitungen vorkommen.

Absende-Adresse

Die Loopback-Adresse für eine bestimmte Gegenstelle. Dies ist entweder ein Interface-Name, eine IPv4- oder IPv6-Adresse oder eine benannte Loopback-Adresse.

6.3.8 Virtuelle Router

Die interfaceabhängige Filterung ermöglicht es – zusammen mit dem Policy-based Routing – für jedes Interface virtuelle Router zu definieren.

Beispiel:

Es werden zwei separate IP-Netze verwendet für Entwicklung und Vertrieb. Beide Netze hängen an verschiedenen Switchports, verwenden aber das gleiche Netz '10.1.1.0/255.255.255.0'. Der Vertrieb soll nur ins Internet dürfen, während die Entwicklung auch auf das Netz einer Partnerfirma ('192.168.1.0/255.255.255.0'') zugreifen darf.

Es ergibt sich folgende Routing-Tabelle (dabei hat die Entwicklungsabteilung das Tag 2 und der Vertrieb das Tag 1):

IP-Adresse	IP-Netzmaske	Rtg-tag	Peer-oder-IP	Distanz	Maskierung	Aktiv
192.168.1.0	255.255.255.0	2	PARTNER	0	nein	ja
192.168.0.0	255.255.0.0	0	0.0.0.0	0	nein	ja
255.255.255.255	0.0.0.0	2	INTERNET	2	ja	ja
255.255.255.255	0.0.0.0	1	INTERNET	2	ja	ja

Stünden Entwicklung und Vertrieb in IP-Netzen mit unterschiedlichen Adressbereichen, wäre die Zuordnung der Routing-Tags über Firewall-Regeln kein Problem. Da aber beide Abteilungen im gleichen IP-Netz stehen, ist nur eine Zuordnung über die Netzwerknamen möglich.

Die Zuweisung der Tags kann direkt bei der Netzwerk-Definition erfolgen:

Netzwerkname	IP-Adresse	Netzmaske	VLAN-ID	Interface	Adressprüfung	Typ	Rtg-Tag
ENTWICKLUNG	10.1.1.1	255.255.255.0	0	LAN-1	streng	Intranet	2
VERTRIEB	10.1.1.1	255.255.255.0	0	LAN-2	streng	Intranet	1

Alternativ kann die Zuweisung der Tags auch über die Kombination von Netzwerkdefinitionen und Firewallregeln erfolgen. Die Netze sind wie folgt definiert:

Netzwerkname	IP-Adresse	Netzmaske	VLAN-ID	Interface	Adressprüfung	Typ	Rtg-Tag
ENTWICKLUNG	10.1.1.1	255.255.255.0	0	LAN-1	streng	Intranet	0
VERTRIEB	10.1.1.1	255.255.255.0	0	LAN-2	streng	Intranet	0

Dann lassen sich durch die Routing-Tags folgende Firewall-Regeln festlegen:

Name	Protokoll	Quelle	Ziel	Aktion	verknuepft	Prio	(...)	Rtg-tag
ENTWICKLUNG	ANY	%Lentwicklung	ANYHOST	%a	ja	255		2
VERTRIEB	ANY	%Lvertrieb	ANYHOST	%a	ja	255		1

Wichtig bei diesen Regeln ist die maximale Priorität (255), damit die Regeln immer als erstes ausgewertet werden. Damit nun trotz dieser Regeln noch eine Filterung nach Diensten möglich ist, muss die Option "verknuepft" in der Firewall-Regel gesetzt sein.

6.4 Die Konfiguration von Gegenstellen

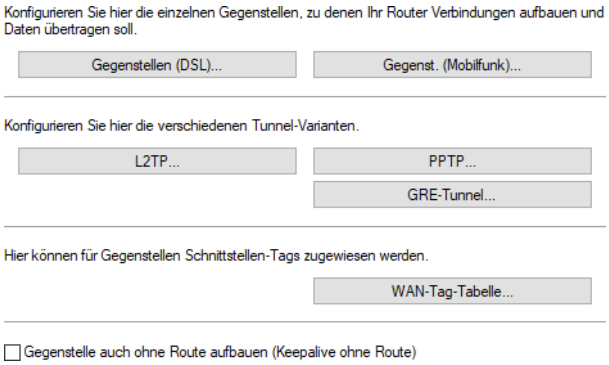
Gegenstellen werden in zwei Tabellen konfiguriert:

- In der Gegenstellenliste (bzw. den Gegenstellenlisten) werden alle Informationen eingestellt, die individuell für nur eine Gegenstelle gelten.
- Parameter für die unteren Protokollebenen (unterhalb von IP) werden in der Kommunikations-Layer-Tabelle definiert.

In diesem Abschnitt wird die Konfiguration der Authentifizierung (Protokoll, Benutzername, Passwort) nicht behandelt. Informationen zur Authentifizierung finden Sie im Abschnitt *Verbindungsaufbau mit PPP* auf Seite 455.

6.4.1 Gegenstellenliste

Die verfügbaren Gegenstellen werden in der Gegenstellenliste mit einem geeigneten Namen und zusätzlichen Parametern angelegt. Für jedes WAN-Interface gibt es eine separate Gegenstellenliste. Die Gegenstellenlisten richten Sie ein unter **Kommunikation** > **Gegenstellen**.



Gegenstelle auch ohne Route aufbauen (Keepalive ohne Route)

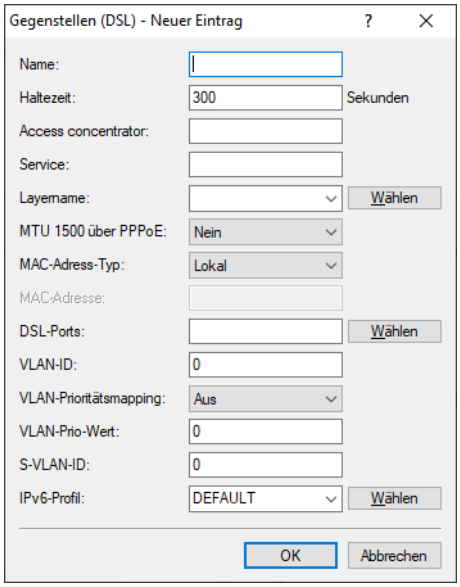
Definiert, ob eine Gegenstelle, z. B. ein VPN-Tunnel oder eine Internetverbindung, auch ohne Route aufgebaut werden soll. Der Aufbau der Gegenstelle ohne explizite Route in der Routing-Tabelle ist inbesondere dann erforderlich, wenn die Gegenseite die Routen übermittelt, z. B. durch DHCP (Classless-Static-Route-Option) oder ein dynamisches Routing-Protokoll.

Bitte beachten Sie bei der Bearbeitung der Gegenstellenlisten folgende Hinweise:

- Werden in zwei Gegenstellenlisten (z. B. DSL-Breitband-Gegenstellen und Einwahl-Gegenstellen) Einträge mit identischen Namen für die Gegenstelle vorgenommen, verwendet das Gerät beim Verbindungsaufbau zu der entsprechenden Gegenstelle automatisch das „schnellere" Interface. Das andere Interface wird in diesem Fall als Backup verwendet.
- Werden in der Liste der DSL-Breitband-Gegenstellen weder Access Concentrator noch Service angegeben, stellt der Router eine Verbindung zum ersten Access Concentrator her, der sich auf die Anfrage über die Vermittlungsstelle meldet.
- Für ein ggf. vorhandenes DSLoL-Interface gelten die gleichen Einträge wie für ein DSL-Interface. Die Einträge dazu werden in der Liste der DSL-Breitband-Gegenstellen vorgenommen.

DSL-Breitband-Gegenstellen

DSL-Breitband-Gegenstellen richten Sie über **Gegenstellen (DSL)** ein.



Name

Mit diesem Namen wird die Gegenstelle in den Router-Modulen identifiziert. Sobald das Router-Modul anhand der IP-Adresse ermittelt hat, bei welcher Gegenstelle das gewünschte Ziel erreicht werden kann, können aus der Gegenstellenliste die zugehörigen Verbindungsparameter ermittelt werden.

Haltezeit

Diese Zeit gibt an, wie lange die Verbindung aktiv bleibt, nachdem keine Daten mehr übertragen wurden. Wird eine Null als Haltezeit angegeben, wird die Verbindung nicht automatisch beendet. Bei einer Haltezeit von 9999 Sekunden werden abgebrochene Verbindungen selbstständig wiederhergestellt (siehe *Dauerverbindung für Flatrates – Keep-alive* auf Seite 464).

VPI / VCI

Geben Sie hier den VPI (Virtual Path Identifier) und den VCI (Virtual Channel Identifier) für Ihre ADSL-Verbindung ein.

Diese Werte werden Ihnen von Ihrem ADSL-Netzbetreiber mitgeteilt. Übliche Werte für VPI/VCI sind zum Beispiel: 0/35, 0/38, 1/32, 8/35, 8/48.

Access concentrator

Der Access Concentrator (AC) steht für den Server, der über diese Gegenstelle erreicht werden kann. Stehen mehrere Provider zur Auswahl, die über Ihren ADSL-Anschluss genutzt werden können, wählen Sie mit dem Namen des AC den Provider aus, der für den IP-Adresskreis dieser Gegenstelle zuständig ist. Der Wert für den AC wird Ihnen von Ihrem Provider mitgeteilt. Wird kein Wert für den AC eingetragen, wird jeder AC angenommen, der den geforderten Service anbietet.

Service

Tragen Sie hier den Dienst ein, den Sie bei Ihrem Provider nutzen möchten. Das kann z. B. einfaches Internet-Surfen sein oder aber auch Video-Downstream. Der Wert für den Service wird Ihnen von Ihrem Provider mitgeteilt. Wird kein Wert für den Service eingetragen, wird jeder Service angenommen, den der geforderte Access concentrator anbietet.

Layername

Wählen Sie den Kommunikations-Layer aus, der für diese Verbindung verwendet werden soll. Die Konfiguration dieser Layer ist in *Layer-Liste* auf Seite 413 beschrieben.

MTU 1500 über PPPoE

Definiert, ob das Gerät im PPPoE eine MTU von 1500 nach *RFC 4638* verhandeln soll. Die Gegenseite muss diese Erweiterung ebenfalls unterstützen.

MAC-Adress-Typ

Wählen Sie, welche MAC-Adresse verwendet werden soll. Falls eine bestimmte MAC-Adresse für den entfernten Gateway angegeben werden muss (**Benutzerdefiniert**), dann geben Sie diese unter **MAC-Adresse** an. Bei **Lokal** werden weitere virtuelle Adressen für jede WAN-Verbindung erzeugt auf Basis der MAC-Adresse des Gerätes. Bei **Global** wird die MAC-Adresse des Gerätes für alle Verbindungen verwendet.

MAC-Adresse

Geben Sie hier ggfs. die benutzerdefinierte MAC-Adresse an.

DSL-Ports

Wählen Sie die zu verwendenden DSL-Ports aus, wenn ihr Gerät über mehr als einen DSL-Port verfügt. Aktivieren Sie die Kanal-Bündelung im verwendeten Layer, um DSL-Anschlüsse zu bündeln.

VLAN-ID

Siehe *VLAN-IDs für DSL-Interfaces* auf Seite 950.

VLAN-Prioritätsmapping

Dieser Eintrag steuert die Funktionsweise des VLAN-Prioritätsmapping.

Aus

VLAN-Prioritätsmapping ist deaktiviert.

1TR-112

Der Wert „1TR112“ mappt die Precedence (also die obersten 3 Bits) des DSCP in das Feld VLAN-Prio. Zusätzlich werden PPP-LCP-Echo-Pakete mit VLAN-Priorität 6 markiert, sowie IGMP-Pakete mit 4 markiert.

DSCP

Der Wert „DSCP“ mappt die Precedence (also die obersten 3 Bits) des DSCP in das Feld VLAN-Prio.

Wert

Alle Pakete, die auf das WAN gensendet werden, werden mit dem Prioritäts-Tag markiert, das unter **VLAN-Prio-Wert** konfiguriert ist. Das passiert aber nur, wenn auch ein VLAN ungleich 0 konfiguriert ist. Sonst würde es der Einstellung „Aus“ entsprechen.

VLAN-Prio-Wert

Dieser Wert wird als VLAN-Prioritätswert gesetzt, wenn **VLAN-Prioritätsmapping** auf „Wert“ eingestellt wurde.

S-VLAN-ID

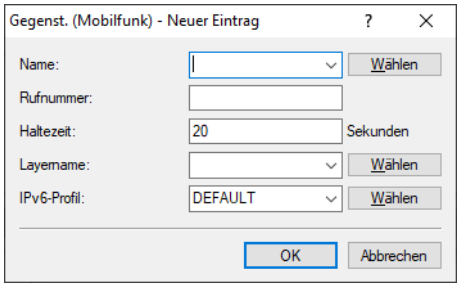
Siehe *Q-in-Q-VLAN* auf Seite 946.

IPv6-Profil

Dieser Eintrag gibt die IPv6-Gegenstelle an. Ein leerer Eintrag schaltet IPv6 für dieses Interface ab. Die IPv6-Gegenstellen konfigurieren Sie unter **IPv6** > **Allgemein** > **IPv6-Schnittstellen** > **WAN-Profile**.

Einwahl-Gegenstellen

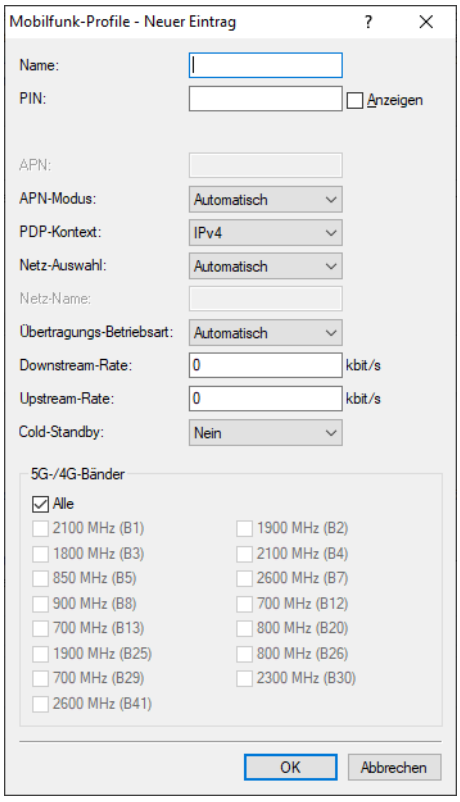
Einwahl-Gegenstellen richten Sie über **Gegenstellen (Mobilfunk)** ein. Abhängig vom Gerät können hier auch andere Einwahlmöglichkeiten zur Verfügung stehen.



Name

Mit diesem Namen wird die Gegenstelle in den Router-Modulen identifiziert. Sobald das Router-Modul anhand der IP-Adresse ermittelt hat, bei welcher Gegenstelle das gewünschte Ziel erreicht werden kann, können aus der Gegenstellenliste die zugehörigen Verbindungsparameter ermittelt werden.

Der Name der Gegenstelle entspricht hier einem **Mobilfunk-Profil** aus **Schnittstellen** > **WAN** > **Mobilfunk-Einstellungen**.



Name

Geben Sie hier einen eindeutigen Namen für dieses Mobilfunk-Profil ein. Dieses Profil kann dann in den WAN-Interface-Einstellungen (Mobilfunk) ausgewählt werden.

PIN

Geben Sie hier die 4-stellige PIN-Nummer der im Mobilfunk-Interface verwendeten Mobilfunk-SIM-Karte ein. Der Router benötigt diese Information, um das Mobilfunk-Interface in Betrieb zu nehmen.

Die SIM-Karte hält selbstständig jeden Fehlversuch auch über eine Unterbrechung der Spannungsversorgung hinweg nach. Auch wenn der Router im Betrieb einen Fehlversuch erkennt und bis zur nächsten Konfigurationsänderung der PIN oder bis zu einem Kartenwechsel nicht wiederholt, sperrt sich die Karte nach 3 Fehlversuchen. Dies erfordert dann die Entsperrung der SIM-Karte mit der in der Regel 8-stelligen PUK- bzw. SuperPIN- Nummer.

APN

Geben Sie hier den Namen des Zugangs-Servers für Mobilfunk-Datendienste ein, kurz APN (Access Point Name). Er ist spezifisch für Ihren Mobilfunk-Dienstanbieter und Sie finden diese Information normalerweise in den Unterlagen Ihres Mobilfunk-Vertrages.

APN-Modus

Definiert in welchem Modus der APN verwendet werden soll.

- Bei Automatisch wird der APN aus der internen Datenbank der Provider-Einstellungen des Betriebssystems genommen. Hierzu wird der Provider aus der SIM-Karte (MCC/MNC) abgefragt und in der internen Datenbank gesucht. Der Modus „Automatisch" funktioniert nur bei öffentlichen Provider-APNs und nicht bei privaten APNs. Bei privaten APNs muss der Modus auf "Manuell" gesetzt werden und der APN in das Feld "APN" eingetragen werden.
- Bei Manuell wird der APN aus dem Feld APN verwendet

PDP-Kontext

Definiert den verwendeten IP-Typ des Packet Data Protocol (PDP) Kontextes.

- IPv4: Es wird eine reine IPv4-Datenverbindung aufgebaut
- IPv4+IPv6: Es wird eine Dual-Stack-Datenverbindung, d.h. IPv4 und IPv6 aufgebaut
- IPv6: Es wird eine reine IPv6-Datenverbindung aufgebaut

Netz-Auswahl

Wenn Sie die automatische Mobilfunk-Netzwahl selektieren, dann bucht sich das Mobilfunk-Interface selbstständig in einem der verfügbaren und erlaubten Mobilfunk-Netze ein. Selektieren Sie hingegen die manuelle Mobilfunk-Netzwahl, dann bucht sich das Mobilfunk-Interface ausschließlich in dem darunter angegebenen Mobilfunk-Netz ein.

Die manuelle Mobilfunk-Netzwahl ist insbesondere dann angeraten, wenn der Router stationär betrieben wird und es häufiger vorkommen kann, dass sich das Mobilfunk-Interface in ein benachbartes oder funktechnisch stärkeres, mitunter aber unerwünschtes oder teureres Mobilfunk-Netz einbucht.

Netz-Name

Wenn Sie die manuelle Mobilfunk-Netzwahl selektiert haben, dann bucht sich das Mobilfunk-Interface ausschließlich in dem hier unter seinem langen Namen angegebenen Mobilfunk-Netz ein.

Übertragungs-Betriebsart

Wählen Sie hier den vom Mobilfunk-Interface bevorzugten Mobilfunk-Datenübertragungs-Standard.

Downstream-Rate / Upstream-Rate

Damit die Quality-of-Service (QoS)-Funktionen der Firewall einwandfrei funktionieren, müssen hier die Übertragungsraten des verwendeten WWAN-Anschlusses angegeben werden.

Wird bei der Downstream- oder der Upstream-Rate 0 eingegeben, so gilt das Interface als unbeschränkt und QoS-Mechanismen können nicht greifen.

5G-/4G-Bänder

Wenn aufgrund ungünstiger Umgebungsbedingungen der Router ständig zwischen zwei Frequenzbändern wechselt, kann das zu Instabilitäten bei der Übertragung führen. Mit dieser Auswahl geben Sie dem Mobilfunk-Router vor, welche Frequenzbänder er verwenden darf bzw. soll.

Rufnummer

Eine Rufnummer wird nur benötigt, wenn die Gegenstelle angerufen werden soll. Das Feld kann leer bleiben, wenn lediglich Rufe angenommen werden sollen. Mehrere Rufnummern für dieselbe Gegenstelle können in der **RoundRobin-Liste** eingetragen werden.

Haltezeit

Diese Zeit gibt an, wie lange die Verbindung aktiv bleibt, nachdem keine Daten mehr übertragen wurden. Wird eine Null als Haltezeit angegeben, wird die Verbindung nicht automatisch beendet. Bei einer Haltezeit von 9999 Sekunden werden abgebrochene Verbindungen selbstständig wiederhergestellt (siehe *Dauerverbindung für Flatrates – Keep-alive* auf Seite 464).

Layername

Wählen Sie den Kommunikations-Layer aus, der für diese Verbindung verwendet werden soll. Die Konfiguration dieser Layer ist in *Layer-Liste* auf Seite 413 beschrieben.

IPv6-Profil

Dieser Eintrag gibt die IPv6-Gegenstelle an. Ein leerer Eintrag schaltet IPv6 für dieses Interface ab. Die IPv6-Gegenstellen konfigurieren Sie unter **IPv6** > **Allgemein** > **IPv6-Schnittstellen** > **WAN-Profile**.

6.4.2 Layer-Liste

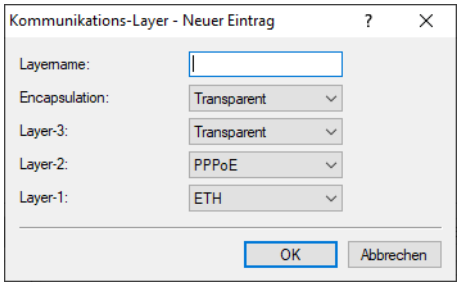
Mit einem Layer definieren Sie eine Sammlung von Protokoll-Einstellungen, die für die Verbindung zu bestimmten Gegenstellen verwendet werden soll. Die Liste der Kommunikations-Layer finden Sie unter:

LANconfig: **Kommunikation** > **Allgemein** > **Kommunikations-Layer**

Konsole: **Setup** > **WAN** > **Layer**

In der Kommunikations-Layer-Liste sind die gängigen Protokollkombinationen bereits vordefiniert. Änderungen oder Ergänzungen sollten Sie nur vornehmen, wenn Gegenstellen inkompatibel zu den vorhandenen Layern sind. Die möglichen Optionen finden Sie in der folgenden Übersicht.

Beachten Sie, dass die im Gerät vorhandenen Parameter vom Funktionsumfang des Gerätes abhängen. Es kann daher sein, dass Ihr Gerät nicht alle hier beschriebenen Optionen anbietet.



Layername

Unter diesem Namen wird der Layer in den Gegenstellenlisten ausgewählt.

Encapsulation

Für die Datenpakete können zusätzliche Kapselungen eingestellt werden:

Transparent

Keine zusätzliche Kapselung.

Ethernet

Kapselung als Ethernet-Frames.

LLC-ETH

Ethernet über ATM mit LLC-Kapselung nach RFC 2684.

LLC-MUX

Multiplexing über ATM mit LLC/SNAP-Kapselung nach RFC 2684. Mehrere Protokolle können im selben VC (Virtual Channel) übertragen werden.

VC-MUX

Multiplexing über ATM durch Aufbau zusätzlicher VCs nach RFC 2684.

Layer-3

Folgende Optionen stehen für die Vermittlungsschicht (oder Netzwerkschicht) zur Verfügung:

Transparent

Es wird kein zusätzlicher Header eingefügt.

PPP

Der Verbindungsaufbau erfolgt nach dem PPP-Protokoll (im synchronen Modus, d. h. bitorientiert). Die Konfigurationsdaten werden der PPP-Tabelle entnommen.

DHCP

Zuordnung der Netzwerkparameter über DHCP.

DHCP (Broadcast-Flag)

Der Verbindungsaufbau erfolgt mit DHCP-Client und gesetztem Broadcast-Flag im DHCP.

Layer-2

In diesem Feld wird der obere Teil der Sicherungsschicht (Data Link Layer) konfiguriert. Folgende Optionen stehen zur Verfügung:

Transparent

Es wird kein zusätzlicher Header eingefügt.

PPPoE

Kapselung der PPP-Protokollinformationen in Ethernet-Frames.

Layer-1

In diesem Feld wird der untere Teil der Sicherungsschicht (Data Link Layer) konfiguriert. Folgende Optionen stehen zur Verfügung:

ETH

Transparentes Ethernet nach IEEE 802.3

WWAN

Für Verbindungen über das interne WWAN-Modem.

XDSL

Für Verbindungen über das interne DSL-Modem.

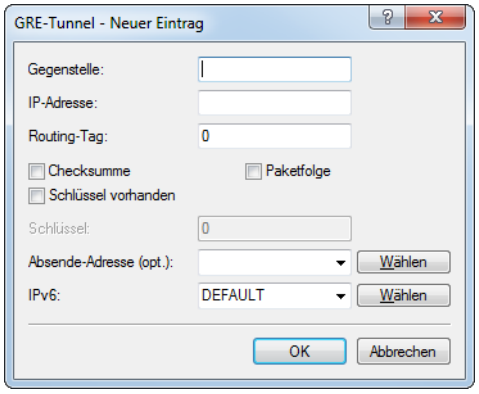
6.5 Generic Routing Encapsulation (GRE)

6.5.1 Grundlagen zum Generic Routing Encapsulation Protokoll (GRE)

Das GRE-Protokoll tunnelt beliebige Layer-3-Datenpakete (u. a. IP, IPsec, ICMP etc.) über eine Point-to-Point-Netzwerkverbindung, indem es diese Daten mit einem IP-Daten-Gerüst umgibt. Das ist unter anderem dann hilfreich, wenn beide Kommunikationspartner ein bestimmtes Übertragungsprotokoll verwenden (z. B. IPsec), das auf dem Übertragungsweg nicht zur Verfügung steht. Da GRE selbst keine Verschlüsselung der getunnelten Daten durchführt, müssen beide Kommunikationspartner für die Absicherung dieser Daten sorgen.

6.5.1.1 Konfiguration eines GRE-Tunnels

Mit LANconfig erfolgt die Konfiguration eines GRE-Tunnels unter **Kommunikation** > **Gegenstellen** > **GRE-Tunnel** nach einem Klick auf **GRE-Tunnel**.



Gegenstelle

Name der Gegenstelle dieses GRE-Tunnels. Verwenden Sie diesen Namen z. B. in der Routing-Tabelle, um Daten durch diesen GRE-Tunnel zu versenden.

IP-Adresse

Adresse des GRE-Tunnel-Endpunktes (gültige IPv4- oder IPv6-Adresse oder FQDN).

Routing-Tag

Routing-Tag für die Verbindung zum GRE-Tunnel-Endpunkt. Anhand des Routing-Tags ordnet das Gerät Datenpakete diesem GRE-Tunnel zu.

Checksumme

Bestimmen Sie hier, ob der GRE-Header eine Checksumme enthalten soll.

Wenn Sie die Checksummenfunktion aktivieren, berechnet das Gerät für die zu übertragenden Daten eine Checksumme und fügt diese dem GRE-Tunnel-Header an. Enthält der GRE-Header der ankommenden Daten eine Checksumme, kontrolliert das Gerät diese mit den übertragenen Daten. Bei einer fehlerhaften oder fehlenden Checksumme verwirft das Gerät die empfangenen Daten.

Bei deaktivierter Checksummenfunktion versendet das Gerät alle Tunnel-Daten ohne Checksumme, und es erwartet Datenpakete ohne Checksumme. Ankommende Datenpakete mit einer Checksumme im GRE-Header verwirft das Gerät.

Schlüssel vorhanden

Bestimmen Sie hier, ob der GRE-Header einen Schlüssel zur Datenflusskontrolle enthalten soll.

Wenn Sie diese Funktion aktivieren, integriert das Gerät den im Feld **Schlüssel** angegebenen Wert in den GRE-Header dieses GRE-Tunnels. Das Gerät ordnet ankommende Datenpakete nur diesem GRE-Tunnel zu, wenn ihr GRE-Header einen identischen Schlüsselwert enthält.

Bei deaktivierter Funktion enthält der GRE-Header abgehender Datenpakete keinen Schlüssel-Wert. Das Gerät ordnet ankommende Datenpakete nur diesem GRE-Tunnel zu, wenn ihr GRE-Header ebenfalls keinen Schlüsselwert enthält.

Schlüssel

Der Schlüssel, der die Datenflusskontrolle in diesem GRE-Tunnel sicherstellt. Anhand dieses Schlüssels ordnen zwei über mehrere GRE-Tunnel verbundene Geräte die Datenpakete dem entsprechenden GRE-Tunnel zu.

Paketfolge

Bestimmen Sie hier, ob der GRE-Header der Datenpakete Informationen zur Reihenfolge der Pakete enthält.

Wenn Sie diese Funktion aktivieren, integriert das Gerät in den GRE-Header der abgehenden Datenpakete einen Zähler, um dem GRE-Tunnel-Endpunkt die Reihenfolge der Datenpakete vorzugeben. Das Gerät wertet die Paketfolge der ankommenden Datenpakete aus und verwirft Pakete mit falscher oder fehlender Paketfolge.

Absende-Adresse

Hier können Sie optional eine Absendeadresse konfigurieren, die das Gerät statt der ansonsten automatisch für die Zieladresse gewählten Absendeadresse verwendet. Mögliche Werte sind:

- Name der IP-Netzwerke, deren Adresse eingesetzt werden soll.
- "INT" für die Adresse des ersten Intranets
- "DMZ" für die Adresse der ersten DMZ
- LB0 bis LBF für die 16 Loopback-Adressen
- Beliebige gültige IP-Adresse



Wenn in der Liste der IP-Netzwerke oder in der Liste der Loopback-Adressen ein Eintrag mit dem Namen „DMZ“ vorhanden ist, verwendet das Gerät die zugehörige IP-Adresse.

IPv6

Dieser Eintrag gibt den Namen der IPv6-WAN-Schnittstelle an. Ein leerer Eintrag schaltet IPv6 für dieses Interface ab. Die IPv6-Gegenstellen konfigurieren Sie unter **IPv6** > **Allgemein** > **WAN-Schnittstellen**.

Falls die Angabe einer IP-Adresse für die Tunnel-Schnittstelle notwendig ist, gehen Sie wie folgt vor:

IPv4

Erstellen Sie unter **Kommunikation** > **Protokolle** > **IP-Parameter** einen neuen Eintrag und geben Sie für den Gegenstellennamen den Namen der GRE-Tunnel-Gegenstelle an. Vergeben Sie anschließend unter **IP-Adresse** und **Netzmaske** die notwendigen Werte.

IPv6

Erstellen Sie unter **IPv6** > **Allgemein** > **IPv6-Adressen** einen neuen Eintrag und geben Sie für den Interface-Namen den Namen der GRE-Tunnel-Gegenstelle an. Vergeben Sie anschließend unter **Adresse/Präfixlänge** die notwendigen Werte.

6.5.2 Ethernet-over-GRE (EoGRE)

Weitere Informationen zum GRE-Potokoll finden Sie unter *Grundlagen zum Generic Routing Encapsulation Protokoll (GRE)*.

Die aktuelle LCOS-Version stellt mehrere „Ethernet over GRE"-Tunnel (EoGRE) zur Verfügung, um Ethernet-Pakete per GRE zu übertragen. Da sich diese Ethernet-Pakete auf OSI-Layer-2 bewegen, bieten diese EoGRE-Tunnel lediglich eine Bridge-Funktionalität an.

Auf diese Weise lassen sich beispielsweise L2VPN (VPN als einfache Level-2-Brigde) oder eine transparente Ethernet-Bridge über WAN realisieren.

6.5.2.1 Konfiguration eines EoGRE-Tunnels

Mit LANconfig erfolgt die Konfiguration eines EoGRE-Tunnels unter **Kommunikation** > **Gegenstellen** > **GRE-Tunnel** nach einem Klick auf **EoGRE-Tunnel** und der Auswahl des entsprechenden Tunnels.



Schnittstelle

Name des gewählten EoGRE-Tunnels.

Aktiv

Aktiviert oder deaktiviert den EoGRE-Tunnel. Deaktivierte EoGRE-Tunnel senden oder empfangen keinen Daten.

Server-Adresse

Adresse des EoGRE-Tunnel-Endpunktes (gültige IPv4- oder IPv6-Adresse oder FQDN).

Routing-Tag

Routing-Tag für die Verbindung zum EoGRE-Tunnel-Endpunkt. Anhand des Routing-Tags ordnet das Gerät Datenpakete diesem EoGRE-Tunnel zu.

Checksumme

Bestimmen Sie hier, ob der GRE-Header eine Checksumme enthalten soll.

Wenn Sie die Checksummenfunktion aktivieren, berechnet das Gerät für die zu übertragenen Daten eine Checksumme und fügt diese dem GRE-Tunnel-Header an. Enthält der GRE-Header der ankommenden Daten eine Checksumme, kontrolliert das Gerät diese mit den übertragenen Daten. Bei einer fehlerhaften oder fehlenden Checksumme verwirft das Gerät die empfangenen Daten.

Bei deaktivierter Checksummenfunktion versendet das Gerät alle Tunnel-Daten ohne Checksumme, und es erwartet Datenpakete ohne Checksumme. Ankommende Datenpakete mit einer Checksumme im GRE-Header verwirft das Gerät.

Schlüssel vorhanden

Bestimmen Sie hier, ob der GRE-Header einen Schlüssel zur Datenflusskontrolle enthalten soll.

Wenn Sie diese Funktion aktivieren, integriert das Gerät den im Feld **Schlüssel** angegebenen Wert in den GRE-Header dieses EoGRE-Tunnels. Das Gerät ordnet ankommende Datenpakete nur diesem EoGRE-Tunnel zu, wenn ihr GRE-Header einen identischen Schlüsselwert enthält.

Bei deaktivierter Funktion enthält der GRE-Header abgehender Datenpakete keinen Schlüssel-Wert. Das Gerät ordnet ankommende Datenpakete nur diesem EoGRE-Tunnel zu, wenn ihr GRE-Header ebenfalls keinen Schlüsselwert enthält.

Schlüssel

Der Schlüssel, der die Datenflusskontrolle in diesem EoGRE-Tunnel sicherstellt. Anhand dieses Schlüssels ordnen zwei über mehrere EoGRE-Tunnel verbundene Geräte die Datenpakete dem entsprechenden EoGRE-Tunnel zu.

Paketfolge

Bestimmen Sie hier, ob der GRE-Header der Datenpakete Informationen zur Reihenfolge der Pakete enthält.

Wenn Sie diese Funktion aktivieren, integriert das Gerät in den GRE-Header der abgehenden Datenpakete einen Zähler, um dem EoGRE-Tunnel-Endpunkt die Reihenfolge der Datenpakete vorzugeben. Das Gerät wertet die Paketfolge der ankommenden Datenpakete aus und verwirft Pakete mit falscher oder fehlender Paketfolge.

6.5.2.2 Lokale Schnittstelle mit einem EoGRE-Tunnel verbinden

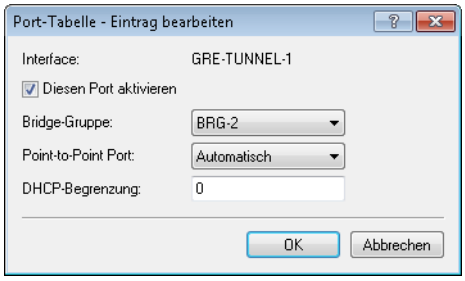
Um eine lokale Schnittstelle mit einem EoGRE-Tunnel zu verbinden, gehen Sie wie folgt vor:

1. Erstellen Sie unter **Kommunikation** > **Gegenstellen** > **GRE-Tunnel** > **EoGRE-Tunnel** einen neuen Eintrag.



Aktivieren Sie den Tunnel und geben Sie unter **Server-Adresse** die Adresse des entfernten Gerätes an, zu dem der EoGRE-Tunnel bestehen soll (IPv4- oder IPv6-Adresse oder FQDN).

2. Ergänzen Sie unter **Schnittstellen** > **LAN** > **Port-Tabelle** eine Bridge-Gruppe um den aktivierten EoGRE-Tunnel.



Aktivieren Sie den Port und wählen Sie die gewünschte Bridge-Gruppe aus.

3. Ergänzen Sie ebenfalls unter **Schnittstellen** > **LAN** > **Port-Tabelle** dieselbe Bridge-Gruppe um das lokale Interface, das Sie über den EoGRE-Tunnel verbinden möchten (z. B. WLAN-1).



Aktivieren Sie den Port und wählen Sie aus der Liste dieselbe Bridge-Gruppe aus, in der sich auch der EoGRE-Tunnel befindet.

6.6 IP-Masquerading

Eine der häufigsten Aufgaben für Router ist heute die Anbindung vieler Arbeitsplätze in einem LAN an das Netz der Netze, das Internet. Jeder soll nach Möglichkeit direkt von seinem Arbeitsplatz aus z. B. auf das Internet zugreifen und sich brandaktuelle Informationen für seine Arbeit holen können.

Damit nicht jeder Arbeitsplatzrechner mit seiner IP-Adresse im gesamten Internet bekannt sein muss, wird das „IP-Masquerading" als Versteck für alle Rechner im Intranet eingesetzt. Beim IP-Masquerading treffen zwei gegensätzliche Forderungen an den Router aufeinander: Zum einen soll er eine im lokalen Netz gültige Intranet-IP-Adresse haben, damit er aus dem LAN erreichbar ist, zum anderen soll er eine im Internet gültige, öffentliche IP-Adresse haben (fest vergeben oder vom Provider dynamisch zugewiesen).

Da diese beiden Adressen prinzipiell nicht in einem logischen Netz liegen dürfen, muss der Router über zwei IP-Adressen verfügen:

- die Intranet IP-Adresse zur Kommunikation mit den Rechnern im LAN
- die öffentliche IP-Adresse zur Kommunikation mit den Gegenstellen im Internet

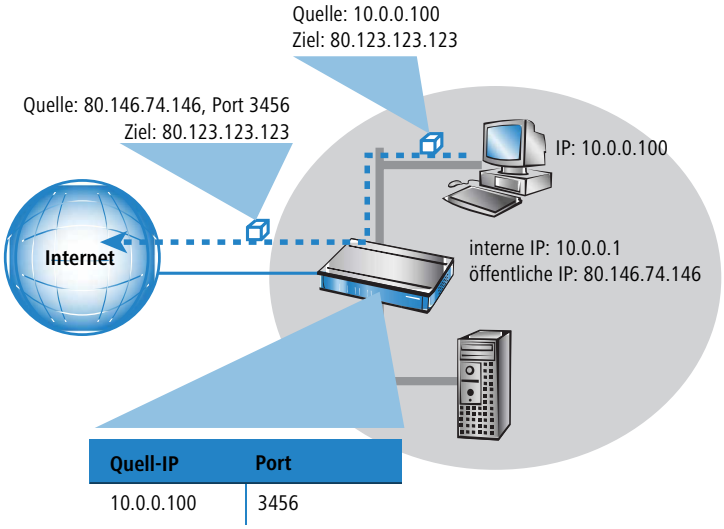
Die Rechner im LAN nutzen den Router dann als Gateway und können selbst nicht erkannt werden. Der Router trennt Internet und Intranet.

Neben den im folgenden aufgeführten Möglichkeiten „Einfaches Masquerading" und „Port Forwarding" unterstützt LCOS auch *WAN Policy-Based NAT* auf Seite 691, welches Masquerading über Firewall-Regeln ermöglicht.

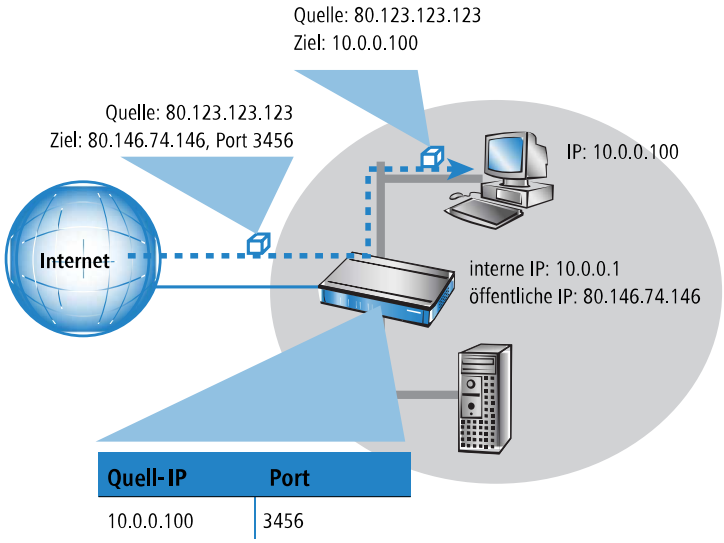
6.6.1 Einfaches Masquerading

6.6.1.1 Wie funktioniert IP-Masquerading?

Das Masquerading nutzt die Eigenschaft der Datenübertragung über TCP/IP aus, dass neben der Quell- und Ziel-Adresse auch Portnummer für Quelle und Ziel verwendet werden. Bekommt der Router nun ein Datenpaket zur Übertragung, merkt er sich die IP-Adresse und den Port des Absenders in einer internen Tabelle. Dann gibt er dem Paket seine eigene IP-Adresse und eine beliebige neue Portnummer. Diesen neuen Port trägt er ebenfalls in der Tabelle ein und leitet das Paket mit den neuen Angaben weiter.



Die Antwort auf dieses Paket geht nun an die IP-Adresse des Routers mit der neuen Absender-Portnummer. Mit dem Eintrag in der internen Tabelle kann der Router diese Antwort nun wieder dem ursprünglichen Absender zuordnen.



6.6.1.2 Welche Protokolle können mit IP-Masquerading übertragen werden?

Das IP-Masquerading funktioniert problemlos für all jene IP-Protokolle, die auf TCP, UDP oder ICMP basieren und dabei ausschließlich über Ports kommunizieren. Zu diesen unproblematischen Protokollen zählt beispielsweise das Basis-Protokoll des World Wide Web: HTTP.

Einzelne IP-Protokolle verwenden zwar TCP oder UDP, kommunizieren allerdings nicht ausschließlich über Ports. Derartige Protokolle verlangen beim IP-Masquerading eine entsprechende Sonderbehandlung. Zu den vom IP-Masquerading im Gerät unterstützten Protokollen mit Sonderbehandlung gehören:

- FTP (über die Standardports)
- PPTP
- IPSec
- IRC

6.6.1.3 Konfiguration des IP-Masquerading

Die Verwendung von IP-Masquerading wird für jede Route in der Routing-Tabelle einzeln festgelegt. Die Routing-Tabelle erreichen Sie wie folgt:

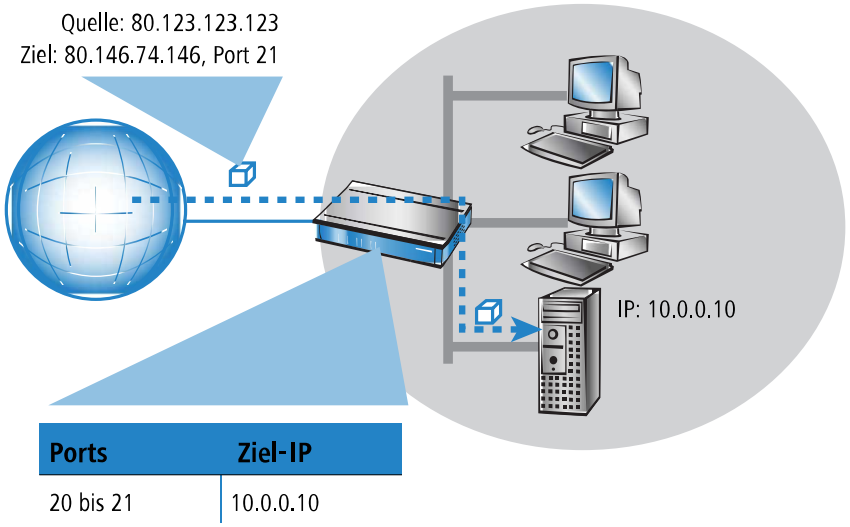
LANconfig: **IP-Router** > **Routing** > **Routing-Tabelle**

Konsole: **Setup** > **IP-Router** > **IP-Routing-Tab**

6.6.2 Port-Forwarding (Inverses Masquerading)

Beim einfachen Masquerading werden alle IP-Adressen im lokalen Netz hinter der IP-Adresse des Routers maskiert (versteckt). Soll nun ein bestimmter Rechner im LAN für Stationen aus dem Internet erreichbar sein (z. B. ein FTP-Server), dann ist bei Einsatz des einfachen Masquerading auch die IP-Adresse des FTP-Servers im Internet nicht bekannt. Ein Verbindungsaufbau zu diesem FTP-Server aus dem Internet ist also so nicht mehr möglich.

Um den Zugriff auf einen solchen Server („exposed host“) im LAN zu ermöglichen, wird in einer Tabelle (Port-Forwarding-Tabelle) die IP-Adresse des FTP-Servers eingetragen mit allen Diensten (Ports), die er auch außerhalb des LANs anbieten soll. Schickt nun ein Rechner aus dem Internet ein Paket an den FTP-Server im LAN, so sieht es für diesen Rechner so aus, als wäre der Router der FTP-Server. Der Router liest anhand des verwendeten Protokolls aus dem Eintrag in der Port-Forwarding-Tabelle die IP-Adresse des FTP-Servers im LAN und leitet das Paket an die dort eingetragene lokale IP-Adresse weiter. Alle Pakete, die vom FTP-Server im LAN kommen (Antworten des Servers), werden wieder hinter der IP-Adresse des Routers versteckt.



Der generelle Unterschied zwischen einfachem und inversem Masquerading:

- Der Zugriff von außen auf einen Dienst (Port) im Intranet muss beim inversen Masquerading manuell durch Angabe einer Port-Nummer definiert werden. In der Port-Forwarding-Tabelle wird dazu der Ziel-Port mit der Intranet-Adresse z. B. des FTP-Servers angegeben.
- Beim Zugriff aus dem LAN auf das Internet hingegen wird der Eintrag in der Tabelle mit Port- und IP-Adress-Informationen automatisch durch den Router selbst vorgenommen.

Die entsprechende Tabelle kann max. 2048 Einträge aufnehmen, also gleichzeitig 2048 Übertragungen zwischen dem maskierten und dem unmaskierten Netz ermöglichen.

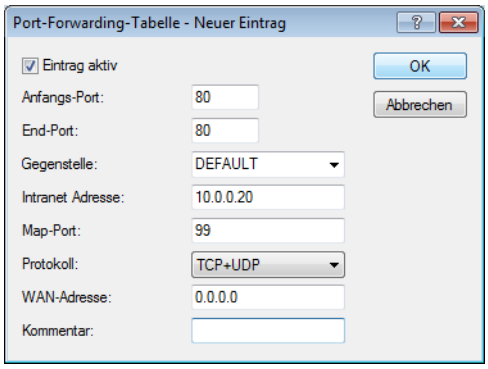
Nach einer einstellbaren Zeit geht der Router jedoch davon aus, dass der Eintrag nicht mehr benötigt wird, und löscht ihn selbständig wieder aus der Tabelle.

Stateful-Inspection und inverses Masquerading: Wenn im Masquerading-Modul ein Port freigeschaltet wird (d. h. alle auf diesem Port empfangenen Pakete sollen an einen Rechner im lokalen Netz weitergeleitet werden),

so erfordert dies bei einer Deny-All Firewall-Strategie einen **zusätzlichen** Eintrag in der Stateful-Inspection Firewall, der den Zugriff aller Rechner auf den jeweiligen Server ermöglicht.

Manchmal ist es allerdings gewünscht, dass der so eingerichtete „exposed host" nicht mit dem standardmäßig verwendeten Port angesprochen wird, sondern aus Sicherheitsgründen ein anderer Port verwendet wird. In diesem Fall wird also nicht nur das Umsetzen von Ports auf eine IP-Adresse benötigt, sondern auch das Umsetzen auf andere Ports (Port-Mapping). Ein weiteres Anwendungsbeispiel für diese Port-Umsetzung ist das Umsetzen von mehreren Ports aus dem WAN auf einen gemeinsamen Port im LAN, die jedoch verschiedenen IP-Adressen zugeordnet werden (N-IP-Mapping).

Bei der Konfiguration des Port-Mappings wird einem Port oder Portbereich (Anfangs-Port bis End-Port) eine IP-Adresse aus dem LAN als Ziel und der im LAN zu verwendende Port (Map-Port) zugewiesen.



LANconfig: **IP-Router** > **Maskierung** > **Port-Forwarding-Tabelle**

Konsole: **Setup** > **IP-Router** > **1-N-NAT** > **Service-Tabelle**

Anfangs-Port

Anfangs-Port für den Dienst.

End-Port

End-Port für den Dienst.

Gegenstelle

Gegenstelle, für die dieser Eintrag gültig ist. Die Verwendung von virtuellen Routern (*Advanced Routing and Forwarding (ARF)* auf Seite 393) erfordert beim Port-Forwarding eine gezielte Auswahl der Gegenstelle. Wird keine Gegenstelle angegeben, gilt der Eintrag für alle Gegenstellen.

Intranet-Adresse

Intranet-Adresse, an die ein im Portbereich liegendes Paket weitergeleitet wird.

Map-Port

Port, mit dem das Paket weitergeleitet wird.

Wird als Map-Port die „0" eingetragen, werden im LAN die gleichen Ports verwendet wie im WAN. Wird ein Portbereich umgesetzt, gibt der Map-Port den ersten verwendeten Port im LAN an. Beim Umsetzen des Portbereichs '1200' bis '1205' auf den internen Map-Port '1000' werden also die Ports von 1000 bis einschließlich 1005 für den Datenverkehr im LAN verwendet.

Das Port-Mapping ist statisch, deshalb können zwei Ports oder Portbereiche nicht auf den gleichen Map-Port eines Ziel-Rechners im LAN umgesetzt werden. Für verschiedene Zielrechner können gleiche Port-Mappings verwendet werden.

Protokoll

Protokoll, für das dieser Eintrag gültig ist.

WAN-Adresse

WAN-Adresse, für die dieser Eintrag gültig ist. Wenn das Gerät über mehr als eine statische IP-Adresse verfügt, kann das Port-Forwarding so auf bestimmte Verbindungen eingeschränkt werden.

Eintrag aktiv

Schaltet den Eintrag ein oder aus.

Kommentar

Kommentar zum definierten Eintrag (64 Zeichen).

6.7 Demilitarisierte Zone (DMZ)

Eine demilitarisierte Zone (DMZ) bietet die Möglichkeit, bestimmte Rechner in einem Netzwerk aus dem Internet erreichbar zu machen. Mit diesen Rechnern in der DMZ werden üblicherweise Internetdienste wie E-Mail o. ä. angeboten. Der Rest des Netzwerks soll natürlich weiterhin für Angreifer aus dem Internet unerreichbar bleiben.

Um diesen Aufbau zu ermöglichen, muss der Datenverkehr zwischen den drei Zonen Internet, DMZ und LAN von einer Firewall geprüft werden. Diese Aufgaben der Firewall können durchaus in einem Gerät (Router) zusammengefasst werden. Dazu braucht der Router drei Interfaces, die getrennt voneinander durch die Firewall überwacht werden können:

- LAN-Interface
- WAN-Interface
- DMZ-Interface

In der Tabelle ist aufgelistet, welche Geräte diese Funktion unterstützen.

6.7.1 Zuordnung der Netzwerkzonen zur DMZ

Die Zuordnung der verschiedenen Netzwerk-Zonen (Adresskreise) zur DMZ, zum LAN und zum ARF wird bei den Adresseinstellungen vorgenommen. Dabei können je nach Verfügbarkeit auch WLAN-Interfaces ausgewählt werden.



LANconfig: **IPv4** > **Allgemein** > **IP-Netzwerke**

Konsole: **Setup** > **TCP-IP**

6.7.2 Adressprüfung bei DMZ- und Intranet-Interfaces

Zur besseren Abschirmung der DMZ (demilitarisierten Zone) und des Intranets gegen unerlaubte Zugriffe kann für die jeweiligen Interfaces eine zusätzliche Adressprüfung über das Intrusion Detection System (IDS) der Firewall aktiviert werden.

Die entsprechenden Schalter heißen **DMZ-Check** bzw. **Intranet-Check** und können die Werte 'loose' bzw. 'strict' annehmen:

- Wenn der Schalter auf 'loose' steht, dann wird jede Quelladresse akzeptiert, wenn das Gerät selbst angesprochen wird.
- Steht der Schalter jedoch auf 'strict', dann muss explizit eine Rückroute vorhanden sein, damit kein IDS-Alarm ausgelöst wird. Das ist also üblicherweise dann der Fall, wenn das Datenpaket eine Absenderadresse enthält, in die das entsprechende Interface auch selbst Daten routen kann. Absenderadressen aus anderen Netzen, in die das Interface nicht routen kann, oder Absenderadressen aus dem eigenen Adresskreis führen daher zu einem IDS-Alarm.

Der Default ist bei allen Geräten 'loose'.

Den Schalter zur Aktivierung von der DMZ- und Intranet-Adressprüfung finden Sie in LANconfig:



LANconfig: **IPv4** > **Allgemein** > **IP-Netzwerke**

Konsole: **Setup** > **TCP-IP**

6.7.3 Unmaskierter Internet-Zugang für Server in der DMZ

Das im vorangegangenen Abschnitt beschriebene inverse Maskieren erlaubt zwar, jeweils einen bestimmten Dienst zu exponieren (z. B. je ein Web-, Mail- und FTP-Server), hat aber z. T. weitere Einschränkungen:

- Der betreffende Dienst des 'exposed host' muss vom Maskierungsmodul unterstützt und verstanden werden. Zum Beispiel benutzen einige VoIP-Server nicht-standardisierte, proprietäre Ports für eine erweiterte Signalisierung. Dadurch können solche Server-Dienste nur an Verbindungen ohne Maskierung betrieben werden.
- Vom Sicherheitsstandpunkt muss beachtet werden, dass sich der 'exposed host' im lokalen Netz befindet. Falls der Rechner unter die Kontrolle eines Angreifers gebracht wird, so kann dieser Rechner als Ausgangsbasis für Angriffe gegen weitere Maschinen im lokalen Netz missbraucht werden.

6.7.3.1 Zwei lokale Netze – Betrieb von Servern in der DMZ

Hierfür ist ein Internetzugang mit mehreren statischen IP-Adressen notwendig. Bitte kontaktieren Sie Ihren ISP ggf. für ein entsprechendes Angebot.

Ein Beispiel: Sie erhalten die Internet IP-Netzadresse 123.45.67.0 mit der Netzmaske 255.255.255.248 vom Provider zugewiesen. Dann könnten Sie die IP-Adressen wie folgt verteilen:

öffentliche DMZ IP-Adresse	Bedeutung/Verwendung
123.45.67.0	Netzadresse
123.45.67.1	Intranet-Gateway
123.45.67.2	Beliebiges Gerät im lokalen Netzwerk, das unmaskierten Zugang ins Internet erhalten soll, beispielsweise ein Web-Server am DMZ-Port

öffentliche DMZ IP-Adresse	Bedeutung/Verwendung
123.45.67.7	Broadcast-Adresse

Alle Rechner und Geräte im Intranet haben keine öffentliche IP-Adresse und treten daher mit der IP-Adresse des Geräts (123.45.67.1) im Internet auf.

6.7.3.2 Trennung von Intranet und DMZ

Obwohl Intranet und DMZ vielleicht bereits schon auf Ethernet-Ebene durch dedizierte Interfaces voneinander getrennt sind, so muss in jedem Fall noch eine Firewall-Regel zur Trennung auf IP-Ebene eingerichtet werden!

Dabei soll der Server-Dienst vom Internet und aus dem Intranet heraus erreichbar sein, aber jeglicher IP-Traffic aus der DMZ Richtung Intranet soll unterbunden werden. Für das obige Beispiel ergäbe sich folgendes:

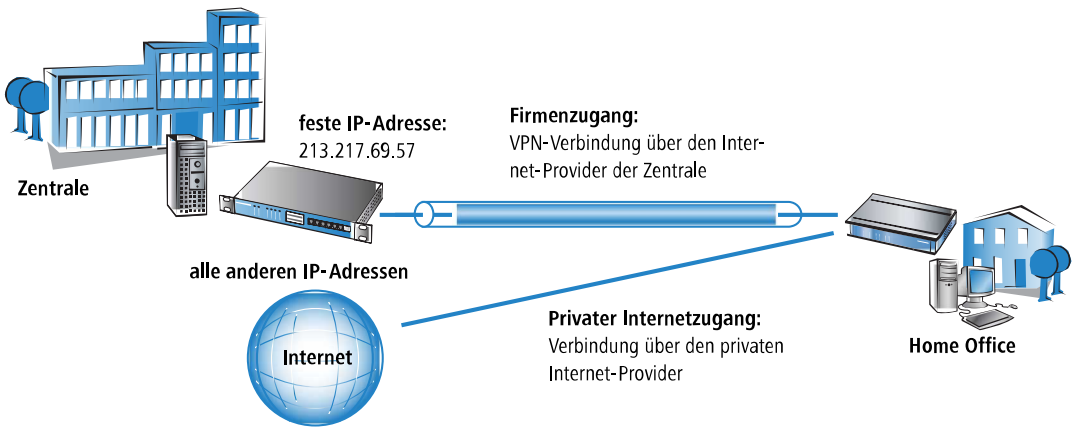
- Bei einer "Allow-All"-Strategie (default): Zugriff von "123.45.67.2" auf "Alle Stationen im lokalen Netz" verbieten
- Bei einer "Deny-All"-Strategie: Zugriff von "Alle Stationen im lokalen Netz" auf "123.45.67.2" erlauben

6.8 Multi-PPPoE

In den meisten Fällen wird auf einem DSL- oder ADSL-WAN-Interface immer nur eine Verbindung zu einer Zeit aufgebaut sein. Es gibt aber durchaus sinnvolle Anwendungen, in denen mehrere parallele Verbindungen auf dem WAN-Interface benötigt werden. Geräte mit DSL- oder ADSL-Interface können bis zu acht verschiedene Kanäle ins WAN parallel auf dem gleichen physikalischen Interface aufbauen.

6.8.1 Anwendungsbeispiel: Home-Office mit privatem Internetzugang

Eine mögliche Anwendung ist z. B. das Home-Office eines Außendienst-Mitarbeiters, der über eine VPN-Verbindung einen Zugang zum Netzwerk der Zentrale erhalten soll. Das Unternehmen zahlt dabei die Kosten für die VPN-Verbindung, der Mitarbeiter im Home-Office zahlt seinen privaten Internet-Datenverkehr selbst.



Um die beiden Datenverbindungen exakt trennen zu können, werden zwei Internetverbindungen für die jeweiligen Provider eingerichtet. Die Default-Route wird in der IP-Routing-Tabelle dann dem privaten Provider zugeordnet, das Netzwerk der Zentrale über die VPN-Verbindung wird über den Provider der Zentrale geroutet.

6.8.2 Konfiguration

Zur Konfiguration eines solchen Szenarios sind im Home-Office-Router die folgenden Schritte notwendig:

- Konfiguration des privaten Internetzugangs, z. B. über den Assistenten von LANconfig oder WEBconfig
- Konfiguration des Internetzugangs, der über die Zentrale abgerechnet wird
- Auswahl des privaten Providers für die Default-Route in der IP-Routing-Tabelle (z. B. manuell in LANconfig oder mit dem Assistenten zur Auswahl des Internetproviders unter WEBconfig)
- Konfiguration der VPN-Verbindung zum Netzwerk der Zentrale
- Zuweisung der VPN-Verbindung zum Provider der Zentrale:

  Damit der Datenverkehr zur Zentrale über den richtigen Internetprovider geroutet wird, muss in der IP-Routing-Tabelle noch ein neuer Eintrag angelegt werden. Darin wird das VPN-Gateway der Zentrale mit seiner festen IP-Adresse und der passenden Netzmaske eingetragen und auf die Gegenstelle für den Internetprovider der Zentrale geleitet.

  Wichtig ist, dass die Route zum Internetprovider der Zentrale maskiert wird, denn sonst würde das Gerät nicht die WAN-Adresse, sondern seine LAN-Adresse in die VPN-Pakete einsetzen und die Verbindung käme niemals zustande.

Weitere Informationen zu diesen Konfigurationsschritten finden Sie an den entsprechenden Stellen in der Dokumentation zum Ihrem Gerät.

Administrator-Rechte des Mitarbeiters im Home-Office: Damit der Mitarbeiter im Home-Office nicht versehentlich die Einstellungen für die Internet-Provider oder den VPN-Zugang verändert, sollten Sie ihm je nach Vereinbarung nur die WEBconfig-Funktionsrechte für die Assistenten „Internet-Zugang“ und „Auswahl von Internet-Providern“ zuweisen.

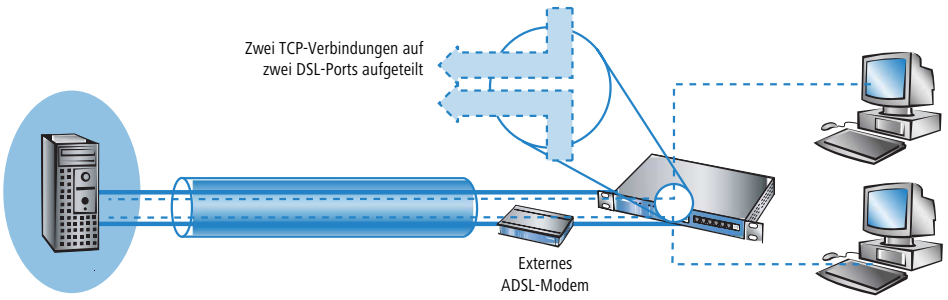
Sorgen Sie mit den entsprechenden Filterregeln im Bereich 'Firewall/QoS' dafür, dass der Internetverkehr nicht versehentlich über das Netzwerk der Zentrale läuft.

6.9 Load-Balancing

Trotz immer weiter steigender Bandbreite auf DSL-Zugängen stellen diese immer noch das Nadelöhr in der Kommunikation dar. In manchen Fällen ist es durchaus sinnvoll, mehrere DSL-Zugänge zu bündeln.

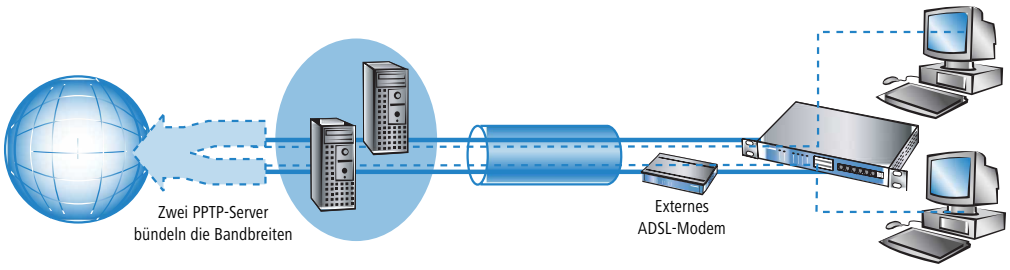
- Load-Balancing

  Beim Load-Balancing werden TCP-Verbindungen dynamisch auf voneinander unabhängigen DSL-Verbindungen verteilt. Dem Anwender steht damit zwar auch die Summen-Bandbreite der gebündelten Kanäle zur Verfügung, dennoch ist jede einzelne TCP-Verbindung auf die Bandbreite des zugewiesenen DSL-Anschlusses beschränkt.



- Indirekte Bündelung für LAN-LAN-Kopplungen

  Bei der indirekten Bündelung wird auf zwei oder mehr voneinander unabhängigen DSL-Verbindungen je eine PPTP-Verbindung aufgebaut. Diese PPTP-Verbindungen werden dann gebündelt. Damit ist dann zumindest für LAN-LAN-Kopplungen durch das Internet hindurch eine echte Kanalbündelung möglich, auch wenn der Internetprovider selbst keine Kanalbündelung anbietet.



6.9.1 DSL-Port-Mapping

Grundvoraussetzung für eine DSL-Kanalbündelung ist die Unterstützung von mehr als einem DSL-Interface pro Gerät. Dazu werden an den Switch eines Routers ein oder mehrere externe DSL-Modems angeschlossen.

Bitte informieren Sie sich in der Hardware-Schnellübersicht Ihres Gerätes, ob dieses den Anschluss externer DSL-Modems unterstützt.

6.9.1.1 Zuordnung der Switch-Ports zu den DSL-Ports

Bei Geräten mit integriertem Switch können je nach Modell einige der LAN-Ports als zusätzlicher WAN-Port zum Anschluss externer DSL-Modems dienen. Diese Ports werden in der Interface-Tabelle als getrennte DSL-Interfaces aufgeführt (DSL-1, DSL-2 usw.). Die DSL-Ports werden in der Liste der WAN-Interfaces als DSL-Interface aktiviert, mit den korrekten Up- und Downstreamraten konfiguriert und in der Liste der LAN-Interfaces den Switch-Ports zugeordnet.

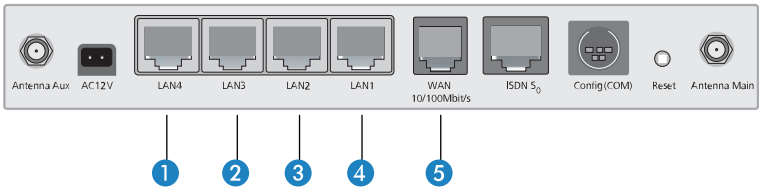
Beispiel LANCOM Wireless 1811 DSL:

Port	Zuordnung	Anschluss	MDI-Modus	Privat-Modus
LAN-1	LAN-1	Auto	Auto	Nein
LAN-2	LAN-1	Auto	Auto	Nein
LAN-3	LAN-1	Auto	Auto	Nein
LAN-4	LAN-1	Auto	Auto	Nein
WAN	DSL-1	Auto	Auto	Nein

- In der Spalte 'Port' steht die Bezeichnung, die die jeweiligen Ports auf der Rückblende des Geräts haben.
- In der Spalte 'Zuordnung' wird die Verwendung des Ports angegeben:
  - keine: Der Port ist deaktiviert
  - LAN-1: Der Port ist dem LAN zugeordnet
  - DSL-1, DSL-2, ... : Der Port ist einem der DSL-Interfaces zugeordnet
  - Monitor: Der Port ist ein Monitor-Port, d. h. es wird alles, was auf den anderen Ports empfangen wird, auf diesem Port wieder ausgegeben. Damit kann an diesem Port z. B. ein Paket-Sniffer (wie Ethereal) angeschlossen werden.

Die Zuordnung der DSL-Ports zu den Ethernetports ist dabei beliebig wählbar. Eine sinnvolle und übersichtliche Zuordnung ergibt sich, wenn Sie die DSL-Ports in umgekehrter Reihenfolge den Ports am Switch zuordnen.

Beispiel LANCOM Wireless 1811 DSL:



1. LAN4 / DSL-2
2. LAN3 / DSL-3
3. LAN2 / DSL-4
4. LAN1 / LAN-1: Dieser Port bleibt für das LAN reserviert
5. WAN / DSL-1: (dedizierter WAN-Port des Geräts)

In der Liste der DSL-Breitband-Gegenstellen wird der zu verwendende DSL-Port angegeben, wenn das Gerät über mehr als einen DSL-Port verfügt:

- Wird kein Port (oder der Port „0“) angegeben, so wählt das Gerät den Port nach dem für die Verbindung gewählten Kommunikations-Layer aus.
  - Wenn auf Layer-1 'ETH' eingestellt ist, wird der erste DSL-Port (also DSL-1) ausgewählt.
- Wird ein bestimmter Port (ungleich „0“) angegeben, so wird dieser für die Verbindung verwendet.

  Beachten Sie, dass der für die Verbindung über diesen Port eingestellte Kommunikations-Layer im Layer 1 auf 'ETH' eingestellt ist.
- Um eine Kanalbündelung über mehrere DSL-Interfaces zu ermöglichen, werden für die Gegenstelle in der Gegenstellenliste die entsprechenden Ports eingetragen (als kommaseparierte Port-Liste '1,2,3' oder als Port-Bereich '1-3'). Bei einer Port-Liste werden die Bündelkanäle genau in der angegebenen Reihenfolge aufgebaut, nur im Fehlerfall werden die Kanäle nach aufsteigender Reihenfolge versucht. Bei einem Port-Bereich werden die Kanäle immer in aufsteigender Reihenfolge aufgebaut.
  - Die Ports müssen in der Liste der Ethernet-Ports als DSL-Port geschaltet sein.
  - Die DSL-Ports müssen in der Liste der WAN-Interfaces als DSL-Interface aktiviert und mit den korrekten Up- sowie Downstreamraten konfiguriert sein.
  - In dem für die Verbindung verwendeten Layer muss die Bündelung aktiviert sein, die auch von der Gegenstelle unterstützt werden muss.
  - Um eine Kanalbündelung mit einem internen ADSL-Interface zu konfigurieren, wird der ADSL-Port '0' **an erster Stelle** in die Liste der Ports aufgenommen (z. B. '0,1,3' als Port-Liste oder '0-3' als Port-Bereich). Für die Gegenstelle muss im verwendeten Kommunikations-Layer auf Layer 1 'AAL-5' eingestellt werden.

    Ein Eintrag in der Gegenstellenliste kann verschiedene Ports (z. B. ADSL und Ethernet) enthalten, kann aber nur **einen** Kommunikations-Layer referenzieren, in dem nur **ein** Layer-1-Protokoll angegeben werden kann. Für die gebündelte Kommunikation über ADSL- und Ethernet-Ports sind jedoch **zwei** verschiedene Layer-1-Protokolle notwendig. Aus diesem Grund wird der Layer 1 in diesen Fällen auf 'AAL-5' für ADSL eingestellt. Da nur ein ADSL-Interface in den Geräten vorhanden sein kann, wird für alle zugebündelten Interfaces automatisch auf den Layer 1 mit 'ETH' für Ethernet-DSL-Ports umgestellt. Diese automatische Layerumstellung gelingt jedoch nur, wenn das ADSL-Interface als erstes für die Bündel-Verbindungen gewählt wird.
  - Bei Geräten mit einem eingebauten DSL-Modem und einem zusätzlichen Ethernet-Interface (DSL oder DSLoL) ist klar, welche Ports bei einer Bündelung verwendet werden. In diesem Fall ist daher die Angabe der Ports in der Gegenstellenliste nicht erforderlich. Bei diesen Geräten wird immer intern eine Port-Liste '0,1' angenommen, damit das interne DSL-Interface als erstes für die Bündelung verwendet wird.

Bei Multi-PPPoE (*Multi-PPPoE* auf Seite 425) teilen sich mehrere PPPoE-Verbindungen eine physikalische DSL-Leitung. Bei Multi-DSL werden mehrere PPPoE-Verbindungen auf die vorhandenen DSL-Interfaces verteilt. Die Anzahl der parallel möglichen Verbindungen ist auf maximal 8 Kanäle begrenzt.

6.9.1.2 Zuordnung der MAC-Adresse zu den DSL-Ports

Wenn ein Gerät durch die Verwendung der Switch-Ports über mehrere DSL(WAN)-Interfaces verfügt, müssen auch entsprechend viele MAC-Adressen zur Unterscheidung der DSL-Ports genutzt werden. Da die zu verwendende MAC-Adresse in manchen Fällen von der Gegenstelle abhängt, die aufgrund der MAC-Adresse die z. B. die Abrechnung eines DSL-Zugangs durchführt, werden die MAC-Adressen für die logischen DSL-Gegenstellen und nicht für die physikalischen DSL-Ports definiert.

Für die Einstellung der MAC-Adresse stehen folgende Optionen zur Verfügung:

- Global: Globale System-MAC-Adresse
- Lokal: aus der globalen Adresse wird eine eindeutige, lokal administrierte MAC-Adresse berechnet
- Benutzerdefiniert: Eine vom Benutzer frei wählbare MAC-Adresse

Jede aufgebaute DSL-Verbindung erhält eine eigene MAC-Adresse. Sollten für zwei Gegenstellen die gleichen MAC-Adressen konfiguriert sein, so wird für die erste aufzubauende Verbindung die konfigurierte MAC-Adresse verwendet. Für die zweite Verbindung wird hingegen aus der konfigurierten MAC-Adresse eine „lokal administrierte MAC-Adresse" errechnet, die somit wieder eindeutig ist. Ebenso wird bei einer Kanalbündelung für die erste Verbindung die konfigurierte MAC-Adresse verwendet für die weiteren Bündelverbindungen eine „lokal administrierte" MAC-Adresse auf Grundlage der konfigurierten MAC-Adresse berechnet. Sollte eine Ihrer Verbindungen über die MAC-Adresse abgerechnet werden, konfigurieren Sie diese MAC-Adresse nur auf der separat abgerechneten Verbindung. Verwenden Sie für alle übrigen Verbindungen eine andere Adresse.

6.9.2 Dynamisches Load-Balancing

Wenn der Internet-Provider eine direkte Bündelung nicht unterstützt, werden mehrere normale DSL-Zugänge über einen Load-Balancer gekoppelt. Hierzu werden zuerst die DSL-Zugänge für die benötigten DSL-Ports eingerichtet. Danach werden diese über eine Load-Balancing-Tabelle miteinander gekoppelt. Diese Liste ordnet einer virtuellen Balancing-Verbindung (das ist die Verbindung, die in der Routing-Tabelle eingetragen wird) die weiteren realen DSL-Verbindungen (Bündel-Verbindungen) zu. Einer Balancing-Verbindung können dabei je nach Anzahl der verfügbaren DSL-Ports mehrere Bündel-Verbindungen zugeordnet werden.

Die Balancing-Verbindung wird als „virtuelle" Verbindung angelegt. Für diese Verbindung werden also keine Zugangsdaten etc. eingetragen. Dieser Eintrag dient nur als „Verteiler", um einem Eintrag in der Routing-Tabelle mit Hilfe der Load-Balancing-Tabelle mehrere „reale" Bündel-Verbindungen zuweisen zu können.

Bei der DSL-Bündelung handelt es sich um eine statische Bündelung. Die evtl. zusätzlichen Kanäle werden also **nicht** nur nach Bedarf des übertragenen Datenvolumens auf- und wieder abgebaut.

Die Entscheidung über das Routing der Datenpakete kann beim Load-Balancing nicht mehr allein anhand der IP-Adressen getroffen werden, da die einzelnen gebündelten DSL-Verbindungen unterschiedliche IP-Adressen haben. Beim Load-Balancing werden daher zusätzlich die Informationen aus der Verbindungsliste der Firewall berücksichtigt. In dieser Liste wird für jede TCP-Verbindung ein Eintrag angelegt, der für das Load-Balancing zusätzlich die Information über den verwendeten DSL-Port bereitstellt.

6.9.2.1 Verbindungsaufbau

Bei der Anforderung für eine Datenübertragung zu einer Balancing-Gegenstelle wird zunächst die **erste** Bündel-Verbindung aus der Load-Balancing-Tabelle aufgebaut. Der weitere Verlauf hängt vom Erfolg der Verbindungsaufbaus ab:

- Wird die Verbindung erfolgreich aufgebaut, werden zunächst alle anstehenden TCP-Verbindungen diesem Kanal zugewiesen. Anschließend werden sukzessive alle konfigurierten Bündel-Verbindungen aufgebaut. Sobald mindestens zwei Bündel-Verbindungen aktiv sind, werden neue TCP-Verbindungen unter den aktiven Bündel-Verbindungen verteilt.
- Scheitert jedoch der Aufbau der ersten Bündel-Verbindung, so wird nacheinander der Aufbau der weiteren Bündel-Verbindungen versucht. Sobald eine der Bündel-Verbindungen aufgebaut werden konnte, werden alle zu diesem Zeitpunkt anstehenden TCP-Verbindungen auf diesen Kanal umgeleitet.

6.9.2.2 Verteilung der Datenlast

Für die Verteilung der Datenlast auf die verfügbaren Kanäle stehen prinzipiell zwei Varianten zur Auswahl:

- Wenn die Bandbreite des jeweiligen Kanals bekannt ist, dann werden die Verbindungen dem Kanal zugewiesen, der die geringste (prozentuale) Auslastung hat.
- Wenn die Bandbreite unbekannt ist, dann wird unterschieden, ob es sich bei der Verbindung um eine TCP-Verbindung handelt oder ob das Gerät eine VPN- oder PPTP-Verbindung aufbauen will.
  - Wenn eine TCP-Verbindung einen Kanal anfordert, dann wird derjenige mit der geringsten absoluten Last ausgewählt.
  - Wenn eine VPN- oder PPTP-Verbindung einen Kanal anfordert, dann werden die PPTP- und VPN-Verbindung gleichmäßig auf die verfügbaren Kanäle verteilt.

Für die sinnvolle Nutzung des Load-Balancing ist daher die Angabe der Bandbreite in der der Liste der WAN-Interfaces unter LANconfig im Konfigurationsbereich **Schnittstellen** > **WAN** unter der Schaltfläche **Interface-Einstellungen** erforderlich (Konsole: **Setup** > **Schnittstellen** > **DSL**).

6.9.2.3 Client-Binding

Der Einsatz von Load-Balancing führt bei Servern zu Problemen, die zur Identifizierung eines angemeldeten Benutzers dessen IP-Adresse verwenden. Wählt der Load-Balancer z. B. beim Aufruf einer neuen Webseite eine andere Internetverbindung als die, über die sich der Benutzer am Server angemeldet hat, wertet der Server das als Verbindungsversuch eines nicht angemeldeten Benutzers. Der Benutzer bekommt bestenfalls erneut einen Anmeldedialog zu sehen, nicht aber die gewünschte Webseite.

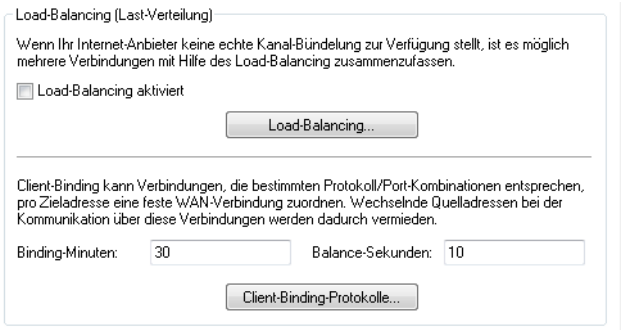
Eine Möglichkeit zur Abhilfe ist, in den Firewall-Regeln den Datenverkehr mit diesem Server auf eine bestimmte Internetverbindung festzulegen (Policy Based Routing). Damit ist jedoch der gesamte Datenverkehr zu diesem Server auf die Bandbreite dieser einen Verbindung beschränkt. Außerdem lassen sich so keine Backup-Verbindung aufbauen, falls die erste Verbindung gestört ist.

Das Client-Binding überwacht im Gegensatz dazu nicht die jeweiligen einzelnen TCP/IP-Sessions, sondern orientiert sich am Client, mit dem bei der ersten Session eine Internetverbindung zustande kommt. Es leitet alle nachfolgenden Sessions ebenfalls über diese Internetverbindung, was im Prinzip dem zuvor angesprochenen Policy Based Routing entspricht. Das erfolgt protokollabhängig, d. h., es überträgt nur Daten des selben Protokolltyps (z. B. HTTPS) über diese Internetverbindung. Lädt der Client sich zusätzlich Daten über eine HTTP-Verbindung, erfolgt das wahrscheinlich über eine andere Verbindung.

Um zu vermeiden, dass nun auch Daten über diese Internetverbindung fließen, die problemlos über parallele Verbindung zu übertragen wären, sorgt ein entsprechender Timer dafür, dass der Load-Balancer für eine definierte Dauer zusätzliche Sessions auf die zur Verfügung stehenden Internetverbindungen verteilt. Erst nach Ablauf des Timers zwingt das Client-Binding eine neue Session wieder auf die ursprüngliche Internetverbindung und startet den Timer neu. Der Server erkennt somit weiterhin den Anmeldestatus des Benutzers anhand seiner aktuellen IP-Adresse.

6.9.2.4 Load-Balancing mit Client-Binding

In LANconfig konfigurieren Sie das Client-Binding unter **IP-Router** > **Routing** im Abschnitt **Load-Balancing (Lastverteilung)**.



Binding-Minuten

Definieren Sie hier die Zeit in Minuten, für die die Binding-Einträge für einen Client gültig sein sollen.

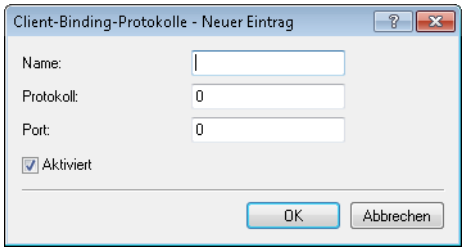
Balance-Sekunden

Um zu vermeiden, dass Daten über die Internetverbindung der Haupt-Session fließen, die problemlos über parallele Verbindung zu übertragen wären, sorgt ein entsprechender Timer dafür, dass der Load-Balancer für eine definierte Dauer zusätzliche Sessions auf die zur Verfügung stehenden Internetverbindungen verteilt. Erst nach Ablauf des Timers zwingt das Client-Binding eine neue Session wieder auf die ursprüngliche Internetverbindung und startet den Timer neu. Der Server erkennt somit weiterhin den Anmeldestatus des Benutzers anhand seiner aktuellen IP-Adresse.

Definieren Sie hier die Zeit in Sekunden, innerhalb der der Load-Balancer neue Sessions nach dem Start der Haupt-Session frei auf andere Internetverbindungen verteilt.

Das Client-Binding erfolgt protokollorientiert. Die entsprechenden Protokolle bestimmen Sie unter **Client-Binding-Protokolle**. Die Tabelle enthält bereits die Standard-Einträge

- HTTPS
- HTTP
- ANY



Name

Enthält eine aussagekräftige Bezeichnung dieses Eintrages.

Protokoll

Enthält die IP-Protokollnummer.

Mehr Informationen über IP-Protokollnummern finden Sie in der *Online-Datenbank* der IANA.

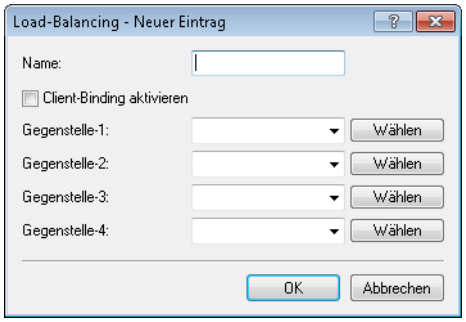
Port

Enthält den Port des IP-Protokolls.

Aktiviert

Aktiviert oder deaktiviert diesen Eintrag.

Das Client-Binding lässt sich unter **Load-Balancing** für den jeweiligen Eintrag aktivieren oder deaktivieren.



6.9.2.5 Load-Balancer aus RADIUS-Konfiguration

Ab LCOS 10.40 unterstützt Ihr Gerät neben der bereits vorhandenen Möglichkeit, einen Load-Balancer über die Konfigurationstabelle des Load-Balancers (siehe *Dynamisches Load-Balancing mit mehreren DSL-Zugängen* auf Seite 438) zu konfigurieren, auch die Möglichkeit, einen Load-Balancer aus übermittelten RADIUS-Attributen für IKEv2 VPN-Tunnel zu erzeugen.

In großen VPN-Szenarien werden zentralseitige Konfigurationen nicht durch Konfigurationseinträge aller notwendigen Parameter eines VPN-Tunnels im Gerät selbst abgelegt, sondern auf einen oder mehrere zentrale RADIUS-Server ausgelagert. Dies dient der besseren Skalierbarkeit und Administration. Sollen in diesen Szenarien auf den zentralseitigen VPN-Gateway mehrere eingehende IKEv2-VPN-Tunnel zu einem Load Blancer zusammengefasst werden, so kann dies über zusätzliche RADIUS-Attribute realisiert werden.

Die Bündel-Gegenstellen eines dynamischen Load-Balancers sind IKEv2-VPN-Clients, die RADIUS-Authorization nutzen. Dabei wird ein VPN-Client dann in einem dynamischen Load-Balancer-Verbund aufgenommen, wenn die RADIUS-Antwort ein entsprechendes RADIUS-Attribut (LCS-Load-Balancer) enthält. Dieses Attribut gibt den Namen des Load-Balancer-Verbundes an und entscheidet zusätzlich darüber, ob Client-Binding (siehe *Client-Binding* auf Seite 430) aktiv sein soll.

Wenn eine solche VPN-Verbindung abbricht, wird der Client wieder aus seinem Load-Balancer-Verbund entfernt. Ein erneuter Verbindungsaufbau muss durch den Client erfolgen.

Ein dynamischer Load-Balancer-Verbund darf nicht denselben Namen wie ein statisch konfigurierter Verbund haben, man kann also statische und dynamische Clients nicht im selben Load-Balancer vermischen.

Für die Konfiguration über einen RADIUS-Server wird die Syntax der Standard-Attribute „Framed-Route“ und „Framed-IPv6-Route“ erweitert, damit dynamisch Routen übermittelt werden können, die auf einen Load-Balancer zeigen. Routen des IKEv2-Routing zeigen automatisch auf den Load-Balancer statt auf das Einwahlinterface, wenn das Attribut „LCS-Load-Balancer“ verwendet wird.

Das Feature wird auch im Zusammenhang mit IKEv2-Routing unterstützt. Die Route auf dem VPN-Gateway wird dann dynamisch von der Gegenseite übermittelt statt die Route per Framed-Route-Attribut vom RADIUS-Server zu empfangen. In diesem Fall muss lediglich das Attribut „LCS-Load-Balancer“ vom RADIUS-Server übermittelt werden.

Tabelle 25: RADIUS-Attribute

ID	Bezeichnung	Bedeutung
22	Framed-Route	IPv4-Routen, die in Richtung des Clients (Next-Hop-Client) auf dem VPN-Gateway in der Routing-Tabelle eingetragen werden sollen. Format (String): <Präfix> [ifc=<Zielinterface>] [rtg_tag=<Routing-Tag>] [admin_distance=<Distanz>] **<Präfix>** IPv4-Adresse + '/' + Präfixlänge oder Netzmaske **ifc=<Zielinterface>** Name des IP-Interfaces oder eines Load-Balancers, auf den die Route zeigen soll, oder „#Ifc". Wenn kein Zielinterface angegeben ist oder es „#Ifc" lautet, dann zeigt die Route auf das VPN-Interface für den betreffenden Einwahlclient. Der Interfacename kann bis zu 16 Zeichen enthalten. **rtg_tag=<Routing-Tag>** Routing-Tag für die Route. Wenn es nicht angegeben wird, bekommt die Route das Tag des Einwahlinterfaces. **admin_distance=<Distanz>** Administrative Distanz der Route als Zahl von 0 bis 255. Wenn sie nicht angegeben wird, bekommt die Route die standardmäßige Distanz für VPN-Routen.
99	Framed-IPv6-Route	IPv6-Routen, die in Richtung des Clients (Next-Hop-Client) auf dem VPN-Gateway in der Routing-Tabelle eingetragen werden sollen. Format (String): <Präfix> [ifc=<Zielinterface>] [rtg_tag=<Routing-Tag>] [admin_distance=<Distanz>] **<Präfix>** IPv6-Adresse + '/' + Präfixlänge **ifc=<Zielinterface>** Name des IP-Interfaces oder eines Load-Balancers, auf den die Route zeigen soll, oder „#Ifc". Wenn kein Zielinterface angegeben ist oder es „#Ifc" lautet, dann zeigt die Route auf das VPN-Interface für den betreffenden Einwahlclient. Der Interfacename kann bis zu 16 Zeichen enthalten. **rtg_tag=<Routing-Tag>** Routing-Tag für die Route. Wenn es nicht angegeben wird, bekommt die Route das Tag des Einwahlinterfaces.

ID	Bezeichnung	Bedeutung
		admin_distance=<Distanz> Administrative Distanz der Route als Zahl von 0 bis 255. Wenn sie nicht angegeben wird, bekommt die Route die standardmäßige Distanz für VPN-Routen.
LANCOM 28	LCS-Load-Balancer	Format (String): <Load-Balancer-Name> [client_binding={no|yes}] Der <Load-Balancer-Name> kann bis zu 16 Zeichen lang sein und gibt eine entsprechende Load-Balancing-Gegenstelle auf den LANCOM Routern an. Diese Gegenstelle wird für das dynamische IKEv2-VPN-Load-Balancing verwendet und darf daher nicht unter **IP-Router** > **Load Balancing** bereits für statisches Load-Balancing verwendet werden. Die Option „client_binding" schaltet das Client Binding (siehe *Client-Binding* auf Seite 430) ein oder aus. Ohne diese Angabe ist Client Binding aus. Der erste sich verbindende IKEv2-VPN-Client gibt diese Einstellung vor. Danach erfolgende andere Einstellungen für das Client Binding in Verbindung mit dieser Load-Balancing-Gegenstelle werden ignoriert.

Beispiel: RADIUS-Attribute für einen einfachen Loadbalancer aus IKEv2-VPN-Tunneln auf der Zentrale

```
LCS-Load-Balancer=LB1
Framed-Route=192.168.45.0/24 ifc=LB1;
```

6.9.3 Statisches Load-Balancing

Neben der im vorhergehenden Abschnitt beschriebenen dynamischen Verbindungsauswahl sind Szenarien vorstellbar, in denen für eine bestimmte TCP-Verbindung immer die gleiche DSL-Verbindung benutzt werden soll. Hierbei sind zwei Fälle zu unterscheiden:

- Ein Server mit einer festen IP-Adresse ist nur über eine dedizierte Verbindung erreichbar. Hierfür reicht die Auswahl anhand der Ziel-IP-Adresse.
- Ein Server verwendet ein Protokoll, das neben einem Kontrollkanal weitere Kanäle zur Datenübertragung benötigt (z. B. FTP, PPTP). Dabei akzeptiert der Server den Aufbau der Datenkanäle nur von der gleichen IP-Adresse, von der auch der Kontrollkanal aufgebaut wurde.

6.9.3.1 Zielbasierte Kanalvorgabe

Für die Zielbasierte Kanalvorgabe genügt es, für den jeweiligen Server einen Eintrag in der Routing-Tabelle aufzunehmen, der als Ziel nicht die „virtuelle" Balancing-Verbindung, sondern eine der Bündel-Verbindungen direkt verwendet.

6.9.3.2 Regelbasierte Kanalvorgabe (Policy-based Routing)

Um die Kanalauswahl aufgrund des Zielports oder der Quelladresse zu entscheiden, werden geeignete Einträge in der Firewall angelegt. Den Firewall-Einträgen wird dabei ein spezielles „Routing-Tag" zugefügt, mit dem über die Routing-Tabelle die gewünschte Kanalauswahl gesteuert werden kann. Weitere Informationen finden Sie unter *Policy-based Routing* auf Seite 385.

6.9.4 Indirekte Bündelung für LAN-LAN-Kopplungen über PPTP

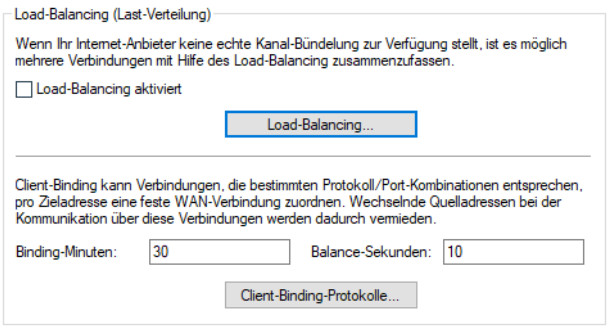
Die indirekte Bündelung erfolgt über gebündelte PPTP-Verbindungen, wodurch sich bei einer LAN-LAN-Kopplung die volle Bandbreite der gebündelten Kanäle nutzen lässt. Bei der Betrachtung der PPTP-Bündelung gibt es drei verschiedene Szenarien:

- Der Client bündelt DSL-Kanäle, der Server steht hinter einen Anschluss mit genügender Bandbreite
- Der Client steht hinter einem breitbandigen Anschluss, doch der Server muss bündeln
- Server und Client bündeln DSL-Kanäle

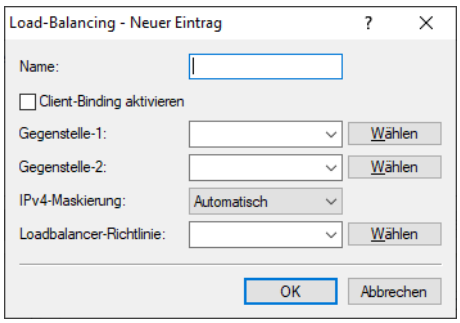
Zur Konfiguration werden lediglich in der Balancing-Tabelle die weiteren PPTP-Adressen aufgeführt.

6.9.5 Konfiguration des Load-Balancing

Um Load-Balancing mit LANconfig zu konfigurieren, wechseln Sie in die Ansicht **IP-Router** > **Routing** > **Load-Balancing**.



Aktivieren Sie dort das Load-Balancing über den Schalter **Load-Balancing aktiviert**. Weitere Einstellungen nehmen Sie unter **Load-Balancing** vor.



Name

Eindeutiger Name für eine virtuelle Load-Balancing-Gegenstelle. Diese Gegenstelle kann dann in der Routing-Tabelle verwendet werden.

Client-Binding aktivieren

Aktiviert oder deaktiviert die Client-Binding Funktion.

Gegenstelle-1

Name einer bereits konfigurierten Gegenstelle mit der weitere zusammengefasst werden sollen.

Gegenstelle-2

Name einer bereits konfigurierten Gegenstelle, die mit der ersten zusammengefasst werden sollen.

IPv4-Maskierung

Stellen Sie hier die IPv4-Maskierung des Load-Balancers ein. Mögliche Werte:

Automatisch

Übernimmt die Maskierungsoption jeder einzelnen Leitung aus der Routing-Tabelle.

Ein

Aktiviert NAT auf allen Gegenstellen im Loadbalancer.

Nein

Deaktiviert NAT auf allen Gegenstellen im Loadbalancer.

Nur Intranet

Aktiviert NAT für Netze vom Typ INTRANET. Die DMZ wird nicht maskiert.

Loadbalancer-Richtlinie

Hier finden Sie einige durch LCOS vordefinierte Load-Balancer-Policies.

DEFAULT

Diese Loadbalancer-Policy hat immer denselben Effekt, wie wenn man keine Policy angibt bzw. die Loadbalancer-Policy-Spalte leer lässt. In der Firewall und im Kommandozeilen-Ping löst sie einen Rückfall auf die Policy aus der Tabelle des Dynamic Path Selection aus.

TRAFFIC

Diese Policy sucht für jeden Kanal die zugehörige unterliegende physikalische Verbindung heraus und besorgt sich ihre absolute Rx-Last und Tx-Last aus den Spalten Rx/s-average und Tx/s-average von **Status** > **WAN** > **Throughput**. Falls für alle diese physikalischen Verbindungen eine physikalische Bandbreite bekannt ist (typischerweise bei kabelgebundenen Verbindungen, aber nicht im Mobilfunk), berechnet sie die relativen Lasten, indem sie die absoluten Lasten durch die jeweilige Bandbreite teilt, sonst arbeitet sie mit den absoluten Lasten weiter. Im nächsten Schritt nimmt sie von Rx- und Tx-Last jeweils die größere. Sie selektiert dann den Kanal mit der geringsten Last.

BANDWIDTH

Die Loadbalancer-Policy BANDWIDTH wählt zufällig einen Kanal aus. Wenn für alle unterliegenden physikalischen Verbindungen eine Bandbreite bekannt ist, ist die Wahrscheinlichkeit für einen bestimmten Kanal proportional zu dieser Bandbreite, d. h. ein 50 MBit/s-Kanal wird fünf mal so häufig gewählt wie ein 10 MBit/s-Kanal. Andernfalls, also wenn mindestens eine Bandbreite nicht bekannt ist, wird der Kanal gleichverteilt ausgewählt.

ROUND-ROBIN

Die Loadbalancer-Policy ROUND-ROBIN wählt die Kanäle reihum aus.

MOST-USED

Mit dieser Policy wählt der Loadbalancer denjenigen Kanal, auf dem gerade die meisten Firewall-Sessions (ungeachtet, ob in Sende- oder Empfangsrichtung und ungeachtet, ob IPv4 oder IPv6) liegen. Diese Policy ist nur als Gegenstück zu Dynamic Path Selection sinnvoll, d. h. wenn etwa ein Filialgerät auf dem Loadbalancer Dynamic Path Selection nutzt, dann sollte die Zentrale auf ihrem zugehörigen Loadbalancer MOST-USED nutzen. Das führt effektiv dazu, dass sich die Zentrale an die Dynamic Path Selection-Entscheidungen der Filiale anpasst, ohne dass die Filiale ihre Entscheidung der Zentrale explizit mitteilen müsste.

Hinweis: Diese Funktion hat nur einen Effekt auf gerouteten Datenverkehr. Alle internen Dienste des LANCOM Routers verwenden ausschließlich die Policy **ROUND-ROBIN**.

Client-Binding kann Verbindungen, die bestimmten Protokoll- / Port-Kombinationen entsprechen, pro Zieladresse eine feste WAN-Verbindung zuordnen. Wechselnde Quelladressen bei der Kommunikation über diese Verbindungen werden dadurch vermieden. Das Client-Binding wird beim Load-Balancing ggf. aktiviert.

Binding-Minuten

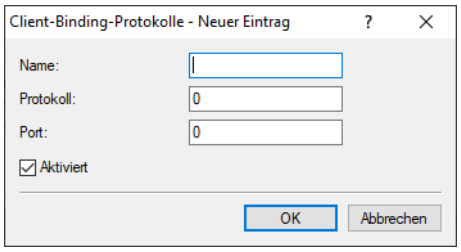
Definieren Sie hier die Zeit in Minuten, für die die Binding-Einträge für einen Client gültig sein sollen.

Balance Sekunden

Um zu vermeiden, dass Daten über die Internetverbindung der Haupt-Session fließen, die problemlos über parallele Verbindung zu übertragen wären, sorgt ein entsprechender Timer dafür, dass der Load-Balancer für eine definierte Dauer zusätzliche Sessions auf die zur Verfügung stehenden Internetverbindungen verteilt. Erst nach Ablauf des Timers zwingt das Client-Binding eine neue Session wieder auf die ursprüngliche Internetverbindung und startet den Timer neu. Der Server erkennt somit weiterhin den Anmeldestatus des Benutzers anhand seiner aktuellen IP-Adresse.

Definieren Sie hier die Zeit in Sekunden, innerhalb der der Load-Balancer neue Sessions nach dem Start der Haupt-Session frei auf andere Internetverbindungen verteilt.

Unter **Client-Binding-Protokolle** konfigurieren Sie die entsprechenden Protokoll- / Port-Kombinationen.



Name

Geben Sie diesem Eintrag einen Namen.

Protokoll

Enthält die IP-Protokollnummer.

Mehr Informationen über IP-Protokollnummern finden Sie in der *Online-Datenbank der IANA*.

Port

Enthält den Port des IP-Protokolls.

Aktiviert

Aktivieren Sie diesen Eintrag.

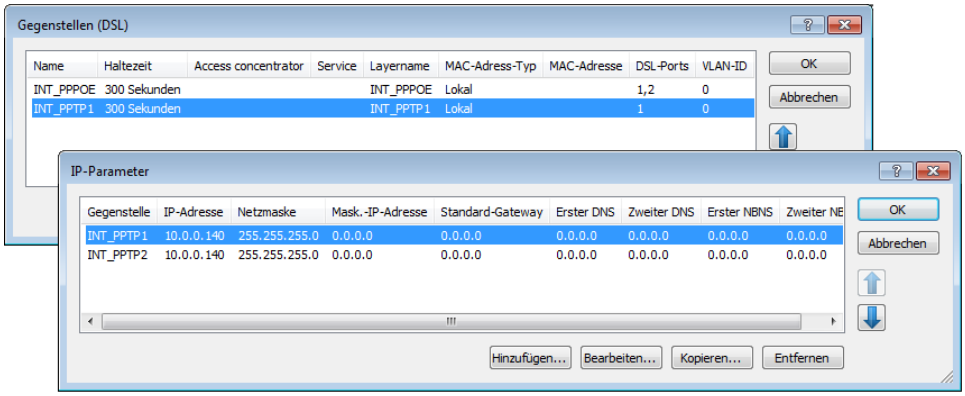
Für die folgenden Beispielkonfigurationen gehen wir davon aus, dass die entsprechenden Gegenstellen mit allen Zugangsdaten bereits eingerichtet sind.

6.9.5.1 Direkte Kanalbündelung über PPTP

Zur Konfiguration der direkten Kanalbündelung über PPTP gehen Sie folgendermaßen vor:

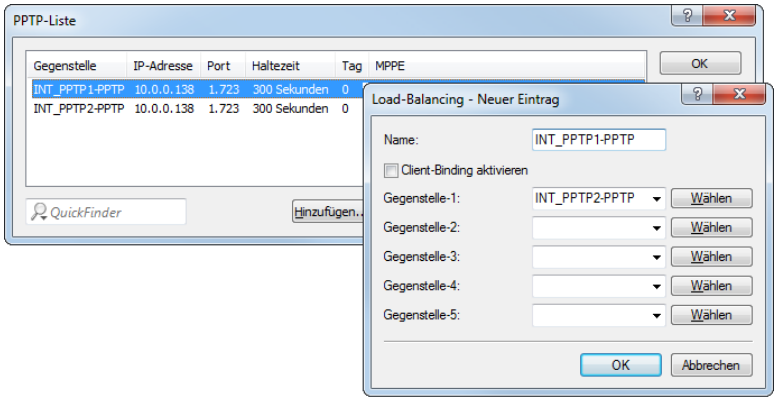
1. Konfigurieren Sie mehrere getrennte PPTP-Verbindungen (z. B. über den Assistenten von LANconfig), die jeweils einen anderen DSL-Port nutzen. Die Verbindungen werden mit den gleichen Werten für die IP-Parameter eingetragen, die in LANconfig unter **Kommunikation** > **Protokolle** > **IP-Parameter** einzusehen sind.

Konsole: **Setup** > **WAN** > **IP-Liste**



2. Eine Bündelung erfolgt dann, wenn für die physikalische Verbindung der PPTP-Gegenstelle in der Load-Balancing-Liste zusätzliche Gegenstellen definiert sind. Die PPTP-Verbindung fordert dann im Bündelfall die nächste physikalische Verbindung an und baut sie dorthin auf. Tragen Sie die Bündelverbindungen in LANconfig über **IP-Router** > **Routing** > **Load-Balancing** ein.

   Konsole: **Setup** > **IP-Router** > **Load-Balancer**

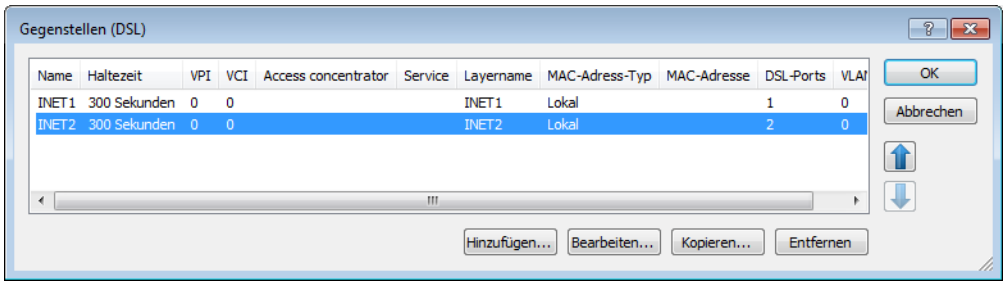


6.9.5.2 Dynamisches Load-Balancing mit mehreren DSL-Zugängen

Für das dynamische Load-Balancing werden zunächst die Internetzugänge z. B. mit den Assistenten von LANconfig eingerichtet, z. B. 'INET1' und 'INET2'.

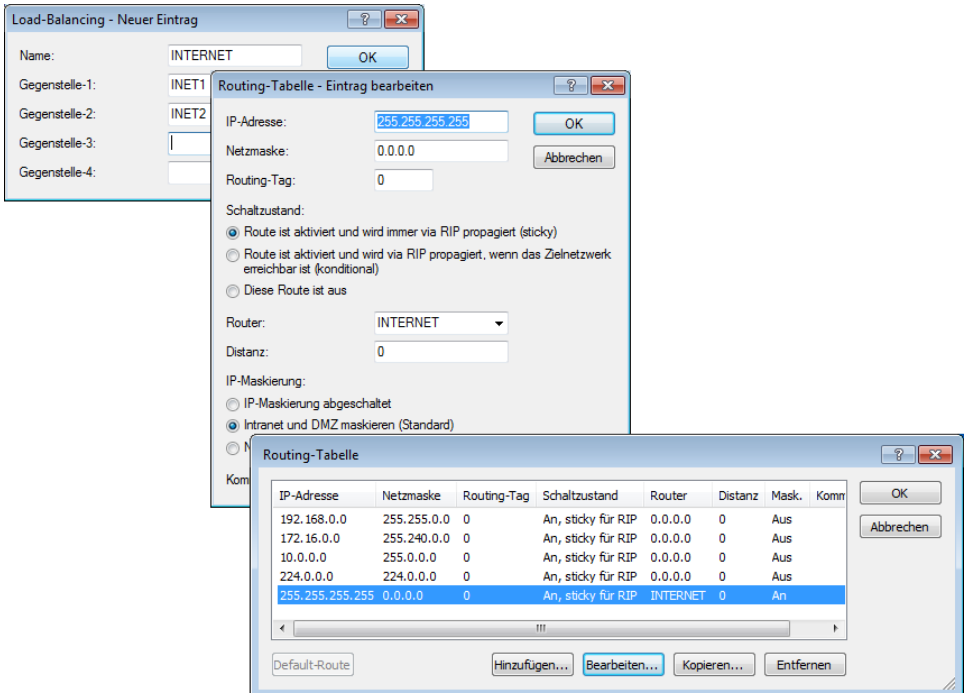
1. Um den Internet-Traffic auf verschiedene DSL-Interfaces zu verteilen, werden den einzelnen Gegenstellen in LANconfig unter **Kommunikation** > **Gegenstellen** > **Gegenstellen (DSL)** unterschiedliche DSL-Ports zugewiesen.

   Konsole: **Setup** > **WAN** > **DSL-Breitband-Gegenstellen**



2. Die beiden DSL-Gegenstellen werden dann in der Load-Balancing-Liste in LANconfig über **IP-Router** > **Routing** > **Load-Balancing** einer neuen, virtuellen Gegenstelle 'INTERNET' zugeordnet.

Konsole: **Setup** > **IP-Router** > **Load-Balancer**



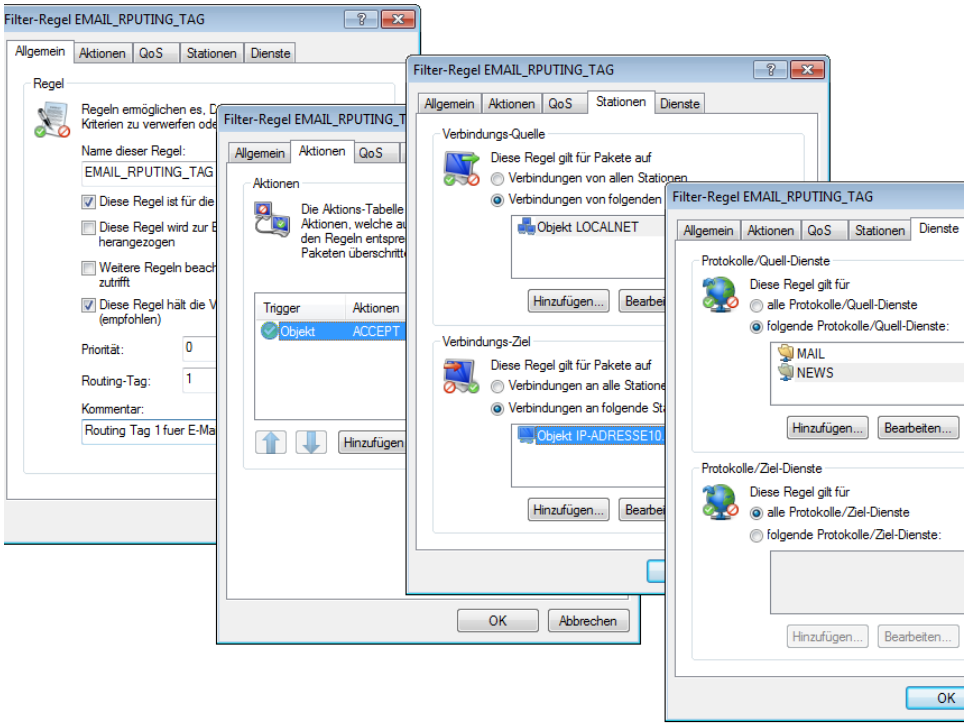
3. Die virtuelle Gegenstelle wird in der Routing-Tabelle in LANconfig über **IP-Router** > **Routing** > **IP-Routing-Tabelle** als Router für die Default-Route eingetragen.

   Konsole: **Setup** > **IP-Router** > **IP-Routing-Tabelle**

   Für den Zugang zum Internet wird nun die virtuelle Gegenstelle 'INTERNET' verwendet. Wenn Daten über diese Verbindung geroutet werden, werden anhand der Load-Balancing-Tabelle die „echten" DSL-Verbindungen aufgebaut und die Daten entsprechend über die gewählten DSL-Ports übertragen.

4. Um den Datenverkehr je nach Anwendung gezielter auf die DSL-Ports zu verteilen, können die Routing-Tags genutzt werden. Soll z. B. der ausgehende E-Mail-Traffic über ein bestimmtes DSL-Interface mit einer bestimmten IP-Adresse geroutet werden, wird in der Firewall unter LANconfig über **Firewall / QoS** > **Regeln** eine entsprechende Regel angelegt, die den Datenverkehr über E-Mail-Dienste von allen lokalen Stationen zum Mail-Server überträgt und dabei das Routing-Tag '1' setzt.

Konsole: **Setup** > **IP-Router** > **Firewall** > **Regel-Tabelle**

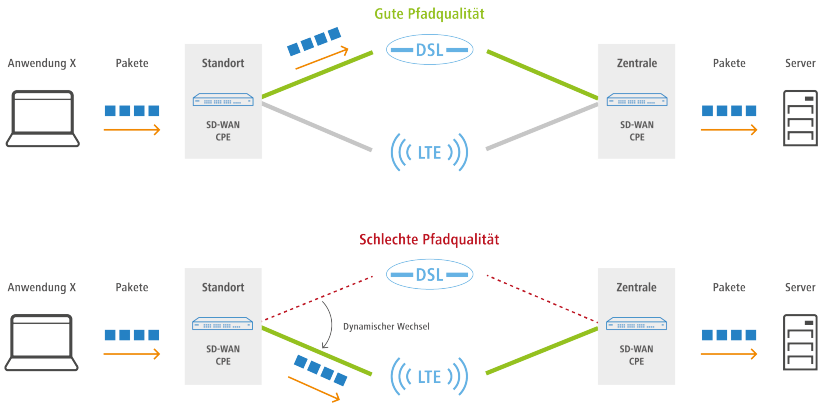


6.10 SD-WAN Dynamic Path Selection

Dynamic Path Selection (DPS) erlaubt die Steuerung von Datenverkehr über die Leitung mit der besten Qualität basierend auf Metriken wie Last, Paketverlust, Latenz oder Jitter um die Anwendungsperformance bei mehreren verfügbaren Leitungen in einem SD-WAN-Szenario zu optimieren.

In SD-WAN-Szenarien sollen MPLS-Leitungen entweder ersetzt oder um kostengünstige Internetverbindungen wie DSL, Kabelinternet, Glasfaser oder 4G/5G ergänzt werden. Mithilfe von Load Balancing kann die Gesamtbandbreite aller zur Verfügung stehenden Leitungen ausgenutzt werden. Um die Performance geschäftskritischer Anwendungen sicherzustellen, kann Dynamic Path Selection eingesetzt werden. Dabei werden alle Leitungen kontinuierlich durch aktives Monitoring mithilfe von ICMP-Paketen überwacht und daraus Metriken für Last, Paketverlust, Latenz und Jitter berechnet. Durch Richtlinien werden Anforderungen der Business-Anwendungen wie z. B. Echtzeitdatenverkehr an Leitungen definiert, beispielweise der erlaubte Paketverlust oder die maximale Latenz eines möglichen Pfades. Der Algorithmus zur Dynamic

Path Selection wählt für Sessions die Leitung mit der besten Qualität aus. Erfüllen mehrere Leitungen die geforderten Richtlinien, so wird ein Load Balancing im Round-Robin-Verfahren über diese Leitungen durchgeführt.



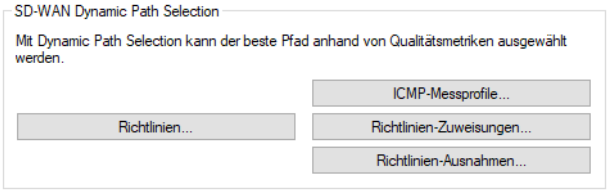
Richtlinien können als „kritisch" definiert werden. Falls keine Leitung diese Richtlinie erfüllt, wird der Datenverkehr über keine Leitung transportiert.

Dynamic Path Selection wird auf einem Load Balancer aktiviert. Ein Load Balancer kann entweder für Internetverbindungen oder SD-WAN-Overlay-Tunnel (VPN) definiert sein. Der Endpunkt für ICMP-Testpakete kann entweder eine beliebige IP-Adresse oder das zentralseitige SD-WAN-Gateway sein.

In der Firewall werden die definierten (Load-Balancer-)Richtlinien für die Anwendungen in entsprechenden Firewall-Regeln verwendet. Dort wird definiert für welchen Datenverkehr bzw. Anwendungen die Load-Balancer-Richtlinie gelten soll.

6.10.1 Konfiguration der Dynamic Path Selection

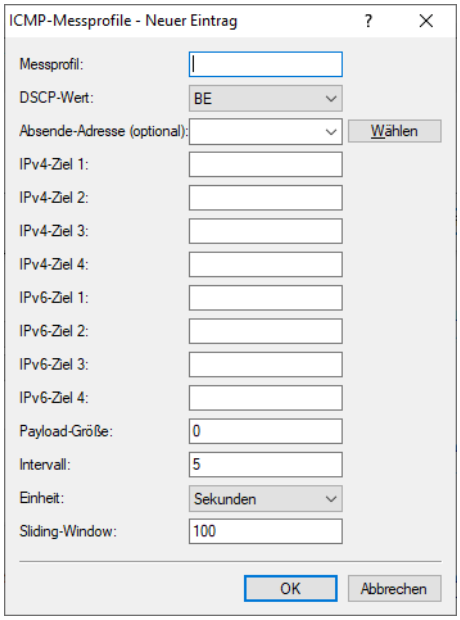
Um Dynamic Path Selection mit LANconfig zu konfigurieren, wechseln Sie in die Ansicht **IP-Router** > **Routing** > **SD-WAN Dynamic Path Selection**.



6.10.1.1 ICMP-Messprofile

ICMP-Messprofile definieren einen Parametersatz, nach dem Messungen auf Basis von ICMP-Pings durchgeführt werden. Aus den Messungen werden Interface-Metriken abgeleitet, die die Verbindungsqualität quantifizieren sollen. Diese Metriken sind: Mittlere Round Trip Time (RTT, Latenz), Jitter und Paketverlustrate (Packet Loss Rate).

Zur Konfiguration der ICMP-Messprofile wechseln Sie in die Ansicht **IP-Router** > **Routing** > **SD-WAN Dynamic Path Selection** > **ICMP-Messprofile**.



Messprofil

Der Name des Profils. Über diesen Namen wird das Profil in DPS-Richtlinien referenziert.

DSCP-Wert

Definiert den DSCP-Wert, der im IP-Header der Messpakete gesetzt wird. DSCP (Differentiated Services Code Point) wird für QoS (Quality of Service) verwendet.

Absende-Adresse (optional)

Referenziert eine benamte Loopback-Adresse, die bei den Messpaketen als Absender verwendet wird. Wenn das Feld leer gelassen wird, wählt der Router selbstständig eine Adresse aus, die zum Absende-Interface passt.

IPv4-Ziel 1-4

Bis zu 4 Messziele als gültige IPv4-Unicast-Adressen oder DNS Hostnamen. Wird 0.0.0.0 eingetragen, wird das Messziel dynamisch vom VPN festgelegt. Wird das Feld leer gelassen, erfolgt keine Messung für die entsprechende Adressfamilie.

IPv6-Ziel 1-4

Bis zu 4 Messziele als gültige IPv6-Unicast-Adressen oder DNS Hostnamen. Wird :: eingetragen, wird das Messziel dynamisch vom VPN festgelegt. Wird das Feld leer gelassen, erfolgt keine Messung für die entsprechende Adressfamilie.

Payload-Größe

Gibt die Größe der Daten nach dem ICMP-Header (Payload-Größe) der versendeten Pings an.

Intervall

Der Abstand in Sekunden zwischen 2 Messungen. Außerdem wird die maximale Round Trip Time vorgegeben. Pakete, die binnen eines Messintervalls nicht beantwortet wurden, zählen als Packet Loss.

Einheit

Gibt an, ob die ICMP-Messungen für den Wert in der Einheit Sekunden oder Millisekunden durchgeführt werden sollen. Mögliche Werte: Sekunden (Default), Millisekunden.

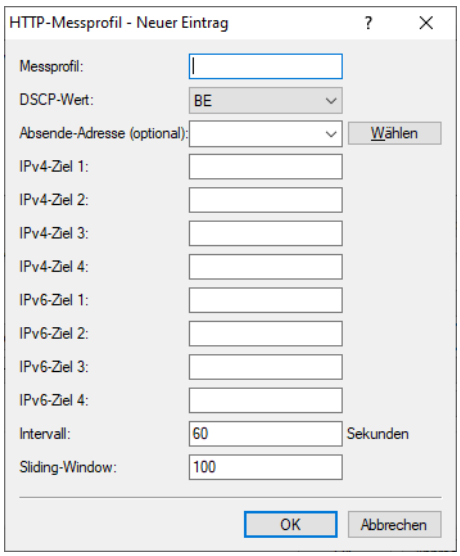
Sliding-Window

Maximale Anzahl an Messwerten, die für die Bestimmung der Interface-Metriken benutzt werden. Wird ein Messwert empfangen, obwohl bereits die hier angegebene Anzahl an Messwerten aufgezeichnet wurde, dann wird der älteste Messwert verworfen.

6.10.1.2 HTTP-Messprofile

HTTP-Messprofile definieren einen Parametersatz, nach dem Messungen auf Basis von HTTP(S)-Verbindungsaufbauten durchgeführt werden. Aus den Messungen werden Interface-Metriken abgeleitet, welche die Verbindungsqualität quantifizieren sollen. Diese Metriken sind: Mittlere Zeit bis zum Aufbau einer HTTP(S)-Verbindung (Latenz), Jitter, und Verbindungsfehler (Paketverlust)-Rate.

Zur Konfiguration der HTTP-Messprofile wechseln Sie in die Ansicht **IP-Router** > **Routing** > **SD-WAN Dynamic Path Selection** > **HTTP-Messprofil**.



Messprofil

Der Name des Profils. Über diesen Namen wird das Profil in DPS-Richtlinien referenziert.

DSCP-Wert

Definiert den DSCP-Wert, der im IP-Header der Messpakete gesetzt wird. DSCP (Differentiated Services Code Point) wird für QoS (Quality of Service) verwendet.

Absende-Adresse (optional)

Referenziert eine benamte Loopback-Adresse, die bei den Messpaketen als Absender verwendet wird. Wenn das Feld leer gelassen wird, wählt der Router selbstständig eine Adresse aus, die zum Absende-Interface passt.

IPv4-Ziel 1-4

Bis zu 4 Messziele als gültige IPv4-Unicast-Adressen oder DNS Hostnamen. Wird 0.0.0.0 eingetragen, wird das Messziel dynamisch vom VPN festgelegt. Wird das Feld leer gelassen, erfolgt keine Messung für die entsprechende Adressfamilie.

IPv6-Ziel 1-4

Bis zu 4 Messziele als gültige IPv6-Unicast-Adressen oder DNS Hostnamen. Wird :: eingetragen, wird das Messziel dynamisch vom VPN festgelegt. Wird das Feld leer gelassen, erfolgt keine Messung für die entsprechende Adressfamilie.

Intervall

Der Abstand in Sekunden zwischen 2 Messungen. Außerdem wird die maximale Round Trip Time vorgegeben. Pakete, die binnen eines Messintervalls nicht beantwortet wurden, zählen als Packet Loss.

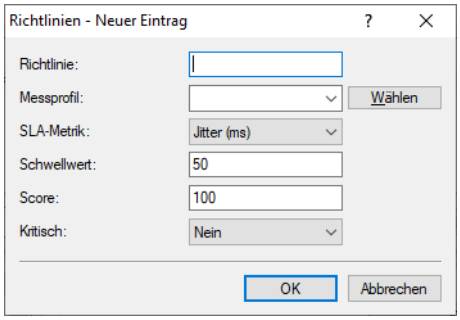
Sliding-Window

Maximale Anzahl an Messwerten, die für die Bestimmung der Interface-Metriken benutzt werden. Wird ein Messwert empfangen, obwohl bereits die hier angegebene Anzahl an Messwerten aufgezeichnet wurde, dann wird der älteste Messwert verworfen.

6.10.1.3 Richtlinien

Um die Verbindungsqualität von Interfaces für die dynamische Pfadauswahl bewerten zu können, können den aus den Messprofilen errechneten Metriken abhängig von Schwellenwerten Punktwerte zugewiesen werden. Diese Punktwerte werden aufsummiert, um das „beste" Interface zu bestimmen. Es ist ebenfalls möglich, einzelne Schwellenwerte als „kritisch" zu bewerten (z. B. ein Jitter <= 30 ms). Die Summe dieser Punkte (Gesamtergebnis) und die überschrittenen kritischen Schwellenwerte stellen die Grundlage für dynamische Load Balancer-Entscheidungen dar. Eine DPS-Richtlinie enthält die Sammlung der Schwellenwerte und Kritikalitätsmarkierungen, die für eine Berechnung der Punktsumme notwendig sind.

Zur Konfiguration der DPS-Richtlinien wechseln Sie in die Ansicht **IP-Router** > **Routing** > **SD-WAN Dynamic Path Selection** > **Richtlinien**.



Richtlinie

Der Name der DPS-Richtlinie. Über diesen Namen wird die Richtlinie in Firewall-Regeln referenziert. Alle Zeilen in dieser Tabelle, die den selben Richtlinien-Namen tragen, werden zu einer Richtlinie zusammengefasst. Somit ist es möglich, u. a. die selbe Metrik mehrfach mit verschiedenen Schwellenwerten in der selben Richtlinie zu verwenden. So lässt sich eine abgestufte Punktebewertung vornehmen (z. B. 10 Punkte bei Latenz <= 100, weitere 10 Punkte bei Latenz <= 50).

Messprofil

Entweder leer oder der Name eines ICMP-Messprofils.

Das Feld muss genau dann leer sein, wenn als **SLA-Metrik** „Last(%)" ausgewählt wird. In allen anderen Fällen muss ein Messprofil angegeben werden.

SLA-Metrik

Die aus den Messungen des eingestellten Messprofils generierte Metrik, deren Wert gegen den Schwellenwert verglichen wird. Mögliche Werte:

- Latenz (ms)
- Jitter (ms)
- Paketverlust (%)
- Last (%)

Die Metrik „Last(%)“ bezeichnet die Auslastung des Interfaces in Prozent der Maximalbandbreite. Dieser Wert wird nicht über gesonderte Messungen ermittelt, daher muss in diesem Fall der Eintrag **Messprofil** leer bleiben.

Schwellwert

Der Schwellenwert, den die gewählte SLA-Metrik nicht unterschreiten darf.

Score

Wenn eine Metrik den gewählten Schwellenwert unterschreitet, dann wird diese Punktzahl zum Gesamtergebnis der Richtlinie dazuaddiert.

Kritisch

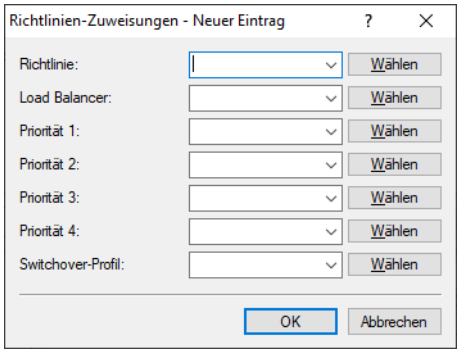
Markierung, ob ein Schwellenwert kritisch ist. Wenn ein als „kritisch“ markierter Schwellenwert nicht unterschritten wird, ist das Gesamtergebnis nicht definiert.

Ein Interface mit einem undefinierten Gesamtergebnis kann nicht durch eine dynamische Load Balancer-Entscheidung ausgewählt werden.

6.10.1.4 Richtlinien-Zuweisungen

Hier legen Sie fest, welche DPS-Richtlinie mit welchem Load Balancer verwendet werden soll, und welche Prioritäten bei Gleichstand des Gesamtergebnisses gelten sollen.

Zur Konfiguration der Richtlinien-Zuweisungen wechseln Sie in die Ansicht **IP-Router** > **Routing** > **SD-WAN Dynamic Path Selection** > **Richtlinien-Zuweisungen**.



Richtlinie

Der Name einer existierenden DPS-Richtlinie aus *Richtlinien* auf Seite 444.

Load Balancer

Name eines Load Balancers (siehe auch *Konfiguration des Load-Balancing* auf Seite 435), der mit dieser Policy bewertet werden soll. Auf allen Interfaces, die zu diesem Load Balancer gehören, werden automatisch Messungen entsprechend der in der Richtlinie referenzierten Messprofile gestartet.

Es ist möglich, das Starten der Messungen für einzelne Interfaces dieses Load Balancers zu unterdrücken. Siehe hierzu *Richtlinien-Ausnahmen* auf Seite 446.

Priorität

Wenn im Rahmen der dynamischen Pfadauswahl mehrere Interfaces das gleiche Polixy-Gesamtergebnis erreichen, wird über die Einträge „Priorität“ bestimmt, welches Interface ausgewählt wird (1 – höchste Priorität, 4 – geringste Priorität). Wenn die Felder leer gelassen werden, dann wird ein Load Balancing nach der standardmäßigen Load-Balancer-Verteilungsstrategie „Round-Robin“ durchgeführt.

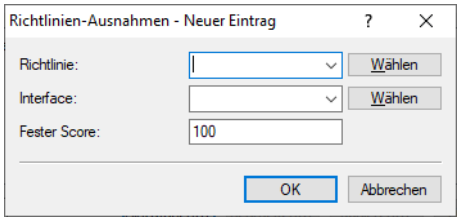
Switchover-Profil

Geben Sie hier den Namen des Switchover-Profils an, dass für diese Richtlinie verwendet werden soll. Siehe hierzu *Switchover-Profile* auf Seite 446.

6.10.1.5 Richtlinien-Ausnahmen

Es ist möglich, einzelne Messprofile nicht auf bestimmte Interfaces anzuwenden, z. B. wenn diese per Volumentarif bezahlt werden.

Zur Konfiguration der Richtlinien-Ausnahmen wechseln Sie in die Ansicht **IP-Router** > **Routing** > **SD-WAN Dynamic Path Selection** > **Richtlinien-Ausnahmen**.



Richtlinie

Der Name einer existierenden DPS-Richtlinie aus *Richtlinien* auf Seite 444.

Interface

Der Name eines Interfaces (z. B. WAN-Gegenstellen, VPN-Tunnel), welches Teil eines Load Balancers ist, der von der Richtlinie bewertet werden soll. Die in der Richtlinie referenzierten Messprofile werden nicht dafür genutzt, um auf dem Interface Messungen zu starten.

Wenn ein Interface Bestandteil mehrerer Load Balancer ist oder wenn mehrere Richtlinien den Load Balancer, der dieses Interface enthält, bewerten sollen, dann muss das Interface für alle in Frage kommenden Richtlinien als Ausnahme eingetragen werden, um die Messungen zu verhindern.

Fester Score

Da es ohne Messungen nicht möglich ist, ein dynamisches Gesamtergebnis zu bestimmen, wird dieser Wert bei allen Entscheidungen zur dynamischen Pfadauswahl als Wert für das Interface verwendet.

6.10.1.6 Switchover-Profile

Standardmäßig werden bei Dynamic Path Selection nur neue Sessions auf eine bessere Leitung verteilt. Sollen existierende Sessions auf eine bessere Leitung aktiv verschoben werden, so muss Session Switchover aktiviert werden. Ein Session Switchover ist nur für unmaskierte Verbindungen wie z. B. VPN oder SD-WAN-Overlays sinnvoll möglich. Bei maskierten Verbindungen würde sich während der Session die öffentliche WAN-Adresse ändern, was z. B. bei SIP-Sessions oder Online Banking vom Server abgelehnt wird. Um Session Switchover zu aktivieren sind zwei Konfigurationsschritte notwendig:

1. Die Firewall-Regeln für Dynamic Path Selection müssen Session Switchover aktiviert haben.

   Dazu muss der Schalter **Dynamic Path Selection Session Switchover** für IPv4 unter **Firewall/QoS** > **IPv4-Regeln** > **Regeln** > **Allgemein** bzw. für IPv6 unter **Firewall/QoS** > **IPv6-Regeln** > **IPv6-Forwarding-Regeln** gesetzt werden.

2. Ein Switchover-Profil muss mit der entsprechenden Richtlinie in der Tabelle Richtlinien-Zuweisungen verlinkt werden

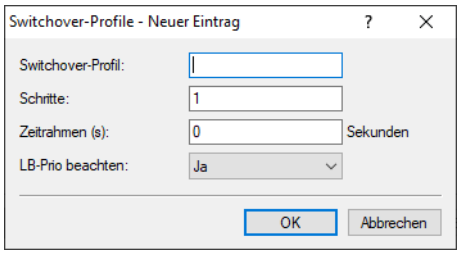
Mit Hilfe des Switchover-Profils kann gesteuert werden, wie schnell die Menge der Sessions auf die neue Leitung bzw. Interface des gleichen Load Balancers umgezogen werden soll.

Um eine Konzentration umziehender Sessions auf einer einzelnen Schnittstelle zu verhindern, werden Sessions i. A. schrittweise in mehreren Gruppen umgezogen, die gleichmäßig auf den konfigurierten Zeitrahmen verteilt werden. Vor

jedem Schritt wird geprüft, ob der Switchover noch notwendig ist, da sich in der Zwischenzeit die Policy-Scores und damit die Rangfolge der Interfaces bzgl. einer Policy verändert haben können. Wenn er nicht mehr notwendig ist, wird der Switchover abgebrochen, und die noch nicht verschobenen Sessions bleiben auf ihrer aktuellen Schnittstelle. Wenn er noch notwendig ist, wird für jede Session zufällig bestimmt, ob sie Teil der in diesem Schritt umziehenden Gruppe ist, oder nicht.

Wenn die Anzahl der Schritte = 1 oder die Gesamtzeit = 0 ist, dann ziehen alle Sessions sofort um.

Zur Konfiguration der HTTP-Messprofile wechseln Sie in die Ansicht **IP-Router** > **Routing** > **SD-WAN Dynamic Path Selection** > **Switchover-Profile**.



Switchover-Profil

Der Name des Switchover-Profils. Über diesen Namen wird das Profil referenziert.

Schritte

Anzahl der Schritte bzw. Gruppen, in der die Menge der Sessions auf die neue Leitung verschoben werden soll.

Zeitrahmen

Zeitrahmen in Sekunden innerhalb dessen die Menge der Sessions auf die neue Leitung verschoben werden soll.

LB-Prio beachten

Dieser Parameter steuert das Verhalten des DPS Session Switchover.

Wenn die Tabelle auf den Default zurückgesetzt wird, erhält die Zeile „AGGRESSIVE-SWITCHOVER" ein „Ja", „SOFT-SWITCHOVER" ein „Nein".

Mögliche Werte:

Ja

Sessions wechseln auch zwischen Interfaces mit gleichem Score, sofern die in *Richtlinien-Zuweisungen* auf Seite 445 vorgegebene Priorisierung eines davon bevorzugt. Passend dazu werden die Ausgabetabellen **Status** > **Firewall** > **Dynamic-Path-Selection** > **IPv4-Preferred-Lines-Log** und **Status** > **Firewall** > **Dynamic-Path-Selection** > **IPv6-Preferred-Lines-Log** in so einem Fall nur noch das höchstpriorisierte Interface als „Preferred" ausweisen. Das ist auch das Interface, zu dem alle Sessions wechseln, mit einer Geschwindigkeit und in entsprechend vielen Zwischenschritten entsprechend der weiteren Parameter im entsprechenden Switchover-Profil.

Diese Einstellung ist z. B. bei folgendem Szenario sinnvoll: Es wird LTE bzw. 5G zusammen mit VDSL verwendet. In manchen Standorten ist LTE / 5G deutlich besser als VDSL. Es soll aber aus Kostengründen zuerst DSL statt LTE / 5G verwendet werden, da dieses nur als Booster genutzt werden soll. Dies funktioniert z. B. auch mit den Prioritäten des Loadbalancers. Mit dem Defaultverhalten wird aber beim Switchover nicht von der schlechten Leitung zur besseren zurück gewechselt.

Dies ist der Default für neue Einträge.

Nein

Das Verhalten des DPS Session Switchover ist, dass dieser nur dann durchgeführt wird, wenn eine andere Leitung tatsächlich besser ist (besserer Score) als die aktuell von der Session verwendete Leitung. Die bei den Load Balancer Policy Assignments mit eintragbarer Priorisierung wird nicht berücksichtigt. Deshalb gibt es keine Switchovers zwischen Interfaces mit identischem Policy-Score.

Dies ist der Default für bereits vor LCOS 10.80 vorhandene Einträge.

6.10.2 Show Kommandos

- `DPS-v4-Policies <Richtlinie> <Gegenstelle>`: Zeigt Informationen über die IPv4-Richtlinien des Dynamic Path Selection für die entsprechende Richtlinie und Gegenstelle.
- `DPS-v4-Score <Richtlinie> <Loadbalancer>`: Zeigt Informationen über den Wert des Dynamic Path Selection bei IPv4 für die entsprechenden Richtlinie und Load-Balancer.
- `DPS-v4-Score-Details <Richtlinie> <Gegenstelle>`: Zeigt Detail-Informationen über den IPv4 Dynamic Path Selection Wert der entsprechenden Richtlinie und Gegenstelle.
- Erweiterung des Ping Kommandos:

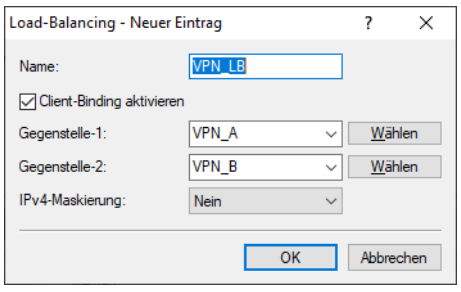
  `ping -l <Richtlinie>`: Verwendet die angegebene Dynamic Path Selection Load-Balancer-Richtlinie, um das abgehende Interface zu bestimmen.

6.10.3 Beispielkonfigurationen

6.10.3.1 Szenario mit zwei VPN-Tunneln über zwei unterschiedliche Internetverbindungen von der Filiale zur Zentrale

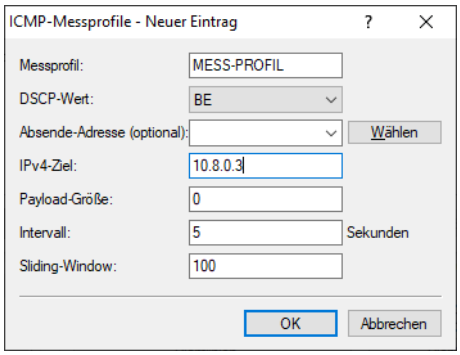
In diesem Beispiel soll Dynamic Path Selection in einem Szenario mit zwei VPN-Tunneln über zwei unterschiedliche Internetverbindungen von der Filiale zur Zentrale für den gesamten Datenverkehr eingerichtet werden. Die IP-Adresse zur Überprüfung der Leitungsqualität per ICMP-Testpaketen ist die private IP-Adresse des zentralseitigen Gateways 10.8.0.3. Ziel ist es, dass immer nur die beste Leitung bzw. VPN-Tunnel basierend auf der Latenz gewählt werden soll.

Dynamic Path Selection wird dabei nur in der Filiale aktiviert. Es wird davon ausgegangen, dass die beiden Internetverbindungen vorhanden sind und die beiden VPN-Tunnel VPN_A und VPN_B bereits zu einem Load Balancer mit Namen VPN_LB eingerichtet wurden:



1. Legen Sie eine neue Tabellenzeile unter **IP-Router** > **Routing** > **SD-WAN Dynamic Path Selection** > **ICMP-Messprofile** an.

Im ersten Schritt wird zunächst ein neues Messprofil angelegt. Das IPv4-Ziel ist hierbei die private IP-Adresse des zentralseitigen Gateways 10.8.0.3. In einem Intervall von 5 Sekunden werden Messpakete zur Evaluierung der Pfade über die VPN-Tunnel (SD-WAN-Overlays) gesendet.



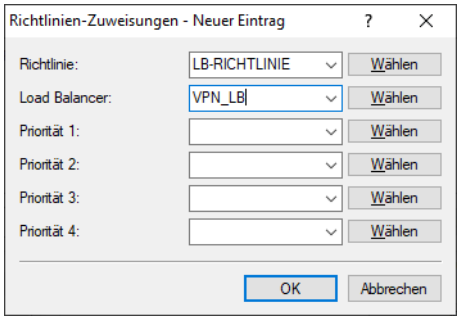
2. Legen Sie eine neue Tabellenzeile unter **IP-Router** > **Routing** > **SD-WAN Dynamic Path Selection** > **Richtlinien** an.

   Im nächsten Schritt wird eine neue Richtlinie angelegt, die als SLA-Metrik „Latenz" einen Schwellenwert von 50 ms besitzt. Wenn der entsprechende VPN-Tunnel eine Latenz unter 50 ms besitzt, so erhält der Pfad einen Score von 100 (Punkten). Eine Verbindung, die dieses Kriterium nicht erfüllt, erhält einen Score von 0, d. h. sie wird also schlechter bewertet. Der Pfad mit dem höchsten Score wird bevorzugter Pfad und somit für den Datenverkehr verwendet. Haben beide Pfade einen identischen Score von 100, so wird ein Load-Balancing zwischen beiden VPN-Tunneln durchgeführt.



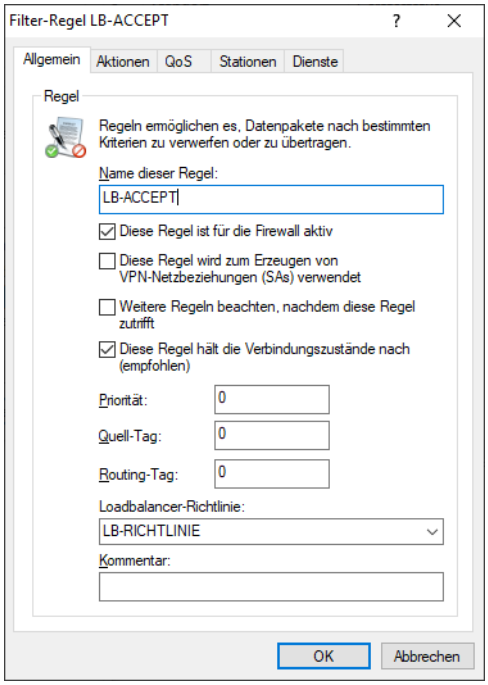
3. Legen Sie eine neue Tabellenzeile unter **IP-Router** > **Routing** > **SD-WAN Dynamic Path Selection** > **Richtlinien-Zuweisungen** an.

   Im Folgenden wird die eben neu erstellte Richtlinie mit dem VPN-Load-Balancer-Verbund VPN_LB verknüpft. Die Felder für Prioritäten können leer bleiben.



4. Legen Sie eine neue Tabellenzeile unter **Firewall/QoS** > **IPv4-Regeln** > **Regeln** an.

Legen Sie eine neue Firewall-Regel an, die allen Datenverkehr akzeptiert und als Load-Balancer-Richtlinie den Wert „LB-RICHTLINIE“ besitzt.



6.11 N:N-Mapping

Das Verfahren der Network Address Translation (NAT) kann für mehrere Dinge benutzt werden:

- um die immer knapper werdenden IPv4-Adressen besser zu nutzen
- um Netze mit gleichen (privaten) Adressbereichen miteinander zu koppeln
- um eindeutige Adressen zum Netzwerkmanagement zu erzeugen

Für die erste Anwendung kommt das sogenannte N:1-NAT, auch als IP-Masquerading (*IP-Masquerading* auf Seite 419) bekannt, zum Einsatz. Hierbei werden alle Adressen (“N”) des lokalen Netzes auf eine einzige (“1”) öffentliche Adresse gemappt. Die eindeutige Zuordnung der Datenströme zu den jeweiligen internen Rechnern erfolgt in der Regel über die Ports der Protokolle TCP und UDP, weshalb man hier auch von NAT/PAT (Network Address Translation/Port Address Translation) spricht.

Durch die dynamische Umsetzung der Ports sind beim N:1-Masquerading nur Verbindungen möglich, die vom internen Netz aus aufgebaut werden. Ausnahme: eine interne IP-Adresse wird statisch einem bestimmten Port zugeordnet, z. B. um einen Server im LAN von außen zugänglich zu machen. Dieses Verfahren nennt man “Inverses Masquerading” (*Port-Forwarding (Inverses Masquerading)* auf Seite 421).

Zur Kopplung von Netzwerken mit gleichen Adressräumen wird ein N:N-Mapping verwendet. Dieses setzt mehrere Adressen (“N”) des lokalen Netzes eineindeutig auf mehrere (“N”) Adressen eines beliebigen anderen Netzes um. Durch diese Umsetzung wird der Adresskonflikt verhindert.

Die Regeln für diese Adressumsetzung werden in einer statischen Tabelle im Gerät definiert. Dabei werden für einzelne Stationen im LAN, Teilnetze oder das gesamte LAN neue IP-Adressen festgelegt, unter denen die Stationen dann mit den anderen Netzen in Kontakt treten können.

Bei einigen Protokollen (z. B. FTP) werden während der Protokollverhandlung Parameter ausgetauscht, die Einfluss auf die Adressumsetzung beim N:N-Mapping haben können. Die entsprechenden Verbindungsinformationen werden bei

diesen Protokollen daher mit den Funktionen der Firewall in einer dynamischen Tabelle festgehalten und zusätzlich zu den Einträgen aus der statischen Tabelle für die korrekte Funktion der Adressumsetzung verwendet.

Die Adressumsetzung erfolgt "Outbound", d. h. bei abgehenden Datenpaketen wird die Quelladresse umgesetzt, und bei eingehenden Datenpaketen wird die Zieladresse umgesetzt, sofern die Adressen im definierten Umsetzungsbereich liegen. Ein "Inbound"-Adressmapping, bei dem bei eingehenden Datenpaketen die Quelladresse (anstelle der Zieladresse) umgesetzt wird, muss stattdessen durch eine entsprechende "Outbound"-Adressumsetzung auf der Gegenseite eingerichtet werden.

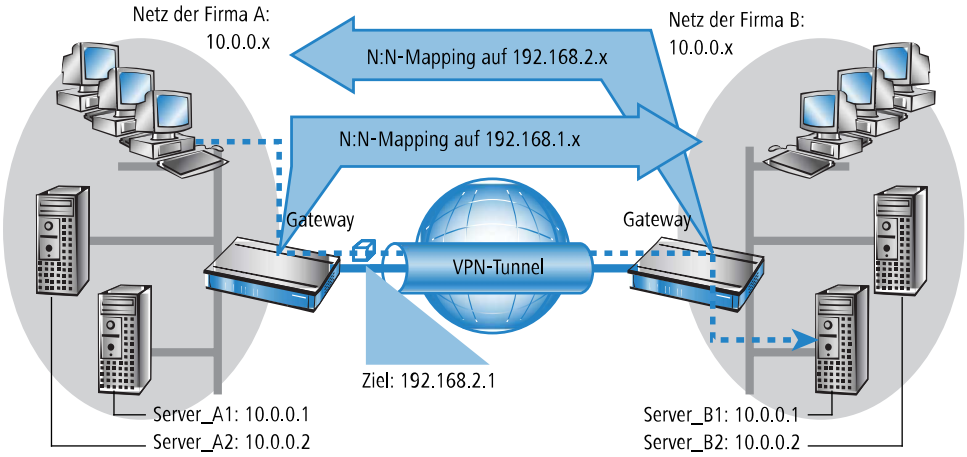
6.11.1 Anwendungsbeispiele

Im folgenden werden die folgenden typischen Anwendungen vorgestellt:

- Kopplung von privaten Netzen, die den gleichen Adressraum belegen
- Zentrale Fernüberwachung durch Dienstleister

6.11.1.1 Netzwerkkopplung

Ein häufig anzutreffendes Szenario stellt die Kopplung zweier Firmennetze dar, die intern den gleichen Adressraum (z. B. 10.0.0.x) belegen. Dies erfolgt meist dann, wenn eine Firma Zugriff auf einen (oder mehrere) Server der anderen erhalten soll:



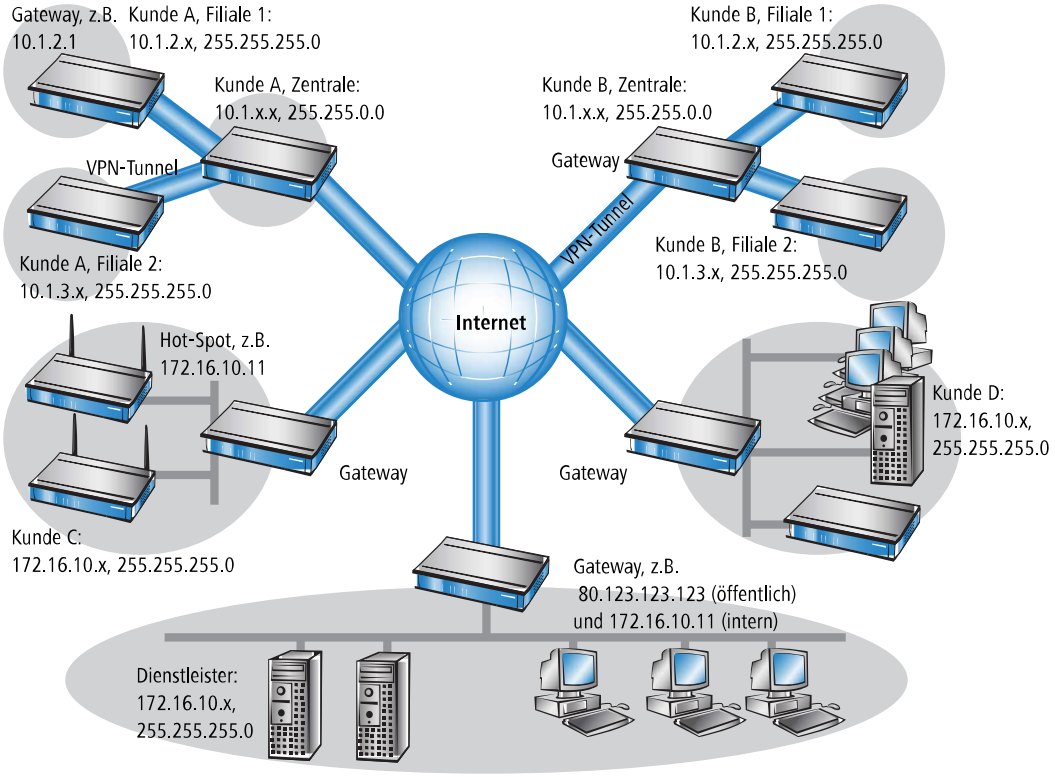
In diesem Beispiel stehen in den Netzen der Firmen A und B Server, die über einen VPN-Tunnel auf das jeweils andere Netz zugreifen wollen. Allen Stationen im LAN soll dabei der Zugang zu den Servern im remoten Netz erlaubt werden. Da beide Netze den gleichen Adresskreis nutzen, ist in dieser Konfiguration zunächst kein Zugriff in das andere Netz möglich. Wenn eine Station aus dem Netz der Firma A auf den Server 1 der Firma B zugreifen will, wird der Adressat (mit einer Adresse aus dem 10.0.0.x-Netz) im eigenen lokalen Netz gesucht, die Anfrage gelangt gar nicht bis zum Gateway.

Mit dem N:N-Mapping werden alle Adressen des LANs für die Kopplung mit dem anderen Netz in einen neuen Adresskreis übersetzt. Das Netz der Firma A wird z. B. auf die 192.168.1.x umgesetzt, das Netz der Firma B auf 192.168.2.x. Unter diesen neuen Adressen sind die beiden LANs nun für das jeweils andere Netz erreichbar. Die Station aus dem Netz der Firma A spricht den Server 1 der Firma B nun unter der Adresse 192.168.2.1 an. Der Adressat liegt nun nicht mehr im eigenen Netz, die Anfrage wird an das Gateway weitergeleitet und das Routing in das andere Netz funktioniert wie gewünscht.

6.11.1.2 Fernwartung und -überwachung von Netzwerken

Der Fernwartung und -überwachung von Netzwerken kommt durch die Möglichkeiten von VPN immer größere Bedeutung zu. Mit der Nutzung der fast flächendeckend vorhandenen Breitband-Internetanschlüsse kann sich der Administrator

von solchen Management-Szenarien unabhängig machen von den unterschiedlichen Datenübertragungstechnologien oder teuren Standleitungen.



In diesem Beispiel überwacht ein Dienstleister von einer Zentrale aus die Netzwerke verschiedener Kunden. Zu diesem Zweck sollen die SNMP-fähigen Geräte die entsprechenden Traps über wichtige Ereignisse automatisch an den SNMP-Trap-Empfänger (z. B. LANmonitor) im Netz des Dienstleisters senden. Der Administrator im LAN des Dienstleisters hat damit jederzeit einen aktuellen Überblick über den Zustand der Geräte.

Die einzelnen Netze können dabei sehr unterschiedlich aufgebaut sein: Die Kunden A und B binden ihre Filialen mit eigenen Netzwerken über VPN-Verbindungen in ihr LAN ein, Kunde C betreibt ein Netz mit mehreren öffentlichen WLAN-Basisstationen als Hot-Spots und Kunde D hat in seinem LAN u. a. einen weiteren Router.

Die Netze der Kunden A und B in der jeweiligen Zentrale und den angeschlossenen Filialen nutzen verschiedene Adresskreise. Zwischen diesen Netzen ist also eine normale Netzwerkkopplung über VPN möglich.

Um den Aufwand zu vermeiden, zu jedem einzelnen Subnetz der Kunden A und B einen eigenen VPN-Tunnel aufzubauen, stellt der Dienstleister nur eine VPN-Verbindung zur Zentrale her und nutzt für die Kommunikation mit den Filialen die ohnehin vorhandenen VPN-Leitungen zwischen der Zentrale und den Filialen.

Die Traps aus den Netzen melden dem Dienstleister, ob z. B. ein VPN-Tunnel auf- oder abgebaut wurde, ob ein User sich dreimal mit dem falschen Passwort einloggen wollte, ob sich ein User an einem Hot-Spot angemeldet hat oder ob irgendwo ein LAN-Kabel aus einem Switch gezogen wurde.

Eine komplette Liste aller SNMP-Traps, die vom Gerät unterstützt werden, finden Sie im Anhang dieses Referenz-Handbuchs.

Das Routing dieser unterschiedlichen Netzwerke stößt dabei sehr schnell an seine Grenzen, wenn zwei oder mehrere Kunden gleiche Adresskreise verwenden. Wenn zusätzlich noch einige Kunden den gleichen Adressbereich nutzen wie der Dienstleister selbst, kommen weitere Adresskonflikte hinzu. In diesem Beispiel hat z. B. einer der Hot-Spots von Kunde C die gleiche Adresse wie das Gateway des Dienstleisters.

Für die Lösung dieser Adresskonflikte gibt es zwei verschiedene Varianten:

- Bei der dezentralen Variante werden den zu überwachenden Geräten per 1:1-Mapping jeweils alternative IP-Adressen für die Kommunikation mit dem SNMP-Empfänger zugewiesen. Diese Adresse ist in der Fachsprache auch als "Loopback-Adresse" bekannt, die Methode wird entsprechend als "Loopback-Verfahren" bezeichnet.

  Die Loopback-Adressen gelten jeweils nur für die Kommunikation mit bestimmten Gegenstellen auf den zugehörigen Verbindungen. Ein Gerät ist damit nicht generell unter dieser IP-Adresse erreichbar.
- Eleganter ist die Lösung des zentralen Mappings: statt jedes einzelne Gateway in den Filialnetzen zu konfigurieren, stellt der Administrator hier die Adressumsetzung im Gateway der Zentrale ein. Dabei werden automatisch auch alle "hinter" der Zentrale liegenden Subnetze mit den erforderlichen neuen IP-Adressen versorgt.

In diesem Beispiel wählt der Administrator des Dienstleisters für das Netz des Kunden B die zentrale Adressumsetzung auf 10.2.x.x, damit die beiden Netze mit eigentlich gleichen Adresskreisen für das Gateway des Dienstleisters wie zwei verschiedene Netz erscheinen.

Für die Kunden C und D wählt er die Adresskreise 192.168.2.x und 192.168.3.x, damit diese Netze sich in ihren Adressen von dem eigenen Netz des Dienstleisters unterscheiden.

Damit das Gateway des Dienstleisters die Netze der Kunden C und D ansprechen kann, richtet er auch für das eigene Netz eine Adressumsetzung auf 192.168.1.x ein.

6.11.2 Konfiguration

6.11.2.1 Einrichten der Adressumsetzung

Die Konfiguration des N:N-Mappings gelingt mit recht wenigen Informationen. Da ein LAN durchaus mit mehreren anderen Netzen per N:N gekoppelt werden kann, können für einen Quell-IP-Bereich bei verschiedenen Zielen auch unterschiedliche Adressumsetzungen gelten. In der NAT-Tabelle können maximal 64 Einträge vorgenommen werden, die folgende Informationen beinhalten:

- **Index**: Eindeutiger Index des Eintrags.
- **Quell-Adresse**: IP-Adresse des Rechners oder Netzes, dass eine alternative IP-Adresse erhalten soll.
- **Quell-Maske**: Netzmaske des Quell-Bereiches.
- **Gegenstelle**: Name der Gegenstelle, über die das entfernte Netzwerk erreicht werden kann.
- **Neue Netz-Adresse**: IP-Adresse oder -Adressbereich, der für die Umsetzung verwendet werden soll.

Für die neue Netzadresse wird jeweils die gleiche Netzmaske verwendet, die auch schon die Quell-Adresse verwendet. Für die Zuordnung von Quell- und Mapping-Adresse gelten folgende Hinweise:

- Bei der Umsetzung von einzelnen Adressen können Quelle und Mapping beliebig zugeordnet werden. So kann z. B. dem Server im LAN mit der IP-Adresse 10.1.1.99 die Mapping-Adresse 192.168.1.88 zugewiesen werden.
- Bei der Umsetzung von ganzen Adressbereichen wird der rechnerbezogene Teil der IP-Adresse direkt übernommen und nur an den netzbezogenen Teil der Mapping-Adresse angehängt. Bei einer Zuweisung von 10.0.0.0/255.255.255.0 nach 192.168.1.0 wird also dem Server im LAN mit der IP-Adresse 10.1.1.99 zwangsweise die Mapping-Adresse 192.168.1.99 zugewiesen.

Der Adressbereich für die Umsetzung muss mindestens so groß sein wie der Quell-Adressbereich.

Bitte beachten Sie, dass die Funktionen des N:N-Mapping nur wirksam sind, wenn die Firewall eingeschaltet ist!

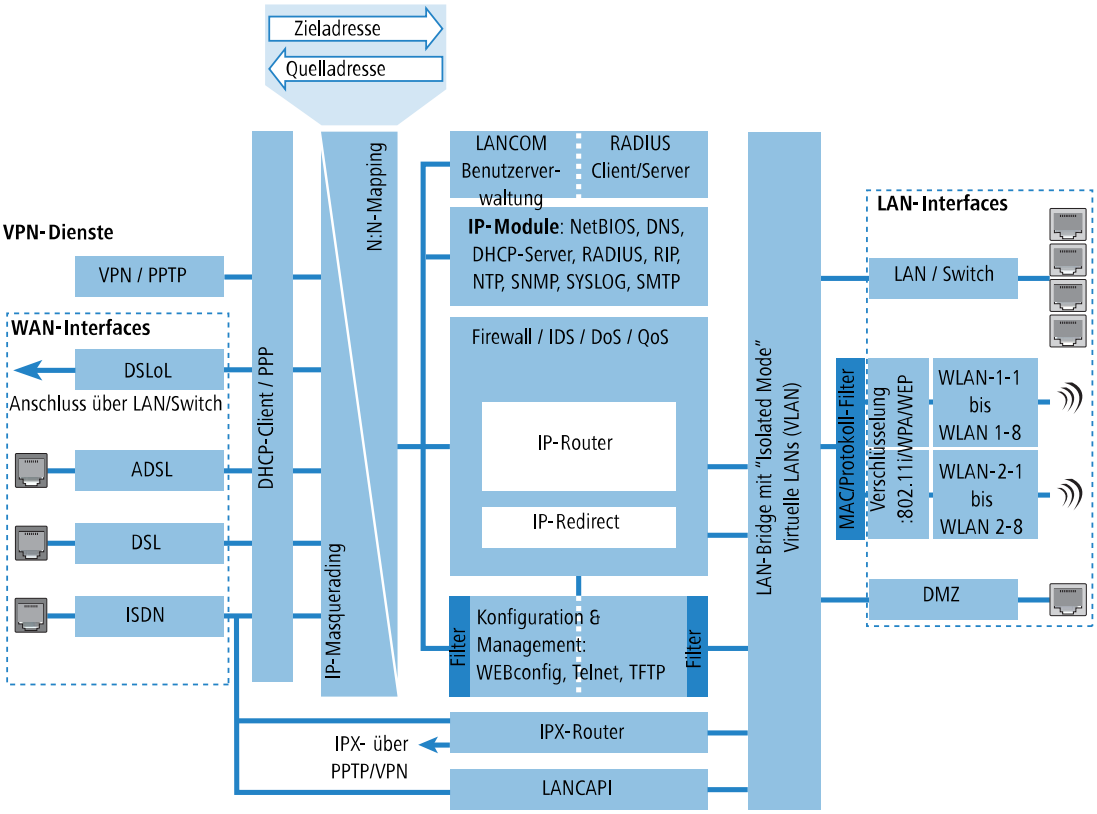
6.11.2.2 Zusätzliche Konfigurationshinweise

Mit dem Einrichten der Adressumleitung in der NAT-Tabelle werden die Netze und Rechner zunächst nur unter einer anderen Adresse im übergeordneten Netzverbund sichtbar. Für das einwandfreie Routing der Daten zwischen den Netzen sind aber noch einige weitere Einstellungen notwendig:

- Einträge in den Routing-Tabellen, damit die Pakete mit den neuen Adressen auch den Weg zum Ziel finden.

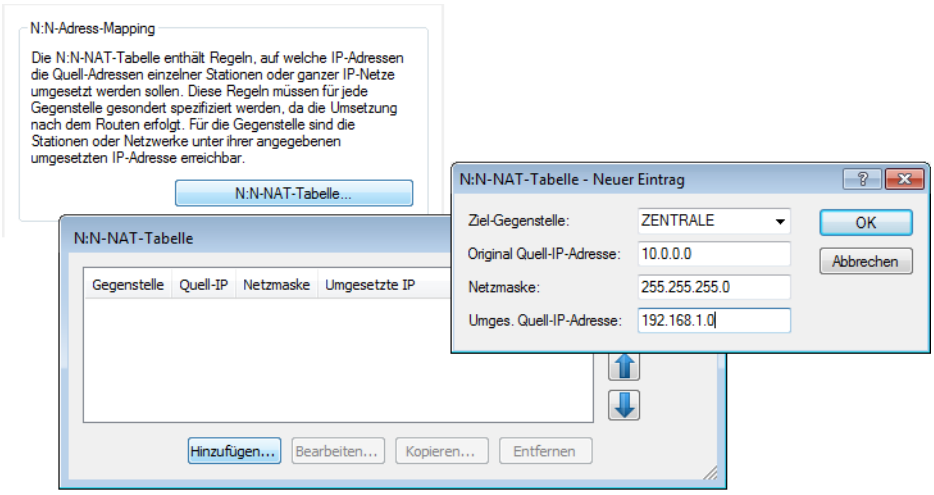
- DNS-Forwarding-Einträge, damit die Anfragen nach bestimmten Geräten in den jeweils anderen Netzen in die gemappten IP-Adressen aufgelöst werden können.
- Die Regeln der Firewalls in den Gateways müssen so angepasst werden, dass ggf. auch der Verbindungsaufbau von außen von den zulässigen Stationen bzw. Netzwerken her erlaubt ist.
- VPN-Regeln für Loopback-Adressen, damit die neu zugewiesenen IP-Adressen auch durch die entsprechenden VPN-Tunnel übertragen werden können.

Die Umsetzung der IP-Adressen findet im Gerät zwischen Firewall und IP-Router auf der einen Seite und dem VPN-Modul auf der anderen Seite statt. Alle Regeln, die sich auf das eigene lokale Netz beziehen, verwenden daher die "ungemappten", originalen Adressen. Die Einträge für das entfernte Netz nutzen also die "gemappten" Adressen der Gegenseite, die auf der VPN-Strecke gültig sind.



6.11.2.3 Konfiguration mit den verschiedenen Tools

Unter LANconfig stellen Sie die Adressumsetzung unter **IP-Router** > **N:N-Mapping** ein:



Konsole: **Setup** > **IP-Router** > **NAT-Tabelle**

6.12 Verbindungsaufbau mit PPP

Geräte von LANCOM unterstützen auch das Point-to-Point Protocol (PPP). PPP ist ein Sammelbegriff für eine ganze Reihe von WAN-Protokollen, die das Zusammenspiel von Routern verschiedener Hersteller erleichtern, denn dieses Protokoll wird von fast allen Herstellern unterstützt.

Und gerade weil das PPP nicht einer bestimmten Betriebsart der Router zugeordnet werden kann und natürlich auch wegen der großen und in Zukunft noch weiter steigenden Bedeutung dieser Protokoll-Familie, möchten wir Ihnen die Funktionen der Geräte im Zusammenhang mit dem PPP hier in einem eigenen Abschnitt vorstellen.

6.12.1 Das Protokoll

6.12.1.1 Was ist PPP?

Das Point-to-Point Protocol (PPP) wurde speziell für Netzwerkverbindungen über serielle Kanäle (auch ISDN, DSL u. ä.) entwickelt und hat sich als Standard für Verbindungen zwischen Routern behauptet. Es realisiert folgende Funktionen:

- Passwortschutz nach PAP, CHAP oder MS-CHAP
- Rückruf-Funktionen
- Aushandlung der über die aufgebaute Verbindung zu benutzenden Netzwerkprotokolle (z. B. IP). Dazu gehören auch für diese Protokolle notwendige Parameter wie z. B. IP-Adressen. Diese Verhandlung läuft über das Protokoll IPCP (IP Control Protocol) ab.
- Aushandeln von Verbindungsparametern wie z. B. der MTU (Maximum Transmission Unit, *Manuelle Definition der MTU* auf Seite 468).
- Überprüfung der Verbindung mit dem LCP (Link Control Protocol)

Für Router-Verbindungen ist PPP der Standard für die Kommunikation zwischen Geräten bzw. der WAN-Verbindungssoftware unterschiedlicher Hersteller. Um eine erfolgreiche Datenübertragung nach Möglichkeit sicherzustellen, erfolgt die Verhandlung der Verbindungsparameter und eine Einigung auf einen gemeinsamen Nenner über standardisierte Steuerungsprotokolle (z. B. LCP, IPCP, CCP), die im PPP enthalten sind.

6.12.1.2 Wozu wird PPP verwendet?

Das Point-to-Point Protocol wird bei folgenden Anwendungen sinnvoll eingesetzt:

- aus Kompatibilitätsgründen z. B. bei Kommunikation mit Fremdroutern
- Access (mit der Übermittlung von Adressen)

Das im Gerät implementierte PPP kann synchron oder asynchron sowohl über eine transparente HDLC-Verbindung als auch über eine X.75-Verbindung verwendet werden.

6.12.1.3 Die Phasen einer PPP-Verhandlung

Der Verbindungsaufbau über PPP startet immer mit einer Verhandlung der Parameter, die für die Verbindung verwendet werden sollen. Diese Verhandlung läuft in vier Phasen ab, deren Kenntnis für die Konfiguration und Fehlersuche wichtig sind.

- Establish-Phase

  Nach einem Verbindungsaufbau über den Datenkommunikationsteil startet die Aushandlung der Verbindungsparameter über das LCP.

  Es wird festgestellt, ob die Gegenstelle auch bereit ist, PPP zu benutzen, die Paketgrößen und das Authentifizierungsprotokoll (PAP, CHAP, MS-CHAP oder keines) werden festgelegt. Danach wechselt das LCP in den Opened-Zustand.

- Authenticate-Phase

  Falls notwendig, werden danach die Passworte ausgetauscht. Bei Authentifizierung nach PAP wird das Passwort nur einmalig übertragen. Bei Benutzung von CHAP oder MS-CHAP wird ein verschlüsseltes Passwort periodisch in einstellbaren Abständen gesendet.

  Evtl. wird in dieser Phase auch ein Rückruf über CBCP (Callback Control Protocol) ausgehandelt.

- Network-Phase

  Im Gerät ist das Protokoll IPCP implementiert.

  Nach erfolgreicher Übertragung des Passwortes kann das Netzwerk-Layer IPCP aufgebaut werden.

  Ist die Verhandlung der Parameter erfolgreich verlaufen, können von dem Router-Modul IP-Pakete auf der geöffneten (logischen) Leitung übertragen werden.

- Terminate-Phase

  In der letzten Phase wird die Leitung geschlossen, wenn die logischen Verbindungen für alle Protokolle abgebaut sind.

6.12.1.4 Die PPP-Verhandlung im Gerät

Der Verlauf einer PPP-Verhandlung wird in der PPP-Statistik der Geräte protokolliert und kann im Fehlerfall mit Hilfe der dort detailliert gezählten Protokoll-Pakete überprüft werden.

Eine weitere Analyse-Möglichkeit bieten die PPP-Trace-Ausgaben. Mit dem Befehl

```
trace + ppp
```

kann die Ausgabe der ausgetauschten PPP-Protokoll-Frames innerhalb einer Terminal-Sitzung gestartet werden. Wird diese Terminal-Sitzung in einem Log-File protokolliert, kann nach Abbruch der Verbindung eine detaillierte Analyse erfolgen.

6.12.2 Alles o.k.? Leitungsüberprüfung mit LCP

Beim Verbindungsaufbau über PPP handeln die beteiligten Geräte ein gemeinsames Verhalten während der Datenübertragung aus. Sie entscheiden z. B. zunächst, ob mit den Einstellungen der Sicherungsverfahren, Namen und Passwörter überhaupt eine Verbindung zustande kommen darf.

Wenn die Verbindung einmal steht, kann mit Hilfe des LCPs die Zuverlässigkeit der Leitung ständig überprüft werden. Innerhalb des Protokolls geschieht dies mit dem LCP-Echo-Request und dem zugehörigen LCP-Echo-Reply. Der LCP-Echo-Request ist eine Anfrage in Form eines Datenpakets, das neben den reinen Nutzdaten zur Gegenstelle übertragen wird. Wenn auf diese Anfrage eine gültige Antwort (LCP-Echo-Reply) zurückgeschickt wird, ist die Verbindung zuverlässig und stabil. Zur dauerhaften Überprüfung der Verbindung wird dieser Request in bestimmten Abständen wiederholt.

Was passiert nun, wenn der Reply ausbleibt? Zuerst werden einige Wiederholungen der Anfrage gestartet, um kurzfristige Störungen der Leitung auszuschließen. Wenn alle diese Wiederholungen unbeantwortet bleiben, wird die Leitung abgebaut und ein Ersatzweg gesucht.

Beim Remote Access von einzelnen Arbeitsplatzrechnern mit Windows-Betriebssystem empfehlen wir, die regelmäßigen LCP-Anfragen des Geräts auszuschalten, weil diese Betriebssysteme die LCP-Echo-Requests nicht beantworten und die Verbindung dadurch abgebaut würde.

Das Verhalten der LCP-Anfragen stellen Sie in der PPP-Liste für jede Verbindung einzeln ein. Mit dem Eintrag in die Felder 'Zeit' und 'Wdh.' legen Sie fest, in welchen Abständen die LCP-Anfrage gestellt werden soll und wie viele Wiederholungen beim Ausbleiben der Antwort gestartet werden, bis die Leitung als gestört bezeichnet werden darf. Mit einer Zeit von '0' und '0' Wiederholungen stellen Sie die LCP-Requests ganz ab.

6.12.3 Zuweisung von IP-Adressen über PPP

Zur Verbindung von Rechnern, die TCP/IP als Netzwerkprotokoll einsetzen, benötigen alle Beteiligten eine gültige und eindeutige IP-Adresse. Wenn nun eine Gegenstelle keine eigene IP-Adresse hat (z. B. der einzelne Arbeitsplatzrechner eines Teleworkers), dann kann das Gerät ihm für die Dauer der Verbindung eine IP-Adresse zuweisen und so die Kommunikation ermöglichen.

Diese Art der Adresszuweisung wird während der PPP-Verhandlung durchgeführt und nur für Verbindungen über das WAN eingesetzt. Die Zuweisung von Adressen mittels DHCP wird dagegen (normalerweise) innerhalb eines lokalen Netzwerks verwendet.

Die Zuweisung einer IP-Adresse wird nur dann möglich, wenn das Gerät die Gegenstelle beim Eintreffen des Anrufs über die Rufnummer oder den Namen identifizieren kann, d. h. die Authentifizierung erfolgreich war.

6.12.3.1 Beispiele

› Remote Access

Die Zuweisung der Adresse wird durch einen speziellen Eintrag in der IP-Routing-Tabelle ermöglicht. Neben dem Eintrag der IP-Adresse, die der Gegenstelle aus dem Feld 'Router-Name' zugewiesen werden soll, wird als Netzmaske die 255.255.255.255 angegeben. Der Routername ist in diesem Fall der Name, mit dem sich die Gegenstelle beim Gerät anmelden muss.

Neben der IP-Adresse werden der Gegenstelle bei dieser Konfiguration auch die Adressen der DNS-Server (Domain Name Server) inkl. des Backup-Servers aus den Einträgen im TCP/IP-Modul übermittelt.

Damit das Ganze funktioniert, muss die Gegenstelle natürlich auch so eingestellt sein, dass sie die IP-Adresse und die Namensserver vom Gerät bezieht. Das geschieht z. B. im DFÜ-Netzwerk von Windows durch die Einträge in den 'TCP-Einstellungen' unter 'IP-Adresse' bzw. 'DNS-Konfiguration'. Hier werden die Optionen 'Vom Server zugewiesene IP-Adresse' und 'Vom Server zugewiesene Namensserveradressen' aktiviert.

› Internet-Zugang

Wird über das Gerät der Zugang zum Internet für ein lokales Netz realisiert, kann die Zuweisung von IP-Adressen den umgekehrten Weg nehmen. Hierbei sind Konfigurationen möglich, in denen das Gerät selbst keine im Internet gültige IP-Adresse hat und sich für die Dauer der Verbindung eine vom Internet-Provider zuweisen lässt. Neben der IP-Adresse erhält das Gerät während der PPP-Verhandlung auch Informationen über DNS-Server beim Provider.

Im lokalen Netz ist das Gerät nur mit seiner intern gültigen Intranet-Adresse bekannt. Alle Arbeitsplatzrechner im lokalen Netz können dann auf den gleichen Internet-Account zugreifen und auch z. B. den DNS-Server erreichen.

Die zugewiesenen Adressen schauen sich Windows-Anwender per LANmonitor an. Neben dem Namen der verbundenen Gegenstelle finden Sie hier die aktuelle IP-Adresse sowie die Adressen von DNS-Servern. Auch Optionen wie die Kanalbündelung oder die Dauer der Verbindung werden angezeigt.

6.12.4 Einstellungen in der PPP-Liste

In der PPP-Liste können Sie für jede Gegenstelle, die mit Ihrem Netz Kontakt aufnimmt, eine eigene Definition der PPP-Verhandlung festlegen.

Darüberhinaus können Sie festlegen, ob die Datenkommunikation über eine IPv4- oder eine IPv6-Verbindung erfolgen soll.

Zur Authentifizierung von Point-to-Point-Verbindungen im WAN wird häufig eines der Protokolle PAP, CHAP, MSCHAP oder MSCHAPv2 eingesetzt. Dabei haben die Protokolle untereinander eine „Hierarchie", d. h. MSCHAPv2 ist ein „höheres" Protokoll als, MSCHAP, CHAP und PAP (höhere Protokolle zeichnen sich durch höhere Sicherheit aus). Manche Einwahlrouter bei den Internetprovidern erlauben vordergründig die Authentifizierung über ein höheres Protokoll wie CHAP, unterstützen im weiteren Verlauf aber nur die Nutzung von PAP. Wenn im Gerät das Protokoll für die Authentifizierung fest eingestellt ist, kommt die Verbindung ggf. nicht zustande, da kein gemeinsames Authentifizierungsprotokoll ausgehandelt werden kann.



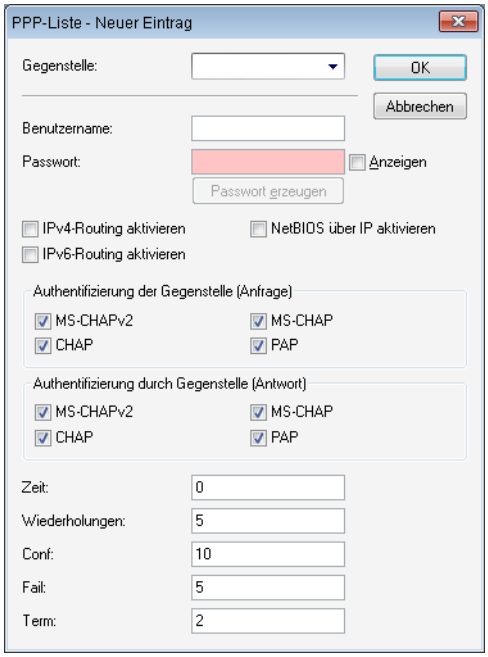
Prinzipiell ist es möglich, während der Verbindungsaushandlung eine erneute Authentifizierung durchzuführen und dafür ein anderes Protokoll auszuwählen, wenn dies zum Beispiel erst durch den Usernamen erkannt werden konnte. Diese erneute Aushandlung wird aber nicht in allen Szenarien unterstützt. Insbesondere bei der Einwahl über UMTS muss daher explizit vom Gerät der Wunsch von der Providerseite nach CHAP abgelehnt werden, um für eine Weiterleitung der Anfragen beim Provider PAP-Userdaten bereitstellen zu können.

Mit der flexiblen Einstellung der Authentifizierungsprotokolle im Gerät wird sichergestellt, dass die PPP-Verbindung wie gewünscht zustande kommt. Dazu können ein oder mehrere Protokolle definiert werden, die zur Authentifizierung von Gegenstellen im Gerät (eingehende Verbindungen) bzw. beim Login des Gerätes in andere Gegenstellen (ausgehende Verbindungen) akzeptiert werden.

- Das Gerät fordert beim Aufbau eingehender Verbindungen das niedrigste der zulässigen Protokolle, lässt aber je nach Möglichkeit der Gegenstelle auch eines der höheren (im Gerät aktivierten) Protokolle zu.
- Das Gerät bietet beim Aufbau ausgehender Verbindungen alle aktivierten Protokolle an, lässt aber auch nur eine Auswahl aus genau diesen Protokollen zu. Das Aushandeln eines der nicht aktivierten, evtl. höheren Protokolle ist nicht möglich.

Die Einstellung der PPP-Authentifizierungsprotokolle finden Sie in der PPP-Liste.

LANconfig: **Kommunikation** > **Protokolle** > **PPP-Liste**



Gegenstelle

Geben Sie hier den Namen der Gegenstelle ein. Dieser Name muss mit einem Eintrag in der Liste der Gegenstellen übereinstimmen. Sie können auch direkt einen Namen aus der Liste der Gegenstellen auswählen.

Bei der PPP-Verhandlung meldet sich die einwählende Gegenstelle mit ihrem Namen beim Gerät an. Anhand des Namens kann das Gerät aus der PPP-Tabelle die zulässigen Werte für die Authentifizierung entnehmen. Manchmal kann die Gegenstelle bei Verhandlungsbeginn nicht über IP-Adresse (PPTP-Einwahl) oder MAC-Adresse (PPPoE-Einwahl) identifiziert werden, die zulässigen Protokolle können also im ersten Schritt nicht ermittelt werden. In diesen Fällen wird die Authentifizierung zunächst mit den Protokollen vorgenommen, die für die Gegenstelle mit dem Namen DEFAULT aktiviert sind. Wenn die Gegenstelle mit diesen Einstellungen erfolgreich authentifiziert wurde, können auch die für die Gegenstelle zulässigen Protokolle ermittelt werden. Wenn bei der Authentifizierung mit den unter DEFAULT eingetragenen Protokollen ein Protokoll verwendet wurde, das für die Gegenstelle nicht erlaubt ist, dann wird eine erneute Authentifizierung mit den erlaubten Protokollen durchgeführt.

Benutzername

Name, mit dem sich Ihr Gerät bei der Gegenstelle anmeldet. Ist hier kein Eintrag vorhanden, wird der Name Ihres Gerätes verwendet.

Passwort

Passwort, das von Ihrem Gerät an die Gegenstelle übertragen wird (falls gefordert). Ein '*' in der Liste zeigt an, dass ein Eintrag vorhanden ist.

IPv4-Routing aktivieren

Aktiviert IPv4-Routing für diese Gegenstelle.

IPv6-Routing aktivieren

Aktiviert IPv6-Routing für diese Gegenstelle.

Authentifizierung der Gegenstelle (Anfrage)

Wählen Sie hier die Sicherungsverfahren aus, mit denen sich eine Gegenstelle bei Ihrem Router authentifizieren kann. Mindestens eines der ausgewählten Sicherungsverfahren muss von der Gegenstelle erfüllt werden. Diese Auswahl wird zum Beispiel bei der lokalen Einwahl benötigt.

Wenn die Gegenstelle ein Internetprovider ist, den Ihr Router anrufen soll, sollten Sie hier **kein** Verfahren selektieren.

Wenn mehr als ein Verfahren selektiert ist, werden sie der Reihe nach zur Authentifizierung herangezogen, bis eines erfolgreich von der Gegenstelle beantwortet werden kann.

Authentifizierung durch Gegenstelle (Antwort)

Wählen Sie hier die Sicherungsverfahren aus, mit denen sich Ihr Router bei der Einwahl authentifizieren darf.

Wenn die Gegenstelle ein Internetprovider ist, den Ihr Router anrufen soll, sollten Sie hier **alle** Verfahren selektieren.

Wenn keines der Verfahren selektiert ist, wird **keine** lokale Authentifizierung gegenüber dieser Gegenstelle akzeptiert.

Zeit

Zeit zwischen zwei Überprüfungen der Verbindung mit LCP (siehe auch LCP). Diese Zeit geben Sie in Vielfachen von 10 Sekunden ein (also z. B. 2 für 20 Sekunden). Der Wert ist gleichzeitig die Zeit zwischen zwei Überprüfungen der Verbindung nach CHAP. Diese Zeit geben Sie in Minuten ein. Für Gegenstellen mit Windows-Betriebssystem muss die Zeit auf 0 gesetzt werden!

Mit dem Wert **0** wird das LCP-Polling deaktiviert.

Wiederholungen

Anzahl der Wiederholungen für den Überprüfungsversuch. Mit mehreren Wiederholungen schalten Sie den Einfluss kurzfristiger Leitungsstörungen aus. Erst wenn alle Versuche erfolglos bleiben, wird die Verbindung abgebaut. Der zeitliche Abstand zwischen zwei Wiederholungen beträgt 1/10 der Zeit zwischen zwei Überprüfungen.

Conf

Mit diesem Parameter wird die Arbeitsweise des PPPs beeinflusst. Der Parameter ist in der RFC 1661 definiert und wird hier nicht näher beschrieben. Falls Sie keine PPP-Verbindungen aufbauen können, finden Sie in dieser RFC im Zusammenhang mit der PPP-Statistik des Routers Hinweise zur Behebung der Störung. Im Allgemeinen sind die Default-Einstellungen ausreichend.

Fail

Mit diesem Parameter wird die Arbeitsweise des PPPs beeinflusst. Der Parameter ist in der RFC 1661 definiert und wird hier nicht näher beschrieben. Falls Sie keine PPP-Verbindungen aufbauen können, finden Sie in diesem RFC im Zusammenhang mit der PPP-Statistik des Routers Hinweise zur Behebung der Störung. Im Allgemeinen sind die Default-Einstellungen ausreichend.

Term

Mit diesem Parameter wird die Arbeitsweise des PPPs beeinflusst. Der Parameter ist in der RFC 1661 definiert und wird hier nicht näher beschrieben. Falls Sie keine PPP-Verbindungen aufbauen können, finden Sie in diesem RFC im Zusammenhang mit der PPP-Statistik des Routers Hinweise. Im Allgemeinen sind die Default-Einstellungen ausreichend.

6.12.5 Die Bedeutung der DEFAULT-Gegenstelle

Bei der PPP-Verhandlung meldet sich die einwählende Gegenstelle mit ihrem Namen beim Gerät an. Anhand des Namens kann das Gerät aus der PPP-Tabelle die zulässigen Werte für die Authentifizierung entnehmen. Manchmal kann die Gegenstelle bei Verhandlungsbeginn nicht über IP-Adresse (PPTP-Einwahl) oder MAC-Adresse (PPPoE-Einwahl) identifiziert werden, die zulässigen Protokolle können also im ersten Schritt nicht ermittelt werden. In diesen Fällen wird die Authentifizierung zunächst mit den Protokollen vorgenommen, die für die Gegenstelle mit dem Namen DEFAULT aktiviert sind. Wenn die Gegenstelle mit diesen Einstellungen erfolgreich authentifiziert wurde, können auch die für die Gegenstelle zulässigen Protokolle ermittelt werden.

Wenn bei der Authentifizierung mit den unter DEFAULT eingetragenen Protokollen ein Protokoll verwendet wurde, das für die Gegenstelle nicht erlaubt ist, dann wird eine erneute Authentifizierung mit den erlaubten Protokollen durchgeführt.

6.12.6 RADIUS-Authentifizierung von PPP-Verbindungen

PPP-Verbindungen können auch über einen externen RADIUS-Server authentifiziert werden. Diese externen RADIUS-Server unterstützen jedoch nicht unbedingt alle verfügbaren Protokolle. Bei der Konfiguration der RADIUS-Authentifizierung können daher auch die zulässigen Protokolle ausgewählt werden. Die LCP-Verhandlung wird mit den erlaubten Protokollen neu gestartet, wenn der RADIUS-Server das ausgehandelte Protokoll nicht unterstützt.

6.12.6.1 WAN-RADIUS-Tabelle

LANconfig: **Kommunikation** > **RADIUS**



Konsole: **Setup** > **WAN** > **RADIUS**

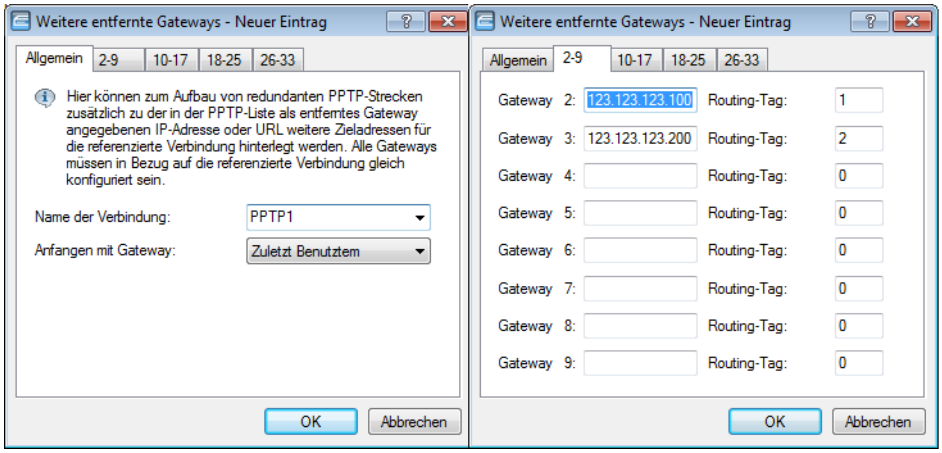
6.12.7 32 zusätzliche Gateways für PPTP-Verbindungen

6.12.7.1 Einleitung

Zur Sicherung der Erreichbarkeit können für jede PPTP-Gegenstelle bis zu 32 zusätzliche Gateways konfiguriert werden, so dass insgesamt pro PPTP-Gegenstelle 33 Gateways genutzt werden können.

6.12.7.2 Konfiguration

Die zusätzlichen PPTP-Gateways weden in einer separaten Liste definiert.



LANconfig: **Kommunikation** > **Gegenstellen** > **PPTP** > **Weitere entfernte Gateways**

Konsole: **Setup** > **WAN** > **Zusaetzliche-PPTP-Gateways**

Name der Verbindung

Wählen Sie hier aus, für welche PPTP-Gegenstelle dieser Eintrag gelten soll.

Mögliche Werte:

- Auswahl aus der Liste der definierten PPTP-Gegenstellen.

Default:

- leer

Anfangen mit

Wählen Sie hier aus, in welcher Reihenfolge die Einträge versucht werden sollen.

Mögliche Werte:

- Zuletzt benutztem: Wählt den Eintrag, zu dem zuletzt erfolgreich eine Verbindung hergestellt werden konnte.
- Erstem: Wählt den ersten Eintrag aus allen konfigurierten Gegenstellen aus.
- Zufall: Wählt zufällig eine der konfigurierten Gegenstellen aus. Mit dieser Einstellung erreichen Sie ein effektives Load-Balancing für die Gateways in der Zentrale.

Default:

- Zuletzt benutztem

Gateway 2 bis 33

Tragen Sie hier die IP-Adressen der zusätzlichen Gateways ein, die für diese PPTP-Gegenstelle verwendet werden können.

Mögliche Werte:

- IP-Adresse oder 63 alphanumerische Zeichen.

Default:

- leer

Routing-Tag

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen entfernten Gateway ermittelt wird.

Mögliche Werte:

› maximal 5 Ziffern.

Default:

› 0

Wenn Sie hier kein Routing-Tag angeben (d. h. das Routing-Tag ist 0), dann wird für den zugehörigen Gateway das in der PPTP-Verbindungsliste für diese Gegenstelle konfigurierte Routing-Tag verwendet.

6.13 DSL-Verbindungsaufbau mit PPTP

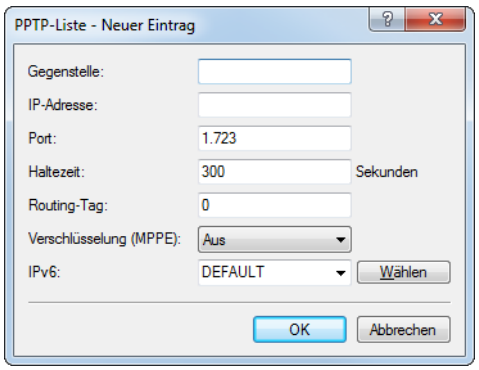
Einige DSL-Anbieter ermöglichen die Einwahl nicht über PPPoE, sondern über PPTP (**P**oint-to-**P**oint **T**unneling **P**rotocol). Bei PPTP handelt es sich um eine Protokoll-Erweiterung von PPP, die vorrangig von Microsoft entwickelt wurde.

PPTP ermöglicht es, „Tunnel" über IP-Netze zu einer Gegenstelle aufzubauen. Unter einem Tunnel versteht man eine logisch abgeschirmte Verbindung, die die übertragenen Daten vor dem unbefugten Zugriff Dritter schützen soll. Dazu wird der Verschlüsselungsalgorithmus RC4 eingesetzt.

6.13.1 Konfiguration von PPTP

Im Gerät werden alle notwendigen PPTP-Parameter vom Internet-Zugangs-Assistenten abgefragt, sobald der Internet-Zugang über PPTP ausgewählt wird. Zusätzlich zu den Eingaben, die auch beim normalen PPPoE-Zugang abgefragt werden, ist dabei nur die IP-Adresse des PPTP-Gateways anzugeben. Beim PPTP-Gateway handelt es sich zumeist um das DSL-Modem. Genauere Informationen stellt Ihnen Ihr DSL-Anbieter zur Verfügung.

Änderungen an der Konfiguration werden in der PPTP-Liste vorgenommen:



LANconfig: **Kommunikation** > **Gegenstellen** > **PPTP** > **PPTP-Liste**

Die PPTP-Konfiguration besteht aus folgenden Parametern:

Gegenstelle

Die Bezeichnung aus der Liste der DSL-Breitband-Gegenstellen.

IP-Adresse

IP-Adresse des PPTP-Gateways, zumeist die Adresse des DSL-Modems.

Port

IP-Port, über den das PPTP-Protokoll läuft. Dem Protokollstandard gemäß sollte immer Port '1.723' angegeben sein.

Haltezeit

Geben Sie an, nach wie vielen Sekunden die Verbindung zu dieser Gegenstelle getrennt werden soll, wenn in dieser Zeit keine Daten mehr übertragen worden sind. Wertebereich 0-3600 Sekunden.

Der Wert 9999 sorgt für einen sofortigen Verbindungsaufbau ohne zeitliche Begrenzung.

Routing-Tag

Routing-Tag für diesen Eintrag.

Verschlüsselung (MPPE)

Schlüssellänge der Verschlüsselung. Siehe auch *MPPE für PPTP-Tunnel* auf Seite 837

IPv6

Dieser Eintrag gibt den Namen der IPv6-WAN-Schnittstelle an. Ein leerer Eintrag schaltet IPv6 für dieses Interface ab. Die IPv6-Gegenstellen konfigurieren Sie unter **IPv6** > **Allgemein** > **WAN-Schnittstellen**.

6.14 Dauerverbindung für Flatrates – Keep-alive

Als Flatrates bezeichnet man pauschale Verbindungstarife, die nicht nach Verbindungszeiten, sondern pauschal für feste Perioden abgerechnet werden. Bei Flatrates lohnt sich der Verbindungsabbau nicht mehr. Im Gegenteil: Neue Mails sollen direkt am PC gemeldet werden, der Heimarbeitsplatz soll kontinuierlich mit dem Firmennetzwerk verbunden sein und man möchte für Freunde und Kollegen über Internet Messenger Dienste pausenlos erreichbar sein. Es ist also wünschenswert, dass Verbindungen ununterbrochen aufrechterhalten werden.

Beim Gerät sorgt das Keep-alive-Verfahren dafür, dass Verbindungen immer dann aufgebaut werden, wenn die Gegenstelle sie gekappt hat.

6.14.1 Konfiguration des Keep-alive-Verfahrens

Das Keep-alive-Verfahren wird in der Gegenstellenliste konfiguriert.

Wird die Haltezeit auf 0 Sekunden gesetzt, so wird die Verbindung nicht aktiv vom Gerät beendet. Der automatische Abbau von Verbindungen, über die längere Zeit keine Daten mehr übertragen wurden, wird mit einer Haltezeit von 0 Sekunden also deaktiviert. Durch die Gegenseite unterbrochene Verbindungen werden in dieser Einstellung allerdings nicht automatisch wiederhergestellt.

Bei einer Haltezeit von 9999 Sekunden wird die Verbindung nach jeder Trennung immer automatisch wieder neu aufgebaut. Ebenso wird die Verbindung nach dem Booten des Gerätes automatisch wieder aufgebaut ('auto reconnect').

6.15 Datenvolumen auf der WAN-Schnittstelle

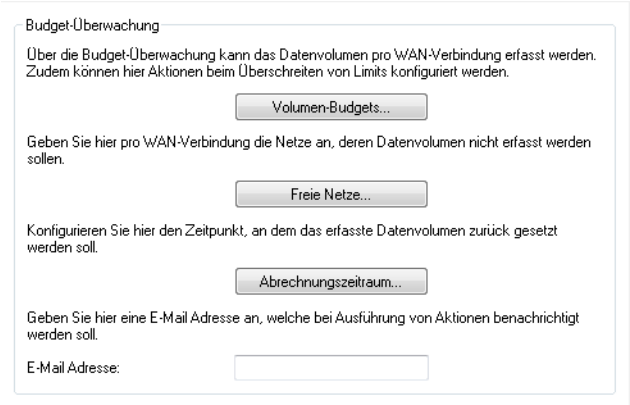
Mobilfunk- oder Festnetzanbieter können je nach Vertrag auch bei Flatrates ab einem bestimmten Datenvolumen eine Drosselung der Übertragungsrate aktivieren. Das Gerät erfasst das verbrauchte Datenvolumen je WAN-Schnittstelle, archiviert die Werte für bis zu 12 Monate und kann bei Erreichen eines festgelegten Grenzwertes Aktionen ausführen. Die Budgets gelten auch für VPN-, PPTP- oder alle weiteren Arten von Gegenstellen.

Beim Monatswechsel speichert das Gerät die Daten des abgelaufenen Monats in einer Archiv-Tabelle und setzt den Zähler des laufenden Monats auf Null zurück. Das aktuelle Datenvolumen sowie die im Archiv gespeicherten Daten können Sie über LANmonitor oder im Status-Menü von WEBconfig einsehen. Das Archiv beinhaltet immer Daten der letzten 12 Monate. Im 13. Monat überschreibt das Gerät automatisch die Archiv-Daten des 1. Monats.

6.15.1 Konfiguration von Datenvolumen-Budgets

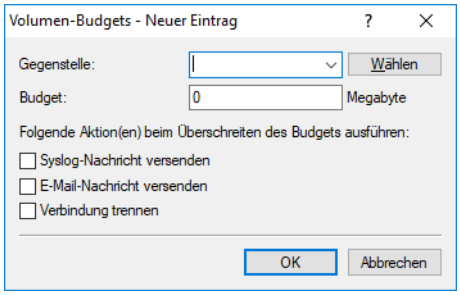
Der folgende Abschnitt beschreibt, wie Sie mit LANconfig die Datenvolumen für Gegenstellen verwalten.

1. Starten Sie LANconfig und öffnen Sie die Konfiguration des Gerätes, für das Sie die Erfassung des Datenvolumens einrichten wollen.
2. Wechseln Sie im Konfigurationsdialog in die Ansicht **Management** > **Budget**.



> Wenn das Gerät bei Überschreiten des festgelegten Datenvolumens eine E-Mail versenden soll (siehe Folgeschritt), geben Sie bereits in diesem Dialog im Feld **E-Mail Adresse** die entsprechende Adresse ein.

3. Klicken Sie auf die Schaltfläche **Volumen-Budgets** und anschließend auf **Hinzufügen**.



Im Feld **Gegenstelle** können Sie die Gegenstelle auswählen, für die Sie das Volumen-Budget angeben wollen. Mit **Wählen** können Sie aus den verfügbaren Gegenstellen auswählen bzw. neue Gegenstellen verwalten.

Geben Sie im Feld **Budget** das Datenvolumen an. Dieser Wert richtet sich meistens nach dem im Provider-Vertrag verhandelten Datenvolumen bis zur Drosselung der Übertragungsrate.

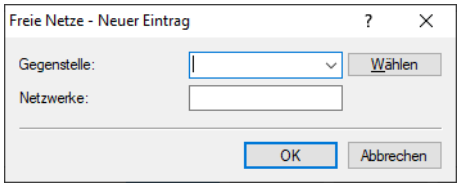
Sie können zusätzlich Aktionen definieren, die das Gerät bei Erreichen des Budgets ausführen soll:

- **Syslog-Nachricht versenden**: Das Gerät erzeugt bei Erreichen der Schwellenwerte 80% und 100% des Budgets eine Syslog-Nachricht (mit dem Flag "Critical"), die Sie im Syslog-Speicher des Gerätes, über LANmonitor oder einen speziellen Syslog-Client auswerten können.
- **E-Mail-Nachricht versenden**: Das Gerät verschickt bei Erreichen der Schwellenwerte 80% und 100% des Budgets eine Benachrichtigung an die E-Mail-Adresse, die Sie im Dialog weiter oben angegeben haben.
- **Verbindung trennen**: Das Gerät trennt die Verbindung zur Gegenstelle.

Die Aktion **Verbindung trennen** aktiviert die Gebührensperre. Das Gerät kann bis zum Ablauf des Monats keine Verbindung mehr zu dieser Gegenstelle aufbauen, wenn Sie nicht zuvor das Volumen-Budget für diese Gegenstelle erhöhen.

Sie können auch festlegen, dass das Gerät mehrere Aktionen ausführen soll. Ist die Aktion **Verbindung trennen** darunter, führt das Gerät diese Aktion als letzte aus.

4. Klicken Sie auf **OK**, um diesen Eintrag in die Tabelle aufzunehmen, und anschließend erneut auf **OK**, um alle Einträge in die Konfiguration des Gerätes zu übernehmen.
5. Wenn die Datenübertragung bestimmter Netze das Volumen-Budget zu einer Gegenstelle nicht belastet, können Sie diese Netze aus der Erfassung herausnehmen. Klicken Sie dazu auf die Schaltfläche **Freie Netze** und anschließend auf **Hinzufügen**.

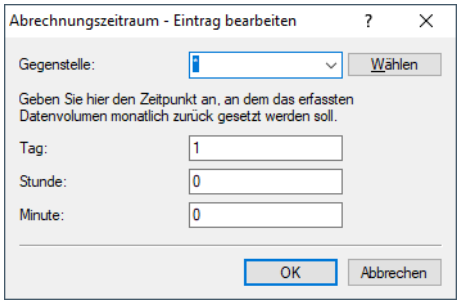


Im Feld **Gegenstelle** können Sie die Gegenstelle auswählen, für die Sie die Ausnahme angeben wollen. Mit **Wählen** können Sie aus den verfügbaren Gegenstellen auswählen bzw. neue Gegenstellen verwalten.

Sie können pro Gegenstelle auch mehrere Einträge vornehmen, indem Sie den Gegenstellennamen um das #-Zeichen und eine Ziffer erweitern (z. B. "INTERNET", "INTERNET#1", "INTERNET#2", ...). Das ist dann sinnvoll, wenn Sie explizit eine Ausnahme definieren möchten, die nur temporär aktiv ist. Sobald diese Ausnahme nicht mehr gültig ist, löschen Sie nur den Eintrag mit der entsprechend nummerierten Gegenstelle.

Im Feld **Netzwerke** können Sie IPv4- und IPv6-Adressen sowie ganze Netze in Prefix-Schreibweise (z. B. "192.168.1.0/24") angeben. Trennen Sie die einzelnen Einträge durch Komma. Auch hier können Sie die Gegenstellennamen um das #-Zeichen und eine Ziffer erweitern.

6. Klicken Sie auf **OK**, um diesen Eintrag in die Tabelle aufzunehmen, und anschließend erneut auf **OK**, um alle Einträge in die Konfiguration des Gerätes zu übernehmen.
7. Um festzulegen, wann das Gerät die monatliche Aufzeichnung von vorne beginnt, klicken Sie auf **Abrechnungszeitraum**.
8. Wenn Sie die Vorgabe ändern möchten, markieren Sie die Zeile mit der Gegenstellen-Bezeichnung "*" und klicken Sie auf die Schaltfläche **Bearbeiten**, ansonsten klicken Sie auf **Hinzufügen**.



Im Feld **Gegenstelle** können Sie die Gegenstelle auswählen, für die Sie den Intervall-Beginn festlegen wollen. Mit **Wählen** können Sie aus den verfügbaren Gegenstellen auswählen bzw. neue Gegenstellen verwalten.

Für den Gegenstellennamen können Sie auch Wildcards verwenden. Die Wildcard "*" gilt in diesem Fall für alle Gegenstellen.

In den Feldern **Tag**, **Stunde** und **Minute** bestimmen Sie, an welchem Tag im Monat und zu welcher Uhrzeit das Gerät das Budget für die angegebene Gegenstelle wieder zurücksetzt.

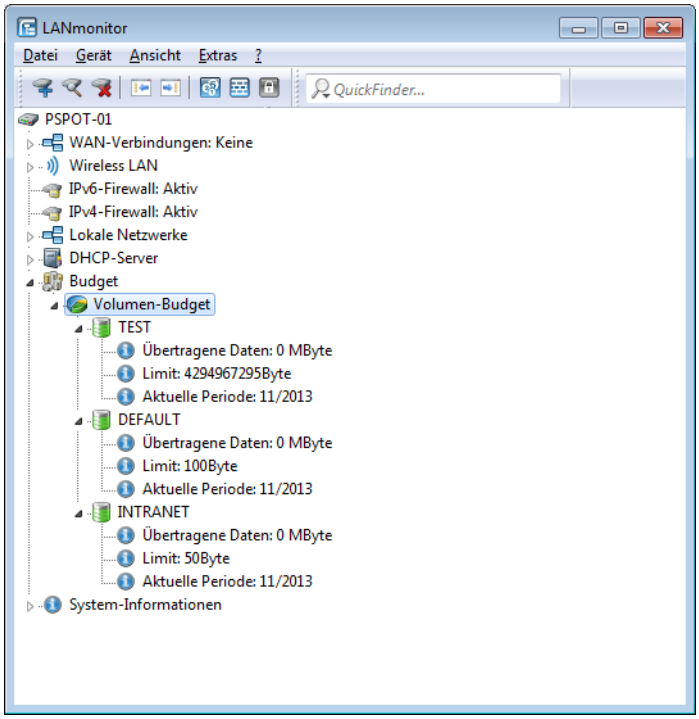
Standardmäßig setzt das Gerät am Monatsersten um 00:00 Uhr das Budget für alle Gegenstellen zurück.

Wenn Sie im Feld **Tag** den Wert "31" eingeben, setzt das Gerät das Budget in Monaten mit weniger Tagen (z. B. Februar oder November) nicht zurück.

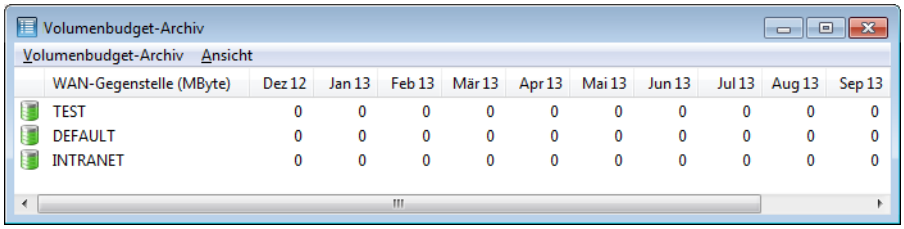
9. Klicken Sie auf **OK**, um diesen Eintrag in die Tabelle aufzunehmen, und anschließend erneut auf **OK**, um alle Einträge in die Konfiguration des Gerätes zu übernehmen.
10. Klicken Sie abschließend auf **OK**, um die Konfiguration ins Gerät zu laden.

6.15.2 Budget-Auswertung

Eingerichtete Volumen-Budgets lassen sich komfortabel mit LANmonitor im Zweig **Budget** auswerten und verwalten.

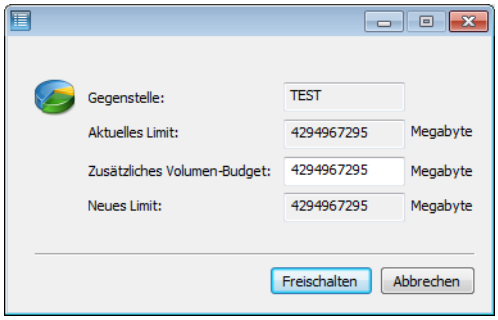


Mit einem Rechts-Klick auf **Volumen-Budget** können Sie alle angezeigten Volumen-Budgets zurücksetzen oder sich das Volumen-Budget-Archiv anzeigen lassen.



WAN-Gegenstelle (MByte)	Dez 12	Jan 13	Feb 13	Mär 13	Apr 13	Mai 13	Jun 13	Jul 13	Aug 13	Sep 13
TEST	0	0	0	0	0	0	0	0	0	0
DEFAULT	0	0	0	0	0	0	0	0	0	0
INTRANET	0	0	0	0	0	0	0	0	0	0

Mit einem Rechtsklick auf eine WAN-Schnittstelle können Sie das Budget für die entsprechende Schnittstelle zurücksetzen oder ein zusätzliches Volumen-Budget freischalten.



6.16 Manuelle Definition der MTU

Verschiedene Internet-Provider betreiben zwar einen eigenen Backbone, bedienen sich aber für die Einwahl ihrer Kunden der Zugangsknoten der Telekom. Dieses „zweistufige" Einwahlverfahren kann zu Problemen mit dem realisierten Datendurchsatz führen:

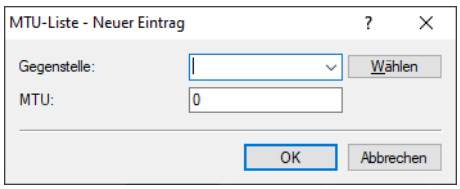
- Bei der Einwahl in den Knoten der Telekom handelt ein Gerät in der PPP-Verhandlung eine zulässige MTU aus, also die maximale Größe eines unfragmentierten Datenpakets. Diese MTU ergibt sich aus dem Minimum der Protokollparameter MRU (Maximum Receive Unit) des eigenen und entfernten Gerätes. Diese MTU wird dann von Seiten des Geräts auch verwendet.
- Bei der Weitergabe der Datenpakete an den Backbone des eigentlichen Providers wird ein zusätzlicher Header aufgeschlagen, die Datenpakete werden also noch einmal größer. Um nun trotzdem wieder in die erlaubte Größe zu passen, werden die Datenpakete fragmentiert, also in kleinere Teile aufgeteilt. Diese zusätzliche Fragmentierung kann zu Geschwindigkeitseinbußen in der Datenübertragung führen.

Um diese Problematik zu umgehen, kann für jede Gegenstelle eine feste MTU eingetragen werden.

6.16.1 Konfiguration

LANconfig: **Kommunikation** > **Protokolle** > **MTU-Liste**

Konsole: **Setup** > **WAN** > **MTU-Liste**



Gegenstelle

Geben Sie hier den Namen der Gegenstelle ein. Dieser Name muss mit einem Eintrag in der Liste der Gegenstellen übereinstimmen. Sie können auch direkt einen Namen aus der Liste der Gegenstellen auswählen.

Es können dabei die Wildcards „?" und „*" an beliebiger Stelle im Namen der Gegenstelle eingegeben werden. „?" steht für genau ein Zeichen. „*" steht für beliebig viele oder auch kein Zeichen. Die MTU-Liste wird dazu absteigend nach Länge des Gegenstellen-Namens und bei gleicher Länge absteigend in alphabetischer Ordnung sortiert. Dadurch stehen vollständige Namen immer vor Namen mit Wildcards.

MTU

Auf der Verbindung zu verwendende MTU.

6.16.2 Statistik

Unter **Status** > **WAN-Statistik** finden Sie die MTU-Statistik, in der für alle aktiven Verbindungen die verwendeten MTUs festgehalten werden. Diese Tabelle ist halbdynamisch und beginnt mit 16 Einträgen. Sie enthält wie die MTU-Liste unter **Setup** > **WAN** zwei Spalten in denen der Gegenstellen-Name und die MTU abgelegt werden.

Gegenstelle	MTU	Bemerkung
INET	1200	Die Gegenstelle INET ist die Internet-Verbindung und hat eine erzwungene MTU von 1200 Bytes.
MULTI	1492	MULTI ist eine PPPoE-Verbindung, auf der die MTU ausgehandelt wurde (daher beträgt sie 1492 Bytes).
TESTVPN	1100	TESTVPN ist eine VPN-Verbindung, die über die Internet-Verbindung aufgebaut wurde. Für VPN-Verbindungen wird ein fester Overhead von 100 Bytes angenommen, weshalb die MTU hier 1100 Bytes beträgt.
TESTVPN-PPTP	1060	TESTVPN-PPTP ist eine PPTP-Verbindung, die über die VPN-Verbindung TESTVPN aufgebaut wurde. Der Overhead von PPTP-Verbindungen beträgt 40 Bytes, weshalb die MTU hier 1060 Bytes beträgt.

MTU-Liste und MTU-Statistik existieren nur auf Geräten mit DSL oder ADSL-Interface.

6.17 Das Rapid-Spanning-Tree-Protokoll

In Netzwerken mit mehreren Switches und Bridges können zwischen zwei angeschlossenen Netzwerkteilnehmern durchaus mehrere physikalische Verbindungen bestehen. Diese redundanten Datenwege sind auch durchaus erwünscht, da sie bei Ausfall einzelner Netzstränge alternative Wege zum Ziel anbieten können. Auf der anderen Seite kann es durch diese Mehrfachverbindungen zu unerwünschten Schleifen (Loops) oder zu mehrfach empfangenen Frames kommen. Beide Effekte stören den reibungslosen Datenverkehr im Netz.

Das Spanning-Tree-Protokoll (STP) ermöglicht die Analyse des Netzwerks auf Layer-2-Ebene und bietet somit auch unterhalb der Routing-Schicht Lösungen zur intelligenten Wegeauswahl zwischen zwei Netzteilnehmern. Durch das Auffinden redundanter Wege zwischen den Netzteilnehmern bildet STP eine eindeutige Struktur, in der Loops und doppelte Pakete vermieden werden. Dazu werden so genannte Bridge Protocol Data Units (BPDUs) als Multicast an eine bestimmte MAC-Adresse gesendet. Die BPDUs ermöglichen das Auffinden von doppelten Strecken sowie der Entfernung und der auf dieser Verbindung verfügbaren Datenrate. Aus diesen Werten errechnet das Spanning-Tree-Protokoll eine Priorität (auch Wege- oder Pfadkosten genannt), mit der die verschiedenen Verbindungen zu behandeln sind. Die Verbindungen mit geringerer Priorität werden deaktiviert und stehen somit nicht für die Clients zur Verfügung. Durch die Reduktion auf nicht redundante Verbindungen zwischen den Clients baut das Protokoll einen Baum auf, in dem von einem zentralen Switch (Root-Bridge) aus alle Verbindungen eindeutig sind.

Die BPDUs werden regelmäßig im Netzwerk verschickt, um die Verfügbarkeit der Verbindungen zu prüfen. Fällt eine der Verbindungen aus, wird die Analyse des Netzwerks erneut ausgelöst, die möglichen Wege und die zugehörigen Prioritäten werden neu festgelegt.

Nach der Initialisierung befinden sich zunächst alle Ports im Zustand „Blocking", in dem nur BPDUs übertragen werden. Anschließend wechseln die Ports über die Zustände Listening und Learning in den Zustand „Forwarding", in dem Nutzdaten über die Ports übertragen werden können.

6.17.1 Classic und Rapid Spanning Tree

Das zunächst verwendete Spannig-Tree-Protokoll nach IEEE 802.1D – im Weiteren auch als Classic Spanning Tree bezeichnet – hatte jedoch das Problem, dass die Aktualisierung der Topologie durch den Ausfall einer Verbindung nur recht langsam umgesetzt wurde: 20 bis 30 Sekunden, je nach Komplexität des Netzwerkes auch bis zu einer Minute braucht das klassische Spanning Tree zum Aufbau neuer Verbindungswege. Für viele Netzwerkdienste sind solch lange Ausfallzeiten nicht akzeptabel.

Das Spanning Tree Protokoll wurde daher verbessert und als „Rapid Spanning Tree Protokoll" (RSTP) zunächst in einem eigenen Standard IEEE 802.1t/w, später als Teil der Neufassung von IEEE 802.1D veröffentlicht. Auch wenn das klassische Spanning Tree Protokoll damit zurückgezogen wurde, wird es in LCOS weiter unterstützt und zur Auswahl angeboten.

6.17.2 Verbesserungen durch Rapid Spanning Tree

Wie zuvor bemerkt ist das Hauptziel von RSTP die beschleunigte Aktivierung von Netzwerkpfaden, wenn eine der aktiven Verbindungen ausfällt. RSTP verzichtet dabei u. a. auf die Zustände Blocking und Listening und reduziert die benötigte Zeit zur Aktualisierung der Netzwerkpfade auf wenige Sekunden. Beim Ausfall eines Netzwerkpfades werden nicht mehr alle Links blockiert, bis die neue Topologie berechnet ist, sondern nur die ausgefallenen Verbindungen fallen für die Nutzung aus.

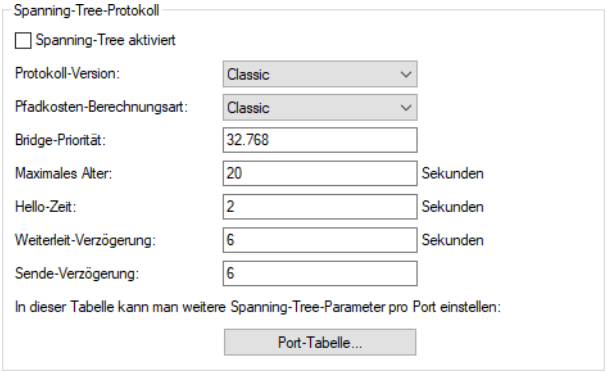
RSTP ermöglicht es dem Administrator darüber hinaus, Informationen über die Topologie des Netzwerk zu konfigurieren:

- Ein Bridge-Port kann dazu als „Grenz-Port" (Edge-Port) definiert werden. Ein Edge-Port ist der einzige Bridge-Port, der zu dem angeschlossenen LAN-Segment führt – an dem LAN-Segment sind also keine anderen Bridges angeschlossen, sondern nur z. B. Workstations oder Server. Da diese Ports nicht zu Loops führen können, wechseln sie sofort in den Forwarding-Zustand, ohne die Ermittlung der Netzwerktopologie abzuwarten. Das RSTP überwacht solche Ports jedoch weiterhin – falls unerwartet doch BPDUs auf einem Edge-Port empfangen werden, weil doch eine andere Bridge am LAN angeschlossen wurde, fällt der Port automatisch in den Normalzustand zurück.
- Ein Bridge-Port kann auch als Point-to-Point-Link eingesetzt werden. In diesem Fall ist der Port direkt mit einer weiteren Bridge verbunden. Da zwischen den beiden Bridges keine weiteren Zwischenstationen auftreten können, kann der Wechsel in den Forwarding-Zustand schneller erfolgen.

Im Idealfall kann RSTP bekannte alternative Netzwerkpfade sofort nutzen, wenn eine Verbindung ausfällt.

6.17.3 Konfiguration des Spanning-Tree-Protokolls

Zur Konfiguration der RSTP- bzw. STP-Funktion im Gerät stehen folgende Parameter bereit:



LANconfig: **Schnittstellen** > **Spanning Tree**

Konsole: **Setup** > **LAN-Bridge** > **Spanning-Tree**

6.17.3.1 Allgemeine Parameter

- Spanning-Tree aktiviert

  Bei ausgeschaltetem Spanning Tree verschickt ein Gerät keine Spanning-Tree-Pakete und leitet empfangene Spanning-Tree-Pakete durch, anstatt sie selber zu verarbeiten.

- Protokoll-Version
  - Classic: Verwendet die Verfahren des klassischen STP zur Bestimmung der Netzwerktopologie.
  - Rapid: Verwendet die Verfahren des RSTP zur Bestimmung der Netzwerktopologie.

RSTP ist kompatibel zu STP. Wenn Komponenten im Netzwerk verwendet werden, die nur das klassische STP unterstützen, werden auch bei Aktivierung von RSTP die Verfahren von STP verwendet.

- Pfadkosten-Berechnung
  - Classic: Verwendet die Verfahren des klassischen STP zur Pfadkostenberechnung.
  - Rapid: Verwendet die Verfahren des RSTP zur Pfadkostenberechnung.
- Bridge-Priorität

  Legt die Priorität der Bridge im LAN fest. Damit kann man beeinflussen, welche Bridge vom Spanning-Tree-Protokoll bevorzugt zur Root-Bridge gemacht wird.

  Aus Gründen der Kompatibilität zu RSTP sollte dieser Wert nur in Schritten von 4096 verändert werden, da bei RSTP die unteren 12 Bit dieses 16-Bit-Wertes für andere Zwecke verwendet werden.
- Maximales Alter

  Dieser Wert bestimmt die Zeit (in Sekunden), nach der eine Bridge über Spanning-Tree empfangene Nachrichten als 'veraltet' verwirft. Dieser Parameter bestimmt, wie schnell der Spanning-Tree-Algorithmus auf Änderungen z. B. durch ausgefallene Bridges reagiert.
- Hello-Zeit

  Dieser Parameter (in Sekunden) legt fest, in welchen Intervallen ein als Root-Bridge ausgewähltes Gerät Spanning-Tree-Informationen ins LAN schickt.
- Weiterleit-Verzögerung

  Diese Zeit (in Sekunden) legt fest, wieviel Zeit mindestens vergehen muss, bevor ein Spanning-Tree-Port den Zustand (Listening, Learning, Forwarding) wechseln darf.

  Bei Verwendung des RSTP hat die Weiterleitungs-Verzögerung oft keine Auswirkung, da das RSTP selbst über geeignete Mechanismen verfügt, um den schnellen Wechsel in den Forwarding-Zustand auszulösen.

  Eine Modifikation dieser drei Zeitwerte wird nur bei genauer Kenntnis des Spanning-Tree-Protokolls empfohlen. Eine Anpassung kann sinnvoll sein, um Reaktionszeiten auf Topologieveränderungen zu optimieren oder eine stabile Funktion in Netzen mit sehr vielen 'Bridge-Hops' zu erreichen.
- Sende-Verzögerung

  Anzahl der BPDUs, die bei RSTP gesendet werden dürfen, bevor eine Sekunde Pause eingelegt wird.

  Bei Verwendung des klassischen STP hat die Sende-Verzögerung keine Auswirkung.

6.17.3.2 Port-Tabelle

In der Port-Tabelle können für alle verfügbaren Ports (LAN, Wireless LAN, Point-to-Point-Strecken) folgende Werte separat eingestellt werden.

- Als Edge-Port kennzeichnen

  Kennzeichnet den Port als Edge-Port, an dem keine weitere Bridge, sondern nur Endgeräte wie Workstations oder Server angeschlossen sind. Edge-Ports wechseln sofort in den Forwarding-Zustand.

  Edge-Ports werden weiterhin vom RSTP überwacht. Werden an einem solchen Port BPDU entdeckt, verliert der Port den Status als Edge-Port.
- Priorität

  Legt die Priorität des Ports fest. Bei mehreren möglichen Netzwerkpfaden mit gleichem Pfadkosten entscheidet die Priorität, welcher Port verwendet wird. Bei Gleichheit der Priorität wird der Port gewählt, der weiter oben in der Liste steht.

Aus Gründen der Kompatibilität zu RSTP darf dieser Wert nur in Schritten von 16 verändert werden, da bei RSTP nur die oberen 4 Bit dieses 16-Bit-Wertes genutzt werden.

- Pfadkosten-Beeinflussung

  Mit diesem Parameter wird die Priorität von gleichwertigen Pfaden gesteuert. Der hier eingestellte Wert wird anstelle der berechneten Pfadkosten für die Auswahl verwendet.

  - Besondere Werte: 0 schaltet die Pfadkosten-Beeinflussung aus.
  - Default: 0

6.17.4 Statusmeldungen über das Spanning-Tree-Protokoll

Die aktuellen Werte des STP können im LAN-Bridge-Status über Telnet oder Browser eingesehen werden.

Console: **Status** > **LAN-Bridge** > **Spanning-Tree**

6.17.4.1 Allgemeine Statusinformationen

- Bridge-ID

  Dies ist die ID des Gerätes, die vom Spanning-Tree-Algorithmus benutzt wird. Sie setzt sich aus der vom Benutzer festgelegten Priorität (obere 16 Bit) und der Geräte-MAC-Adresse (untere 48 Bit) zusammen.

- Root-Bridge

  Die ID des momentan zur Root-Bridge gewählten Geräts.

- Root-Port

  Der Port, über den von diesem Gerät aus die Root-Bridge erreicht werden kann. Falls das Gerät gerade selber die Root-Bridge ist, wird das mit dem Sonderwert '255' angezeigt.

- Root-Pfadkosten

  Die aufsummierten Pfad-Kosten aller Hops, um von diesem Gerät aus die Root-Bridge zu erreichen.

- Protokoll-Version

  Aktuell eingestellte Protokollversion zur Bestimmung der Netzwerktopologie.

- Pfadkosten-Berechnung

  Aktuell eingestellte Protokollversion zur Pfadkostenberechnung.

- Bridge-Priorität

  Aktuell eingestellte Priorität der Bridge.

6.17.4.2 Informationen in der Port-Tabelle

In der Port-Tabelle können für alle verfügbaren Ports (LAN, Wireless LAN, Point-to-Point-Strecken) folgende Werte eingesehen werden.

- Priorität

  Die aus der Port-Konfiguration übernommene Priorität dieses Ports.

- **Status**

  Der momentane Status des Ports:

  - disabled: keinerlei Pakete über diesen Port senden oder empfangen. Das tritt ein, wenn der Port entweder manuell deaktiviert wurde oder einen negativen Link-Status hat.
  - Listening: Zwischenzustand auf dem Weg zur Aktivierung. Es wird nur auf Spanning-Tree-Pakete gehört, Datenpakete werden ignoriert und auch nicht an diesen Port weitergeleitet.

- Learning: weiterer Zwischenzustand. Gegenüber 'listening' werden zusätzlich MAC-Adressen von an diesem Port ankommenden Datenpaketen gelernt, es werden aber weiterhin keine Datenpakete weitergeleitet.
- Forwarding: der Port ist vollständig aktiv, Datenpakete werden in beiden Richtungen entgegengenommen und weitergeleitet
- Blocking: Spanning Tree hat diesen Port als redundant erkannt und für Datenverkehr deaktiviert.

- **Root**

  Die ID der über diesen Port zu erreichenden Root-Bridge.

- **Bridge**

  Dies ist die ID der Bridge, über welche die Root-Bridge erreicht werden kann.

- **Kosten**

  Dieser Wert gibt die 'Kosten' für diesen Port an. Der Wert ergibt sich aus der Technologie (Ethernet, WLAN etc.) des Ports sowie der Bandbreite. Verwendete Werte sind z. B.:

Übertragungstechnologie	Kosten für Classic Spanning Tree	Kosten für Rapid Spanning Tree
Ethernet 10 MBit	100	2000000
Ethernet 100 MBit	19	200000
Ethernet 1000 MBit	4	200000
WLAN 2 MBit	500	12500000
WLAN 11 MBit	140	4000000
WLAN 54 MBit	35	900000
WLAN 108 MBit	25	450000

Wurden manuell Pfadkosten für einen Port vorgegeben, erscheint in dieser Spalte der konfigurierte Wert.

6.17.4.3 Informationen in der RSTP-Port-Statistik

In der RSTP-Port-Tabelle können für alle verfügbaren Ports (LAN, Wireless LAN, Point-to-Point-Strecken) folgende Werte eingesehen werden.

- **Rolle**

  Root- oder Nicht-Root-Bridge.

- Learning

  Port im Learning-Zustand.

- Forwarding

  Port im Forwarding-Zustand.

- Edge-Port

  Port als Edge-Port definiert.

- Protokoll-Version

  Klassisch oder Rapid.

- **Kosten**

  Eingestellte Kosten für diesen Port.

6.18 Die Aktions-Tabelle

6.18.1 Einleitung

Über die Aktions-Tabelle werden Aktionen gesteuert, die bei einem Zustandswechsel von WAN-Verbindungen ausgelöst werden. Als WAN-Verbindung kommen dabei sowohl die direkten Verbindungen z. B. zum Internetprovider in Frage als auch die darüber liegenden VPN-Verbindungen, z. B. bei der Anbindung von Filialen an eine Zentrale. Jede Aktion ist an eine Bedingung geknüpft, die den Zustandswechsel der WAN-Verbindung beschreibt (Aufbau, Abbau, Ende, Fehler oder Aufbaufehler). Als Aktionen können grundsätzlich alle Befehle genutzt werden, die über die Telnet-Konsole zur Verfügung stehen. Darüber hinaus können die Aktionen Benachrichtigungen per E-Mail oder SYSLOG versenden, einen HTTP-Aufruf absetzen oder eine DNS-Anfrage versenden. Mit verschiedenen Variablen können Informationen wie die aktuelle IP-Adresse oder der Name des Gerätes oder eine Fehlermeldung mit in die Aktionen eingebaut werden.

6.18.2 Aktionen für Dynamic DNS

Damit auch Systeme mit dynamischen IP-Adressen über das WAN – also beispielsweise über das Internet – erreichbar sind, existieren eine Reihe von sog. Dynamic DNS-Server Anbietern. Die Server bei diesen Diensten ordnen die aktuelle IP-Adresse eines Gerätes dem gewählten FQDN-Namen zu (Fully Qualified Domain Name, z. B. "MyDevice.dynDNS.org").

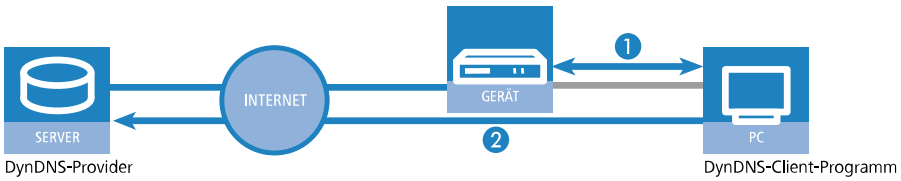
Der Vorteil liegt auf der Hand: Wenn Sie z. B. eine Fernwartung über WEBconfig/HTTP durchführen wollen, dann brauchen Sie lediglich den Dynamic DNS-Namen zu kennen. Außerdem können die DynDNS-Namen auch zum Aufbau von VPN-Verbindungnen zwischen Gegenstellen mit wechselnden IP-Adressen genutzt werden.

Damit die Zuordnung von aktueller IP-Adresse und DynDNS-Name jederzeit funktioniert, muss bei jeder Änderung der IP-Adresse der entsprechende Eintrag auf dem DynDNS-Server aktualisiert werden. Diese Änderung wird von einem Dynamic-DNS-Client ausgelöst.

- Der DynDNS-Server, der von den DynDNS-Dienstleistern im Internet angeboten wird, steht mit Internet-DNS-Servern in Verbindung.
- Der Dynamic-DNS-Client kann als separates Clientprogramm auf einer Workstation laufen. Alternativ ist im Gerät ein Dynamic-DNS-Client integriert. Er kann zu einer Vielzahl von Dynamic-DNS-Serviceanbietern Kontakt aufnehmen und bei jeder Änderung seiner IP-Adresse automatisch ein vorher angelegtes Benutzerkonto zur DNS-Namensauflösung beim Dynamic-DNS-Anbieter aktualisieren.

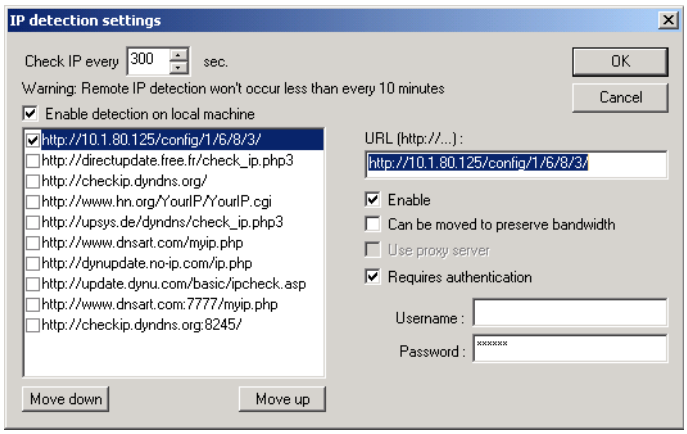
6.18.2.1 Dynamic-DNS-Client auf der Workstation

Dynamic-DNS-Anbieter unterstützen eine Reihe von PC-Clientprogrammen, die über verschiedene Methoden die aktuell zugewiesene IP-Adresse eines Geräts ermitteln können **1** und im Falle einer Änderung an den jeweiligen Dynamic-DNS-Server übertragen **2**.



Die aktuelle WAN-seitige IP-Adresse eines Geräts kann unter folgender Adresse ausgelesen und dann in ein geeignetes Clientprogramm eingetragen werden:

```
http://<Adresse des Geräts>/config/1/6/8/3/
```



6.18.2.2 Dynamic-DNS-Client im Gerät über HTTP

Alternativ kann das Gerät die aktuelle WAN-IP auch direkt an den DynDNS-Anbieter übertragen:



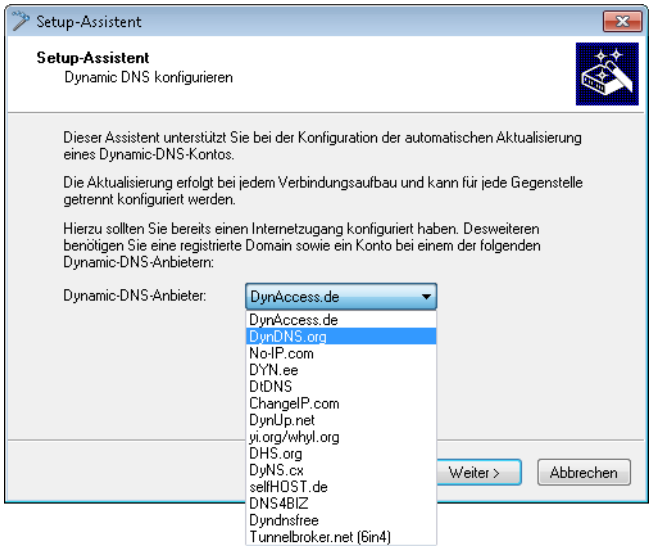
DynDNS-Provider

Dazu definieren Sie eine Aktion, die z. B. nach jedem Verbindungsaufbau automatisch eine HTTP-Anfrage an den DynDNS-Server sendet, dabei die benötigten Informationen über das DynDNS-Konto übermittelt und so ein Update der Registrierung auslöst. Eine solche HTTP-Anfrage an den Anbieter DynDNS.org kann z. B. so aussehen:

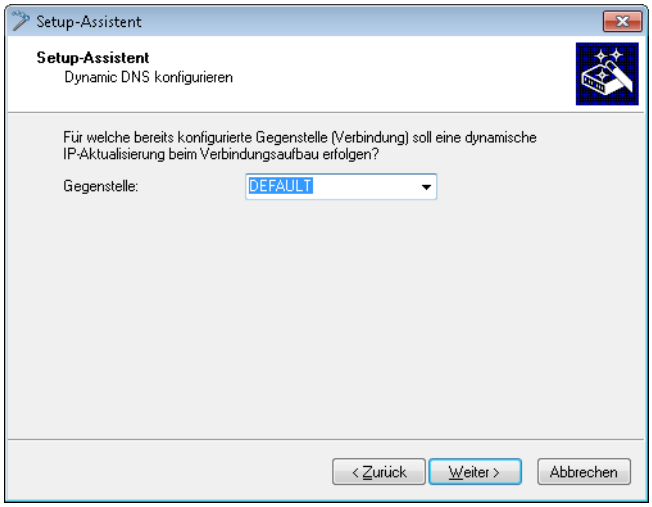
```
http://Username:Password@members.dyndns.org/nic/update?system=dyndns&hostname=%h&myip=%a
```

Damit übermittelt das Gerät den Hostnamen der Aktion und seine aktuelle IP-Adresse an das durch Username und Password spezifizierte Konto beim DynDNS-Dienstleister DynDNS.org, der daraufhin den entsprechenden Eintrag aktualisiert. Die dazu notwendigen Einstellungen können Sie komfortabel mit dem Setup-Assistenten von LANconfig vornehmen.

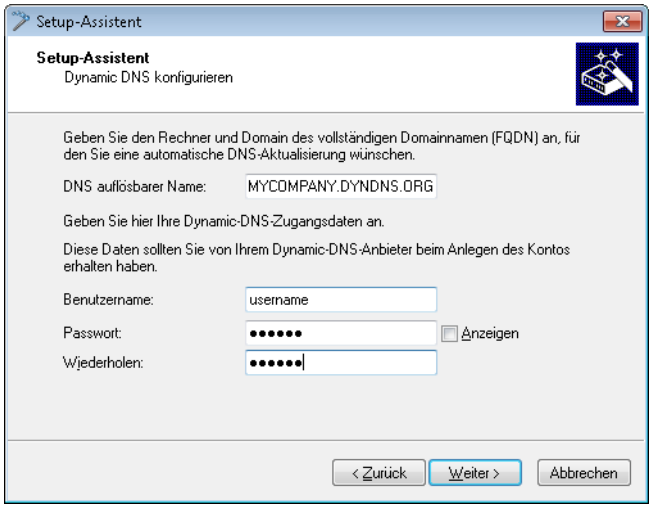
Wählen Sie aus der Liste zunächst den Dienstleister aus, den Sie verwenden möchten.



Bestimmen Sie jetzt die WAN-Gegenstelle, für die die Aktion gelten soll.



Geben Sie abschließend noch Ihre Zugangsdaten ein.



Der Setup-Assistent ergänzt die beschriebene Basis-Aktion um weitere anbieter-spezifischen Parameter, die hier nicht näher beschrieben sein sollen. Außerdem legt der Setup-Assistent weitere Aktionen an, die das Verhalten des Geräts steuern für den Fall, dass der DynDNS-Dienstleister die Aktualisierung nicht im ersten Versuch erfolgreich durchführen konnte.

6.18.2.3 Dynamic-DNS-Client im Gerät über GnuDIP

Als Alternative zur Aktualisierung der DynDNS-Informationen über eine einfache HTTP-Anfrage nutzen manche Dienste das GnuDIP-Protokoll. Das GnuDIP-Protokoll basiert auf einem Challenge-Response-Mechanismus:

1. Der Client öffnet die Verbindung zum GnuDIP-Server.
2. Der Server antwortet mit einem für die Sitzung berechneten Zufallswert.
3. Der Client erzeugt aus dem Zufallswert und dem Password einen Hashwert und sendet diesen an den Server zurück.
4. Der Server prüft diesen Hashwert und meldet das Ergebnis in Form einer Ziffer zurück an den Client.

Das GnuDIP-Protokoll kann die Nachrichten zwischen Client und Server entweder auf einer einfachen TCP-Verbindung austauschen (Standard-Port 3495) oder als CGI-Skript auf einem Internetserver laufen. Die Variante über einen HTTP-Aufruf des CGI-Skripts hat den Vorteil, dass auf dem Server kein weiterer Port für GnuDIP geöffnet werden muss, außerdem sichert HTTPS zusätzlich gegen passives Abhören und Offline-Wörterbuch-Attacken.

Die Anfragen an einen GnuDIP-Server werden aus dem Gerät mit einer Aktion in der folgenden Form ausgelöst:

- gnudip://<srv>[:port][/pfad]?<parameter>
  - <srv> – Die Adresse des GnuDIP-Servers.
  - [:port] – Die Angabe des Ports ist optional, falls nicht definiert, werden die Standardwerte verwendet (3495 für TCP, 80 bzw. 443 für HTTP/HTTPS).
  - [/pfad] – Die Pfadangabe wird nur bei HTTP/HTTPS benötigt, um den Speicherort des CGI-Skriptes zu definieren.

  Die folgenden Parameter erweitern den Aufruf:

  - method=<tcp|http|https> – Wählt das Protokoll aus, das für die Übertragung zwischen GnuDIP-Server und -Client verwendet werden soll. Hier kann nur genau ein Protokoll gewählt werden.
  - user=<username> – Gibt den Benutzernamen für das Konto auf dem GnuDIP-Server an.
  - pass=<password> – Gibt das Kennwort für das Konto auf dem GnuDIP-Server an.
  - domn=<domain> – Gibt die DNS-Domäne an, in der sich der DynDNS-Eintrag befindet.
  - reqc=<0|1|2> – Definiert die Aktion, die mit der Anfrage ausgelöst werden soll. Mit der Aktion <0> wird eine dedizierte IP-Adresse an den Server übermittelt, die für das Update verwendet werden soll. Mit der Aktion <1> wird ein DynDNS-Eintrag gelöscht. Mit der Aktion <2> wird ein Update ausgelöst, es wird aber keine IP-Adresse an den Server übermittelt. Statt dessen verwendet der Server die IP-Adresse des GnuDIP-Clients für das Update.
  - addr=<address> – Gibt für eine Aktion mit dem Parameter <0> die IP-Adresse an, die für das Update des DynDNS-Eintrags verwendet werden soll. Fehlt diese Angabe bei einer <0>-Aktion, so wird die Anfrage wie eine <2>-Aktion behandelt.

  Beim GnuDIP-Protokoll entspricht der Hostname, der registriert werden soll, dem an den Server übermittelten Benutzernamen. Wenn der Benutzername z. B. "myserver" lautet und die DNS-Domäne "mydomain.org", dann wird der DNS-Name "myserver.mydomain.org" registriert.

  Sie können z. B. mit der folgenden Aktion eine DynDNS-Aktualisierung bei einem DynDNS-Anbieter über das GnuDIP-Protokoll durchführen, sobald eine Verbindung aufgebaut wurde, und dabei die aktuelle IP-Adresse des Geräts (%a) übertragen:

  - gnudip://gnudipsrv?method=tcp&user=myserver&domn=mydomain.org &pass=password&reqc=0&addr=%a

  Um einen DynDNS-Eintrag zu löschen, wenn z. B. eine Verbindung getrennt wurde, verwenden Sie die folgende Aktion:

  - gnudip://gnudipsrv?method=tcp&user=myserver&domn=mydomain.org &pass=password&reqc=1

  Der Zeilenumbruch dient jeweils nur der Lesbarkeit und wird nicht in die Aktion eingetragen.

Der GnuDIP-Server gibt als Ergebnis der Anfrage einen der folgenden Werte an den GnuDIP-Client zurück (vorausgesetzt, die Verbindung zwischen Server und Client konnte hergestellt werden):

- 0 – Der DynDNS-Eintrag wurde erfolgreich aktualisiert.
- 0:Adresse – Der DynDNS-Eintrag wurde erfolgreich mit der angegebenen Adresse aktualisiert.
- 1 – Die Authentifizierung am GnuDIP-Server war nicht erfolgreich.
- 2 – Der DynDNS-Eintrag wurde erfolgreich gelöscht.

Diese Antworten können in den Aktionen des Geräts ausgewertet werden, um bei Bedarf weitere Aktionen einzuleiten.

6.18.3 Weitere Beispiele für Aktionen

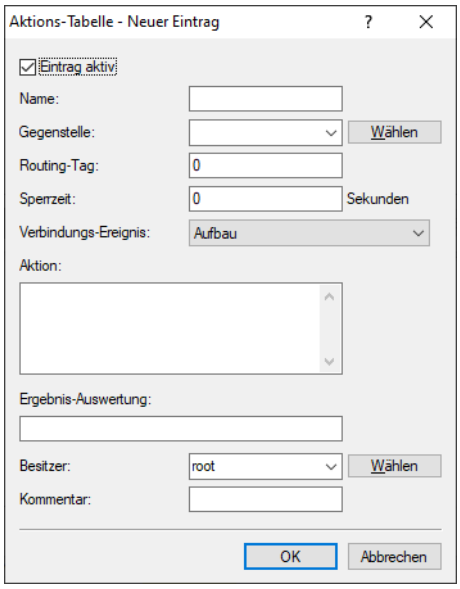
6.18.3.1 Information über Verbindungsabbruch als SMS auf Mobiltelefon melden

Mit dem Platzhalter %t kann die aktuelle Zeit über ein Ereignis in eine Benachrichtigung mit aufgenommen werden. So kann z. B. der Abbruch einer wichtigen VPN-Verbindung per E-Mail oder SMS an das Mobiltelefon eines Systemadministrators gemeldet werden.

Folgende Voraussetzungen müssen für die Benachrichtigung erfüllt sein:

- Der Zustand der VPN-Verbindung muss überwacht werden, z. B. durch die „Dead-Peer-Detection" DPD.
- Das Gerät muss als NTP-Client konfiguriert sein, damit das Gerät über eine aktuelle Systemzeit verfügt.
- Ein SMTP-Konto zum Versand der E-Mails muss eingerichtet sein.

Wenn diese Voraussetzungen erfüllt sind, kann die Benachrichtigung eingerichtet werden. Legen Sie dazu in der Aktionstabelle einen neuen Eintrag an, z. B. mit LANconfig unter **Kommunikation** > **Allgemein** > **Aktionstabelle**.



In dem Eintrag wählen Sie die Gegenstelle aus, für die ein Verbindungsabbruch gemeldet werden soll. Dazu wählen Sie als Ereignis den 'Abbruch' und geben als Aktion den Versand einer Mail ein:

```
mailto:admin@mycompany.de?subject=VPN-Verbindung abgebrochen um %t?body=VPN-Verbindung zu Filiale 1 wurde unterbrochen.
```

Mit dieser Aktion wird bei Abbruch der Verbindung eine Mail an den Administrator versendet, dabei wird die Zeit bei Verbindungsabbruch in den Betreff eingefügt.

Wenn die Mail an ein entsprechendes Mail2SMS-Gateway gesendet wird, kann die Benachrichtigung auch direkt auf ein Mobiltelefon zugestellt werden.

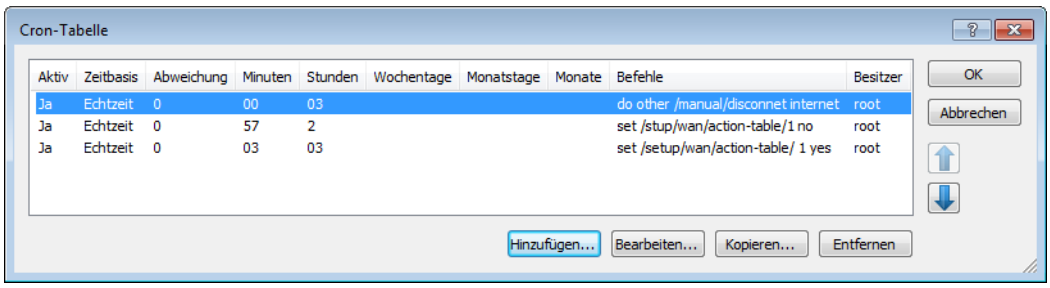
In einem komplexen Aufbau mit mehreren Filialen wird im Gerät der Zentrale für jede Gegenstelle ein passender Eintrag angelegt. Zur Überwachung der Zentrale selbst wird eine Aktion in einem Gerät in einer der Filialen angelegt. So kann der Administrator auch dann benachrichtigt werden, wenn das VPN-Gateway der Zentrale selbst ausfällt und vielleicht keine Nachricht mehr versenden kann.

6.18.3.2 Beispiel: Benachrichtigung bei Zwangstrennung der DSL-Verbindung unterdrücken

Je nach Anbieter wird die für VPN-Verbindungen genutzte DSL-Leitung einmal alle 24 Stunden zwangsweise getrennt. Damit der Administrator nicht auch über diese regelmäßigen Unterbrechungen informiert wird, kann die Benachrichtigung für die Zeit der Zwangstrennung ausgeschaltet werden.

Dazu wird zunächst mit einer Aktion die Zwangstrennung auf einen definierten Zeitpunkt gelegt, üblicherweise in die Nacht, wenn die Internetverbindung nicht benötigt wird. Der Eintrag wird z. B. auf 3:00 Uhr nachts gelegt und trennt die Internetverbindung mit dem Befehl `do other/manual/disconnect internet`.

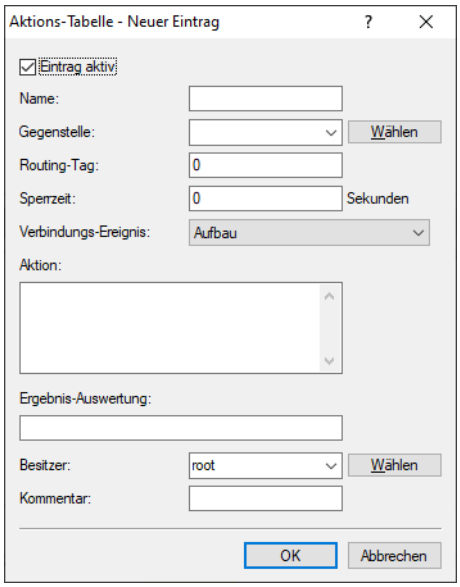
Mit zwei weiteren Cron-Befehlen `set /setup/wan/action-table/1 yes/no` wird der entsprechende Eintrag in der Aktionstabelle drei Minuten vor 3.00 Uhr aus- und drei Minuten nach 3:00 Uhr wieder eingeschaltet. Die Ziffer 1 nach dem Pfad zu Aktionstabelle steht dabei als Index für den ersten Eintrag der Tabelle.



6.18.4 Konfiguration

In der Aktions-Tabelle können Sie Aktionen definieren, die das Gerät ausführen soll, wenn sich der Zustand einer WAN-Verbindung ändert.

Im LANconfig finden Sie die Aktions-Tabelle unter **Kommunikation** > **Allgemein** > **Aktions-Tabelle**



Eintrag aktiv

Aktiviert oder deaktiviert diesen Eintrag.

Name

Name der Aktion. Diesen Namen können Sie mit dem Platzhalter `%h` (Hostname) in den Feldern **Aktion** und **Ergebnis-Auswertung** referenzieren.

Gegenstelle

Name der Gegenstelle, deren Zustandswechsel die in diesem Eintrag definierte Aktion auslösen soll.

Routing-Tag

Über das Routing-Tag bestimmen Sie, über welche Gegenstelle das Gerät die Aktion ausführt. Diese Gegenstelle muss natürlich mit dem entsprechenden Routing-Tag versehen sein.

Sperrzeit

Unterbricht die wiederholte Ausführung der in diesem Eintrag definierten Aktion für die eingestellte Zeit in Sekunden (max. 10 Zeichen).

Verbindungs-Ereignis

Die Aktion erfolgt, wenn der hier eingestellte Zustandswechsel der WAN-Verbindung eintritt. Mögliche Werte sind:

Aufbau

Die Aktion erfolgt, wenn das Gerät die Verbindung erfolgreich aufgebaut hat.

Abbau ohne Fehler

Die Aktion erfolgt, wenn das Gerät die Verbindung selbst beendet (z. B. durch eine manuelle Trennung oder den Ablauf einer Haltezeit).

Ende (Abbau oder Abbruch)

Die Aktion erfolgt, sobald die Verbindung beendet ist (unabhängig vom Grund für den Verbindungsabbau).

Abbruch mit Fehler

Die Aktion erfolgt, wenn die Verbindung beendet ist, das Gerät selbst aber diesen Abbau nicht ausgelöst oder erwartet hat.

Aufbaufehler

Die Aktion erfolgt, wenn ein Verbindungsaufbau nicht erfolgreich war.

Volumen erreicht

Die Aktion erfolgt, wenn das festgelegte Volumen erreicht ist.

Volumen zurückgesetzt

Die Aktion erfolgt, wenn ein Zustandswechsel von „Volumen überschritten" zu „Volumen nicht mehr überschritten" stattfindet; also z. B. Sie ein überschrittenes Volumen zurücksetzen oder das Gerät nach dem Überschreiten eine neue Abrechnungsperiode beginnt. Ist zum Zeitpunkt der Rücksetzung das Volumen noch nicht überschritten, erfolgt keine Aktion.

Aktion

Hier beschreiben Sie die Aktion, die das Gerät beim Zustandswechsel der WAN-Verbindung ausführen soll. Pro Eintrag dürfen Sie nur eine Aktion angeben (max. 250 Zeichen). Für jeden der folgenden Werte ist der Doppelpunkt (:) Teil des Aktions-Wertes. Mögliche Werte sind:

exec:

Mit diesem Präfix leiten Sie alle Befehle ein, wie Sie sie auch an der Konsole eingegeben würden. Sie können z. B. mit der Aktion `exec:do /o/m/d` alle bestehenden Verbindungen beenden.

dnscheck:

Mit diesem Präfix leiten Sie eine IPv4-DNS-Namensauflösung ein. Sie können z. B. mit der Aktion `dnscheck:myserver.dyndns.org` die IPv4-Adresse des angegebenen Servers ermitteln.

dnscheck6:

Mit diesem Präfix leiten Sie eine IPv6-DNS-Namensauflösung ein. Sie können z. B. mit der Aktion `dnscheck6:myserver.dyndns.org` die IPv6-Adresse des angegebenen Servers ermitteln.

http:

Mit diesem Präfix lösen Sie eine HTTP-Get-Anfrage aus. Sie können z. B. mit der folgenden Aktion eine DynDNS-Aktualisierung bei dyndns.org durchführen:

```
http://username:password@members.dyndns.org/nic/update?system=dyndns&hostname=%h&myip=%a
```

Die Bedeutung der Platzhalter `%h` und `%a` erfahren Sie weiter unten.

https:

Wie `http:`, nur über eine verschlüsselte Verbindung.

gnudip:

Mit diesem Präfix lösen Sie eine Anfrage über das GnuDIP-Protokoll an einen entsprechenden DynDNS-Server aus. Sie können z. B. mit der folgenden Aktion eine DynDNS-Aktualisierung bei einem DynDNS-Anbieter über das GnuDIP-Protokoll durchführen:

```
gnudip://gnudipsrv?method=tcp&user=myserver&domn=mydomain.org&pass=password&reqc=0&addr=%a
```

Die Bedeutung des Platzhalters `%a` erfahren Sie in den folgenden Absätzen.

repeat:

Mit diesem Präfix und der Angabe einer Zeit in Sekunden erfolgen alle Aktionen mit der Bedingung "Aufbau" wiederholt, sobald die Verbindung aufgebaut ist. Mit der Aktion `repeat:300` erfolgen z. B. alle Aufbau-Aktionen wiederholt im fünf Minuten-Rythmus.

mailto:

Mit diesem Präfix lösen Sie den Versand einer E-Mail aus. Sie können z. B. mit der folgenden Aktion eine E-Mail an den Systemadministrator versenden, sobald eine Verbindung beendet ist: `mailto:admin@mycompany.de?subject=VPN-Verbindung abgebrochen um %t?body=VPN-Verbindung zu Filiale 1 wurde unterbrochen.`

Mögliche Variablen zur Erweiterung der Aktionen sind:

%a

WAN-IPv4-Adresse der WAN-Verbindung, in deren Kontext diese Aktion erfolgt.

Wird der String `&myip=%a` in den Einträgen der Aktions-Tabelle entfernt, übernimmt der DynDNS-Provider die IP-Adresse des Paketes, von dem die Anfrage stammt. Dies ist besonders in Szenarien sinnvoll, in denen eine IP-Adresse aus einem privaten IP-Adress-Bereich verwendet wird.

%x

Das aktuelle IPv6-LAN-Präfix als String im Format „fd00:0:0:1::/64“.

%{x*Netzwerkname*}

Z. B. `%{xTESTNETZ}` für das aktuelle IPv6-LAN-Präfix des Netzwerks TESTNETZ als String im Format „fd00:0:0:1::/64“.

Die Variable `%x` überträgt nur die Werte des Netzwerks mit dem festen Namen INTRANET. Hiermit kann auch der LAN-Netzwerkname übergeben werden, der für diese Variable verwendet wird.

%y

Die aktuelle IPv6-LAN-Adresse des Geräts als String im Format „fd00::1:2a0:57ff:fa1b:9d7b“.

%{y*Netzwerkname*}

Z. B. `%{yTESTNETZ}` für die aktuelle IPv6-LAN-Adresse des Geräts im Netzwerk TESTNETZ als String im Format „fd00::1:2a0:57ff:fa1b:9d7b“.

Die Variable `%y` überträgt nur die Werte des Netzwerks mit dem festen Namen INTRANET. Hiermit kann auch der LAN-Netzwerkname übergeben werden, der für diese Variable verwendet wird.

%z

WAN-IPv6-Adresse der WAN-Verbindung, in deren Kontext diese Aktion erfolgt.

%H

Hostname der WAN-Verbindung, in deren Kontext diese Aktion erfolgt.

%h

Wie `%H`, nur Hostname in Kleinbuchstaben.

%c

Verbindungsname der WAN-Verbindung, in deren Kontext diese Aktion erfolgt.

%n

Der Gerätename.

%s

Die Seriennummer des Gerätes.

%m

MAC-Adresse des Gerätes (wie im Sysinfo)

%t

Uhrzeit und Datum im Format „YYYY-MM-DD hh:mm:ss".

%e

Bezeichnung des Fehlers, der bei einem nicht erfolgreichen Verbindungsaufbau gemeldet wurde.

Der Gebrauch der Variablen `%z` erfordert die Angabe der IPv6-Adresse. Wenn Sie keine Adresse bereitstellen, führt das Gerät das Skript nicht aus.

Die Variable `%z` steht ausschließlich bei nativen IPv6-WAN-Verbindungen und nicht bei Tunnel-Verbindungen (6to4, 6in4, 6rd) zur Verfügung.

Das Ergebnis der Aktionen werten Sie anschließend im Feld **Ergebnis-Auswertung** aus.

Ergebnis-Auswertung

Das Ergebnis der Aktion können Sie hier auswerten, um je nach Ergebnis eine bestimmte Anzahl von Einträge beim Abarbeiten der Aktions-Tabelle zu überspringen. Mögliche Werte für die Aktionen sind (maximal 50 Zeichen):

contains=

Dieses Präfix prüft, ob das Ergebnis der Aktion die definierte Zeichenkette enthält.

isequal=

Dieses Präfix prüft, ob das Ergebnis der Aktion der definierten Zeichenkette genau entspricht.

?skipiftrue=

Dieses Suffix überspringt die definierte Anzahl von Zeilen in der Liste der Aktionen, wenn das Ergebnis der Abfrage mit „contains" oder „isequal" das Ergebnis WAHR liefert.

?skipiffalse=

Dieses Suffix überspringt die definierte Anzahl von Zeilen in der Liste der Aktionen, wenn das Ergebnis der Abfrage mit „contains" oder „isequal" das Ergebnis FALSCH liefert.

Optionale Variablen für die Aktionen sind dieselben wie für die Aktion oben.

Beispiel: Mit einem DNS-Check fragt das Gerät die IP-Adresse einer Adresse der Form „myserver.dyndns.org“ ab. Mit der Prüfung `contains=%a?skipiftrue=2` können Sie die beiden folgenden Einträge der Aktions-Tabelle überspringen, wenn die mit dem DNS-Check ermittelte IP-Adresse mit der aktuellen IP-Adresse des Gerätes (%a) übereinstimmt.

Besitzer

Besitzer der Aktion. Mit den Rechten dieses Besitzers werden die exec-Aktionen ausgeführt. Verfügt der Besitzer nicht über die notwendigen Rechte (z. B. Administratoren mit Leserechten), so kann das Gerät die Aktion nicht ausführen.

Kommentar

Vergeben Sie einen aussagekräftigen Kommentar für diesen Eintrag.

6.19 Verwendung der seriellen Schnittstelle im LAN

6.19.1 Einleitung

COM-Port-Server sind in der IT als Geräte bekannt, die Daten zwischen TCP- und seriellen Anschlüssen übertragen. Die Anwendungsmöglichkeiten sind vielfältig:

- Einbinden von Geräten mit serieller Schnittstelle, aber ohne Netzwerkschnittstelle in ein Netzwerk.
- Fernwartung von Geräten, die nur eine serielle Schnittstelle zur Konfiguration anbieten.
- Virtuelle Verlängerung einer seriellen Verbindung zwischen zwei Geräten mit serieller Schnittstelle über ein Netzwerk.

Nahezu alle Geräte verfügen über eine serielle Schnittstelle, die entweder zur Konfiguration oder zum Anschluss eines Modems genutzt werden kann. In manchen Fällen wird diese Schnittstelle jedoch für keine der beiden Möglichkeiten genutzt, ein COM-Port-Server in der Nähe des Gerätes wäre aber erwünscht. In diesen Fällen kann das Gerät seine serielle Schnittstelle als COM-Port-Server nutzen, wobei die Kosten für einen externen COM-Port-Server eingespart werden. Wenn auch der Fokus dieser Anwendung auf der seriellen Konfigurationsschnittstelle der Geräte liegt, so können je nach Modell über entsprechende CardBus- oder USB-Adapter weitere serielle Schnittstellen bereitgestellt werden, sodass in einem Gerät mehrere Instanzen des COM-Port-Servers genutzt werden können.

6.19.2 Betriebsarten

Ein COM-Port-Server kann in zwei verschiedenen Betriebsarten genutzt werden:

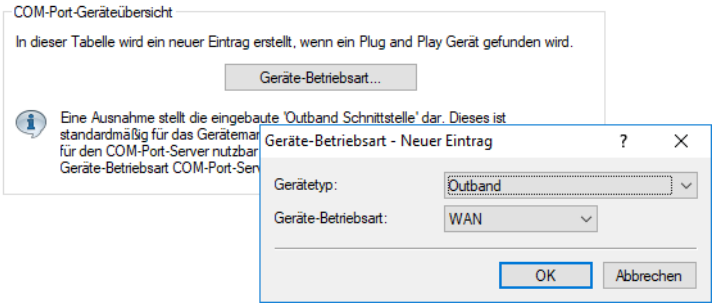
- Server-Modus: Der COM-Port-Server wartet auf einem definierten TCP-Port auf Anfragen zum Aufbau von TCP-Verbindungen. Diese Betriebsart wird z. B. für Fernwartungen genutzt.
- Client-Modus: Sobald ein an die serielle Schnittstelle angeschlossenes Gerät aktiv wird, öffnet der COM-Port-Client eine TCP-Verbindung zu einer definierten Gegenstelle. Diese Betriebsart wird z. B. für Geräte genutzt, die nur über eine serielle Schnittstelle verfügen, denen aber ein Netzwerkzugang bereitgestellt werden soll.

In beiden Fällen wird eine transparente Verbindung zwischen der seriellen Schnittstelle und der TCP-Verbindung hergestellt: Datenpakete, die auf der seriellen Schnittstelle empfangen werden, werden auf der TCP-Verbindung weitergeleitet und umgekehrt. Eine häufige Anwendung im Server-Modus ist die Installation eines virtuellen COM-Port-Treibers auf der Gegenstelle, die sich mit dem COM-Port-Server verbindet. Mit einem solchen Treiber kann die TCP-Verbindung wie ein zusätzlicher COM-Port der Gegenstelle von den dort laufenden Anwendungen genutzt werden. Die Norm IETF RFC 2217 definiert entsprechende Erweiterungen des Telnet WILL/DO-Protokolls, mit denen die Anfragen zur Verhandlung der seriellen Verbindung (Bitrate, Daten- und Stopp-Bits, Handshake) an den COM-Port-Server übertragen werden können. Da die Verwendung dieses Protokolls optional ist, können im COM-Port-Server sinnvolle Defaultwerte eingestellt werden.

6.19.3 Konfiguration der seriellen Schnittstellen

Die seriellen Schnittstellen können im Gerät für verschiedene Anwendungen genutzt werden, z. B. für den COM-Port-Server oder als WAN-Schnittstelle. In der Geräte-Tabelle können den einzelnen seriellen Geräten bestimmte Anwendungen zugewiesen werden. Sobald ein HotPlug-fähiger USB-Adapter erkannt wird, wird automatisch ein neuer Eintrag für die von diesem USB-Adapter bereitgestellten seriellen Schnittstellen in dieser Tabelle erzeugt. Diese Automatik erleichert die Konfiguration der seriellen Geräte. Eine Ausnahme stellt die eingebaute serielle Schnittstelle dar, die standardmäßig zur Konfiguration genutzt wird. Um diese Schnittstelle für den COM-Port-Server oder WAN-Anwendungen zu nutzen, können in der Gerätetabelle manuell Einträge hinzugefügt werden.

LANconfig: **Sonstige Dienste** > **COM-Ports** > **Geräte-Betriebsart**



Konsole: **Setup** > **COM-Ports** > **Geräte**

Gerätetyp

Auswahl aus der Liste der im Gerät verfügbaren seriellen Schnittstellen.

Geräte-Betriebsart

Aktivierung des Ports für den COM-Port-Server.

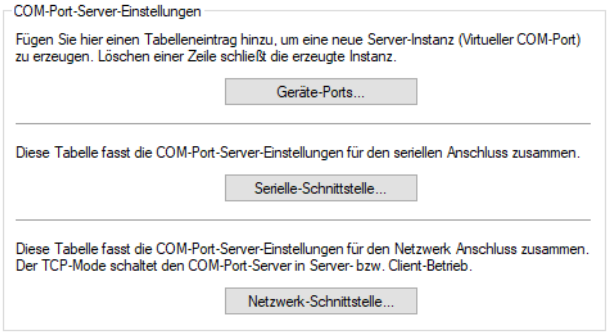
6.19.4 Konfiguration des COM-Port-Servers

Die Konfiguration des COM-Port-Servers umfasst drei Tabellen. Allen drei Tabellen gemeinsam ist die Identifikation eines bestimmten Ports auf einer seriellen Schnittstelle über die Werte Device-Type und Port-Nummer. Da manche seriellen Geräte wie z. B. eine CardBus-Karte mehrere Ports haben, muss der verwendete Port explizit angegeben werden. Bei einem Gerät mit nur einem Port wie bei der seriellen Konfigurationsschnittstelle wird die Port-Nummer auf Null gesetzt.

6.19.4.1 Betriebs-Einstellungen

Diese Tabelle aktiviert den COM-Port-Server auf einem Port einer bestimmten seriellen Schnittstelle. Fügen Sie dieser Tabelle eine Zeile hinzu, um eine neue Instanz des COM-Port-Servers zu starten. Löschen Sie eine Zeile, um die entsprechende Server-Instanz abzubrechen. Mit dem Schalter **In Betrieb** kann eine Server-Instanz in der Tabelle deaktiviert werden.

Wenn eine Server-Instanz angelegt oder aktiviert wird, werden die anderen Tabellen der COM-Port-Serverkonfiguration nach Einträgen mit übereinstimmenden Werten für Gerätetyp und Port-Nummer durchsucht. Falls kein passender Eintrag gefunden wird, verwendet die Server-Instanz sinnvolle Default-Werte.



LANconfig: **Sonstige Dienste** > **COM-Ports** > **Geräte-Ports**

Konsole: **Setup** > **COM-Ports** > **COM-Port-Server** > **Geraete**

Gerätetyp

Auswahl aus der Liste der im Gerät verfügbaren seriellen Schnittstellen.

Port

Manche seriellen Geräte wie z. B. die CardBus haben mehr als einen seriellen Port. Tragen Sie hier die Nummer des Ports ein, der auf der seriellen Schnittstelle für den COM-Port-Server genutzt werden soll.

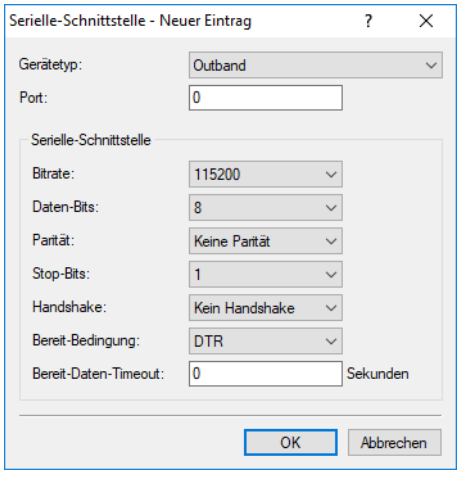
In Betrieb

Aktiviert den COM-Port-Server auf dem gewählten Port der gewählten Schnittstelle.

6.19.4.2 COM-Port-Einstellungen

Diese Tabelle enthält die Einstellungen für die Datenübertragung auf der seriellen Schnittstelle.

Bitte beachten Sie, dass alle diese Parameter durch die Gegenstelle überschrieben werden können, wenn die RFC-2217-Verhandlung aktiviert ist; die aktuellen Einstellungen können im Status-Menü eingesehen werden.



LANconfig: **Sonstige Dienste** > **COM-Ports** > **Serielle Schnittstelle**

Konsole: **Setup** > **COM-Ports** > **COM-Port-Server** > **COM-Port-Einstellungen**

Gerätetyp

Auswahl aus der Liste der im Gerät verfügbaren seriellen Schnittstellen.

Port

Manche seriellen Geräte wie z. B. die CardBus haben mehr als einen seriellen Port. Tragen Sie hier die Nummer des Ports ein, der auf der seriellen Schnittstelle für den COM-Port-Server genutzt werden soll.

Bitrate

Verwendete Bitrate auf dem COM-Port.

Daten-Bits

Anzahl der Daten-Bits.

Parität

Auf dem COM-Port verwendetes Prüfverfahren.

Stop-Bits

Anzahl der Stop-Bits.

Handshake

Auf dem COM-Port verwendete Datenflusskontrolle.

Bereit-Bedingung

Eine wichtige Eigenschaft eines seriellen Ports ist die Bereit-Bedingung. Der COM-Port-Server überträgt keine Daten zwischen dem seriellen Port und dem Netzwerk, solange er sich nicht im Zustand „Bereit" befindet. Außerdem wird der Wechsel zwischen den Zuständen „Bereit" und „Nicht-Bereit" verwendet, um im Client-Modus TCP-Verbindungen aufzubauen bzw. abzubrechen. Die Bereitschaft des Ports kann auf zwei verschiedene Arten ermittelt werden. Im DTR-Modus (Default) wird nur der DTR-Handshake überwacht. Die serielle Schnittstelle wird solange als bereit angesehen, wie die DTR-Leitung aktiv ist. Im Daten-Modus wird die serielle Schnittstelle als bereit betrachtet, sobald sie Daten empfängt. Wenn für die eingestellte Timeout-Zeit keine Daten empfangen werden, fällt der Port zurück in den Zustand „Nicht-Bereit".

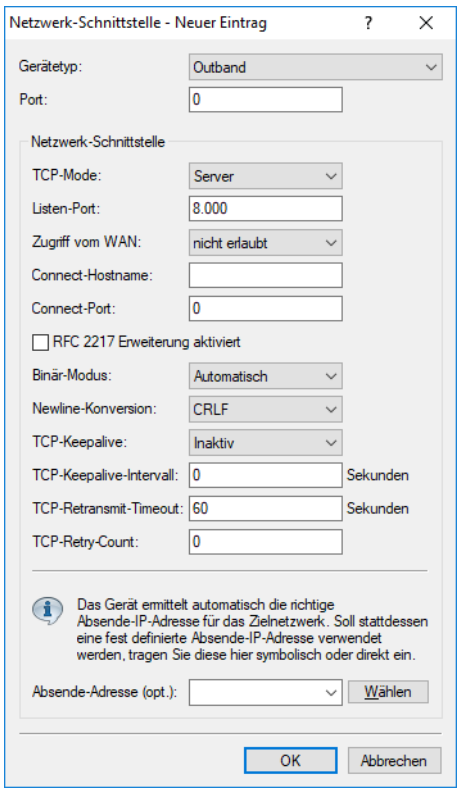
Bereit-Daten-Timeout

Der Timeout schaltet den Port wieder in den Zustand Nicht-Bereit, wenn keine Daten empfangen werden. Mit einem Timeout von Null wird diese Funktion ausgeschaltet. In diesem Fall ist der Port immer bereit, wenn der Daten-Modus gewählt ist.

6.19.4.3 Netzwerk-Einstellungen

Diese Tabelle enthält alle Einstellungen, die das Verhalten des COM-Ports im Netzwerk definieren.

Bitte beachten Sie, dass alle diese Parameter durch die Gegenstelle überschrieben werden können, wenn die RFC-2217-Verhandlung aktiviert ist; die aktuellen Einstellungen können im Status-Menü eingesehen werden.



LANconfig: **Sonstige Dienste** > **COM-Ports** > **Netzwerk-Schnittstelle**

Konsole: **Setup** > **COM-Ports** > **COM-Port-Server** > **Netzwerk-Einstellungen**

Gerätetyp

Auswahl aus der Liste der im Gerät verfügbaren seriellen Schnittstellen.

Port

Manche seriellen Geräte wie z. B. die CardBus haben mehr als einen seriellen Port. Tragen Sie hier die Nummer des Ports ein, der auf der seriellen Schnittstelle für den COM-Port-Server genutzt werden soll.

TCP-Mode

Jede Instanz des COM-Port-Servers überwacht im Server-Modus den definierten Listen-Port auf eingehende TCP-Verbindungen. Pro Instanz ist nur eine aktive Verbindung erlaubt, alle anderen Verbindungsanfragen werden abgelehnt. Im Client-Modus versucht die Instanz eine TCP-Verbindung über einen definierten Port zur angegebenen Gegenstelle aufzubauen, sobald der Port bereit ist. Die TCP-Verbindung wird wieder geschlossen, sobald der Port nicht mehr bereit ist. In beiden Fällen schließt ein Gerät die offenen Verbindungen bei einem Neustart des Gerätes.

Listen-Port

Auf diesem TCP-Port erwartet der COM-Port im TCP-Server-Modus eingehende Verbindungen.

Zugriff vom WAN

Der Zugriff auf diese serielle Schnittstelle vom WAN ist **erlaubt**, **nicht erlaubt** oder **nur über VPN erlaubt**.

Connect-Hostname

Zu diesem Host baut der COM-Port im TCP-Client-Modus eine Verbindung auf, sobald sich der Port im Zustand „Bereit" befindet.

Connect-Port

Über diesen TCP-Port baut der COM-Port im TCP-Client-Modus eine Verbindung auf, sobald sich der Port im Zustand „Bereit" befindet.

RFC 2217 Erweiterung aktiviert

Die RFC 2217-Erweiterung kann für beide TCP-Modi aktiviert werden. Wenn diese Erweiterung eingeschaltet ist, signalisiert ein Gerät seine Bereitschaft, Telnet-Steuerungssequenzen zu akzeptieren, mit der Sequenz IAC DO COM-PORT-OPTION. In der Folge werden auf dem COM-Port die entsprechenden Optionen verwendet, die konfigurierten Default-Werte werden überschrieben. Außerdem versucht der Port, für Telnet das lokale Echo und den Line Mode zu verhandeln. Die Verwendung der RFC 2217-Erweiterung ist auch bei nicht kompatibler Gegenstelle unkritisch, möglicherweise werden dann unerwartete Zeichen bei der Gegenstelle angezeigt. Als Nebeneffekt führt die Verwendung der RFC 2217-Erweiterung dazu, dass der Port einen regelmäßigen Alive-Check durchführt, indem Telnet-NOPs zur Gegenstelle gesendet werden.

Binär-Modus

Serielle Daten werden binär weitergeleitet, d. h. es erfolgt keine CR / LF (Carriage Return / Line Feed) Anpassung.

Newline-Konversion

Die Einstellung Newline-Konversion definiert die Zeichensequenz, die zum seriellen Anschluss geschickt wird, wenn ein Zeilenschaltungs-Zeichen im Nicht-Binärmodus erkannt wird. Die Standardeinstellung (CRLF) bildet das ab, was über die TCP-Verbindung empfangen wurde, aber dies ist nicht unbedingt die korrekte Einstellung für alle Applikationen. Beispielsweise interpretieren einige Unix Konsolen diese Sequenz als eine unerwünschte doppelte Zeilenschaltung, so dass ein einzelner Zeilenvorschub (LF) oder Rücklauf (CR) angebrachter wäre. Wenn der Outband-Anschluss eines anderen LANCOM Gerätes mit der seriellen Schnittstelle verbunden wird, werden CRLF oder CR funktionieren, aber kein LF, weil CR Zeichen vom LANCOM Gerät für das Auto-Bauding-Feature verwendet werden.

TCP-Keepalive

Wenn aktiviert, dann werden regelmässig Dummy-Pakete zur Gegenseite geschickt. Diese Pakete beinhalten keinen Payload, hindern aber Firewalls und NAT Gateways daran, die Verbindung zu verwerfen, da sie immer aktiv erscheint. In Erweiterung zu RFC 1122 bietet TCP Keep-Alive drei Betriebsmodi:

Inaktiv

Es werden keine Pakete in Leerlaufzeiten versendet.

Aktiv

Pakete werden regelmässig versendet, wobei das Fehlen von Antwortpaketen keine weiteren Auswirkungen hat. Verbindungen zu Firewalls oder NAT Gateways werden aufrecht erhalten. Ein vollständiger Abbruch der TCP-Verbindung wird nicht erkannt. Dieser Betriebsmodus wird für Serverbetrieb empfohlen.

Proaktiv

Zusätzlich erwartet der TCP-Stack Antworten zu seinen Keep-Alive Paketen und wird eine abgebrochene TCP-Verbindung melden, wenn nach mehreren Versuchen keine Antwort erhalten wird. Die Anzahl der Versuche ist dieselbe wie beim **TCP-Retry-Count**.

TCP-Keepalive-Intervall

Hier legen Sie fest, wie oft der TCP-Stack Keep-Alive-Pakete überträgt. Beim Wert 0 wird der interne Standardwert von 7200 Sekunden verwendet.

TCP-Retransmit-Timeout

Die Zeitspanne, nach der eine Übertragungswiederholung gestartet wird. Beachten Sie, dass die Zeitspanne, bis eine Verbindung als abgebrochen erkannt wird, die Dauer aller Übertragungswiederholungen beinhaltet.

TCP-Retry-Count

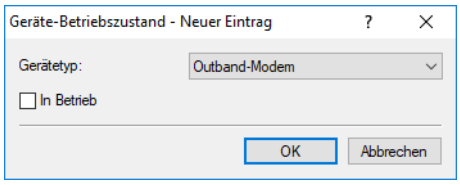
Die Gesamtzahl aller Übertragungswiederholungen wird hier begrenzt. Ein Wiederholungszähler von 0 spezifiziert den Standardwert von 5 Wiederholungen.

Absende-Adresse

Über diese Adresse kann der COM-Port angesprochen werden. Dies ist die eigene IP-Adresse, die als Quelladresse beim Verbindungsaufbau benutzt wird. Sie wird z. B. verwendet, um die IP-Route festzulegen, über die die Verbindung aufgebaut wird.

6.19.5 Konfiguration der WAN-Geräte

Die Tabelle mit den WAN-Geräten dient nur als Status-Tabelle. Alle Hotplug-Geräte (über USB oder CardBus angeschlossen) tragen sich selbst in diese Tabelle ein.



LANconfig: **Sonstige Dienste** > **COM-Ports** > **Geräte-Betriebszustand**

Konsole: **Setup** > **COM-Ports** > **WAN** > **Geraete**

Gerätetyp

Liste der im Gerät verfügbaren seriellen Schnittstellen.

In Betrieb

Status des angeschlossenen Gerätes.

6.19.6 Status-Informationen über die seriellen Verbindungen

Für jede Instanz des COM-Port-Servers werden verschiedene Statistiken und Zustandswerten erfasst. Der serielle Port, den die Instanz verwendet, wird in den beiden ersten Spalten der Tabelle angegeben – hier werden die bei der Konfiguration eingetragenen Werte für Device-Type und Port-Nummer angezeigt.

6.19.6.1 Netzwerk-Status

Konsole: **Status** > **COM-Ports** > **COM-Port-Server** > **Netzwerk-Status**

Diese Tabelle enthält alle Informationen über die aktuellen und die vorherigen TCP-Verbindungen.

- Device-Type

  Liste der im Gerät verfügbaren seriellen Schnittstellen.

- Port-Nummer

  Nummer des Ports, der auf der seriellen Schnittstelle für den COM-Port-Server genutzt wird.

- Connection-Status

  Mögliche Werte:

  - Verbunden: Eine Verbindung ist aktiv (Server- oder Client-Modus).
  - Hoerend: Diese Instanz arbeitet im Server-Modus, derzeit ist keine TCP-Verbindung aktiv.
  - Nicht-hoerend: Im Server-Modus konnte der angegebene TCP-Port nicht für eingehende Verbindungen reserviert werden, z. B. weil er bereits von einer anderen Applikation belegt ist.

- Leer: Diese Instanz arbeitet im Client-Modus und der Port ist nicht bereit, daher wird derzeit keine TCP-Verbindung aufgebaut.
- Verbinden: Der Port hat den Zustand “Bereit” erreicht, es wird eine Verbindung aufgebaut.

- Last-Error

  Zeigt im Client-Modus den Grund für den letzten Verbindungsfehler an. Im Server-Modus hat dieser Wert keine Bedeutung.

- Remote-Address

  Zeigt die IP-Adresse der Gegenstelle bei einer erfolgreichen TCP-Verbindung an.

- Local-Port

  Zeigt den verwendeten lokalen TCP-Port bei einer erfolgreichen TCP-Verbindung an.

- Remote-Port

  Zeigt den verwendeten entfernten TCP-Port bei einer erfolgreichen TCP-Verbindung an.

6.19.6.2 COM-Port-Status

Diese Tabelle zeigt den Zustand des seriellen Ports und die auf diesem Port aktuell verwendeten Einstellungen.

- Device-Type

  Liste der im Gerät verfügbaren seriellen Schnittstellen.

- Port-Nummer

  Nummer des Ports, der auf der seriellen Schnittstelle für den COM-Port-Server genutzt wird.

- Port-Status

  Mögliche Werte:

  - Nicht-Vorhanden: Der serielle Port ist derzeit nicht für den COM-Port-Server verfügbar, z. B. weil der USB- oder CardBus-Adapter entfernt wurde oder weil die Schnittstelle von einer anderen Funktion des Geräts verwendet wird.
  - Nicht-Bereit: Der serielle Port ist prinzipiell für den COM-Port-Server verfügbar, derzeit aber nicht bereit für eine Datenübertragung, z. B. weil die DTR-Leitung nicht aktiv ist. Im Client-Zustand wird kein Verbindungsaufbau versucht, solange der Port in diesem Zustand ist.
  - Bereit: Der serielle Port ist verfügbar und bereit für eine Datenübertragung. Im Client-Zustand wird versucht, eine TCP-Verbindung aufzubauen, sobald der Port in diesem Zustand ist.

  Bitte beachten Sie, dass der Port-Status auch im Server-Modus von Bedeutung ist. Alle TCP-Verbindungsanfragen werden akzeptiert, allerdings wird die COM-Port-Instanz erst dann Daten zwischen dem seriellen Port und dem Netzwerk übertragen, wenn der serielle Port den Zustand “Bereit” erreicht hat. Die folgenden Spalten zeigen die Einstellungen, die auf dem seriellen Port aktuell verwendet werden. Sie entsprechen entweder den konfigurierten Werten oder den Werten, die bei der Verhandlung über die RFC2217-Erweiterungen ermittelt wurden.

- Bit-Rate

  Verwendete Bitrate auf dem COM-Port.

- Daten-Bits

  Anzahl der Daten-Bits.

- Paritaet

  Auf dem COM-Port verwendetes Prüfverfahren.

- Stop-Bits

  Anzahl der Stop-Bits.

- Handshake

  Auf dem COM-Port verwendete Datenflusskontrolle.

6.19.6.3 Byte-Counters

In dieser Tabelle werden die eingehenden und ausgehenden Datenpakete auf dem seriellen Port und der Netzwerk-Seite angezeigt.

Diese Werte werden nicht zurückgesetzt, wenn der entsprechende Anschluss geöffnet oder geschlossen wird.

- Device-Type

  Liste der im Gerät verfügbaren seriellen Schnittstellen.
- Port-Nummer

  Nummer des Ports, der auf der seriellen Schnittstelle für den COM-Port-Server genutzt wird.
- Seriell-Tx

  Anzahl der auf der seriellen Schnittstelle gesendeten Bytes.
- Seriell-Rx

  Anzahl der auf der seriellen Schnittstelle empfangenen Bytes.
- Netzwerk-Tx

  Anzahl der auf der Netzwerkseite gesendeten Bytes.
- Netzwerk-Rx

  Anzahl der auf der Netzwerkseite empfangenen Bytes.

6.19.6.4 Port-Errors

In dieser Tabelle werden die Fehler auf dem seriellen Port angezeigt. Diese Fehler können auf ein fehlerhaftes Kabel oder auf Fehler in der Konfiguration hinweisen.

- Device-Type

  Liste der im Gerät verfügbaren seriellen Schnittstellen.
- Port-Nummer

  Nummer des Ports, der auf der seriellen Schnittstelle für den COM-Port-Server genutzt wird.
- Paritaets-Fehler

  Anzahl der Fehler aufgrund einer nicht übereinstimmenden Prüfsumme.
- Rahmen-Fehler

  Anzahl der fehlerhaften Datenpakete.

6.19.6.5 Verbindungen

In dieser Tabelle werden die erfolgreichen und gescheiterten TCP-Verbindungen angezeigt, sowohl im Server wie auch im Client-Modus.

- Device-Type

  Liste der im Gerät verfügbaren seriellen Schnittstellen.
- Port-Nummer

  Nummer des Ports, der auf der seriellen Schnittstelle für den COM-Port-Server genutzt wird.
- Server-gestattet

Anzahl der Verbindungen, die der COM-Port-Server gestattet hat.

- Server-abgelehnt

  Anzahl der Verbindungen, die der COM-Port-Server abgelehnt hat.

- Client-erfolgreich

  Anzahl der Verbindungen, die der COM-Port-Client erfolgreich aufgebaut hat.

- Client-DNS-Fehler

  Anzahl der Verbindungen, die der COM-Port-Client aufgrund von DNS-Fehlern nicht aufbauen konnte.

- Client-TCP-Fehler

  Anzahl der Verbindungen, die der COM-Port-Client aufgrund von TCP-Fehlern nicht aufbauen konnte.

- Client-Gegenstelle-getrennt

  Anzahl der Verbindungen, bei denen der COM-Port-Client von der Gegenstelle getrennt wurde.

6.19.6.6 Delete-Values

Diese Aktion löscht alle Werte in den Status-Tabellen.

6.19.7 COM-Port-Adapter

Zum Anschluss von Geräten mit seriellen Schnittstellen an ein Geräten stehen folgende Möglichkeiten bereit:

Adapter	Geräte
COM-Port-Adapter	Alle mit serieller Konfigurationsschnittstelle
USB-Seriell-Adapter	Alle mit USB-Schnittstelle

Der COM-Port-Adapter muss als beidseitiger Sub-D Stecker mit folgender PIN-Belegung ausgeführt werden:

Pin	Signal	Signal	Pin
2	RxD	TxD	3
3	TxD	RxD	2
4	DTR	DSR	6
5	GND	GND	5
6	DSR	DTR	4
7	RTS	CTS	8
8	CTS	RTS	7

6.20 IGMP- / MLD-Snooping

6.20.1 Einleitung

Alle Geräte mit WLAN-Schnittstellen verfügen über eine „LAN-Bridge“, die für die Übertragung der Daten zwischen den Ethernet-Ports und den WLAN-Schnittstellen sorgen. Die LAN-Bridge arbeitet dabei in vielen Aspekten wie ein Switch. Die zentrale Aufgabe eines Switches – im Gegensatz zu einem Hub – besteht darin, Pakete nur an den Port weiterzuleiten, an dem der Empfänger angeschlossen ist. Dazu bildet der Switch automatisch aus den eingehenden Datenpaketen eine Tabelle, in der die Absender-MAC-Adressen den Ports zugeordnet werden.

Wenn eine Ziel-Adresse eines eingehenden Pakets in dieser Tabelle gefunden wird, kann der Switch das Paket gezielt an den richtigen Port weiterleiten. Wird die Ziel-Adresse nicht gefunden, so leitet der Switch das Paket an alle Ports weiter. D. h. ein Switch kann ein Paket nur dann zielgerichtet weiterleiten, wenn die Zieladresse schon einmal als Absenderadresse eines Pakets über einen bestimmten Port bei ihm eingegangen ist. Broadcast- oder Multicast-Pakete können aber niemals als Absenderadresse in einem Paket eingetragen sein, darum werden diese Pakete immer auf alle Ports „geflutet".

Während dieses Verhalten für Broadcasts die richtige Aktion ist (Broadcasts sollen schließlich alle möglichen Empfänger erreichen), ist es für Multicasts nicht unbedingt die gewünschte Lösung. Multicasts richten sich in der Regel an eine bestimmte Gruppe von Empfängern in einem Netzwerk, nicht aber an alle:

- Videostreams werden z. B. häufig als Multicast übertragen, aber nicht alle Stationen im Netzwerk sollen einen bestimmten Stream empfangen.
- Verschiedene Anwendungen im medizinischen Bereich nutzen Multicasts, um Daten an bestimmte Endgeräte zu übertragen, die nicht an allen Stationen eingesehen werden sollen.

Bei einer LAN-Bridge im Gerät wird es daher auch Ports geben, an denen kein einziger Empfänger des Multicasts angeschlossen ist. Das „überflüssige" Versenden der Multicasts auf Ports ohne Empfänger ist zwar kein Fehler, es führt aber zu Performance-Problemen:

- Viele Stationen können die unerwünschten Multicasts nicht in der Hardware der Netzwerkadapter aussortieren, sondern reichen die Pakete einfach an die höher gelegenen Protokollschichten weiter, was zu einer höheren Belastung der CPU führt.
- Gerade in WLANs kann die unnötige Aussendung der Multicasts zu einer deutlichen Einschränkung der verfügbaren Bandbreite führen, wenn keiner der angemeldeten WLAN-Clients Bedarf für den Multicast hat.

Mit dem Internet Group Management Protocol (IGMP) für IPv4 bzw. Multicast Listener Discovery (MLD) für IPv6 stellt die TCP/IP-Protokollfamilie Protokolle bereit, mit denen die Netzwerkstationen dem Router, an dem sie angeschlossen sind, das Interesse an bestimmten Multicasts mitteilen können. Dazu registrieren sich die Stationen bei den Routern für bestimmte Multicast-Gruppen, von denen Sie die entsprechenden Pakete beziehen wollen (Multicast-Registration). IGMP und MLD nutzen dazu spezielle Nachrichten zum Anmelden (Join-Messages) und Abmelden (Leave-Messages).



Die Information, in welchen Multicast-Gruppen sich eine Station registrieren kann oder soll, erhält die Station über andere Protokolle außerhalb von IGMP / MLD.

Sowohl IGMP als auch MLD können als Layer-3-Protokolle nur IP-Subnetze entsprechend der Anmeldungen an Multicast-Gruppen verwalten. Die in den Netzwerkstrukturen vorhandenen Geräte wie Bridges, Switches oder WLAN Access Points leiten die Pakete aber oft nur auf Layer 2 weiter, so dass IGMP und MLD zunächst keine Funktionen bieten, um die Pakete zielgerichtet durch diese Netzwerkstrukturen zu leiten. Die Bridges nutzen daher die Multicast-Registrierung zwischen Stationen und Routern, um zusätzliche Informationen über die zielgerichtete Verteilung der Multicasts zu erhalten. IP-Multicasts müssen nur an die Ports weitergeleitet werden, an denen sich ein Router befindet, der Multicast-Routing beherrscht und die Pakete in bestimmte IP-Subnetze weiterleiten kann. Dieses Verfahren wird bei IPv4 als IGMP-Snooping und bei IPv6 als MLD-Snooping bezeichnet. Die Bridges, die eigentlich die Entscheidung für das Weiterleiten der Pakete anhand der MAC auf Layer 2 treffen, nutzen damit zusätzlich die Layer 3-Informationen der IP-Multicast-Pakete.

Für die weitere Beschreibung der Funktionen des IGMP- / MLD-Snooping im LCOS werden zwei wesentliche Begriffe unterschieden:

- Ein Port ist „Mitglied einer Multicast-Gruppe", wenn mindestens eine daran angeschlossene Station Pakete für eine bestimmte Multicast-Adresse empfangen möchte. Diese Multicast-Registrierung kann sowohl dynamisch über IGMP- oder MLD-Snooping gelernt wie auch manuell konfiguriert sein.
- Ein Port ist ein „Router-Port", wenn daran ein Router angeschlossen ist, der Multicast-Routing beherrscht und die Pakete in bestimmte IP-Subnetze weiterleiten kann.
- Eine Multicast-Gruppe ist „nicht registriert", wenn kein Port der Bridge Mitglied dieser Multicast-Gruppe ist.

6.20.2 Ablauf des IGMP- / MLD-Snooping

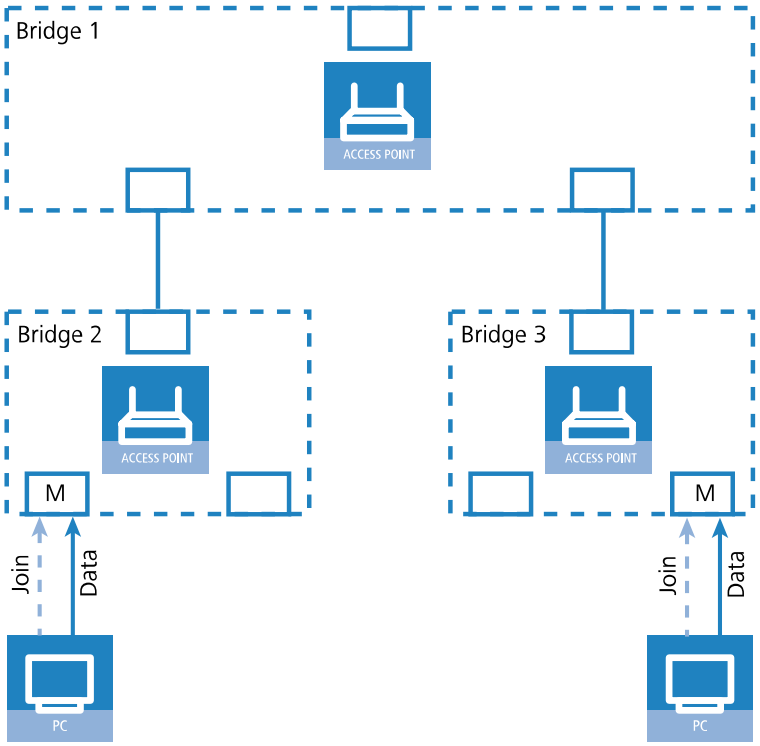
Beim Empfang eines Pakets unterscheidet die Bridge zunächst, ob es sich um einen Broadcast, Multicast oder Unicast handelt. Broadcasts und Unicasts werden wie üblich weitergeleitet, d. h. entweder auf alle Ports oder nur auf den Port, an den entsprechend des Eintrags in der MAC-Tabelle der Empfänger angeschlossen ist.

Für die IP-Multicast-Pakete werden zwei Typen unterschieden (abgeschnittene Pakete oder Pakete mit ungültiger Prüfsumme werden dabei verworfen):

- IGMP- / MLD-Nachrichten werden je nach Inhalt unterschiedlich behandelt:
  - Eine Join-Message führt dazu, dass der Port, über den das Paket eingeht, Mitglied der entsprechenden Multicast-Gruppe wird. Diese Nachricht wird nur an Router-Ports weitergeleitet.
  - Leave-Messages werden nicht beachtet, da das IGMP- / MLD-Snooping im LCOS passiv ist Somit verschwinden Joins nur durch Alterung aus der Tabelle.
  - Eine eingehende IGMP- / MLD-Anfrage macht den Port zu einem Router-Port. Diese Nachrichten werden an alle Ports weitergeleitet.
  - Alle anderen IGMP- / MLD-Nachrichten werden an alle Ports weitergeleitet – dabei werden keine der Port-Eigenschaften geändert.
- Wenn es sich bei einem IP-Multicast-Paket nicht um eine IGMP- / MLD-Nachricht handelt, wird die Ziel-Adresse ausgewertet. Pakete für die IPv4-Zieladresse „224.0.0.x" bzw. bei IPv6 „FF02::1" werden dabei an alle Ports weitergeleitet, weil dieser „reservierte" Bereich von Protokollen ohne richtige IGMP- / MLD-Registrierung verwendet wird. Für alle anderen Pakete wird die Zieladresse in der Tabelle der IGMP- / MLD-Mitgliedschaften ermittelt:
  - Wenn die Adresse gefunden wird, wird das Paket an die entsprechenden Ports weitergeleitet.
  - Wenn die Adresse nicht gefunden wird, wird das Paket je nach Konfiguration entweder verworfen, an alle Ports oder ausschließlich an alle Router-Ports weitergeleitet.

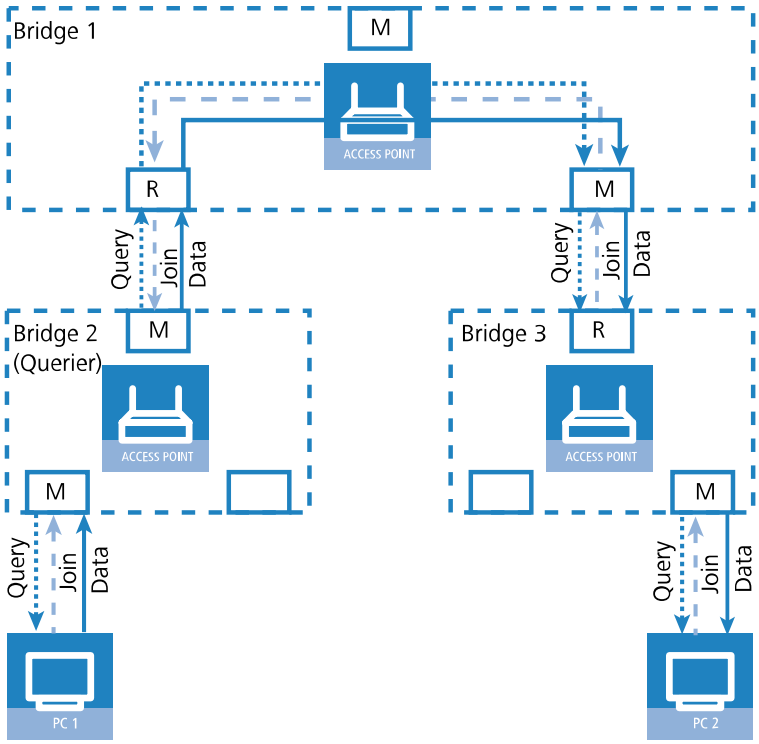
6.20.3 IGMP- / MLD-Snooping über mehrere Bridges hinweg

Wie beschrieben leitet IGMP- / MLD-Snooping eingehende Join- oder Leave-Nachrichten nur über Router-Ports weiter. In einer Struktur mehrerer Bridges sind zu Beginn alle Ports weder Router-Port noch Mitglied einer Multicast-Gruppe. Wenn sich die an den Bridges angeschlossenen Stationen für eine Multicast-Gruppe registrieren, wird der verwendete Port automatisch Mitglied dieser Gruppe. In dieser Phase ist allerdings keiner der Ports als Router-Port aktiviert, daher werden die Join-Nachrichten auch nicht an andere Bridges weitergeleitet. Die übergeordneten Bridges erfahren also nichts von der Mitgliedschaft des Ports in der gewünschten Multicast-Gruppe.



Die Bridges müssen also über Router-Ports verfügen, damit sich die Informationen über die Mitgliedschaften in Multicast-Gruppen verbreiten können. Da die Ports der Bridge nur durch IGMP- / MLD-Anfragen zu Router-Ports werden können, muss einer der Multicast-fähigen Router im Netzwerk die Aufgabe übernehmen, die benötigten IGMP- / MLD-Anfragen in Netzwerk zu streuen. Dieser Router wird auch als IGMP- / MLD-Querier bezeichnet. Für den Fall, dass kein Multicast-Router im Netzwerk vorhanden ist, können die Access Points einen Querier simulieren. Um parallele Anfragen von unterschiedlichen Querier-Instanzen zu vermeiden, schaltet sich eine Querier-Instanz ab, wenn ein anderer Querier mit niedrigerer IP-Adresse gefunden wird. Die Verteilung der IGMP- / MLD-Informationen durch den Querier lässt sich an folgendem Beispiel erklären:

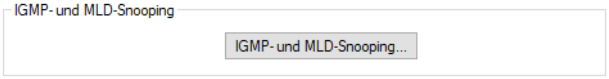
1. Der Querier (im Beispiel Bridge 2) sendet in regelmäßigen Abständen IGMP- / MLD-Anfragen über alle verfügbaren Ports aus (gepunktete Linien). Diese Anfragen kennzeichnen in der nächsten Bridge (Bridge 1) den Port, auf dem die Anfrage eingeht, als Router-Port (R). PC 1 antwortet auf diese Anfrage mit einer Join-Nachricht für alle Multicast-Gruppen (helle gestrichelte Linien), in welchen diese Station sich registrieren möchte. Der Port, an dem PC 1 an Bridge 2 angeschlossen ist, wird damit Mitglied der entsprechenden Multicast-Gruppe(n).
2. Außerdem versendet die Bridge 1 die Anfragen über alle anderen Ports an angeschlossene Bridges und Stationen weiter unten in der Struktur. In Bridge 3 wird der Port, über den die Anfrage eingeht, dadurch zum Router-Port (R).
3. Auch die an Bridge 3 angeschlossene Station (PC 2) antwortet auf diese Anfrage mit einer Join-Nachricht für alle registrierten Multicast-Gruppen. Der Port, an dem PC 2 an Bridge 3 angeschlossen ist, wird damit Mitglied der entsprechenden Multicast-Gruppe(n).
4. Bridge 3 leitet diese Join-Nachricht über den Router-Port weiter an Bridge 1. Der empfangende Port von Bridge 1 wird damit auch Mitglied der Multicast-Gruppen, für die sich PC 2 registriert hat.
5. Im letzten Schritt leitet Bridge 1 die Join-Nachricht von PC 2 über den Router-Port weiter an Bridge 2, wo der empfangende Port ebenfalls Mitglied der Multicast-Gruppen von PC 2 wird.

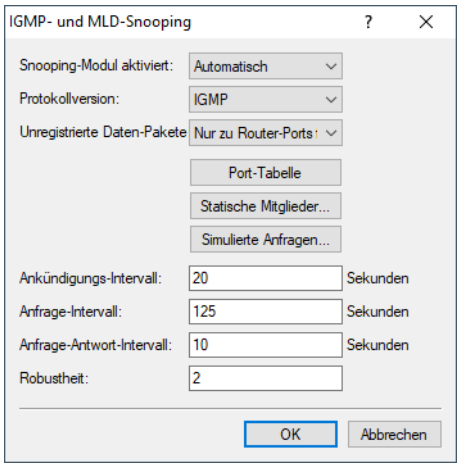


Wenn nun PC 1 einen Multicast aussendet für eine der von PC 2 registrierten Multicast-Gruppen, leiten alle Bridges (2, 1 und dann 3) die Pakete jeweils über den Mitglieds-Port weiter bis zu PC 2.

6.20.4 Konfiguration

Die Konfiguration des IGMP- / MLD-Snooping finden Sie im LANconfig unter **Schnittstellen** > **Snooping** > **IGMP- und MLD-Snooping**





Snooping-Modul aktiviert

Aktiviert oder deaktiviert IGMP- / MLD-Snooping für das Gerät und alle definierten Querier-Instanzen. Ohne IGMP- / MLD-Snooping verhält sich die Bridge wie ein einfacher Switch und sendet alle Multicasts auf alle Ports weiter.

Mögliche Werte:

- Ein
- Aus
- Automatisch

Default:

- Automatisch

In der Einstellung **Automatisch** aktiviert die Bridge das IGMP- / MLD-Snooping nur, wenn auch Querier im Netz vorhanden sind.

Wenn diese Funktion deaktiviert ist, sendet die Bridge alle IP-Multicast-Pakete über alle Ports. Bei einer Änderung des Betriebszustandes setzt die Bridge die IGMP- / MLD-Snooping-Funktion vollständig zurück, d. h. sie löscht alle dynamisch gelernten Werte (Mitgliedschaften, Router-Port-Eigenschaften).

Protokollversion

Geben Sie die unterstützten Protokolle an: IGMP, MLD oder beide.

Unregistrierte Datenpakete

Diese Option definiert die Verarbeitung von Multicast-Paketen mit Ziel-Adressen außerhalb des reservierten Adress-Bereiches „224.0.0.x" bzw. bzw. bei IPv6 „FF02::1", für die weder dynamisch gelernte noch statisch konfigurierte Mitgliedschaften vorhanden sind.

Mögliche Werte:

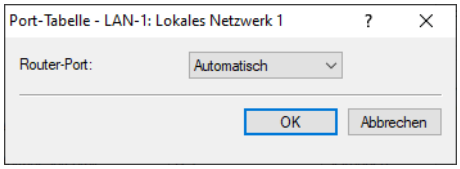
- Nur zu Router-Ports fluten: Sendet diese Pakete an alle Router-Ports.
- Zu allen Ports fluten: Sendet diese Pakete an alle Ports.
- Verwerfen: Verwirft diese Pakete.

Default:

- Nur-Router-Ports

Port-Tabelle

In dieser Tabelle können Sie die Port-bezogenen Einstellungen für IGMP- / MLD-Snooping vornehmen.



Port

Auf diesen Port beziehen sich die Einstellungen.

Mögliche Werte:

- Auswahl aus der Liste der im Gerät verfügbaren Ports.

Default:

- N/A

Router-Port

Diese Option definiert das Verhalten des Ports.

Mögliche Werte:

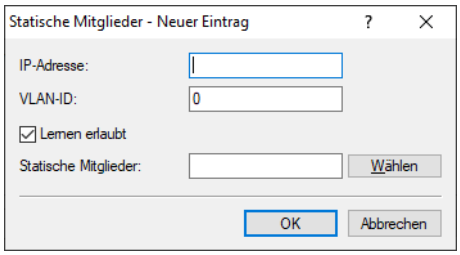
- Ja: Dieser Port verhält sich immer wie ein Router-Port, unabhängig von den IGMP-Anfragen oder Router-Meldungen, die die Bridge auf diesem Port evtl. empfängt.
- Nein: Dieser Port verhält sich nie wie ein Router-Port, unabhängig von den IGMP-Anfragen oder Router-Meldungen, die die Bridge auf diesem Port evtl. empfängt.
- Automatisch: Dieser Port verhält sich wie ein Router-Port, wenn eine IGMP-Anfragen oder Router-Meldung empfangen wurde. Der Port verliert diese Eigenschaft wieder, wenn die Bridge auf diesem Port für die Dauer von "Robustheit*Anfrage-Intervall+(Anfrage-Antwort-Intervall/2)" keine entsprechenden Pakete empfängt.

Default:

- Automatisch

Statische Mitglieder

Diese Tabelle erlaubt die manuelle Definition von Mitgliedschaften, die z. B. nicht automatisch gelernt werden können oder sollen.



IP-Adresse

Die IP-Adresse der manuell definierten Multicast-Gruppe.

Mögliche Werte:

- Gültige IP-Multicast-Adresse.

VLAN-ID

Die VLAN-ID, auf welche die Bridge diese statische Mitgliedschaft anwenden soll. Für eine IP-Multicast-Adresse können Sie durchaus mehrere Einträge mit unterschiedlichen VLAN-IDs eintragen.

Mögliche Werte:

- 0 bis 4096.

Default:

- 0

Besondere Werte:

- Wenn „0“ als VLAN gewählt wird, werden die IGMP- / MLD-Anfragen ohne VLAN-Tag ausgegeben. Dieser Wert ist daher nur sinnvoll, wenn die Verwendung von VLAN generell deaktiviert ist.

Lernen erlaubt

Mit dieser Option aktivieren Sie das automatische Lernen von Mitgliedschaften für diese Multicast-Gruppe. Wenn das automatische Lernen deaktiviert ist, verschickt die Bridge die Pakete nur über die für die Multicast-Gruppe manuell definierten Ports.

Statische Mitglieder

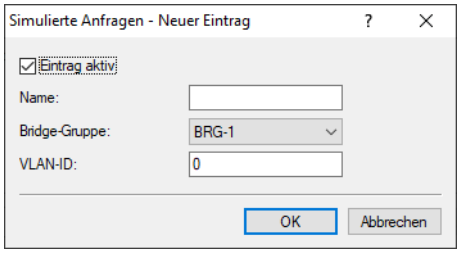
An diese Ports stellt die Bridge die Pakete mit der entsprechenden IP-Multicast-Adresse immer zu, unabhängig von empfangenen Join-Nachrichten.

Mögliche Werte:

- Kommaseparierte Liste der gewünschten Ports, maximal 215 alphanumerische Zeichen.

Simulierte Anfragen

Diese Tabelle enthält alle im Gerät definierten simulierten Querier. Diese Einheiten werden eingesetzt, wenn kein Multicast-Router im Netzwerk vorhanden ist, aber dennoch die Funktionen des IGMP- / MLD-Snooping benötigt werden. Um die Querier auf bestimmte Bridge-Gruppen oder VLANs einzuschränken, können Sie mehrere unabhängige Querier definieren, welche dann die entsprechenden VLAN-IDs nutzen.



Eintrag aktiv

Aktiviert oder deaktiviert die Querier-Instanz.

Name

Name der Querier-Instanz.

Mögliche Werte:

- 8 alphanumerische Zeichen.

Bridge-Gruppe

Schränkt die Querier-Instanz auf eine bestimmte Bridge-Gruppe ein.

Mögliche Werte:

- Auswahl aus der Liste der verfügbaren Bridge-Gruppen
- keine

Default:

- BRG-1

Besondere Werte:

- Ist „keine" Bridge-Gruppe gewählt, gibt die Bridge die IGMP- / MLD-Anfragen auf allen Brigde-Gruppen aus.

VLAN-ID

Schränkt die Querier-Instanz auf ein bestimmtes VLAN ein.

Mögliche Werte:

- 0 bis 4096

Default:

- 0

Besondere Werte:

- Ist „0“ als VLAN-ID gewählt, gibt die Bridge die IGMP- / MLD-Anfragen ohne VLAN-Tag aus. Dieser Wert ist daher nur sinnvoll, wenn die Verwendung von VLAN generell deaktiviert ist.

Ankündigungs-Intervall

Intervall in Sekunden, in dem die Geräte Pakete aussenden, mit denen sie sich als Multicast-fähige Router bekanntmachen. Aufgrund dieser Information können andere IGMP- / MLD-Snooping-fähige Geräte schneller lernen, welche ihrer Ports Sie als Router-Ports verwenden sollen. Beim Aktivieren von Ports kann ein Switch z. B. eine entsprechende Anfrage nach Multicast-Routern versenden, die der Router mit einer solchen Bekanntmachung beantworten kann. Diese Methode ist je nach Situation ggf. deutlich schneller als die alternative Lernmöglichkeit über die IGMP- / MLD-Anfragen.

Mögliche Werte:

- 4 bis 180 Sekunden

Default:

- 20 Sekunden

Anfrage-Intervall

Intervall in Sekunden, in dem ein Multicast-fähiger Router (oder ein simulierter Querier) IGMP- / MLD-Anfragen an die Multicast-Adresse `224.0.0.1` bzw. bei IPv6 „FF02::1“ schickt und damit Rückmeldungen der Stationen über die Mitgliedschaft in Multicast-Gruppen auslöst. Diese regelmäßigen Abfragen beeinflussen den Zeitpunkt, nach dem die Bridge die Mitgliedschaft in bestimmten Multicast-Gruppen „altern“ lässt und löscht.

- Ein Querier sendet nach der Anfangsphase IGMP- / MLD-Anfragen in diesem Intervall.
- Ein Querier kehrt zurück in den Querier-Status nach einer Zeit von „Robustheit*Anfrage-Intervall+(Anfrage-Antwort-Intervall/2)“.
- Ein Router-Port verliert seine Eigenschaften nach einer Alterungszeit von „Robustheit*Anfrage-Intervall+(Anfrage-Antwort-Intervall/2)“.

Mögliche Werte:

- Zahl aus 10 Ziffern größer als 0.

Default:

- 125

Das Anfrage-Intervall muss größer als das Anfrage-Antwort-Intervall sein.

Anfrage-Antwort-Intervall

Intervall in Sekunden, welches das das Timing zwischen den IGMP- / MLD-Anfragen und dem Altern der Router-Ports bzw. Mitgliedschaften beeinflusst.

Intervall in Sekunden, in dem ein Multicast-fähiger Router (oder ein simulierter Querier) Antworten auf seine IGMP- / MLD-Anfragen erwartet. Diese regelmäßigen Abfragen beeinflussen den Zeitpunkt, nach dem die Mitgliedschaft in bestimmten Multicast-Gruppen „altern“ und gelöscht werden.

Mögliche Werte:

› Zahl aus 10 Ziffern größer als 0.

Default:

› 10

Das Anfrage-Antwort-Intervall muss kleiner als das Anfrage-Intervall sein.

Robustheit

Dieser Wert bestimmt die Robustheit des IGMP- / MLD-Protokolls. Diese Option toleriert den Paketverlust von IGMP- / MLD-Anfragen gegenüber den Join-Nachrichten.

Mögliche Werte:

› Zahl aus 10 Ziffern größer als 0.

Default:

› 2

6.20.5 IGMP- / MLD-Status

6.20.5.1 Allgemeine Statistiken

Die Status-Meldungen zu IGMP- / MLD-Snooping finden Sie unter:

Konsole: **Status** > **LAN-Bridge-Statistiken** > **IGMP-Snooping**

› In-Betrieb

Zeigt an, ob das IGMP- / MLD-Snooping aktiviert oder deaktiviert ist.

› IPv4-Pakete

Zeigt die gesamte Anzahl der IPv4-Multicast-Pakete, die auf allen Ports empfangen wurden, unabhängig davon, ob es sich um IGMP-Pakete handelt oder nicht.

› IPv6-Pakete

Zeigt die gesamte Anzahl der IPv6-Multicast-Pakete, die auf allen Ports empfangen wurden, unabhängig davon, ob es sich um MLD-Pakete handelt oder nicht.

› Daten-Pakete

Zeigt die gesamte Anzahl der nicht beschädigten IP-Multicast-Pakete, die auf allen Ports empfangen wurden, und bei denen es sich nicht um IGMP- / MLD-Pakete handelt.

› Steuer-Pakete

Zeigt die gesamte Anzahl der nicht beschädigten IGMP- / MLD-Pakete, die auf allen Ports empfangen wurden.

› Defekte-Pakete

Zeigt die gesamte Anzahl der beschädigten Daten- oder IGMP- / MLD-Pakete, die auf allen Ports empfangen wurden. Mögliche Ursachen für die Beschädigung der Pakete sind IP-Prüfsummenfehler oder abgeschnittene Pakete.

Aus Performance-Gründen werden IP-Prüfsummen nur für IGMP- / MLD-Pakete ausgewertet, nicht für den Datenteil der Multicast-Pakete. Daher werden Pakete mit einer fehlerhaften Prüfsumme im TCP- / UDP- oder IP-Header nicht erkannt. Diese Pakete werden als Datenpakete gezählt.

› Werte-loeschen

Diese Aktion löscht alle Statistik-Einträge.

6.20.5.2 Port-Status

Diese Tabelle zeigt alle Port-bezogenen Statistiken.

Konsole: **Status** > **LAN-Bridge-Statistiken** > **IGMP-Snooping** > **Port-Status**

- Router-Port

  Zeigt an, ob der Port derzeit als Router-Port genutzt wird oder nicht, unabhängig davon, ob dieser Zustand statisch konfiguriert oder dynamisch gelernt wurde.

- IPv4-Pakete

  Zeigt die gesamte Anzahl der IPv4-Multicast-Pakete, die auf diesem Port empfangen wurden, unabhängig davon, ob es sich um IGMP-Pakete handelt oder nicht.

- IPv6-Pakete

  Zeigt die gesamte Anzahl der IPv6-Multicast-Pakete, die auf diesem Port empfangen wurden, unabhängig davon, ob es sich um MLD-Pakete handelt oder nicht.

- Daten-Pakete

  Zeigt die gesamte Anzahl der nicht beschädigten IP-Multicast-Pakete, die auf diesem Port empfangen wurden und bei denen es sich nicht um IGMP- / MLD-Pakete handelt.

- Steuer-Pakete

  Zeigt die gesamte Anzahl der nicht beschädigten IGMP- / MLD-Pakete, die auf diesem Port empfangen wurden.

- Defekte-Pakete

  Zeigt die gesamte Anzahl der beschädigten Daten- oder IGMP- / MLD-Pakete, die auf diesem Port empfangen wurden. Mögliche Ursachen für die Beschädigung der Pakete sind IP-Prüfsummenfehler oder abgeschnittene Pakete.

  Aus Performance-Gründen werden IP-Prüfsummen nur für IGMP- / MLD-Pakete ausgewertet, nicht für den Datenteil der Multicast-Pakete. Daher werden Pakete mit einer fehlerhaften Prüfsumme im TCP/UDP- oder IP-Header nicht erkannt. Diese Pakete werden als Datenpakete gezählt.

6.20.5.3 Gruppen

Diese Tabelle zeigt alle dem Gerät bekannten Mitgliedschaften von Multicast-Gruppen, unabhängig davon, ob sie statisch konfiguriert oder dynamisch gelernt wurden. Wenn für eine Multicast-Gruppe sowohl statische als auch dynamische Mitgliedschaften existieren, werden diese in separaten Einträgen angezeigt.

Konsole: **Status** > **LAN-Bridge-Statistiken** > **IGMP-Snooping** > **Gruppen**

- Adresse

  Zeigt die IP-Multicast-Adresse der Gruppe.

- VLAN-Id

  Zeigt die VLAN-ID, für welche dieser Eintrag gültig ist.

- Lernen-erlauben

  Zeigt an, on für die Gruppe neue Mitgliedschaften dynamisch gelernt werden dürfen oder nicht.

- Statische-Mitglieder

  Zeigt die Liste der statisch für die Gruppe definierten Mitglieder.

- Dynamische-Mitglieder

Zeigt die Liste der dynamisch für die Gruppe gelernten Mitglieder.

6.20.5.4 Simulierte-Anfrager

Die Tabelle zeigt den Status aller definierten und aktiven IGMP- / MLD-Querier-Instanzen.

- Name

  Zeigt den Namen der Multicast-Gruppe.

- Bridge-Gruppe

  Zeigt die Bridge-Gruppe, für welche dieser Eintrag gültig ist.

- VLAN-Id

  Zeigt das VLAN, für welches dieser Eintrag gültig ist.

- Status

  Zeigt den Status des Eintrags.

  - Initial: Die Querier-Instanz wurde gerade gestartet und sendet IGMP- / MLD-Anfragen in kurzen Intervallen (viermal schneller als das definierte Anfrage-Intervall).
  - Querier: Die Querier-Instanz betrachtet sich selbst als den aktiven Querier und sendet IGMP- / MLD-Anfragen in den als Anfrage-Intervall definierten Abständen.
  - Non-Querier: Eine andere Querier-Instanz mit einer niedrigeren IP-Adresse wurde erkannt, die hier aufgeführte Instanz sendet keine IGMP- / MLD-Anfragen.

6.21 Konfiguration des WWAN-Zugriffs

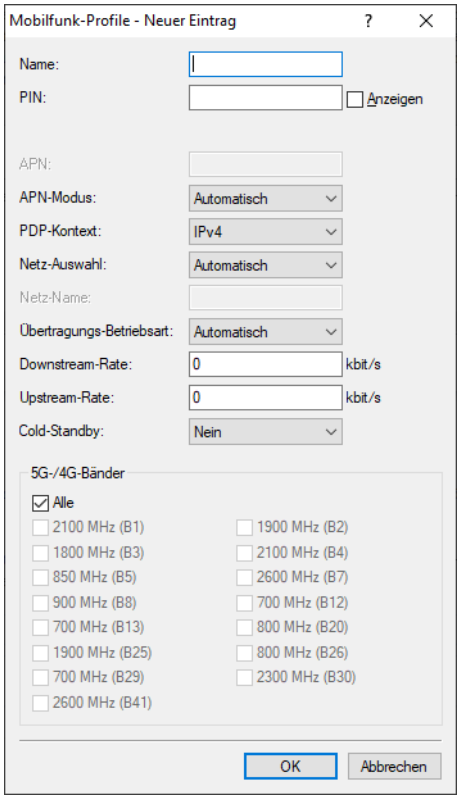
Das nachfolgende Tutorial zeigt Ihnen, wie Sie bei Geräten mit einem internen Mobilfunk-Modem manuell den WAN-Zugriff über das Mobilfunknetz (WWAN) konfigurieren. Dazu legen Sie für Ihren Provider zunächst ein Mobilfunk-Profil an oder verändern ein bereits vorkonfiguriertes Profil, und weisen dieses Profil anschließend der WAN-Schnittstelle des Gerätes zu.

Für einen einfacheren und schnelleren Konfigurationsweg steht Ihnen alternativ auch ein entsprechender Setup-Assistent (**Internet-Zugang einrichten**) zur Verfügung.

Hier haben Sie auch die Möglichkeit, für die Mobilfunk-Standards entsprechende Generationsbezeichnungen anzugeben und diese anzeigen zu lassen.

1. Öffnen Sie in LANconfig den Konfigurationsdialog für Ihr Gerät und wechseln Sie in die Ansicht **Schnittstellen** > **WAN**.
2. Wählen Sie in der Tabelle **Mobilfunk-Profile** ein vorkonfiguriertes Profil zur Bearbeitung aus oder fügen Sie für Ihren Provider ein neues Profil hinzu.

Der Vollständigkeit wegen beschreibt dieses Tutorial die Anlage eines neuen Profils.



3. Geben Sie unter **Name** den gleichen Namen wie die Gegenstelle für das Mobilfunk-Profil an.
4. Geben Sie unter **PIN** die 4-stellige PIN der verwendeten Mobilfunk-SIM-Karte ein. Das Gerät benötigt diese Information, um das Mobilfunk-Modem in Betrieb zu nehmen.

   Die SIM-Karte protokolliert jeden Fehlversuch mit einer ungeeigneten PIN. Die Anzahl dieser Fehlversuche bleibt auch dann erhalten, wenn das Gerät zwischenzeitlich vom Stromnetz getrennt ist. Nach 3 Fehlversuchen sperrt sich die SIM-Karte gegen weitere Zugangsversuche. In diesem Zustand benötigen Sie die in der Regel 8-stelligen PUK oder SuperPIN, um die Sperre aufzuheben.
5. Sofern Ihr Gerät mehrere SIM-Karten aufnehmen kann, wählen Sie über **SIM Steckplatz** die SIM-Karte aus, die Sie mit dem Profil verknüpfen wollen.

   Die Auswahl **Profil inaktiv** deaktiviert das Mobilfunk-Profil. Wählen Sie diese Option, falls Sie lediglich eine Profil-Vorlage anlegen und die Mobilfunk-Einrichtung zu einem späteren Zeitpunkt abschließen wollen.

   Nur aktivierte Profile sind in der Auswahl in LANmonitor sichtbar.
6. Geben Sie unter **APN** den Namen des Zugangs-Servers für die Datendienste Ihres Mobilfunk-Providers ein.
   Der APN (Access Point Name) ist spezifisch für jeden Mobilfunk-Provider. Sie finden diese Information normalerweise in den Unterlagen Ihres Mobilfunk-Vertrages.
7. Geben Sie unter **PDP-Kontext** den Typ des PDP-Kontextes für das Mobilfunk-Profil an.
   Der PDP-Kontext beschreibt die Unterstützung der Adressräume, welche das Backbone des betreffenden Mobilfunkanbieters für Verbindungen aus dem Mobilfunknetz ins Internet anbietet. Dies kann entweder IPv4 oder IPv6 allein, oder die Unterstützung für beide Adressräume umfassen (Dual-Stack). Clients, die den betreffenden Mobilfunkanbieter nutzen wollen, müssen mindestens einen der angegebenen Adressräume unterstützen.
8. Geben Sie den bevorzugten Modus für die **Netz-Auswahl** an:

Automatisch

Das Mobilfunk-Modem bucht sich automatisch in dem Mobilfunk-Netz ein, welches zuletzt erfolgreich verwendet wurde. Schlägt der Einbuchungsvorgang fehl, bucht sich das Mobilfunk-Interface automatisch in das auf der SIM-Karte hinterlegte Heimnetz (HPLMN) ein.

Kann sich das Mobilfunk-Modem ebenfalls nicht in das auf der SIM-Karte hinterlegte Heimnetz einbuchen, wird eine auf der SIM-karte vorhandene PLMN-Liste der bevorzugten Roaming-Partner der Reihe nach mit Einbuchungsversuchen abgearbeitet. Das Mobilfunk-Interface verbindet sich dann unabhängig von der Signalqualität mit dem ersten Mobilfunknetzwerk, welches verfügbar ist.

Falls keines der o. g. Netze verfügbar ist, wird eines der verfügbaren PLMN-Netze mit „guter" Signalqualitat per Zufall gewählt, danach die PLMN-Netze mit ausreichender, nicht guter Signalqualität, absteigend geordnet nach Signalqualität.

Sobald der Einbuchungsvorgang erfolgreich ist, wird dieses Netz verwendet. Ein Wechsel zu einem anderem Netz findet bis zum Verbindungsabbruch nicht statt. Der Provider kann allerdings einen Wechsel der Zelle und der Zugangsart anstoßen, wenn er es für sinnvoll erachtet.

Manuell

Das Mobilfunk-Modem bucht sich ausschließlich in das im Feld **Netz-Name** spezifizierte Mobilfunk-Netz ein.



Die manuelle Mobilfunk-Netzwahl eignet sich insbesondere dann, wenn Sie das Gerät stationär betreiben und Sie häufige Einbuchungsvorgänge in ein benachbartes oder funktechnisch stärkeres, mitunter aber unerwünschtes oder teureres Mobilfunk-Netz feststellen.



Wenn das manuell eingestellte Mobilfunk-Netzwerk nicht verfügbar ist, kann keine Verbindung aufgebaut werden, da das Mobilfunk-Modem sich immer nur in das manuell angegebene Netzwerk einbucht.

Bei Einstellung **Manuell** und leerem Feld **Netz-Name** wird nach einem Scan in der Konsole mit dem Befehl

```
do /Status/Modem-Mobile/Scan-Networks -s
```

das Beste gefundene Netz in das Feld **Netz-Name** eingetragen.

Halb-automatisch

Bei diesem Verfahren bucht sich das Mobilfunk-Modem zunächst in das Mobilfunk-Netz ein, welches im Feld **Netz-Name** eingetragen ist. Schlägt der Einbuchungsvorgang fehl, bucht sich das Mobilfunk-Modem in das auf der SIM-Karte hinterlegte Heimnetz (HPLMN) ein.

Falls das HPLMN nicht verfügbar ist, wird analog zur automatischen Netzwahl auch der „Operator controlled PLMN selector" (Roaming Partner), zufällig gewähltes gutes Netz, bestes schwaches Netz (in der genannten Reihenfolge) versucht.

Nach Qualität

Das Mobilfunk-Modem sucht in einem Scan-Vorgang, welcher manuell in LANmonitor oder über die Konsole angestoßen werden muss, alle verfügbaren Mobilfunk-Netze und bucht sich im Mobilfunk-Netz, welches die beste Signalqualität aufweist, ein. Schlägt der Einbuchungsvorgang fehl, verwendet das Mobilfunk-Interface die **Halb-automatische** Netzauswahl.

Konsolenbefehle

`do /Status/Modem-Mobile/Scan-Networks -s -f`

Mit diesem Befehl wird eine bestehende WAN-Verbindung über ein Mobilfunk-Netz zunächst getrennt, anschließend wird ein erweiterter Scan-Vorgang durchgeführt und das beste Netz wird daraufhin ausgewählt und in die Konfiguration übernommen.

Dieser Befehl bietet sich in Verbindung mit der Netz-Auswahl **Halb-automatisch** und **Manuell** an. Das gespeicherte Netzwerk gilt auch nach einem Geräte-Neustart (Cold / Warm boot) bis Scan-Networks -s / -e

ausgeführt wird, für alle Modi ausser **Automatisch**. Die Ergebnisse des Scans sind unter **Status** > **Modem-Mobile** > **Network-List** verfügbar.

```
do /Status/Modem-Mobile/Scan-Networks -e -f
```

Mit diesem Befehl wird eine bestehende WAN-Verbindung über ein Mobilfunk-Netz zunächst getrennt und im Anschluss ein erweiterter Scan-Vorgang durchgeführt. Der Parameter -e sorgt dafür, dass das Beste gefundene Netz verwendet, dieses aber nicht in der Konfiguration eingetragen wird. Der Eintrag erfolgt jedoch im Status-Baum.

```
do /Status/Modem-Mobile/Scan-Networks -s
```

Mit diesem Befehl wird ein Netzwerk-Scan nur bei einer inaktiven WWAN-Verbindung durchgeführt.



Wenn Sie den manuellen Scanvorgang regelmäßig automatisch durchführen möchten, können Sie dazu in der Cron-Tabelle des LANCOM Routers einen Eintrag konfigurieren. Tragen Sie dazu den Befehl

```
do /Status/Modem-Mobile/Scan-Networks -s -f
```

in den Konfigurationsdialog ein.

LANmonitor

Im LANmonitor können Sie die o. g. Scan-Vorgänge durchführen, indem Sie einen rechten Mausklick auf der Netzliste durchführen und aus dem Kontextmenü den gewünschten Vorgang auswählen. Da der Scan-Vorgang **Verbindung trennen und bestes Netz auswählen** am effektivsten ist, sollte dieser bevorzugt durchgeführt werden.

9. Sofern Sie die manuelle Netz-Auswahl gewählt haben, geben Sie unter **Netz-Name** die exakte Bezeichnung Ihres Heimnetzes an.
10. Geben Sie unter **Übertragungs-Betriebsart** die bevorzugte Übertragungsart innerhalb des Mobilfunknetzes an:

Automatisch

Automatische Wahl der Übertragungs-Betriebsart

LTE(4G)+UMTS(3G)

Kombinierter LTE-UMTS-Betrieb

LTE(4G)+GPRS(2G)

Kombinierter LTE-GPRS-Betrieb

LTE(4G)

Ausschließlicher LTE-Betrieb

UMTS(3G)+GPRS(2G)

Kombinierter UMTS-GPRS-Betrieb

UMTS(3G)

Ausschließlicher UMTS-Betrieb

GPRS(2G)

Ausschließlicher GPRS-Betrieb

11. Geben Sie unter **Downstream-Rate** und **Upstream-Rate** die Übertragungsraten des verwendeten Mobilfunk-Anschlusses an, damit die Quality-of-Service (QoS)-Funktionen der Firewall einwandfrei funktionieren.

Bei einem Wert von `0` gilt die Mobilfunk-Schnittstelle in der betreffenden Richtung als unbeschränkt und die QoS-Mechanismen greifen nicht.

12. Geben Sie unter **Cold-Standby** an, ob das Mobilfunk-Modem im Nicht-Backup-Fall ins Mobilfunknetz eingebucht sein soll. Bei „Ja" ist das Mobilfunk-Modem im Nicht-Backup-Fall nicht im Mobilfunknetz eingebucht. Im Backup-Fall dauert es entsprechend länger bis das Modul eine vollständige Backup-Verbindung aufgebaut hat. Diese Funktion wird nur im Zusammenhang mit der Nutzung der Backup-Tabelle unterstützt. Diese Funktion hat keine Auswirkung bzw. ist nicht möglich bei der Verwendung von Administrativen Distanzen, da dort das WWAN-Modem immer eine aktive Datenverbindung aufgebaut hat. Default: Nein.
13. Wenn aufgrund ungünstiger Umgebungsbedingungen der Router ständig zwischen zwei Frequenzbändern wechselt, kann das zu Instabilitäten bei der Übertragung führen. Mit der Auswahl im Abschnitt **LTE-Bänder** geben Sie dem Mobilfunk-Modem vor, welche Frequenzbänder verwendbar sind.

    Alle

    Alle Frequenzbänder sind aktiviert.

    2100 MHz (B1)

    2,1GHz-Band ist aktiviert.

    1800 MHz (B3)

    1,8GHz-Band ist aktiviert.

    2600 MHz (B7)

    2,6GHz-Band ist aktiviert.

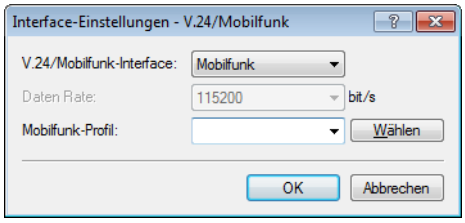
    900 MHz (B8)

    900MHz-Band ist aktiviert.

    800 MHz (B20)

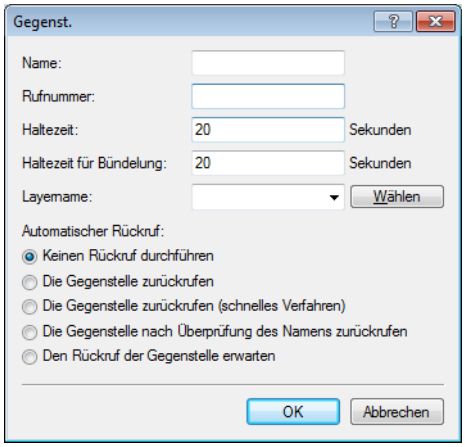
    800MHz-Band ist aktiviert.

    Diese Auswahl schränkt nur die Frequenzbänder bei der Übertragung im LTE-Standard ein. Für UMTS und GPRS bleiben grundsätzlich alle Bänder erlaubt.
14. Klicken Sie **OK**, um die Einstellungen zu speichern.
15. Klicken Sie in der Ansicht **Schnittstellen** > **WAN** auf **Interface-Einstellungen** und wählen Sie **V.24/Mobilfunk**.
16. Wählen Sie in der Liste **V.24/Mobilfunk-Interface** den Wert **Mobilfunk**.
17. Wählen Sie unter **Mobilfunk-Profil** das zuvor für Ihren Mobilfunk-Provider angelegte Profil aus.



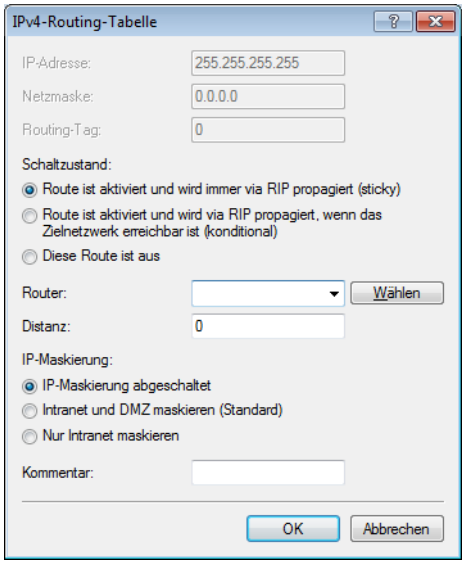
18. Klicken Sie **OK**, um die Einstellungen zu speichern.

19. Klicken Sie in der Ansicht **Kommunikation** > **Gegenstellen** auf **Gegenst. (Mobilfunk/…)** und fügen Sie ein neues Profil hinzu.



20. Tragen Sie unter **Name** den gleichen Namen wie das Mobilfunkprofil ein.
21. Tragen Sie unter **Rufnummer** die Einwahl-Rufnummer Ihres Mobilfunk-Providers ein. Sofern Ihr Provider Ihnen keine Einwahl-Rufnummer mitgeteilt hat, tragen Sie hier `*99#` ein.
22. Tragen Sie unter **Haltezeit** die Zeit ein, nach welcher das Gerät die Verbindung zur Gegenstelle trennt, wenn in dieser Zeit kein Datenpaket übertragen wird

    Geben Sie z. B. einen Wert von `300` Sekunden ein, um einen akzeptablen Kompromiss zwischen Leerauf-Haltekosten und Kosten durch den Verbindungsaufbau zu wahren. Bei einem Wert von `0` hält das Gerät die Verbindung solange aufrecht, bis sie abgebrochen und beendet wird. Bei einem Wert von `9999` baut das Gerät die Verbindung automatisch immer wieder neu auf.
23. Wählen Sie als **Layernamen** den Vorgabewert `WWAN` aus.
24. Klicken Sie **OK**, um die Einstellungen zu speichern.
25. Klicken Sie in der Ansicht **IP-Router** > **Routing** auf **IPv4-Routing-Tabelle-Liste** und fügen Sie die **Default-Route** (`255.255.255.255`) hinzu.



26. Geben Sie unter **Router** das zuvor unter **Gegenst. (Mobilfunk/…)** angelegte Profil an.
27. Setzen Sie die **IP-Maskierung** auf **Intranet und DMZ maskieren (Standard)**.

28. Klicken Sie **OK**, um die Einstellungen zu speichern.

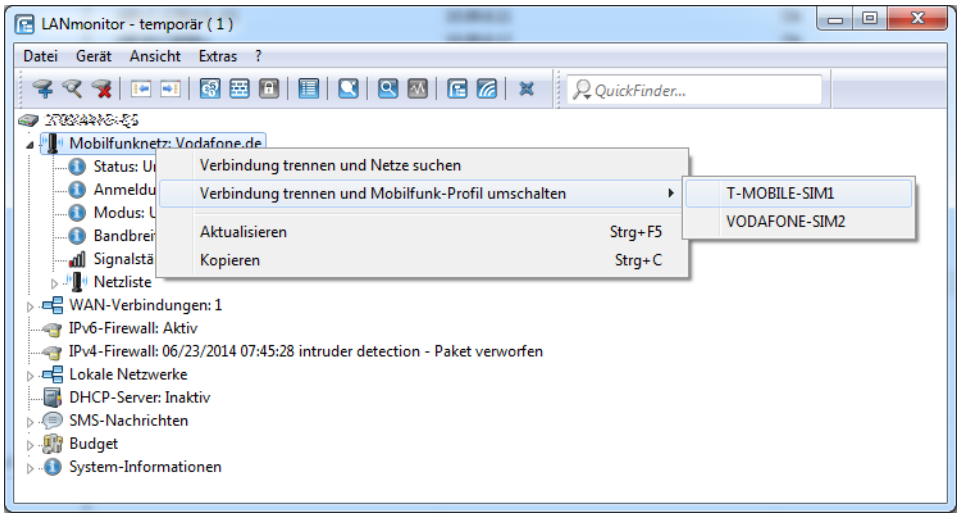
29. Schreiben Sie die Änderungen zurück auf das Gerät.

Die Konfiguration des WWAN-Zugriffs ist damit abgeschlossen.

6.22 Umschalten zwischen Mobilfunk-Profilen oder SIM-Karten

Sofern Sie für eine SIM-Karte unterschiedliche Mobilfunk-Profile oder für mehrere SIM-Karten ein Mobilfunk-Profil angelegt haben, lässt sich mit LANmonitor zwischen diesen Profilen umschalten. Die nachfolgenden Schritte zeigen Ihnen, wie Sie im Betrieb ein alternatives Profil oder eine alternative SIM-Karte auswählen.

1. Wählen Sie im LANmonitor Ihr Gerät aus.
2. Öffnen Sie auf dem Eintrag **Mobilfunknetz** das Kontextmenü und wählen Sie **Verbindung trennen und Mobilfunk-Profil umschalten**.



3. Wählen Sie das Mobilfunk-Profil aus, auf das Sie umschalten wollen.

Das Gerät trennt daraufhin die Verbindung zum Mobilfunknetz und verbindet sich mit dem gewählten Mobilfunk-Profil erneut.

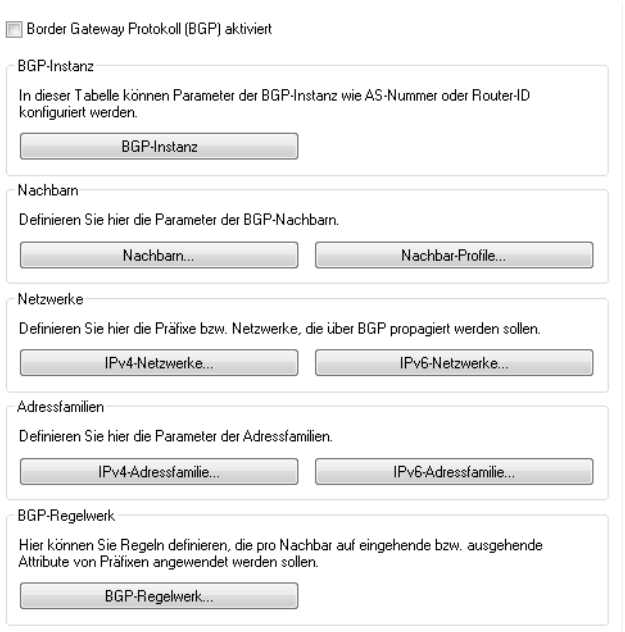
6.23 BGPv4

6.23.1 Border Gateway Protokoll Version 4 (BGPv4)

Das Netzwerk eines Netzproviders bezeichnet man auch als „Autonomes System" (AS). Das Border Gateway Protokoll Version 4 (BGPv4) dient dazu, Routinginformationen zwischen autonomen Systemen auszutauschen (eBGP: External BGP) und diese Informationen an die Router des eigenen AS zu verteilen (iBGP: Internal BGP).

6.23.1.1 BGPv4 mit LANconfig konfigurieren

Um BGPv4 mit LANconfig zu konfigurieren, wechseln Sie in die Ansicht **Routing Protokolle** > **BGP**.



BGP aktivieren

Um die BGP-Funktion zu aktivieren, markieren Sie die Option **Border Gateway Protokoll (BGP) aktiviert**.

BGP-Instanz

LCOS ordnet die BGP-Konfiguration des BGP-Routers einer sogenannten **BGP-Instanz** zu. Diese BGP-Instanz enthält z. B. die AS-Nummer und die Router-ID des Routers.

Aktuell unterstützt LCOS nur eine BGP-Instanz gleichzeitig.

Nachbarn

Als **Nachbarn** gelten die BGP-Gateways anderer autonomer Systeme. Die autonomen Systeme müssen dabei nicht direkt benachbart, aber mindestens einem benachbarten BGP-Gateway bekannt sein.

Zur komfortablen Konfiguration der BGP-Nachbarn erfolgt die Verwaltung über **Nachbar-Profile**.

Netzwerke

Der BGP-Router propagiert an die BGP-Nachbarn, welche Netzwerke er verwaltet.

Adressfamilien

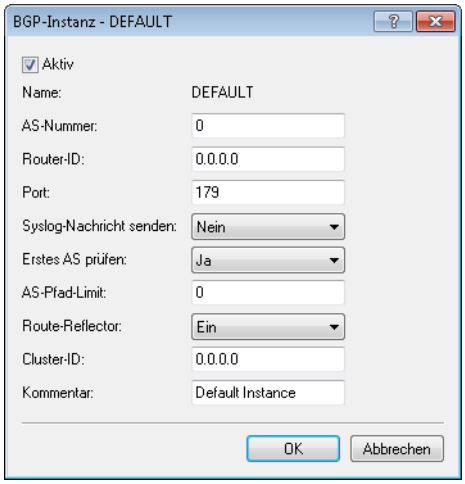
Der BGP-Router ordnet die BGP-Nachbarn Adressfamilien zu, um die Kommunikation mit diesen Nachbarn komfortabel zu verwalten.

BGP-Regelwerk

Filterregeln ermöglichen dem BGP-Router zu entscheiden, wie er ausgehende und ankommende BGP-Nachrichten behandeln soll.

BGP-Instanz

Die BGP-Instanz des Gerätes konfigurieren Sie unter **BGP-Instanz**.



Aktiv

Aktiviert oder deaktiviert diese BGP-Instanz.

Diese Einstellung ist nur wirksam, wenn BGP im Gerät aktiv ist.

Name

Enthält den Namen der BGP-Instanz.

Da das Gerät nur eine BGP-Instanz gleichzeitig unterstützt, ist bereits ein Eintrag „DEFAULT" vorgegeben.

AS-Nummer

Die AS-Nummer, die dieser BGP-Instanz zugeordnet ist.

Ein Verbindungsaufbau zu einem BGP-Router, der keine 32Bit-großen AS-Nummern unterstützt, ist nur dann möglich, wenn Sie hier eine 16Bit-AS-Nummer eintragen (kleiner 65536).

Router-ID

Die Router-ID (IPv4-Adresse), die dieser BGP-Instanz zugeordnet ist.

Die Router-ID muss unter allen Nachbarn eines BGP-Routers eindeutig sein.

Bei Verwendung von IPv6-Verbindungen vergeben Sie hier eine fiktive IPv4-Adresse oder eine beliebige IPv4-Adresse des Routers.

Port

Enthält den Port, auf dem die BGP-Instanz auf ankommende Verbindungen von Nachbarn reagiert.

Syslog-Nachricht senden

Das Gerät kann Ereignisse wie Verbindungsabbrüche von Nachbarn, die mit dieser BGP-Instanz verbunden sind, im Syslog speichern. Mit dieser Option aktivieren oder deaktivieren Sie diese Funktion.

Erstes AS prüfen

Prüft, ob die erste AS-Nummer im AS-Pfad bei empfangenen Update-Nachrichten der AS-Nummer des Nachbarn entspricht. Falls dies nicht der Fall ist, wird diese Route verworfen.

Diese Prüfung muss deaktiviert werden, wenn der Router mit einem BGP-Route-Server verbunden ist, der zwar Routen verteilt, aber nicht selbst im Routing-Pfad liegt bzw. sein eigenes AS in den AS-Pfad einfügt.

AS-Pfad-Limit

Maximale Anzahl von erlaubten AS-Nummern im AS-Pfad bei empfangenen Update-Nachrichten. Wird das Limit überschritten, verwirft das Gerät die entsprechende Route. Ein AS-Pfad-Limit kann vor Nachrichten von fehlerhaft konfigurierten Routern schützen, die zu lange AS-Pfade ankündigen.

Route-Reflector

Definiert, ob der Router die Funktion eines Route-Reflectors übernehmen soll.

Beim Einsatz von iBGP müssen normalerweise alle BGP-Router voll vermascht sein, d. h., jeder BGP-Router muss zu jedem BGP-Router eine BGP-Verbindung aufgebaut haben. Ein Route-Reflector hebt diese Anforderung auf und ermöglicht es, dass iBGP-Router z. B. eine sternförmige Topologie aufbauen können. Der Route-Reflector leitet dann iBGP-Routen an alle Route-Reflector-Clients weiter.

Ein Route-Reflector kann sowohl Route-Reflector-Clients als auch normale BGP-Clients bedienen. Auf dem Client muss in beiden Fällen keine gesonderte Konfiguration erfolgen.

Cluster-ID

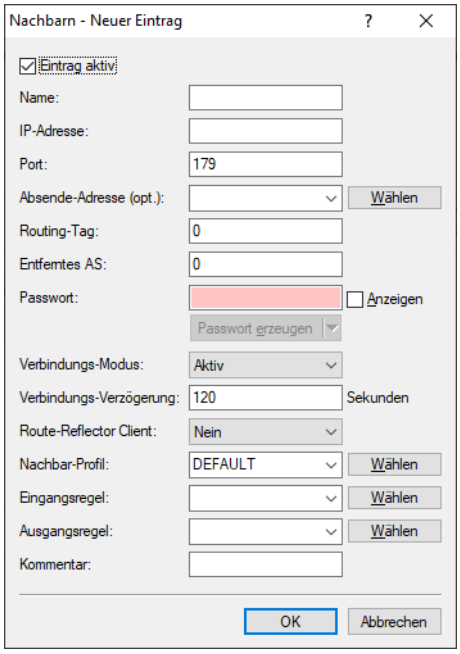
Cluster-ID des Routers, falls dieser als Route-Reflector konfiguriert wird. Die Eingabe erfolgt im Format einer IPv4-Adresse.

Kommentar

Kommentar zu dieser BGP-Instanz.

Nachbarn

Die BGP-Nachbarn des Gerätes konfigurieren Sie unter **Nachbarn**.



Eintrag aktiv

Aktiviert oder deaktiviert den Eintrag für diesen BGP-Nachbarn.

Die Aktivierung des BGP-Nachbarn startet ggf. einen BGP-Verbindungsaufbau.

Bei deaktiviertem BGP-Nachbarn ist eine Verbindung zu ihm nicht möglich.

Name

Enthält den Namen des BGP-Nachbarn.

IP-Adresse

Enthält die IP-Adresse (IPv4 oder IPv6) des BGP-Nachbarn, zu dem das Gerät in den Verbindungsarten „Aktiv" oder „Verzögert" eine BGP-Verbindung aufbaut. Bei Verwendung einer Link-Lokalen IPv6-Adresse muss diese mit % und dem Namen des logischen Interfaces angegeben werden, z. B. „fe80::1%INTRANET".

Alternativ haben Sie die Möglichkeit, ein gesamtes IPv4-Subnetz zu konfigurieren, z. B. 192.168.1.0/24. In diesem Fall akzeptiert der Router BGP-Verbindungen anderer Router aus dem Subnetz 192.168.1.0 mit der Subnetzmaske 255.255.255.0. Dafür ist es erforderlich, den Verbindungs-Modus als "Passiv" zu definieren.

IPv6-Subnetze werden nicht unterstützt.

Dieser Eintrag muss identisch zu der IP-Adresse (z. B. physikalische Interface-Adresse, Loopback-Adresse) sein, die dieser Nachbar bei einer ankommenden Verbindung meldet.

Port

Enthält den Port, auf dem der BGP-Nachbar einkommende BGP-Nachrichten erwartet und den das Gerät entsprechend für ausgehende Verbindungen in den Verbindungsarten „Aktiv" oder „Verzögert" verwendet.

Ankommende Verbindungen nimmt das Gerät auf jedem vom Sender verwendeten Quell-Port an.

Absende-Adresse (opt.)

Enthält die Absender-Adresse (IPv4 oder IPv6), die das Gerät dem BGP-Nachbarn bei einem Verbindungsaufbau mitteilt.

Die Angabe ist optional und nur in den Verbindungsarten „Aktiv" oder „Verzögert" relevant.

Routing-Tag

Enthält das Routing-Tag. Stimmt das Routing-Tag nicht mit dem der ankommenden Verbindung überein, verweigert das Gerät den Verbindungsaufbau.

Entferntes AS

Enthält die AS-Nummer des BGP-Nachbarn.

Ist die AS-Nummer des BGP-Nachbarn identisch zur AS-Nummer der eigenen BGP-Instanz des Gerätes, handelt es sich bei dem Nachbarn um einen iBGP-Peer (Internal BGP) innerhalb des eigenen AS.

Passwort

Gerät und BGP-Nachbar übertragen dieses Passwort als MD5-Signatur in den TCP-Paketen, um sich zu authentifizieren.

Ohne die Angabe eines Passwortes ist die Authentifizierung deaktiviert.

Verbindungs-Modus

Bestimmt den Modus, mit dem eine Verbindung vom Gerät zu diesem BGP-Nachbarn zustande kommt. Folgende Modi sind möglich:

- **Aktiv**: In diesem Modus versucht das Gerät eine Verbindung zum BGP-Nachbarn aufzubauen, sobald u. a. eine der folgenden Bedingungen erfüllt ist:
  - Die Konfiguration des BGP-Nachbarn ist komplett.
  - Sie führen im WEBconfig oder über die Konsole die Aktion **Manueller-Start** aus.
  - Sie starten das Gerät.
  - Sie aktivieren die BGP-Instanz unter **Routing-Protokolle** > **BGP** > **BGP-Instanz**.
  - Sie aktivieren diesen BGP-Nachbarn unter **Eintrag aktiv**.

  Wenn der aktive Verbindungsaufbau nicht gelingt, dann wird dieser nach 120 Sekunden erneut versucht.
- **Passiv**: In diesem Modus baut das Gerät nicht aktiv eine Verbindung zum BGP-Nachbarn auf, sondern wartet auf eine entsprechende Verbindungsanfrage vom BGP-Nachbarn.
- **Verzögert**: In diesem Modus baut das Gerät eine Verbindung zum BGP-Nachbarn erst nach Ablauf einer Verzögerungszeit auf. Die Bedingungen zum Aufbau einer Verbindung sind identisch zum Modus „Aktiv".

Verbindungs-Verzögerung

Gibt die Zeit in Sekunden an, die das Gerät in der Verbindungsart „Verzögert" wartet, bis es eine Verbindung zu einem BGP-Nachbarn aufbaut.

Route-Reflector Client

Definiert, ob der entsprechende Nachbar als Route-Reflector-Client behandelt werden soll, so dass das Gerät iBGP-Routen zu diesem Client reflektiert.

Dieser Schalter ist nur dann wirksam, falls

- das Gerät in der BGP-Instanz als Route-Reflector konfiguriert wurde, d. h. selbst Route-Reflector ist und
- die entfernte AS-Nummer der eigenen AS-Nummer entspricht (iBGP).

Nachbar-Profil

Enthält den Namen des BGP-Nachbar-Profils aus **Routing-Protokolle** > **BGP** > **Nachbar-Profile**.

Bei fehlendem oder falschem Eintrag gilt der BGP-Nachbar als nicht vollständig konfiguriert und eine Verbindung zu ihm ist nicht möglich.

Eingangsregel

Gibt an, nach welchen Regeln das Gerät die eingehenden Verbindungen von diesem BGP-Nachbarn filtert.

Die Regeln konfigurieren Sie unter **Routing-Protokolle** > **BGP** > **BGP-Regelwerk** > **Filter**.

Wenn Sie dieses Feld leer lassen, filtert das Gerät die ankommenden Verbindungen entsprechend der Default-Regel unter **Routing-Protokolle** > **BGP** > **BGP-Regelwerk** > **Standard**.

Ausgangsregel

Gibt an, nach welchen Regeln das Gerät die ausgehenden Verbindungen von diesem BGP-Nachbarn filtert.

Die Regeln konfigurieren Sie unter **Routing-Protokolle** > **BGP** > **BGP-Regelwerk** > **Filter**.

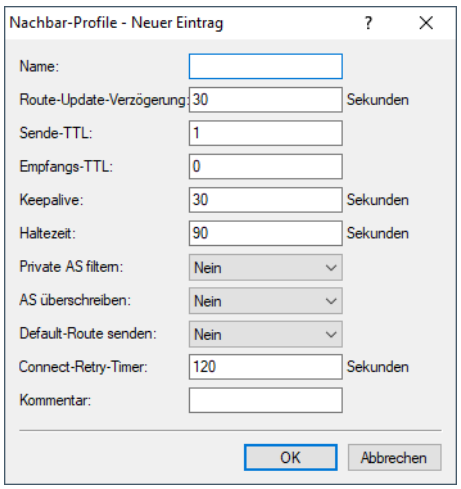
Wenn Sie dieses Feld leer lassen, filtert das Gerät die ankommenden Verbindungen entsprechend der Default-Regel unter **Routing-Protokolle** > **BGP** > **BGP-Regelwerk** > **Standard**.

Kommentar

Enthält einen Kommentar zu diesem BGP-Nachbarn.

Nachbar-Profile

Die Profile der BGP-Nachbarn des Gerätes konfigurieren Sie unter **Nachbar-Profile**.



Name

Enthält den Namen des Profils.

Dieser Name ist u. a. für die Angabe in folgenden Tabellen vorgesehen:

- **Nachbar-Profil** unter **Routing-Protokolle** > **BGP** > **Nachbarn**
- **Nachbar-Profil** unter **Routing-Protokolle** > **BGP** > **IPv4-Adressfamilie**
- **Nachbar-Profil** unter **Setup** > **Routing-Protokolle** > **BGP** > **IPv6-Adressfamilie**

Route-Update-Verzögerung

Enthält die Zeit in Sekunden, die das Gerät mindestens zwischen dem Versenden von BGP-Update-Nachrichten an die BGP-Nachbarn mit diesem Profil wartet.

Sende-TTL

Bestimmt die TTL (time to live), die das Gerät den TCP-Paketen an die BGP-Nachbarn dieses Profils hinzufügt.

Bei direkt verbundenen Nachbarn beträgt dieser Wert „1“. Für eBGP-Umgebungen erhöhen Sie diesen Wert für jeden Hop um 1.

In iBGP-Sitzungen ignoriert das Gerät diesen Wert und verwendet stattdessen standardmäßig den maximalen TTL-Wert.

Dieser Wert muss „0“ betragen, wenn **Empfangs-TTL** einen Wert ungleich „0“ besitzt. Das Gerät verwendet automatisch den Wert „1“, wenn sowohl **Sende-TTL** als auch **Empfangs-TTL** den Wert „0“ besitzen.

Empfangs-TTL

Bestimmt die TTL (time to live), die die ankommenden TCP-Pakete von BGP-Nachbarn dieses Profils mindestens beinhalten müssen. Ankommende TCP-Pakete mit geringerer TTL nimmt das Gerät nicht an.

In iBGP-Sitzungen ignoriert das Gerät diesen Wert.

Wenn dieser Wert ungleich „0“ ist, setzt das Gerät den Wert für **Sende-TTL** intern auf „255“.

Dieser Wert muss „0“ betragen, wenn **Sende-TTL** einen Wert ungleich „0“ besitzt.

Keepalive

Bestimmt die Zeit für den Keepalive-Timer in Sekunden. Nach Ablauf dieser Zeit sendet das Gerät eine Keepalive-Meldung an die Nachbarn dieses Profils, um die BGP-Verbindung aufrecht zu erhalten.

Das Gerät muss mindestens dreimal pro Haltezeit eine Keepalive-Nachricht schicken. Der Wert darf deshalb max. ein Drittel der Haltezeit betragen. Bei einem höheren Wert oder einem Wert gleich „0" verwendet LCOS intern automatisch ein Drittel der Haltezeit.

Haltezeit

Falls der Router innerhalb der konfigurierten (BGP-)Haltezeit keine regelmäßigen BGP Keepalive-, Update- oder Notification-Nachrichten erhält, beendet der Router die BGP-Session und sendet eine Notification mit dem Fehlercode „Hold Timer Expired".

Das Gerät verhandelt diesen Wert mit dem BGP-Nachbarn bei einem Verbindungsaufbau. Der niedrigere der beiden Werte gilt danach als gültig.

Ist das Resultat dieser Verhandlung ein Wert von „0", setzt das Gerät diese Verbindung solange auf gültig, bis es eine Verbindungsfehlermeldung erhält oder die Verbindung zusammenbricht. In dieser Zeit sendet es keine Keepalive-Nachrichten an die BGP-Nachbarn, selbst wenn der Keepalive-Timer eine Zeitdauer enthält.

Die Werte „1" und „2" sind gemäß RFC nicht erlaubt.

Private AS filtern

Kontrolliert die Behandlung von privaten AS-Einträgen (64512 - 65535, 4200000000 - 4294967294) aus der `AS_PATH`-Liste von ausgehenden Network Layer Reachability Information-Nachrichten (NLRI) zum Update der BGP-Nachbarn dieses Profils.

Bei iBGP-Verbindungen hat diese Option keine Funktion.

AS überschreiben

Aktiviert oder deaktiviert das Überschreiben von AS-Nummern im `AS_PATH` ausgehender Network Layer Reachability Information (NLRI).

Bei aktivierter Option überschreibt das Gerät alle AS-Nummern des BGP-Nachbarn mit der eigenen AS-Nummer.

Default-Route senden

Dieser Schalter bestimmt das Verhalten der Propagation von Default Routen. Mögliche Werte:

Ja

Default Routen werden in BGP Phase 3 (Bestimmung der Routen zur Redistribution) wie normale Routen behandelt.

Nein

Default Routen werden ignoriert, die nicht als Quelle die Tabelle der statischen BGP Routen haben (*IPv4-Netzwerke* auf Seite 517 oder *IPv6-Netzwerke* auf Seite 517).

Connect-Retry Timer

Definiert die Zeit in Sekunden, die der Router bei einem fehlgeschlagenen BGP-Verbindungsaufbau wartet bis zum nächsten Verbindungsversuch. In der Regel wird dieser Schalter nur benötigt, wenn die Gegenseite im Verbindungsmodus „passiv" ist, um den Verbindungsaufbau zu beschleunigen. Default: 120 Sekunden

Kommentar

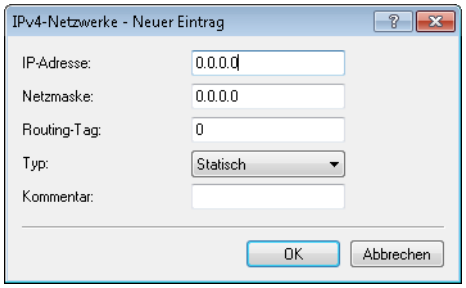
Kommentar zu diesem Eintrag.

IPv4-Netzwerke

In dieser Tabelle konfigurieren Sie die IPv4-Netzwerke, die das Gerät an die BGP-Nachbarn verteilt.

Die Verteilung dieser Netzwerke ist abhängig von den Einschränkungen unter **Routing-Protokolle** > **BGP** > **IPv4-Adressfamilie**.

Die Mindestangabe für einen neuen gültigen Eintrag ist eine **IP-Adresse**.



IP-Adresse

Beinhaltet die IPv4-Adresse oder das Präfix des Netzwerkes.

Netzmaske

Beinhaltet die IPv4-Netzmaske des Netzwerkes.

Die Route wird zur Default-Route dieser Adressfamilie, wenn dieser Eintrag die Default-Einstellung `0.0.0.0` besitzt.

Routing-Tag

Enthält das Routing-Tag für dieses Netzwerk.

Die Tabelle unter **Routing-Protokolle** > **BGP** > **IPv4-Adressfamilie** nutzt diesen Eintrag zur Filterung der Kommunikation mit den BGP-Nachbarn.

Typ

Bestimmt, ob das Gerät dieses Netzwerk generell für Ankündigungen nutzt oder nur, wenn dieses Netzwerk in der aktiven Routing-Tabelle erscheint.

- In der Einstellung „Statisch" ist das Netzwerk immer für Ankündigungen ausgewählt.
- In der Einstellung „Dynamisch" ist das Netzwerk nur für Ankündigungen ausgewählt, wenn es in der aktiven Routing-Tabelle erscheint.

Kommentar

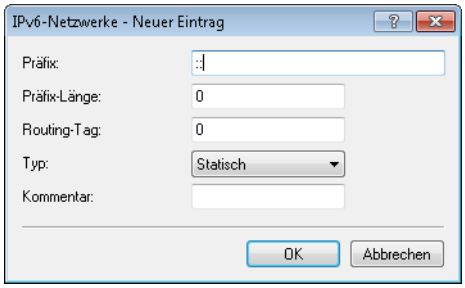
Kommentar zu diesem Eintrag.

IPv6-Netzwerke

In dieser Tabelle konfigurieren Sie die IPv6-Netzwerke, die das Gerät an die BGP-Nachbarn verteilt.

Die Verteilung dieser Netzwerke ist abhängig von den Einschränkungen unter **Routing-Protokolle** > **BGP** > **IPv6-Adressfamilie**.

Die Mindestangabe für einen neuen gültigen Eintrag ist ein **Präfix**.



Präfix

Beinhaltet das Präfix (IPv6-Adressteil) des Netzwerkes.

Präfix-Länge

Beinhaltet die Präfix-Länge des IPv6-Netzwerkes.

Die Route wird zur Default-Route dieser Adressfamilie, wenn dieser Eintrag die Default-Einstellung `0` besitzt.

Routing-Tag

Enthält das Routing-Tag für dieses Netzwerk.

Die Tabelle unter **Routing-Protokolle** > **BGP** > **IPv6-Adressfamilie** nutzt diesen Eintrag zur Filterung der Kommunikation mit den BGP-Nachbarn.

Typ

Bestimmt, ob das Gerät dieses Netzwerk generell für Ankündigungen nutzt oder nur, wenn dieses Netzwerk in der aktiven Routing-Tabelle erscheint.

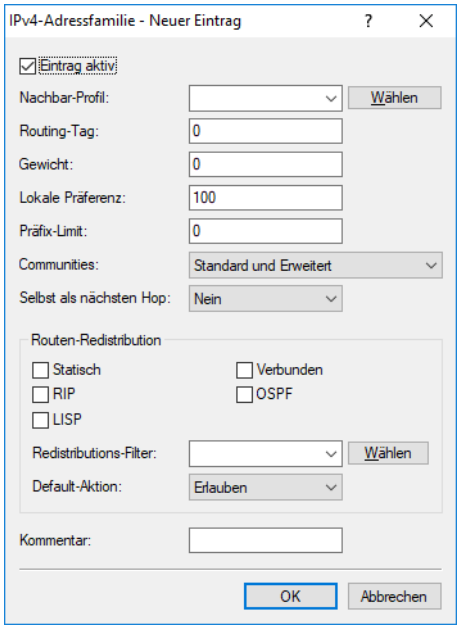
- In der Einstellung „Statisch" ist das Netzwerk immer für Ankündigungen ausgewählt.
- In der Einstellung „Dynamisch" ist das Netzwerk nur für Ankündigungen ausgewählt, wenn es in der aktiven Routing-Tabelle erscheint.

Kommentar

Kommentar zu diesem Eintrag.

IPv4-Adressfamilie

In dieser Tabelle konfigurieren Sie die Einstellungen der IPv4-Parameter, die für alle Geräte eines BGP-Nachbar-Profils gelten.



Eintrag aktiv

Aktiviert oder deaktiviert den Versand von IPv4-NLRI dieser Adressfamilie an die BGP-Nachbarn, die dieses Nachbar-Profil verwenden.

Nachbar-Profil

Enthält den Namen des entsprechenden Nachbar-Profils, wie er unter **Routing-Protokolle** > **BGP** > **Nachbar-Profile** gespeichert ist.

Routing-Tag

Legt fest, dass das Gerät Routen nur dann weiter verteilt, wenn diese das konfigurierte Routing-Tag aus der Routing-Tabelle verwenden. Empfangene Routen des Nachbarn speichert das Gerät für dieses Routing-Tag in der Routing-Tabelle ab.

Gewicht

Gibt die Standard-Gewichtung für NLRI an.

Diese Angabe beeinflusst die Bevorzugung von gleichen Präfix-Ankündigungen, die das Gerät von unterschiedlichen BGP-Nachbarn erhalten hat. Das Präfix mit der höheren Gewichtung erhält den Vorzug.

„Gewicht" ist ein proprietäres Attribut, das das Gerät nicht in BGP-Update-Nachrichten an andere eBGP-Nachbarn propagiert. Dieses Attribut ist somit nur auf dem lokalen Router gültig.

Lokale Präferenz

Ähnlich der Einstellung bei **Gewicht** ermöglicht diese Angabe die Bevorzugung von gleichen Präfix-Ankündigungen, die das Gerät von unterschiedlichen BGP-Nachbarn erhalten hat. Das Präfix mit der höheren Gewichtung erhält den Vorzug. Dieser Wert überschreibt nicht die Lokale Präferenz für Präfixe, die bereits ein Attribut LOCAL_PREF besitzen (z. B. bei iBGP). Die Präferenz dieser Präfixe muss über eine entsprechende Regel mit Hilfe des BGP-Regelwerks angepasst werden.

„Lokale Präferenz“ ist ein BGP-Standard-Attribut (`LOCAL_PREF`), das das Gerät per iBGP an Nachbarn propagiert. Alle Pfade besitzen in der Standardeinstellung eine „Lokale Präferenz“ von 100.

Präfix-Limit

Bestimmt die Anzahl der akzeptierten Präfixe pro BGP-Nachbar des angegebenen Nachbar-Profils.

Alle Präfixe, die über dieses Limit hinausgehen, verwirft das Gerät.

Communities

Bestimmt, welche Community-Attribute die NLRI dieser Adressfamilie an eBGP-Nachbarn enthalten darf, die das entsprechende Nachbar-Profil verwenden.

Wenn sowohl die Option „Standard“ als auch die Option „Erweitert“ deaktiviert sind, überträgt das Gerät keine Community-Attribute in den NLRI zu eBGP-Nachbarn.

Diese Option hat keine Funktion bei der Kommunikation mit iBGP-Nachbarn.

Eigene IP-Adresse als nächsten Hop setzen

Aktiviert oder deaktiviert den Austausch des Nexthops durch die eigene IP-Adresse in den NLRI.

Mögliche Werte:

Ja

Tauscht in den NLRI die IP-Adresse des Nexthops gegen die eigene IP-Adresse aus.

Nein

Lässt die IP-Adresse des Nexthops in den NLRI unverändert.

Immer

Tauscht in den NLRI immer die IP-Adresse des Nexthops gegen die eigene IP-Adresse aus auch wenn das Gerät als Route Reflector konfiguriert ist.

Routen weiter verteilen

Bestimmt, ob das Gerät bestimmte Routen an BGP-Nachbarn dieses Profils weiterleiten soll.

- Statisch: Das Gerät verteilt statische Routen aus der Routing-Tabelle an die BGP-Nachbarn.
- Verbunden: Das Gerät verteilt Routen von direkt angeschlossenen Netzwerken an die BGP-Nachbarn.
- RIP: Das Gerät verteilt RIP-Routen aus der Routing-Tabelle an die BGP-Nachbarn.
- OSPF: Das Gerät verteilt OSPF-Routen aus der Routing-Tabelle an die BGP-Nachbarn.
- LISP: Das Gerät verteilt LISP-Routen aus der Routing-Tabelle an die BGP-Nachbarn.

Wenn keine Option ausgewählt ist, verteilt das Gerät keine Routen an die BGP-Nachbarn dieses Nachbar-Profils (Default-Einstellung).

Redistributions-Filter

Name der Präfix-Filterliste aus *Präfix-Listen* auf Seite 378.

Default-Aktion

Definiert, wie Präfixe standardmäßig behandelt werden sollen, die in der Präfix-Liste konfiguriert sind. Mögliche Werte:

Erlauben

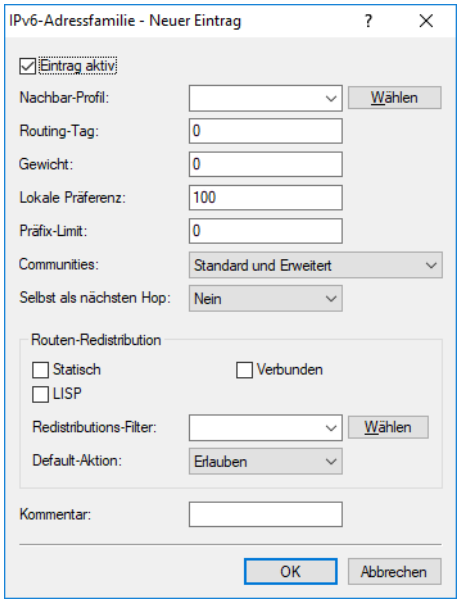
Verweigern

Kommentar

Kommentar zu diesem Eintrag.

IPv6-Adressfamilie

In dieser Tabelle konfigurieren Sie die Einstellungen der IPv6-Parameter, die für alle Geräte eines BGP-Nachbar-Profils gelten.



Eintrag aktiv

Aktiviert oder deaktiviert den Versand von IPv6-NLRI dieser Adressfamilie an die BGP-Nachbarn, die dieses Nachbar-Profil verwenden.

Nachbar-Profil

Enthält den Namen des entsprechenden Nachbar-Profils, wie er unter **Routing-Protokolle** > **BGP** > **Nachbar-Profile** gespeichert ist.

Routing-Tag

Legt fest, dass das Gerät Routen nur dann weiter verteilt, wenn diese das konfigurierte Routing-Tag aus der Routing-Tabelle verwenden. Empfangene Routen des Nachbarn speichert das Gerät für dieses Routing-Tag in der Routing-Tabelle ab.

Gewicht

Gibt die Standard-Gewichtung für NLRI an.

Diese Angabe beeinflusst die Bevorzugung von gleichen Präfix-Ankündigungen, die das Gerät von unterschiedlichen BGP-Nachbarn erhalten hat. Das Präfix mit der höheren Gewichtung erhält den Vorzug.

„Gewicht“ ist ein proprietäres Attribut, das das Gerät nicht in BGP-Update-Nachrichten an andere eBGP-Nachbarn propagiert. Dieses Attribut ist somit nur auf dem lokalen Router gültig.

Lokale Präferenz

Ähnlich der Einstellung bei **Gewicht** ermöglicht diese Angabe die Bevorzugung von gleichen Präfix-Ankündigungen, die das Gerät von unterschiedlichen BGP-Nachbarn erhalten hat. Das Präfix mit der höheren Gewichtung erhält den Vorzug. Dieser Wert überschreibt nicht die Lokale Präferenz für Präfixe, die bereits ein Attribut LOCAL_PREF besitzen (z. B. bei iBGP). Die Präferenz dieser Präfixe muss über eine entsprechende Regel mit Hilfe des BGP-Regelwerks angepasst werden.

„Lokale Präferenz" ist ein BGP-Standard-Attribut (`LOCAL_PREF`), das das Gerät per iBGP an Nachbarn propagiert. Alle Pfade besitzen in der Standardeinstellung eine „Lokale Präferenz" von 100.

Präfix-Limit

Bestimmt die Anzahl der akzeptierten Präfixe pro BGP-Nachbar des angegebenen Nachbar-Profils.

Alle Präfixe, die über dieses Limit hinausgehen, verwirft das Gerät.

Communities

Bestimmt, welche Community-Attribute die NLRI dieser Adressfamilie an eBGP-Nachbarn enthalten darf, die das entsprechende Nachbar-Profil verwenden.

Wenn sowohl die Option „Standard" als auch die Option „Erweitert" deaktiviert sind, überträgt das Gerät keine Community-Attribute in den NLRI zu eBGP-Nachbarn.

Diese Option hat keine Funktion bei der Kommunikation mit iBGP-Nachbarn.

Eigene IP-Adresse als nächsten Hop setzen

Aktiviert oder deaktiviert den Austausch des Nexthops durch die eigene IP-Adresse in den NLRI.

Mögliche Werte:

Ja

Tauscht in den NLRI die IP-Adresse des Nexthops gegen die eigene IP-Adresse aus.

Nein

Lässt die IP-Adresse des Nexthops in den NLRI unverändert.

Immer

Tauscht in den NLRI immer die IP-Adresse des Nexthops gegen die eigene IP-Adresse aus auch wenn das Gerät als Route Reflector konfiguriert ist.

Routen weiter verteilen

Bestimmt, ob das Gerät bestimmte Routen an BGP-Nachbarn dieses Profils weiterleiten soll.

- Statisch: Das Gerät verteilt statische Routen aus der Routing-Tabelle an die BGP-Nachbarn.
- Verbunden: Das Gerät verteilt Routen von direkt angeschlossenen Netzwerken an die BGP-Nachbarn.
- LISP: Das Gerät verteilt LISP-Routen aus der Routing-Tabelle an die BGP-Nachbarn.

Wenn keine Option ausgewählt ist, verteilt das Gerät keine Routen an die BGP-Nachbarn dieses Nachbar-Profils (Default-Einstellung).

Redistributions-Filter

Name der Präfix-Filterliste aus *Präfix-Listen* auf Seite 378.

Default-Aktion

Definiert, wie Präfixe standardmäßig behandelt werden sollen, die in der Präfix-Liste konfiguriert sind. Mögliche Werte:

Erlauben

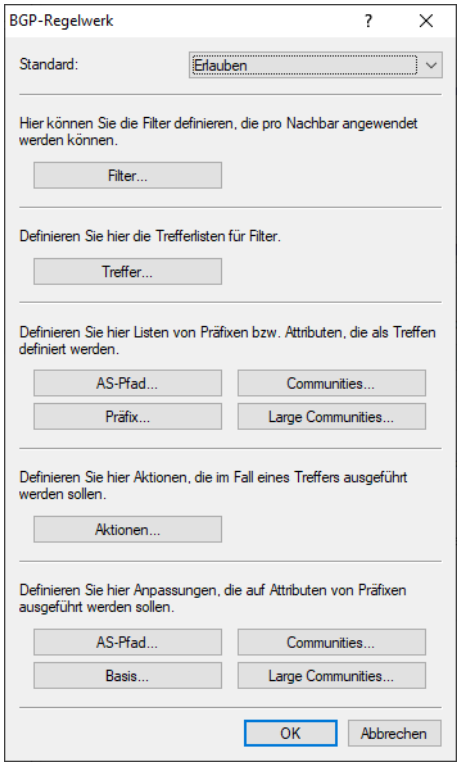
Verweigern

Kommentar

Kommentar zu diesem Eintrag.

BGP-Regelwerk

In diesem Abschnitt konfigurieren Sie die Filter-Einstellungen für ausgehende und ankommende NLRI.



Standard

Das Gerät wendet für einen BGP-Nachbarn diese Standardregel an, wenn unklar ist, ob es dessen Präfix akzeptieren oder ablehnen soll. Die Ursache dafür kann sein:

- Für diesen BGP-Nachbarn ist keine Regel konfiguriert.
- Der angegebene Filter existiert nicht.
- Kein Filter unter **Filter** trifft zu.

Filter

Definieren Sie hier die Filter, die pro Nachbar zur Verfügung stehen sollen.

Trefferlisten

Definieren Sie hier die Trefferlisten für Filter.

Präfix- und Attribut-Listen

Definieren Sie hier Listen von Präfixen und Attributen, die das Gerät als Treffer erkennen soll.

Aktionen

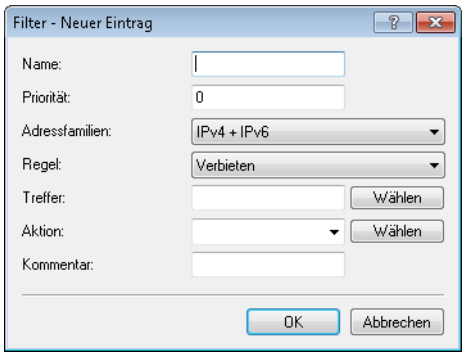
Definieren Sie hier Aktionen, die das Gerät im Falle eines Treffers ausführen soll.

Anpassungen

Definieren Sie hier Anpassungen, die das Gerät auf Präfix-Attribute anwenden soll.

Filter

Diese Tabelle enthält Filter, die eine NLRI von einem oder an einen BGP-Nachbarn durchlaufen muss, wenn dieser Nachbar entsprechend konfiguriert ist.



Name

Enthält den Namen für diesen Eintrag.

Bei mehreren Filtereinträgen mit identischem Namen bearbeitet das Gerät diese Filter gemäß der konfigurierten Priorität, bis ein Filter auf die NLRI zutrifft. Danach beendet das Gerät den Filterdurchlauf.

Priorität

Gibt die Priorität dieses Eintrages an.

Falls Einträge mit einem identischen Namen existieren, gehören diese Einträge zur selben Filterkette. Das Gerät arbeitet die Einträge dieser Filterkette entsprechend ihrer jeweiligen Priorität ab. Ein höherer Wert bedeutet eine höhere Priorität.

Adressfamilien

Gibt an, für welche Adressfamilie dieser Filter gilt.

Ohne ausgewählte Option ist dieser Eintrag deaktiviert.

Regel

Gibt an, ob das Gerät die gefilterte NLRI weiter verarbeiten soll, wenn dieser Filter für diese NLRI gültig ist.

- Ablehnen: Es erfolgt keine weitere Verarbeitung.
- Erlauben: Das Gerät verarbeitet die NLRI weiter.

Treffer

Gibt den Namen eines Eintrages aus der Tabelle **Treffer** an.

Das Gerät wendet diesen Filter an, wenn die NLRI mit den Kriterien übereinstimmt.

Wenn dieses Feld auf einen ungültigen Namen verweist, verweigert das Gerät die NLRI und führt keine weiteren Filter in der aktuellen Filterkette aus.

Aktion

Gibt an, welche Aktion aus der Tabelle **Aktion** das Gerät auf die NLRI anwenden soll.

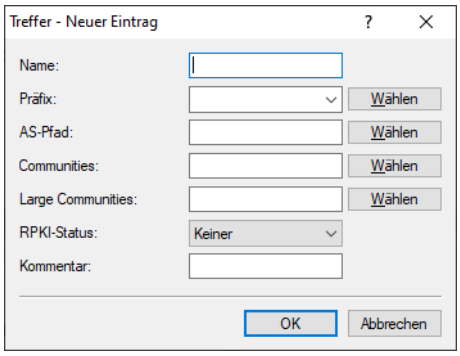
Wenn dieses Feld leer ist oder auf einen ungültigen Namen verweist, führt das Gerät keine Aktion aus.

Kommentar

Kommentar zu diesem Eintrag.

Treffer

Diese Tabelle kombiniert Präfix- und Attribut-Listen, um mehrere Listeneinträge auf Übereinstimmungen mit NLRI abzugleichen.



Name

Enthält den Namen für diesen Eintrag.

Präfix

Enthält den entsprechenden Eintrag der Liste unter **Präfix**.

AS-Pfad

Enthält den entsprechenden Eintrag der Liste unter **AS-Pfad** im Abschnitt „Präfix- und Attribut-Listen".

Communities

Enthält den entsprechenden Eintrag der Liste unter **Communities** im Abschnitt „Präfix- und Attribut-Listen".

Large Communities

Enthält den entsprechenden Eintrag der Liste unter **Large Communities** im Abschnitt „Präfix- und Attribut-Listen".

RPKI-Status

Der Resource Public Key Infrastructure (RPKI)-Status von Präfixen kann in einem BGP-Regelwerk verwendet werden und somit in Regeln auf ein BGP-Präfix angewendet werden. Es wird nicht empfohlen, ungültige Präfixe abzulehnen, sondern diesen eine niedrigere Präferenz zuzuweisen. In diesem Fall wird eine BGP-Regel definiert, die auf Präfixe mit dem RPKI-Status „ungültig" zutrifft. Als Aktion wird die Präferenz dieses Präfixes beispielsweise auf den Wert 10 gesetzt. Ein einmal abgelehntes Präfix wird nicht gespeichert und steht auch später im Prozess nicht mehr zur Verfügung es sei denn das Präfix wird vom BGP-Nachbarn erneut übertragen und neu bewertet.

Keiner

Der RPKI-Status wird nicht ausgewertet.

Nicht gefunden

Der Eintrag trifft zu, falls der PRKI-Status des Präfixes als „nicht gefunden“ markiert wird.

Ungültig

Der Eintrag trifft zu, falls der der PRKI-Status des Präfixes als „ungültig“ markiert wird.

Gültig

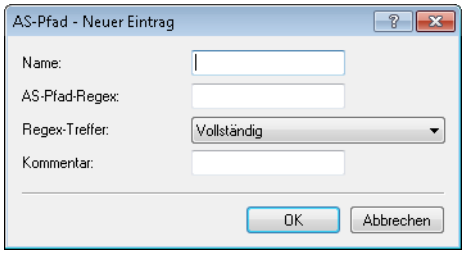
Der Eintrag trifft zu, falls der PRKI-Status des Präfixes als „gültig“ markiert wird.

Kommentar

Kommentar zu diesem Eintrag.

AS-Pfad (Attribut-Liste)

Diese Tabelle enthält AS-Pfad-Listen, um NLRIs anhand ihres `AS_PATH`-Attributes zu erkennen.



Name

Enthält den Namen für diesen Eintrag.

AS-Pfad-Regex

Enthält einen regulären Ausdruck, der das `AS_PATH`-Attribut der NLRI überprüft. Beispiele:

- `.*_100`: filtert alle NLRIs, die in „AS100“ ihren Ursprung haben.
- `.*_(100|200)`: filtert alle NLRIs,die in „AS100“ oder „AS200“ ihren Ursprung haben.
- `100_(.*_)?(500|400)_.*`: filtert alle NLRIs vom BGP-Nachbarn mit der AS-Nummer „AS100“ und die vorher zusätzlich den Weg über Netzwerke mit den AS-Nummern „AS500“ oder „AS400“ (oder beide) genommen haben.
- `100_(500|400|123)_.*`: filtert alle NLRIs vom BGP-Nachbarn mit der AS-Nummer „AS100“ und die dieser vorher direkt von BGP-Nachbarn mit den AS-Nummern „AS500“, „AS400“ oder „AS123“ erhalten hat.
- `100_(100_)*(300_)*300`: filtert alle NLRIs vom BGP-Nachbarn mit der AS-Nummer „AS100“ und die dieser vorher von seinem BGP-Nachbarn mit der AS-Nummer „AS300“ erhalten hat. Dieser Ausdruck berücksichtigt auch AS-Prepend Pfade.
- `100_.*_200`: filtert alle NLRIs vom BGP-Nachbarn mit der AS-Nummer „AS100“ und die im Netzwerk mit der AS-Nummer „AS200“ gestartet sind. Die Route, die die NLRIs vom „AS200“ bis zum „AS100“ genommen haben, ist hierbei unwichtig.

Regex-Treffer

Bestimmt, wie detailliert der reguläre Ausdruck unter **AS-Pfad-Regex** mit dem `AS_PATH`-Attribut der NLRI übereinstimmen muss, damit der Listeneintrag gültig ist.

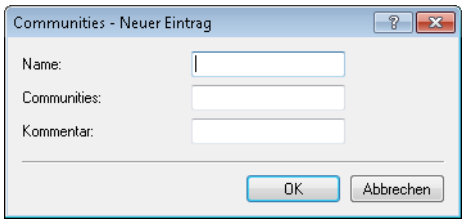
- Vollständig: Der reguläre Ausdruck beschreibt das gesamte `AS_PATH`-Attribut der NLRI.
- Teilweise: Der reguläre Ausdruck beschreibt nur Abschnitte des `AS_PATH`-Attributes.

Kommentar

Kommentar zu diesem Eintrag.

Communities (Attribut-Liste)

Diese Tabelle enthält Community-Listen, um NLRIs anhand ihres Community-Attributes zu erkennen.



Name

Enthält den Namen für diesen Eintrag.

Communities

Enthält Communities, die dem Community-Attribut der NLRI für eine Übereinstimmung entsprechen müssen.

Die Angabe der Communities erfolgt als kommaseparierte Liste (`<AS-Nummer1>:<Wert1>,<AS-Nummer2>:<Wert2>,<AS-Nummer3>:<Wert3>`).

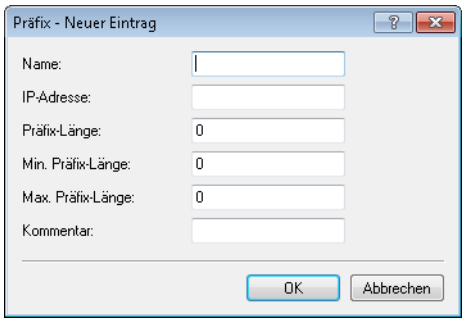
Kommentar

Kommentar zu diesem Eintrag.

Präfix (Attribut-Liste)

Diese Tabelle enthält Präfix-Listen, um NLRIs anhand ihres Netzwerkes (Präfix) und ihrer Netzmaske (Präfix-Länge) zu erkennen.

Ein Eintrag kann mehrere Präfixe enthalten.



Name

Enthält den Namen für diesen Eintrag.

IP-Adresse

Enthält die IPv4- oder IPv6-Adresse des Netzwerkes.

Präfix-Länge

Enthält die Netzmaske oder Präfix-Länge des Netzwerkes.

Dieser Eintrag legt fest, wie viele höchstwertige Bits (Most Significant Bit, MSB) der IP-Adresse für eine Übereinstimmung notwendig sind.

Die Präfix-Länge der NLRI muss für eine Übereinstimmung diesem Wert exakt entsprechen, wenn nicht für „Min. Präfix-Länge" und „Max. Präfix-Länge" andere Werte vorgegeben sind.

Beim Wert „0" stimmt das Netzwerk der NLRI dann überein, wenn es aus derselben IP-Adressfamilie stammt, die unter „IP-Adresse" vorgegeben ist.

Min. Präfix-Länge

Enthält die minimale Präfix-Länge, die das Netzwerk der NLRI für eine Übereinstimmung aufweisen darf.

Max. Präfix-Länge

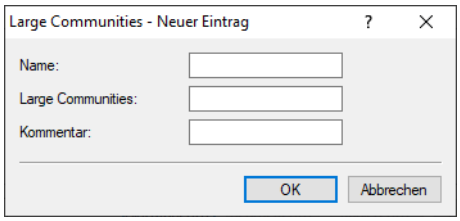
Enthält die maximale Präfix-Länge, die das Netzwerk der NLRI für eine Übereinstimmung aufweisen darf.

Kommentar

Kommentar zu diesem Eintrag.

Large Communities (Attribut-Liste)

Diese Tabelle enthält Large Community-Listen, um NLRIs anhand ihres Large-Community-Attributes zu erkennen.



Name

Enthält den Namen für diesen Eintrag.

Large Communities

Enthält Large Communities, die dem Large-Community-Attribut der NLRI für eine Übereinstimmung entsprechen müssen.

Die Angabe der Communities erfolgt als kommaseparierte Liste.

Struktur einer Large Community: *<Global Administrator bzw. ASN>*:*<Local Data Part 1>*:*<Local Data Part 2>*

Beispiel einer einzelnen Large Community: `64496:4294967295:2`

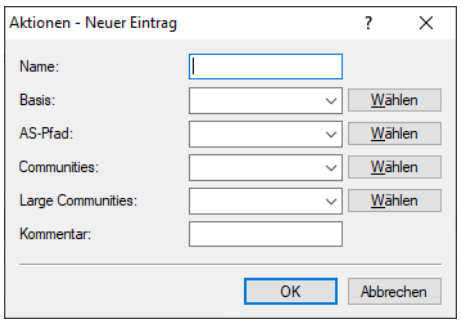
Beispiel als kommaseparierte Liste: `64496:4294967295:2, 64496:0:0`

Kommentar

Kommentar zu diesem Eintrag.

Aktionen

Diese Tabelle kombiniert Anpassungs-Listen, um mehrere Anpassungen auf NLRI mit einer Aktion durchzuführen.



Name

Enthält den Namen für diesen Eintrag.

Basis

Enthält den Namen für die Manipulation von Basis-Einträgen der NLRI.

Dieser Eintrag bezieht sich auf die Einträge der Anpassungs-Tabelle unter **Basis**.

AS-Pfad

Enthält den Namen für die Manipulation von `AS_PATH`-Attributen der NLRI.

Dieser Eintrag bezieht sich auf die Einträge der Anpassungs-Tabelle unter **AS-Pfad**.

Communities

Enthält den Namen für die Manipulation von Community-Einträgen der NLRI.

Dieser Eintrag bezieht sich auf die Einträge der Anpassungs-Tabelle unter *Communities (Anpassungs-Liste)* auf Seite 530.

Large Communities

Enthält den Namen für die Manipulation von Large-Community-Einträgen der NLRI.

Dieser Eintrag bezieht sich auf die Einträge der Anpassungs-Tabelle unter *Large Communities (Anpassungs-Liste)* auf Seite 533.

Kommentar

Kommentar zu diesem Eintrag.

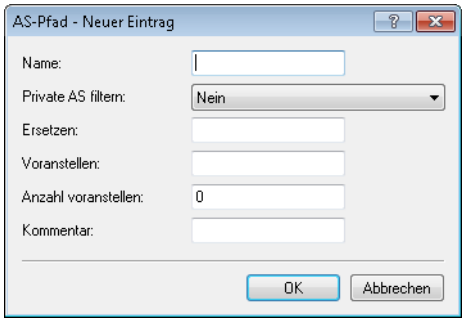
AS-Pfad (Anpassungs-Liste)

Diese Tabelle enthält Manipulationen der `AS_PATH`-Attribute von NLRI.

Wenn eine Aktion auf einen Eintrag dieser Tabelle zugreift, führt das Gerät alle in der entsprechenden Zeile aufgeführten Änderungen in der folgenden Reihenfolge durch:

1. „Private AS Filtern“
2. „Ersetzen“

3. Gemeinsam „Anzahl voranstellen“ und „Voranstellen“



Name

Enthält den Namen für diesen Eintrag.

Private AS filtern

Wenn konfiguriert, ändert das Gerät die Angabe der privaten AS-Nummern im `AS_PATH`-Attribut einer NLRI gemäß dieser Einstellung.

- Nein: Das Gerät behält die vorhandenen privaten AS-Nummern der NLRI.
- Entfernen: Das Gerät entfernt alle privaten AS-Nummern.
- Ersetzen: Das Gerät tauscht die vorhandenen privaten AS-Nummern gegen die AS-Nummer der aktuellen BGP-Instanz.

Ersetzen

Wenn konfiguriert, ändert das Gerät das `AS_PATH`-Attribut der NLRI auf den hier angegebenen Wert.

Voranstellen

Wenn konfiguriert, stellt das Gerät dem `AS_PATH`-Attribut der NLRI so oft den hier angegebenen Wert voran, wie unter „Anzahl voranstellen“ konfiguriert. Besondere Werte:

- `self`: Das Gerät stellt dem `AS_PATH`-Attribut der NLRI seine eigene AS-Nummer voran.
- `last`: Das Gerät stellt dem `AS_PATH`-Attribut der NLRI die zuletzt vorangestellte AS-Nummer voran.

Anzahl voranstellen

Bestimmt, wie oft das Gerät dem `AS_PATH`-Attribut der NLRI eine AS-Nummer voranstellen soll.

Kommentar

Kommentar zu diesem Eintrag.

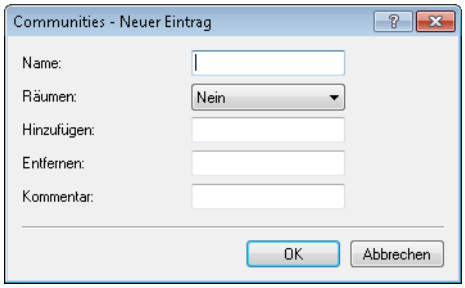
Communities (Anpassungs-Liste)

Diese Tabelle enthält Manipulationen der Community-Attribute von NLRI.

Wenn eine Aktion auf einen Eintrag dieser Tabelle zugreift, führt das Gerät alle in der entsprechenden Zeile aufgeführten Änderungen in der folgenden Reihenfolge durch:

1. „Räumen“
2. „Hinzufügen“

3. „Entfernen“



Name

Enthält den Namen für diesen Eintrag.

Räumen

Legt fest, ob das Gerät unbekannte Communities aus der NLRI löscht.

Bekannte Communities bleiben auch dann bestehen, wenn diese Option auf „Ja“ steht.

Bekannte Communities sind:

- `no-peer`
- `no-export`
- `no-advertise`
- `no-export-subconfed`
- `graceful-shutdown`

Mehr Informationen hierzu finden Sie unter *RFC 1997* und *RFC 3765*.

Hinzufügen

Legt fest, welche Communities das Gerät einer NLRI hinzufügt.

Die Angabe der Communities erfolgt als kommaseparierte Liste (`<AS-Nummer1>:<Wert1>,<AS-Nummer2>:<Wert2>,<AS-Nummer3>:<Wert3>`).

Entfernen

Legt fest, welche Communities das Gerät aus einer NLRI entfernt.

Die Angabe der Communities erfolgt als kommaseparierte Liste (`<AS-Nummer1>:<Wert1>,<AS-Nummer2>:<Wert2>,<AS-Nummer3>:<Wert3>`).

Bekannte Communities lassen sich nicht aus NLRI entfernen. Bekannte Communities sind:

- `no-peer`
- `no-export`
- `no-advertise`
- `no-export-subconfed`
- `graceful-shutdown`

Folgende Eingabeformate sind für Communities möglich:

Eingabeformat	Community
1:2	Standard Community
1.2.3.4:1	IPv4 spezifische Extended Community
roc:1.2.3.4:1	IPv4 spezifische Route Origin Extended Community (Site-of-Origin (SoO))
rtc:1.2.3.4:1	IPv4 spezifische Route Target Extended Community
ext2:1:2	zwei Byte AS Extended Community
ext4:1:2	vier Byte AS Extended Community
roc:1:2	zwei Byte AS Route Origin Extended Community (Site-of-Origin (SoO))
rtc:1:2	zwei Byte AS Route Origin Extended Community
roc:ext4:1:2	vier Byte AS Route Origin Extended Community (Site-of-Origin (SoO))

Kommentar

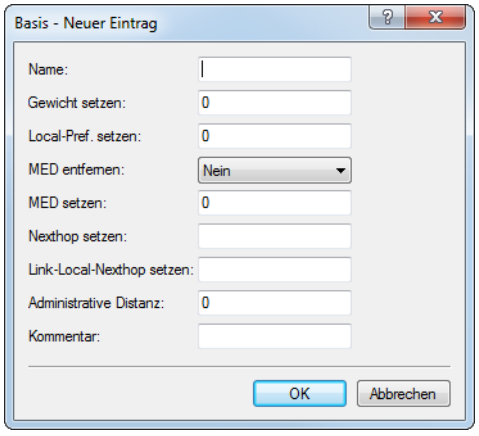
Kommentar zu diesem Eintrag.

Basis (Anpassungs-Liste)

Diese Tabelle enthält Manipulationen der Basis-Attribute von NLRIs.

Wenn eine Aktion auf einen Eintrag dieser Tabelle zugreift, führt das Gerät alle in der entsprechenden Zeile aufgeführten Änderungen durch.

Die Angabe von Basis-Attributen ist optional. Wenn die Aktion nur ein Basis-Attribut ändern soll, geben Sie an der entsprechenden Stelle den zu ändernden Wert ein und lassen Sie die übrigen Attribute in der jeweiligen Standardeinstellung.



Name

Enthält den Namen für diesen Eintrag.

Gewicht setzen

Das Gerät ändert die Gewichtung einer NLRI auf den hier angegebenen Wert.

Lokale Präferenz

Das Gerät ändert den lokalen Präferenz-Wert einer NLRI auf den hier angegebenen Wert.

MED entfernen

Das Gerät löscht bei der Einstellung „Ja“ den Multi Exit Discriminator (MED) einer NLRI, bevor es die Einstellung unter „MED setzen“ verarbeitet.

MED setzen

Das Gerät ändert den Multi Exit Discriminator (MED) einer NLRI auf den hier angegebenen Wert. Falls die NLRI keinen MED beinhaltet, erzeugt das Gerät dieses Attribut.

Nexthop setzen

Das Gerät ändert die Nexthop-IP-Adresse einer NLRI auf den hier angegebenen Wert. Mögliche Werte sind eine IPv4-Adresse oder eine globale IPv6-Adresse.

Link-Local-Nexthop setzen

Das Gerät ändert den IPv6 Link-Local-Nexthop einer NLRI auf den hier angegebenen Wert. Ist nur wirksam bei IPv6-Präfixen.

Administrative Distanz

Definiert, mit welcher „Administrativen Distanz“ empfangene Präfixe im BGP in die Routing-Tabelle eingetragen werden sollen. Die Liste der fest definierten „Administrativen Distanzen“ der verschiedenen Systemdienste bzw. Routing-Protokolle können auf der Konsole per `show admin-distance` angezeigt werden.

Kommentar

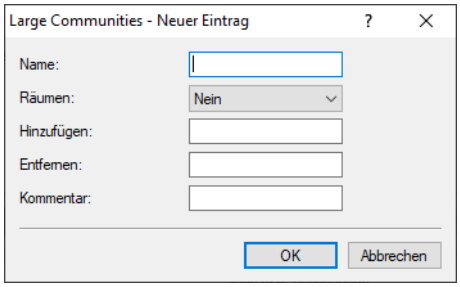
Kommentar zu diesem Eintrag.

Large Communities (Anpassungs-Liste)

Diese Tabelle enthält Manipulationen der Large-Community-Attribute von NLRI.

Wenn eine Aktion auf einen Eintrag dieser Tabelle zugreift, führt das Gerät alle in der entsprechenden Zeile aufgeführten Änderungen in der folgenden Reihenfolge durch:

1. **Räumen**
2. **Hinzufügen**
3. **Entfernen**



Name

Enthält den Namen für diesen Eintrag.

Räumen

Legt fest, ob das Gerät unbekannte Large Communities aus der NLRI löscht.

Hinzufügen

Legt fest, welche Large Communities das Gerät einer NLRI hinzufügt. Die Angabe der Large Communities erfolgt als kommaseparierte Liste.

Struktur einer Large Community: *<Global Administrator bzw. ASN>*:*<Local Data Part 1>*:*<Local Data Part 2>*

Beispiel einer einzelnen Large Community: `64496:4294967295:2`

Beispiel als kommaseparierte Liste: `64496:4294967295:2, 64496:0:0`

Entfernen

Legt fest, welche Large Communities das Gerät einer NLRI entfernt. Die Angabe der Large Communities erfolgt als kommaseparierte Liste.

Struktur einer Large Community: *<Global Administrator bzw. ASN>*:*<Local Data Part 1>*:*<Local Data Part 2>*

Beispiel einer einzelnen Large Community: `64496:4294967295:2`

Beispiel als kommaseparierte Liste: `64496:4294967295:2, 64496:0:0`

Kommentar

Kommentar zu diesem Eintrag.

6.23.2 Algorithmus für die Auswahl des besten Pfades

Der folgende Algorithmus wird zur Auswahl des besten Pfades angewendet:

1. Der Next-Hop aus der BGP-Update-Nachricht ist erreichbar.
2. Das eigene AS kommt nicht im `AS-Path` vor.
3. Der Next-Hop ist keine eigene Adresse.
4. Höchstes Gewicht
5. Höchste Lokale Präferenz
6. Kürzester `AS_PATH` (`AS_SET` zählt als Länge 1)
7. Niedrigster Origin (IGP < EGP < Incomplete)
8. Niedrigster MED

   Gilt nur, wenn die verglichenen Routen aus dem gleichen Nachbar-AS stammen.

9. eBGP wird vor iBGP bevorzugt.
10. Niedrigste Router ID
11. Nachbar mit niedrigster IP-Adresse
12. Nachbar mit niedrigstem RTG-Tag
13. Der älteste Pfad wird gegenüber einem neu gelernten Pfad bevorzugt.

6.23.2.1 Beeinflussung des Routing-Algorithmus durch Attribute

Sie haben die Möglichkeit, die Auswahl des besten Pfades zu einem Ziel mittels folgender Attribute zu beeinflussen:

Gewicht

Gewicht ist ein proprietäres Attribut, welches nicht in BGP-Update-Nachrichten an Nachbarn propagiert wird. „Gewicht" ist somit nur auf dem lokalen Router gültig. Sie haben die Möglichkeit, das Attribut lokal entweder pro Adressfamilie oder durch Filterregeln zu setzen.

Lokale Präferenz

Lokale Präferenz ist ein BGP-Standard-Attribut (`LOCAL_PREF`) und wird per iBGP an Nachbarn propagiert.

Alle Pfade besitzen standardmäßig eine lokale Präferenz von 100 (Default). Das Attribut wird in der Praxis

z. B. dazu verwendet, bestimmte Präfixe zu bevorzugen. Das Attribut kann entweder pro Adressfamilie oder durch Filterregeln gesetzt werden.

AS_PATH

Der AS-Pfad (AS-Path) gibt den zurückgelegten Pfad einer Route an. Durch Filterregeln kann der AS-Pfad manipuliert werden, indem z. B. die eigene AS-Nummer mehrfach vorangestellt wird. Dadurch erscheint der AS-Path bei einem Nachbarn länger.

Origin

Origin ist ein BGP-Standard-Attribut, das an alle Nachbarn propagiert wird. Dieses Attribut definiert den Ursprung einer Route. Dies kann ein Interior Gateway Protokoll (IGP), das Exterior Gateway-Protokoll (EGP, RFC 904) oder „Incomplete" sein. Dabei steht „Incomplete" für die Redistribution durch ein anderes Routing-Protokoll. Das Attribut **Origin** wird automatisch vom Router gesetzt. Routen, die in BGP durch einen Eintrag in der IPv4- / IPv6-Netzwerktabelle hinzugefügt werden, erhalten den Ursprung IGP. Routen, die in den Adressfamilien zum Weiterverteilen konfiguriert werden, erhalten den Ursprung „Incomplete".

MED

MED (`MULTI_EXIT_DISC`) ist ein optionales BGP-Attribut, um mehrere Eingänge oder Ausgänge zum gleichen Nachbar-AS zu unterscheiden. Das Attribut kann durch Filterregeln gesetzt werden.

Router ID

Die Router ID, auch als BGP-Identifier bezeichnet, ist die eindeutige Identifikation eines Routers. Diese besteht aus der IPv4-Adresse des Routers. Die Router ID können Sie unter **BGP-Instanz** > **Router ID** manuell konfigurieren.

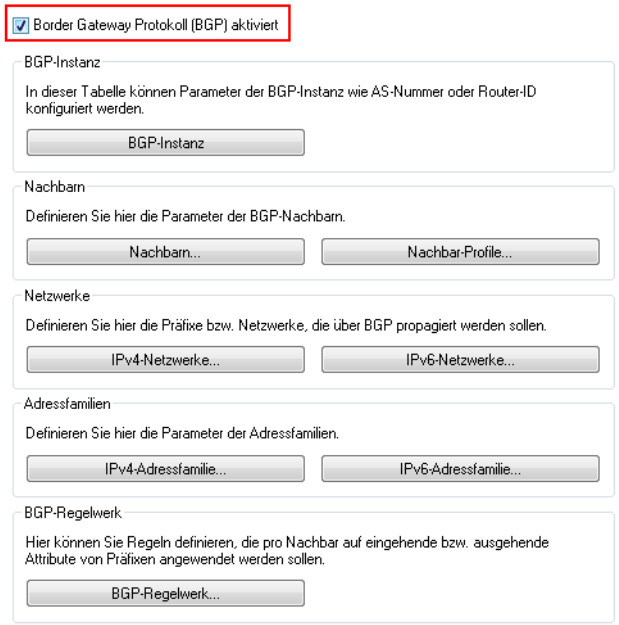
6.23.3 Tutorial: Einrichtung von BGPv4 unter LANconfig

Zwei LANCOM Router sind über eine WAN-Verbindung miteinander verbunden und sollen über BGP bestimmte IPv4-Netzwerke propagieren. Bei den Routern handelt es sich um einen LANCOM 1800VAW in der Zentrale und einen LANCOM 1800VA-4G in der Filiale.

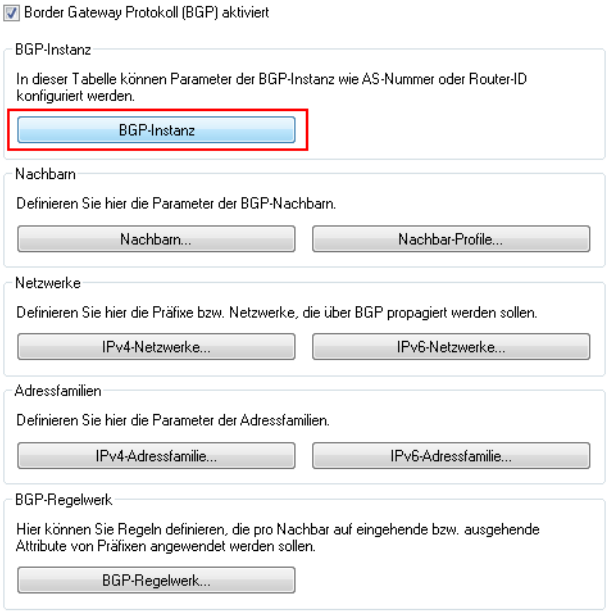
Eine bestehende WAN-Verbindung zwischen beiden Geräten wird vorausgesetzt.

1. **Aktivieren von BGP**: Öffnen Sie den Menüpunkt **Routing-Protokolle** > **BGP** in der Konfiguration der beiden Router und setzen Sie den Haken in der Checkbox **Border Gateway Protokoll (BGP) aktiviert**. Hiermit haben Sie BGP auf

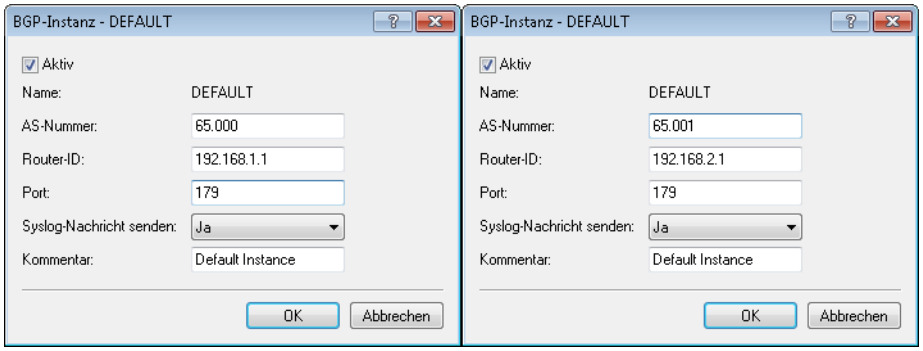
dem jeweiligen Gerät aktiviert. In den nächsten Schritten konfigurieren Sie die einzelnen BGP-Instanzen, die zugehörigen Nachbarn und die zu propagierenden Netze konfiguriert.



2. **Konfiguration der einzelnen BGP-Instanzen**: Um die BGP-Instanz des jeweiligen Routers zu konfigurieren, klicken Sie auf die Schaltfläche **BGP-Instanz**.



3. Bestimmen Sie im Konfigurationsfenster die allgemeinen Informationen zu der BGP-Instanz des jeweiligen Routers. Im folgenden Screenshot sind die Konfigurationen für beide Geräte zum direkten Vergleich nebeneinander aufgeführt.



In der linken Bildhälfte ist der LANCOM 1800VAW abgebildet, rechts sehen Sie die Parameter des LANCOM 1800VA-4G.

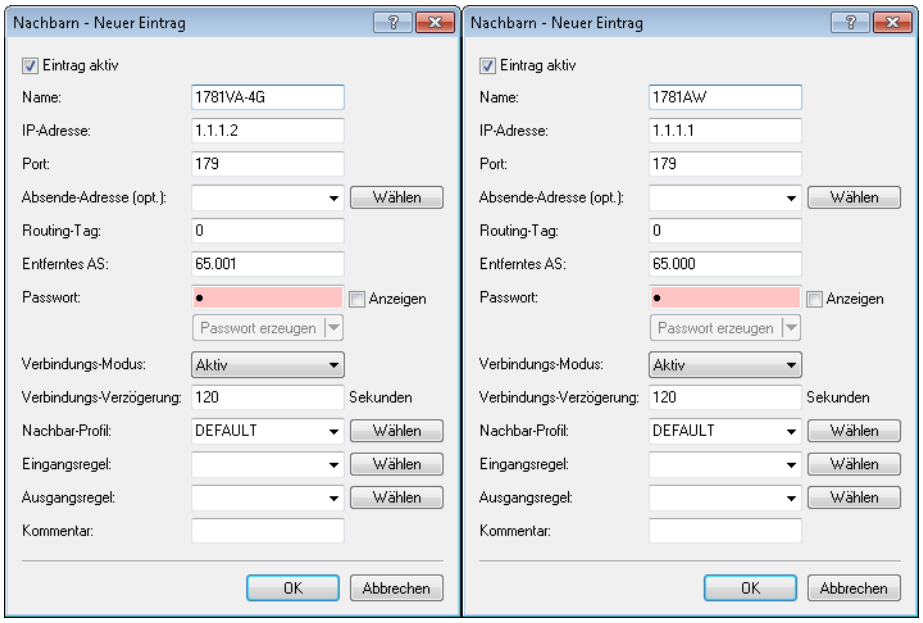
Parameter	Beschreibung
Checkbox **Aktiv**	Aktivieren Sie die BGP-Instanz des Routers. Dies ist notwendig, damit eine Kommunikation zwischen den beiden Routern möglich ist.
AS-Nummer	Die AS-Nummer (Nummer des **A**utonomen **S**ystems) fasst Router unter der gleichen Administration zusammen. Geben Sie hier unterschiedliche Nummern ein, handelt es sich um eBGP-Peers. Bei identischen Nummern handelt es sich um Peers im selben AS (iBGP). Welche Einträge gültig sind, erfahren Sie unter *http://www.iana.org/assignments/as-numbers/as-numbers.xhtml*.
Router-ID	Hinterlegen Sie eine IP-Adresse des Routers. Tragen Sie `0.0.0.0` ein, wird die IP-Adresse automatisch ermittelt. Die Router-ID muss unter allen Nachbarn eines BGP-Routers eindeutig sein. Hier sind unterschiedliche Einträge notwendig.
Port	Konfigurieren Sie den TCP-IP-Port, den der Router für eingehende BGP-Verbindungen nutzt. Der Default-Wert ist 179.
Syslog-Nachrichten senden	Geben Sie an, ob das Gerät Syslog-Nachrichten erzeugen soll. Diese können Sie bequem über WEBconfig einsehen.
Kommentar	Tragen Sie einen Kommentar ein, der das spätere Nachvollziehen der Konfiguration erleichtert.

4. **Konfiguration der BGP-Nachbarn**: Nachdem die Konfiguration der BGP-Instanz abgeschlossen ist, ist es notwendig, die zugehörigen Nachbarn zu definieren, mit denen die Informationen der zu propagierenden Netze ausgetauscht werden. Klicken Sie dazu auf die Schaltfläche **Nachbarn**.



5. Klicken Sie auf die Schaltfläche **Hinzufügen**, um einen neuen BGP-Nachbarn zu konfigurieren. Bestimmen Sie im Konfigurationsfenster die Informationen zu den BGP-Nachbarn der einzelnen Router.

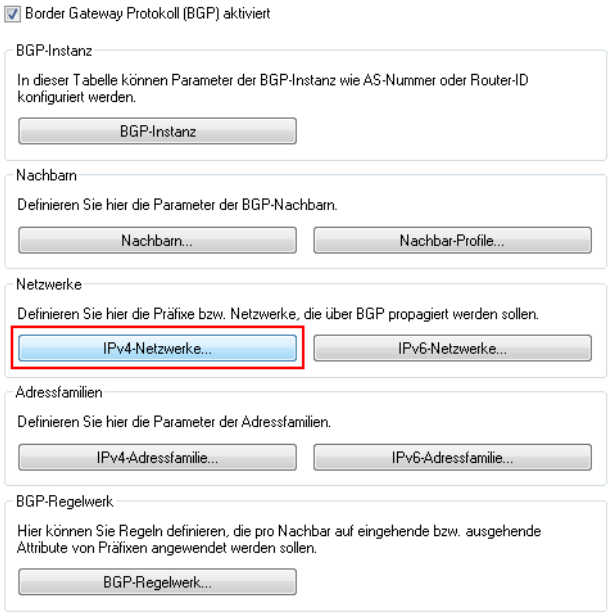
Im folgenden Screenshot sind die Konfigurationen für beide Geräte zum direkten Vergleich nebeneinander aufgeführt. Hierbei wird nur auf die Konfigurationsparameter eingegangen, die von den Default-Werten abweichen.



In der linken Bildhälfte ist der LANCOM 1800VAW abgebildet, rechts sehen Sie die Parameter des LANCOM 1800VA-4G.

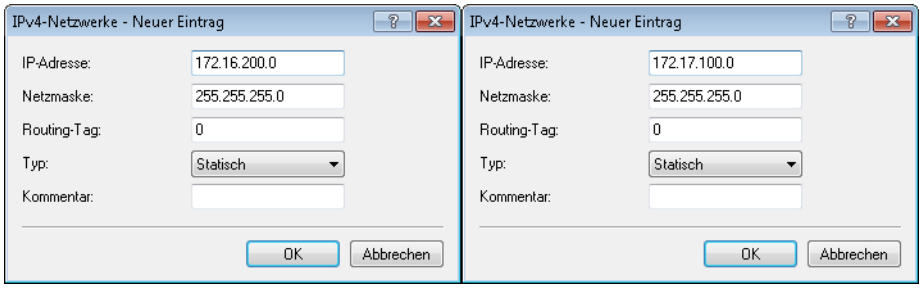
Parameter	Beschreibung
Eintrag aktiv	Aktivieren Sie den Eintrag für den entsprechenden Nachbarn.
Name	Weisen Sie dem Nachbarn einen Namen zu. In diesem Beispiel wird eine abgekürzte Version der Gerätebezeichnung zur einfachen Identifizierung in der Konfiguration verwendet.
IP-Adresse	Tragen Sie die IP-Adresse ein, unter der der Nachbar zu erreichen ist. In diesem Beispiel ist die WAN-Adresse des 1800VAW `1.1.1.1` und die des 1800VA-4G `1.1.1.2`.
Entferntes AS	Tragen Sie die in **Schritt 2** definierten AS-Nummern der entsprechenden Nachbarn ein.
Passwort	Tragen Sie ein Passwort ein, mit dem die Kommunikation zwischen den beiden BGP-Nachbarn durch einen MD5-Hash verschleiert wird. Das Passwort muss auf beiden Seiten identisch sein.

6. **Konfiguration der zu propagierenden IPv4-Netzwerke**: Konfigurieren Sie die Netzwerke, die die einzelnen BGP-Instanzen propagieren. Klicken Sie dazu auf die Schaltfläche **IPv4-Netzwerke**.



7. Klicken Sie auf die Schaltfläche **Hinzufügen**, um ein neues IPv4-Netzwerk zu definieren, welches propagiert werden soll.

Im folgenden Screenshot sind die Konfigurationen für beide Geräte zum direkten Vergleich nebeneinander aufgeführt. Hierbei wird nur auf die Konfigurationsparameter eingegangen, die von den Default-Werten abweichen.



In der linken Bildhälfte ist der LANCOM 1800VAW abgebildet, rechts sehen Sie die Parameter des LANCOM 1800VA-4G.

Parameter	Beschreibung
IP-Adresse	Der IPv4-Adressbereich des zu propagierenden Netzwerkes.
Netzmaske	Die zum definierten Netzwerk gehörige Netzmaske.
Typ	Der Typ, mit dem die Propagierung erfolgen soll. In diesem Beispiel statisch, um eine möglichst einfache Konfiguration zu zeigen.

8. Schreiben Sie die Konfiguration in beide Geräte zurück.
9. Die Überprüfung der BGP-Verbindung erfolgt einfach über die Kommandozeile. Der Befehl `show bgp-neighbor` zeigt alle aktiven Nachbarn und deren Status an.

```
> show bgp-neighbor
BGP-Neighbors:

1.1.1.2, Rtg-Tag 0
 BGP-State: ESTABLISHED, up for 00:09:23
 remote AS 65001, remote router id 192.168.1.161, eBGP
 Neighbor capabilities:
  Four-octets ASN capability: advertised and received
  Address family IPv4 NLRI used for unicast forwarding: advertised and received
> _
```

6.23.4 Tutorial: Präferenz von Präfixen einrichten

„Präferenz" ist ein optionales BGP-Attribut, mit dessen Hilfe Sie Pfade zu einem entsprechenden Präfix bevorzugen können. Das Gerät bevorzugt einen Pfad mit einer höheren Präferenz gegenüber einem Pfad mit einer niedrigeren Präferenz.

Innerhalb eines AS übertragen die iBGP-Nachbarn untereinander das BGP-Attribut `LOCAL_PREFERENCE`. Zwischen benachbarten AS übertragen die eBGP-Nachbarn dieses Attribut nicht.

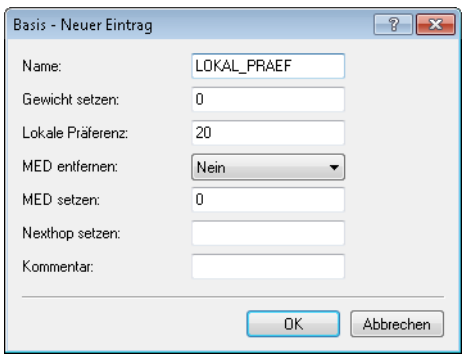
Es gibt zwei Methoden, um Präferenzen zu konfigurieren:

- Pro Adressfamilie
- Durch Regeln

Dieses Beispiel erläutert die Konfiguration, um das Präfix eines BGP-Nachbarn mit der Präferenz „200"gegenüber dem Präfix eines anderen BGP-Nachbarn mit der Präferenz „100"zu priorisieren.

Die Defaulteinstellung für Präferenzen ist „100". Dementsprechend genügt es, nur den zu bevorzugenden Nachbarn mit der Präferenz „200" zu konfigurieren.

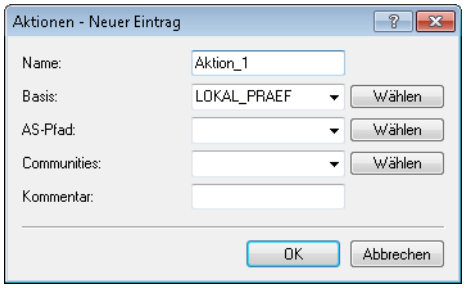
1. Erstellen Sie unter **Routing-Protokolle** > **BGP** > **BGP-Regelwerk** > **Basis** einen neuen Eintrag zur Manipulation von Basis-Attributen der NLRI (in diesem Fall das Basis-Attribut `LOCAL_PREFERENCE`).



Vergeben Sie dem Eintrag einen aussagekräftigen Namen.

Unter **Lokale Präferenz** geben Sie den Wert „200" für die neue lokale Präferenz ein.

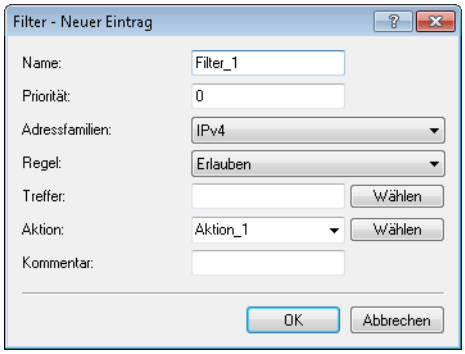
2. Definieren Sie unter **Routing-Protokolle** > **BGP** > **Aktionen** eine neue Aktion.



Vergeben Sie der Aktion einen aussagekräftigen Namen.

Wählen Sie unter **Basis** den zuvor erstellten Basis-Eintrag aus.

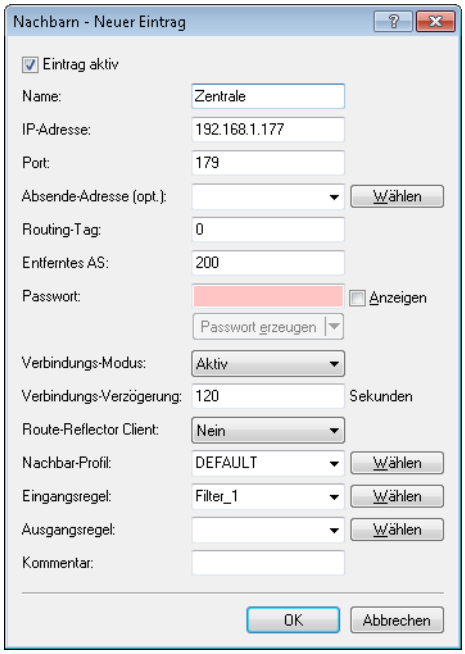
3. Erstellen Sie unter **Routing-Protokolle** > **BGP** > **BGP-Regelwerk** > **Filter** einen neuen Filter.



Vergeben Sie dem Filter einen aussagekräftigen Namen.

Wählen Sie unter **Adressfamilien** das entsprechende Verbindungsprotokoll zum BGP-Nachbarn aus. Mit der Einstellung „Erlauben" im Feld **Regel** bestimmen Sie, dass das Gerät die abgehende NLRI verändern soll. Wählen Sie unter **Aktion** die zuvor erstellte Aktion aus.

4. Erstellen Sie unter **Routing-Protokolle** > **BGP** > **Nachbarn** einen neuen Eintrag für einen BGP-Nachbarn.



Vergeben Sie dem Nachbarn einen aussagekräftigen Namen und konfigurieren Sie seine IP-Adresse sowie die Nummer des entfernten AS, in dem er sich befindet.

Wenn Sie für diesen BGP-Nachbarn kein eigenes Nachbar-Profil erstellt haben, verwenden Sie das „Default"-Profil.

Wählen Sie unter **Eingangsregel** den zuvor erstellten Filter aus.

5. Um die Konfiguration zu prüfen, öffnen Sie eine Terminalverbindung zum Gerät.

   Der Befehl `show bgp-policy Filter_1` zeigt die aktuelle Einstellung der Regel „Filter_1" an.

```
> show bgp-policy Filter_1
Traverse chain "Filter_1"
   Inspect filter of priority 0
      Match IPv4 routes
      Execute action "Aktion_1"
         No AS-path override configured
         Apply basic override "LOKAL_PRAEF"
            Set local preference to 200
         No community override configured
      Permit route
> _
```

   Der Befehl `show bgp-v4-adj-rib-in` zeigt die Routing Information Base (RIB) an.

```
> show bgp-v4-adj-rib-in
IPv4 Unicast Adj-RIB-In

 192.168.1.177, Rtg-Tag 0

  Prefix            Next Hop       Local-Pref  Weight  MED AS Path
  ------------------------------------------------------------------
  192.168.210.0/24  192.168.1.177         200       0    0 AS sequence: 200
  192.168.211.0/24  192.168.1.177         200       0    0 AS sequence: 200

> _
```

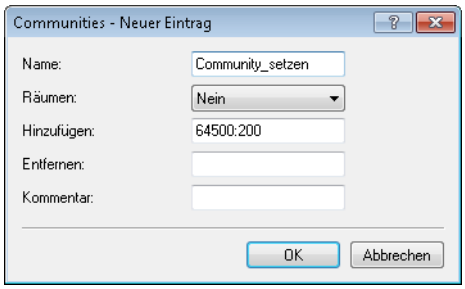
6.23.5 Tutorial: Community-Attribut setzen

„Community" ist ein optionales BGP-Attribut, mit dessen Hilfe Sie Präfixe in logischen Gruppen zusammenfassen und darüber identifizieren können. Auf diese Gruppen lassen sich Ein- und Ausgangsregeln anwenden. Zu einem Präfix können Sie mehrere Communities definieren.

Neben den bekannten Communities `NO-ADVERTISE`, `GRACEFUL-SHUTDOWN` oder `NO-EXPORT` ist die Bedeutung einer Community vom Provider frei definierbar. So definiert z. B. der Provider des AS „64500", dass Kunden-Routen mit der Community „64500:200" mit der Präferenz „200" zu behandeln sind und Routen mit der Community „64500:90" mit der Präferenz „90".

Das folgende Beispiel erläutert die Erweiterung aller abgehenden Routen mit Community „64500:200".

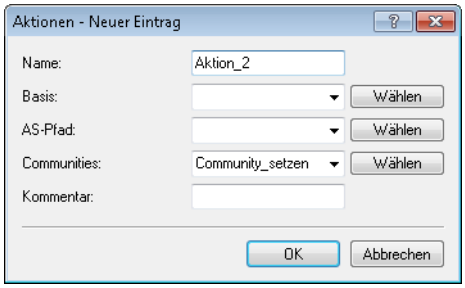
1. Erstellen Sie unter **Routing-Protokolle** > **BGP** > **BGP-Regelwerk** > **Communities (Anpassungen)** einen neuen Community-Eintrag.



   Vergeben Sie der Community einen aussagekräftigen Namen.

   Unter **Hinzufügen** geben Sie den Wert „64500:200" für das Community-Attribut an. Diesen Wert fügt das Gerät dem Community-Attribut der abgehenden NLRI an.

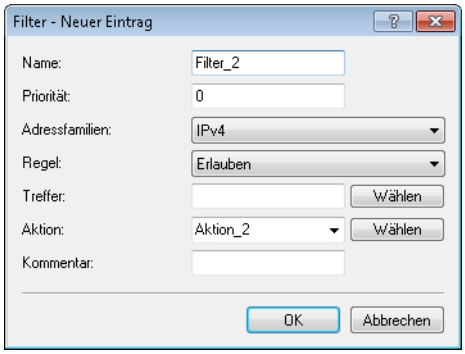
2. Definieren Sie unter **Routing-Protokolle** > **BGP** > **Aktionen** eine neue Aktion.



Vergeben Sie der Aktion einen aussagekräftigen Namen.

Wählen Sie unter **Communities** die zuvor erstellte Community aus.

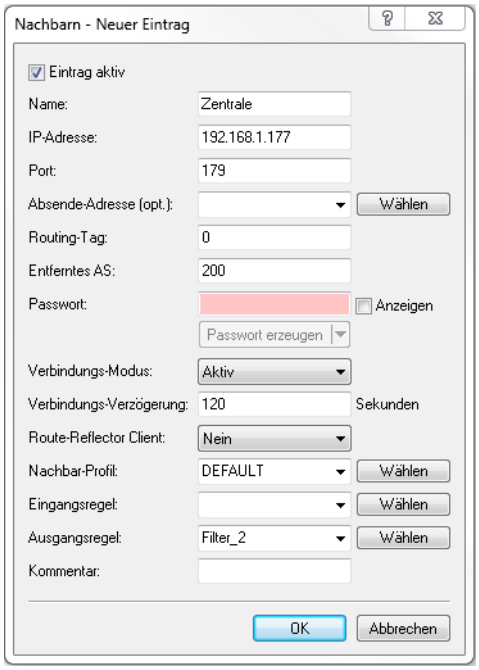
3. Erstellen Sie unter **Routing-Protokolle** > **BGP** > **BGP-Regelwerk** > **Filter** einen neuen Filter.



Vergeben Sie dem Filter einen aussagekräftigen Namen.

Wählen Sie unter **Adressfamilien** das entsprechende Verbindungsprotokoll zum BGP-Nachbarn aus. Mit der Einstellung „Erlauben“ im Feld **Regel** bestimmen Sie, dass das Gerät die abgehende NLRI verändern soll. Wählen Sie unter **Aktion** die zuvor erstellte Aktion aus.

4. Erstellen Sie unter **Routing-Protokolle** > **BGP** > **Nachbarn** einen neuen Eintrag für einen BGP-Nachbarn.



   Vergeben Sie dem Nachbarn einen aussagekräftigen Namen und konfigurieren Sie seine IP-Adresse sowie die Nummer des entfernten AS, in dem er sich befindet.

   Wenn Sie für diesen BGP-Nachbarn kein eigenes Nachbar-Profil erstellt haben, verwenden Sie das „Default"-Profil.

   Wählen Sie unter **Ausgangsregel** den zuvor erstellten Filter aus.

5. Um die Konfiguration zu prüfen, öffnen Sie eine Terminalverbindung zum Gerät.

   Der Befehl `show bgp-policy Filter_2` zeigt die aktuelle Einstellung der Regel „Filter_2" an.

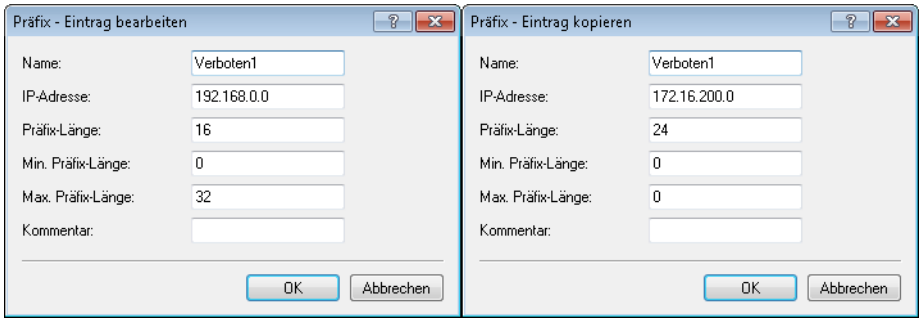
```
> show bgp-policy Filter_2
Traverse chain "Filter_2"
   Inspect filter of priority 0
      Match IPv4 routes
      Execute action "Aktion_2"
         No AS-path override configured
         No basic override configured
         Apply community override "Community_setzen"
            Add community 64500:200
      Permit route
> _
```

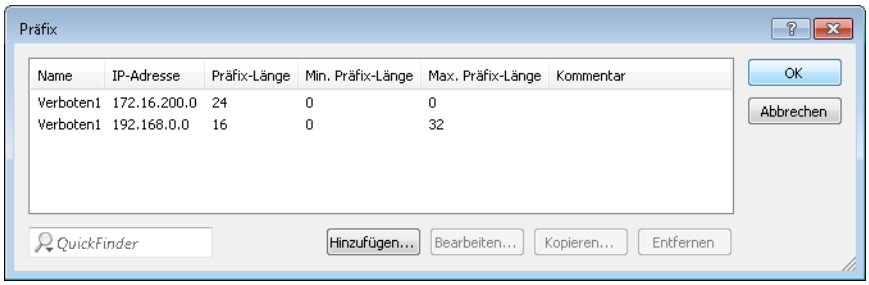
6.23.6 Tutorial: Empfangene Präfixe filtern

Dieses Beispiel erläutert die Konfiguration, um die folgenden ankommenden Präfixe eines BGP-Nachbarn auszufiltern:

- alle Präfixe aus dem Bereich „192.168.0.0/16"
- das einzelne Präfix „172.16.200.0/24"

1. Erstellen Sie unter **Routing-Protokolle** > **BGP** > **BGP-Regelwerk** > **Präfix** zwei neue Präfix-Einträge mit den zu filternden Präfixen.



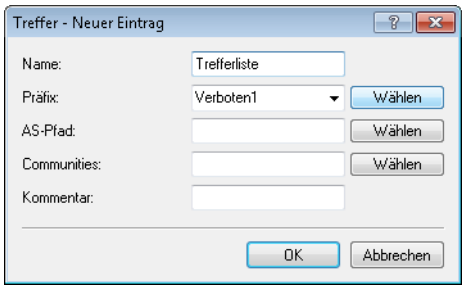


Vergeben Sie den Einträgen jeweils einen aussagekräftigen Namen.

Für jedes zu filternde Präfix geben Sie jeweils einen Eintrag an, der jedoch immer den gleichen Namen besitzt.

Bestimmen Sie je Eintrag die IP-Adresse sowie die benötigte Präfix-Länge.

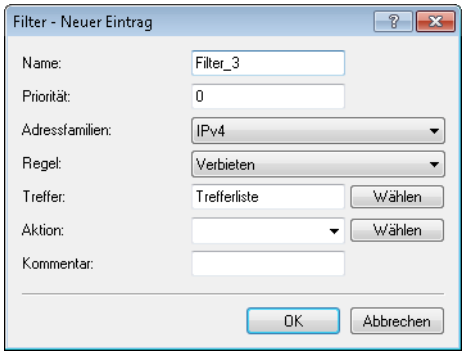
2. Definieren Sie unter **Routing-Protokolle** > **BGP** > **BGP-Regelwerk** > **Treffer** einen Treffer für den zuvor erstellten Präfix-Eintrag.



Vergeben Sie dem Eintrag einen aussagekräftigen Namen.

Wählen Sie unter **Präfix** die zuvor erstellte Präfix-Bezeichnung aus.

3. Erstellen Sie unter **Routing-Protokolle** > **BGP** > **BGP-Regelwerk** > **Filter** einen neuen Filter.



Vergeben Sie dem Filter einen aussagekräftigen Namen.

Wählen Sie unter **Adressfamilien** das entsprechende Verbindungsprotokoll zum BGP-Nachbarn aus. Mit der Einstellung „Verbieten" im Feld **Regel** bestimmen Sie, dass das Gerät die ankommenden Präfixe herausfiltern soll. Wählen Sie unter **Treffer** den zuvor erstellten Treffer aus.

4. Um die Konfiguration zu prüfen, öffnen Sie eine Terminalverbindung zum Gerät.

Der Befehl `show bgp-policy Filter_3` zeigt die aktuelle Einstellung der Regel „Filter_3" an.

```
> show bgp-policy Filter_3
Traverse chain "Filter_3"
   Inspect filter of priority 0
      Match IPv4 routes
      Assess match "Trefferliste"
         Evaluate prefix list "Verboten1"
            Analyze prefix 172.16.200.0
               Match IPv4 routes
               Match route's 24 MSB
               Match route prefix length in [24, 24]
            Analyze prefix 172.168.0.0
               Match IPv4 routes
               Match route's 16 MSB
               Match route prefix length in [16, 32]
         No AS-path list configured
         No community list configured
      Deny route
> _
```

6.24 OSPF

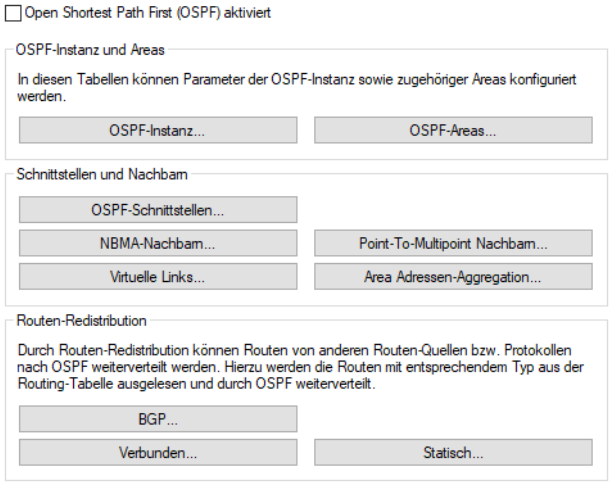
Open Shortest Path First (OSPF) ist ein Link State Routing Protokoll nach RFC 2328. Es gehört zur Kategorie der **Interior-Gateway-Protokolle** (IGP). Dabei tauschen die Router regelmäßig Link-Status-Informationen per Link State Advertisement (LSA) aus. Die Router finden sich automatisch im lokalen Netzwerk per Multicast. OSPF wird in der Regel dazu verwendet um in großen Netzen (LANs) interne Routinginformationen auszutauschen.

Jeder Router hat dabei eine identische Kopie der Datenbank (Link State Database, LSDB) vorliegen, woraus er Router mit Hilfe des Dijkstra-Algorithmus (Shortest Path First, SPF) den Kürzeste-Pfad-Baum bestimmt.

Im Gegensatz hierzu gehört BGP zur Kategorie der **Exterior Gateway Protokolle** (EGP) und wird in der Regel dazu verwendet, um Routen zwischen autonomen Systemen oder innerhalb von VPNs auszutauschen.

6.24.1 OSPF mit LANconfig konfigurieren

Um OSPF mit LANconfig zu konfigurieren, wechseln Sie in die Ansicht **Routing Protokolle** > **OSPF**.



Open Shortest Path First (OSPF) aktiviert

Um die OSPF-Funktion zu aktivieren, markieren Sie die Option **Open Shortest Path First (OSPF) aktiviert**.

OSPF-Instanz

Die Tabelle **OSPF-Instanz** definiert die OSPF-Instanzen auf diesem Gerät. Es werden mehrere gleichzeitig aktive OSPF-Instanzen auf einem Gerät unterstützt. Jede Instanz entspricht dann einem autonomen System bzw. einer OSPF-Domäne.

OSPF-Areas

Die Tabelle **OSPF-Areas** definiert die Parameter der OSPF-Areas.

OSPF-Schnittstellen

In dieser Tabelle werden die Schnittstellen definiert, auf denen OSPF verwendet werden soll.

NBMA-Nachbarn

Non-Broadcast-Multiaccess-Netzwerke sind Netzwerke, in denen mehrere Router vorhanden sind, aber kein Broadcast unterstützt wird. OSPF emuliert in diesem Netzwerktyp den Betrieb in einem Broadcast-Netzwerk. In diesem Netzwerktyp wird ein Designierter Router gewählt.

Die Kommunikation findet nicht per Multicast statt, sondern per Unicast. Nachbarschaftsbeziehungen müssen manuell konfiguriert werden, da sich die Router nicht automatisch per Multicast finden können.

Point-To-Multipoint Nachbarn

In einem Point-To-Multipoint-Netzwerk werden alle Nachbarn so behandelt als wären Point-To-Point-Nachbarn über ein Nicht-Broadcast-Netzwerk direkt verbunden. Es wird keine Designierter Router gewählt, die Kommunikation erfolgt per Multicast.

Virtuelle Links

In dieser Tabelle können Virtuelle Links (auch bezeichnet als Transit-Area) definiert werden. Grundsätzlich müssen bei OSPF alle Areas direkt mit der Backbone-Area verbunden sein. In Fällen, wo dies nicht möglich ist, können virtuelle Links verwendet werden. Ein virtueller Link verbindet einen Router durch eine nicht-Backbone-Area mit der Backbone-Area.

Area Adressen-Aggregation

Um die Anzahl der Einträge in den Routing-Tabellen zu reduzieren, können durch Adressen-Aggregation an Area-Grenzen, beim Übergang von einer Nicht-Backbone-Area zur Backbone-Area, IP-Adressen zusammengefasst werden. Das entsprechende Subnetz wird als Summary LSA angekündigt.

BGP

Dynamisch gelernte Routen aus BGP-Quellen bzw. -Protokollen können nach OSPF weiterverteilt werden.

Verbunden

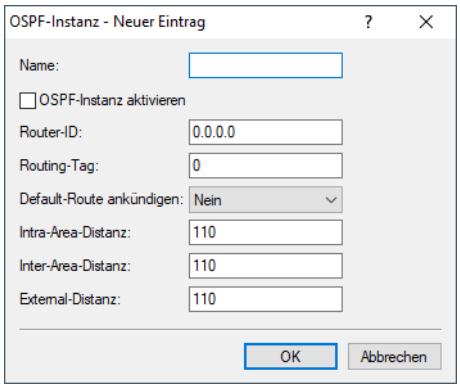
Verbundene Routen, d. h. Routen, die vom Betriebssystem automatisch in die Routing-Tabelle eingetragen werden, können nach OSPF weiterverteilt werden.

Statisch

Statische Routen, d. h. Routen, die manuell vom Benutzer in die Routing-Tabelle eingetragen werden, können nach OSPF weiterverteilt werden.

6.24.1.1 OSPF-Instanz

Die OSPF-Instanz des Gerätes konfigurieren Sie unter **OSPF-Instanz**.



Name

Enthält den Namen der OSPF-Instanz.

OSPF-Instanz aktivieren

Aktiviert bzw. deaktiviert diese OSPF-Instanz.

Router-ID

Enthält die 32 Bit Router-ID (repräsentiert als IPv4-Adresse), die dieser OSPF-Instanz zugeordnet ist. Die Router-ID identifiziert diesen Router eindeutig innerhalb einer OSPF-Domäne.

Routing-Tag

Enthält das dieser Instanz zugeordnete Routing-Tag.

Default-Route ankündigen

Definiert, ob dieser Router in dieser Instanz die Default-Route ankündigen bzw. propagieren soll.

Mögliche Werte:

Nein (Default)

Der Router kündigt keine Default-Route an.

Ja

Der Router kündigt die Default-Route immer an, unabhängig davon, ob die Default-Route in seiner Routing-Tabelle vorhanden ist.

Dynamisch

Der Router kündigt die Default Route nur an, falls die Default-Route in seiner Routing-Tabelle auch vorhanden ist.

Intra-Area-Distanz

Definiert die Administrative Distanz, mit der OSPF empfangende Routen des Typs Intra-Area in die Routing-Tabelle einfügt.

Inter-Area-Distanz

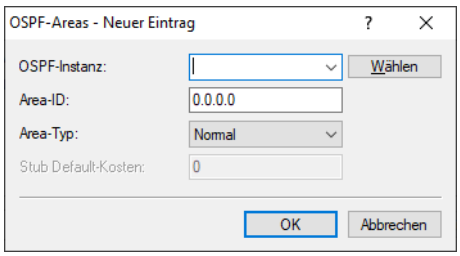
Definiert die Administrative Distanz, mit der OSPF empfangende Routen des Typs Inter-Area in die Routing-Tabelle einfügt.

External-Distanz

Definiert die Administrative Distanz, mit der OSPF empfangende Routen des Typs External in die Routing-Tabelle einfügt.

6.24.1.2 OSPF-Areas

Die Parameter der OSPF-Areas konfigurieren Sie unter **OSPF-Areas**.



OSPF-Instanz

Enthält den Namen der OSPF-Instanz.

Area-ID

Die Area-ID (dargestellt als IPv4-Adresse) identifiziert die Area.

Falls diese Instanz die Backbone Area sein soll, so muss der Wert 0.0.0.0 verwendet werden.

Area-Typ

Legt den Typ der Area fest.

Mögliche Werte:

Normal (Default)

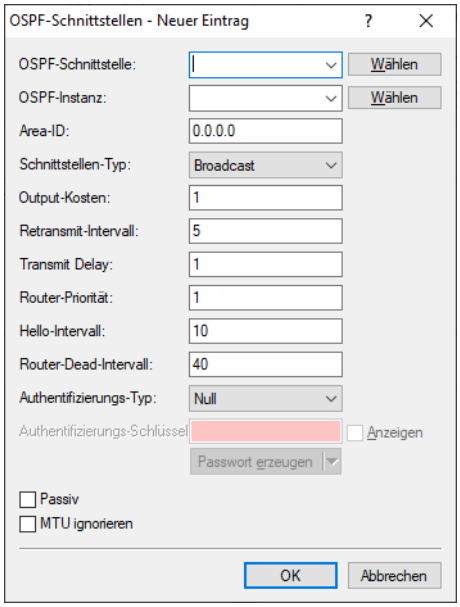
Stub

Stub-Default-Kosten

Falls die Area als Stub Area konfiguriert ist und der Router selbst Area Border Router ist, bezeichnet der Parameter **Stub-Default-Kosten** die Kosten der Default Summary-LSA, die dieser Router in dieser Area ankündigen soll.

6.24.1.3 OSPF-Schnittstellen

Definiert die Schnittstellen, auf denen OSPF verwendet werden soll.



OSPF-Schnittstelle

Enthält die Schnittstelle (IPv4-Netzwerk oder WAN-Gegenstelle), wo OSPF aktiviert werden soll.

OSPF-Instanz

Enthält den Namen der OSPF Instanz.

Area-ID

Identifiziert die Area über eine IPv4-Adresse.

Schnittstellen-Typ

Definiert den Schnittstellen-Typ.

Mögliche Werte:

Broadcast

Ethernet-basiertes Netzwerk, es wird ein Designierter Router gewählt, es wird Multicast zur Kommunikation verwendet.

Point-to-Point

Netzwerk, das nur aus zwei Routern besteht (z. B. GRE-Tunnel), oder Ethernets per P2P-Link, es wird kein Designierter Router gewählt, es wird Multicast zur Kommunikation verwendet.

Point-to-Multipoint

Netzwerk als „Hub-and-Spoke-Topologie“, es wird ein Designierter Router gewählt, es wird Multicast zur Kommunikation verwendet.

Non-Broadcast Multi-Access (NBMA)

Point-to-Multipoint-Netzwerke, die kein Broadcast bzw. Multicast unterstützen, es wird ein Designierter Router gewählt, es wird Unicast zur Kommunikation verwendet, die Nachbarn müssen manuell konfiguriert werden.

Output-Kosten

Definiert die Kosten, um ein Paket auf dieser Schnittstelle zu senden, dargestellt in der Link State Metrik. Die Ankündigung erfolgt als als Link-Kosten für diese Schnittstelle in den LSA-Nachrichten des Routers.

Der Wert muss immer größer als Null sein.

Retransmit-Intervall

Enthält die Anzahl an Sekunden zwischen LSA-Wiederholungen (Retransmissions).

Transmit Delay

Enthält die geschätzte Anzahl an Sekunden, die benötigt wird, um ein Link-State-Update-Paket über diese Schnittstelle zu übertragen.

Router-Priorität

Definiert die Priorität dieses Routers auf dieser Schnittstelle bei der Wahl zum Designierten Router (DR). Der Router mit der höchsten Priorität wird Designierter Router (Designated Router).

Der Wert 0 verhindert, dass der Router Designierter Router auf dieser Schnittstelle wird.

Hello-Intervall

Enthält das Intervall in Sekunden, in dem dieser Router auf der Schnittstelle Hello-Nachrichten versendet.

Router-Dead-Intervall

Legt die verstrichene Zeit, nach der ein Router als nicht mehr verfügbar gilt, seitdem seine Nachbarn zuletzt Hello-Nachrichten von ihm empfangen haben, in Sekunden fest.

Dieser Wert muss größer als das Hello-Intervall sein.

Authentifizierungs-Typ

Enthält die Authentifizierungsmethode, die für diese Schnittstelle verwendet werden soll.

Mögliche Werte:

Null

Einfaches Passwort

Kryptographisch-MD5

Authentifizierungs-Schlüssel

Enthält den Authentifizierungsschlüssel für dieses Netzwerk.

Hierzu darf nicht der Authentifizierungs-Typ **Null** gewählt worden sein.

Passiv

Definiert, ob OSPF aktiv oder passiv auf dieser Schnittstelle arbeiten soll.

Mögliche Werte:

Ja

Es werden keine Routing-Updates sowie Hello-Nachrichten von diesem Router auf diesem Interface versendet. Ebenso werden keine eingehenden OSPF-Nachrichten verarbeitet. Die entsprechende Route bzw. Netzwerk dieser Schnittstelle wird aber weiterhin in die LSDB eingefügt und damit auf anderen Schnittstellen angekündigt.

Nein (Default)

MTU ignorieren

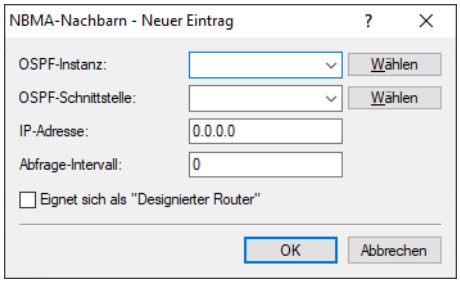
Deaktiviert die Überprüfung des MTU-Werts in Database Description Paketen.

Dies ermöglicht, dass Router eine vollständige Nachbarschaftsbeziehung etablieren können, obwohl die MTU der entsprechenden Schnittstellen nicht einheitlich ist.

6.24.1.4 NBMA-Nachbarn

Non-Broadcast-Multiaccess-Netzwerke sind Netzwerke, in denen mehrere Router vorhanden sind, aber kein Broadcast unterstützt wird. OSPF emuliert in diesem Netzwerktyp den Betrieb in einem Broadcast-Netzwerk. Hierzu wird zuvor ein Designierter Router gewählt.

Die Kommunikation findet nicht per Multicast statt, sondern per Unicast. Nachbarschaftsbeziehungen müssen manuell konfiguriert werden, da sich die Router nicht automatisch per Multicast finden können.



OSPF-Instanz

Enthält den Namen der OSPF-Instanz.

OSPF-Schnittstelle

Enthält die Schnittstelle (IPv4-Netzwerk oder WAN-Gegenstelle), wo OSPF aktiviert werden soll.

IP-Adresse

Enthält IPv4-Adresse des Nachbar-Routers (Router auf der Gegenseite).

Abfrage-Intervall

Enthält das Intervall, in dem Hello-Nachrichten zu diesem Router gesendet werden.

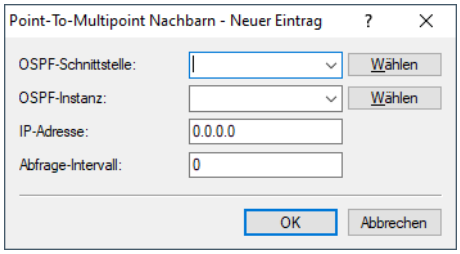
Der Wert Null deaktiviert das Senden von Hello-Nachrichten.

Eignet sich als "Designierter Router"

Definiert, ob das lokale Gerät selbst als Designierter Router wählbar ist.

6.24.1.5 Point-To-Multipoint Nachbarn

In einem Point-To-Multipoint-Netzwerk werden alle Nachbarn so behandelt, als wären sie wie Point-To-Point-Nachbarn über ein Nicht-Broadcast-Netzwerk direkt miteinander verbunden. Es wird keine Designierter Router gewählt, und die Kommunikation erfolgt per Multicast.



OSPF-Schnittstelle

Enthält die Schnittstelle (IPv4-Netzwerk oder WAN-Gegenstelle), wo OSPF aktiviert werden soll.

OSPF-Instanz

Enthält den Namen der OSPF-Instanz.

IP-Adresse

Enthält IPv4-Adresse des Nachbar-Routers (Router auf der Gegenseite).

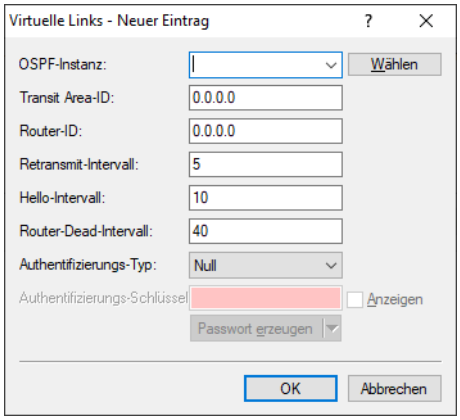
Abfrage-Intervall

Enthält das Intervall, in dem Hello-Nachrichten zu diesem Router gesendet werden.

Der Wert Null deaktiviert das Senden von Hello-Nachrichten.

6.24.1.6 Virtuelle Links

In dieser Tabelle können Virtuellen Links (auch bezeichnet als Transit-Area) definiert werden. Grundsätzlich müssen bei OSPF alle Areas direkt mit der Backbone-Area verbunden sein. In Fällen, wo dies nicht möglich ist, können virtuelle Links verwendet werden. Ein virtueller Link verbindet einen Router durch eine nicht-Backbone-Area mit der Backbone-Area.



OSPF-Instanz

Enthält den Namen der OSPF-Instanz.

Transit Area-ID

Enthält die Area-ID der Transit-Area, definiert als IPv4-Adresse.

Router-ID

Enthält die Router-ID des Routers auf der Gegenseite des virtuellen Links als IPv4-Adresse.

Retransmit-Intervall

Enthält die Anzahl an Sekunden zwischen LSA-Wiederholungen (Retransmissions).

Hello-Intervall

Definiert das Intervall in Sekunden, in dem dieser Router auf der Schnittstelle Hello-Nachrichten versendet.

Router-Dead-Intervall

Legt die verstrichene Zeit, nach der ein Router als nicht mehr verfügbar gilt, seitdem seine Nachbarn zuletzt Hello-Nachrichten von ihm empfangen haben, in Sekunden fest.

Dieser Wert muss größer als das Hello-Intervall sein.

Authentifizierungs-Typ

Enthält die Authentifizierungsmethode, die für diese Schnittstelle verwendet werden soll.

Mögliche Werte:

Null

Einfaches Passwort

Kryptographisch-MD5

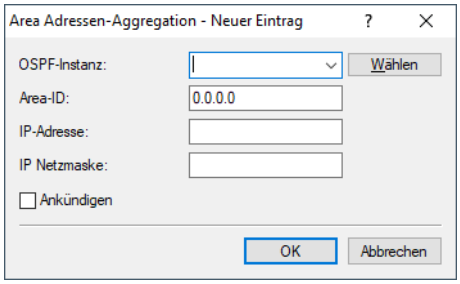
Authentifizierungs-Schlüssel

Enthält den Authentifizierungsschlüssel für dieses Netzwerk.

Hierzu darf nicht der Authentifizierungs-Typ **Null** gewählt worden sein.

6.24.1.7 Area Addressen-Aggregation

Um die Anzahl der Einträge in den Routing-Tabellen zu reduzieren, können durch Adressen-Aggregation an Area-Grenzen, beim Übergang von einer Nicht-Backbone-Area zur Backbone-Area, IP-Adressen zusammengefasst werden. Das entsprechende Subnetz wird als Summary-LSA angekündigt.



OSPF-Instanz

Enthält den Namen der OSPF-Instanz.

Area-ID

Identifiziert die Area über eine IPv4-Adresse.

Falls diese Instanz die Backbone Area sein soll, so muss der Wert 0.0.0.0 verwendet werden.

IP-Adresse

Enthält die IPv4-Adresse.

IP Netzmaske

Enthält die IPv4-Subnetzmaske.

Ankündigen

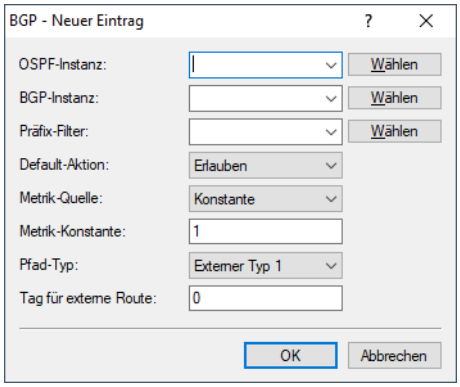
Aktiviert bzw. deaktiviert das Ankündigen dieser Adressen-Aggregation.

6.24.1.8 Route-Redistribution

Durch Routen-Redistribution können Routen von anderen Routen-Quellen bzw. Protokollen nach OSPF weiterverteilt werden. Hierzu werden die Routen mit entsprechendem Typ aus der Routing-Tabelle ausgelesen und durch OSPF weiterverteilt.

6.24.1.9 BGP

Das Weiterverteilen von dynamisch gelernte Routen aus dem Border Gateway Protocol konfigurieren Sie unter **BGP**.



OSPF-Instanz

Enthält den Namen der OSPF-Instanz.

BGP-Instanz

Enthält den Namen der BGP-Instanz.

Präfix-Filter

Name der Präfix-Filterliste aus *Präfix-Listen* auf Seite 378.

Default-Aktion

Definiert, wie Präfixe standardmäßig behandelt werden sollen, die in der Präfix-Liste konfiguriert sind. Mögliche Werte:

Erlauben

Verweigern

Metrik-Quelle

Definiert, welche Quelle zum Setzen der OSPF-Metrik verwendet wird.

Mögliche Werte:

Konstante

Es wird eine benutzerdefinierte konstante Metrik verwendet.

Protokoll

Es wird der Wert "Lokale Präferenz" des BGP-Präfix verwendet bzw. importiert.

Metrik-Konstante

Falls als Metrik-Quelle "Konstante" konfiguriert ist, wird der Wert Metrik-Konstante für die OSPF-Metrik der importierten Routen verwendet.

Pfad-Typ

Definiert, als welcher Typ die Routen in OSPF importiert werden.

Mögliche Werte:

Externer Typ 1

Die OSPF-Metrik wird gebildet aus der Redistribution-Metrik bzw. Metrik-Konstanten + Total Path Metrik, um diesen ASBR zu erreichen.

Im OSPF-Routing-Algorithmus von Routern werden Typ 1 Routen vor Typ 2 Routen grundsätzlich bevorzugt.

Externer Typ 2

Die OSPF-Metrik wird gebildet aus der Redistribution-Metrik bzw. Metrik-Konstanten.

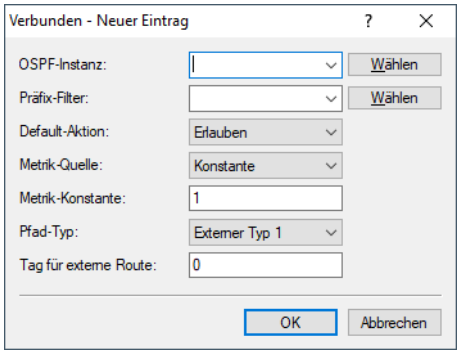
Tag für externe Route

Definiert, mit welchem External-Route-Tag die Routen importiert werden.

Der Wert wird von OSPF selbst nicht ausgewertet.

6.24.1.10 Verbunden

Das Weiterverteilen von Routen, die vom Betriebssystem automatisch in die Routing-Tabelle eingetragen werden, konfigurieren Sie unter **Verbunden**.



OSPF-Instanz

Enthält den Namen der OSPF-Instanz.

Präfix-Filter

Name der Präfix-Filterliste aus *Präfix-Listen* auf Seite 378.

Default-Aktion

Definiert, wie Präfixe standardmäßig behandelt werden sollen, die in der Präfix-Liste konfiguriert sind. Mögliche Werte:

Erlauben

Verweigern

Metrik-Quelle

Definiert, welche Quelle zum Setzen der OSPF-Metrik verwendet wird.

Mögliche Werte:

Konstante

Es wird eine benutzerdefinierte konstante Metrik verwendet.

Protokoll

Der Wert wird automatisch gesetzt.

Metrik-Konstante

Falls als Metrik-Quelle "Konstante" konfiguriert ist, wird der Wert Metrik-Konstante für die OSPF-Metrik der importierten Routen verwendet.

Pfad-Typ

Definiert, als welcher Typ die Routen in OSPF importiert werden.

Mögliche Werte:

Externer Typ 1

Die OSPF-Metrik wird gebildet aus der Redistribution-Metrik bzw. Metrik-Konstanten + Total Path Metrik, um diesen ASBR zu erreichen.

Im OSPF-Routing-Algorithmus von Routern werden Typ 1 Routen vor Typ 2 Routen grundsätzlich bevorzugt.

Externer Typ 2

Die OSPF-Metrik wird gebildet aus der Redistribution-Metrik bzw. Metrik-Konstanten.

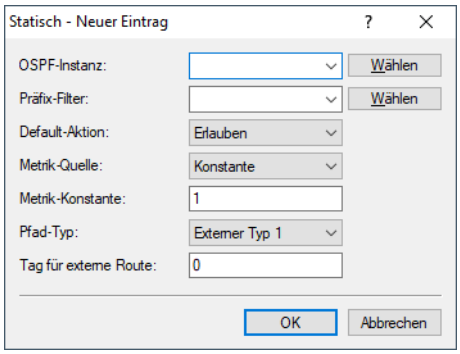
Tag für externe Route

Definiert, mit welchem External-Route-Tag die Routen importiert werden.

Der Wert wird von OSPF selbst nicht ausgewertet.

6.24.1.11 Statisch

Das Weiterverteilen statischer Routen, d. h. Routen, die manuell vom Benutzer in die Routing-Tabelle eingetragen werden, konfigurieren Sie unter **Statisch**.



OSPF-Instanz

Enthält den Namen der OSPF-Instanz.

Präfix-Filter

Name der Präfix-Filterliste aus *Präfix-Listen* auf Seite 378.

Default-Aktion

Definiert, wie Präfixe standardmäßig behandelt werden sollen, die in der Präfix-Liste konfiguriert sind. Mögliche Werte:

Erlauben

Verweigern

Metrik-Quelle

Definiert, welche Quelle zum Setzen der OSPF-Metrik verwendet wird.

Mögliche Werte:

Konstante

Es wird eine benutzerdefinierte konstante Metrik verwendet.

Protokoll

Der Wert wird automatisch gesetzt.

Metrik-Konstante

Falls als Metrik-Quelle "Konstante" konfiguriert ist, wird der Wert Metrik-Konstante für die OSPF-Metrik der importierten Routen verwendet.

Pfad-Typ

Definiert, als welcher Typ die Routen in OSPF importiert werden.

Mögliche Werte:

Externer Typ 1

Die OSPF-Metrik wird gebildet aus der Redistribution-Metrik bzw. Metrik-Konstanten + Total Path Metrik, um diesen ASBR zu erreichen.

Im OSPF-Routing-Algorithmus von Routern werden Typ 1 Routen vor Typ 2 Routen grundsätzlich bevorzugt.

Externer Typ 2

Die OSPF-Metrik wird gebildet aus der Redistribution-Metrik bzw. Metrik-Konstanten.

Tag für externe Route

Definiert, mit welchem External-Route-Tag die Routen importiert werden.

Der Wert wird von OSPF selbst nicht ausgewertet.

6.24.2 Show-Commands über CLI

Ihnen stehen folgende Show-Kommandos zur Verfügung:

- **show ospf-config**

  Zeigt eine Zusammenfassung der konfigurierten OSPF-Instanzen an.

- **show ospf-database**

  Zeigt die OSPF-Datenbank an.

- **show ospf-graph**

  Zeigt die OSPF-Areas als Graphenbeschreibung im Graphviz-Format an.

- **show ospf-neighbor**

  Zeigt Informationen über OSPF-Nachbarn an.

- **show ospf-rib**

Zeigt Informationen über die OSPF Routing Information Base an.

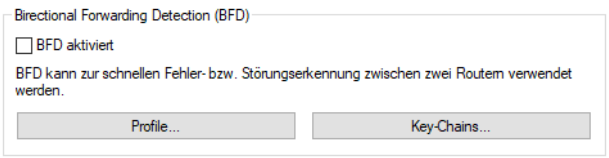
6.25 Bidirectional Forwarding Detection (BFD)

Bidirectional Forwarding Detection nach *RFC 5880* ist ein einfaches Hello-Protokoll um den Verlust einer Verbindung zwischen zwei Routern festzustellen. Hello-Pakete werden in einem definierten Intervall von beiden Routern gesendet. Werden in einem bestimmten Intervall diese Hello-Pakete nicht empfangen, so wird angenommen, dass die Verbindung unterbrochen ist. Im Zusammenspiel mit BGP bietet BFD die Möglichkeit schneller einen Verbindungsverlust zu erkennen, da die BFD-Timer deutlich kleiner gewählt werden können als die BGP-Timer.

Durch das Anpassen des Timer-Intervalls kann die Erkennung von Verbindungsverlusten schneller bzw. langsamer gesteuert werden. Je geringer das Timer-Intervall, umso schneller werden Verbindungsverluste erkannt.

- BFD unterstützt IPv4 und IPv6.
- Ein Echo-Modus wird nicht unterstützt.
- BFD ist ein Protokoll, welches deutlich System-Ressourcen verbraucht bzw. CPU-Zeit und Bandbreite benötigt. BFD wird ausschließlich in Software verarbeitet. Hardware-Verarbeitung wird für BFD nicht unterstützt.
- Wird das Hello-Intervall sehr klein gewählt, so kann es zu BFD-Flapping bzw. zur Erkennung von False-Positives kommen. Treten False-Positives auf, so wird empfohlen das Hello-Intervall zu vergrößern.
- Es wird empfohlen, dass Hello-Intervall nicht unter 250ms zu verwenden.

In LANconfig konfigurieren Sie BFD unter **Routing Protokolle** > **Allgemein** > **Bidirectional Forwarding Detection (BFD)**.

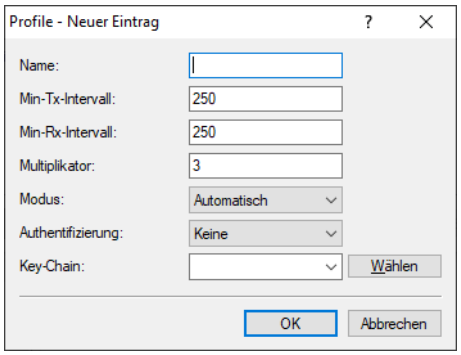


BFD aktiviert

Aktiviert bzw. Deaktiviert BFD global.

6.25.1 Profile

Zur Konfiguration der BFD-Profile wechseln Sie in die Ansicht **IP-Router** > **Allgemein** > **Bidirectional Forwarding Detection (BFD)** > **Profile**.



Name

Vergeben Sie einen aussagekräftigen Namen für dieses BFD-Profil. Der Name wird, falls BFD zusammen mit BGP verwendet werden soll, bei dem entsprechenden BGP-Nachbarn verlinkt.

Min-Tx-Intervall

Minimum Intervall in Millisekunden zwischen gesendeten BFD-Kontrollnachrichten. (Wertebereich 1-9999 Millisekunden, Default 250)

Min-Rx-Intervall

Minimum Intervall in Millisekunden zwischen empfangenen BFD-Kontrollnachrichten. (Wertebereich 1-9999 Millisekunden, Default 250)

Multiplikator

Anzahl von nicht empfangenen Paketen bis ein Interface als Down deklariert wird. Wird der Multiplikator mit dem Intervall multipliziert, so ergibt sich die Zeit, bis eine Verbindung als unterbrochen erkannt wird. (Wertebereich 1-255, Default 3)

Modus

Definiert, ob der BFD-Nachbar Single-Hop oder Multi-Hop verbunden ist. Im Single-Hop-Modus wird UDP-Zielport 3784 und Time-to-Live von 1 im IP-Header verwendet. Der Multi-Hop-Modus verwendet UDP-Port 4784. Bei Automatisch wird der Single-Hop-Modus verwendet, falls die Route zum Nachbarn vom Typ Connected LAN oder WAN ist, sonst Multi-Hop. Standardmäßig sind eBGP-Sessions Single-Hop. iBGP-Sessions können Multi-Hop sein. Mögliche Werte:

- Automatisch
- Single-Hop
- Multi-Hop

Default: Automatisch

Authentifizierung

Definiert die für BFD-Nachrichten verwendete Art der Authentifizierung. Mögliche Werte:

- Keine
- Passwort
- MD5
- MD5-Meticulous
- SHA1
- SHA1-Meticulous

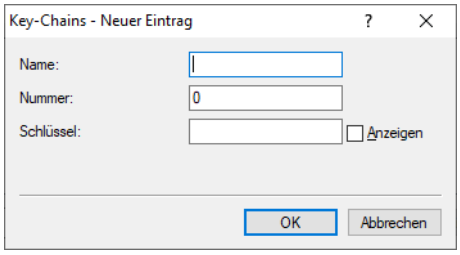
Default: Keine

Key-Chain

Name der Key-Chain aus der Tabelle *Key-Chain*. Definiert den verwendeten Schlüssel für die BFD-Nachrichten. Beim Parameter **Authentifizierung** muss ein anderer Wert außer „Keiner" konfiguriert sein.

6.25.2 Key-Chains

Zur Konfiguration der Key-Chains wechseln Sie in die Ansicht **IP-Router** > **Allgemein** > **Bidirectional Forwarding Detection (BFD)** > **Key-Chains**.



Name

Vergeben Sie einen aussagekräftigen Namen für diese Key-Chain. Über diesen wird diese Key-Chain in den *BFD-Profilen* referenziert.

Nummer

Nummer der Key-Chain.

Schlüssel

Schlüssel bzw. Passwort für diese Key-Chain.

6.25.3 Show-Kommandos über CLI

Ihnen stehen folgende Show-Kommandos zur Verfügung:

- **show BFD-v4-details**

  Zeigt Details zu den IPv4-BFD-Verbindungen an.

- **show BFD-v6-details**

  Zeigt Details zu den IPv6-BFD-Verbindungen an an.

- **show BFD-v4-status**

  Zeigt den Status der IPv4-BFD-Verbindungen an.

- **show BFD-v6-status**

  Zeigt den Status der IPv6-BFD-Verbindungen an.

6.26 BGP RPKI-RTR

Das Border Gateway Protokoll (BGP) ist grundsätzlich anfällig für sog. Route-Hijacking, d. h. das Routen von nicht-autorisierten Routern angekündigt werden können und somit Datenverkehr vom eigentlichen Ziel auf sich umlenken können. Diese Situation kann sowohl durch Fehlkonfigurationen als auch durch explizite Angriffe versursacht werden.

Resource Public Key Infrastructure (RPKI) ist ein kryptographisches Verfahren, um Routing-Datensätze, die aus Präfix und Autonomen System (AS) bestehen, zu signieren und zu validieren. Dieser Datensatz wird als Route Origin Authorization (ROA) bezeichnet. Weitere Informationen zu RPKI finden sich in *RFC 6480*.

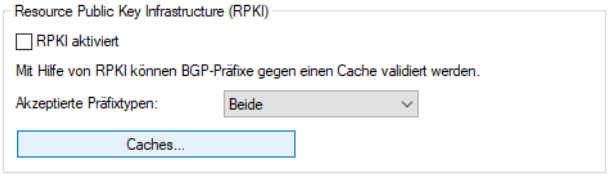
LCOS unterstützt das Resource Public Key Infrastructure to Router Protokoll (RTR) nach *RFC 8210*, mit dem der Router von einem Validator bzw. Cache Informationen über validierte Routen und zugehöriger AS-Nummer erhält. Diese Informationen werden dazu verwendet, um im BGP-Prozess zu prüfen, ob ein Präfix bzw. eine Route von dem korrekten Origin AS versendet wird. Ebenso wird geprüft, ob die Präfixlänge den Informationen aus dem ROA-Datensatz entspricht.

Dieser Cache kann entweder selbst auf einem eigenen Server für eigene Präfixe betrieben werden oder es wird ein öffentlicher Validator verwendet.

Öffentliche RPKI-Caches enthalten eine große Anzahl von ROA-Einträgen. Aufgrund des Speicherverbrauchs wird empfohlen RPKI nur auf Geräten mit genügend Hauptspeicher (mehr als 2 GB) zu verwenden wie z. B. zentralseitige Geräte oder der vRouter mit entsprechend großem Arbeitsspeicher.

6.26.1 RPKI konfigurieren

RPKI finden Sie in LANconfig unter **Routing-Protokolle** > **Allgemein** > **Resource Public Key Infrastructure (RPKI)**. Mit Hilfe von RPKI können BGP-Präfixe gegen einen Cache validiert werden. Dazu wird in der Tabelle **Treffer** des BGP-Regelwerks eine Auswahlmöglichkeit für den RPKI-Status des jeweiligen Präfixes angeboten. Siehe *Treffer* auf Seite 525.



RPKI aktiviert

Aktiviert bzw. Deaktiviert RPKI.

Akzeptierte Präfixtypen

Definiert welche ROA-Präfixtypen (IPv4 bzw. IPv6) gespeichert werden sollen. Um Arbeitsspeicher zu optimieren, wird empfohlen, den Präfixtyp auf die tatsächlich verwendete Adressfamilie (IPv4, IPv6) einzuschränken.

Mögliche Werte:

Beide

Sowohl IPv4- als auch IPv6 RPKI-Datensätze werden im Gerät gespeichert (Default).

IPv4

Nur IPv4-RPKI-Datensätze werden im Gerät gespeichert.

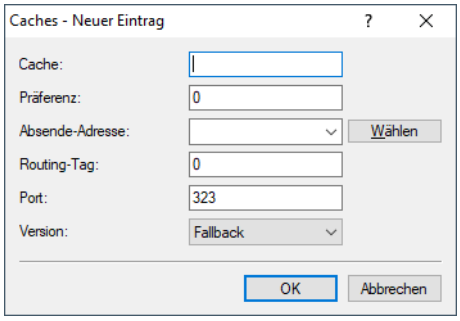
IPv6

Nur IPv6-RPKI-Datensätze werden im Gerät gespeichert

6.26.1.1 RPKI-Caches

In dieser Tabelle kann der verwendete RPKI-Validator bzw. RPKI-Cache konfiguriert werden. Als Transportprotokoll wird TCP unterstützt.

Die Einstellungen zu den RPKI-Chaches finden Sie in LANconfig unter **Routing-Protokolle** > **Allgemein** > **Resource Public Key Infrastructure (RPKI)** > **Caches**.



Cache

IPv4-, IPv6-Adresse oder Hostname unter der der RPKI-Cache erreicht wird.

Präferenz

Präferenz des Caches, falls mehrere Caches verwendet werden. Geringere Werte resultieren in einer höheren Präferenz. Default: 0

Absende-Adresse

Konfigurieren Sie optional eine Absende-Adresse, die der RPKI-Client statt der ansonsten automatisch für die Zieladresse gewählten Absende-Adresse verwendet. Falls Sie z. B. Loopback-Adressen konfiguriert haben, können Sie diese hier als Absende-Adresse angeben.

Routing-Tag

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen Cache ermittelt wird. Default: 0

Port

Port des RPKI-Caches. Default: 323

Version

Verwendete Protokollversion des PRKI-RTR-Protokolls. Mögliche Werte:

Fallback

Die Kommunikation mit dem Cache wird mit Version 1 gestartet und ggf. auf Version 0 heruntergeschaltet.

Null

Es wird Protokollversion 0 zur Kommunikation mit dem Cache verwendet.

Eins

Es wird Protokollversion 1 zur Kommunikation mit dem Cache verwendet.

6.26.2 Show-Kommandos über CLI

Ihnen stehen folgende Show-Kommandos zur Verfügung:

- **show rpki-v4-cache**

  Zeigt alle aktuell gespeicherten IPv4 ROAs an, die vom Cache empfangen wurden.

- **show rpki-v6-cache**

  Zeigt alle aktuell gespeicherten IPv6 ROAs an, die vom Cache empfangen wurden.

- **show rpki-status**

  Zeigt den aktuellen Status des RPKI-Clients an.

- **show bgp-prefix <Präfix>**

  Das Show-Kommando zeigt neben den BGP-Präfix-Informationen auch den RPKI-Status des jeweiligen Präfixes (`Not found`, `Valid`, `Invalid`, `Not available`). Folgender RPKI-Status für ein BGP-Präfix ist möglich:

  - `Not found`: Der Vaildator hat keine Informationen über dieses Präfix und das zugehörige AS zurückgeliefert. Es kann somit nicht bestimmt werden, ob der Eintrag gültig oder ungültig ist.
  - `Valid`: Der Validator hat Informationen zurückgeliefert die mit dem Präfix und AS im BGP übereinstimmen. Der Eintrag ist somit gültig.
  - `Not valid`: Der Validator hat Informationen zurückgeliefert die mit dem Präfix und AS nicht übereinstimmen. Entweder ist das Origin AS nicht korrekt oder die Präfixlänge stimmt nicht mit den Daten im Validator überein.

- `Not available`: Es liegen keine Daten zur Prüfung aus dem Vailidator vor. RPKI ist entweder nicht aktiv oder das Gerät hat noch keine Daten vom Validator abgerufen. Das Präfix ist schon im BGP vorhanden bevor Informationen aus dem Validator vorliegen.

- **show bgp-v4-rib**

  Es wurde die Spalte ROA-AS hinzugefügt, die das AS enthält, das zur RPKI-Prüfung verwendet wurde. Ebenso die Spalte ROA-Flag, die das Ergebnis des ROA-Checks enthält.

- **show bgp-v6-rib**

  Es wurde die Spalte ROA-AS hinzugefügt, die das AS enthält, das zur RPKI-Prüfung verwendet wurde. Ebenso die Spalte ROA-Flag, die das Ergebnis des ROA-Checks enthält.

6.27 Locator / ID Separation Protocol (LISP)

Das Locator / ID Separation Protocol (LISP) nach RFC 6830 ist eine neue Routing-Architektur, das eine IP-Adresse in zwei Entitäten aufspaltet: Routing Locator (RLOC) und Endpoint Identifier (EID). Das Ziel ist eine hochskalierbare Routing-Architektur mit integriertem Routing- und Tunnel- bzw. Overlay-Protokoll zu erreichen.

Klassische Routing-Protokolle wie RIP, OSPF oder BGP arbeiten nach dem „Push-Prinzip" und verteilen proaktiv ihre besten Routen an ihre Nachbarn. Die Skalierbarkeit dieser Architektur ist nur begrenzt, insbesondere stellen sehr große BGP-Tabellen bzw. Routing-Tabellen zunehmend eine Herausforderung dar.

LISP arbeitet nach dem „Pull-Prinzip" und funktioniert ähnlich wie das Domain Name System (DNS). LISP-Router registrieren ihre Netze, genannt Endpoint Identifiers (EID), bei einer zentralen Instanz, genannt Map-Server bzw. Map-Resolver. Neben dem EID registrieren sie ebenso ihre globale (WAN-) Adresse, genannt Routing Locator (RLOC). Dadurch wird eine Trennung in Ortsinformation (Locator) und Identität (ID) erreicht.

Möchte ein anderer Router Daten zu einem entfernten LISP-Netz übertragen, so wird zunächst der LISP Map-Resolver nach den Zuordnungen zwischen dem angefragten EID-Präfix und dem Routing Locator befragt. Im nächsten Schritt wird zwischen beiden LISP-Routern ein Datentunnel etabliert.

LISP bringt aktuell keine Verschlüsselung des Datentunnels mit und wird in der Regel beim Einsatz in unsicheren Netzen wie dem Internet mit VPN kombiniert. Anwendungsszenarien für LISP sind Multi-VPNs.

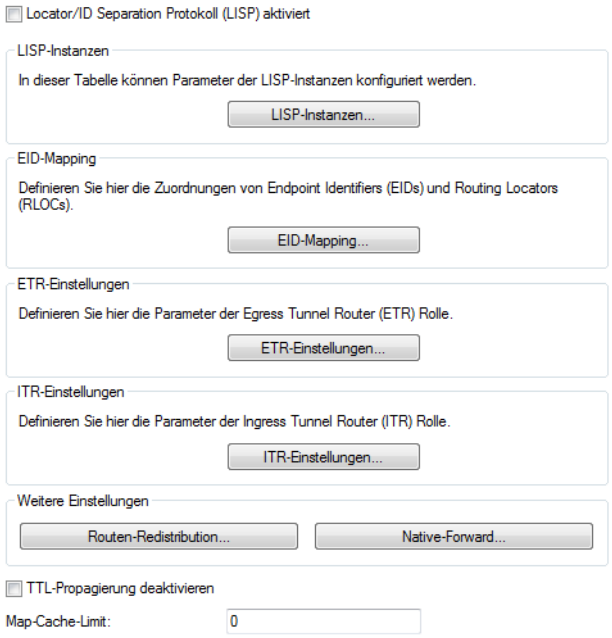
LCOS unterstützt ab Version 10.20 die folgenden Rollen:

- Ingress Tunnel Router (ITR)
- Egress Tunnel Router (ETR)

Nicht unterstützt wird aktuell die Rolle des Map-Servers bzw. des Map-Resolvers.

6.27.1 Konfiguration

Die Konfiguration des LISP-Routings finden Sie in LANconfig unter **Routing Protokolle** > **LISP**. Über den Schalter **Locator / ID Separation Protocol (LISP) aktiviert** wird dieses Routing-Protokoll ein- bzw. ausgeschaltet.



TTL-Propagierung deaktivieren

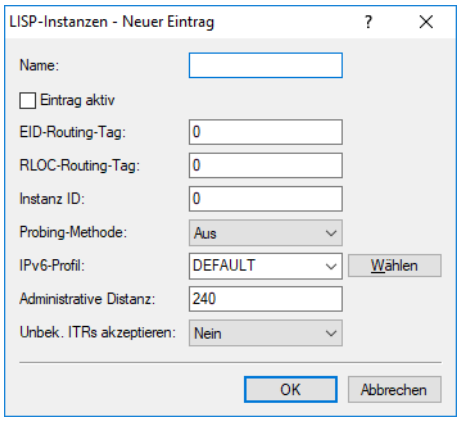
Bei Aktivierung wird vom ITR die Time-To-Live (TTL) nicht vom äußeren in den inneren Header kopiert. Dadurch erscheint für einen Client bei der Ausführung von Traceroute der LISP-Tunnel als ein Hop. Falls deaktiviert, dann werden alle Hops zwischen ITR und ETR durch Traceroute angezeigt.

Map-Cache-Limit

Definiert die maximale Anzahl von Einträgen im Map-Cache über alle LISP-Instanzen. Nach dem Erreichen des Limits werden neue Einträge abgelehnt. Erst nachdem ältere Einträge im Map-Cache ungültig geworden sind werden neue Einträge akzeptiert. Eine 0 bedeutet keine Beschränkung.

LISP-Instanzen

Diese Tabelle enthält die globale Konfiguration der LISP-Instanzen auf dem Gerät.



Name

Definiert einen eindeutigen Namen für eine LISP-Instanz. Dieser Name wird in weiteren LISP-Tabellen referenziert.

Eintrag aktiv

Aktiviert oder deaktiviert diese LISP-Instanz.

EID-Routing-Tag

Routing-Tag des Endpoint Identifiers (EID) dieser Instanz.

RLOC-Routing-Tag

Routing-Tag des Routing Locators (RLOC) dieser Instanz.

Instanz-ID

LISP Instance ID als numerischer Tag aus RFC 8060 (LISP Canonical Address Format (LCAF)) zur Segmentierung der Netze im Zusammenhang mit ARF.

Probing-Methode

Definiert die Methode mit der die Erreichbarkeit der RLOCs der Map-Cache-Einträge periodisch geprüft wird. Möglich Methoden:

- Aus: Die Erreichbarkeit der RLOCs wird nicht periodisch geprüft.
- RLOC-Probing: Die Erreichbarkeit der RLOCs wird durch LISP RLOC-Nachrichten periodisch geprüft.

IPv6-Profil

Name des IPv6-WAN-Profils aus der IPv6-WAN-Interface-Tabelle. Ein Eintrag wird zwingend benötigt, falls IPv6-EIDs verwendet werden.

Administrative Distanz

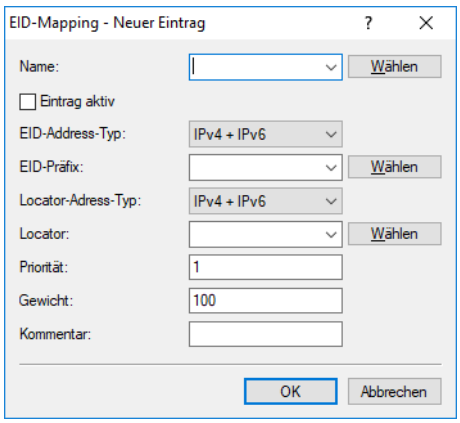
Die administrative Distanz dieser LISP-Instanz.

Unbekannte ITRs akzeptieren

Definiert, ob der Router LISP-Datenpakete von unbekannten ITRs annehmen soll, für die kein Map-Cache-Eintrag vorhanden ist. Diese Funktionalität wird insbesondere für Szenarien benötigt in denen PITR und PETR über unterschiedliche Server bzw. IP-Adressen betrieben werden.

EID-Mapping

Diese Tabelle definiert die Abbildung von EIDs auf RLOCs, die beim Map-Server registriert werden sollen.



Name

Referenziert den Namen der LISP-Instanz.

Eintrag aktiv

Aktiviert oder deaktiviert dieses EID-Mapping.

EID-Adress-Typ

Protokollversion des EID-Präfix bei Referenzierung des EID-Präfix über einen Interface- bzw. Netzwerknamen. Mögliche Werte:

- **IPv4**: Es wird nur das IPv4-Präfix des referenzierten Interfaces verwendet.
- **IPv6**: Es wird nur das IPv6-Präfix des referenzierten Interfaces verwendet.
- **IPv4+IPv6**: Es wird sowohl das IPv4-Präfix als auch das IPv6-Präfix des referenzierten Interfaces verwendet.

EID-Präfix

EID-Präfix des EID-Mappings. Mögliche Werte sind ein IPv4-Netzwerkname oder ein IPv6-Interface, z. B. INTRANET, oder eine benannte Loopbackadresse.

Locator-Adress-Typ

Protokollversion des RLOCs bei Referenzierung des EID-Präfix über einen Interface-Namen. Mögliche Werte:

- **IPv4**: Es wird nur die IPv4-Adresse als RLOC des referenzierten Interfaces verwendet.
- **IPv6**: Es wird nur die IPv6-Adresse als RLOC des referenzierten Interfaces verwendet.
- **IPv4+IPv6**: Es wird sowohl die IPv4-Adresse als auch die IPv6-Adresse als RLOC des referenzierten Interfaces verwendet.

Locator

RLOC des EID-Mappings. Mögliche Werte sind benannte Gegenstellen, IPv6-WAN-Interfaces, oder Loopback-Interfaces.

Priorität

Die Priorität des EID-Mappings. Default: 1.

Gewicht

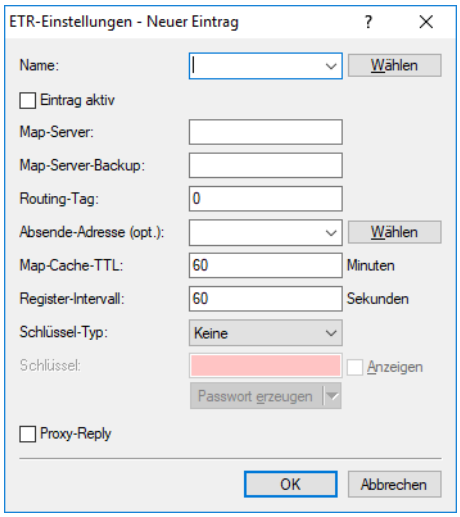
Das Gewicht des EID-Mappings. Default: 100.

Kommentar

Geben Sie eine aussagekräftige Beschreibung für diesen Eintrag an.

ETR-Einstellungen

Diese Tabelle definiert die Parameter für die Rolle als Egress Tunnel Router (ETR).



Name

Referenziert den Namen der LISP-Instanz.

Eintrag aktiv

Aktiviert oder deaktiviert diese ETR-Einstellungen.

Map-Server

IPv4- oder IPv6-Adresse des LISP Map-Servers

Map-Server-Backup

IPv4- oder IPv6-Adresse des LISP Backup-Map-Servers. Die LISP-Registrierung wird parallel sowohl an den primären Map-Server als auch an den Backup-Map-Server gesendet.

Routing-Tag

Routing-Tag, das zum Erreichen des Map-Servers verwendet werden soll.

Absende-Adresse (opt)

Enthält die Absender-Adresse als benanntes Interface, die bei LISP-Kommunikation mit dem Map-Server verwendet wird.

Map-Cache-TTL

Time-To-Live der EID-Mappings in Minuten, die beim Map-Server registriert werden.

Register-Intervall

Registrierungsintervall in Sekunden, in dem Map-Registrierungen an den Map-Server gesendet werden.

Schlüssel-Typ

Verwendeter Algorithmus für die Authentifizierung am Map-Server. Mögliche Werte:

- Keine
- HMAC-SHA-1-96
- HMAC-SHA-256-128

Schlüssel

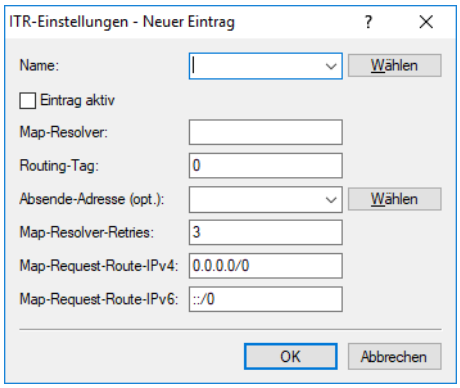
Schlüssel bzw. Passwort, mit dem die Registrierung des EID-Mappings am Map-Server erfolgt.

Proxy-Reply

Definiert, ob das Proxy-Reply-Bit in Map-Registrierungen gesetzt wird. In diesem Fall agiert der Map-Server als Proxy und antwortet stellvertretend für den ETR bei Map-Requests.

ITR-Einstellungen

Diese Tabelle definiert die Parameter für die Rolle als Ingress Tunnel Router (ITR).



Name

Referenziert den Namen der LISP-Instanz.

Eintrag aktiv

Aktiviert oder deaktiviert diese ITR-Einstellungen.

Map-Resolver

IPv4- oder IPv6-Adresse des LISP Map-Resolvers.

Routing-Tag

Routing-Tag, das zum Erreichen des Map-Resolvers verwendet wird.

Absende-Adresse (opt)

Enthält die Absender-Adresse als benanntes Interfaces, die bei LISP-Kommunikation mit dem Map-Resolver verwendet wird.

Map-Resolver-Retries

Anzahl der Wiederholungen bei Map-Anfragen an den Map-Resolver. Default: 3

Map-Request-Route-IPv4

Definiert die IPv4-Route bzw. das Präfix für die LISP-Map-Requests durchgeführt werden sollen.

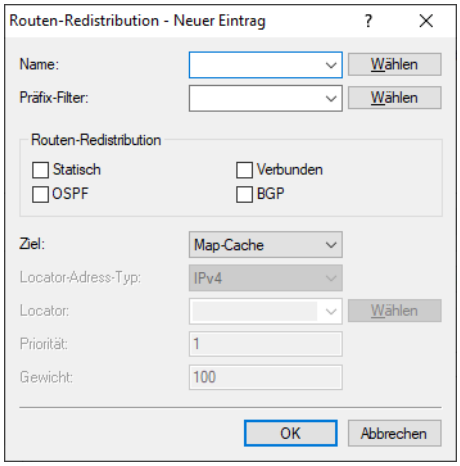
Map-Request-Route-IPv6

Definiert die IPv6-Route bzw. das Präfix für die LISP-Map-Requests durchgeführt werden sollen.

Routen-Redistribution

Durch Routen-Redistribution können Routen aus der Routing-Tabelle in den LISP-Map-Cache importiert werden. Für diese Routen werden entsprechende Map-Requests durchgeführt.

Ebenso können durch Routen-Redistribution Routen aus der Routing-Tabelle importiert werden und dynamisch als EID-Präfix beim Map-Server registriert werden.



Name

Referenziert den Namen der LISP-Instanz.

Präfix-Filter

Name der Präfix-Filterliste aus *Präfix-Listen* auf Seite 378. Für die Präfixe aus dieser Liste wird die Routen-Redistribution erlaubt.

Routen weiter verteilen

Definiert die Routenquellen der importierten Routen.

- **Statisch**: Das Gerät importiert statische Routen aus der Routing-Tabelle in den LISP-Map-Cache oder in die EID-Tabelle als EID-Präfix.
- **Verbunden**: Das Gerät importiert von direkt angeschlossenen Netzwerken aus der Routing-Tabelle in den LISP-Map-Cache oder in die EID-Tabelle als EID-Präfix.
- **OSPF**: Das Gerät importiert OSPF-Routen aus der Routing-Tabelle in den LISP-Map-Cache oder in die EID-Tabelle als EID-Präfix.
- **BGP**: Das Gerät importiert BGP-Routen aus der Routing-Tabelle in den LISP-Map-Cache oder in die EID-Tabelle als EID-Präfix.

Ziel

Definiert das Ziel der nach LISP importierten Routen. Mögliche Werte:

- **Map-Cache**: Importiert die Routen in den Map-Cache. Für diese Routen führt LISP Map-Requests aus.
- **EID-Tabelle**: Import die Routen in die LISP-EID-Tabelle. Diese Routen werden beim Map-Server als EID-Präfix mit dem konfigurierten RLOC registriert.

Locator-Adress-Typ

Protokollversion des RLOCs bei Referenzierung des EID-Präfix über einen Interface-Namen. Mögliche Werte:

- **IPv4**: Es wird nur die IPv4-Adresse als RLOC des referenzierten Interfaces verwendet.
- **IPv6**: Es wird nur die IPv6-Adresse als RLOC des referenzierten Interfaces verwendet.
- **IPv4+IPv6**: Es wird sowohl die IPv4-Adresse als auch die IPv6-Adresse als RLOC des referenzierten Interfaces verwendet.

Locator

Definiert den RLOC mit dem die importierten EID-Präfixe beim Map-Server registriert werden. Mögliche Werte sind benannte Gegenstellen, IPv6-WAN-Interfaces, oder Loopback-Interfaces.

Priorität

Die Priorität. Default: 1

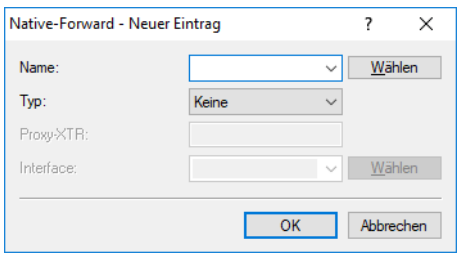
Gewicht

Das Gewicht. Default: 100

Native-Forward

Sollen LISP-Netzwerke mit Nicht-LISP-Netzwerken kommunizieren, dann können Proxy-Router verwendet werden. Diese Rollen werden als Proxy Ingress Tunnel Router (Proxy-ITR) und Proxy Egress Tunnel Router (Proxy-ETR) bezeichnet.

Erhält ein LISP-Router vom Map-Resolver eine negative Antwort, d. h. es liegt keine Abbildung zwischen angefragten EID zu einem RLOC vor, so kann der LISP-Router die zugehörigen Pakete entweder an einen Proxy xTR senden (Paket mit LISP-Header) oder über ein anderes lokales Interface versenden (Paket ohne LISP-Header).



Name

Referenziert den Namen der LISP-Instanz.

Typ

Definiert, auf welchem Weg Pakete zu Nicht-LISP-Netzwerken gesendet werden sollen.

- **Keine**: Pakete zu Nicht-LISP-Netzwerken werden nicht weitergeleitet und verworfen
- **Proxy xTR**: Pakete zu Nicht-LISP-Netzwerken werden an einen Proxy xTR gesendet
- **Interface**: Pakete zu Nicht-LISP-Netzwerken werden über ein lokales Interface gesendet

Proxy xTR

IPv4- oder IPv6-Adresse des Proxy xTRs über den Pakete zu Nicht-LISP-Netzwerken gesendet werden.

Interface

Name des Interfaces über das Pakete zu Nicht-LISP-Netzwerken gesendet werden.

6.27.2 LISP-Tutorial

In diesem Tutorial soll das ARF-Netzwerk mit Namen INTRANET und Tag 1 als LISP-Netzwerk konfiguriert werden. Dazu wird das Netzwerk mit seinem Präfix als EID-Präfix beim MAP-Server 1.1.1.1 registriert. Die Registrierung erfolgt über die WAN-Gegenstelle INTERNET (Default-Route) mit Tag 0. Die IP-Adresse auf der Gegenstelle INTERNET kann dabei dynamisch oder statisch sein. Diese Adresse wird als RLOC-Adresse beim MAP-Server registriert.

Daten aus dem INTRANET sollen in den LISP-Tunnel geschickt werden. Dazu stellt der Router für alle unbekannten Ziele einen Map-Request an den MAP-Resolver 1.1.1.1.

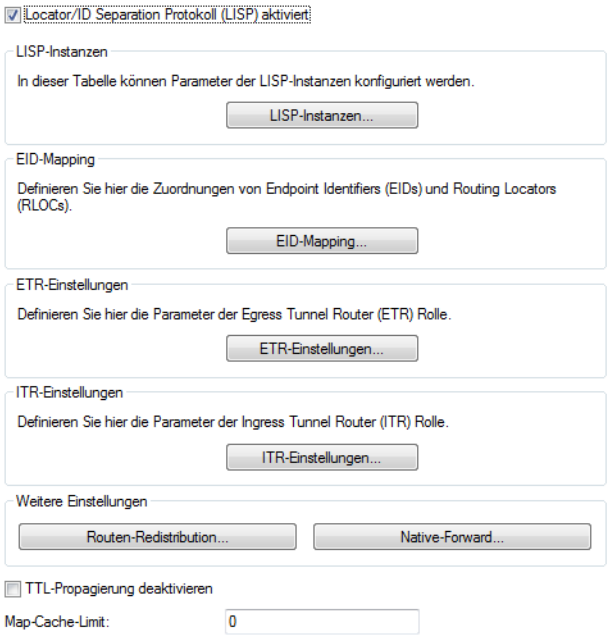
Liefert der Map-Resolver ein positives Mapping, so baut LISP automatisch einen dynamischen Tunnel zum entfernten LISP-Router auf und trägt entsprechende Routen in die Routing-Tabelle ein.

Liefert der Map-Resolver ein negatives Mapping, d. h. das Ziel-Präfix ist unbekannt bzw. auf dem Map-Server / Resolver nicht registriert, so kann das Paket optional ohne Tunnel direkt über die Gegenstelle INTERNET versendet werden (Native Forward).

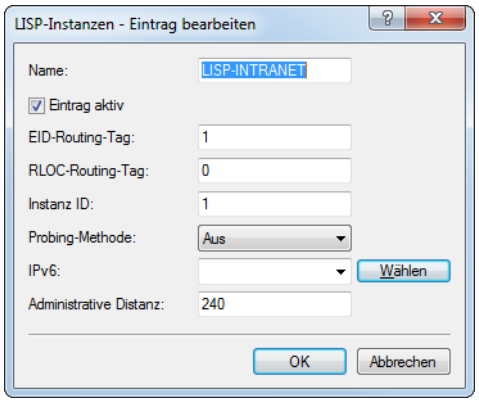
Eine manuelle Konfiguration von LISP-Routen ist nicht erforderlich. Diese werden von LISP automatisch angelegt und wieder entfernt.

Es müssen grundsätzlich immer manuell Einträge für die jeweiligen Routing-Tags in der WAN-Tag-Tabelle angelegt werden.

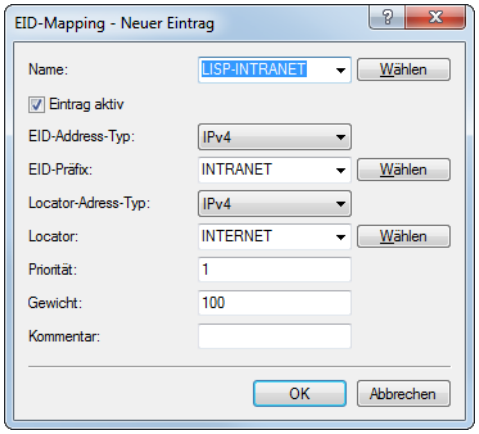
1. Aktivieren Sie als erstes das LISP-Protokoll unter **Routing Protokolle** > **LISP** > **Locator/ID Separation-Protokoll (LISP) aktiviert**.



2. Legen Sie einen neuen Eintrag in der Tabelle der LISP-Instanzen an. Gehen Sie dazu nach **Routing Protokolle** > **LISP** > **LISP-Instanzen** und klicken auf **Hinzufügen**.
   a) Geben Sie dieser LISP-Instanz einen **Namen**, z. B. LISP-INTRANET.
   b) Setzen Sie den **Eintrag aktiv**.
   c) Setzen Sie das **EID-Routing-Tag** auf 1.
   d) Setzen Sie das **RLOC-Routing-Tag** auf den Wert des Tags der WAN-Gegenstelle INTERNET, hier also 0.
   e) Setzen Sie die **Instanz ID** auf den im LISP-Map-Server angelegten Wert, hier also 1 wie das Tag des INTRANET.
   f) Nehmen Sie bei **IPv6** den Eintrag **DEFAULT** weg, da wir hier nur IPv4 betrachten.

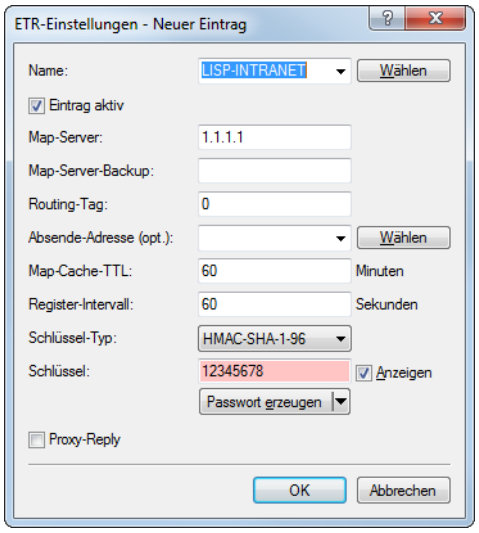


3. Legen Sie einen neuen Eintrag in der Tabelle EID-Mapping an, über den die Vreknüpfung des EID-Präfixes und des Locators erfolgen. Gehen Sie dazu nach **Routing Protokolle** > **LISP** > **EID-Mapping** und klicken auf **Hinzufügen**.
   a) Wählen Sie als **Name** den der zuvor angelegten LISP-Instanz, hier LISP-INTRANET.
   b) Setzen Sie den **Eintrag aktiv**.
   c) Setzen Sie sowohl den **EID-Adress-Typ** als auch den **Locator-Adress-Typ** auf IPv4.
   d) Wählen Sie als **EID-Präfix** INTRANET.
   e) Wählen Sie als **Locator** INTERNET.

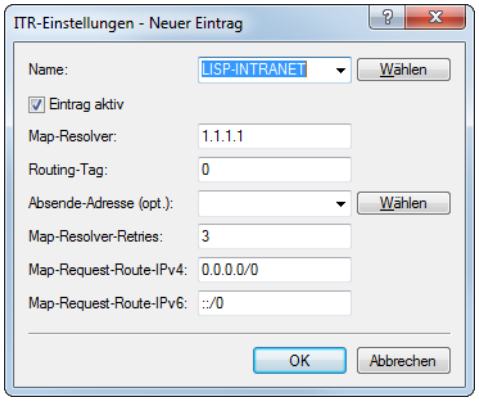


4. Legen Sie einen neuen Eintrag mit den Parametern zur Kommunikation mit dem Map-Server in der Tabelle ETR-Einstellungen an. Gehen Sie dazu nach **Routing Protokolle** > **LISP** > **ETR-Einstellungen** und klicken auf **Hinzufügen**.
   a) Wählen Sie als **Name** den der zuvor angelegten LISP-Instanz, hier LISP-INTRANET.
   b) Setzen Sie den **Eintrag aktiv**.
   c) Setzen Sie den **Map-Server** auf 1.1.1.1.
   d) Setzen Sie das **Routing-Tag** auf 0.

e) Setzen Sie den **Schlüssel-Typ** und **Schlüssel** für die Verbindung mit dem Map-Server. Diese müssen mit dem auf Map-Server konfigurierten Typ und Passwort übereinstimmen. In diesem Beispiel nehmen wir HMAC-SHA-1-96 und 12345678.

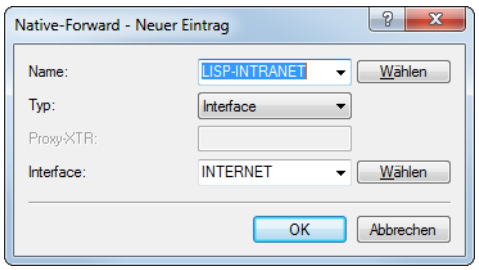


5. Legen Sie einen neuen Eintrag mit den Parametern zur Kommunikation mit dem Map-Resolver in der Tabelle ITR-Einstellungen an. Gehen Sie dazu nach **Routing Protokolle** > **LISP** > **ITR-Einstellungen** und klicken auf **Hinzufügen**.
   a) Wählen Sie als **Name** den der zuvor angelegten LISP-Instanz, hier LISP-INTRANET.
   b) Setzen Sie den **Eintrag aktiv**.
   c) Setzen Sie den **Map-Resolver** auf 1.1.1.1.
   d) Setzen Sie das **Routing-Tag** auf 0.



6. Optional: Pakete an Zieladressen, die keine LISP-Netze sind, können direkt über ein lokales Interfrace, also ohne Verwendung des LISP-Tunnels, versendet werden. In unserem Beispiel wird hierzu das Interface INTERNET verwendet. Legen Sie einen neuen Eintrag in der Tabelle Native-Forward an. Gehen Sie dazu nach **Routing Protokolle** > **LISP** > **Native-Forward** und klicken auf **Hinzufügen**.
   a) Wählen Sie als **Name** den der zuvor angelegten LISP-Instanz, hier LISP-INTRANET.
   b) Setzen Sie den **Typ** auf **Interface**.

c) Wählen Sie als **Interface** INTERNET.



7. Legen Sie unter **Kommunikation** > **Gegenstellen** > **WAN-Tag-Tabelle** mit einem Klick auf **Hinzufügen** einen Eintrag für die gerade erstellte LISP-Instanz mit der Instanz-ID 1 an.

   Für jede LISP-Instanz muss in der WAN-Tag-Tabelle ein Eintrag mit dem zugehörigen Schnittstellen-Tag für EID / ARF-Netz angelegt werden.

   Dazu muss ein Eintrag angelegt werden, wobei der Gegenstellenname LISP-<LISP-Instanz-ID>* lautet. Der Gegenstellename wird gebildet aus dem Schlüsselwort LISP, ergänzt um die entsprechende LISP-Instanz-ID (in Hexadezimal-Form) sowie um die Wildcard *. Dies dient der eindeutigen Zuordnung des ankommenden Datenverkehrs der LISP-Tunnel zu EID / ARF-Netzwerk.

   Die Instanz-ID muss Hexadezimal ohne führendes 0x angegeben werden.

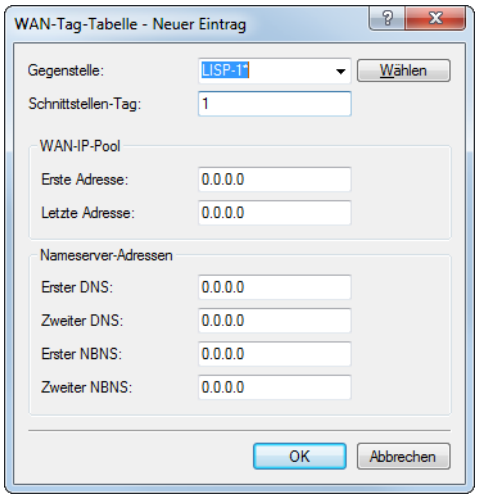
   Darstellung: LISP-<LISP-Instanz-ID>*

   Beispiele:

   - für die LISP-Instanz 1: LISP-1*
   - für die LISP-Instanz 15: LISP-F*

   a) Geben Sie in das Feld **Gegenstelle** nach dem gerade beschriebenen Muster für die LISP-Instanz mit der Instanz-ID 1 den Wert „LISP-1*“ ein.

   b) Als **Schnittstellen-Tag** geben Sie die 1 ein.



Fertig!

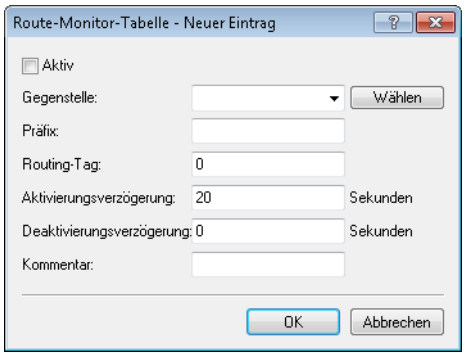
6.28 Route-Monitor

Der Route-Monitor überwacht Verbindungen zu Netzwerken verschiedener Provider und stellt im Fehlerfall eine Backup-Verbindung her. Die Überwachung geschieht über ein Trigger-Präfix, das der Provider in seinem Routing-Protokoll zur Verfügung stellt, z. B. beim Border Gateway Protokoll (BGP). Sobald die Route zu einem Provider-Netzwerk unerreichbar ist, erklärt der Route-Monitor das entsprechende Trigger-Präfix im eigenen Netzwerk für ungültig und öffnet eine Backup-Verbindung zum Provider-Netzwerk.

6.28.1 Route-Monitor mit LANconfig konfigurieren

Um den Route-Monitor zu aktivieren, wechseln Sie in die Ansicht **Kommunikation** > **Backup** und markieren Sie die Option **Route-Monitor aktiviert**.

Um den Route-Monitor zu konfigurieren, öffnen Sie die **Route-Monitor-Tabelle**.



Aktiv

Gibt an, ob diese Backup-Verbindung aktiv ist.

Gegenstelle

Enthält den Namen der Backup-Gegenstelle.

Präfix

Enthält das Präfix (IPv4- oder IPv6-Adresse), das der Route-Monitor überwachen soll.

Routing-Tag

Enthält das Routing-Tag des zu überwachenden Präfixes.

Aktivierungsverzögerung

Enthält die Verzögerung in Sekunden, die das Gerät nach dem Ausbleiben des Präfixes wartet, bis es die Verbindung zur Backup-Gegenstelle aufbaut.

Deaktivierungsverzögerung

Definiert die Verzögerung in Sekunden, die das Gerät nach dem Auftauchen des Präfixes wartet, bis es die Verbindung zur Backup-Gegenstelle wieder abbaut.

Beim Wert „0" beendet das Gerät die Verbindung zur Backup-Gegenstelle sofort beim Auftauchen des Präfixes (keine Verzögerung).

Kommentar

Kommentar zu diesem Eintrag.

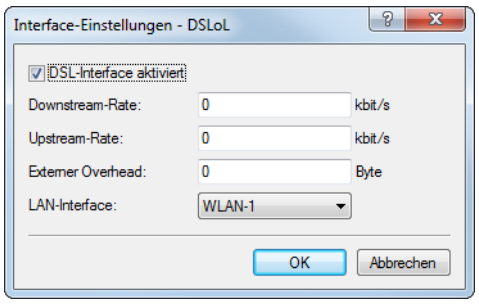
6.29 DSLoL für WLAN-Router

Eine IPv4-Maskierung („NAT“) ist nur über eine WAN-Verbindung möglich. Wenn man in Richtung eines LAN- oder WLAN-Interface maskieren will, dann muss das entsprechende LAN- oder WLAN-Interface als DSL-Port deklariert werden, so dass dieser für den Aufbau einer WAN-Verbindung (typischerweise IPoE oder DHCPoE) verwendet werden kann.

Dies war bis LCOS 10.12 nur für Access Points möglich. Ab LCOS 10.20 ist DSLoL auch für WLAN-Router verfügbar.

Ein exemplarisches Szenario für DSLoL:

Ein WLAN-Router soll verwendet werden, um eine Internetverbindung primär über WLAN herzustellen. Dazu wird der WLAN-Clientmodus verwendet. Ist das WLAN nicht verfügbar, soll stattdessen als Backup die Internetverbindung über LTE hergestellt werden. Hierzu wird ganz regulär eine LTE-Verbindung konfiguriert; sowie unter Zuhilfenahme von DSLoL über das WLAN-Interface eine weitere Internetverbindung über WLAN. Dazu in LANconfig unter **Schnittstellen** > **WAN** > **Interface-Einstellungen** > **DSLoL** die Option **DSL-Interface aktiviert** auswählen und diesem Interface das vorher als WLAN-Client eingerichtete WLAN als **LAN-Interface** zuweisen.



Nun kann die LTE-Verbindung als Backup für die WLAN / DSLoL-Internetverbindung konfiguriert werden.

7 IPv6

7.1 IPv6-Grundlagen

IPv4 (Internet Protocol Version 4) ist ein Protokoll zur eindeutigen Adressierung von Teilnehmern in einem Netzwerk und definierte bislang alle weltweit vergebenen IP-Adressen. Da der so gebotene Adressraum Grenzen hat, tritt das IPv6 (Internet Protocol Version 6) in die Fußstapfen des bisherigen Standards. IPv6 bietet durch einen anderen IP-Adressaufbau ein breiteres Spektrum für IP-Adressen und vergrößert somit die möglich Anzahl an Teilnehmern in Netzwerken weltweit.

7.1.1 Warum IP-Adressen nach dem Standard IPv6?

Folgende Gründe führten zur einer Entwicklung des neuen IPv6-Standards:

- IPv4 deckt einen Adressraum von etwa vier Milliarden IP-Adressen ab, mit denen Teilnehmer in Netzwerken eindeutige Identitäten erhalten. Bei der Implementierung des IPv4-Standards in den 1980er-Jahren galt dieser Adressraum als überaus ausreichend. Durch das enorme Wachstum des World Wide Web und der unvorhergesehenen Vielzahl an Rechnern und kommunizierenden Geräten entsteht eine Adressknappheit, die der IPv6-Standard beheben soll.
- Der größere Adressraum des IPv6 erschwert das Scannen von IP-Adressen durch Viren und Trojaner. Auf diese Weise bietet das breitere Spektrum einen größeren Schutz vor Angriffen.
- IPv6 wurde nach sicherheitstechnischen Anforderungen implementiert. So enthält es das Sicherheitsprotokoll IPSec (IP Security). Dieses sorgt für eine sichere Kommunikation im Netzwerk auf dem 3. Layer, während viele Sicherheitsmechanismen des IPv4 erst auf höheren Ebenen greifen.
- Durch einfachere und feste Bezeichnungen der Datenpakete sparen Router Rechenleistung und beschleunigen somit ihren Datendurchsatz.
- IPv6 ermöglicht eine einfachere und schnellere Übertragung von Daten in Echtzeit und eignet sich somit für Multi-Media-Anwendungen wie Internet-Telefonie oder Internet-TV.
- So genannte mobile IPs ermöglichen es, sich mit einer festen IP-Adresse in verschiedenen Netzwerken anzumelden. So kann man sich mit seinem Laptop im Heimnetzwerk, im Café oder am Arbeitsplatz mit derselben IP-Adresse anmelden.

7.1.2 Aufbau einer IP-Adresse nach IPv6-Standard

IPv6-Adressen sind 128 Bit lang und decken somit einen Adressbereich von rund 340 Sextillionen möglichen Netzwerkteilnehmern ab. Sie bestehen aus 8 Blöcken zu je 16 Bit und werden als hexadezimale Zahl notiert. Das folgende Beispiel zeigt eine mögliche IPv6-Adresse:

„2001:0db8:0000:0000:0000:54f3:dd6b:0001/64“

Um die Lesbarkeit solcher IP-Adressen zu verbessern, entfallen Nullen, die am Anfang eines Ziffernblocks stehen. Darüber hinaus kann eine einzige Gruppe von Blöcken entfallen, die komplett aus Nullen bestehen. Für das oben gezeigte Beispiel wäre eine möglich Darstellungsweise demnach die folgende:

„2001:db8::54f3:dd6b:1/64“

Eine IPv6-Adresse besteht aus zwei Komponenten: einem Präfix und einem Interface Identifier. Das Präfix bezeichnet die Zugehörigkeit der IP-Adresse zu einem Netzwerk, während der Interface Identifier z. B. im Fall der Autokonfiguration aus einer Link Layer Adresse erzeugt wird und somit zu einer Netzwerkkarte gehört. Das Gerät kann Interface Identifier auch mit Hilfe von Zufallszahlen generieren. Dies erhöht die Sicherheit. Auf diese Weise können mehrere IPv6-Adressen einem Teilnehmer zugeordnet werden.

Das Präfix beschreibt den ersten Teil der IP-Adresse. Die Länge des Präfix steht als Dezimalzahl hinter einem Schrägstrich. Für das hier genannte Beispiel lautet das Präfix:

„2001:db8::/64“

Der übrige Teil der IP-Adresse stellt den Interface Identifier dar. Dieser lautet für das angebene Beispiel:

„::54f3:ddb6:1“

Gegenüber den IP-Adressen nach dem Standard IPv4 ergeben sich für den Aufbau der neuen IPv6-Adressen einige Änderungen:

- Während IPv4-Adressen einen Adressraum von 32 Bit abdecken, entsteht durch die neue Länge von 128 Bit ein deutlich größerer Adressbereich von IPv6. IPv6-Adressen sind daher viermal so lang wie eine IPv4-Adresse.
- Eine Schnittstelle kann mehrere IPv6-Adressen haben, bedingt durch die mögliche Zuweisung mehrerer Präfixe zu einem Interface Identifier. Im IPv4-Standard besitzt jede Schnittstelle ausschließlich eine IP-Adresse.
- Die automatische Zuweisung von IPv4-Adressen erfolgt immer über einen DHCP-Server. IPv6 hingegen beherrscht eine Autokonfiguration, welche die Verwendung eines DHCP-Server überflüssig macht. Es besteht allerdings immer noch die Option, einen DHCP-Server einzusetzen oder die IP-Adressen statisch zu konfigurieren.

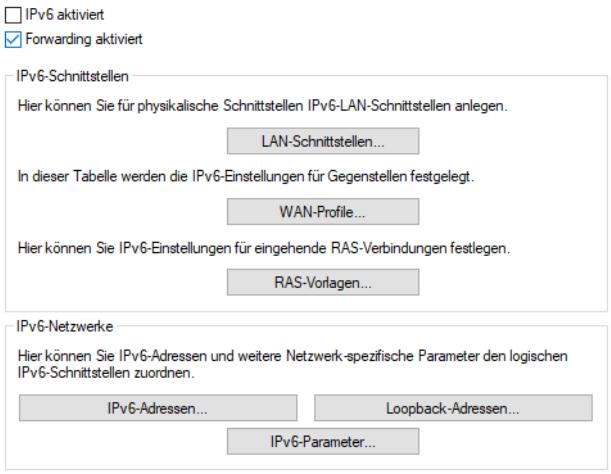
7.1.3 Migrationsstufen

IPv6 ist in Netzwerken auf verschiedene Arten verfügbar. Man unterscheidet bei IPv6-Umgebungen zwischen nativem IPv6 und IPv6, das über einen Tunnel entsteht.

- **Reines (oder natives) IPv6:** Reines IPv6 bezeichnet ein Netzwerk, das nach Außen über IPv6 kommuniziert. Auf dieses können Teilnehmer mit IPv4-Internetzugang nur zugreifen, wenn der Router eine der unten beschriebenen Tunneltechnologien einsetzt.
- **IPv6 via Dual Stack:** Dual Stack bezeichnet den parallelen Betrieb von IPv4 und IPv6 in einem Netzwerk.
- **IPv6 Tunneling:** Wenn ein Router keinen nativen IPv6-Internetzugang hat, besteht die Möglichkeit, mit Hilfe eines Tunnels auf IPv6-Netzwerke zuzugreifen.

7.2 Grundeinstellungen

Auf der Konfigurationsseite **IPv6** > **Allgemein** nehmen Sie die Grundeinstellungen vor.



IPv6 aktiviert

Sie haben die Möglichkeit, IPv6 im Gerät zu aktivieren oder zu deaktivieren.

Forwarding aktiviert

Forwarding dient der Paketweiterleitung zwischen IPv6-Schnittstellen. Diese Option ist standardmäßig aktiviert.

IPv6-Schnittstellen

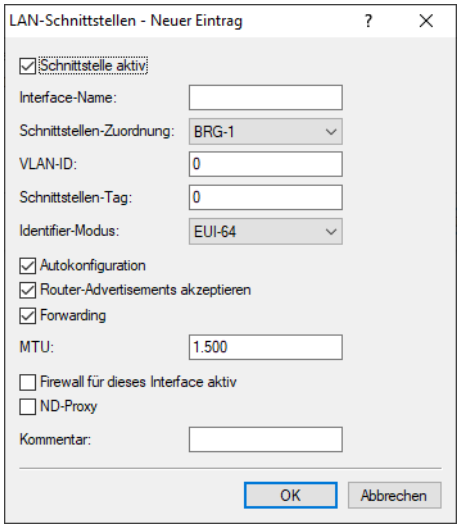
Über die Schaltflächen **LAN-Schnittstellen**, **WAN-Profile** und **RAS-Vorlagen** gelangen Sie zu den Tabellen, die Ihnen die Möglichkeiten bieten, neue Schnittstellen hinzuzufügen sowie bestehende Schnittstellen zu konfigurieren oder zu löschen.

IPv6-Netzwerke

Die Schaltflächen **IPv6-Adressen** und **IPv6-Parameter** dienen dazu, den Schnittstellen IPv6-Adressen zuzuordnen sowie die Parameter der Schnittstellen (Gateway-Adresse, erster und zweiter DNS) zu konfigurieren. Über die Schaltfläche **Loopback-Adressen** lassen sich IPv6-Loopback-Adressen definieren, die das Gerät als zusätzliche Absenderadresse ansieht.

7.2.1 LAN-Schnittstellen

Für jedes existierende IPv4-Netzwerk müssen Sie zusätzlich unter **LAN-Schnittstellen** ein äquivalentes IPv6-Netzwerk anlegen. Dabei müssen die Einstellungen zu Schnittstellen-Bindung, Routing-Tag und VLAN-ID zu den Einstellungen des jeweiligen IPv4-Netzwerks passen. Da ein Gerät beliebig viele IPv6-Adressen haben kann, müssen Sie unter **IPv6-Adressen** statisch konfigurierte IPv6-Adressen hinzufügen.



Die Einträge in der Tabelle **LAN-Schnittstellen** haben folgende Bedeutung:

Schnittstelle aktiv

Aktiviert bzw. deaktiviert diese LAN-Schnittstelle.

Interface-Name

Benennen Sie das logische IPv6-Interface, für das das physikalische Interface (Schnittstellen-Zuordnung) und die VLAN-ID gelten sollen.

Schnittstellen-Zuordnung

Wählen Sie die physikalische Schnittstelle aus, die zusammen mit der VLAN-ID das logische IPv6-Interface bilden soll. Eine Zuordnung „beliebig" wie bei IPv4 ist bei IPv6 nicht mehr möglich.

VLAN-ID

Wählen Sie die VLAN-ID aus, die zusammen mit der physikalischen Schnittstelle das logische IPv6-Interface bilden soll.

Schnittstellen-Tag

Tragen Sie hier als Schnittstellen-Tag einen Wert ein, der das Netzwerk eindeutig spezifiziert. Alle Pakete, die das Gerät auf diesem Netzwerk empfängt, erhalten intern eine Markierung mit diesem Tag. Das

Schnittstellen-Tag ermöglicht eine Trennung der für dieses Netzwerk gültigen Routen auch ohne explizite Firewall-Regel.

Identifiert-Modus

Definiert, wie automatisch erzeugte IPv6-Adressen auf dem jeweiligen Interface des Geräts erzeugt werden.

EUI-64

Automatisch erzeugte IPv6-Adressen auf dem konfigurierten Interface werden nach dem EUI-64-Prinzip generiert, d. h. die MAC-Adresse wird als Basis für den Host-Anteil der IPv6-Adresse verwendet.

Stabil-Privat

Automatisch erzeugte IPv6-Adressen auf dem konfigurierten Interface werden nach RFC 7217 gebildet. Die Erzeugung basiert nicht mehr auf der eindeutigen MAC-Adresse des Geräts oder der Schnittstelle, sondern aus Datenschutzgründen auf einem Teil aus Zufallswerten sowie dem empfangenen Provider-Präfix. Der erzeugte Interface Identifier ist immer stabil bzw. identisch, solange das empfange Präfix identisch ist. Bei wechselndem Präfix ändert sich auch der Interface-Identifier und somit die gesamte IPv6-Adresse des Geräts.

Autokonfiguration

Aktivieren bzw. deaktivieren Sie die automatische Konfiguration von Adressen (SLAAC oder DHCPv6) in der Client-Rolle für dieses Interface.

Falls das Gerät selbst auf diesem Interface Router-Advertisements versendet, erzeugt es auch bei aktivierter Autokonfiguration keine IPv6-Adressen aus empfangenen Router-Advertisements von anderen Routern.

Router Advertisements akzeptieren

Aktivieren bzw. deaktivieren Sie die Auswertung empfangener Router-Advertisement-Nachrichten. Bei deaktivierter Auswertung übergeht das Gerät die über Router-Advertisements empfangenen Präfix-, DNS- und Router-Informationen.

Forwarding

Aktivieren bzw. deaktivieren Sie die Weiterleitung von Datenpaketen an andere Interfaces. Wenn Sie das Forwarding deaktivieren, überträgt das Gerät auch keine Router-Advertisements über dieses Interface.

MTU

Bestimmen Sie die gültige MTU auf dem entsprechenden Link.

Firewall für dieses Interface aktiv

Hier haben Sie die Möglichkeit, die Firewall für das Interface einzeln zu deaktivieren, wenn die globale Firewall für IPv6-Schnittstellen aktiv ist.

ND-Proxy

Aktiviert bzw. deaktiviert die IPv6 Neighbor Discovery-Proxyfunktionalität. Der ND-Proxy entspricht dem IPv4-Pendant ARP-Proxy. Mit dem ND-Proxy binden Sie entfernte IPv6-Stationen in Ihr lokales Netz so ein, als befänden sie sich in Ihrem lokalen Netz. Der Router antwortet dann stellvertretend auf Neighbor-Discovery-Pakete für die entfernte Station.

Mögliche Szenarien:

- Ein vorgeschalteter Router unterstützt keine DHCPv6-Präfix Delegierung. Der nachgeschaltete Router aktiviert den ND-Proxy und verwendet auf seiner LAN- und WAN-Schnittstelle das gleiche /64-Präfix. Das LAN-Präfix wird aus dem Router Advertisement des vorgeschalteten Routers der WAN-Schnittstelle erzeugt. Damit ist eine Kommunikation zwischen Stationen im LAN zu Stationen im WAN möglich, die das gleiche /64-Präfix verwenden.
- Ein VPN-Gateway weist Einwahlclients eine IPv6-Adresse aus dem gleichen Präfix zu, das schon auf einer lokalen Schnittstelle konfiguriert ist. Dieser Router muss den ND-Proxy aktivieren, damit eine Kommunikation

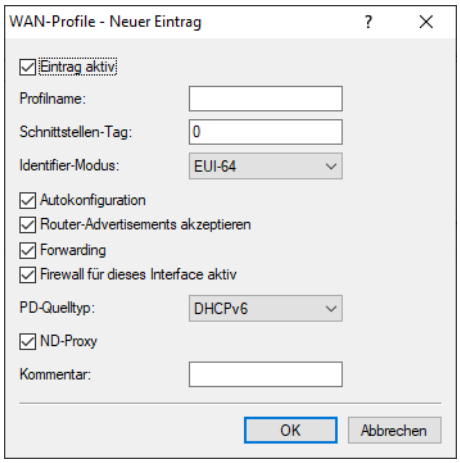
zwischen Einwahl-Client und Stationen im lokalen LAN mit dem gleichen IPv6-Präfix möglich ist. Das Szenario ist analog zum ARP-Proxy für IPv4.

Kommentar

Vergeben Sie einen aussagekräftigen Kommentar für diesen Eintrag.

7.2.2 WAN-Profile

Für jede existierende Gegenstelle, auf der Sie IPv6 benutzen wollen, müssen Sie zusätzlich unter **WAN-Profile** eine äquivalente logische IPv6-WAN-Schnittstelle als Profil anlegen. Dieses Profil kann dann bei der Gegenstelle ausgewählt werden.



Die Einträge in der Tabelle **WAN-Profile** haben folgende Bedeutung:

Eintrag aktiv

Aktiviert bzw. deaktiviert dieses Profil einer logischen IPv6-WAN-Schnittstelle.

Profilname

Geben Sie dem Profil des logischen IPv6-Interface einen Namen. Über diesen Namen kann das Profil bei der entsprechenden IPv6-Gegenstelle ausgewählt werden. Voreingestellt ist immer das Profil „DEFAULT“. Falls ein leerer Eintrag als IPv6-Gegenstelle ausgewählt wird, dann ist IPv6 für diese Gegenstelle nicht aktiv.

Ein Profil in der Tabelle WAN-Schnittstellen kann von Gegenstellen mehrfach referenziert werden.

Schnittstellen-Tag

Tragen Sie hier als Schnittstellen-Tag einen Wert ein, der das Netzwerk eindeutig spezifiziert. Alle Pakete, die das Gerät auf diesem Netzwerk empfängt, erhalten intern eine Markierung mit diesem Tag. Das Schnittstellen-Tag ermöglicht eine Trennung der für dieses Netzwerk gültigen Routen auch ohne explizite Firewall-Regel.

Identifiert-Modus

Definiert, wie automatisch erzeugte IPv6-Adressen auf dem jeweiligen Interface des Geräts erzeugt werden.

EUI-64

Automatisch erzeugte IPv6-Adressen auf dem konfigurierten Interface werden nach dem EUI-64-Prinzip generiert, d. h. die MAC-Adresse wird als Basis für den Host-Anteil der IPv6-Adresse verwendet.

Stabil-Privat

Automatisch erzeugte IPv6-Adressen auf dem konfigurierten Interface werden nach RFC 7217 gebildet. Die Erzeugung basiert nicht mehr auf der eindeutigen MAC-Adresse des Geräts oder der Schnittstelle, sondern aus Datenschutzgründen auf einem Teil aus Zufallswerten sowie dem empfangenen Provider-Präfix. Der erzeugte Interface Identifier ist immer stabil bzw. identisch, solange das empfange Präfix identisch ist. Bei wechselndem Präfix ändert sich auch der Interface-Identifier und somit die gesamte IPv6-Adresse des Geräts.

Autokonfiguration

Aktivieren bzw. deaktivieren Sie die automatische Konfiguration von Adressen (SLAAC oder DHCPv6) in der Client-Rolle für dieses Interface.

Router Advertisements akzeptieren

Aktivieren bzw. deaktivieren Sie die Auswertung empfangener Router-Advertisement-Nachrichten. Bei deaktivierter Auswertung übergeht das Gerät die über Router-Advertisements empfangenen Präfix-, DNS- und Router-Informationen.

Forwarding

Aktivieren bzw. deaktivieren Sie die Weiterleitung von Datenpaketen an andere Interfaces. Wenn Sie das Forwarding deaktivieren, überträgt das Gerät auch keine Router-Advertisements über dieses Interface.

Firewall für dieses Interface aktiv

Hier haben Sie die Möglichkeit, die Firewall für das Interface einzeln zu deaktivieren, wenn die globale Firewall für IPv6-Schnittstellen aktiv ist. Um die Firewall für alle Schnittstellen global zu aktivieren, markieren Sie unter **Firewall/QoS** > **Allgemein** die Option **IPv6-Firewall/QoS aktiviert**.

Wenn Sie die globale Firewall deaktivieren, dann ist auch die Firewall einer einzelnen Schnittstelle inaktiv. Das gilt auch dann, wenn Sie diese mit dieser Option aktiviert haben.

PD-Quelltyp

Mit dieser Option legen Sie fest, wie der Router die Präfix-Delegation durchführt:

DHCPv6

Die Präfix-Delegation erfolgt über DHCPv6.

Router-Advertisement

Die Präfix-Delegation erfolgt über Router-Advertisement, der DHCPv6-Client startet dabei nicht.

In Mobilfunknetzwerken mit IPv6-Unterstützung ist erst ab 3GPP-Release 10 eine Unterstützung von DHCPv6-Präfix-Delegation vorgesehen. Damit ist es in Mobilfunknetzen vor Release 10 nur möglich, einem Endgerät genau ein /64-Präfix z. B. durch Router-Advertisements zuzuweisen. Bei Smartphones oder Laptops lässt sich mit dieser Methode einfach eine IPv6-Unterstützung realisieren. Router benötigen bei IPv6 aber mindestens ein weiteres Präfix, das sie an Clients ins LAN propagieren können.

Die IPv6-Präfix-Delegation vom WWAN ins LAN macht es möglich, dass Clients das auf der WAN-Mobilfunkseite zugewiesene /64-Präfix im LAN verwenden können. Damit ist ein Betrieb eines Routers in einem IPv6-Mobilfunknetzwerk ohne DHCPv6-Präfix-Delegation und Neighbor Discovery Proxy (ND-Proxy) möglich. Der Router kündigt das bezogene /64-Präfix per Router-Advertisement im LAN an, statt es auf dem WAN-Interface hinzuzufügen. Clients können dann aus diesem Präfix eine Adresse generieren und diese für die IPv6-Kommunikation benutzen.

Es gelten folgende Einschränkungen:

- Sie können das Feature nur auf Punkt-zu-Punkt-Verbindungen (z. B. PPP oder Mobilfunk-Schnitstellen) nutzen, wobei die Gegenstelle automatisch allen Datenverkehr an den Router sendet, es sei denn, der ND-Proxy wird zusätzlich aktiviert.
- Sie können nur genau ein IPv6-Netz im LAN anlegen, da nur ein /64-Präfix zur Verfügung steht.

ND-Proxy

Aktiviert bzw. Deaktiviert die IPv6 Neighbor Discovery-Proxyfunktionalität. Der ND-Proxy entspricht dem IPv4 Pendant ARP-Proxy. Mit dem ND-Proxy binden Sie entfernte IPv6-Stationen in Ihr lokales Netz so ein, als befänden sie sich in Ihrem lokalen Netz. Der Router antwortet dann stellvertretend auf Neighbor-Discovery-Pakete für die entfernte Station.

Beispielszenarien:

- Ein vorgeschalteter Router unterstützt keine DHCPv6-Präfix Delegierung. Der nachgeschaltete Router aktiviert den ND-Proxy und verwendet auf seiner LAN- und WAN-Schnittstelle das gleiche /64-Präfix. Das LAN-Präfix wird aus dem Router Advertisement des vorgeschalteten Routers der WAN-Schnittstelle erzeugt. Damit ist eine Kommunikation zwischen Stationen im LAN zu Stationen im WAN möglich, die das gleiche /64-Präfix verwenden.
- Ein VPN-Gateway weist Einwahlclients eine IPv6-Adresse aus dem gleichen Präfix zu, das schon auf einer lokalen Schnittstelle konfiguriert ist. Dieser Router muss den ND-Proxy aktivieren, damit eine Kommunikation zwischen Einwahl-Client und Stationen im lokalen LAN mit dem gleichen IPv6-Präfix möglich ist. Das Szenario ist analog zum ARP-Proxy für IPv4.

Kommentar

Vergeben Sie einen aussagekräftigen Kommentar für diesen Eintrag.

7.2.3 RAS-Vorlagen

Grundsätzlich existieren zwei Wege, um die Konfiguration von RAS-Gegenstellen zu verwalten:

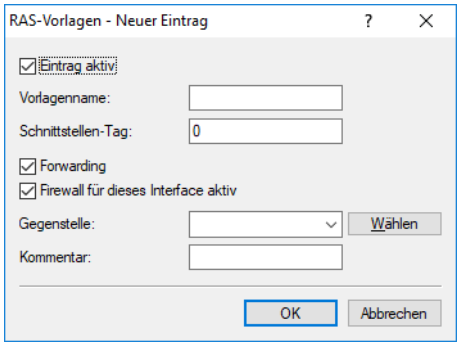
Die Benutzerdaten bzw. die Konfigurationen sind lokal im Gerät gespeichert.

Der Vorteil dieser Variante ist, dass man auf einen RADIUS-Server verzichtet und damit Verwaltung und Kosten der Netzinfrastruktur gering hält.

Die Benutzerdaten bzw. die Konfigurationen sind auf einen externen RADIUS-Server ausgelagert.

Der Vorteil dieser Variante liegt in der zentralen Benutzerverwaltung bei umfangreichen verteilten Netzwerk-Szenarien.

Für RAS-Zugänge über IPv6 müssen Sie zusätzlich unter **RAS-Vorlagen** die entsprechende RAS-Schnittstelle einrichten.



Die Einträge in der Tabelle **RAS-Vorlagen** haben folgende Bedeutung:

Eintrag aktiv

Aktivieren oder deaktivieren Sie hier diese RAS-Vorlage.

Vorlagenname

Definieren Sie hier den Namen der RAS-Schnittstelle, über die die IPv6-Gegenstellen zugreifen.

Schnittstellen-Tag

Tragen Sie hier als Schnittstellen-Tag einen Wert ein, der das Netzwerk eindeutig spezifiziert. Alle Pakete, die das Gerät auf diesem Netzwerk empfängt, erhalten intern eine Markierung mit diesem Tag. Das Schnittstellen-Tag ermöglicht eine Trennung der für dieses Netzwerk gültigen Routen auch ohne explizite Firewall-Regel.

Forwarding

Aktivieren bzw. deaktivieren Sie die Weiterleitung von Datenpaketen an andere Interfaces.

Firewall für dieses Interface aktiv

Hier haben Sie die Möglichkeit, die Firewall für jedes Interface einzeln zu deaktivieren, wenn die globale Firewall für IPv6-Schnittstellen aktiv ist. Um die Firewall für alle Schnittstellen global zu aktivieren, markieren Sie unter **Firewall/QoS** > **Allgemein** die Option **IPv6-Firewall/QoS aktiviert**.

Wenn Sie die globale Firewall deaktivieren, dann ist auch die Firewall einer einzelnen Schnittstelle inaktiv. Das gilt auch dann, wenn Sie diese mit dieser Option aktiviert haben.

Gegenstelle

Bestimmen Sie hier eine Gegenstelle oder eine Liste von Gegenstellen für RAS-Einwahl-Benutzer.

Die folgenden Werte sind möglich:

- Eine einzelne Gegenstelle aus den Tabellen unter **Setup** > **WAN** > **PPTP-Gegenstellen**, **Setup** > **WAN** > **L2TP-Gegenstellen** oder **Setup** > **PPPoE-Server** > **Namenliste**.
- Dem Platzhalter "*", der bewirkt, dass diese Schnittstelle für alle PPTP-, PPPoE- und L2TP-Gegenstellen gilt.
- Dem Platzhalter "*" als Suffix oder Präfix von Gegenstellen, z. B. "FIRMA*" oder "*TUNNEL".

Durch den Platzhalter-Mechanismus bilden Sie bei IPv6-RAS-Diensten mehrere Gegenstellen auf sogenannte Template-Schnittstellen ab. Diese Template-Schnittstellen sind als normale Schnittstellen bei IPv6-Diensten wie DHCPv6-Server oder Router Advertisements einsetzbar. Darüber lässt sich z. B. eine Gruppe von RAS-Schnittstellen aus einem IPv6-Präfix-Pool bedienen.

Kommentar

Vergeben Sie einen aussagekräftigen Kommentar für diesen Eintrag.

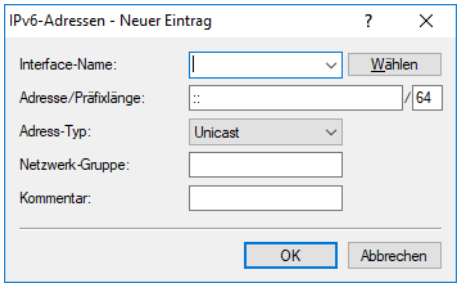
Informationen zu den RADIUS-Attributen für IPv6-RAS-Dienste finden Sie unter *Erweiterung der RADIUS-Attribute für IPv6-RAS-Dienste* auf Seite 1605.

Wenn RAS-Clients einen IPv6-DNS-Server zugewiesen oder per Präfix-Delegation Präfixe delegiert bekommen sollen, so müssen Sie unter **IPv6** > **DHCPv6** einen entsprechenden Eintrag in der Tabelle **DHCPv6-Netzwerke** anlegen.

Wollen Sie einen Benutzer anhand der PPP-Liste authentifizieren, so müssen Sie unter **Kommunikation** > **Protokolle** > **PPP-Liste** bei diesem Benutzer die Option **IPv6-Routing** aktivieren.

7.2.4 IPv6-Adressen

In der Tabelle **IPv6-Adressen** können Sie sowohl IPv6-Adressen für LAN-Schnitsttellen als auch für WAN-Schnittstellen anlegen.



Die Einträge in der Tabelle **IPv6-Adressen** haben folgende Bedeutung:

Interface-Name

Benennen Sie das Interface, dem Sie das IPv6-Netz zuordnen wollen.

Adresse / Präfixlänge

Vergeben Sie eine IPv6-Adresse inklusive Präfixlänge für dieses Interface.

Die Präfixlänge beträgt standardmäßig 64 Bit („/64“). Verwenden Sie für die IPv6-Adresse möglichst keine längeren Präfixe, da zahlreiche IPv6-Mechanismen (z. B. die Autokonfiguration) von maximal 64 Bit Länge ausgehen.

Beispiel:

- Global Unicast Adresse: 2001:db8::1/64
- Unique Local Adresse: fd00::1/64

Verbindungslokale Adressen sind pro Interface fest vorgegeben und nicht konfigurierbar.

Adress-Typ

Bestimmen Sie den Typ der IPv6-Adresse.

Mögliche Optionen:

- Unicast

  Beim Adresstyp Unicast können sie eine vollständige IPv6-Adresse im Feld **Adresse / Präfixlänge** inkl. Interface Identifier angeben, z. B. „2001:db8::1234/64“.

- Anycast

  Beim Adresstyp Anycast können sie ebenfalls eine vollständige IPv6-Adresse im Feld **Adresse / Präfixlänge** inkl. Interface Identifier angeben, z. B. „2001:db8::1234/64“. Intern behandelt das Gerät diese Adresse als Anycast-Adresse.

- EUI-64

  Beim Adresstyp EUI-64 entspricht die IPv6-Adresse der IEEE-Norm „EUI-64“. Die MAC-Adresse der Schnittstelle stellt damit einen eindeutig identifizierbaren Bestandteil der IPv6-Adresse dar. Ein korrektes Eingabeformat für eine IPv6-Adresse inkl. Präfixlänge nach EUI-64 würde lauten: „2001:db8:1::/64“. EUI-64 ignoriert einen eventuell konfigurierten Interface Identifier der jeweiligen IPv6-Adresse und ersetzt ihn durch einen Interface Identifier nach EUI-64. Die Präfixlänge bei EUI-64 muss zwingend „/64“ sein.

- Delegiert, Autokonfiguration

Die IPv6-Adresse wird aus dem empfangenen Router Advertisement Präfix auf dem ausgewählten Interface (Feld **Interface-Name**) und dem Host-Identifier aus dem Feld **Adresse / Präfixlänge** gebildet. Im Feld **Adresse / Präfixlänge** kann z. B. der Wert „::2/64“ eingetragen werden, zusammen mit dem Präfix „2001:db8::/64“ auf dem Interface ergibt sich dann entsprechend die Adresse „2001:db8::2/64“.

- Delegiert, DHCPv6

  Die IPv6-Adresse wird aus dem empfangenen delegierten DHCPv6-Präfix auf dem ausgewählten Interface (Feld **Interface-Name**) und dem Host-Identifier aus dem Feld **Adresse / Präfixlänge** gebildet. Im Feld **Adresse / Präfixlänge** kann z. B. der Wert „::2/64“ eingetragen werden, zusammen mit dem Präfix „2001:db8::/56“ auf dem Interface ergibt sich dann entsprechend die Adresse „2001:db8::2/64“. Ebenso kann eine Adresse aus einem beliebigen Subnetz des delegierte Präfix gebildet werden, z. B. aus „0:0:0:0001::1“ und dem Präfix „2001:db8::/56“ wird die Adresse „2001:db8:0:0001::1/64“.

- Stabil-Privat

  Automatisch erzeugte IPv6-Adressen auf dem konfigurierten Interface werden nach RFC 7217 gebildet. Die Erzeugung basiert nicht mehr auf der eindeutigen MAC-Adresse des Geräts oder der Schnittstelle, sondern aus Datenschutzgründen auf einem Teil aus Zufallswerten sowie dem empfangenen Provider-Präfix. Der erzeugte Interface Identifier ist immer stabil bzw. identisch, solange das empfange Präfix identisch ist. Bei wechselndem Präfix ändert sich auch der Interface-Identifier und somit die gesamte IPv6-Adresse des Geräts.

Netzwerk-Gruppe

Vergeben Sie einen aussagekräftigen Namen für diese Kombination aus IPv6-Adresse und Präfix. Diese Bezeichnung der Netzwerk-Gruppe muss nicht eindeutig sein. Somit können mehrere verschiedene Präfixe auch einer Netzwerk-Gruppe angehören.

Die Netzwerk-Gruppe kann z.B. in der IPv6-Firewall in der Stations-Tabelle **Firewall/QoS** > **IPv6-Regeln** > **Stations-Objekte** im Feld **Netzwerk-Name** referenziert werden, wenn dort der **Typ** „Benamtes Netz“ eingestellt wird. Dann besteht die Station aus allen Präfixen dieser Netzwerk-Gruppe.

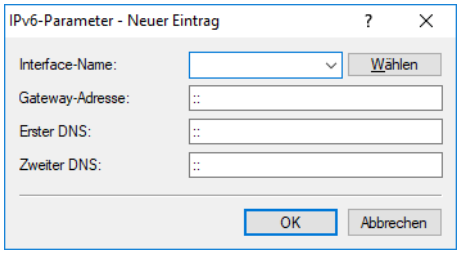
Deweiteren kann man sie im VPN in der Tabelle **VPN** > **Allgemein** > **Netzwerk-Regeln** > **IPv6-Regeln** im Feld **Lokale Netzwerke** referenzieren. Dadurch landen alle Präfixe der Netzwerk-Gruppe auf der lokalen Seite der Netzbeziehung.

Kommentar

Vergeben Sie einen aussagekräftigen Kommentar für diesen Eintrag.

7.2.5 IPv6-Parameter

In der Tabelle **IPv6-Parameter** können Sie statische Parameter für LAN- oder WAN-Schnittstellen wie einen IPv6-DNS-Server oder IPv6-Gateway manuell konfigurieren, falls Sie keine Autokonfiguration oder DHCPv6 verwenden.



Die Einträge in der Tabelle **IPv6-Parameter** haben folgende Bedeutung:

Interface-Name

Benennen Sie das Interface, für das Sie die IPv6-Parameter konfigurieren wollen.

Gateway-Adresse

Bestimmen Sie das verwendete IPv6-Gateway für dieses Interface.

Dieser Parameter überschreibt Gateway-Informationen, die das Gerät beispielsweise über Router-Advertisements empfängt.

Erster DNS

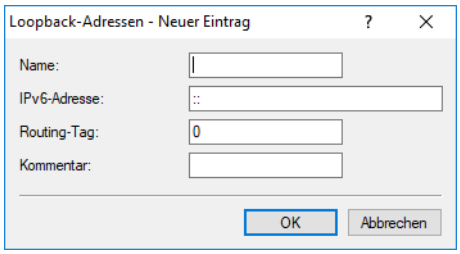
Bestimmen Sie den ersten IPv6-DNS-Server für dieses Interface.

Zweiter DNS

Bestimmen Sie den zweiten IPv6-DNS-Server für dieses Interface.

7.2.6 Loopback-Adressen

In der Tabelle **Loopback-Adressen** lassen sich IPv6-Loopback-Adressen festlegen. Das Gerät sieht jede dieser Adressen als eigene Adresse an, die auch dann verfügbar ist, wenn z. B eine physikalische Schnittstelle deaktiviert ist.



Die Einträge in der Tabelle **Loopback-Adressen** haben folgende Bedeutung:

Name

Vergeben Sie hier einen eindeutigen Namen für diese Loopback-Adresse.

IPv6-Adresse

Geben Sie hier eine gültige IPv6-Adresse ein.

Routing-Tag

Geben Sie hier das Routing-Tag des Netzes an, zu dem die Loopback-Adresse gehört. Nur die Pakete mit dem entsprechenden Routing-Tag erreichen diese Adresse.

Kommentar

Tragen Sie hier einen optionalen Kommentar ein.

7.2.7 Einrichtung eines IPv6-Internetzugangs

Sie haben die Möglichkeit einen Zugang zu einem IPv6-Netz einzurichten, wenn

- Sie ein IPv6-fähiges Gerät besitzen,
- eine Tunneltechnologie benutzen und
- Ihr Provider ein natives IPv6-Netz unterstützt oder Sie einen Zugang zu einem so genannten Tunnelbroker haben, der Ihre IPv6-Datenpakete vermittelt.

7.2.7.1 IPv6-Zugang über den Setup-Assistenten von LANconfig

Der Setup-Assistent unterstützt Sie bei der Konfiguration des IPv6-Zugangs für Ihre Geräte.

Folgende Optionen stehen Ihnen im Assistenten zur Verfügung:

- *Den IPv6-Zugang bei einem neuen, unkonfigurierten Gerät einrichten.*

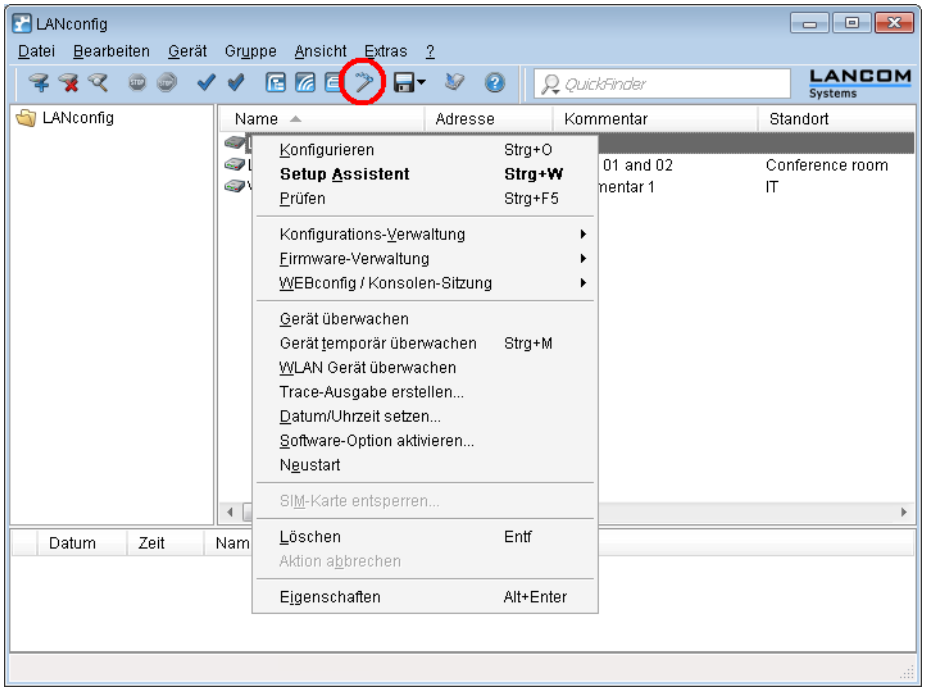
› *Den IPv6-Zugang bei einem bestehenden Gerät zusätzlich zum bestehenden IPv4-Zugang einrichten.*

Setup-Assistent – IPv6 bei einem neuen Gerät einrichten

Wenn Sie ein neues Gerät angeschlossen, aber noch nicht konfiguriert haben, haben Sie die Möglichkeit per Setup-Assistent IPv4- und IPv6-Verbindungen herzustellen.

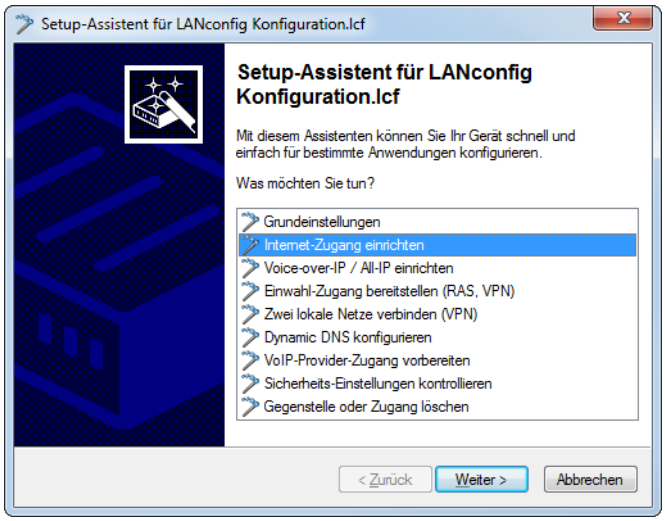
Um Ihre Eingaben zu übernehmen und zum nächsten Dialog zu gelangen, klicken Sie jeweils auf **Weiter**.

1. Starten Sie den Setup-Assistenten in LANconfig. Markieren Sie dazu das zu konfigurierende Gerät. Den Setup-Assistenten starten Sie nun entweder per Rechtsklick im sich öffnenden Menü oder per Zauberstab-Icon in der Symbolleiste.



Abhängig sowohl von den Möglichkeiten Ihres Gerätes als auch den Optionen Ihres Internet-Providers unterscheidet sich der Assistent in den angezeigten Optionen.

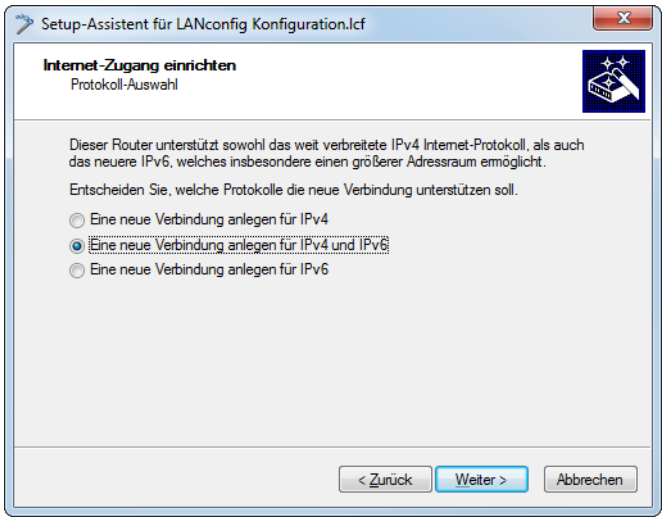
2. Wählen Sie im Setup-Assistenten die Option **Internet-Zugang einrichten**.



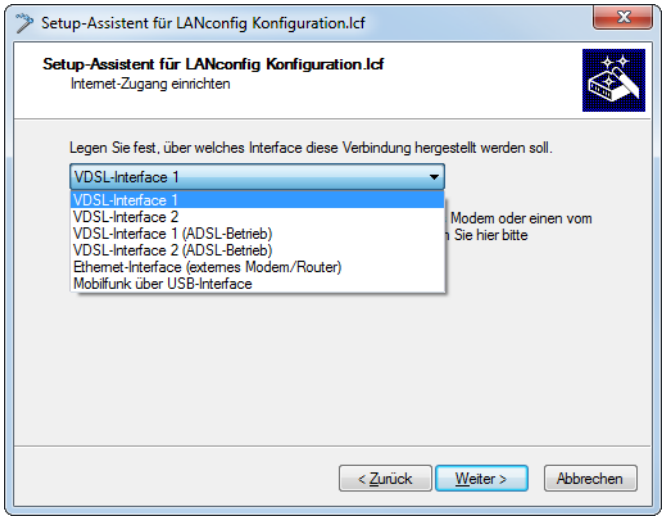
3. Sie haben die Möglichkeit, zwischen den folgenden Optionen zu wählen:

- Eine Verbindung sowohl für IPv4 als auch für IPv6 herstellen. Dies ist die empfohlene Option für ein neues Gerät.
- Eine reine IPv4-Verbindung herstellen.
- Eine reine IPv6-Verbindung herstellen.
- Eine vorhandene IPv4-Verbindung um IPv6 erweitern

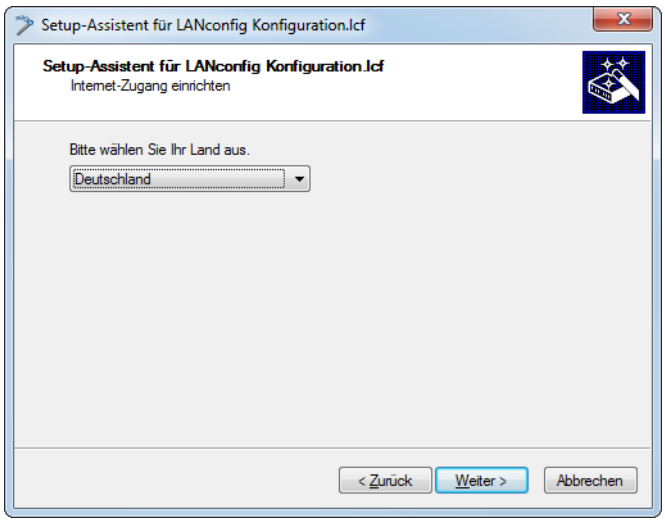
Nachfolgend führen wir Sie durch die Einrichtung einer Dual-Stack-Verbindung. Aktivieren Sie die entsprechende Auswahl.



4. Bestimmen Sie die Schnittstelle, über die Sie die Verbindung herstellen wollen.



5. Wählen Sie aus der Liste Ihr Land aus.

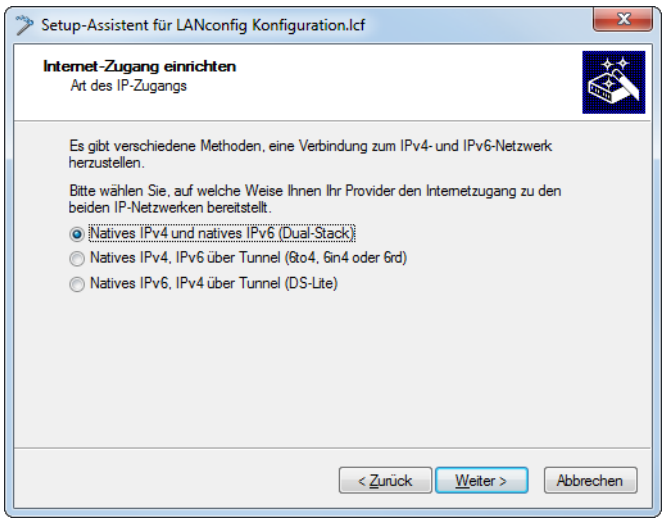


6. Wählen Sie Ihren Internet-Provider aus.

   Sie haben folgende Einträge zur Auswahl:

   - Eine Auswahl relevanter Internet-Provider
   - Internet-Zugang über PPP over ATM
   - Internet-Zugang über PPP over Ethernet
   - Internet-Zugang über Plain Ethernet
   - Internet-Zugang über PPTP
   - Internet-Zugang über DHCP
   - Internet-Zugang mit statischer IP

7. Abhängig von Ihrem Internet-Provider gibt es verschiedene Möglichkeiten für die Art des IP-Zugangs.



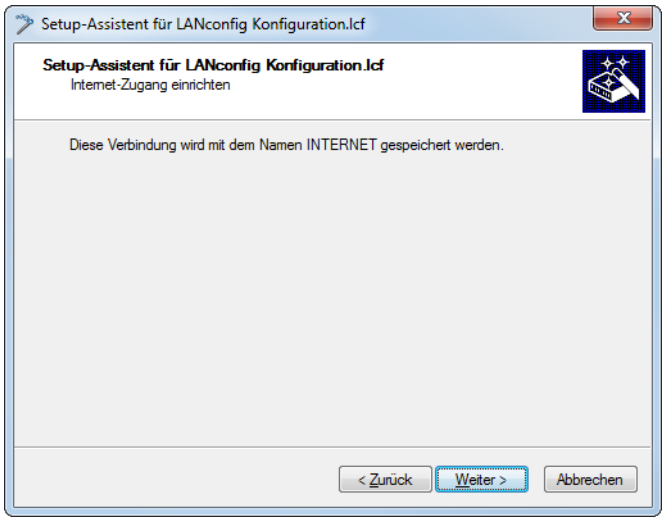
   Sie haben folgende Optionen zur Auswahl:

   - **Natives IPv4 und natives IPv6 (Dual-Stack)**: Konfigurieren Sie eine direkte Verbindung ohne Tunnel.
   - **Natives IPv4, IPv6 über Tunnel**: Starten Sie den Assistenten zur Konfiguration eines 6to4-, 6in4- oder 6rd-Tunnels.
   - **Natives IPv6, IPv4 über Tunnel (DS-Lite)**: Starten Sie den Assistenten zur Konfiguration eines DS-Lite-Tunnels.

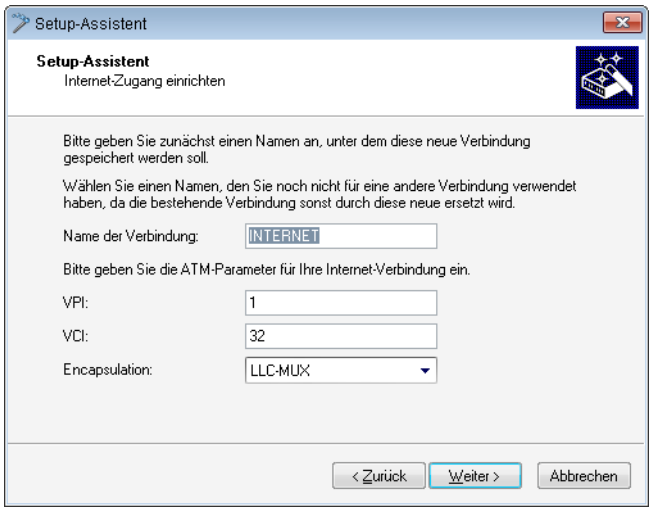
Aktivieren Sie die Option für die Einrichtung einer nativen IPv6-Internet-Verbindung.

8. Der Name für diese Verbindung ist „INTERNET".

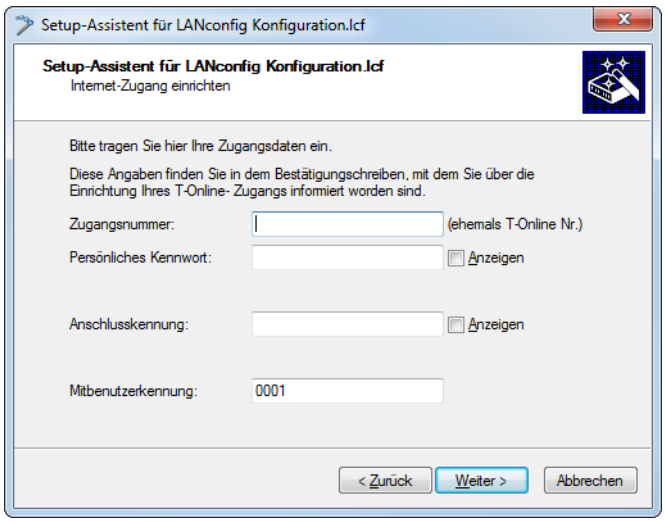
Falls bereits eine Verbindung mit diesem Namen existiert, dann können Sie einen eigenen Namen für diese Verbindung angeben.



Wenn Sie den Internet-Zugang alternativ z. B. über eine PPPoE-Verbindung einrichten wollen, geben Sie zusätzlich noch die entsprechenden ATM-Parameter ein.

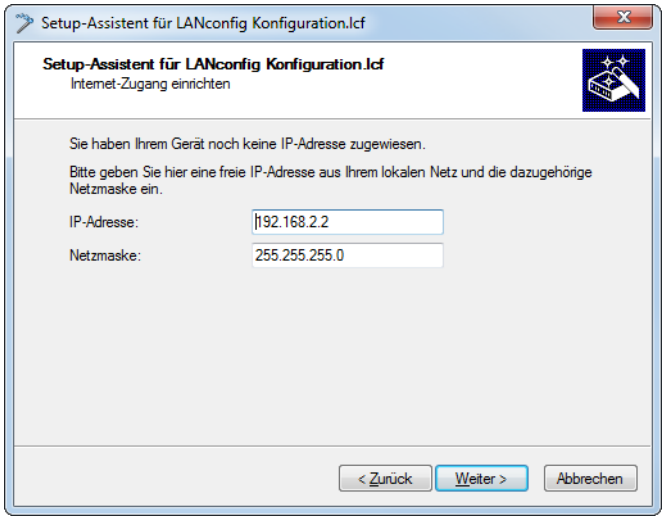


9. Tragen Sie die Zugangsdaten ein, die Ihnen Ihr Provider bei der Errichtung Ihres Internetzugangs mitgeteilt hat.

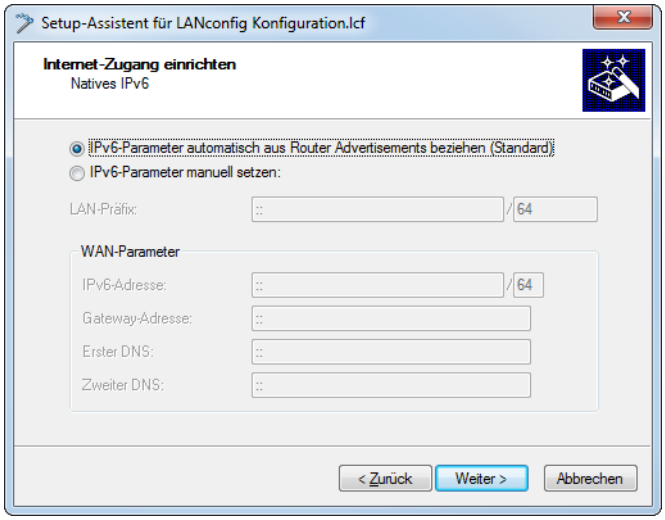


Je nach Provider können sich Art und Anzahl der Felder unterscheiden.

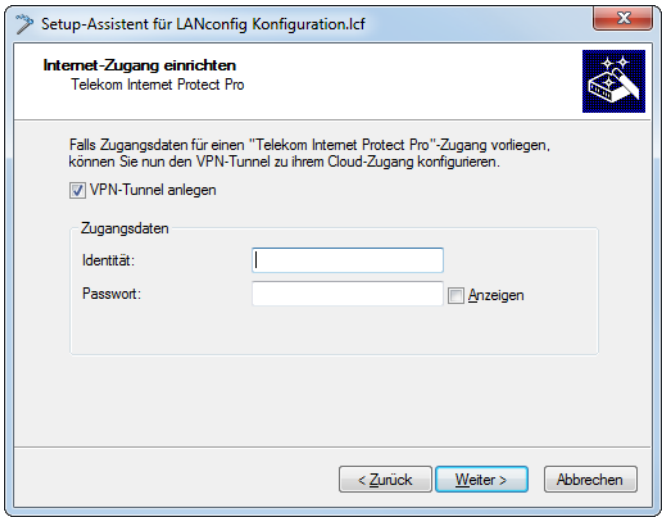
10. Falls Ihr Gerät noch keine IP-Adresse besitzt, tragen Sie eine neue IP-Adresse sowie die entsprechende Netzmaske ein.



11. Übernehmen Sie die Default-Einstellung **IPv6-Parameter automatisch aus Router-Advertisements beziehen.**



12. Abhängig vom Internet-Provider können weitere Optionen eingerichtet werden.



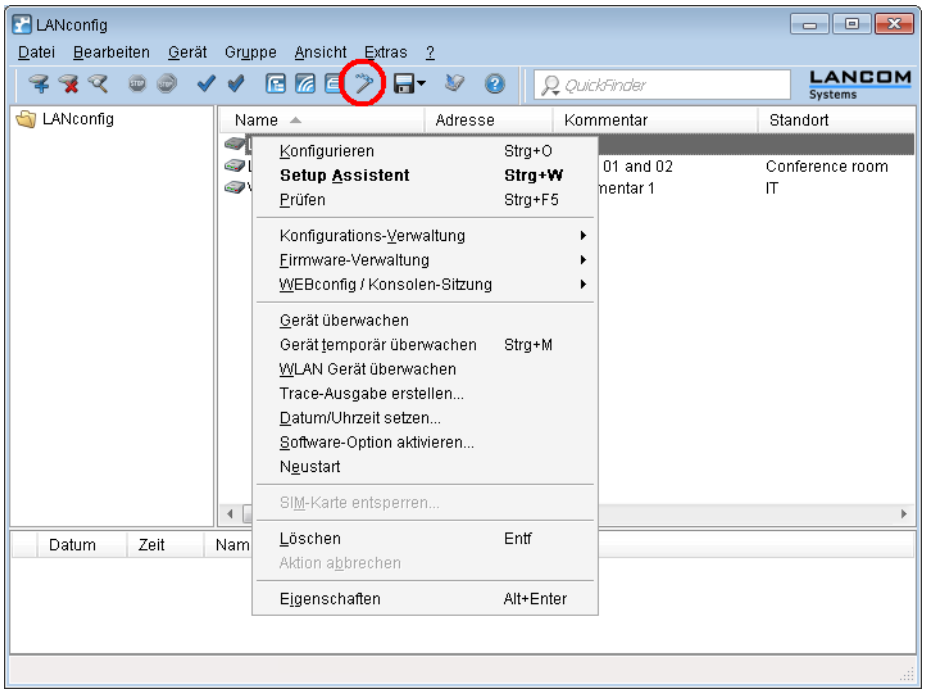
13. Sie haben die Einrichtung des nativen IPv6-Internetzugangs abgeschlossen. Klicken Sie abschließend auf **Fertig stellen**, damit der Assistent Ihre Eingaben im Gerät speichern kann.

Setup-Assistent – IPv6 bei einem bestehenden Gerät einrichten

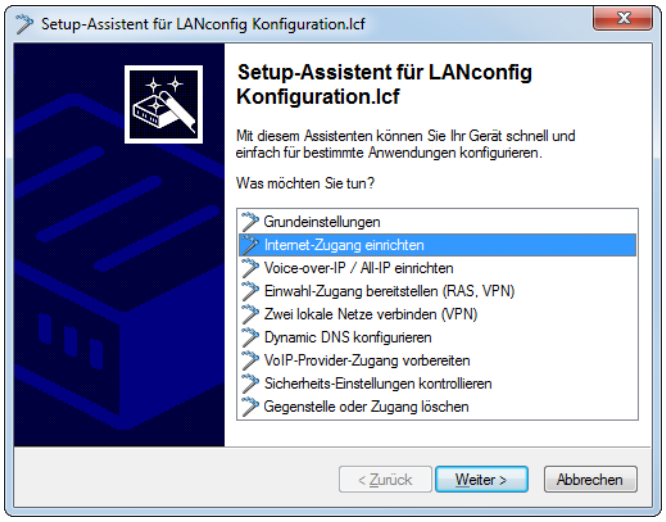
Wenn Sie ein Gerät für IPv4 konfiguriert haben und zusätzlich eine IPv6-Verbindung einrichten wollen, haben Sie die Möglichkeit, diese IPv6-Verbindungen über den Setup-Assistenten herzustellen.

Um Ihre Eingaben zu übernehmen und zum nächsten Dialog zu gelangen, klicken Sie jeweils auf **Weiter**.

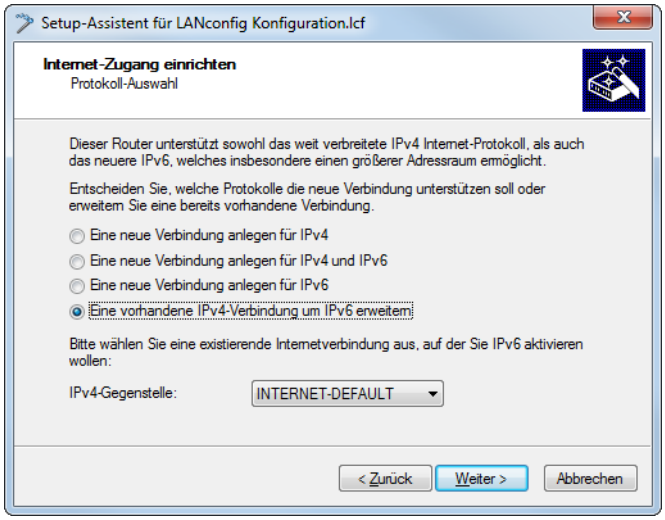
1. Starten Sie den Setup-Assistenten in LANconfig. Markieren Sie dazu das zu konfigurierende Gerät. Den Setup-Assistenten starten Sie entweder per Rechtsklick im sich öffnenden Menü oder per Zauberstab-Icon in der Symbolleiste



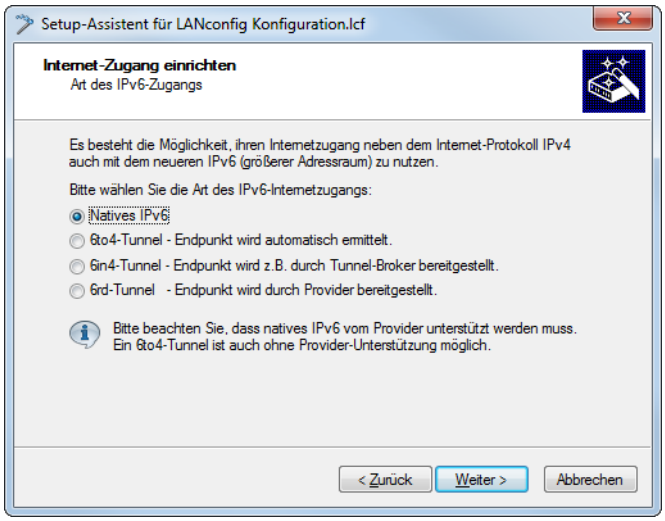
2. Wählen Sie im Setup-Assistenten die Option **Internet-Zugang einrichten**. Klicken Sie anschließend auf **Weiter**.



3. Da ihr Gerät bereits IPv4 beherrscht, bietet der Setup-Assistent Ihnen die Möglichkeit, diese existierende Einstellung um IPv6 zu erweitern. Wählen Sie diese Option und klicken Sie anschließend auf **Weiter**.



4. Wählen Sie die Art des IPv6-Internet-Zugangs.

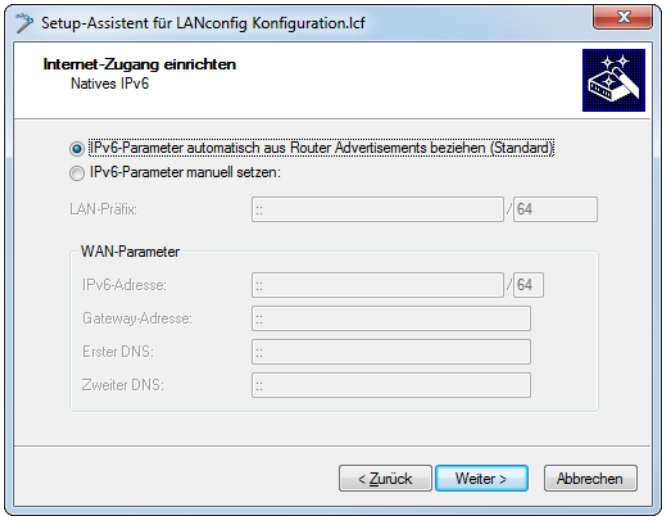


Sie haben folgende Optionen zur Auswahl:

- **Natives IPv6**: Konfigurieren Sie eine direkte Verbindung ohne Tunnel.
- **6to4-Tunnel**: Starten Sie den Assistenten zur Konfiguration eines 6to4-Tunnels.
- **6in4-Tunnel**: Bestimmen Sie in der Eingabemaske die Parameter für den 6in4-Tunnel.
- **6rd-Tunnel**: Bestimmen Sie in der Eingabemaske die Parameter für den 6rd-Tunnel.

Aktivieren Sie die Option für die Einrichtung einer nativen IPv6-Internet-Verbindung.

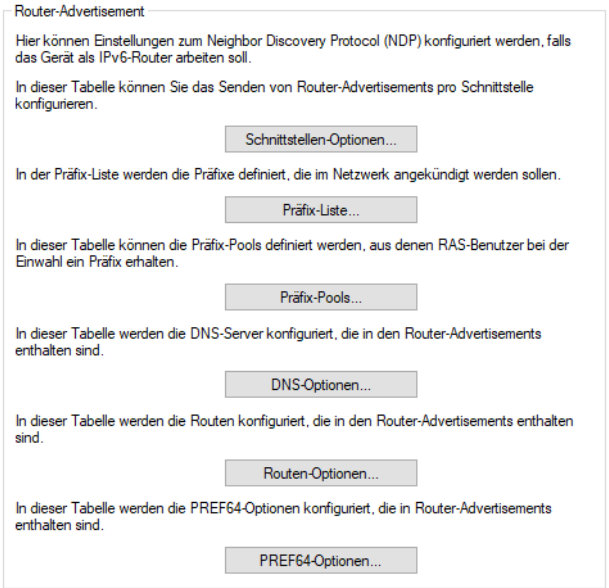
5. Übernehmen Sie die Voreinstellung **IPv6-Parameter automatisch aus Router-Advertisements beziehen.**



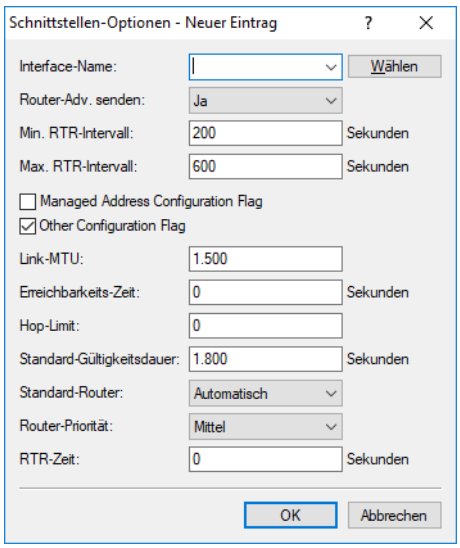
6. Sie haben die Einrichtung des nativen IPv6-Internetzugangs abgeschlossen. Klicken Sie abschließend auf **Fertig stellen**, damit der Assistent Ihre Eingaben im Gerät speichern kann.

7.3 Router-Advertisement

In der Konfiguration **Router-Advertisement** bieten sich Ihnen mehrere Schaltflächen mit Optionen zu Einstellungen des Neighbor Discovery Protocol (NDP), falls das Gerät als IPv6-Router arbeiten soll:



7.3.1 Schnittstellen-Optionen



Hier aktivieren oder deaktivieren Sie die folgenden Funktionen von Schnittstellen:

Interface-Name

Definiert den Namen des logischen Interfaces, auf dem Router-Advertisements gesendet werden sollen.

Router-Adv. senden

Reguliert periodisches Senden von Router-Advertisements und das Antworten auf Router Solicitations.

Min. RTR-Intervall

Definiert die minimal erlaubte Zeit zwischen dem Senden von Unsolicited Multicast Router-Advertisements in Sekunden. Min-RTR-Intervall und Max-RTR-Intervall bilden ein Zeitintervall, in dem Router-Advertisements zufällig verteilt versendet werden. Erlaubte Werte liegen zwischen 3 Sekunden und 0,75 * Max-RTR-Intervall. Standard ist 200 Sekunden.

Max. RTR-Intervall

Maximaler Wert des RTR-Intervalls. Standard ist 600 Sekunden.

Managed Address Configuration Flag

Wenn diese Funktion aktiv ist, konfiguriert ein Client, der dieses Router-Advertisement empfängt, Adressen durch Stateful Autoconfiguration (DHCPv6). Clients beziehen dann auch automatisch andere Informationen, wie z. B. DNS-Server.

Other Configuration Flag

Wenn diese Funktion aktiv ist, versucht ein Client, zusätzliche Informationen, z. B. DNS-Server-Adressen, über DHCPv6 zu beziehen. Ob ein Client Adressen durch Autokonfiguration bilden soll, können Sie pro Präfix in der **Präfix-Liste** unter **Autokonfiguration erlauben (SLAAC)** bestimmen.

Link-MTU

Definiert die gültige MTU auf dem entsprechenden Link.

Erreichbarkeits-Zeit

Definiert die Zeit, die der Router als erreichbar gelten soll. Beim Standard 0 werden in den Router-Advertisements keine Vorgaben zur Erreichbarkeits-Zeit propagiert.

Hop-Limit

Definiert die maximale Anzahl von Routern, über die ein IP-Datenpaket weitergeschickt werden darf. Ein Router entspricht hierbei einem "Hop". Standard ist 0 und bedeutet, dass kein Hop-Limit definiert ist.

Standard-Router

Definiert das Verhalten, wie sich das Gerät als Standardgateway bzw. Router ankündigen soll. Die Parameter haben folgende Funktionen:

Automatisch

Solange eine WAN-Verbindung besteht, setzt das Gerät eine positive Router-Lifetime in den Router-Advertisement-Nachrichten. Das führt dazu, dass ein Client diesen Router als Standard-Gateway verwendet.

Besteht die WAN-Verbindung nicht mehr, so setzt der Router die Router-Lifetime auf 0. Ein Client verwendet dann diesen Router nicht mehr als Standard-Gateway.

Immer

Die Router-Lifetime ist unabhängig vom Status der WAN-Verbindung immer positiv, d. h. größer 0.

Nie

Die Router-Lifetime ist immer 0.

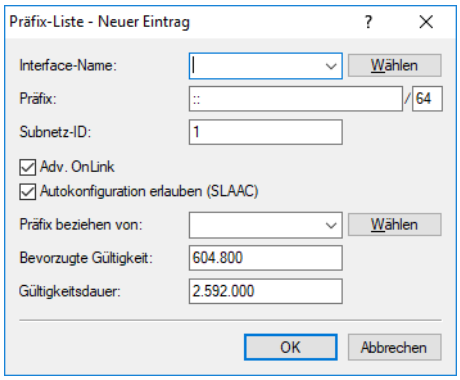
Router-Priorität

Definiert die Präferenz dieses Routers. Clients tragen diese Präferenz in ihre lokale Routing-Tabelle ein.

RTR-Zeit

Definiert die Zeit in Sekunden zwischen aufeinanderfolgenden Sendungen von Neighbor-Solicitations-Nachrichten an einen Nachbarn, wenn die Adresse aufgelöst oder die Erreichbarkeit getestet wird.

7.3.2 Präfix-Liste



Setzen Sie die Präfix-Optionen verwendeter Schnittstellen. Möglich sind folgende Einstellungen:

Interface-Name

Definiert den Namen des logischen Interfaces auf dem Router-Advertisements gesendet werden sollen.

Präfix

Tragen Sie hier ein Präfix ein, das in Router-Advertisements angekündigt wird, z. B. „2001:db8::/64“. Die Präfixlänge muss immer exakt „/64“ sein, da es sonst für Clients unmöglich ist, Adressen durch Hinzufügen ihrer Interface-Identifier (mit Länge 64 Bit) zu generieren. Soll ein vom Provider delegiertes Präfix automatisch weiter propagiert werden, so setzen Sie hier „::/64“ und den Namen des entsprechenden WAN-Interfaces unter dem Parameter **Präfix beziehen von** ein.

Subnetz-ID

Tragen Sie hier die Subnetz-ID ein, die mit dem vom Provider delegierten Präfix kombiniert werden soll. Weist der Provider z. B. das Präfix „2001:db8:a::/48“ zu und ist die Subnetz-ID „0001“ oder kurz „1“, so enthält das Router-Advertisement auf diesem Interface das Präfix „2001:db8:a:0001::/64“. Die maximale Subnetzlänge bei einem 48 Bit langen delegierten Präfix ist 16 Bit (65.536 Subnetze), d. h. mögliche Subnetz-IDs von „0000“ bis „FFFF“. Bei einem delegierten Präfix von „/56“ ist die maximale Subnetzlänge 8 Bit (256 Subnetze), d. h. Subnetz-IDs von „00“ bis „FF“. In der Regel wird die Subnetz-ID „0“ zur automatischen Bildung der WAN-IPv6-Adresse verwendet. Deshalb starten Subnetz-IDs für LANs bei „1“. Die Default-Einstellung ist „1“.

Adv. OnLink

Gibt an, ob dieses Präfix direkt auf das Interface gebunden ist ('On Link').

Autokonfiguration erlauben (SLAAC)

Gibt an, ob der Client das Präfix für die Stateless Address Autoconfiguration (SLAAC) verwenden soll. Die Default-Einstellung ist „aktiviert“.

Präfix beziehen von

Definiert den Namen des Interfaces, auf dem ein Präfix über DHCPv6-Präfix-Delegation oder Tunnel empfangen wird. Aus diesem Präfix kann pro Interface ein Subnetz abgeleitet und propagiert werden.

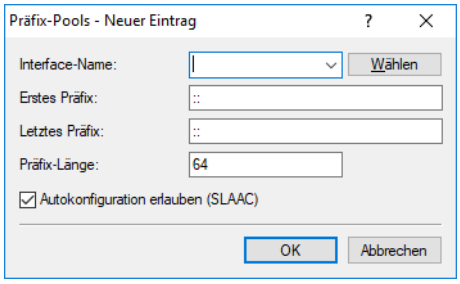
Bevorzugte Gültigkeit

Definiert die Zeit, wie lange eine IPv6-Adresse als „bevorzugt“ (preferred) gelten soll. Ist die bevorzugte Gültigkeitsdauer einer Adresse abgelaufen, so wird sie als „abgelehnt“ (deprecated) markiert und nur noch für bereits existierende Sessions verwendet, aber nicht mehr für neue.

Gültigkeitsdauer

Definiert die Zeit, wie lange eine IPv6-Adresse als „gültig“ (valid) betrachtet werden soll bis sie „ungültig“ (invalid) und dementsprechend verworfen wird.

7.3.3 Präfix-Pools



Diese Tabelle enthält Präfix-Pools, aus denen RAS-Benutzer einen Präfix bei der Einwahl über IPv6 erhalten. Möglich sind folgende Einstellungen:

Interface-Name

Bestimmt den Namen der RAS-Schnittstelle, für die dieser Präfix-Pool gelten soll.

Erster Präfix

Definiert das erste Präfix des Pools, das der Einwahl-Benutzer durch Router-Advertisement zugeteilt bekommt, z. B. „2001:db8::“. Jeder Benutzer erhält dabei genau ein /64-Präfix aus dem Pool.

Letzter Präfix

Definiert das letzte Präfix des Pools, das der Einwahl-Benutzer durch Router-Advertisement zugeteilt bekommt, z. B. „2001:db9:FFFF::“. Jeder Benutzer erhält dabei genau ein /64-Präfix aus dem Pool.

Präfix-Länge

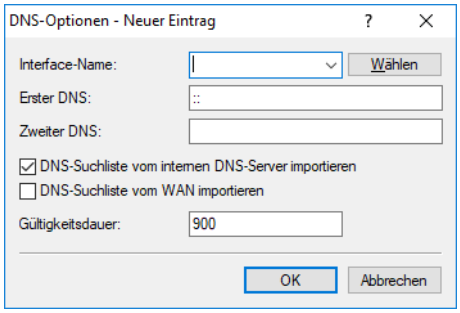
Definiert die Länge des Präfixes, das der Einwahl-Benutzer per Router-Advertisement zugewiesen bekommt. Die Größe des Einwahl-Pools richtet sich nur nach dem ersten und letzen Präfix. Jeder Benutzer erhält dabei genau ein /64-Präfix aus dem Pool zugewiesen.

Damit ein Client aus dem Präfix per Autokonfiguration eine IPv6-Adresse bilden kann, muss die Präfix-Länge immer 64 Bit betragen.

Autokonfiguration erlauben (SLAAC)

Gibt an, ob der Client das Präfix für eine Stateless Address Autoconfiguration (SLAAC) verwenden kann.

7.3.4 DNS-Optionen



Definiert die DNS-Informationen in Router-Advertisements nach RFC 6106. Möglich sind folgende Einstellungen:

Interface-Name

Name des Interfaces, auf dem der IPv6-DNS-Server Informationen in Router-Advertisements ankündigt.

Erster DNS

IPv6-Adresse des ersten IPv6-DNS-Servers (Recursive DNS-Server, RDNSS, nach RFC 6106) für dieses Interface.

Zweiter DNS

IPv6-Adresse des zweiten IPv6-DNS-Servers für dieses Interface.

DNS-Suchliste vom internen DNS-Server importieren

Gibt an, ob die DNS-Suchliste (DNS Search List) bzw. die eigene Domäne für dieses logische Netzwerk vom internen DNS-Server eingefügt werden soll, z. B. „intern“. Die eigene Domäne ist unter **DNS** > **Allgemein** > **Allgemeine Einstellungen** konfigurierbar. Die Default-Einstellung ist **aktiviert**.

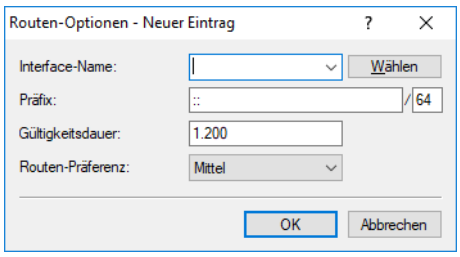
DNS-Suchliste vom WAN inportieren

Gibt an, ob die vom Provider übertragene DNS-Suchliste (z. B. provider-xy.de) in diesem logischen Netzwerk angekündigt werden soll. Diese Funktion steht nur dann zur Verfügung, wenn in der Präfix-Liste das entsprechende WAN-Interface unter **Präfix beziehen von** verknüpft ist.

Gültigkeitsdauer

Definiert die Zeit in Sekunden, die ein Client diesen DNS-Server zur Namensauflösung verwenden darf.

7.3.5 Routen-Optionen



Definiert die Routen-Option in Router-Advertisements nach RFC 4191 (Route Information Option). Möglich sind folgende Einstellungen:

Interface-Name

Definiert den Namen des logischen Interfaces, auf dem Router-Advertisements mit dieser Routen-Option gesendet werden sollen.

Präfix

Präfix der Routen-Option, z. B. „2001:db8::/32“.

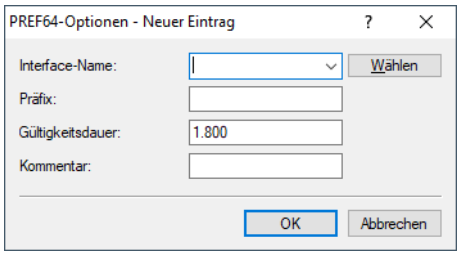
Gültigkeitsdauer

Dauer in Sekunden, für welche die Route gültig sein soll.

Routen-Präferenz

Präferenz der Route. Mögliche Werte sind „Hoch“, „Mittel“ (Default) und „Niedrig“.

7.3.6 PREF64-Optionen



In dieser Tabelle kann die Präfix-Option in Router Advertisements (PREF64-Option nach *RFC 8781*) für NAT64-Präfixe konfiguriert werden, die an Clients im Router Advertisement angekündigt werden soll. Clients übernehmen dieses Präfix z. B. für 464XLAT.

Interface-Name

Geben Sie den Namen des Interfaces an, auf welchem die PREF64-Option angekündigt werden soll.

Präfix

Definiert das NAT64-Präfix mit Präfixlänge, z. B. 64:ff9b::/96

Gültigkeitsdauer

Gültigkeitsdauer des NAT64-Präfixes in Sekunden. Default: 1800 Sekunden.

Kommentar

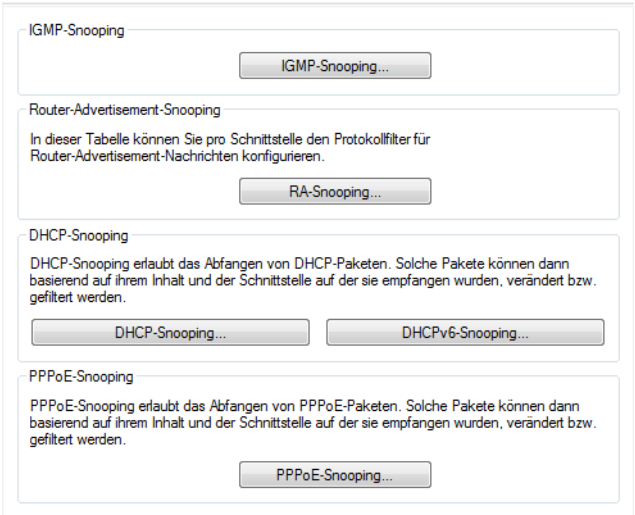
Vergeben Sie einen aussagekräftigen Kommentar.

7.3.7 Router-Advertisement-Snooping

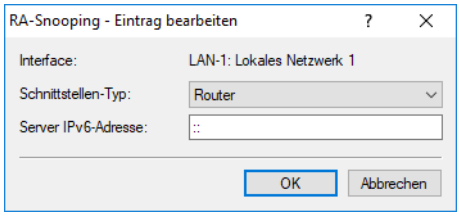
In einem IPv6-Netz senden Router periodisch oder auf Anfrage Router-Advertisements, um sich angeschlossenen Clients als Gateway zu präsentieren. Diesen Mechanismus können Angreifer wie beim DHCPv4 nutzen, um anfragenden Clients eine fehlerhafte oder schadhafte Netzkonfiguration zu übermitteln.

Beim RA-Snooping vermittelt das Gerät nur Router-Advertisements von Routern, nicht aber von Clients. Über die Angabe einer Router-Adresse lassen sich die Router-Advertisments auf einen bestimmten Router als Sender einschränken.

Im LANconfig können Sie das RA-Snooping unter **Schnittstellen** > **Snooping** mit einem Klick auf **RA-Snooping** für jede Schnittstelle separat festlegen.



Nach Auswahl der entsprechenden Schnittstelle können Sie die folgenden Einstellungen festlegen:



Schnittstellen-Typ

Bestimmen Sie hier den bevorzugten Schnittstellen-Typ. Die folgende Auswahl ist möglich:

Router

Das Gerät vermittelt alle RAs, die an dieser Schnittstelle ankommen (Default).

Client (aktiviert Sperre)

Das Gerät verwirft alle RAs, die an dieser Schnittstelle ankommen.

Server IPv6-Adresse

Sofern Sie den Schnittstellen-Typ **Router** gewählt haben, geben Sie hier eine optionale Router-Adresse an. Bei Angabe einer Router-Adresse vermittelt das Gerät nur RAs des entsprechenden Routers.

Unter dem Schnittstellen-Typ **Client** ignoriert das Gerät dieses Eingabefeld.

7.4 DHCPv6

Im Vergleich zu IPv4 benötigen Clients in einem IPv6-Netzwerk wegen der Autokonfiguration keine automatischen Adresszuweisungen über einen entsprechenden DHCP-Server. Da aber bestimmte Informationen wie DNS-Server-Adressen nicht per Autokonfiguration übertragen werden, ist es in bestimmten Anwendungsszenarien sinnvoll, auch bei IPv6 einen DHCP-Dienst im Netzwerk zur Verfügung zu stellen.

DHCPv6-Server

Die Verwendung eines DHCPv6-Servers ist bei IPv6 optional. Grundsätzlich unterstützt ein DHCPv6-Server zwei Betriebsarten:

- **Stateless**: Der DHCPv6-Server verteilt keine Adressen, sondern nur Informationen, z. B. DNS-Server-Adressen. Bei dieser Methode generiert sich ein Client seine IPv6-Adresse durch die „Stateless Address Autokonfiguration (SLAAC)". Dieses Verfahren ist besonders attraktiv u. a. für kleine Netzwerke, um den Verwaltungsaufwand möglichst gering zu halten.
- **Stateful**: Der DHCPv6-Server verteilt IPv6-Adressen, ähnlich wie bei IPv4. Dieses Verfahren ist deutlich aufwändiger, da ein DHCPv6-Server die Adressen vergeben und verwalten muss.

Ein DHCPv6-Server verteilt nur die Optionen, die ein IPv6-Client explizit bei ihm anfragt, d. h., der Server vergibt einem Client nur dann eine Adresse, wenn dieser explizit eine Adresse anfordert.

Zusätzlich kann der DHCPv6-Server Präfixe zur weiteren Verteilung an Router weitergeben. Dieses Verfahren wird als „Präfix-Delegierung" bezeichnet. Ein DHCPv6-Client muss allerdings ebenfalls dieses Präfix explizit angefragt haben.

DHCPv6-Client

Durch die Autokonfiguration in IPv6-Netzwerken gestaltet sich die Konfiguration der angeschlossenen Clients sehr einfach und komfortabel.

Damit ein Client jedoch auch Informationen z. B. über DNS-Server erhalten kann, müssen Sie das Gerät so konfigurieren, dass es bei Bedarf den DHCPv6-Client aktiviert.

Die Einstellungen für den DHCPv6-Client sorgen dafür, dass das Gerät beim Empfang bestimmter Flags im Router-Advertisment den DHCPv6-Client startet, um spezielle Anfragen beim zuständigen DHCPv6-Server zu stellen:

- **M-Flag**: Erhält ein entsprechend konfiguriertes Gerät ein Router-Advertisment mit gesetztem „M-Flag", dann fordert der DHCPv6-Client eine IPv6-Adresse sowie andere Informationen wie DNS-Server, SIP-Server oder NTP-Server beim DHCPv6-Server an.
- **O-Flag**: Bei einem „O-Flag" fragt der DHCPv6-Client beim DHCPv6-Server nur nach Informationen wie DNS-Server, SIP-Server oder NTP-Server, nicht jedoch nach einer IPv6-Adresse.

  Wenn das „M-Flag" gesetzt ist, muss nicht zwingend auch das „O-Flag" gesetzt sein.

Bei IPv6 wird die Default-Route nicht über DHCPv6 verteilt, sondern über Router-Advertisements.

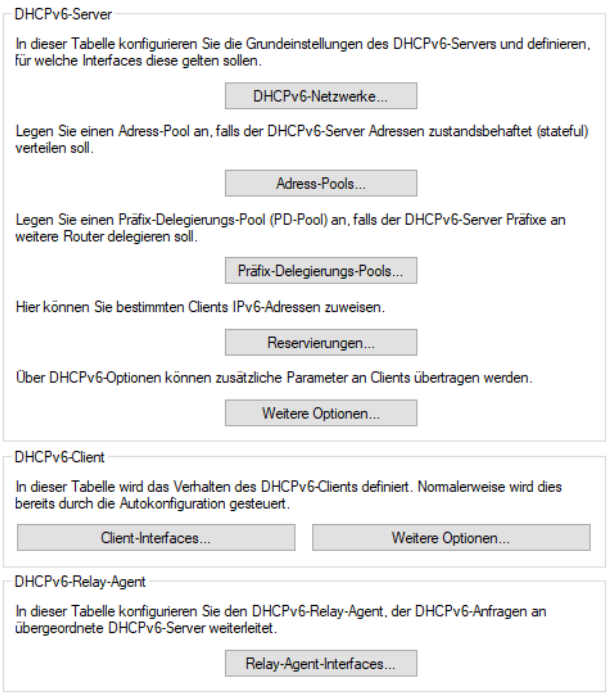
Relay-Agent

Ein DHCPv6-Relay-Agent leitet DHCP-Nachrichten zwischen DHCPv6-Clients und DHCPv6-Servern weiter, die sich in unterschiedlichen Netzwerken befinden (Layer 3).

Lightweight-DHCPv6-Relay-Agent

Ein Lightweight-DHCPv6-Relay-Agent (LDRA) nach RFC 6221 ermöglicht die Erzeugung und Weitergabe von Relay-Agent-Informationen zwischen DHCPv6-Clients und DHCPv6-Servern auf Layer 2.

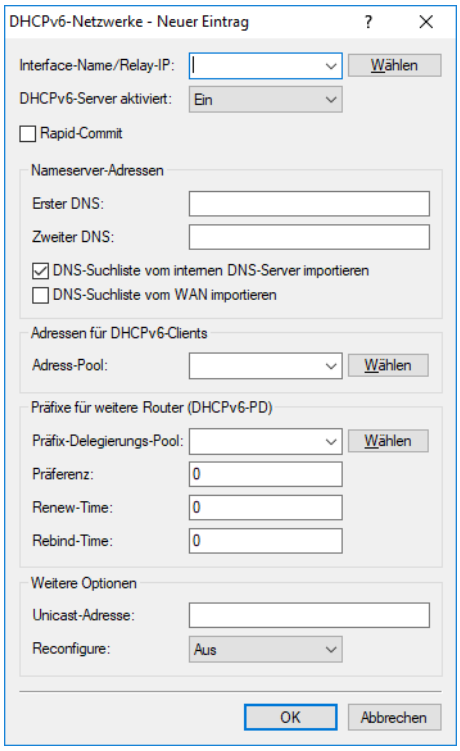
In LANconfig finden Sie die Einstellungen unter **IPv6** > **DHCPv6**:



7.4.1 DHCPv6-Server

7.4.1.1 DHCPv6-Netzwerke

In dieser Tabelle konfigurieren Sie die Grundeinstellungen des DHCPv6-Servers und definieren, für welche Interfaces diese gelten sollen.



Interface-Name/Relay-IP

Name des Interfaces, auf dem der DHCPv6-Server arbeitet, z. B. „INTRANET“. Alternativ hinterlegen Sie hier die IPv6-Adresse des entfernten DHCPv6 Relay-Agenten.

DHCPv6-Server aktiviert

Aktiviert bzw. deaktiviert den Eintrag.

Rapid-Commit

Bei aktiviertem Rapid-Commit antwortet der DHCPv6-Server direkt auf eine Solicit-Anfrage mit einer Reply-Nachricht.

Der Client muss explizit die Rapid-Commit-Option in seiner Anfrage setzen.

Erster DNS

IPv6-Adresse des ersten DNS-Servers. Der Wert „::“ bedeutet, dass der DHCPv6-Server seine eigene Adresse als DNS-Server den Clients ankündigt.

Zweiter DNS

IPv6-Adresse des zweiten DNS-Servers.

DNS-Suchliste vom internen DNS-Server importieren

Gibt an, ob die DNS-Suchliste (DNS Search List) bzw. die eigene Domäne für dieses logische Netzwerk vom internen DNS-Server eingefügt werden soll, z. B. „intern“. Die eigene Domäne ist unter **DNS** > **Allgemein** > **Allgemeine Einstellungen** konfigurierbar. Die Default-Einstellung ist „aktiviert“.

DNS-Suchliste vom WAN importieren

Gibt an, ob die vom Provider übertragene DNS-Suchliste (z. B. provider-xy.de) in diesem logischen Netzwerk angekündigt werden soll. Die Default-Einstellung ist „deaktiviert“.

Adress-Pool

Name des für dieses Interface verwendeten Adress-Pools.

Verteilt der DHCPv6-Server seine Adressen *stateful*, müssen Sie entsprechende Adressen in die Tabelle **Adress-Pools** eintragen.

Präfix-Delegierungs-Pool

Name des Präfix-Pools, den der DHCPv6-Server verwenden soll.

Soll der DHCPv6-Server Präfixe an weitere Router delegieren, müssen Sie entsprechende Präfixe in der Tabelle **Präfix-Delegierungs-Pools** eintragen.

Präferenz

Befinden sich mehrere DHCPv6-Server im Netzwerk, so können Sie über die Präferenz steuern, welchen Server die Clients bevorzugen sollen. Der primäre Server muss dafür eine höhere Präferenz haben als die Backup-Server.

Renew-Time

Definiert die Zeit in Sekunden, zu der der Client den Server wieder kontaktieren soll (durch Renew-Nachricht), um seine vom Server erhaltene Adresse / Präfix zu verlängern. Der Parameter wird auch als T1 bezeichnet.

Rebind-Time

Definiert die Zeit, zu der der Client einen beliebigen Server kontaktieren soll (durch Rebind-Nachricht), um seine erhaltene Adresse / Präfix verlängern zu lassen. Das Rebind-Ereignis tritt nur ein, falls der Client keine Antwort auf seine Renew-Anfrage erhält. Der Parameter wird auch als T2 bezeichnet. Bei der Voreinstellung von 0 geschieht dies automatisch.

Unicast-Adresse

Standardmäßig reagiert der DHCPv6-Server ausschließlich auf Multicast-Anfragen. Wenn der DHCPv6-Server auf eine Unicast-Anfrage reagieren soll, so kann hier diese IPv6-Adresse konfiguriert werden. In der Regel reicht Multicast zur Kommunikation aus.

Reconfigure

Jede IPv6-Adresse bzw. jedes IPv6-Präfix hat eine vom Server vorgegebene Lebenszeit. In gewissen Intervallen fragt ein Client beim Server an, um seine Adresse zu verlängern (sogenannte Renew / Rebind-Zeiten).

Die Reconfigure-Funktion ermöglicht dem DHCPv6-Server, die Clients im Netzwerk zu einer Erneuerung der Leases / Bindings aufzufordern. Wenn der Client mit dem Server beim ersten Kontakt erfolgreich eine Re-Konfiguration (Reconfigure) ausgehandelt hat, dann kann der Server den Client jederzeit auffordern, seine Adresse oder andere Informationen zu aktualisieren. Der Mechanismus wird durch den sogenannten *Reconfigure Key* geschützt, so dass nur der ursprüngliche Server mit dem richtigen Schlüssel den Client auffordern kann. Erhält der Client eine Reconfigure-Nachricht ohne gültigen Reconfigure-Key, so verwirft der Client diese Aufforderung zur Re-Konfiguration.

Unterstützt wird das *Reconfigure Key Authentication Protocol* nach RFC 3315 für die Optionen *Renew* und *Information-Request*, sowie *Rebind* nach RFC 6644. Das Auslösen der Rekonfiguration erfolgt auf der Konsole des Gerätes durch einen do-Befehl im Status-Baum:

```
do /Status/IPv6/DHCPv6/Server/Reconfigure
```

Der Befehl erwartet folgende Parameter:

- `renew`: (optional, Default) Fordert den Client auf, ein Renew für seine Adresse und / oder sein Präfix durchzuführen.
- `rebind`: (optional) Fordert den Client auf, ein Rebind für seine Adresse und / oder sein Präfix durchzuführen.
- `info`: (optional) Fordert den Client auf, ein Information-Request zu senden, um z. B. seinen DNS-Server zu aktualisieren.
- `-c <Client-ID>`: Die Reconfigure-Funktion gilt für den Client mit der angegebenen Client-ID.
- `-b <Adresse/Präfix>`: Die Reconfigure-Funktion gilt für den Client mit der angegebenen Adresse bzw. dem angegebenen Präfix.
- `-i <Interface/Relay>`: Die Reconfigure-Funktion gilt allen Clients, die am angegebenen Interface bzw. Relay angeschlossen sind.
- `-a`: Die Reconfigure-Funktion gilt für alle Clients.

Den Status eines Clients in Bezug auf Reconfigure finden Sie unter **Status** > **IPv6** > **DHCPv6** > **Server** > **Clients**.

In LANconfig stehen Ihnen folgende Einstellungen für das Reconfigure zur Auswahl:

Aus

Deaktiviert die Reconfigure-Funktion.

Verbieten

Clients, die die Reconfigure-Option in Anfragen gesetzt haben, werden vom Server abgelehnt und erhalten keine Adressen, Präfixe oder andere Optionen.

Erlauben

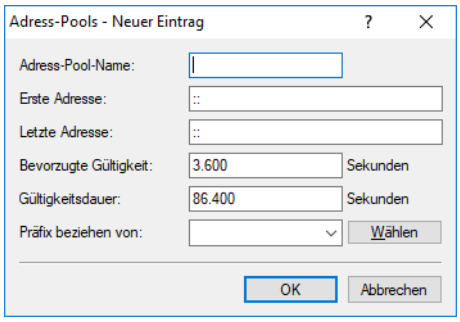
Hat ein Client die Reconfigure-Option in Anfragen gesetzt, so verhandelt der Server mit dem Client die nötigen Parameter, um zu einem späteren Zeitpunkt ein Reconfigure zu starten.

Erzwingen

Clients müssen die Reconfigure-Option in ihren Anfragen setzen, sonst lehnt der Server diese Clients ab. Dieser Modus ist dann sinnvoll, wenn Sie sichergehen wollen, dass der Server ausschließlich Clients bedient, die Reconfigure unterstützen. Dadurch ist gewährleistet, dass alle Clients zu einem späteren Zeitpunkt erfolgreich durch Reconfigure ihre Adressen, Präfixe oder weiteren Informationen aktualisieren können.

7.4.1.2 Adress-Pools

In dieser Tabelle definieren Sie einen Adress-Pool, falls der DHCPv6-Server Adressen stateful verteilen soll:



Adress-Pool-Name

Name des Adress-Pools

Erste Adresse

Erste Adresse des Pools, z. B. „2001:db8::1“

Letzte Adresse

Letzte Adresse des Pools, z. B. „2001:db8::9“

Bevorzugte Gültigkeit

Bestimmen Sie hier die Zeit in Sekunden, die der Client diese Adresse als „bevorzugt“ verwenden soll. Nach Ablauf dieser Zeit führt ein Client diese Adresse als „deprecated“.

Gültigkeitsdauer

Bestimmen Sie hier die Zeit in Sekunden, die der Client diese Adresse als „gültig“ verwenden soll.

Wenn Sie ein Präfix eines WAN-Interfaces zur dynamischen Bildung der Adressen verwenden, ist das Konfigurieren der Werte **Bevorzugte Gültigkeit** und **Gültigkeitsdauer** gesperrt. In diesem Fall ermittelt das Gerät diese Werte automatisch aus den vorgegebenen Werten des delegierten Präfixes des Providers.

Präfix beziehen von

Mit diesem Parameter können Sie den Netzwerk-Clients Adressen aus dem Präfix zuteilen, das der Router vom WAN-Interface per DHCPv6-Präfix-Delegation vom Provider bezogen hat. Wählen Sie hier das entsprechende WAN-Interface aus. Hat der Provider beispielsweise das Präfix „2001:db8::/64“ zugewiesen, dann können Sie beim Parameter **Erste Adresse** den Wert „::1“ und bei **Letzte Adresse** den Wert „::9“ eingeben. Zusammen mit dem vom Provider delegierten Präfix „2001:db8::/64“ erhalten Clients dann Adressen aus dem Pool von „2001:db8::1“ bis „2001:db8::9“. Ist das Provider-Präfix größer als „/64“, z. B. „/48“ oder „/56“, so müssen Sie das Subnetting für das logische Netzwerk in den Adressen berücksichtigen.

Beispiel:

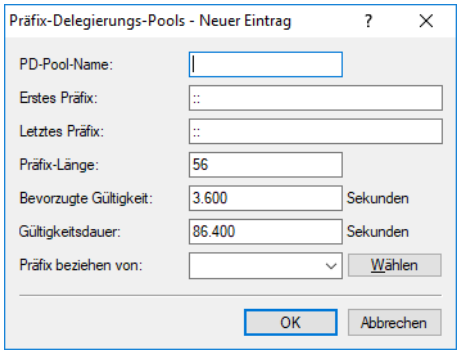
- Zugewiesenes Provider-Präfix: 2001:db8:abcd:aa::/56
- /64 als Präfix des logischen Netzwerks (Subnetzt-ID 1): 2001:db8:abcd:aa01::/64

- Erste Adresse: 0:0:0:0001::1
- Letzte Adresse: 0:0:0:0001::9

Sie sollten diesen Mechanismus nur verwenden, wenn der Provider ein festes Präfix zuweist. Ansonsten kann es passieren, dass der Provider dem Router ein neues Präfix delegiert hat, aber der Client noch eine Adresse aus dem Pool mit dem alten Präfix besitzt.

7.4.1.3 Präfix-Delegierungs-Pools

In dieser Tabelle bestimmen Sie Präfixe, die der DHCPv6-Server an weitere Router delegieren soll:



PD-Pool-Name

Name des PD-Pools

Erstes Präfix

Erstes zu delegierendes Präfix im PD-Pool, z. B. „2001:db8:1100::“

Letztes Präfix

Letztes zu delegierendes Präfix im PD-Pool, z. B. „2001:db8:FF00::“

Präfix-Länge

Länge der Präfixe im PD-Pool, z. B. „56“ oder „60“

Bevorzugte Gültigkeit

Bestimmen Sie hier die Zeit in Sekunden, die der Client dieses Präfix als „bevorzugt“ verwenden soll. Nach Ablauf dieser Zeit führt ein Client diese Adresse als „deprecated“.

Gültigkeitsdauer

Bestimmen Sie hier die Zeit in Sekunden, die der Client dieses Präfix als „gültig“ verwenden soll.

Wenn Sie ein Präfix eines WAN-Interfaces zur dynamischen Bildung der Adressen verwenden, dann sind die Werte **Bevorzugte Gültigkeit** und **Gültigkeitsdauer** gesperrt. In diesem Fall ermittelt das Gerät diese Werte automatisch aus den vorgegebenen Werte des delegierten Präfixes des Providers.

Präfix beziehen von

Mit diesem Parameter können Sie weiteren Routern im Netzwerk Präfixe aus dem vom Provider zugewiesenem Präfix zuteilen (Präfix Delegation). Wählen Sie hier das entsprechende WAN-Interface aus.

Beispiel:

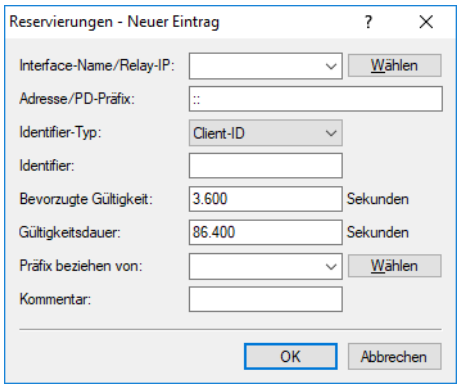
- Zugewiesenes Provider-Präfix: 2001:db8:abcd:aa::/56
- Präfix beziehen von: INTERNET
- Erstes Präfix: 0:0:0:0010::
- Letztes Präfix: 0:0:0:00F0::

› Präfix-Länge: 60

In diesem Beispiel delegiert der Router aus dem vom Provider dynamisch bezogenen Präfix „2001:db8:abcd:aa::/56“ jeweils Präfixe mit der Länge „/60“ von „2001:db8:abcd:aa10::“ bis „2001:db8:abcd:aaf0::“.

7.4.1.4 Reservierungen

Wenn Sie Clients feste IPv6-Adressen oder Routern feste Präfixe zuweisen wollen, können Sie in dieser Tabelle pro Client eine Reservierung vornehmen:



Interface-Name / Relay-IP

Name des Interfaces, auf dem der DHCPv6-Server arbeitet, z. B. „INTRANET“. Alternativ können Sie auch die IPv6-Adresse des entfernten Relay-Agenten eintragen.

Adresse / PD-Präfix

IPv6-Adresse oder PD-Präfix, das Sie statisch zuweisen wollen.

Identifier-Typ

Dieser Typ gibt an, wie der **Identifier** zu interpretieren ist.

Client-ID

Der Identifier gibt die Client-DUID an, z. B. 0003000100a057000001.

MAC-Adresse

Der Identifier gibt eine MAC-Adresse an, z. B. 00a057000001. Wenn der Client direkt mit dem Server kommuniziert, dann wird die MAC-Adresse aus dem DHCPv6-Paket genommen. Wenn Relay-Agents dazwischen sind, dann wird sie aus der Client-Link-Layer-Address-Option (Code 79, RFC 6939) der Relay-Forward-Message des client-nächsten Relay-Agents genommen.

Schnittstellen-ID

Der Identifier gibt die Schnittstellen-ID aus der Schnittstellen-ID-Option (Code 18) der Relay-Forward-Message des client-nächsten Relay-Agents an. Dies funktioniert nur mit einem Relay-Agent.

Remote-ID

Der Identifier gibt die Remote-ID aus der Remote-ID-Option (Code 37, RFC 4649) der Relay-Forward-Message des client-nächsten Relay-Agents an. Dies funktioniert nur mit einem Relay-Agent.

Identifier

Eindeutiger Bezeichner zur Identifizierung des DHCPv6-Clients. Der verwendete Typ zur Identifizierung wird durch den Parameter Identifier-Typ konfiguriert.

Mögliche Formate:

- Angabe als Client-DUID, z. B. 0003000100a057000001
- Angabe als MAC-Adresse z. B. 00a057000001
- Angabe als Interface-ID oder Remote-ID, z. B. „INTRANET“

Bevorzugte Gültigkeit

Bestimmen Sie hier die Zeit in Sekunden, die der Client diese Adresse als „bevorzugt“ verwenden soll. Nach Ablauf dieser Zeit führt ein Client diese Adresse als „deprecated“.

Gültigkeitsdauer

Bestimmen Sie hier die Zeit in Sekunden, die der Client diese Adresse als „gültig“ verwenden soll.

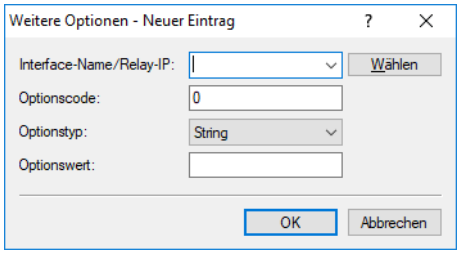
Wenn Sie ein Präfix eines WAN-Interfaces zur dynamischen Bildung der Adressen verwenden, ist das Konfigurieren der Werte **Bevorzugte Gültigkeit** und **Gültigkeitsdauer** gesperrt. In diesem Fall ermittelt das Gerät diese Werte automatisch aus den vorgegebenen Werte des delegierten Präfixes des Providers.

Präfix beziehen von

Name des WAN-Interfaces, von dem der Client das Präfix zur Adress- bzw. Präfixbildung verwenden soll.

7.4.1.5 DHCPv6-Optionen

Mithilfe dieses Features kann der DHCPv6-Server seinen DHCPv6-Clients beliebige DHCPv6-Optionen übertragen.



Interface-Name / Relay-IP

Bestimmt den Namen der IPv6-Schnittstelle bzw. die entfernte IPv6-Adresse eines Relay-Agenten, für die der DHCPv6-Server die weitere Option verteilen soll.

Damit diese Option auch an Clients ausgeliefert wird, muss der Client den entsprechenden Optionscode auch in seiner Anfrage erfragen.

Optionscode

Enthält den Code der DHCPv6-Option.

Optionstyp

Legt den Typ der DHCPv6-Option fest. Zur Auswahl stehen:

String

Übernimmt die Zeichen als String.

Alle weiteren Typen verwenden komma- und leerzeichenseparierte Listen, wobei leere Listenelemente ignoriert werden und eine leere Liste erlaubt ist und zu einer Option der Länge 0 führt.

Integertypen

Akzeptiert ganze Zahlen. Diese sind dezimal, oktal mit vorangestellter 0 und hexadezimal mit vorangestelltem 0x ohne Beachtung der Groß- / Kleinschreibung einzugeben. Der Wertebereich geht bei Integer8 von -128 bis 127, bei Integer16 von -32768 bis 32767 und bei Integer32 von -2147483648 bis 2147483647, jeweils inklusive. Ein Vorzeichen + oder - ist generell zulässig.

IPv6-Address

Akzeptiert IPv6-Adressen ohne Beachtung der Groß- / Kleinschreibung in allen zulässigen Darstellungen, inklusive der gemischten IPv4- / IPv6-Darstellung von Mapped-V4-Adressen (z. B. „::ffff:1.2.3.4“).

Domain-List

Akzeptiert alle Strings, die Labels ergeben, welche höchstens 63 Zeichen lang sind. Leere Labels sind erlaubt, werden aber ignoriert. Eine Domain-List endet immer mit dem leeren Label 0.

Hexdump

Erwartet in jedem Block nur Hexziffern ohne 0x-Präfix und füllt jeden Block ggf. mit einer führenden 0 zu gerader Länge auf und übernimmt anschließend den Block **Bigendian**.

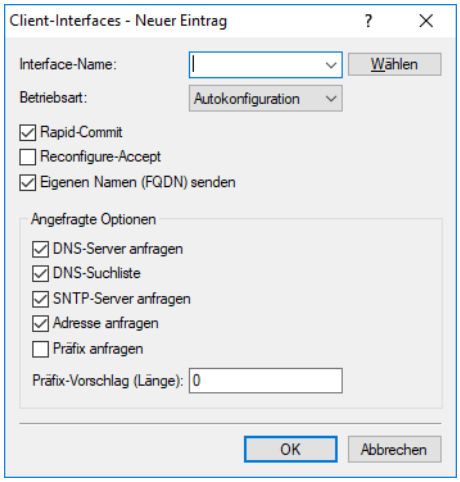
Optionswert

Enthält den Inhalt der DHCPv6-Option, formatiert entsprechend dem Optionstyp.

7.4.2 DHCPv6-Client

7.4.2.1 Client-Interfaces

Definieren Sie in dieser Tabelle das Verhalten des DHCPv6-Clients.



Normalerweise steuert bereits die Autokonfiguration das Client-Verhalten. Deshalb sind in dieser Tabelle nur Einträge nötig, falls Sie den Client *Standalone* betreiben oder bestimmte Optionen, die von den Standard-Einstellungen abweichen, verwenden wollen.

Interface-Name

Name des Interfaces, auf dem der DHCPv6-Client arbeitet Dies können LAN-Interfaces oder WAN-Interfaces (Gegenstellen) sein, z. B. „INTRANET“ oder „INTERNET“.

Betriebsart

Bestimmt, ob und wie das Gerät den Client aktiviert. Mögliche Werte sind:

Autokonfiguration

Das Gerät wartet auf Router-Advertisements und startet dann den DHCPv6-Client. Diese Option ist die Standardeinstellung.

Ein

Das Gerät startet den DHCPv6-Client sofort, sobald die Schnittstelle aktiv wird, ohne auf Router-Advertisements zu warten. Dabei ignoriert das Gerät die Vorgaben aus Router-Advertisements.

Aus

Der DHCPv6-Client ist auf diesem Interface deaktiviert. Auch, wenn das Gerät Router-Advertisements empfängt, startet es den Client nicht.

Rapid-Commit

Bei aktiviertem Rapid-Commit versucht der Client, mit nur zwei Nachrichten vom DHCPv6-Server eine IPv6-Adresse zu erhalten. Ist der DHCPv6-Server entsprechend konfiguriert, antwortet er auf diese Solicit-Anfrage sofort mit einer Reply-Nachricht.

Reconfigure-Accept

Wenn der Client mit dem Server beim ersten Kontakt erfolgreich eine Re-Konfiguration (Reconfigure) ausgehandelt hat, dann kann der Server den Client jederzeit auffordern, seine Adresse oder andere Informationen zu aktualisieren. Der Mechanismus wird durch den sogenannten *Reconfigure Key* geschützt, so dass nur der ursprüngliche Server mit dem richtigen Schlüssel den Client auffordern kann. Erhält der Client eine Reconfigure-Nachricht ohne gültigen Reconfigure-Key, so verwirft der Client diese Aufforderung zur Re-Konfiguration. Der Client unterstützt dazu das *Reconfigure Key Authentication Protocol* nach RFC 3315 für die Optionen „Renew" und „Information-Request", sowie „Rebind" nach RFC 6644.

Für WAN-Interfaces ist diese Option standardmäßig aktiviert.

Eigenen Namen (FQDN) senden

Der Client sendet den eigenen Hostnamen (Fully Qualified Domain Name). Diese Option ist standardmäßig auf LAN-Interfaces aktiv.

DNS-Server anfragen

Legt fest, ob der Client beim DHCPv6-Server nach DNS-Servern fragen soll.

Sie müssen diese Option aktivieren, damit das Gerät Informationen über einen DNS-Server erhält.

DNS-Suchliste

Der Client fragt die DNS-Suchliste an.

SNTP-Server anfragen

Legt fest, ob der DHCPv6-Client beim DHCPv6-Server eine Liste von SNTP-Servern (Simple Network Time Protocol) anfragt.

Hierzu muss das regelmäßige Synchronisieren mit einem Timeserver in *Konfiguration des Zeit-Servers unter LANconfig* aktiviert sein.

Adresse anfragen

Legt fest, ob der Client beim DHCPv6-Server nach einer IPv6-Adresse fragen soll.

Diese Option sollten Sie nur dann aktivieren, wenn der DHCPv6-Server die Adressen über dieses Interface stateful, d. h. nicht durch SLAAC, verteilt.

Präfix anfragen

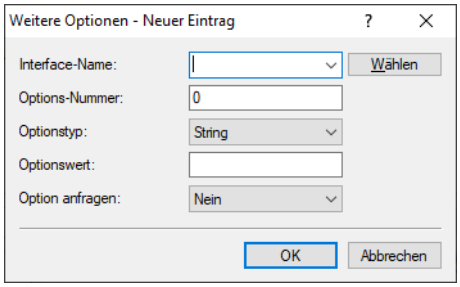
Legt fest, ob der DHCPv6-Client beim DHCPv6-Server eine gewünschte Präfix-Länge anfragt. Eine Aktivierung dieser Option ist nur dann sinnvoll, wenn das Gerät selber als Router arbeitet und Präfixe weiterverteilt. Auf WAN-Interfaces ist diese Option standardmäßig aktiviert, damit der DHCPv6-Client ein Präfix beim Provider anfragt, das er ins lokale Netzwerk weiterverteilen kann. Auf LAN-Interfaces ist diese Option standardmäßig deaktiviert, weil ein Gerät im lokalen Netzwerk eher als Client und nicht als Router arbeitet.

Präfix-Vorschlag (Länge)

Dies ist ein Vorschlag des Clients an den Server bezüglich der Länge des vom Server gewünschten Präfixes.

7.4.2.2 Weitere Optionen

Sie können für den DHCPv6-Client bestimmte Optionen konfigurieren, die dann übertragen werden. Dies ist erforderlich, wenn der Internet-Provider bestimmte Daten in DHCPv6-Nachrichten erwartet. Die Optionen können in der Tabelle DHCPv6-Optionen unter **IPv6** > **DHCPv6** > **DHCPv6-Client** > **Weitere Optionen** frei konfiguriert werden.



Interface-Name

Interface auf dem der DHCPv6-Client diese Option verwenden soll, z. B. WAN-Gegenstelle oder IPv6-LAN-Netzwerk.

Options-Nummer

Definiert die vergebene IANA-Nummer der DHCPv6-Option wie diese im RFC definiert ist.

Optionstyp

Definiert den Typ der DHCPv6-Option. Mögliche Werte: String, Integer8, Integer16, Integer32, IPv6-Adressen, Domain-List, Hexdump oder Dont-send

Der Options-Typ „Dont-send" bewirkt, dass kein Optionsinhalt gesendet wird, sondern nur die Optionsnummer im Option-Request, falls im RFC kein Optionswert vorgesehen ist.

Optionswert

Definiert den Inhalt der DHCPv6-Option

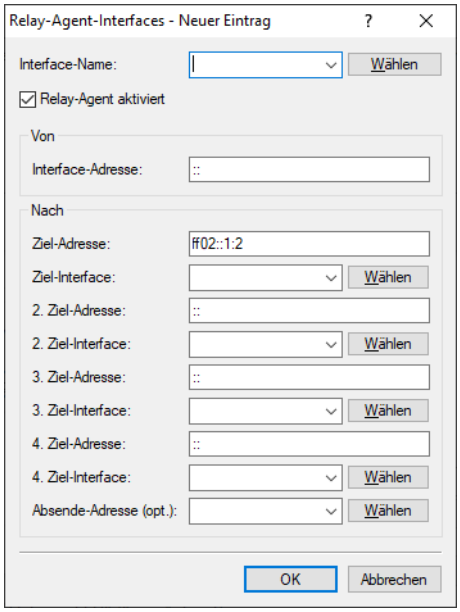
Dabei kann, außer bei String, auch eine Komma- und / oder Leerzeichen-separierte Liste angegeben werden. Für Integerwerte gelten die C-Codierungen für Zahlen, d. h. 0x ergibt einen Hexwert und wenn die Zahl mit 0 beginnt ist es ein Oktal-Wert. Zusätzlich kann beim Typ Integer8 auch ein einzelner Hex-String (mit gerader Länge) ohne Separator angegeben werden. Vorhandene Werte in den Standard-Optionen können überschrieben werden. Die folgenden Optionen können nicht überschrieben bzw. konfiguriert werden: Elapsed-Time, Server-DUID, Reconfigure-Accept und Rapid-Commit.

Option anfragen

Definiert, ob die Optionsnummer im DHCPv6-Request angefragt werden soll. Das Verhalten wird über das jeweilige RFC der DHCPv6-Option definiert. Mögliche Werte: Ja, Nein

7.4.3 DHCPv6-Relay-Agent

Ein DHCPv6-Relay-Agent leitet DHCP-Nachrichten zwischen DHCPv6-Clients und DHCPv6-Servern weiter, die sich in unterschiedlichen Netzwerken befinden. Definieren Sie in dieser Tabelle das Verhalten des DHCPv6-Relay-Agents.



Interface-Name

Name des Interfaces, auf dem der Relay-Agent Anfragen von DHCPv6-Clients entgegennimmt, z. B. „INTRANET".

Relay-Agent aktiviert

Aktiviert oder deaktiviert den Relay-Agent auf dem Gerät.

Interface-Adresse

Eigene IPv6-Adresse des Relay-Agents auf dem Interface, das unter Interface-Name konfiguriert ist. Diese IPv6-Adresse wird als Absenderadresse in den weitergeleiteten DHCP-Nachrichten verwendet. Über diese Absenderadresse kann ein DHCPv6-Server einen Relay-Agenten eindeutig identifizieren. Die explizite Angabe der Interface-Adresse ist nötig, da ein IPv6-Host durchaus mehrere IPv6-Adressen pro Schnittstelle haben kann.

Ziel-Adresse

IPv6-Adresse des (Ziel-) DHCPv6-Servers, an den der Relay-Agent DHCP-Anfragen weiterleiten soll. Die Adresse kann entweder eine Unicast- oder linklokale Multicast-Adresse sein. Bei Verwendung einer linklokalen Multicast-Adresse muss zwingend das Ziel-Interface angegeben werden, über das der DHCPv6-Server zu erreichen ist. Unter der linklokalen Multicast-Adresse „ff02::1:2" sind alle DHCPv6-Server und Relay-Agenten auf einem lokalen Link erreichbar.

Über die Parameter **2. Ziel-Adresse** bis **4. Ziel-Adresse** können Sie weitere Server-Ziele definieren.

Bei mehreren konfigurierten Server-Zielen werden die Anfragen immer an alle konfigurierten Server gleichzeitig gesendet.

Ziel-Interface

Das Ziel-Interface, über das der übergeordnete DHCPv6-Server oder der nächste Relay-Agent zu erreichen ist. Die Angabe ist zwingend erforderlich, wenn unter der Ziel-Adresse eine linklokale Multicast-Adresse konfiguriert wird, da linklokale Multicast-Adressen immer nur auf dem jeweiligen Link gültig sind.

Über die Parameter **2. Ziel-Interface** bis **4. Ziel-Interface** können Sie weitere Server-Ziele definieren.

Bei mehreren konfigurierten Server-Zielen werden die Anfragen immer an alle konfigurierten Server gleichzeitig gesendet.

Absende-Adresse (opt.)

Vergeben Sie hier eine optionale Absendeadresse an, die der Relay-Agent für Pakete in Richtung DHCPv6-Server verwendet.

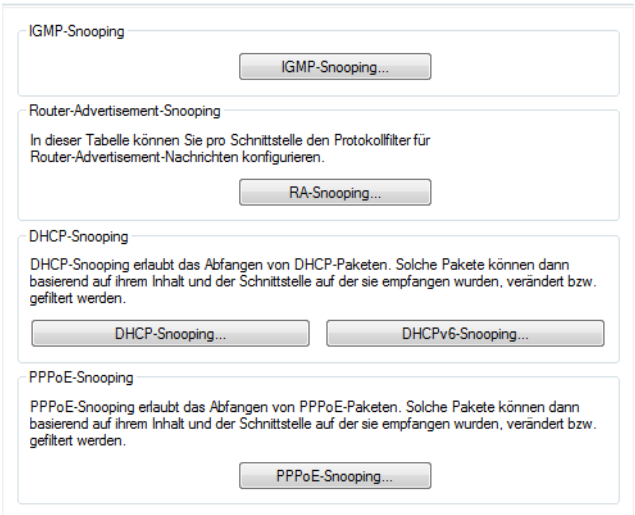
7.4.4 Lightweight-DHCPv6-Relay-Agent (LDRA)

Im Gegensatz zu einem DHCPv6-Relay-Agent, der über alle IPv6-Funktionen (wie z. B. ICMPv6) verfügt und Datenpakete im Netz routen kann (Layer 3), ermöglicht ein Lightweight-DHCPv6-Relay-Agent nach RFC 6221 nur die Erzeugung und Weitergabe von Relay-Agent-Informationen zwischen DHCPv6-Clients und DHCPv6-Servern (Layer 2).

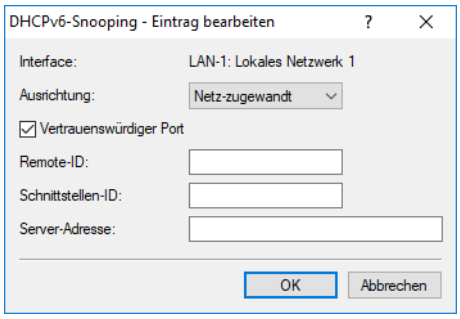
Anders als beim DHCPv4-Snooping fügt der LDRA den DHCPv6-Paketen nicht einfach Informationen zum Relay-Agent an, sondern er verpackt die Nachricht des Clients in eine eigene Option, stellt seinen Relay-Agent-Header voran und schickt erst anschließend dieses DCHPv6-Paket mit zusätzlichen Informationen an den DHCPv6-Server weiter (Relay Forward Message).

Der DHCPv6-Server wertet dieses Datenpaket aus und schickt eine gleichermaßen verpackte Antwort an den Relay-Agent. Der extrahiert die Nachricht und sendet sie an den anfragenden Client (Relay Reply Message).

Im LANconfig können Sie das DHCPv6-Snooping unter **Schnittstellen** > **Snooping** mit einem Klick auf **DHCPv6-Snooping** für jede Schnittstelle separat festlegen.



Nach Auswahl der entsprechenden Schnittstelle können Sie die folgenden Einstellungen festlegen:



Ausrichtung

Hier aktivieren bzw. deaktivieren Sie das DHCPv6-Snooping. Die folgende Auswahl ist möglich:

- **netz-zugewandt**: Über diese Schnittstelle kommuniziert der LDRA mit einem DHCPv6-Server.
- **client-zugewandt**: Über diese Schnittstelle kommuniziert der LDRA mit den ans Netz angeschlossenen DHCPv6-Clients.

In der Werkseinstellung **netz-zugewandt** ist der LDRA deaktiviert.

Vertrauenswürdiger Port

Der LDRA leitet sowohl DHCP-Anfragen von Clients als auch DHCP-Antworten von DHCP-Servern weiter, wenn diese Option aktiviert ist. Ist diese Schnittstelle als nicht vertrauenswürdig eingestuft, verwirft der LDRA DHCPv6-Anfragen an dieser Schnittstelle. DHCPv6-Antworten, die nicht die korrekte Interface-ID enthalten, leitet der LDRA ebenfalls nicht an den Client weiter.

Remote-Id

Die Remote-ID nach RFC 4649 kennzeichnet eindeutig den Client, der eine DHCPv6-Anfrage stellt.

Schnittstellen-Id

Die Interface-ID kennzeichnet eindeutig die Schnittstelle, über die ein Client eine DHCPv6-Anfrage stellt.

Server-Adresse

Hier können Sie die IPv6-Adresse eines DHCPv6-Servers festlegen.



Lassen Sie dieses Feld leer, wenn Sie Antworten von allen DHCPv6-Servern im Netz erhalten wollen. Ansonsten reagiert der LDRA nur auf DHCPv6-Antworten des Servers, dessen Adresse Sie angegeben haben. Antworten von anderen DHCPv6-Servern verwirft der LDRA in diesem Fall.

Sie können für **Remote-Id** und **Schnittstellen-Id** die folgenden Variablen verwenden:

- `%%`: fügt ein Prozent-Zeichen ein.
- `%c`: fügt die MAC-Adresse der Schnittstelle ein, auf der der Relay-Agent den DHCP-Request erhalten hat. Handelt es sich um eine WLAN-SSID, ist das die entsprechende BSSID.
- `%i`: fügt den Namen der Schnittstelle ein, auf der der Relay-Agent den DHCP-Request erhalten hat.
- `%n`: fügt den Namen des DHCP-Relay-Agents ein, wie er z. B. unter **Setup** > **Name** festgelegt ist.
- `%v`: fügt die VLAN-ID des DHCP-Request-Pakets ein. Diese VLAN-ID stammt entweder direkt aus dem VLAN-Header des DHCP-Datenpakets oder aus der VLAN-ID-Zuordnung für diese Schnittstelle.
- `%p`: fügt den Namen der Ethernet-Schnittstelle ein, die das DHCP-Datenpaket empfangen hat. Diese Variable ist hilfreich bei Geräten mit eingebautem Ethernet-Switch oder Ethernet-Mapper, da diese mehr als eine physikalische Schnittstelle auf eine logische Schnittstelle mappen können. Bei anderen Geräten sind `%p` und `%i` identisch.
- `%s`: fügt die WLAN-SSID ein, wenn das DHCP-Paket von einem WLAN-Client stammt. Bei anderen Clients enthält diese Variable einen leeren String.
- `%e`: fügt die Seriennummer des Relay-Agents ein, wie sie z. B. unter **Management** > **Allgemein** zu finden ist.

7.5 IPv6-Firewall

7.5.1 Funktion

Während die IPv4-Firewall ausschließlich das Forwarding der IP-Daten kontrolliert, regelt die IPv6-Firewall auch die Funktionen der Access-Listen aller IPv6-Server-Dienste. Die IPv6-Firewall entspricht damit eher dem klassischen Design von Firewalls, die die Inbound- und Outbound-Kommunikation sowie das Forwarding separat unterstützen. Da im Gerät dessen Konfiguration gezielt die Kommunikation steuert, verzichtet das Gerät auf eine Outbound-Firewall.

7.5.2 Konfiguration

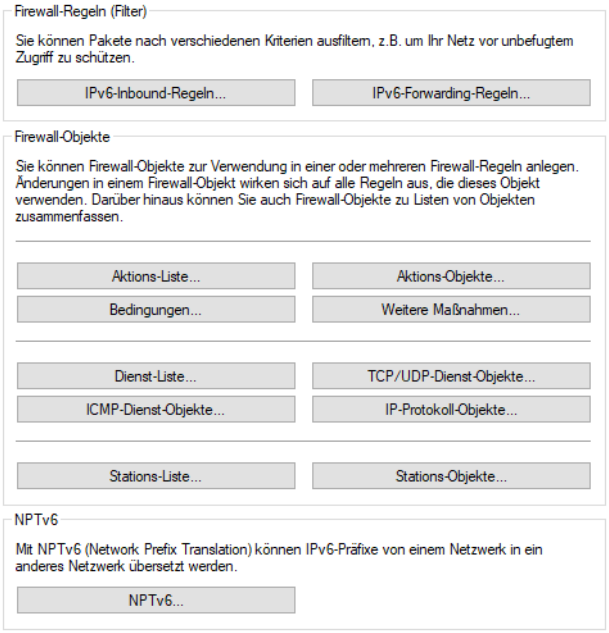
Die Konfiguration der IPv6-Firewall entspricht weitgehend der Konfiguration der IPv4-Firewall, erfolgt jedoch getrennt von dieser.

Die Inbound- und Forwarding-Firewall verfügen jeweils über eine eigene Regeltabelle, die sich in Umfang und Aufbau an die entsprechende Regelstruktur der IPv4-Firewall anlehnen.

Die Regeln sind nach absteigender Priorität sortiert, d. h., die Regel mit der höchsten Priorität steht in der Liste oben. Bei gleicher Priorität erfolgt eine Sortierung anhand der Genauigkeit analog zur Verfahrensweise bei IPv4. Falls die Regel vorgibt, weitere Regeln zu beachten, führt die Firewall der Reihe nach auch die nachfolgenden Filterregeln aus. Ansonsten beendet die Firewall die Filterung, nachdem sie die aktuell zutreffende Regel angewendet hat.

7.5.2.1 Konfiguration der IPv6-Firewall-Regeln

Mit LANconfig können Sie die Firewall-Regeln unter **Firewall/QoS** > **IPv6-Regeln** festlegen.



Standardmäßig sind bereits einige Objekte und Listen für die wichtigsten Anwendungsfälle vorgegeben.

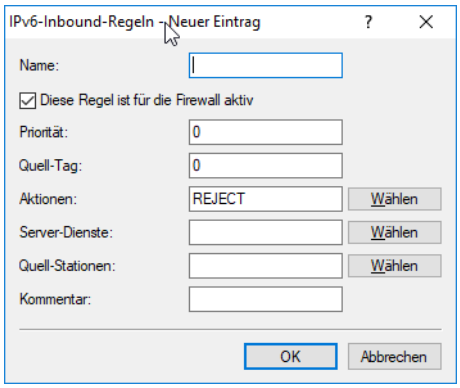
Sie können Listen oder Objekte nicht löschen, wenn die Firewall diese in einer Forwarding- oder Inbound-Regel verwendet.

IPv6-Inbound-Regeln

Über die Schaltfläche **IPv6-Inbound-Regeln** legen Sie Regeln fest, nach denen die IPv6-Firewall den ankommenden Datenverkehr behandeln soll.

Standardmäßig sind bereits einige Regeln für die wichtigsten Anwendungsfälle vorgegeben.

Klicken Sie auf **Hinzufügen**, um eine neue Regel festzulegen.



Sie können die folgenden Eigenschaften der Regel bestimmen:

Name

Bestimmt den Namen der Regel.

Diese Regel ist für die Firewall aktiv

Aktiviert die Regel.

Priorität

Bestimmt die Priorität der Regel: Je höher der Wert, desto höher die Priorität.

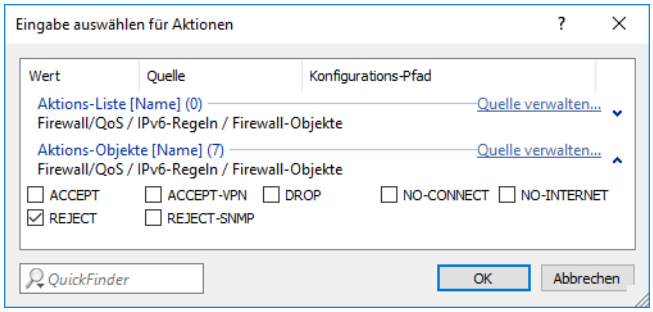
Quell-Tag

Geben Sie hier ein Schnittstellen- bzw. Routing-Tag an (Tag-Kontext), wenn die Regel nur für derart markierte Pakete gelten soll. Der Standard-Wert 0 bedeutet, dass diese Regel für alle Pakete ungeachtet des Schnittstellen- bzw. Routing-Tags gilt.

Sollen tatsächlich nur Pakete mit dem Schnittstellen- bzw. Routing-Tag 0 beachtet werden, so muss hier 65535 angegeben werden.

Aktionen

Bestimmt die Aktion, die die Firewall bei gültiger Regel ausführen soll. Über **Wählen** können Sie aus einer Liste eine Aktion oder eine Aktions-Liste auswählen.



Wenn Sie hier einen neuen Eintrag eingeben, taucht dieser zunächst unter **Unbekannte Quelle** auf. Markieren Sie anschließend den Eintrag einer Quelle, der Sie den neuen Eintrag zuordnen möchten und klicken

anschließend auf **Quelle verwalten**. Bestimmen Sie die Werte für diesen Eintrag, und speichern Sie das neue Objekt. Der neue Eintrag taucht nun als neues Objekt in der Liste der entsprechenden Quelle auf.

Server-Dienste

Bestimmt die Dienste, auf die die Firewall die Regel anwenden soll. Über **Wählen** können Sie aus einer Liste einen Dienst oder eine Dienste-Liste auswählen.

Quell-Stationen

Bestimmt die Quell-Stationen, auf die die Firewall die Regel anwenden soll. Über **Wählen** können Sie aus einer Liste einen Station oder eine Stations-Liste auswählen.

Kommentar

Vergeben Sie hier eine aussagefähige Beschreibung der Filterregel.

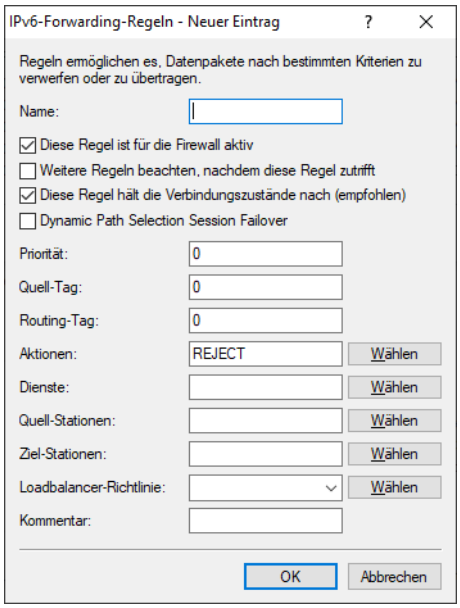
IPv6-Forwarding-Regeln

Über die Schaltfläche **IPv6-Forwarding-Regeln** legen Sie Regeln fest, nach denen die IPv6-Firewall den weiterzuleitenden Datenverkehr behandeln soll.

Standardmäßig sind bereits einige Regeln für die wichtigsten Anwendungsfälle vorgegeben.

Um die Reihenfolge der Regeln zu ändern, markieren Sie in der Tabelle die entsprechende Regel und verschieben diese über einen Klick auf eine Pfeil-Schaltfläche nach oben oder unten in der Tabelle. Die Firewall wendet die Regel nacheinander von oben nach unten an.

Klicken Sie auf **Hinzufügen**, um eine neue Regel festzulegen.



Sie können die folgenden Eigenschaften der Regel bestimmen:

Name

Bestimmt den Namen der Regel.

Diese Regel ist für die Firewall aktiv

Aktiviert die Regel.

Weitere Regeln beachten, nachdem diese Regel zutrifft

Wenn Sie diese Option aktivieren, führt die Firewall zusätzlich die nachfolgenden Regeln der Liste aus. Das ist dann sinnvoll, wenn die Firewall z. B. zunächst eine Gruppen-Regel und anschließend jeweils eine Regel für die einzelnen Gruppen-Objekte anwenden soll.

Diese Regel hält die Verbindungszustände nach (empfohlen)

Aktivieren Sie diese Option, wenn die Regel die TCP-Verbindungszustände nachhalten soll.

Dynamic Path Selection Session Failover

Gibt an, ob die Sessions dieser Regeln im Falle einer besseren Leitung bei Verwendung von Dynamic Path Selection auf diese verschoben werden sollen. Dies ist nur für umaskierte Verbindungen, z. B. VPN-Verbindungen möglich. Siehe auch *Switchover-Profile* auf Seite 446.

Priorität

Bestimmt die Priorität der Regel: Je höher der Wert, desto höher die Priorität.

Quell-Tag

Geben Sie hier ein Schnittstellen- bzw. Routing-Tag an (Tag-Kontext), wenn die Regel nur für derart markierte Pakete gelten soll. Der Standard-Wert 0 bedeutet, dass diese Regel für alle Pakete ungeachtet des Schnittstellen- bzw. Routing-Tags gilt.

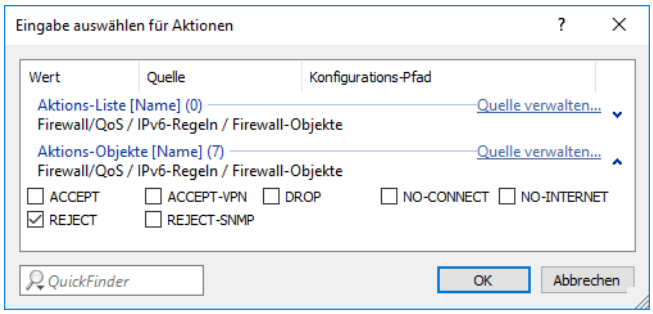
Sollen tatsächlich nur Pakete mit dem Schnittstellen- bzw. Routing-Tag 0 beachtet werden, so muss hier 65535 angegeben werden.

Routing-Tag

Tragen Sie hier als Schnittstellen-Tag einen Wert ein, der das Netzwerk eindeutig spezifiziert. Alle Pakete, die das Gerät auf diesem Netzwerk empfängt, erhalten intern eine Markierung mit diesem Tag. Das Schnittstellen-Tag ermöglicht eine Trennung der für dieses Netzwerk gültigen Routen.

Aktionen

Bestimmt die Aktion, die die Firewall bei gültiger Regel ausführen soll. Über **Wählen** können Sie aus einer Liste eine Aktion oder eine Aktions-Liste auswählen.



Wenn Sie hier einen neuen Eintrag eingeben, taucht dieser zunächst unter **Unbekannte Quelle** auf. Markieren Sie anschließend den Eintrag einer Quelle, der Sie den neuen Eintrag zuordnen möchten und klicken anschließend auf **Quelle verwalten**. Bestimmen Sie die Werte für diesen Eintrag, und speichern Sie das neue Objekt. Der neue Eintrag taucht nun als neues Objekt in der Liste der entsprechenden Quelle auf.

Dienste

Bestimmt die Dienste, auf die die Firewall die Regel anwenden soll. Über **Wählen** können Sie aus einer Liste einen Dienst oder eine Dienste-Liste auswählen.

Quell-Stationen

Bestimmt die Quell-Stationen, auf die die Firewall die Regel anwenden soll. Über **Wählen** können Sie aus einer Liste einen Station oder eine Stations-Liste auswählen.

Ziel-Stationen

Bestimmt die Ziel-Stationen, auf die die Firewall die Regel anwenden soll. Über **Wählen** können Sie aus einer Liste einen Station oder eine Stations-Liste auswählen.

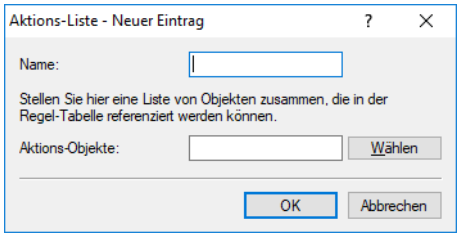
Kommentar

Vergeben Sie hier eine aussagefähige Beschreibung der Filterregel.

Aktions-Liste

Über die Schaltfläche **Aktions-Liste** können Sie Aktionen zu Gruppen zusammenfassen. Die Aktionen definieren Sie vorher unter **Aktions-Objekte**.

Klicken Sie auf **Hinzufügen**, um eine neue Regel festzulegen.



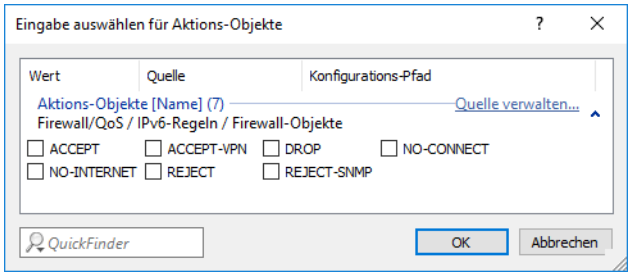
Sie können die folgenden Eigenschaften einer Liste festlegen:

Name

Bestimmt den Namen der Liste.

Aktions-Objekte

Bestimmt die Objekte, die Sie in dieser Liste zusammenfassen möchten. Über **Wählen** können Sie aus einer Liste ein oder mehrere Objekte auswählen.

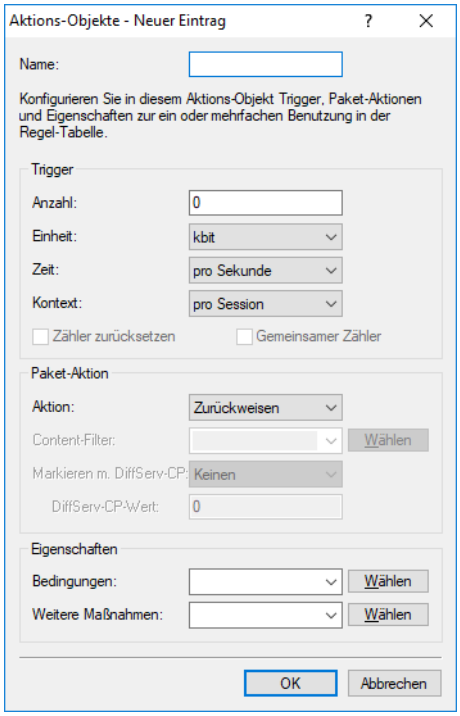


Wenn Sie hier einen neuen Eintrag eingeben, taucht dieser zunächst unter **Unbekannte Quelle** auf. Markieren Sie anschließend den Eintrag einer Quelle, der Sie den neuen Eintrag zuordnen möchten und klicken anschließend auf **Quelle verwalten**. Bestimmen Sie die Werte für diesen Eintrag, und speichern Sie das neue Objekt. Der neue Eintrag taucht nun als neues Objekt in der Liste der entsprechenden Quelle auf.

Aktions-Objekte

Über die Schaltfläche **Aktions-Objekte** definieren Sie Aktionen, die die IPv6-Firewall bei gültiger Filterregel ausführen kann.

Klicken Sie auf **Hinzufügen**, um eine neue Aktion festzulegen.



Sie können die folgenden Eigenschaften des Objektes bestimmen:

Name

Bestimmt den Namen des Objektes.

Anzahl

Bestimmt das Limit, bei dessen Überschreiten die Firewall die Aktion ausführt.

Einheit

Bestimmt die Einheit des Limits. Wählen Sie im Drop-Down-Menü den entsprechenden Wert aus.

Zeit

Bestimmt, für welchen Messzeitraum die Firewall das Limit ansetzt. Wählen Sie im Drop-Down-Menü den entsprechenden Wert aus.

Kontext

Bestimmt, in welchem Kontext die Firewall das Limit ansetzt. Wählen Sie im Drop-Down-Menü den entsprechenden Wert aus.

Zähler zurücksetzen

Wenn Sie diese Option aktivieren, setzt die Firewall den Zähler nach Ausführen der Aktion wieder zurück.

Diese Option können Sie nur aktivieren, wenn Sie unter **Zeit** den Wert „absolut" ausgewählt haben.

Gemeinsamer Zähler

Wenn Sie diese Option aktivieren, zählt die Firewall alle Aktions-Trigger gemeinsam.

Diese Option können Sie nur aktivieren, wenn Sie unter **Kontext** die Werte „pro Station" oder „global" ausgewählt haben.

Aktion

Bestimmt die Aktion, die die Firewall bei Erreichen des Limits ausführt.

Die folgende Auswahl ist möglich:

Zurückweisen

Die Firewall weist das Datenpaket zurück und sendet einen entsprechenden Hinweis an den Absender.

Verwerfen

Die Firewall verwirft das Datenpaket ohne Benachrichtigung.

Übertragen

Die Firewall akzeptiert das Datenpaket.

Prüfen durch Proxy

Der Proxy überprüft das Datenpaket.

Content-Filter

Das Profil des Content Filters. Siehe *Firewall-Einstellungen für den Content Filter* auf Seite 1706

Markieren mit DiffServ-CP

Bestimmt die Priorität der Datenpakete (Differentiated Services, DiffServ), mit der die Firewall die Datenpakete übertragen soll.

Diese Option können Sie nur festlegen, wenn Sie unter **Aktion** den Wert „Übertragen" ausgewählt haben.

Weitere Informationen zu den DiffServ-CodePoints finden Sie im Kapitel *Quality-of-Service* auf Seite 696.

DiffServ-CP-Wert

Bestimmt den Wert für den Differentiated Services Code Point (DSCP).

Diese Option können Sie nur festlegen, wenn Sie unter **Markieren mit DiffServ-CP** die Option „Wert" ausgewählt haben.

Bedingungen

Bestimmt, welche Bedingungen zusätzlich zur Ausführung der Aktion erfüllt sein müssen. Die Bedingungen können Sie unter *Bedingungen* auf Seite 623 definieren.

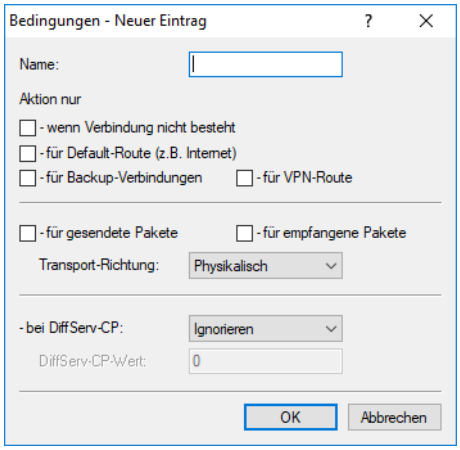
Weitere Maßnahmen

Bestimmt, welche Trigger-Aktionen die Firewall zusätzlich zur Filterung der Datenpakete starten soll. Die Trigger-Aktionen können Sie unter *Weitere Maßnahmen* auf Seite 625 definieren.

Bedingungen

Über die Schaltfläche **Bedingungen** definieren Sie Bedingungen, die zum Anwenden der Forwarding- und Inbound-Regeln erfüllt sein müssen.

Klicken Sie auf **Hinzufügen**, um eine neue Bedingung festzulegen.



Sie können die folgenden Eigenschaften der Bedingung bestimmen:

Name

Bestimmt den Namen des Objektes.

Aktion nur – wenn Verbindung nicht besteht

Aktivieren Sie diese Option, wenn die Firewall die Aktion nur ausführen soll, wenn keine Verbindung besteht.

Aktion nur – für Default-Route (z. B. Internet)

Aktivieren Sie diese Option, wenn die Firewall die Aktion nur ausführen soll, wenn die Verbindung über die Default-Route besteht.

Aktion nur – für Backup-Verbindungen

Aktivieren Sie diese Option, wenn die Firewall die Aktion nur ausführen soll, wenn es sich um eine Backup-Verbindung handelt.

Aktion nur – für VPN-Route

Aktivieren Sie diese Option, wenn die Firewall die Aktion nur ausführen soll, wenn es sich um eine VPN-Verbindung handelt.

Aktion nur – für gesendete Pakete

Aktivieren Sie diese Option, wenn die Firewall die Aktion nur ausführen soll, wenn es sich um gesendete Datenpakete handelt.

Aktion nur – für empfangene Pakete

Aktivieren Sie diese Option, wenn die Firewall die Aktion nur ausführen soll, wenn es sich um empfangene Datenpakete handelt.

Transport-Richtung

Bestimmt, ob die Transportrichtung sich auf den logischen Verbindungsaufbau oder die physikalische Datenübertragung über das jeweilige Interface bezieht.

Aktion nur – bei DiffServ-CP

Bestimmt, welche Priorität die Datenpakete (Differentiated Services, DiffServ) besitzen müssen, damit die Bedingung erfüllt ist.

Weitere Informationen zu den DiffServ-CodePoints finden Sie im Kapitel *Quality-of-Service* auf Seite 696.

DiffServ-CP-Wert

Bestimmt den Wert für den Differentiated Services Code Point (DSCP).

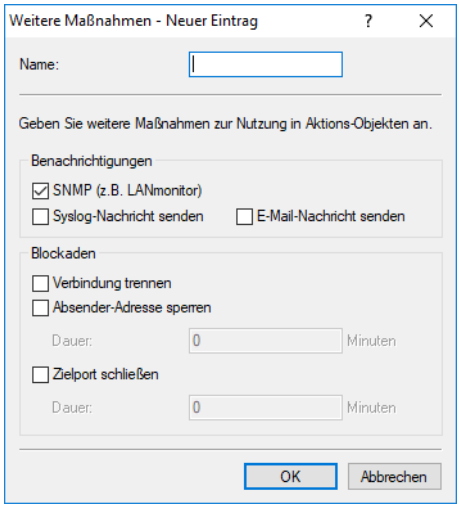
Geben Sie hier einen Wert ein, wenn Sie im Feld **bei DiffServ-CP** die Option "Wert" ausgewählt haben.

Weitere Informationen zu den DiffServ-CodePoints finden Sie im Kapitel *Quality-of-Service* auf Seite 696.

Weitere Maßnahmen

Über die Schaltfläche **Weitere Maßnahmen** definieren Sie weitere Maßnahmen, die die Firewall nach Anwenden der Forwarding- und Inbound-Regeln ausführen kann.

Klicken Sie auf **Hinzufügen**, um eine neue Maßnahme festzulegen.



Sie können die folgenden Eigenschaften der Trigger-Aktion bestimmen:

Name

Bestimmt den Namen des Objektes.

SNMP (z. B. LANmonitor)

Aktivieren Sie diese Option, wenn die Firewall eine Benachrichtigung über SNMP versenden soll. Diese Benachrichtigung können Sie z. B. mit LANmonitor empfangen.

SYSLOG-Nachricht senden

Aktivieren Sie diese Option, wenn die Firewall eine SYSLOG-Nachricht versenden soll.

Weitere Informationen zu SYSLOG finden Sie im Abschnitt *Das SYSLOG-Modul* auf Seite 323.

E-Mail-Nachricht senden

Aktivieren Sie diese Option, wenn die Firewall eine E-Mail-Nachricht versenden soll.

Wenn Sie eine Benachrichtigung per E-Mail erhalten möchten, müssen Sie unter **Firewall/QoS** > **Allgemein** > **Administrator E-Mail** eine entsprechende E-Mail-Adresse angeben.

Verbindung trennen

Aktivieren Sie diese Option, wenn die Firewall die Verbindung trennen soll.

Absender-Adresse sperren

Aktivieren Sie diese Option, wenn die Firewall die Absender-Adresse sperren soll. Die Firewall trägt die gesperrte IP-Adresse, die Sperrzeit sowie die zugrunde liegende Regel in die **Hostsperrliste** unter **Status** > **IPv6** > **Firewall** ein.

Dauer

Wenn die Firewall den Absender sperren soll, können Sie hier die Dauer der Sperrung in Minuten festlegen. Der Wert 0 deaktiviert die Sperre, da die Sperrzeit praktisch nach 0 Minuten abläuft.

Zielport schließen

Aktivieren Sie diese Option, wenn die Firewall den Ziel-Port sperren soll. Die Firewall trägt die gesperrte Ziel-IP-Adresse, das Protokoll, den Ziel-Port, die Sperrzeit sowie die zugrunde liegende Regel in die **Portsperrliste** unter **Status** > **IPv6** > **Firewall** ein.

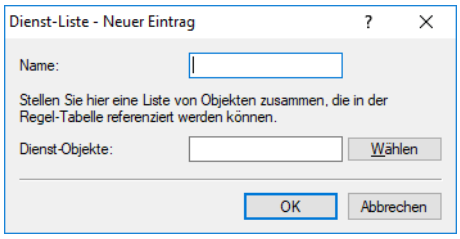
Dauer

Wenn die Firewall den Zielport schließen soll, können Sie hier die Dauer der Sperrung in Minuten festlegen. Der Wert 0 deaktiviert die Sperre, da die Sperrzeit praktisch nach 0 Minuten abläuft.

Dienst-Liste

Über die Schaltfläche **Dienst-Liste** können Sie Dienste zu Gruppen zusammenfassen. Die Dienste definieren Sie vorher unter **TCP/UDP-Dienst-Objekte**, **ICMP-Dienst-Objekte** und **IP-Protokoll-Objekte**.

Klicken Sie auf **Hinzufügen...**, um eine neue Dienst-Liste festzulegen.



Sie können die folgenden Eigenschaften einer Liste festlegen:

Name

Bestimmt den Namen der Liste.

Dienst-Objekte

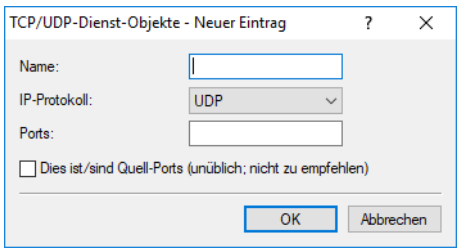
Bestimmt die Objekte, die sie in dieser Liste zusammenfassen möchten. Über **Wählen** können Sie aus einer Liste ein oder mehrere Objekte auswählen.

Wenn Sie hier einen neuen Eintrag eingeben, taucht dieser zunächst unter **Unbekannte Quelle** auf. Markieren Sie anschließend den Eintrag einer Quelle, der Sie den neuen Eintrag zuordnen möchten und klicken anschließend auf **Quelle verwalten**. Bestimmen Sie die Werte für diesen Eintrag, und speichern Sie das neue Objekt. Der neue Eintrag taucht nun als neues Objekt in der Liste der entsprechenden Quelle auf.

TCP/UDP-Dienst-Objekte

Über die Schaltfläche **TCP/UDP-Dienst-Objekte** definieren Sie TCP/UDP-Dienste, die die IPv6-Firewall für Filterregeln verwenden kann.

Klicken Sie auf **Hinzufügen**, um einen neuen Dienst festzulegen.



Sie können die folgenden Eigenschaften der Regel bestimmen:

Name

Bestimmt den Namen des Objektes.

IP-Protokoll

Bestimmt das Protokoll des Dienstes

Ports

Bestimmt die Ports des Dienstes. Trennen Sie mehrere Ports jeweils durch ein Komma.

Listen mit den offiziellen Protokoll- und Portnummern finden Sie im Internet unter *www.iana.org*.

Dies ist/sind Quell-Ports

Bestimmt, ob es sich bei den angegebenen Ports um Quell-Ports handelt.

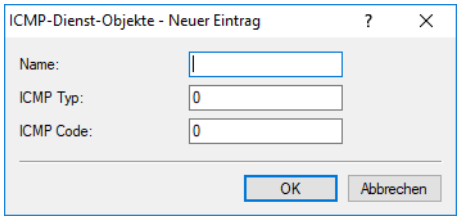
In bestimmten Szenarien kann es sinnvoll sein, einen Quell-Port anzugeben. Normalerweise ist es aber unüblich, so dass die Auswahl nicht zu empfehlen ist.

ICMP-Dienst-Objekte

Über die Schaltfläche **ICMP-Dienst-Objekte** definieren Sie ICMP-Dienste, die die IPv6-Firewall für Filterregeln verwenden kann.

Listen mit den offiziellen ICMP-Typen und -Codes finden Sie im Internet unter *www.iana.org*.

Klicken Sie auf **Hinzufügen**, um einen neuen Dienst festzulegen.



Sie können die folgenden Eigenschaften der Regel bestimmen:

Name

Bestimmt den Namen des Objektes.

ICMP Typ

Bestimmt den Typ des ICMP-Dienstes.

ICMP Code

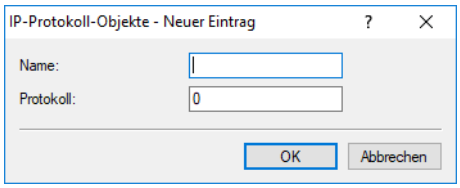
Bestimmt den Code des ICMP-Dienstes.

IP-Protokoll-Objekte

Über die Schaltfläche **IP-Protokoll-Objekte** definieren Sie Internet-Protokoll-Objekte, die die IPv6-Firewall für Filterregeln verwenden kann.

Listen mit den offiziellen Protokoll- und Portnummern finden Sie im Internet unter *www.iana.org*.

Klicken Sie auf **Hinzufügen**, um ein neues Objekt festzulegen.



Sie können die folgenden Eigenschaften der Regel bestimmen:

Name

Bestimmt den Namen des Objektes.

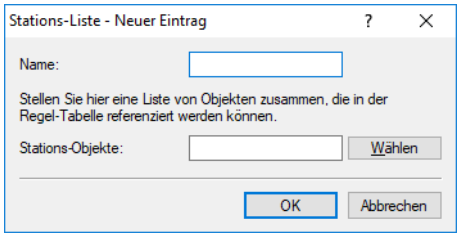
Protokoll

Bestimmt die Protokoll-Nummer.

Stations-Liste

Über die Schaltfläche **Stations-Liste** können Sie Stationen zu Gruppen zusammenfassen. Die Stationen definieren Sie vorher unter **Stations-Objekte**.

Klicken Sie auf **Hinzufügen**, um eine neue Liste festzulegen.



Sie können die folgenden Eigenschaften einer Liste festlegen:

Name

Bestimmt den Namen der Liste.

Stations-Objekte

Bestimmt die Objekte, die sie in dieser Liste zusammenfassen möchten. Über **Wählen** können Sie aus einer Liste ein oder mehrere Objekte auswählen.

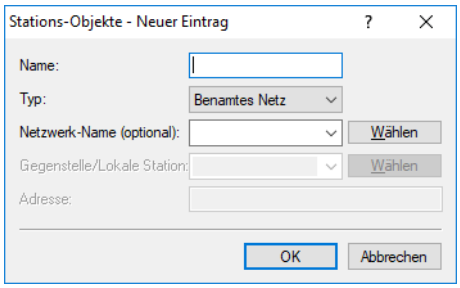
Wenn Sie hier einen neuen Eintrag eingeben, taucht dieser zunächst unter **Unbekannte Quelle** auf. Markieren Sie anschließend den Eintrag einer Quelle, der Sie den neuen Eintrag zuordnen möchten und klicken

anschließend auf **Quelle verwalten**. Bestimmen Sie die Werte für diesen Eintrag, und speichern Sie das neue Objekt. Der neue Eintrag taucht nun als neues Objekt in der Liste der entsprechenden Quelle auf.

Stations-Objekte

Über die Schaltfläche **Stations-Objekte** definieren Sie Stationen, die die IPv6-Firewall für Filterregeln verwenden kann.

Klicken Sie auf **Hinzufügen**, um ein neues Objekt anzulegen.



Sie können die folgenden Eigenschaften der Objekte festlegen:

Name

Bestimmt den Namen des Objektes.

Typ

Bestimmt den Stationstyp. Von der Auswahl hängt ab, welche der nachfolgenden Tabellenspalten (**Netzwerk-Name**, **Gegenstelle/Lokale Station** und **Adresse/Präfix**) ausgefüllt werden müssen. Mögliche Werte:

Benanntes Netz

Name eines lokalen Netzwerks z. B. INTRANET.

- Nur die Spalte **Netzwerk-Name** ist auszufüllen.
- Sie kann einen Interface-Namen enthalten, dann besteht die Station aus allen Netzen an diesem Interface.
- Falls Sie eine Netzwerk-Gruppe eintragen, dann besteht die Station aus allen Präfixen unter *IPv6-Adressen* auf Seite 585 mit dieser Gruppe.

Gegenstelle

Name einer WAN-Gegenstelle z. B. INTERNET.

- Nur die Spalte **Gegenstelle/Lokale Station** ist auszufüllen.
- Sie kann ein WAN-Interface oder ein RAS-Template enthalten und löst zu allen Präfixen / Netzen auf, zu denen eine Route über dieses WAN-Interface oder über ein RAS-Interface zu diesem Template existiert.

Netzwerk-Präfix

IPv6-Präfix

- Nur die Spalte **Adresse/Präfix** ist auszufüllen.
- Sie enthält ein IPv6-Präfix, z. B. „2001:db8::/32“.

Host-Identifier bzw. Interface Identifier

- Die Spalten **Netzwerk-Name** und **Adresse/Präfix** sind beide auszufüllen
- **Netzwerk-Name** enthält ein WAN-Interface oder ein RAS-Template.
- **Adresse/Präfix** enthält einen IPv6-Identifier. Dies sind die letzten 64 Bit der IPv6-Adresse eines IPv6-Hosts, z. B. „::2a0:57ff:fe1b:3a6a“. Der Wert muss zwei führende Doppelpunkte enthalten.

- Dieser Identfier wird mit allen Netzen des Interfaces unter **Netzwerk-Name** bzw. den Netzwerken des RAS-Interfaces zum angegebenen Template zu einer Adresse kombiniert.
- Außerdem wird zu jedem dieser Interfaces eine link-lokale Adresse mit diesem Identifier gebildet.

IP-Adresse

- Nur die Spalte **Adresse/Präfix** ist auszufüllen.
- Sie enthält eine IPv6-Adresse, z. B. „2001:db8::1“

Lokale Station

Name eines lokalen IPv6-Hosts bzw. einer lokalen Station.

- Die Spalte **Gegenstelle/Lokale Station** ist auszufüllen und enthält einen Hostnamen.
- Die Spalte **Netzwerk-Name** ist optional und kann ein LAN-Interface enthalten.
- Der Hostname wird mit Hilfe des DHCPv6-Servers oder des DNS-Servers im Gerät zu einer Hostadresse aufgelöst.
- Wenn ein Interface angegeben wurde, dann wird die Adresse nur genommen, falls sie über dieses Interface erreicht wird.

MAC-Adresse

Damit können Regeln für Ressourcen im internen Netzwerk angelegt werden, die anhand ihrer MAC-Adresse identifiziert werden. In Dual-Stack-Netzwerken erleichtert dies die Korrelation zu IPv4-Stationsobjekten, die ebenfalls anhand ihrer MAC-Adresse mit einer IPv4-Regel behandelt werden.

- Die Spalte **Netzwerk-Name** ist optional und kann einen Netzwerknamen enthalten, in dem sich das Stations-Objekt befindet.
- Die Spalte **Adresse/Präfix** enthält die MAC-Adresse anhand derer das Objekt identifiziert werden soll.

MAC-Adressen sind nur in Regeln als Quelle erlaubt, nicht jedoch als Ziel.

Delegiertes Präfix

Damit kann insbesondere im Falle eines dynamischen Provider-Präfixes eine Regel für nachgeschaltete Router oder Ressourcen definiert werden.

- Die Spalte **Netzwerk-Name** ist optional und kann einen Netzwerknamen enthalten, in dem sich das Stations-Objekt befindet. Dies kann als Einschränkung auf das lokale Netzwerk verwendet werden.
- Die Spalte **Gegenstelle/Lokale Station** ist erforderlich und sollte die Gegenstelle enthalten, von der das delegierte Präfix bezogen bzw. abgeleitet wird.
- Die Spalte **Adresse/Präfix** enthält ein Präfix oder eine Adresse, die mit dem vom Provider bezogenen Präfix verknüpft (Oder-Verknüpfung) wird. Wenn sich das Objekt auf das gesamte Präfix beziehen soll, so kann entweder ::/0 konfiguriert werden oder der Eintrag leer gelassen werden.

  Beispiel: Der Provider delegiert das Präfix 2001:db8:1234::/48 auf der Gegenstelle INTERNET.

  - Soll das Subnetz abcd verwendet werden, so muss als **Adresse/Präfix** der Wert 0:0:0:abcd::/48 konfiguriert werden.
  - Soll nur die Adresse 2001:db8:0:23::dead:beef/128 verwendet werden, so muss als **Adresse/Präfix** 0:0:0:23::dead:beef/128 konfiguriert werden.
  - Soll das gesamte Präfix verwendet werden, so muss als **Adresse/Präfix** ::/0 konfiguriert werden oder der Eintrag leer gelassen werden.

Netzwerk-Name

Geben Sie hier den Namen des Netzwerkes ein, wenn Sie im Feld **Typ** die entsprechende Option ausgewählt haben.

Gegenstelle/Lokale Station

Geben Sie hier den Namen der Gegenstelle ein, wenn Sie im Feld **Typ** die entsprechende Option ausgewählt haben.

Adresse/Präfix

Geben Sie hier die Adresse ein, wenn Sie im Feld **Typ** die entsprechende Option ausgewählt haben.

NPTv6

NPTv6 (Network Prefix Translation) nach *RFC 6296* erlaubt die Umsetzung eines IPv6-Präfixes auf ein anderes IPv6-Präfix. Die Umsetzung erfolgt 1:1, d. h. eine Adresse aus Präfix A wird auf eine Adresse aus Präfix B umgesetzt. Es wird dabei nur der Präfix-Teil umgesetzt, der Host-Teil bleibt erhalten. Dieses Verfahren arbeitet somit „Stateless". Mit NPTv6 ist es nicht möglich, wie bei IPv4, ein ganzes Netzwerk hinter einer Adresse zu maskieren.

Anwendungsszenarien für NPTv6 sind z. B. VPNs oder Netzwerke mit dynamischen Präfixen wo Adressunabhängigkeit erreicht werden soll. Teilt der Provider ein dynamisches Präfix zu, so ändert sich in der Regel das Präfix bei jedem Verbindungsaufbau. Dies ist aber nicht gewünscht, wenn bestimmte Ressourcen feste IP-Adressen benötigen. Mit NPTv6 werden dann Adressen aus dem (privaten) ULA-Bereich fd00::/8 an die Clients im Netzwerk vergeben und durch eine NPTv6-Regel diese Adressen auf das Provider-Präfix umgesetzt.

Ein weiterer Anwendungsfall ist ein Load Balancer-Szenario mit mehreren Internetprovidern, wobei jeder Provider ein eigenes Präfix vergibt. Mit NPTv6 werden dann Adressen aus dem ULA-Bereich fd00::/8 an die Clients im Netzwerk vergeben und durch mehrere NPTv6-Regeln diese Adressen auf die Provider-Präfixe umgesetzt.

NPTv6 garantiert Prüfsummenneutralität, d. h. die umgesetzte IPv6-Adresse wird so geändert, dass die Prüfsumme im IPv6-Paket nicht angepasst werden muss. Deshalb wird eine Adresse X nicht exakt 1:1 in Adresse Y umgesetzt, sondern es müssen in der Adresse 16 Bit für die Prüfsummenneutralität beim Umsetzen kodiert werden.

Die Position der 16 Bits ist abhängig von den Präfixen, die umgesetzt werden sollen. Bei Präfixen, die länger als 48 Bit sind, z. B. /56 oder /60, wird aufgrund der Prüfsummenneutralität (16 Bit) auch ein Teil des Interface-Identifier beim Mapping geändert. Dies betrifft den Zugriff von außen auf interne Stationen im LAN. Nur bei Präfixen die 48 Bit oder kürzer sind, z. B. /48 oder /40 können die 16 Bit im Präfix kodiert werden.

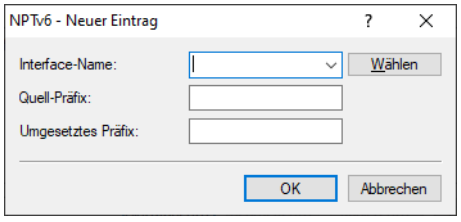
Bei dynamischen Präfixen ändern sich die 16 Bit bei jeder neuen Präfix-Zuweisung. Zugriffe von außen auf das interne Netzwerk sind daher nur sinnvoll bei einem statischen Provider-Präfix möglich, da sich durch die Änderung der 16 Bits auch die gesamte Adresse ändert.

Ein Zugriff von außen auf Stationen im LAN ist also nur mit einem statischen /48 Provider-Präfix problemlos möglich aufgrund der gleichbleibenden IPv6-Adressen der internen Station nach der Umsetzung durch den Router.

Eine mögliche Lösung für den Zugriff von außen bei NPTv6 bei dynamischen Präfixen und Präfixen länger als /48, ist die Verwendung eines DynDNS-Clients direkt auf der Station im LAN, die in der Update-URL nicht ihre Adresse selbst einsetzen, sondern der Provider die empfangene IP-Adresse registriert.

Die IPv6-Firewall muss für NPTv6 grundsätzlich aktiviert sein.

In LANconfig erfolgt die Konfiguration unter **Firewall/QoS** > **IPv6-Regeln** > **NPTv6**.



Interface-Name

Name des Netzwerks bzw. der Gegenstelle, auf der NPTv6 gemacht werden soll. Soll ein Präfix für ein dynamisches Provider-Präfix umgesetzt werden, so muss hier der Name der Internet-Verbindung bzw. Gegenstelle, z. B. INTERNET, konfiguriert werden.

Quell-Präfix

Präfix des Quellnetzwerks, z. B. ein explizites Präfix fd00::/64.

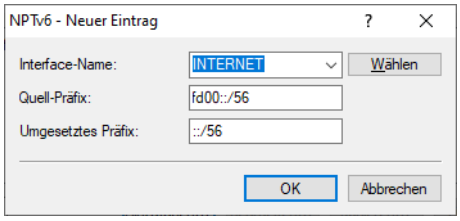
Umgesetztes Präfix

Präfix auf das das Quell-Präfix umgesetzt werden soll. Es kann entweder ein explizites Präfix wie 2001:db8::/32 oder der Platzhalter :: mit entsprechender Präfixlänge, falls der Provider ein dynamisches Präfix vergibt, konfiguriert werden.

Beispiele

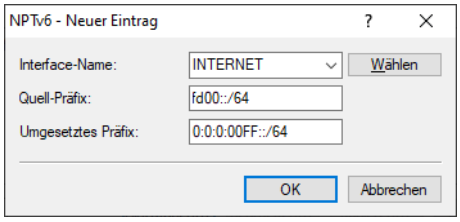
Beispiel 1

Der Provider (Gegenstelle INTERNET) vergibt ein dynamisches Präfix mit Länge /56. Im Intranet ist das Präfix fd00::/64 konfiguriert. Das Quell-Präfix fd00::/56 soll auf das gesamte Provider-Präfix (::/56) 1:1 umgesetzt werden.



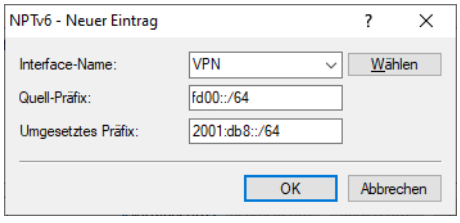
Beispiel 2

Der Provider (Gegenstelle INTERNET) vergibt ein dynamisches Präfix mit Länge /56. Im Intranet ist das Präfix fd00::/64 konfiguriert. Das Quell-Präfix fd00::/64 soll auf das spezielle Subnetz „FF" aus dem dynamischen Provider-Präfix umgesetzt werden. Als umgesetztes Präfix wird der Platzhalter :: mit Subnetz-ID FF konfiguriert, d. h. 0:0:0:00FF::/64.



Beispiel 3

Für ein VPN-Szenario soll das interne Quell-Präfix fd00::/64 auf das Präfix 2001:db8::/64 umgesetzt werden.



Show-Commands über CLI

Ihnen stehen folgende Show-Kommandos zur Verfügung:

- **show ipv6-npt**

  Zeigt die NPTv6-Umsetzungsregel an.

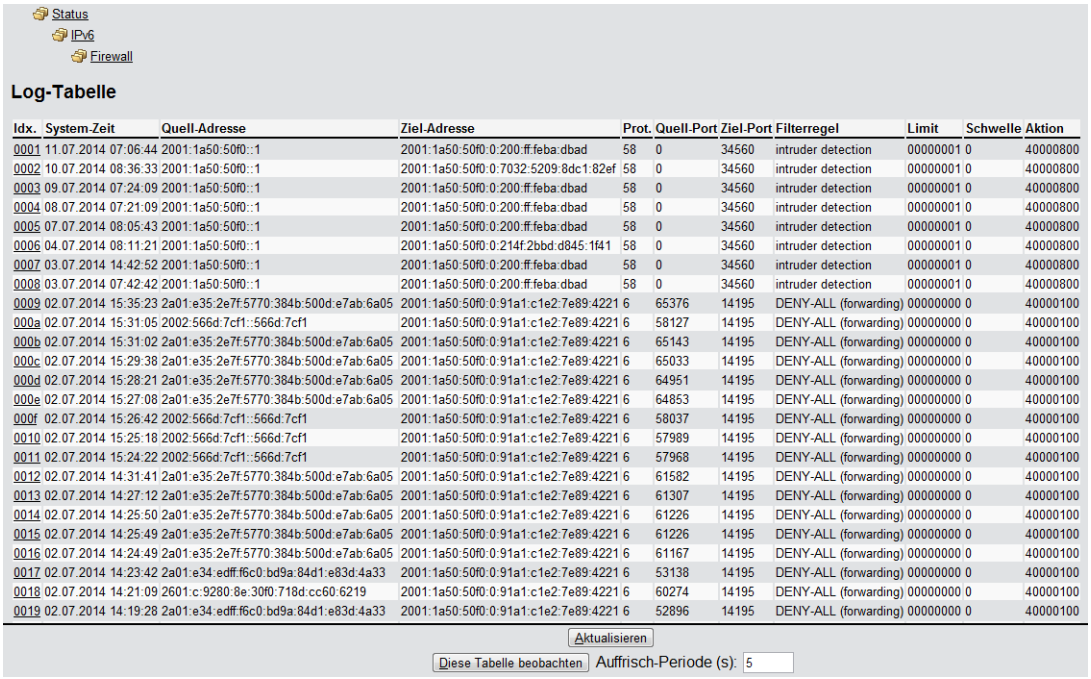
7.5.3 IPv6-Firewall-Log-Tabelle

Die IPv6-Firewall stellt analog zur IPv4-Firewall eine Log-Tabelle für Ereignisse im IPv6-Umfeld bereit.

Die Syntax dieser Log-Tabelle entspricht der IPv4-Log-Tabelle mit Ausnahme des IP-Adressformats (IPv6-Adressen liegen in hexadezimaler, IPv4-Adressen in dezimaler Form vor).

7.5.3.1 IPv6-Firewall-Log-Tabelle über WEBconfig auswerten

Sie können die IPv6-Log-Tabelle im WEBconfig über **Extras** > **LCOS-Menübaum** > **Status** > **IPv6** > **Firewall** > **Log-Tabelle** öffnen.



Idx.	System-Zeit	Quell-Adresse	Ziel-Adresse	Prot.	Quell-Port	Ziel-Port	Filterregel	Limit	Schwelle	Aktion
0001	11.07.2014 07:06:44	2001:1a50:50f0::1	2001:1a50:50f0:0:200:ff:feba:dbad	58	0	34560	intruder detection	00000001	0	40000800
0002	10.07.2014 08:36:33	2001:1a50:50f0::1	2001:1a50:50f0:0:7032:5209:8dc1:82ef	58	0	34560	intruder detection	00000001	0	40000800
0003	09.07.2014 07:24:09	2001:1a50:50f0::1	2001:1a50:50f0:0:200:ff:feba:dbad	58	0	34560	intruder detection	00000001	0	40000800
0004	08.07.2014 07:21:09	2001:1a50:50f0::1	2001:1a50:50f0:0:200:ff:feba:dbad	58	0	34560	intruder detection	00000001	0	40000800
0005	07.07.2014 08:05:43	2001:1a50:50f0::1	2001:1a50:50f0:0:200:ff:feba:dbad	58	0	34560	intruder detection	00000001	0	40000800
0006	04.07.2014 08:11:21	2001:1a50:50f0::1	2001:1a50:50f0:0:214f:2bbd:d845:1f41	58	0	34560	intruder detection	00000001	0	40000800
0007	03.07.2014 14:42:52	2001:1a50:50f0::1	2001:1a50:50f0:0:200:ff:feba:dbad	58	0	34560	intruder detection	00000001	0	40000800
0008	03.07.2014 07:42:42	2001:1a50:50f0::1	2001:1a50:50f0:0:200:ff:feba:dbad	58	0	34560	intruder detection	00000001	0	40000800
0009	02.07.2014 15:35:23	2a01:e35:2e7f:5770:384b:500d:e7ab:6a05	2001:1a50:50f0:0:91a1:c1e2:7e89:4221	6	65376	14195	DENY-ALL (forwarding)	00000000	0	40000100
000a	02.07.2014 15:31:05	2002:566d:7cf1::566d:7cf1	2001:1a50:50f0:0:91a1:c1e2:7e89:4221	6	58127	14195	DENY-ALL (forwarding)	00000000	0	40000100
000b	02.07.2014 15:31:02	2a01:e35:2e7f:5770:384b:500d:e7ab:6a05	2001:1a50:50f0:0:91a1:c1e2:7e89:4221	6	65143	14195	DENY-ALL (forwarding)	00000000	0	40000100
000c	02.07.2014 15:29:38	2a01:e35:2e7f:5770:384b:500d:e7ab:6a05	2001:1a50:50f0:0:91a1:c1e2:7e89:4221	6	65033	14195	DENY-ALL (forwarding)	00000000	0	40000100
000d	02.07.2014 15:28:21	2a01:e35:2e7f:5770:384b:500d:e7ab:6a05	2001:1a50:50f0:0:91a1:c1e2:7e89:4221	6	64951	14195	DENY-ALL (forwarding)	00000000	0	40000100
000e	02.07.2014 15:27:08	2a01:e35:2e7f:5770:384b:500d:e7ab:6a05	2001:1a50:50f0:0:91a1:c1e2:7e89:4221	6	64853	14195	DENY-ALL (forwarding)	00000000	0	40000100
000f	02.07.2014 15:26:42	2002:566d:7cf1::566d:7cf1	2001:1a50:50f0:0:91a1:c1e2:7e89:4221	6	58037	14195	DENY-ALL (forwarding)	00000000	0	40000100
0010	02.07.2014 15:25:18	2002:566d:7cf1::566d:7cf1	2001:1a50:50f0:0:91a1:c1e2:7e89:4221	6	57989	14195	DENY-ALL (forwarding)	00000000	0	40000100
0011	02.07.2014 15:24:22	2002:566d:7cf1::566d:7cf1	2001:1a50:50f0:0:91a1:c1e2:7e89:4221	6	57968	14195	DENY-ALL (forwarding)	00000000	0	40000100
0012	02.07.2014 14:31:41	2a01:e35:2e7f:5770:384b:500d:e7ab:6a05	2001:1a50:50f0:0:91a1:c1e2:7e89:4221	6	61582	14195	DENY-ALL (forwarding)	00000000	0	40000100
0013	02.07.2014 14:27:12	2a01:e35:2e7f:5770:384b:500d:e7ab:6a05	2001:1a50:50f0:0:91a1:c1e2:7e89:4221	6	61307	14195	DENY-ALL (forwarding)	00000000	0	40000100
0014	02.07.2014 14:25:50	2a01:e35:2e7f:5770:384b:500d:e7ab:6a05	2001:1a50:50f0:0:91a1:c1e2:7e89:4221	6	61226	14195	DENY-ALL (forwarding)	00000000	0	40000100
0015	02.07.2014 14:25:49	2a01:e35:2e7f:5770:384b:500d:e7ab:6a05	2001:1a50:50f0:0:91a1:c1e2:7e89:4221	6	61226	14195	DENY-ALL (forwarding)	00000000	0	40000100
0016	02.07.2014 14:24:49	2a01:e35:2e7f:5770:384b:500d:e7ab:6a05	2001:1a50:50f0:0:91a1:c1e2:7e89:4221	6	61167	14195	DENY-ALL (forwarding)	00000000	0	40000100
0017	02.07.2014 14:23:42	2a01:e34:edff:f6c0:bd9a:84d1:e83d:4a33	2001:1a50:50f0:0:91a1:c1e2:7e89:4221	6	53138	14195	DENY-ALL (forwarding)	00000000	0	40000100
0018	02.07.2014 14:21:09	2601:c:9280:8e:30f0:718d:cc60:6219	2001:1a50:50f0:0:91a1:c1e2:7e89:4221	6	60274	14195	DENY-ALL (forwarding)	00000000	0	40000100
0019	02.07.2014 14:19:28	2a01:e34:edff:f6c0:bd9a:84d1:e83d:4a33	2001:1a50:50f0:0:91a1:c1e2:7e89:4221	6	52896	14195	DENY-ALL (forwarding)	00000000	0	40000100

Die Einträge haben folgende Bedeutung:

- **Idx.**: Fortlaufender Index. Darüber lässt sich die Tabelle auch über SNMP abfragen.
- **System-Zeit**: System-Zeit in UTC-Kodierung (wird bei der Ausgabe der Tabelle in Klartext umgewandelt).
- **Quell-Adresse**: Quell-Adresse des gefilterten Pakets.
- **Ziel-Adresse**: Ziel-Adresse des gefilterten Pakets.
- **Prot.**: Protokoll (TCP, UDP etc.) des gefilterten Pakets.
- **Quell-Port**: Quell-Port des gefilterten Pakets (nur bei portbehafteten Protokollen).
- **Ziel-Port**: Ziel-Port des gefilterten Pakets (nur bei portbehafteten Protokollen).
- **Filterregel**: Name der Regel, die den Eintrag erzeugt hat. Erfolgt die Filterung auf Grund mehrerer Regeln, listet die Spalte alle entsprechenden Regeln auf. Falls der Platz nicht ausreicht, erscheint das Kürzel '...'.
- **Limit**: Bitfeld, das das überschrittene Limit beschreibt, durch das die Firewall den Filter angewendet hat. Es sind zur Zeit folgende Werte definiert:
  - 0x01: Absolute Anzahl
  - 0x02: Anzahl pro Sekunde

- 0x04: Anzahl pro Minute
- 0x08: Anzahl pro Stunde
- 0x10: globales Limit
- 0x20: Byte-Limit (wenn nicht gesetzt, handelt es sich um ein Paket-Limit)
- 0x40: Limit gilt nur in Empfangsrichtung
- 0x80: Limit gilt nur in Senderichtung

- **Schwelle**: überschrittener Grenzwert des auslösenden Limits.
- **Aktion**: Bitfeld, das alle ausgeführten Aktionen aufführt. Es sind zur Zeit folgende Werte definiert:
  - 0x00000001: Accept
  - 0x00000100: Reject
  - 0x00000200: Aufbaufilter
  - 0x00000400: Internet-(Defaultrouten-)Filter
  - 0x00000800: Drop
  - 0x00001000: Disconnect
  - 0x00004000: Quell-Adresse sperren
  - 0x00020000: Ziel-Adresse und -Port sperren
  - 0x20000000: Sende SYSLOG-Benachrichtigung
  - 0x40000000: Sende SNMP-Trap
  - 0x80000000: Sende E-Mail

Alle Firewall-Aktionen erscheinen ebenfalls im IP-Router-Trace.

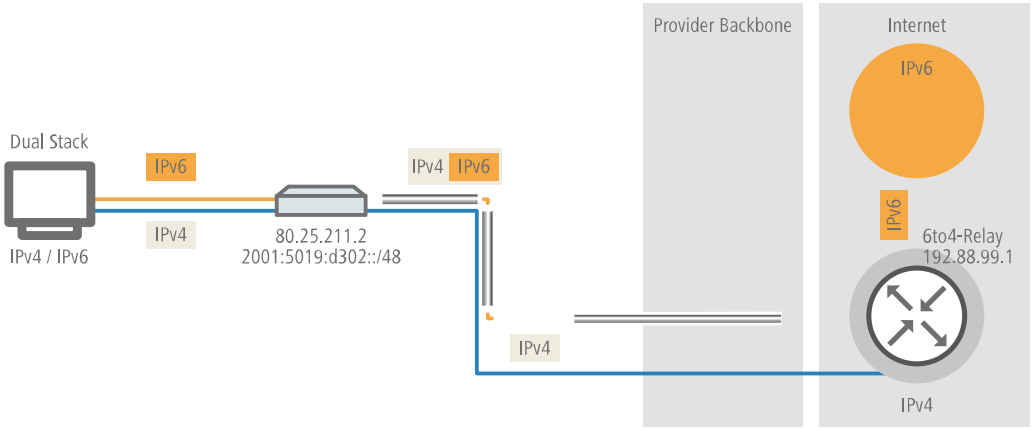
7.6 IPv6-Tunneltechnologien

7.6.1 6to4-Tunnel

Mit dem 6to4-Tunnel haben Sie die Möglichkeit auf einfache Weise eine Verbindung zwischen zwei IPv6-Netzwerken über ein IPv4-Netzwerk herzustellen. Dazu wird ein so genannter 6to4-Tunnel erstellt:

- Ein Router zwischen lokalen IPv6-Netzwerken und einem IPv4-Netzwerk dient als Vermittler zwischen den Netzwerken.
- Der Router hat sowohl eine öffentliche IPv4-Adresse, als auch eine IPv6-Adresse. Die IPv6-Adresse setzt sich aus einem IPv6-Präfix und der IPv4-Adresse in hexadezimaler Schreibweise zusammen. Hat ein Router z. B. die IPv4-Adresse 80.25.211.2 , so wird diese zunächst in hexadezimale Schreibweise umgerechnet: 5019:d302. Ergänzend dazu kommt ein IPv6-Präfix (z. B. 2002::/16), so dass die IPv6-Adresse für den Router wie folgt aussieht: 2002:5019:d302::/48.
- Schickt ein Gerät aus dem IPv6-Netzwerk Datenpakete über den Router an eine IPv6-Zieladresse, dann schachtelt der Router die IPv6-Pakete zunächst in ein Paket mit einem IPv4-Header. Das geschachtelte Paket leitet der Router

anschließend an ein 6to4-Relay weiter. Das 6to4-Relay entpackt das Paket und leitet es an das gewünschte Ziel weiter. Die folgende Abbildung zeigt das Funktionsprinzip des 6to4-Tunnels:

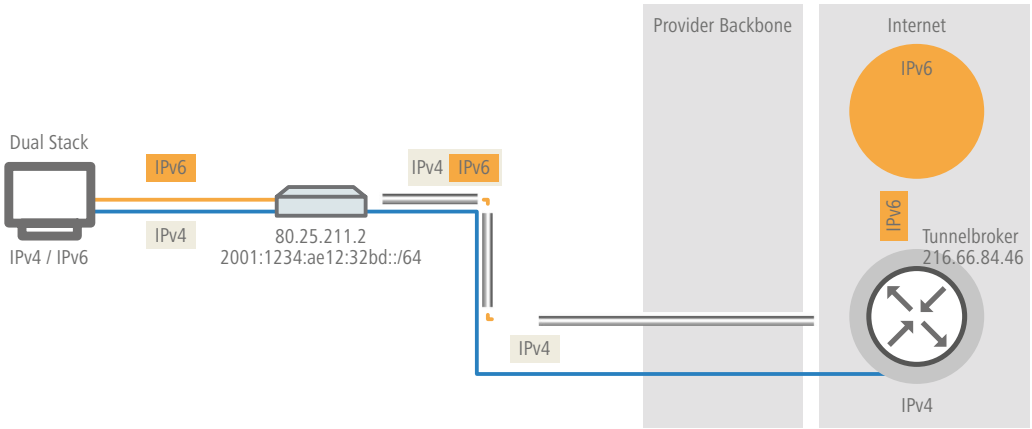


6to4-Tunnel stellen eine dynamische Verbindung zwischen IPv6- und IPv4-Netzwerken her: die Antwortpakete werden möglicherweise über ein anderes 6to4-Relay zurückgeleitet, als auf dem Hinweg. Daher handelt es sich beim 6to4-Tunnel nicht um eine Punkt zu Punkt-Verbindung. Der Router sucht für jede neue Verbindung stets das nächstgelegene öffentliche 6to4-Relay. Dies geschieht über die Anycast-Adresse 192.88.99.1. Dieser Aspekt ist zum einen ein Vorteil des 6to4-Tunnels, stellt aber gleichzeitig auch einen Nachteil dar. Öffentliche 6to4-Relays benötigen keine Anmeldung und sind frei zugänglich. Desweiteren benötigt die dynamische Verbindung wenig Konfigurationsaufwand. Auf diese Weise ist es für jeden Nutzer möglich, einfach und schnell einen 6to4-Tunnel über ein öffentliches Relay zu erzeugen.

Andererseits führt die dynamische Verbindung dazu, dass der Nutzer keinen Einfluss auf die Wahl der 6to4-Relays hat. Daher besteht vom Provider des Relays die Möglichkeit, Daten mitzuschneiden oder zu manipulieren.

7.6.2 6in4-Tunnel

6in4 Tunnel dienen der Verbindung zweier Hosts, Router oder der Verbindung zwischen Host und Router. 6in4 Tunnel können somit zwei IPv6 Netzwerke über ein IPv4 Netzwerk verbinden. Die Abbildung zeigt einen statischen 6in4-Tunnel zwischen dem lokalen Router und einem 6in4-Gateway eines Tunnelbrokers.



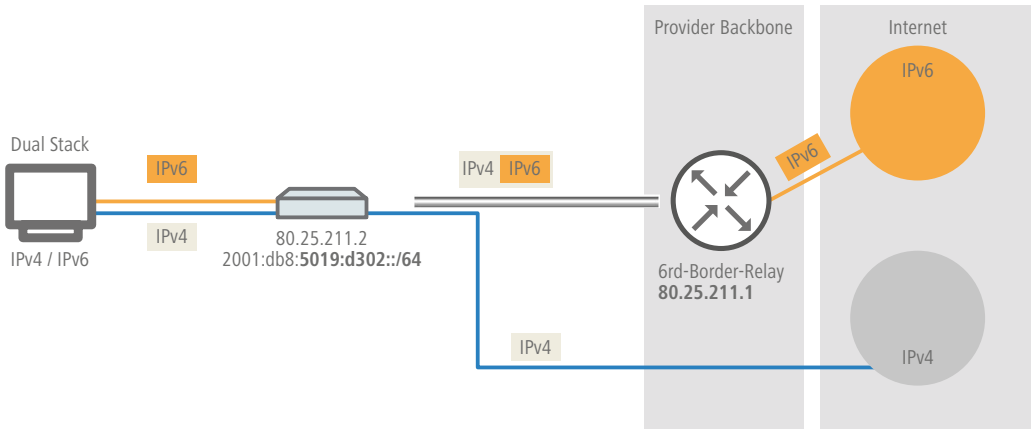
Es handelt sich hierbei um einen dedizierten, bekannten Dienst und Betreiber. Die Endpunkte sind festgelegt und der Tunnelbroker weist ein statisches Präfix zu. Die Vorteile einer 6in4 Lösung sind also sowohl feste 6in4-Gateways als auch das Wissen um den Betreiber. Das feste Präfix des Tunnelbrokers bestimmt darüber hinaus die Anzahl der möglichen Subnetze, die genutzt werden können. Ein 64 Bit Präfix (z. B. 2001:db8::/64) erlaubt die Nutzung eines Subnetzes. Bei einem 48 Bit Präfix stehen sogar 16 Bit des 64 Bit Präfix-Anteils zur Verfügung. Damit lassen sich bis zu 65536 Subnetze realisieren.

Der Nachteil der 6in4-Technologie ist der höhere Administrationsaufwand. Eine Anmeldung beim gewählten Tunnelbroker ist notwendig. Hinzu kommt die statische Konfiguration der Tunnelendpunkte. Im Falle einer dynamisch bezogenen IPv4-Adresse müssen die Daten regelmäßig aktualisiert werden. Letzteres kann allerdings von einem Router, beispielsweise mit Hilfe eines Skriptes, automatisch erledigt werden.

6in4 stellt eine vergleichsweise sichere und stabile Technologie für einen IPv6-Internetzugang dar. Diese Technologie ist somit auch zum Betrieb von Webservern geeignet, die über IPv6 erreicht werden sollen. Der Nachteil ist lediglich der erhöhte adminstrative Aufwand. Diese Technologie ist somit für den professionellen Einsatz geeignet.

7.6.3 6rd-Tunnel

6rd (rapid deployment) ist eine Weiterentwicklung von 6to4. Die zugrunde liegende Funktionsweise ist identisch. Der Unterschied besteht darin, dass ein spezifisches Relay genutzt wird, welches der Provider betreibt. Dies löst die zwei grundlegenden Probleme der 6to4-Technologie, die mangelnde Sicherheit und Stabilität. Das Präfix wird bei 6rd entweder manuell konfiguriert oder über DHCP (IPv4) übermittelt, was den Konfigurationsauswand weiter reduziert. Die Abbildung zeigt eine schematische Darstellung eines 6rd Szenarios.



Der Provider weist dem Router ein Präfix (2001:db8::/32) zu, welches vom Router durch die IPv4-Adresse ergänzt wird. Die somit erzeugte IPv6-Adresse hat die Form: 2001:db8:5019:d302::/64. 6rd ist somit aus zwei Perspektiven interessant. Es ermöglicht dem Provider auf einfache Art und Weise seinen Kunden das IPv6 Internet zugänglich zu machen. Zusätzlich vereinfacht es die Nutzung für die Kunden erheblich. Sie müssen weder die Sicherheitsrisiken von 6to4 hinnehmen noch den Konfigurationsaufwand von 6in4 investieren.

7.6.4 Dual-Stack Lite (DS-Lite)

Dual-Stack Lite, kurz DS-Lite, dient dazu, dass Internet-Provider ihren Kunden über eine IPv6-Verbindung Zugang zu IPv4-Servern verschaffen können. Das ist z. B. dann erforderlich, wenn der Kunde weiterhin IPv4-Geräte verwendet, der Internet-Provider allerdings aufgrund knapper IPv4-Adressen dem Kunden nur eine IPv6-Adresse vergeben kann. Im Gegensatz zu den anderen drei IPv6-Tunnelverfahren "6in4", "6rd" und "6to4" dient DS-Lite also dazu, IPv4-Pakete über eine IPv6-Verbindung zu übertragen (IPv4-über-IPv6-Tunnel).

Der Router verpackt dazu die IPv4-Pakete in einen IPv4-in-IPv6-Tunnel und übermittelt sie unmaskiert an den Provider. Der führt anschließend eine NAT mit einer seiner eigenen verbliebenen IPv4-Adressen durch.

Zur Definition eines DS-Lite-Tunnels benötigt der Router nur die IPv6-Adresse des Tunnel-Endpunkts sowie das Routing-Tag, über das er diese Adresse erreichen kann.

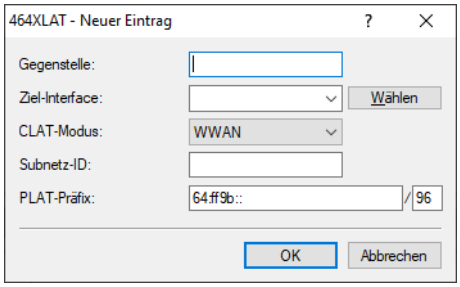
Standardmäßig verwendet der Router die IPv4-Adresse des entsprechenden internen Netzes, z. B. vom "INTRANET". Möchte man stattdessen eine andere IP-Adresse (z. B. 192.0.0.2) vorgeben, muss diese zusammen mit dem Gegenstellennamen des DS-Lite-Tunnels in der IP-Parameter-Liste angelegt sein.

Die Angabe eines IPv4-DNS-Servers ist für einen DS-Lite-Tunnel nicht ratsam, da dessen Einträge die NAT-Tabelle des Internet-Providers unnötig füllen würden.

7.6.5 464XLAT

464XLAT nach *RFC 6877* ist ein Übersetzungsverfahren von IPv4 zu IPv6 und wieder zu IPv4. Das Verfahren wird häufig von Mobilfunkprovidern eingesetzt, um in einem IPv6-Only-APN auf Basis von NAT64 Zugang zu IPv4 zu ermöglichen. An 464XLAT sind zwei Seiten beteiligt: Die Client-Seite bzw. der Client-Translator (CLAT – Customer-Side Translator) sowie der Provider-Translator (PLAT – Provider-Side Translator) bzw. das NAT64-Gateway des Providers. Das LCOS unterstützt die CLAT-Seite, um einem Netzwerk hinter einem Router Zugang zu IPv4-Netzwerken zu ermöglichen. Im Unterschied zu DS-Lite, bei dem ein 4in6-Tunnel zum AFTR-Gateway aufgebaut wird, verwendet 464XLAT eine Übersetzung (Translation) des IPv4-Pakets nach IPv6. Auf der PLAT-Seite wird das Paket zurück in IPv4 übersetzt. Aufgrund der zweifachen Übersetzung ergibt sich der Name 464. In der Regel wird das NAT64-Präfix 64:ff9b::/96 auf der Provider-Seite zur Übersetzung verwendet. Um 464XLAT zu verwenden, muss zunächst eine IPv6-Verbindung konfiguriert werden. Anschließend wird eine 464XLAT-Gegenstelle hinzugefügt. Auf diese Gegenstelle zeigt dann die IPv4-Default-Route.

In LANconfig erfolgt die Konfiguration unter **IPv6** > **Tunnel** > **464XLAT**.



Gegenstelle

Vergeben Sie einen eindeutigen Namen für diese Gegenstelle. Max. 16 Zeichen in Großbuchstaben.

Ziel-Interface

Name des darunterliegenden WAN-Interface bzw. der darunterliegenden Gegenstelle, z. B. INTERNET. Max. 16 Zeichen in Großbuchstaben.

CLAT-Modus

Definiert, mit welcher Methode das CLAT-Präfix erzeugt werden soll.

DHCPv6-PD

Verwendet der Internetprovider DHCPv6 Präfix Delegation, z. B. bei DSL oder Kabelverbindungen, so muss der CLAT-Modus DHCPv6-PD verwendet werden. Über die Subnet ID kann gesteuert werden, welches Subnetz des delegierten Präfixes für das CLAT-Präfix verwendet werden soll. Die Subnetz ID kann z. B. als „0“, „1“ oder „FF“ konfiguriert werden.

WWAN (Default)

Ist die Internetverbindung eine Mobilfunkverbindung (WWAN), so muss der CLAT-Modus WWAN verwendet werden. Das CLAT-Präfix wird aus dem /64 WAN-Präfix gebildet. Die Subnet-ID muss 0 oder leer sein. In der IPv4-Routing-Tabelle muss für die WAN-Verbindung NAT aktiviert werden.

Statisch

Verwendet der Internetprovider ein statisches Präfix, so kann im Feld Subnet-ID das statische /64 Präfix für das CLAT-Präfix verwendet werden, z. B. 2001:db8:: (ohne die Angabe /64). Dieser Modus kann auch verwendet werden, falls 464XLAT auf einer VPN-Verbindung oder einem Tunnel-Interface verwendet werden soll. In diesem Fall muss das VPN-Interface eine statische IPv6-Adresse konfiguriert haben.

Subnetz-ID

Subnetz-ID die mit dem delegierten DHCPv6-Präfix des Providers verknüpft wird. In das resultierende Präfix wird die IPv4-Quelladresse eingebettet, wenn das Paket ins WAN gesendet wird. Im Falle einer WWAN-Verbindung (/64-Präfix) kann entweder der Wert 0 konfiguriert werden, oder der Parameter kann leer

gelassen werden (Default). Wird für CLAT-Modus der Wert statisch verwendet, so kann im Feld Subnetz-ID das statische /64 Präfix als CLAT-Präfix konfiguriert werden, z. B. 2001:db8:: (ohne die Angabe /64).

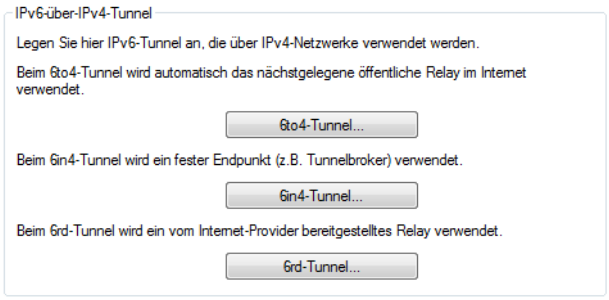
Beispiel für Subnetz-IDs: 0, 1, 12, 1f3b oder 2001:db8::

PLAT-Präfix

IPv6-Präfix, das auf der Providerseite zur Übersetzung verwendet wird. Wenn der Wert leer gelassen wird, wird eine DNS Präfix-Discovery nach *RFC 7050* durchgeführt, um das PLAT-Präfix automatisch zu ermitteln. Default: 64:ff9b::/96

7.6.6 Tunnel einrichten

In der Konfiguration **Tunnel** legen Sie über 3 Schaltflächen IPv6-Tunnel an, die über IPv4-Netzwerke verwendet werden. Diese benötigen Sie, um den Zugang zum IPv6-Internet über eine IPv4-Verbindung herzustellen.



6to4-Tunnel

Diese Schaltfläche öffnet die Einstellung von 6to4-Tunneln.

Verbindungen über einen 6to4-Tunnel nutzen Relays, die der Backbone des IPv4-Internet-Providers auswählt. Der Administrator des Geräts hat keinen Einfluss auf die Auswahl des Relays. Darüber hinaus kann sich das verwendete Relay ohne Wissen des Administrators ändern. Aus diesem Grund sind Verbindungen über einen 6to4-Tunnel **ausschließlich für Testzwecke** geeignet. Vermeiden Sie insbesondere Datenverbindungen über einen 6to4-Tunnel für den Einsatz in Produktivsystemen oder die Übertragung sensibler Daten.

6in4-Tunnel

Diese Schaltfläche öffnet die Einstellung von 6in4-Tunneln.

6in4-Tunnel haben einen höheren administrativen Aufwand, stellen aber eine sichere und stabile Technologie für einen IPv6-Internetzugang dar. Diese Möglichkeit ist auch für den professionellen Einsatz geeignet.

6rd-Tunnel

Diese Schaltfläche öffnet die Einstellung von 6rd-Tunneln.

6rd-Tunnel sind sowohl für Endanwender als auch für den professionellen Einsatz geeignet, da es nicht den Konfigurationsaufwand von 6in4-Tunneln erfordert, aber dennoch nicht die Sicherheitsrisiken von 6to4-Tunneln hat.

7.6.6.1 Einrichtung eines 6to4-Tunnels

Die Verwendung eines 6to4-Tunnels bietet sich an, wenn

- Ihr Gerät IPv6-fähig ist und Sie auf IPv6-Dienste zugreifen möchten,
- Ihr Provider jedoch kein natives IPv6-Netz unterstützt und

- Sie keinen Zugang zu einem so genannten Tunnelbroker haben, der Ihre IPv6-Datenpakete vermittelt.

Bei der Verwendung eines 6to4-Tunnels erhält das Gerät keine IPv6-Adresse bzw. kein IPv6-Präfix des Providers, da dieser keine IPv6-Funktionalität anbietet.

Das Gerät berechnet ein eigenes, eindeutiges Präfix aus "2002::/16" und der Hexadezimal-Darstellung der eigenen, öffentlichen IPv4-Adresse, die der Provider liefert. Diese Anwendung funktioniert daher ausschließlich dann, wenn das Gerät tatsächlich eine öffentliche IPv4-Adresse besitzt. Das Gerät erhält z. B. keine öffentlich gültige IPv4-Adresse, sondern nur eine IPv4-Adresse aus einem privaten Adressbereich, wenn

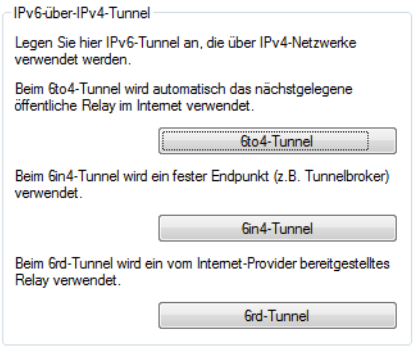
- das Gerät einen Internetzugang über Mobilfunk herstellt und der Provider dafür nur private IP-Adressen zur Verfügung stellt; oder
- das Gerät selbst nicht den Zugang zum Internet herstellt, sondern "hinter" einem anderen Router steht.

Verbindungen über einen 6to4-Tunnel nutzen Relays, die der Backbone des IPv4-Internet-Providers auswählt. Der Administrator des Gerätes hat keinen Einfluss auf die Auswahl des Relays. Darüber hinaus kann sich das verwendete Relay ohne das Wissen des Administrators ändern. Aus diesem Grund sind Verbindungen über einen 6to4-Tunnel **ausschließlich für Testzwecke** geeignet. Vermeiden Sie insbesondere Datenverbindungen über einen 6to4-Tunnel für den Einsatz in Produktivsystemen oder die Übertragung sensibler Daten.

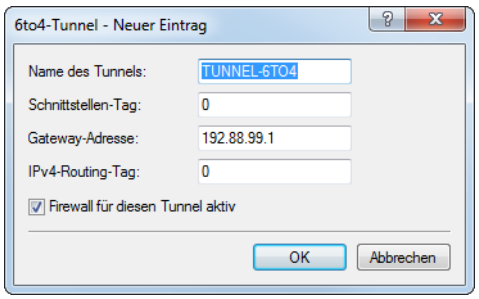
Konfiguration

Um einen 6to4-Tunnel über LANconfig einzurichten, gehen Sie wie folgt vor:

1. Starten Sie LANconfig. LANconfig sucht nun automatisch im lokalen Netz nach Geräten.
2. Wählen Sie das Gerät aus, für das Sie den 6to4-Tunnel einrichten wollen. Markieren Sie es mit einem Links-Klick und starten Sie die Konfiguration in der Menüleiste über **Gerät** > **Konfigurieren**.
3. Wechseln Sie im Konfigurationsdialog in die Ansicht **IPv6** > **Tunnel** und klicken Sie auf **6to4-Tunnel**.



4. Klicken Sie auf **Hinzufügen**, um einen neuen 6to4-Tunnel anzulegen.



5. Vergeben Sie den Namen des 6to4-Tunnels.
6. Tragen Sie als **Schnittstellen-Tag** einen Wert ein, der das Netzwerk eindeutig spezifiziert. Alle Pakete, welche dieses Gerät auf diesem Netzwerk empfängt, erhalten intern eine Markierung mit diesem Tag. Das Schnittstellen-Tag ermöglicht eine Trennung der für dieses Netzwerk gültigen Routen auch ohne explizite Firewall-Regel.

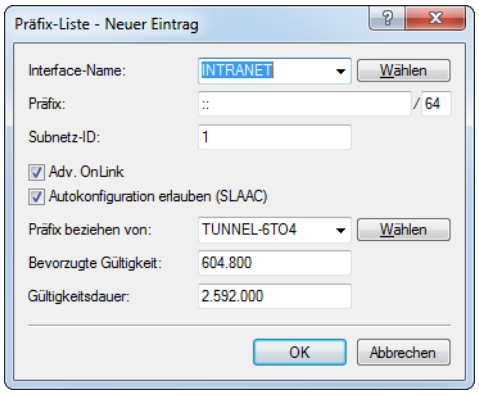
7. Die **Gateway-Adresse** ist per Default vorbelegt mit der Anycast-Adresse "192.88.99.1".
8. Bestimmen Sie hier das Routing-Tag, mit dem das Gerät die Route zum zugehörigen entfernten Gateway ermittelt. Das **IPv4-Routing-Tag** gibt an, über welche getaggte IPv4-Route die Datenpakete ihre Zieladresse erreichen.
9. Als Default-Wert ist die Firewall dieses Tunnels aktiv.

   Wenn Sie die globale Firewall deaktivieren, deaktivieren Sie ebenfalls die Firewall für den Tunnel.

10. Übernehmen Sie Ihre Eingaben mit **OK**.
11. Wechseln Sie in das Verzeichnis **IPv6** > **Router-Advertisements**.

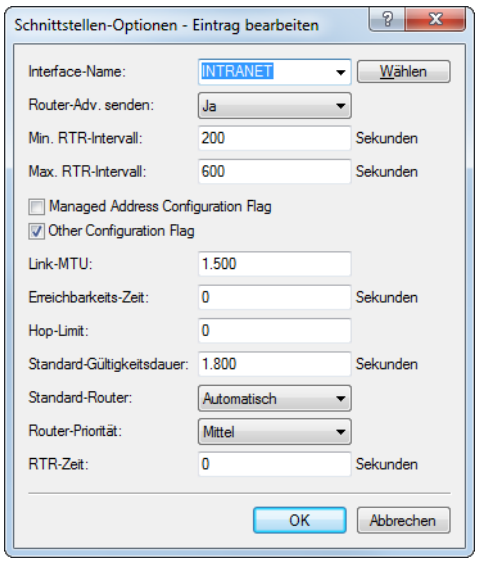


12. Öffnen Sie die **Präfix-Liste** und klicken Sie auf **Hinzufügen**.



13. Vergeben Sie einen Namen für das Interface, das den 6to4-Tunnel verwenden wird, z. B. "INTRANET".
14. Bestimmen Sie als **Präfix** den Wert "::/64", um das vom Provider vergebene Präfix automatisch und in voller Länge zu übernehmen.
15. Übernehmen Sie den Default-Wert "1" für die **Subnetz-ID**.
16. Übernehmen Sie die aktivierte Option **Autokonfiguration erlauben (SLAAC)**.
17. Übernehmen Sie im Feld **Präfix-Delegation von** aus der Liste den Namen des Tunnels, den Sie zuvor definiert haben, im Beispiel oben "TUNNEL-6TO4".
18. Übernehmen Sie Ihre Eingaben mit **OK**.
19. Im Verzeichnis **IPv6** > **Router-Advertisements** öffnen Sie die **Schnittstellen-Optionen** und klicken auf **Bearbeiten** für den Eintrag INTRANET.

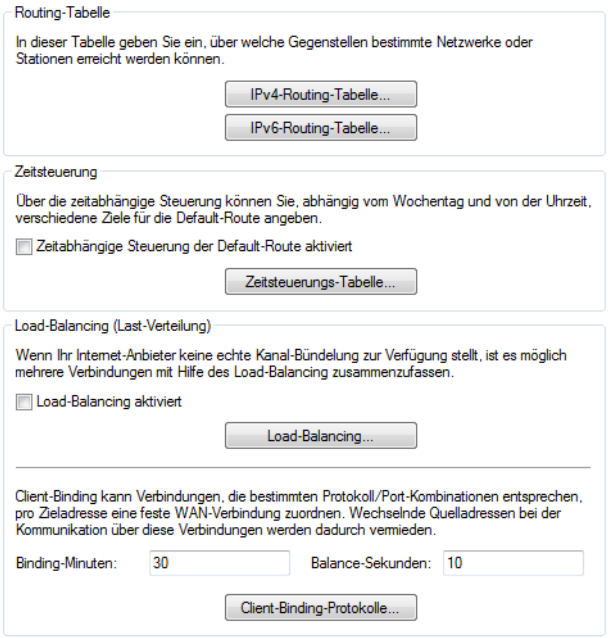
20. Wählen Sie im Drop-Down-Menü **Router Advertisements senden** die Option "Ja".



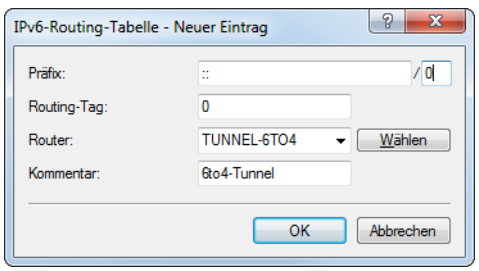
21. Übernehmen Sie alle weiteren Default-Werte unverändert.

22. Speichern Sie die Eingaben mit **OK**.

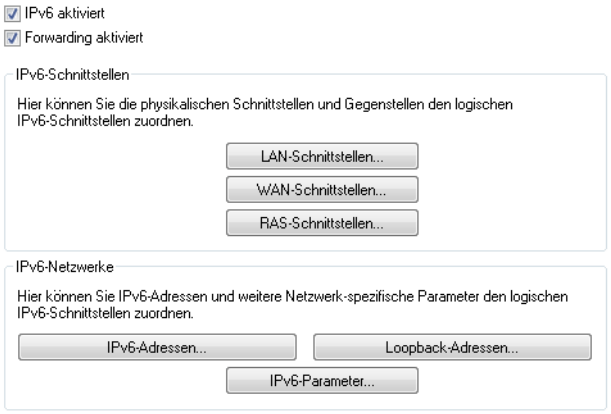
23. Wechseln Sie in das Verzeichnis **IP-Router** > **Routing**.



24. Öffnen Sie die **IPv6-Routing-Tabelle** und klicken auf **Hinzufügen**.



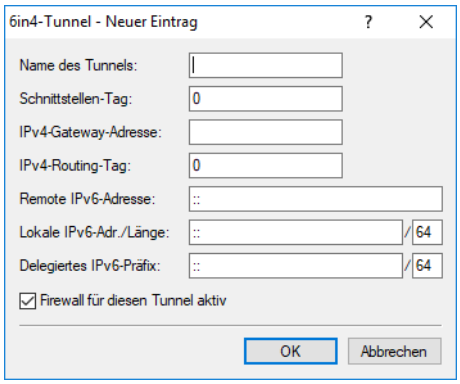
25. Vergeben Sie als **Präfix** den Wert "::/0".
26. Übernehmen Sie für **Routing-Tag** den Default-Wert "0".
27. Im Feld **Router** wählen Sie aus der Liste den Namen des Tunnels aus, den Sie definiert haben, im Beispiel oben "TUNNEL-6TO4".
28. Vergeben Sie einen aussagekräftigen **Kommentar** für diesen Eintrag.
29. Speichern Sie die Eingaben mit **OK**.
30. Wechseln Sie in das Verzeichnis **IPv6** > **Allgemein** und aktivieren Sie den IPv6-Stack.



7.6.6.2 Konfiguration eines 6in4-Tunnels

Über die Schaltfläche **6in4-Tunnel** öffnen Sie die Konfiguration für einen 6in4-Tunnel.

Klicken Sie auf **Hinzufügen**, um einen neuen Tunnel anzulegen.



Sie können die folgenden Parameter des Tunnels bestimmen:

Name des Tunnels

Bestimmt den Namen des 6in4-Tunnels.

Schnittstellen-Tag

Tragen Sie hier als Schnittstellen-Tag einen Wert ein, der das Netzwerk eindeutig spezifiziert. Alle Pakete, die auf diesem Netzwerk empfangen werden, werden intern mit diesem Tag markiert.

Das Schnittstellen-Tag ermöglicht eine Trennung der für dieses Netzwerk gültigen Routen auch ohne explizite Firewall-Regel.

IPv4-Gateway-Adresse

IPv4-Adresse des entfernten 6in4-Gateways. Der Tunnel wird nur aufgebaut, falls das Gateway per Ping erreichbar ist.

IPv4-Routing-Tag

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen entfernten Gateway ermittelt wird.

Remote IPv6-Adresse

IPv6-Adresse des entfernten Tunnelendpunkts auf dem Transfernetz , z. B. 2001:db8::1.

Lokale IPv6-Adr. / Länge

Lokale IPv6-Adresse des Gerätes auf dem Transfernetz z. B. 2001:db8::2/64.

Delegiertes IPv6-Präfix

Präfix, das vom entfernten Gateway zum lokalen Gerät geroutet wird und im LAN verwendet werden soll, z. B. 2001:db8:1:1::/64 oder 2001:db8:1::/48.

Firewall für diesen Tunnel aktiv

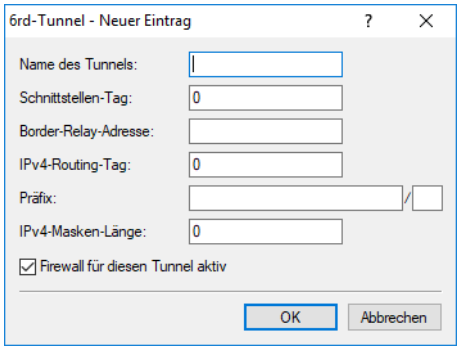
Hier haben Sie die Möglichkeit, die Firewall für dieses Tunnel-Interface ein- oder auszuschalten, wenn die globale IPv6-Firewall aktiv ist. Um die IPv6-Firewall global zu aktivieren, wählen Sie **IPv6-Firewall / QoS aktiviert** im Menü **Firewall / QoS** > **Allgemein**.

Wenn Sie die globale IPv6-Firewall deaktivieren, dann ist auch die Firewall einer einzelnen Schnittstelle inaktiv, selbst wenn Sie diese mit dieser Option aktiviert haben.

7.6.6.3 Konfiguration eines 6rd-Tunnels

Über die Schaltfläche **6rd-Tunnel** öffnen Sie die Konfiguration für einen 6rd-Tunnel.

Klicken Sie auf **Hinzufügen**, um einen neuen Tunnel anzulegen.



Sie können die folgenden Parameter des Tunnels bestimmen:

Name des Tunnels

Bestimmt den Namen des 6rd-Tunnels.

Schnittstellen-Tag

Tragen Sie hier als Schnittstellen-Tag einen Wert ein, der das Netzwerk eindeutig spezifiziert. Alle Pakete, die auf diesem Netzwerk empfangen werden, werden intern mit diesem Tag markiert.

Das Schnittstellen-Tag ermöglicht eine Trennung der für dieses Netzwerk gültigen Routen auch ohne explizite Firewall-Regel.

Border-Relay-Adresse

Dies ist die IPv4-Adresse des 6rd-Border-Relays.

Wird dieses Feld leer gelassen, so werden die Daten per DHCPv4 bezogen.

IPv4-Routing-Tag

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen entfernten Gateway ermittelt wird.

Präfix

Das vom Provider für 6rd-Dienste verwendete Präfix, z.B. 2001:db8::/32.

Wird das 6rd-Präfix über DHCPv4 zugewiesen (d.h. die Border-Relay-Adresse ist leer), so wird dieses Feld ignoriert bzw. kann leer bleiben.

IPv4-Masken-Länge

Definiert die Anzahl der höchstwertigen Bits der IPv4-Adressen, die identisch innerhalb einer 6rd-Domäne sind. Ist die Maskenlänge beispielsweise 0, so gibt es keine identischen Bits und die gesamte IPv4-Adresse wird verwendet, um das delegierte 6rd-Präfix zu erzeugen.

Die Maskenlänge wird vom Provider vorgegeben.

Beispiel: Die IPv4-Adresse des Routers sei 192.168.1.99 (in hex: c0a8:163). Dann sind beispielsweise folgende Kombinationen möglich:

6rd-Domäne	Maskenlänge	6rd-Präfix
2001:db8:1::/32	0	2001:db8:1:c0a8:163::/64
2001:db8:1:2::/48	16	2001:db8:1:2:163::/64
2001:db8:1:2:3300::/56	24	2001:db8:1:2:3363::/64

Standard ist 0.

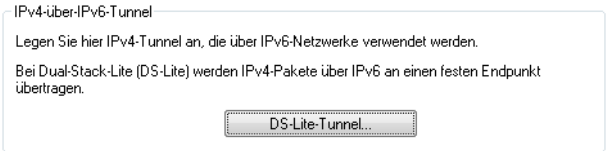
Firewall für diesen Tunnel aktiv

Hier haben Sie die Möglichkeit, die Firewall für dieses Tunnel-Interface ein- oder auszuschalten, wenn die globale IPv6-Firewall aktiv ist. Um die IPv6-Firewall global zu aktivieren, wählen Sie **IPv6-Firewall / QoS aktiviert** im Menü **Firewall / QoS** > **Allgemein**.

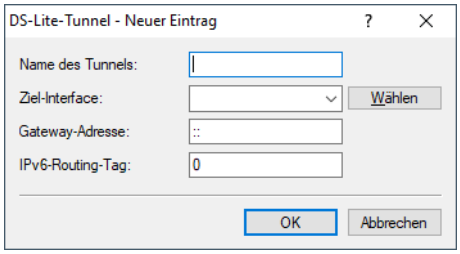
Wenn Sie die globale IPv6-Firewall deaktivieren, dann ist auch die Firewall einer einzelnen Schnittstelle inaktiv, selbst wenn Sie diese mit dieser Option aktiviert haben.

7.6.6.4 Einrichtung eines Dual-Stack Lite (DS-Lite) Tunnels

Einen DS-Lite-Tunnel richten Sie in LANconfig ein über **IPv6** > **Tunnel** mit einem Klick auf **DS-Lite-Tunnel**.



Klicken Sie anschließend auf **Hinzufügen** und geben Sie die Bezeichnung des Tunnels, die IPv6-Adresse des Gateways und das Routing-Tag ein.



Name des Tunnels

Dieser Eintrag bestimmt den Namen des IPv4-über-IPv6-Tunnels.

Ziel-Interface

Name des darunterliegenden WAN-Interface bzw. der darunterliegenden Gegenstelle, z. B. INTERNET. Max. 16 Zeichen in Großbuchstaben.

Gateway-Adresse

Dieser Eintrag definiert die Adresse des DS-Lite-Gateways, den sogenannten Address Family Transition Router (AFTR).

Die folgenden Werte sind möglich:

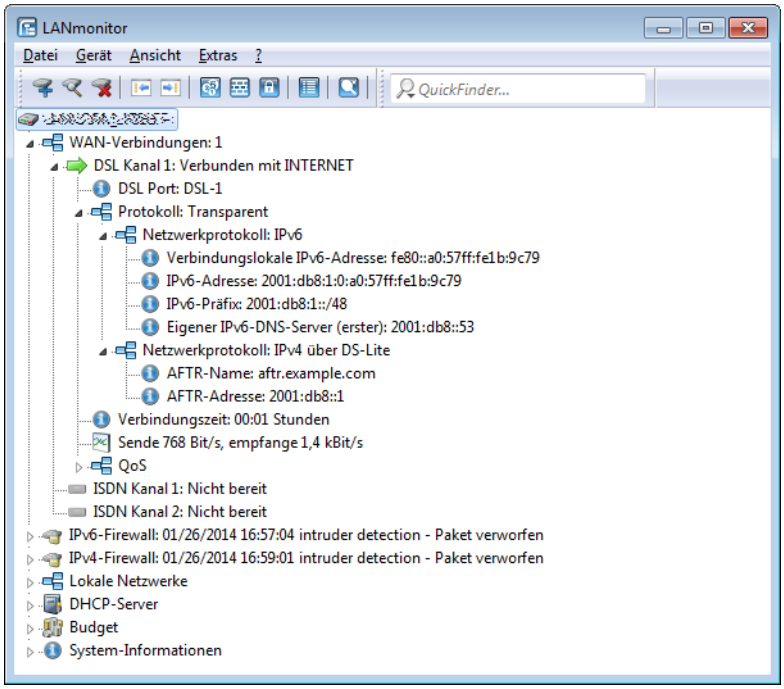
- Eine IPv6-Adresse, z. B. 2001:db8::1
- Ein per DNS auflösbarer FQDN (Fully Qualified Domain Name), z. B. aftr.example.com
- Die IPv6 Unspecified Address „::“ bestimmt, dass das Gerät die Adresse des AFTRs per DHCPv6 beziehen soll (Werkseinstellung).
- Ein leeres Feld verhält sich wie bei der Eingabe von „::“.

IPv6-Routing-Tag

Das Routing-Tag spezifiziert eindeutig die Route zum DS-Lite-Gateway.

Da bei DS-Lite das NAT durch den Provider erfolgt, ist die Funktion vieler Anwendungen von den Einstellungen des Provider-NATs abhängig (z. B. SIP, IRC oder IPSec). PPTP funktioniert über DS-Lite nicht. Wenn der Provider kein Portforwarding eingerichtet hat, funktionieren auch IPv4-Serverdienste nicht mehr.

Über den LANmonitor lassen sich die Status-Tabelle und die Anzahl der aktuellen DS-Lite-Verbindungen darstellen:

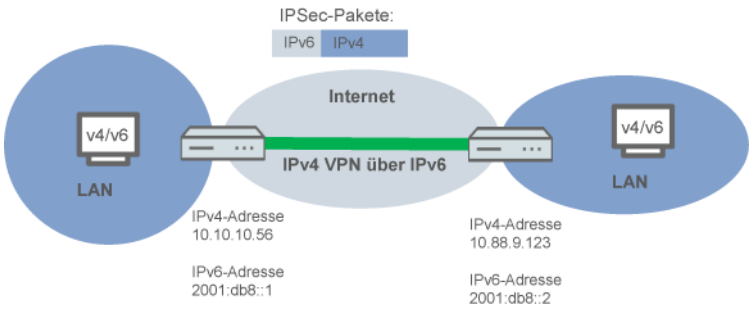


7.6.6.5 IPv4-VPN-Tunnel über IPv6

Bietet ein Provider keine öffentlichen IPv4-Adressen mehr an, so kann ein VPN-Tunnel, der IPv4-Netzwerke koppelt, auch über IPv6-WAN-Adressen aufgebaut werden.

Dazu müssen für die VPN-Gateway-Adressen IPv6-Adressen konfiguriert werden.

Im dargestellten Beispiel werden zwei lokale IPv4-Netzwerke über einen IPv4-VPN-Tunnel verbunden, welcher über eine IPv6-Internet-Verbindung aufgebaut wurde. Hierbei werden über die IPv6-Internetverbindung (nativ oder über Tunnelbroker) die IPv4-VPN-Pakete mit einem IPv6-Header an die Gegenstelle gesendet.



Setup-Assistent – IPv4-VPN-Verbindung über IPv6 einrichten

Der Setup-Assistent zur Verbindung zweier lokaler Netze unterstützt Sie bei der Einrichtung einer VPN-Verbindung.

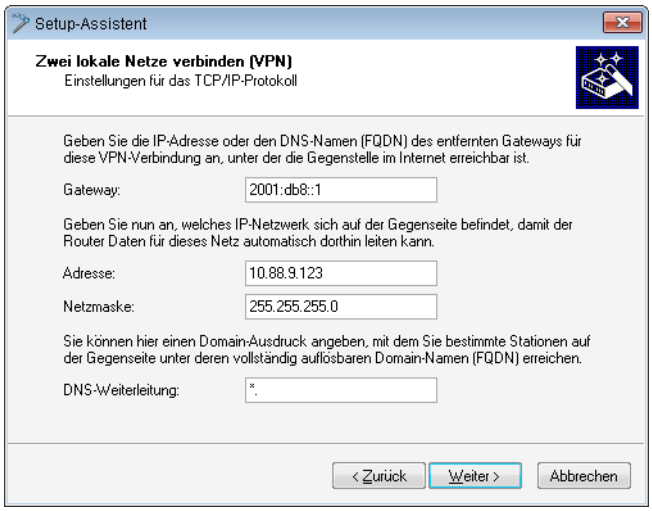
1. Starten Sie LANconfig.

   LANconfig sucht nun automatisch im lokalen Netz nach Geräten. Sobald LANconfig mit der Suche fertig ist, zeigt es in der Liste alle gefundenen Geräte mit Namen, evtl. einer Beschreibung, der IP-Adresse und dem Status an.

2. Markieren Sie Ihr Gerät im Auswahlfenster von LANconfig und wählen Sie die Schaltfläche **Setup Assistent** oder aus der Menüleiste den Punkt **Extras** > **Setup Assistent**.

   LANconfig liest zunächst die Gerätekonfiguration aus und zeigt dann das Auswahlfenster der möglichen Anwendungen.

3. Wählen Sie die Aktion **Zwei lokale Netze verbinden**.
4. Folgen Sie den Anweisungen des Assistenten und geben Sie die notwendigen Daten ein.
5. Geben Sie als Gateway-Adresse die IPv6-Adresse des Gateways ein.



6. Schließen Sie den Assistenten dann mit **Fertig stellen** ab.

   Der Setup-Assistent schreibt die Konfiguration in das Gerät.

8 Firewall

Für die meisten Firmen und viele Privatanwender ist eine Arbeit ohne das Internet nicht mehr denkbar. E-Mail und Web sind für die Kommunikation und Informationsrecherche unverzichtbar. Jede Verbindung der Rechner aus dem eigenen, lokalen Netzwerk mit dem Internet stellt aber eine potentielle Gefahr dar: Unbefugte können über diese Internet-Verbindung versuchen, Ihre Daten einzusehen, zu verändern oder Ihre Rechner zu manipulieren.

In diesem Kapitel widmen wir uns daher einem sehr wichtigen Thema: der Firewall als Abwehrmaßnahme vor diesen Zugriffen. Neben einer kurzen Einführung in das Thema Internetsicherheit zeigen wir Ihnen, welchen Schutz Ihnen ein Router bei richtiger Konfiguration bieten kann und wie Sie die entsprechenden Einstellungen konkret vornehmen.

8.1 Gefährdungsanalyse

Um die geeigneten Maßnahmen zur Gewährleistung der Sicherheit planen und umsetzen zu können, muss man sich zunächst einmal über die möglichen Gefahrenquellen im Klaren sein:

- Welche Gefahren bedrohen das eigene LAN bzw. die eigenen Daten?
- Über welche Wege verschaffen sich Eindringlinge den Zugang zu Ihrem Netzwerk?

Das Eindringen in geschützte Netzwerke bezeichnen wir im Weiteren dem allgemeinen Sprachgebrauch folgend als „Angriff", den Eindringling daher auch als „Angreifer".

8.1.1 Die Gefahren

Die Gefahren im Internet entspringen grundsätzlich ganz verschiedenen Motiven. Zum einen versuchen die Täter, sich persönlich zu bereichern oder die Opfer gezielt zu schädigen. Durch das immer stärker verbreitete Know-How der Täter ist das „Hacken" aber auch schon zu einer Art Sport geworden, bei dem sich oft Jugendliche darin messen, wer die Hürden der Internetsicherheit am schnellsten überwindet.

Was auch immer im einzelnen Fall das Motiv ist, die Absichten der Täter laufen meistens auf die folgenden Muster hinaus:

- Einblick in vertrauliche Informationen wie Betriebsgeheimnisse, Zugangsinformationen, Passwörter für Bankkonten etc.
- Nutzung der Rechner im LAN für die Zwecke der Eindringlinge, z. B. für die Verbreitung von eigenen Inhalten, Angriffe auf dritte Rechner, etc.
- Verändern der Daten auf den Rechnern im LAN, z. B. um sich auf diese Weise weitere Zugangsmöglichkeiten zu schaffen
- Zerstören von Daten auf den Rechnern im LAN
- Lahmlegen von Rechnern im LAN oder der Verbindung mit dem Internet

Wir beschränken uns hier auf die Angriffe auf lokale Netzwerke (LAN) bzw. auf Arbeitsplatzrechner und Server in solchen LANs.

8.1.2 Die Wege der Täter

Um ihrem Unwesen nachgehen zu können, brauchen die Täter natürlich zunächst einen Weg für den Zugriff auf Ihre Rechner und Daten. Im Prinzip stehen dazu folgende Wege offen, solange sie nicht gesperrt bzw. geschützt sind:

- Über die zentrale Internetverbindung, z. B. über einen Router
- Über dezentrale Verbindungen ins Internet, z. B. Modems an einzelnen PCs oder Mobiltelefone an Notebooks

- Über Funknetzwerke, die als Ergänzung zum drahtgebundenen Netzwerk eingesetzt werden

In diesem Kapitel betrachten wir ausschließlich die Wege über die zentrale Internetverbindung, über den Router.

Hinweise zum Schutz der Funknetzwerke entnehmen Sie bitte den entsprechenden Kapiteln dieses Referenz-Handbuchs bzw. der jeweiligen Gerätedokumentation.

8.1.3 Die Methoden

Normalerweise haben fremde Personen natürlich keinen Zugang zu Ihrem lokalen Netz oder den Rechnern darin. Ohne die entsprechenden Zugangsdaten oder Passwörter kann also niemand auf den geschützten Bereich zugreifen. Wenn das Ausspionieren dieser Zugangsdaten nicht möglich ist, versuchen die Angreifer auf einem anderen Weg zum Ziel zu kommen.

Ein grundlegender Ansatz dabei ist es, auf einem der zugelassenen Wege für den Datenaustausch Daten in das Netzwerk einzuschmuggeln, die dann von innen her den Zugang für den Angreifer öffnen. Durch Anhänge in E-Mails oder aktive Inhalte auf Webseiten kann so z. B. ein kleines Programm auf einen Rechner aufgespielt werden, der diesen anschließend zum Absturz bringt. Den Absturz nutzt das Programm dann, um einen neuen Administrator auf dem Rechner anzulegen, der anschließend aus der Ferne für weitere Aktionen im LAN genutzt werden kann.

Wenn der Zugang über E-Mail oder WWW nicht möglich ist, kann der Angreifer auch ausspähen, ob ein Server im LAN bestimmte Dienste anbietet, die er für seine Zwecke nutzen kann. Da die Dienste auf den Servern über bestimmte Ports im TCP/IP-Protokoll identifiziert werden, wird das Suchen nach offenen Ports auch als Port-Scanning bezeichnet. Der Angreifer startet dabei mit einem bestimmten Programm entweder allgemein im Internet oder nur auf bestimmten Netzwerken eine Anfrage nach den gewünschten Diensten und bekommt von ungeschützten Rechnern auch die entsprechende Antwort.

Eine dritte Möglichkeit besteht darin, sich in eine bestehende Datenverbindung einzuklinken und diese als Trittbrettfahrer zu nutzen. Dabei hört der Angreifer die Internetverbindung des Opfers ab und analysiert die Verbindungen. Eine aktive FTP-Verbindung nutzt er dann z. B., um auf dieser Verbindung seine eigenen Datenpakete mit in das zu schützende LAN zu schleusen.

Eine Variante dieser Methode ist der "man-in-the-middle". Dabei hört der Angreifer zunächst die Kommunikation zwischen zwei Rechnern ab und klinkt sich dann dazwischen.

8.1.4 Die Opfer

Die Frage nach dem Gefährdungsgrad für einen Angriff beeinflusst in hohem Maße den Aufwand, den man für die Abwehr treffen will oder muss. Um einzuschätzen, ob Ihr Netzwerk als Opfer für einen Angreifer besonders interessant ist, können Sie folgende Kriterien heranziehen:

- Besonders gefährdet sind Netzwerke von allgemein bekannten Firmen oder Institutionen, in denen wertvolle Informationen vermutet werden. Dazu gehören z. B. die Ergebnisse einer Forschungsabteilung, die von Industriespionen gerne eingesehen werden, oder Bankserver, auf denen das große Geld verteilt wird.
- In zweiter Linie sind aber auch die Netzwerke von kleineren Organisationen gefährdet, die vielleicht nur für ganz bestimmte Gruppen interessant sind. Auf den Rechnern von Steuerberatern, Rechtsanwälten oder Ärzten schlummern sicherlich auch einige Informationen, die für Dritte durchaus interessant sein können.
- Nicht zuletzt sind aber auch die Rechner und Netzwerke Opfer von Angriffen, die augenscheinlich überhaupt keinen Nutzen für die Angreifer bieten. Gerade die „Script-Kiddies", die aus jugendlichem Ehrgeiz ihre Möglichkeiten austesten, suchen manchmal einfach nur nach einem wehrlosen Opfer, um sich für höhere Aufgaben zu üben.

  Der Angriff auf einen eigentlich gar nicht interessanten, ungeschützten Rechner einer Privatperson kann auch dem Zweck dienen, eine Ausgangsbasis für Attacken auf die eigentlichen Ziele im zweiten Schritt vorzubereiten. Der „uninteressante" Rechner wird damit zur Quelle des Angriffs im zweiten Schritt, der Angreifer kann seine Identität verschleiern.

Unter dem Strich kann man also festhalten, dass die statistische Wahrscheinlichkeit für einen Angriff auf das Netzwerk der Global Player in der Industrie zwar größer ist als auf das Kleinst-Netzwerk im Home-Office. Aber auf der anderen

Seite ist es bei einem schutzlos im Internet aufgestellten Rechner wahrscheinlich nur eine Frage der Zeit, bis er evtl. sogar zufällig einmal das Opfer von Angriffen wird.

8.2 Was ist eine Firewall?

Der Begriff der „Firewall" wird sehr unterschiedlich interpretiert. Wir möchten an dieser Stelle erläutern, was im Rahmen dieses Handbuchs mit der Firewall gemeint ist:

Eine Firewall ist eine Zusammenstellung von Komponenten, die an einer zentralen Stelle den Datenaustausch zwischen zwei Netzwerken überwacht. Meistens überwacht die Firewall dabei den Datenaustausch zwischen einem internen, lokalen Netzwerk (LAN) und einem externen Netzwerk wie dem Internet.

Die Firewall kann dabei aus Hard- und / oder Softwarekomponenten bestehen:

- In reinen Hardware-Systemen läuft oft die Firewall-Software auf einem proprietären Betriebssystem.
- Die Firewall-Software kann aber auch auf einem normalen Rechner mit Linux, Unix oder Windows laufen, der für diese Aufgabe abgestellt wurde.
- Als dritte und häufig anzutreffende Alternative läuft die Firewall-Software direkt in dem Router, der das LAN mit dem Internet verbindet.

Wir betrachten in den folgenden Abschnitten nur die Firewall in einem Router.

Die Funktionen „Intrusion Detection" und „DoS-Abwehr" gehören in manchen Anwendungen mit zum Umfang einer Firewall. In diesem Router sind diese Funktionen natürlich auch enthalten, aber als separate Module neben der Firewall realisiert. Weitere Informationen dazu finden Sie in den Abschnitten *Abwehr von Einbruchsversuchen: Intrusion Detection* auf Seite 686 und *Schutz vor Denial-of-Service-Angriffen* auf Seite 687.

8.2.1 Die Aufgaben einer Firewall

8.2.1.1 Prüfung der Datenpakete

Wie überwacht die Firewall den Datenverkehr? Im Prinzip arbeitet die Firewall wie ein Pförtner für Datenpakete: Jedes Paket wird daraufhin geprüft, ob es die Türe des Netzwerks (die Firewall) in der gewünschten Richtung passieren darf oder nicht. Für diese Prüfung werden verschiedene Kriterien verwendet, die im Sprachgebrauch der Firewalls „Regeln" oder „Richtlinien" bezeichnet werden. Nach der Art der Informationen, die für die Erstellung der Regeln verwendet und im Betrieb der Firewall geprüft werden, unterscheidet man verschiedene Typen von Firewalls.

Wichtig ist vor allem der Aspekt der zentralen Positionierung: nur wenn wirklich der gesamte Datenverkehr zwischen innen und außen über die Firewall läuft, kann sie ihre Aufgabe sicher erfüllen. Jeder alternative Weg kann die Sicherheit der Firewall herabsetzen oder gar ausschalten. Diese zentrale Stellung der Firewall vereinfacht nebenbei auch die Wartung: eine Firewall als gemeinsamer Übergang zwischen zwei Netzwerken ist sicherlich einfacher zu pflegen als eine „Personal Firewall" auf jedem der im LAN angeschlossenen Rechner.

Prinzipiell arbeiten Firewalls an der Schnittstelle zwischen zwei oder mehreren Netzwerken. Für die folgenden Ausführungen werden wir als Beispiel nur den Übergang zwischen einem lokalen Netzwerk in einem Unternehmen und dem Internet betrachten. Diese Erklärungen lassen sich aber sinngemäß auch auf andere Netzwerk-Konstellationen übertragen, z. B. für den Schutz eines Subnetzes der Personalabteilung in einem Unternehmen gegen die restlichen Netzwerkbenutzer.

8.2.1.2 Protokollierung und Alarmierung

Eine wichtige Funktion einer Firewall ist neben dem Prüfen der Datenpakete und der richtigen Reaktion auf die Ergebnisse dieser Prüfung auch die Protokollierung aller Aktionen, die bei der Firewall ausgelöst wurden. Durch die Auswertung dieser Protokolle kann der Admin Rückschlüsse auf die erfolgten Angriffe ziehen und auf Grund dieser Informationen ggf. die Konfiguration der Firewall weiter verbessern.

Die Protokollierung alleine kommt aber manchmal zu spät. Oft kann durch ein sofortiges Eingreifen des Admins ein größerer Schaden verhindert werden. Aus diesem Grund verfügen Firewalls meistens über eine Alarmierungsfunktion, bei der die Meldungen der Firewall z. B. per E-Mail an den Administrator gemeldet werden.

8.2.2 Unterschiedliche Typen von Firewalls

Im Laufe der letzten Jahre hat sich die Arbeitsweise von Firewalls immer weiter entwickelt. Unter dem Oberbegriff Firewall werden eine ganze Reihe unterschiedlicher technischer Konzepte angeboten, mit denen das LAN geschützt werden soll. Hier stellen wir die wichtigsten Typen vor.

8.2.2.1 Paketfilter

Von einer paketfilterbasierten Firewall spricht man, wenn der Router nur die Angaben im Header der Datenpakete prüft und anhand dieser Informationen entscheidet, ob das Paket durchgelassen werden soll oder nicht. Zu den geprüften Informationen der Datenpakete gehören:

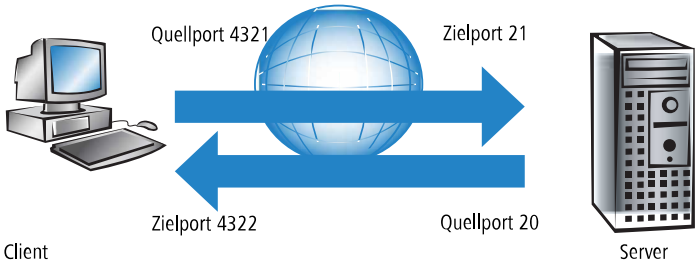
- IP-Adresse von Quelle und Ziel
- Übertragungsprotokoll (TCP, UDP oder ICMP)
- Portnummern von Quelle und Ziel
- MAC-Adresse

Die in einer paketfilterorientierten Firewall definierten Regeln legen z. B. fest, ob die Pakete von einem bestimmten IP-Adresskreis in das lokale Netzwerk weitergeleitet werden dürfen oder ob Pakete für bestimmte Dienste (d. h. mit speziellen Portnummern) gefiltert werden sollen. Durch diese Maßnahmen kann die Kommunikation mit bestimmten Rechnern, ganzen Netzwerken oder über bestimmte Dienste eingeschränkt oder verhindert werden. Die Regeln können dabei auch kombiniert werden, so kann z. B. der Zugang zum Internet über den TCP-Port 80 nur Rechnern mit bestimmten IP-Adressen erlaubt werden, während dieser Dienst für alle anderen Rechner gesperrt ist.

Die Konfiguration von paketfilternden Firewalls ist recht einfach, die Liste mit den zugelassenen oder verbotenen Paketen kann sehr schnell erweitert werden. Da auch die Anforderungen an die Performance eines Paketfilters mit recht geringen Mitteln erreicht werden kann, sind Paketfilter in der Regel direkt in Routern implementiert, die ohnehin als Schnittstelle zwischen den Netzwerken eingesetzt werden.

Nachteilig für die Paketfilter wirkt sich aus, dass die Liste der Regeln nach einiger Zeit nicht mehr so einfach zu überschauen ist. Außerdem werden bei einigen Diensten die Ports für die Verbindung dynamisch ausgehandelt. Um diese Kommunikation zu ermöglichen, muss der Administrator also alle dazu möglicherweise verwendeten Ports offen lassen, was der Grundausrichtung in den meisten Sicherheitskonzepten entgegenspricht.

Ein Beispiel für einen Vorgang, der für einfache Paketfilter recht problematisch ist, ist der Aufbau einer FTP-Verbindung von einem Rechner im eigenen LAN zu einem FTP-Server im Internet. Beim üblicherweise verwendeten aktiven FTP sendet der Client (aus dem geschützten LAN) eine Anfrage von einem Port im oberen Bereich (>1023) an den Port 21 des Servers. Dabei teilt der Client dem Server mit, auf welchem Port er die Verbindung erwartet. Der Server baut daraufhin von seinem Port 20 eine Verbindung zum gewünschten Port des Clients auf.



Um diesen Vorgang zu ermöglichen, muss der Administrator des Paketfilters alle Ports für eingehende Verbindungen öffnen, da er nicht vorher weiß, zu welchen Ports der Client die FTP-Verbindung anfordert. Eine Alternative ist über das passive FTP gegeben. Dabei baut der Client selbst die Verbindung zum Server auf über einen Port, den er vorher dem Server mitgeteilt hat. Dieses Verfahren wird jedoch nicht von allen Clients/Servern unterstützt.

Wenn man die Firewall weiterhin mit einem Pförtner vergleicht, prüft dieser Türsteher nur, ob er den Boten mit dem Paket an der Tür kennt oder nicht. Wenn der Kurier bekannt ist und schon einmal in das Gebäude hinein durfte, darf er auch bei allen folgenden Aufträgen ungehindert und unkontrolliert in das Gebäude bis zum Arbeitsplatz des Empfängers.

8.2.2.2 Stateful-Packet-Inspection

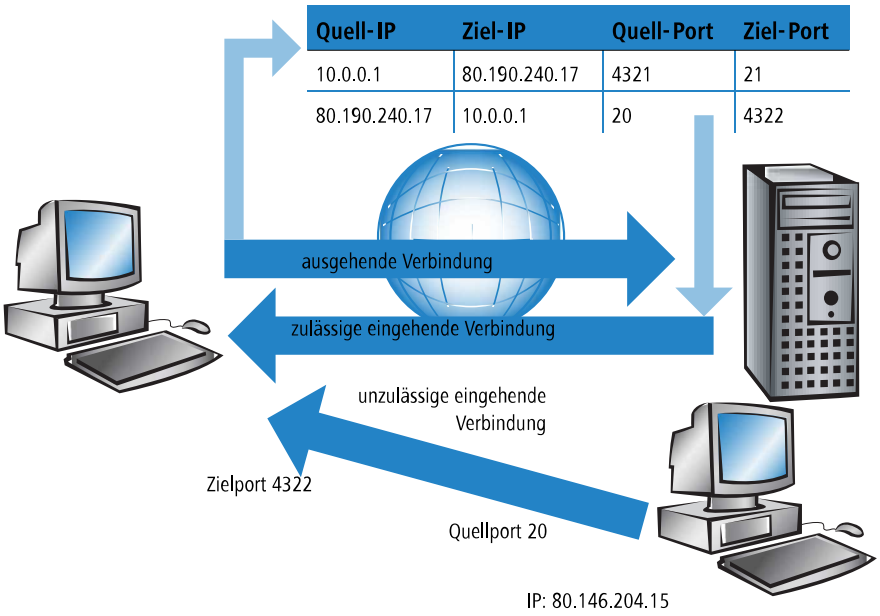
Die Stateful-Packet-Inspection (SPF) oder kurz Stateful Inspection erweitert den Ansatz der Paketfilter um eine Prüfung weiterer Verbindungsinformationen. Neben der eher statischen Tabelle mit den zugelassenen Ports und Adressbereichen wird bei dieser Variante eine dynamische Tabelle gepflegt, in die Informationen über den Zustand der einzelnen Verbindungen eingetragen werden. Diese dynamische Tabelle ermöglicht es, alle gefährdeten Ports zunächst zu sperren und nur bei Bedarf für eine zulässige Verbindung (festgelegt durch Quell- und Zieladresse) einen Port zu öffnen. Das Öffnen der Ports geschieht dabei immer nur vom geschützten Netzwerk zum ungeschützen hin, also meistens vom LAN zum WAN (Internet). Datenpakete, die nicht zu einer in der Zustandstabelle gespeicherten Verbindung gehören, werden automatisch verworfen.



Die Filter-Regeln einer Stateful-Inspection Firewall sind – anders als bei klassischen Portfilter-Firewalls – richtungsabhängig: Eine Verbindung kann immer nur von der Quelle zum Ziel aufgebaut werden; es sei denn, für die Rückrichtung ist ein expliziter Eintrag vorhanden. Ist eine Verbindung aufgebaut, so werden nur die zu dieser Verbindung gehörenden Datenpakete – in beide Richtungen natürlich – übertragen. Damit lassen sich z. B. alle Zugriffe, die unaufgefordert und nicht aus dem lokalen Netz heraus erfolgen, zuverlässig abblocken.

Zusätzlich kann die Stateful Inspection aus dem Verbindungsaufbau ableiten, ob dabei zusätzliche Kanäle für den Datenaustausch ausgehandelt werden. Einige Protokolle wie z. B. FTP (für den Datentransfer), T.120, H.225, und H.245 (für Netmeeting oder IP-Telefonie), PPTP (für VPN-Tunnel) oder IRC (für den Chat) signalisieren beim Aufbau der Verbindung vom LAN zum Internet durch den verwendeten Quell-Port, dass sie weitere Ports mit der Gegenstelle vereinbaren. Die Stateful Inspection trägt dann auch diese zusätzlichen Ports in der Verbindungsliste mit ein, natürlich auch hier wieder beschränkt auf die jeweiligen Quell- und Ziel-Adressen.

Sehen wir uns dazu noch einmal das Beispiel FTP-Download an. Bei Starten der FTP-Sitzung baut der Client vom Quell-Port '4321' eine Verbindung zum Ziel-Port '21' beim Server auf. Die Stateful Inspection erlaubt diesen ersten Aufbau, sofern das FTP-Protokoll von den lokalen Rechnern nach außen freigegeben ist. In die dynamische Tabelle trägt die Firewall Quell- und Zieladresse sowie die jeweiligen Ports ein. Gleichzeitig kann die Stateful Inspection die Steuerinformationen einsehen, die an den Port 21 des Servers gesendet werden. Aus diesen Steuersignalen geht hervor, dass der Client damit eine Verbindung des Servers von dessen Port 20 auf den Port 4322 des Clients anfordert. Die Firewall trägt auch diese Werte in die dynamische Tabelle ein, weil die Verbindung in das LAN hinein vom Client angefordert wird. Der Server kann also anschließend wie gewünscht die Daten an den Client senden.



Versucht hingegen ein anderer Rechner im Internet, den gerade offenen Port 4322 im LAN zu nutzen, um selbst Daten von seinem Port 20 auf dem geschützten Client abzulegen, wird dieser Versuch von der Firewall unterbunden, denn die IP-Adresse des Angreifers passt nicht zur erlaubten Verbindung!

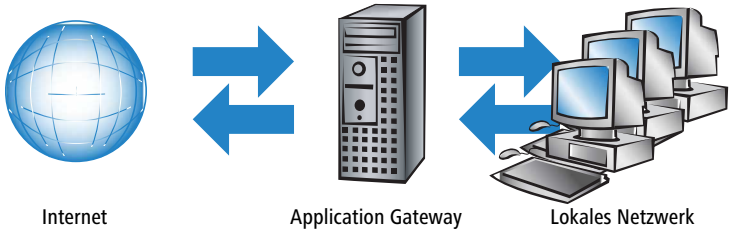
Nach der erfolgreichen Datenübertragung verschwinden die Einträge automatisch wieder aus der dynamischen Tabelle, die Ports werden also wieder geschlossen.

Eine Firewall mit Stateful-Inspection ist zudem meistens in der Lage, die empfangenen Datenpakete zu re-assemblieren, also einzelne Bestandteile zwischenzuspeichern und wieder zu einem gesamten Paket zusammenzubauen. Dadurch können bei fragmentierten Paketen nicht nur die einzelnen Teile von der Firewall geprüft werden, sondern auch das vollständige IP-Paket.

Dieser Pförtner macht seine Aufgabe also schon deutlich besser. Wenn in dieser Firma jemand einen Kurier bestellt, muss er parallel dazu auch den Pförtner anrufen und mitteilen, das er einen Kurier erwartet, um welche Uhrzeit der da sein wird und was auf dem Lieferschein des Paketes steht. Nur wenn diese Angaben beim Eintreffen des Kuriers mit dem Eintrag im Logbuch des Pförtners übereinstimmen, wird er den Kurier durchlassen. Bringt der Kurier nicht nur ein Paket, sondern gleich zwei, wird nur das mit dem richtigen Lieferschein durchgelassen. Ebenso wird auch ein zweiter Kurier, der Durchlass zu dem Mitarbeiter verlangt, an der Pforte abgewiesen.

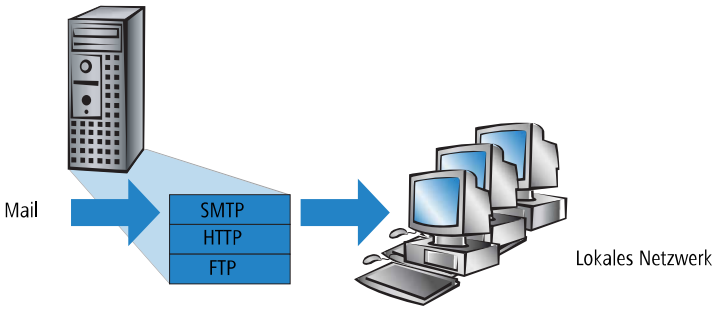
8.2.2.3 Application Gateway

Die Application Gateways erweitern die Adressprüfung der Paketfilter und die Verbindungsüberwachung der Stateful-Packet-Inspection um die Prüfung der Inhalte auf Anwendungsebene. Das Application Gateway läuft aufgrund der hohen Anforderungen an die Hardware-Performance in der Regel auf einem separaten Rechner. Dieser Rechner steht zwischen dem lokalen Netzwerk und dem Internet. Aus beiden Richtungen gesehen ist dieser Rechner die einzige Möglichkeit, mit dem jeweils anderen Netzwerk Daten auszutauschen. Es gibt keine direkte Verbindung zwischen den beiden Netzwerken, sondern immer nur bis zum Application Gateway.



Das Application Gateway steht damit als eine Art Vertreter (Proxy) für jedes der beiden Netzwerke da. Eine andere Bezeichnung für diese Konstellationen ist die des „dualhomed Gateway", weil dieser Rechner sozusagen in zwei Netzwerken zu Hause ist.

Für jede Anwendung, die über dieses Gateway erlaubt werden soll, wird auf dem Gateway ein eigener Dienst eingerichtet, z. B. SMTP für Mail, HTTP zum Surfen im Internet oder FTP für den Datendownload.



Dieser Dienst nimmt die Daten an, die von einer der beiden Seiten empfangen werden, und bildet sie für die jeweils andere Seite wieder ab. Was auf den ersten Blick wie ein ziemlich unnötiges Spiegeln vorhandener Daten aussieht, stellt bei näherem Hinsehen aber das tiefgreifende Konzept der Application Gateways dar: Es gibt in dieser Konstellation niemals eine direkte Verbindung z. B. zwischen einem Client im lokalen Netzwerk und einem Server im Internet. Die Rechner im LAN „sehen" immer nur den Proxy, die Rechner aus dem Internet ebenfalls. Diese physikalische Trennung von LAN und WAN macht es einem Angreifer schon sehr viel schwerer, in das geschützte Netzwerk einzudringen.

In der Übersetzung in das Pförtner-Beispiel wird das Paket hier am Tor abgegeben, der Kurier darf gar nicht selbst auf das Firmengelände. Der Pförtner nimmt das Paket an, öffnet es nach Prüfung von Anschrift und Lieferschein und kontrolliert den Inhalt. Wenn das Paket alle diese Hürden erfolgreich genommen hat, bringt ein firmeninterner Bote das Paket selbst weiter zum Empfänger in der Firma. Er wird damit zum Vertreter des Kuriers auf dem Firmengelände. Umgekehrt müssen alle Mitarbeiter, die ein Paket verschicken wollen, den Pförtner anrufen, der das Paket am Arbeitsplatz abholen lässt und am Tor an einen bestellten Kurier übergibt.

Die Funktion eines Application Gateways wird vom Gerät aufgrund der hohen Anforderungen an die Hardware nicht unterstützt.

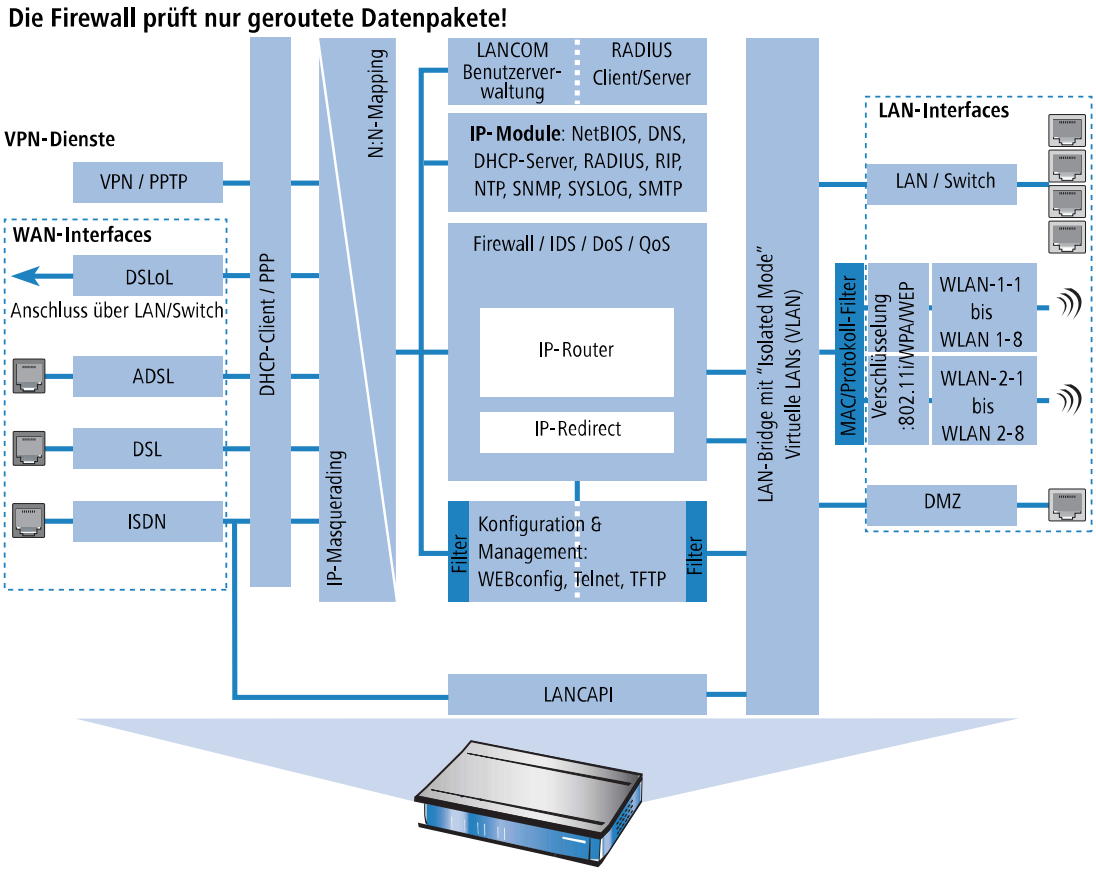
8.3 Die Firewall im Gerät

Nach den allgemeinen Erläuterungen zu den Gefahren aus dem Internet sowie den Aufgaben und Typen von Firewalls finden sich in diesem Kapitel Beschreibungen zu den speziellen Funktionen der Firewall im Gerät und Hinweise auf die konkrete Konfiguration.

Bei Geräten mit integrierter oder nachträglich über Software-Option freigeschalteter VoIP-Funktion werden die für die Voice-Verbindungen benötigen Ports automatisch freigeschaltet!

8.3.1 So prüft die Firewall im Gerät die Datenpakete

Die Firewall filtert aus dem gesamten Datenstrom, der über den IP-Router des Geräts läuft, diejenigen Datenpakete heraus, für die eine bestimmte Behandlung vorgesehen ist.



Die Firewall prüft nur die Datenpakete, die vom IP-Router im Gerät geroutet werden. In der Regel sind das die Datenpakete, die zwischen den internen Netzwerken (LAN, WLAN, DMZ) und der „Außenwelt" über eines der WAN-Interfaces ausgetauscht werden. Die Kommunikation z. B. zwischen LAN und WLAN untereinander wird normalerweise nicht über den Router abgewickelt, sofern die LAN-Bridge den direkten Austausch erlaubt. Hier wirken also auch nicht die Regeln der Firewall. Gleiches gilt für die so genannten „internen Dienste" wie Telnet, TFTP, SNMP und den Webserver für die Konfiguration über WEBconfig. Die Datenpakete dieser Dienste laufen nicht über den Router und werden daher auch nicht durch die Firewall beeinflusst.

Durch die Positionierung hinter dem Masquerading-Modul (aus Sicht des WANs) arbeitet die Firewall dabei mit den „echten" internen IP-Adressen der LAN-Stationen, nicht mit der nach außen bekannten Internetadresse des Geräts.

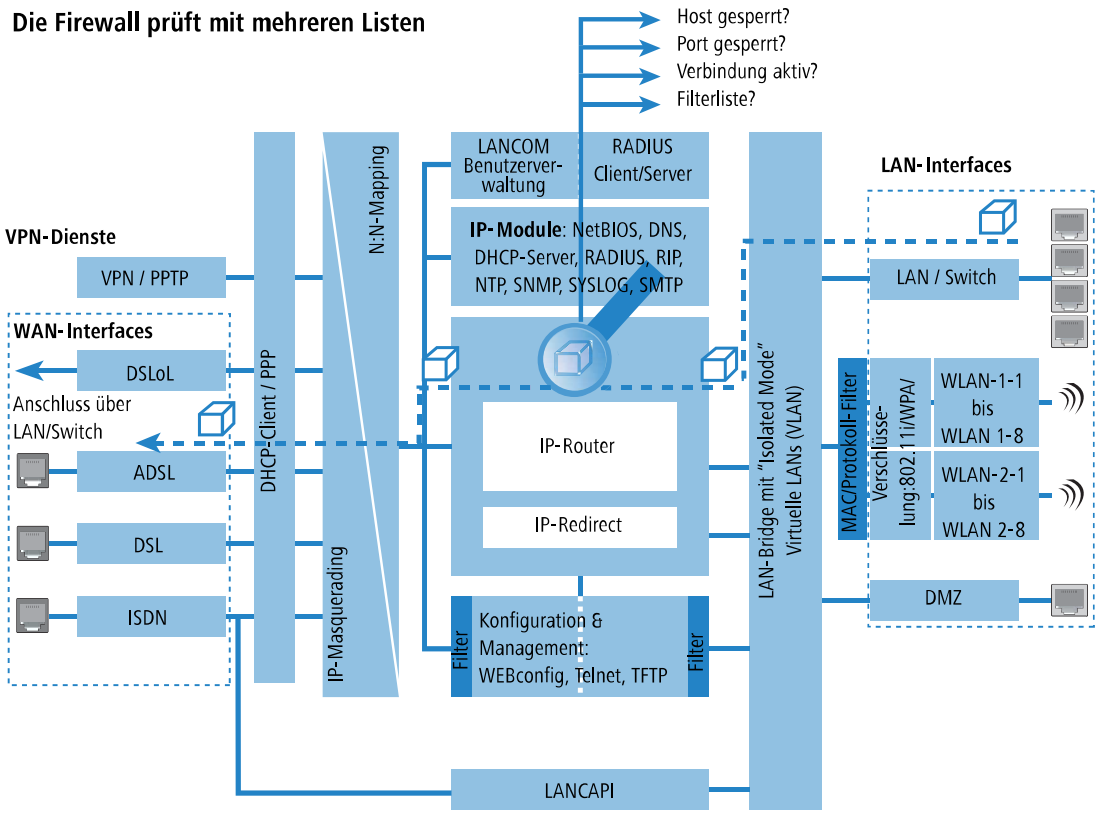
Die Firewall im Gerät verwendet für die Prüfung der Datenpakete mehrere Listen, die aus den Firewall-Regeln, den daraus ausgelösten Firewall-Aktionen oder den aktiven Datenverbindungen automatisch erzeugt werden:

- Hostsperrliste
- Portsperrliste
- Verbindungsliste

› Filterliste

Und so setzt die Firewall die Listen ein, wenn ein Datenpaket über den IP-Router geleitet werden soll:

1. Zuerst wird nachgeschaut, ob das Paket von einem Rechner kommt, der in der **Hostsperrliste** vermerkt ist. Ist der Absender gesperrt, wird das Paket verworfen.
2. Ist der Absender dort nicht gesperrt, wird in der **Portsperrliste** geprüft, ob die verwendete Port#8239;/ Protokoll-Kombination auf dem Zielrechner geschlossen ist. In diesem Fall wird das Paket verworfen.
3. Sind Absender und Ziel in den beiden ersten Listen nicht gesperrt, wird geprüft, ob für dieses Paket ein Verbindungseintrag in der **Verbindungsliste** existiert. Existiert ein solcher Eintrag, dann wird mit dem Paket so verfahren, wie in der Liste vermerkt ist.
4. Wird für das Paket kein Eintrag gefunden, dann wird die **Filterliste** durchsucht, ob ein passender Eintrag vorhanden ist und die dort angegebene Aktion ausgeführt. Wenn die Aktion besagt, dass das Paket akzeptiert werden soll, so wird ein Eintrag in der Verbindungsliste vorgenommen und etwaige weitere Aktionen dort vermerkt.



Existiert für ein Datenpaket keine explizite Firewall-Regel, so wird das Paket akzeptiert ('Allow-All'). Damit ist eine Abwärtskompatibilität zu bestehenden Installationen gegeben. Für einen maximalen Schutz durch die Stateful-Inspection beachten Sie bitte den Abschnitt *Aufbau einer expliziten Deny-All-Strategie* auf Seite 673.

Bleibt die Frage, woher die vier Listen ihre Informationen beziehen:

› In der Hostsperrliste werden die Stationen aufgeführt, die aufgrund einer Firewall-Aktion für eine bestimmte Zeit gesperrt sind. Die Liste ist dynamisch, neue Einträge können fortlaufend durch entsprechende Aktionen der Firewall hinzugefügt werden, nach Ablauf der Sperrzeit verschwinden die Einträge automatisch.

› In der Portsperrliste werden die Protokolle und Dienste aufgeführt, die aufgrund einer Firewall-Aktion für eine bestimmte Zeit gesperrt sind. Auch diese Liste ist dynamisch, neue Einträge können fortlaufend durch entsprechende Aktionen der Firewall hinzugefügt werden, nach Ablauf der Sperrzeit verschwinden die Einträge automatisch.

› In der Verbindungsliste wird für jede aufgebaute Verbindung ein Eintrag vorgenommen, wenn das geprüfte Paket von der Filterliste akzeptiert wird. In der Verbindungsliste wird festgehalten, von welcher Quelle zu welchem Ziel,

über welches Protokoll und welchen Port eine Verbindung aktuell erlaubt ist. Darüber hinaus wird in dieser Liste festgehalten, wie lange der Eintrag noch in der Liste stehen bleibt und welche Firewall-Regel den Eintrag erzeugt hat. Diese Liste ist sehr dynamisch und permanent „in Bewegung".

- Die Filterliste wird aus den Regeln der Firewall erzeugt. Die darin enthaltenen Filter sind statisch und ändern sich nur beim Hinzufügen, Bearbeiten oder Löschen von Firewall-Regeln.

Alle Listen, die von der Firewall zur Prüfung der Datenpakete herangezogen werden, basieren also letztendlich auf den Firewall-Regeln (*Die Parameter der Firewall-Regeln* auf Seite 664).

8.3.2 Besondere Protokolle

Ein wichtiger Punkt bei der Verbindungsüberwachung ist die Behandlung von Protokollen, die dynamisch Ports und#8239;/ oder Adressen aushandeln, über die die weitere Kommunikation passiert. Beispiele für diese Protokolle sind FTP oder auch viele UDP-basierte Protokolle. Hier ist es nötig, dass zusätzlich zu der ersten Verbindung ggf. weitere Verbindungen geöffnet werden. (siehe dazu auch *Unterschiedliche Typen von Firewalls* auf Seite 651).

8.3.2.1 UDP-Verbindungen

UDP ist eigentlich ein zustandsloses Protokoll, trotzdem kann man auch bei UDP-basierten Protokollen von einer nur kurzfristigen Verbindung sprechen, da es sich meistens um Request#8239;/ Response-basierte Protokolle handelt, bei denen ein Client seinen Request an den Well-Known Port des Servers (z. B. 53 für DNS) richtet, und dieser darauf den Response wieder an den vom Client gewählten Quellport sendet:

Port Client	Verbindung	Port Server
12345	Request	53
	→	
12345	Response	53
	←	

Wenn der Server hingegen größere Datenmengen z. B. über TFTP senden will und auf dem Well-Known Port nicht zwischen Requests und Acknowledges unterscheiden möchte oder kann, so schickt er zunächst das Response-Paket an den Quellport des Absenders. Dabei setzt er aber als eigenen Quellport einen freien Port ein, auf dem er nun mit dem Client Daten austauschen möchte:

Port Client	Verbindung	Port Server
12345	Request	69
	→	
12345	Response	54321
	←	
12345	AckData	54321
	→	
12345	Data/Ack	54321
	←	

Während sich die Datenübertragung nun über die Ports 12345 und 54321 abspielt, kann der Server auf dem Well-Known Port (69) weitere Requests annehmen. Wenn das Gerät eine „Deny-All-Strategie" verfolgt, wird durch die erste Anfrage des Clients ein Eintrag in der Verbindungsliste erzeugt, der nur die Datenpakete des Servers auf Port 69 zulässt. Die Antwort des Servers würde dabei also einfach verworfen. Um dies zu verhindern, wird beim Anlegen des Eintrags in der Verbindungsliste der Zielport der Verbindung zunächst freigehalten, und erst beim Eintreffen des ersten Antwortpakets gesetzt, wodurch beide möglichen Fälle einer UDP Verbindung abgedeckt werden.

8.3.2.2 TCP-Verbindungen

TCP-Verbindungen können nicht einfach nur durch die Prüfung der Ports nachgehalten werden. Bei einigen Protokollen wie z. B. FTP oder PPTP sind Prüfungen der Nutzdaten nötig, um alle später ausgehandelten Verbindungen zu öffnen, und nur die wirklich zu den Verbindungen gehörenden Pakete zu akzeptieren. Dies entspricht einer vereinfachten Version dessen, was auch beim IP-Masquerading gemacht wird, nur ohne Adress- und Port-Mapping. Es reicht aus, die Verhandlung nachzuverfolgen, die entsprechenden Ports zu öffnen und mit der Hauptverbindung zu verknüpfen. Damit werden diese Ports einerseits mit dem Schließen der Hauptverbindung ebenfalls geschlossen, und andererseits hält der Datenverkehr auf den Nebenverbindungen auch die Hauptverbindung weiter offen.

8.3.2.3 ICMP-Verbindungen

Für ICMP werden zwei Fälle unterschieden: Das sind zum einen die ICMP-Request / Reply-Verbindungen, wie sie z. B. beim "ping" verwendet werden, zum anderen die ICMP-Fehlermeldungen, die als Antwort auf ein beliebiges IP-Paket empfangen werden können.

ICMP Request / Reply-Verbindungen können eindeutig durch den vom Initiator verwendeten Identifier zugeordnet werden, d. h. in der Zustandsdatenbank wird beim Senden eines ICMP-Requests ein Eintrag erstellt, der nur ICMP-Replies mit dem korrekten Identifier durchlässt. Alle anderen ICMP-Replies werden stillschweigend verworfen.

Bei ICMP-Fehlermeldungen steht der IP-Header und die ersten 8 Bytes des IP-Pakets (i. A. UDP- oder TCP-Header) innerhalb des ICMP-Pakets. Anhand dieser Information wird beim Empfang einer ICMP-Fehlermeldung der zugehörige Eintrag in der Zustandsdatenbank gesucht. Das Paket wird nur weitergeleitet, wenn ein solcher Eintrag existiert, ansonsten wird es stillschweigend verworfen. Zusätzlich dazu werden potentiell gefährliche ICMP-Fehlermeldungen (Redirect-Route) herausgefiltert.

8.3.2.4 Verbindungen sonstiger Protokolle

Bei allen anderen Protokollen können keine verwandten Verbindungen nachgehalten werden, d. h. bei ihnen kann nur eine Verbindung zwischen den beteiligten Hosts in der Zustandsdatenbank aufgenommen werden. Diese können auch nur von einer Seite aus initiiert werden, es sei denn, in der Firewall ist ein dedizierter Eintrag für die "Gegenrichtung" vorhanden.

8.3.3 Allgemeine Einstellungen der Firewall

Neben den einzelnen Firewall-Regeln, die für die Einträge in den Filter- Verbindungs- und Sperrlisten sorgen, gelten einige Einstellungen für die Firewall allgemein:

- *Firewall / QoS-Aktivierung*
- *Administrator-E-Mail*
- *Fragmente*
- *Sitzungswiederherstellung*
- *Ping-Block*
- *Stealth-Modus*
- *Authentifizierungs-Port tarnen*
- *Applikations-Definitionen*
- *Layer-7-Anwendungserkennung*
- *Anwendungsbasiertes Routing*

8.3.3.1 Firewall / QoS-Aktivierung

Mit dieser Option wird die gesamte Firewall inklusive der Quality-of-Service-Funktionen jeweils für IPv4 respektive IPv6 ein- bzw. ausgeschaltet.

Bitte beachten Sie, dass die Funktionen des N:N-Mapping nur wirksam sind, wenn die Firewall eingeschaltet ist!

8.3.3.2 Administrator-E-Mail

Zu den Aktionen, die die Firewall auslösen können, gehört auch die Alarmierung des Administrators per E-Mail. Die Administrator-E-Mail ist die Mail-Adresse, an die die entsprechenden Alarmierungs-Mails verschickt werden.

8.3.3.3 Fragmente

Manche Angriffe aus dem Internet versuchen, die Firewall durch fragmentierte Pakete (also in mehrere kleine Einheiten aufgeteilte Pakete) zu überlisten. Zu den Haupteigenschaften einer Stateful Inspection gehört auch die Fähigkeit, fragmentierte Pakete wieder zusammenzusetzen, um anschließend das gesamte IP-Paket prüfen zu können.

Das gewünschte Verhalten der Firewall kann zentral eingestellt werden. Dabei stehen folgende Möglichkeiten zur Auswahl:

- **Filtern**: Die fragmentierten Pakete werden von der Firewall direkt verworfen.
- **Weiterleiten**: Die fragmentierten Pakete werden ohne weitere Prüfung von der Firewall weitergeleitet, sofern die gültigen Filtereinstellungen das zulassen.
- **Re-assemblieren**: Die fragmentierten Pakete werden zwischengespeichert und wieder zu einem kompletten IP-Paket zusammengesetzt. Das wieder zusammengesetzte Paket wird dann nach den gültigen Filtereinstellungen geprüft und entsprechend behandelt.

8.3.3.4 Sitzungswiederherstellung

Die Firewall trägt in der Verbindungsliste alle aktuell erlaubten Verbindungen ein. Die Einträge verschwinden nach einer bestimmten Zeit (Timeout) automatisch wieder aus der Verbindungsliste, wenn keine Daten über die Verbindung übertragen werden und den Timeout zurücksetzen.

Manchmal werden die Verbindungen gemäß den allgemeinen Alterungs-Einstellungen beendet, bevor die mit einer Anfrage angeforderten Datenpakete von der Gegenstelle empfangen wurden. In diesem Fall steht möglicherweise in der Verbindungsliste noch ein Eintrag für eine zulässige Verbindung, die Verbindung selbst ist aber nicht mehr vorhanden.

Der Parameter "Sitzungswiederherstellung" bestimmt das Verhalten der Firewall für Pakete, die auf eine ehemalige Verbindung schließen lassen:

- **Verbieten**: Die Firewall stellt die Sitzung auf keinen Fall wieder her und verwirft das Paket.
- **Verbieten für Default-Route**: Die Firewall stellt die Sitzung nur wieder her, wenn das Paket nicht über die Default-Route empfangen wurde.
- **Verbieten für WAN-Interfaces**: Die Firewall stellt die Sitzung nur wieder her, wenn das Paket nicht über eines der WAN-Interfaces empfangen wurde.
- **Erlauben**: Die Firewall stellt die Verbindung grundsätzlich wieder her, wenn das Paket zu einer "ehemaligen" Verbindung aus der Verbindungsliste gehört.



Da die Funktion der virtuellen Router auf der Auswertung der Schnittstellen-Tags basiert, müssen neben den ungetaggten Default-Routen auch weitere Routen als „Default-Routen" einbezogen werden:

- Wenn ein Paket auf einem **WAN-Interface** empfangen wird, dann gilt diese WAN-Schnittstelle für die Firewall als Defaultroute, wenn entweder eine getaggte oder eine ungetaggte Defaultroute auf diese WAN-Schnittstelle verweist.
- Wenn ein Paket auf einem **LAN-Interface** empfangen wird und auf eine WAN-Schnittstelle geroutet werden soll, dann gilt diese WAN-Schnittstelle als Defaultroute, wenn entweder die ungetaggte Defaultroute oder eine mit dem Interface-Tag getaggte Defaultroute auf diese WAN-Schnittstelle verweist.

Ebenso greifen Defaultrouten-Filter auch, wenn sich die Defaultroute im LAN befindet. Hierbei gilt, dass der Filter dann greift, wenn

- ein Paket über ein getaggtes LAN-Interface empfangen wurde und über eine mit dem Interface getaggte Default-Route gesendet werden soll, oder
- ein Paket von einem weiteren Router in einem getaggten LAN-Interface empfangen wurde und eine mit dem Interface-Tag versehene Default-Route zur Quelladresse des Pakets existiert, oder
- ein Paket vom WAN empfangen wurde und auf eine beliebig getaggte Default-Route im LAN gesendet werden soll

8.3.3.5 Ping-Blocking

Eine – nicht unumstrittene – Methode, die Sicherheit zu erhöhen, ist das Verstecken des Routers; frei nach der Methode: „Wer mich nicht sieht, wird auch nicht versuchen mich anzugreifen…". Viele Angriffe beginnen mit der Suche nach Rechnern und / oder offenen Ports über eigentlich recht harmlose Anfragen, z. B. mit Hilfe des ping-Befehls oder mit einem Portscan. Jede Antwort auf diese Anfragen, auch die „Ich bin nicht hier"-Antwort, zeigt dem Angreifer, dass er ein potenzielles Ziel gefunden hat. Denn wer antwortet, der ist auch da. Um diese Rückschlüsse zu verhindern, kann das Gerät die Antworten auf diese Anfragen unterdrücken.

Um dies zu erreichen, kann das Gerät angewiesen werden, ICMP-Echo-Requests nicht mehr zu beantworten. Gleichzeitig werden auch die bei einem traceroute benutzten TTL-Exceeded Meldungen unterdrückt, so dass das Gerät weder durch ein ping noch ein traceroute gefunden werden kann.

Mögliche Einstellungen sind:

- **Aus**: ICMP-Antworten werden nicht blockiert
- **Immer**: ICMP-Antworten werden immer blockiert
- **WAN**: ICMP-Antworten werden auf allen WAN-Verbindungen blockiert
- **Default Route**: ICMP-Antworten werden auf der Default-Route (i.d.R. Internet) blockiert

Für die Auswahl der „Default-Routen" gelten hier die gleichen Hinweise wie bei *Sitzungswiederherstellung* auf Seite 659.

8.3.3.6 TCP-Stealth-Modus

Neben ICMP-Meldungen verrät auch das Verhalten bei TCP- und UDP-Verbindungen, ob sich an der angesprochenen Adresse ein Rechner befindet. Je nach umgebendem Netzwerk kann es sinnvoll sein, wenn TCP- und UDP-Pakete einfach verworfen werden, anstatt mit einem TCP-Reset bzw. einer ICMP-Meldung (port unreachable) zu antworten, wenn kein Listener für den jeweiligen Port existiert. Das jeweils gewünschte Verhalten kann im Gerät eingestellt werden.

Werden Ports ohne Listener versteckt, so ergibt sich auf maskierten Verbindungen das Problem, dass der "authenticate"- bzw. "ident"-Dienst nicht mehr funktioniert (bzw. nicht mehr korrekt abgelehnt wird). Der entsprechende Port kann daher gesondert behandelt werden (*Authentifizierungs-Port tarnen* auf Seite 660).

Mögliche Einstellungen sind:

- **aus**: Alle Ports sind geschlossen und TCP-Pakete werden mit einem TCP-Reset beantwortet
- **immer**: Alle Ports sind versteckt und TCP-Pakete werden stillschweigend verworfen.
- **WAN**: Auf der WAN-Seite sind alle Ports versteckt und auf der LAN-Seite geschlossen
- **Default-Route**: Die Ports sind auf der Default-Route (i.d.R. Internet) versteckt und auf allen anderen Routen geschlossen

Für die Auswahl der „Default-Routen" gelten hier die gleichen Hinweise wie bei *Sitzungswiederherstellung* auf Seite 659.

8.3.3.7 Authentifizierungs-Port tarnen

Wenn TCP- oder UDP-Ports versteckt werden, können z. B. die Anfragen von Mailservern zur Authentifizierung der Benutzer nicht mehr richtig beantwortet werden. Die Anfragen der Server laufen dann in einen Timeout, die Zustellung der Mails verzögert sich erheblich.

Auch bei aktiviertem TCP-Stealth-Modus erkennt die Firewall die Absicht einer Station im LAN, eine Verbindung zu einem Mailserver aufzubauen. Daraufhin wird der benötigte Port für die Authentifizierungsanfrage kurzzeitig (für 20 Sekunden) geöffnet.

Dieses Verhalten der Firewall im TCP-Stealth-Modus kann mit dem Parameter "Authentifizierungs-Port tarnen" gezielt unterdrückt werden.

Das Aktivieren der Option “Authentifizierungs-Port tarnen“ kann zu erheblichen Verzögerungen beim Versand und Empfang z. B. von E-Mails oder News führen!

Ein Mail- oder News-Server, der mit Hilfe dieses Dienstes etwaige zusätzliche Informationen vom User anfordert, läuft dann zunächst in einen störenden Timeout, bevor er beginnt, die Mails auszuliefern. Dieser Dienst benötigt also einen eigenen Schalter um ihn zu verstecken bzw. “konform” zu halten.

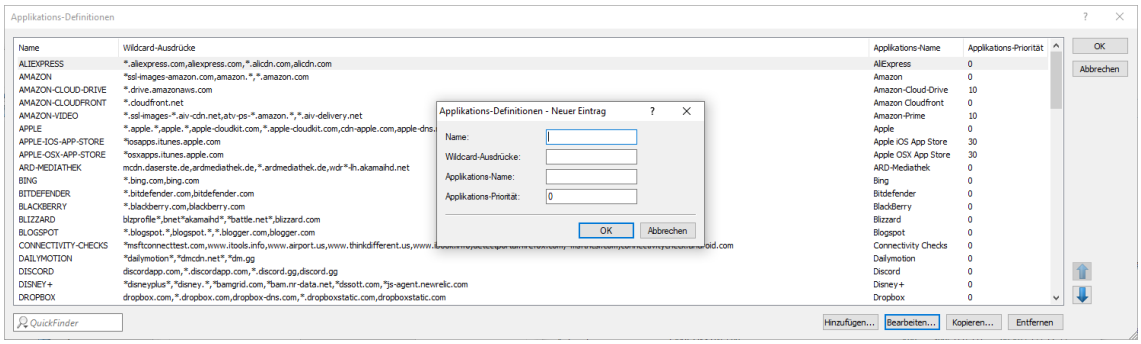
Die Problematik dabei ist nun allerdings, dass eine Einstellung, die alle Ports versteckt, den ident-Port aber zurückweist, unsinnig ist – denn allein dadurch, dass der Ident-Port zurückgewiesen wird, wäre das Gerät zu sehen.

Das Gerät bietet zur Lösung dieses Problems an, Ident-Anfragen nur von den Mail- und News-Servern abzulehnen, und bei Anfragen von allen anderen Rechnern diese einfach zu verwerfen. Hierzu werden bei der Abfrage eines Mail- (SMTP, POP3, IMAP2) oder News-Servers (NNTP) für eine kurze Zeit (20 Sekunden) ident-Anfragen von den jeweiligen Servern abgelehnt.

Ist die Zeit abgelaufen, so wird der Port wieder versteckt.

8.3.3.8 Applikationsdefinitionen für die Layer-7-Erkennung und die Layer-7-Applikationskontrolle

Die Applikationsdefinitionen für die Layer-7-Erkennung und die Layer-7-Applikationskontrolle finden Sie als zentrale Tabelle für DNS-basierte Anwendungen (Layer-7 App) in LANconfig unter **Konfiguration** > **Firewall/QoS** > **Allgemein** > **Applikations-Definitionen** (Konsole: **Setup** > **App-Definitionen**).



Name

Der Name für das Ziel. Der Name wird verwendet, um auf dieses Objekt zu verweisen.

Es kann mehrere Einträge für einen Namen geben, indem dem Namen des Ziels das Zeichen # angehängt und eine maximal dreistellige Zahl hinzugefügt wird (z. B. „LANCOM“, „LANCOM#1“, „LANCOM#2“ usw.).

Für die Verwendung dieses Eintrags in der Firewall muss dieser unter **Konfiguration** > **Firewall/QoS** > **Allgemein** > **DNS-Ziel Listen** referenziert werden.

Wildcard-Ausdrücke

Enthält eine mittels Kommata oder Leerzeichen separierte Liste von Wildcardausdrücken. Die Ausdrücke können beliebig viele ? (ein beliebiges Zeichen) und * (mehrere beliebige Zeichen) enthalten, z. B. „*.lancom.*“. Die Eingabe ist auf 252 Zeichen beschränkt. Wenn Sie für einen Dienst mehr DNS-Wildcard-Ausdrücke benötigen, dann können Sie mehrere DNS-Ziele in der **DNS-Ziel-Liste** zu einem referenzierbaren Objekt zusammenfassen.

Unicodezeichen für internationalisierte Domainnamen können wie folgt eingegeben werden:

- UTF-8: Hier müssen ein bis vier Bytes einzeln als '\x', gefolgt von zwei hexadezimalen Ziffern, eintragen werden.
- UTF-16: Hier müssen ein oder zwei Doppelbytes als '\u', gefolgt von vier hexadezimalen Ziffern, eintragen werden.

- UTF-32: Hier muss der Wert als '\U', gefolgt von acht hexadezimalen Ziffern, eintragen werden.

Für die Layer-7-Applikationserkennung legen Sie mit dieser Tabelle die zu überwachenden HTTP / HTTPS-Dienste fest. Geben Sie dazu zusätzlich die Hostnamen-Bestandteile der Anwendung an.

Applikations-Name

Name für die Überwachung von HTTP / HTTPS-Verbindungen im Rahmen der Layer-7-Applikationserkennung (z. B. Youtube). Mit der Angabe dieses Namens wird die Layer-7-Applikationserkennung aktiviert.

Applikations-Priorität

Mit der Angabe der Priorität können Sie festlegen, in welcher Reihenfolge die jeweiligen Dienste ausgewertet werden, wenn bestimmte Hostnamen-Bestandteile in mehreren Einträgen definiert sind (z. B. *google).

8.3.3.9 SD-WAN Application Routing / Layer-7-Applikationskontrolle

Profitieren Sie von einem deutlichen Performance-Gewinn bei der Nutzung moderner Business-Anwendungen in der Cloud (z. B. Microsoft Office 365, AWS, etc). Application Routing leitet anhand definierter Regeln vertrauenswürdige Anwendungen von der Filiale direkt ins Internet. Dies entlastet sowohl die VPN-Strecke zur Zentrale als auch die Internetleitung in der Zentrale.

Microsoft empfiehlt diese Betriebsart explizit für Office 365. Da diese Web-basierten Dienste häufig keine feste IP-Adresse haben, ist nur eine Erkennung anhand der DNS-Namen möglich. Zu diesem Zweck können entsprechende DNS-Ziele in der Firewall mit einem passenden Wildcardausdruck erstellt werden, sodass diese Pakete mit einem anderen Routingtag markiert werden, um dann später im Router direkt ins Internet geroutet zu werden. Alternativ kann an dieser Stelle auch eine Layer-7-Applikationskotrolle in der Firewall realisiert werden. Somit bewahren Sie die Kontrolle über die Nutzung internetbasierter Anwendungen in Ihrem Netzwerk. Durch die Definition von Regeln für DNS-basierte Anwendungen entscheiden Sie selbst, welche Dienste erlaubt, gesperrt, limitiert oder priorisiert werden.

Wenn nun ein Benutzer ein solches DNS-Ziel in seinem Browser aufruft, dann schickt sein Rechner eine DNS-Anfrage für diese Domäne. Der DNS-Forwarder im LANCOM Router leitet diese Anfrage dann an den Internet Service Provider weiter. Wenn die Antwort kommt, dann speichert der Router die zurückgelieferte IP-Adresse und diese Auflösung steht fortan der Firewall zur Verfügung. Anschließend geht die Antwort an den ursprünglich anfragenden Rechner weiter. Somit kann der Browser die Verbindung zu der zurückgelieferten IP-Adresse öffnen. Die Firewall erkennt die gerade vorher gelernte IP-Adresse und kann ein entsprechendes Routing-Tag zuweisen. Daneben sind auch andere definierte Firewall-Aktionen wie Erlauben, Sperren, Limitieren oder Priorisieren für dieses Ziel anwendbar.

Dadurch, dass die Firewall sich über die DNS-Auflösung genau die Adresse merkt, die der Benutzer für die Domäne anschließend verwendet, funktioniert dieser Mechanismus auch, wenn der Domänenname auf viele unterschiedliche oder zeitlich wechselnde IP-Adressen auflöst.

Einsatzempfehlungen

Der LANCOM Router muss als DNS-Server bzw. DNS-Forwarder im Netz dienen, d. h. Clients im lokalen Netzwerk müssen den Router als DNS-Server verwenden. Zusätzlich muss die direkte Nutzung von DNS-over-TLS und DNS-over-HTTPS (ggf. browserintern) mit externen DNS-Servern durch Clients verhindert werden.

Dies kann wie folgt erreicht werden:

- Der DHCP-Server muss die IP-Adresse des Routers als DNS-Server verteilen (wird standardmäßig vom Internet-Wizard eingerichtet)
- Einrichtung von Firewall-Regeln, die die direkte Nutzung von externen DNS-Servern verhindern, z. B. durch Sperrung des ausgehenden Ports 53 (UDP) für Clients aus dem entsprechenden Quellnetzwerk
- Einrichtung von Firewall-Regeln, die die direkte Nutzung von externen DNS-Servern mit Unterstützung von DNS-over-TLS verhindern, z. B. durch Sperrung des ausgehenden Ports 853 (TCP) für Clients aus dem entsprechenden Quellnetzwerk
- DNS-over-HTTPS (DoH) im Browser deaktivieren



Hinweise zur Synchronisierung der DNS-Datenbank der Firewall:

Da die Firewall ihre Informationen aus den DNS-Anfragen der Clients lernt, kann es in bestimmten Situationen dazu kommen, dass die DNS-Datenbank noch nicht vollständig ist. Dies kann in folgenden Situationen passieren:

- Es wird eine neue Firewall-Regel hinzugefügt, der Client hat aber noch einen DNS-Eintrag zwischengespeichert
- Kurz nach Neustart des Routers und der Client hat aber noch einen DNS-Eintrag zwischengespeichert

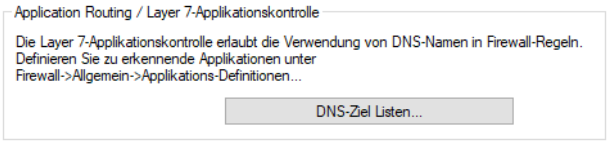
In diesen Fällen hilft ein Leeren des DNS-Cache auf dem Client, ein Reboot des Clients oder ein Timeout des DNS-Eintrags auf dem Client.

Eigene Dienste wie z. B. ping vom Router selbst laufen nicht über die erstellten Firewall-Regeln. Mit Hilfe von ping auf einen vollständigen DNS-Namen (nicht Wildcard-Ausdruck) kann die Erzeugung von Regelauflösungen (DNS zu IP-Adressen) bei Bedarf entweder auf der CLI (einmalig) oder per Cron-Job durchgeführt werden.

Wenn unterschiedliche DNS-Namen auf dieselbe IP-Adresse aufgelöst werden, dann können diese nicht unterschieden werden. In diesem Fall trifft immer die erste Regel zu, die einen dieser DNS-Namen referenziert. Das sollte bei großen Dienstanbietern kein Problem sein. Bei kleinen Websites, die vom selben Anbieter gehostet werden, könnte es jedoch auftreten.

Konfiguration

Die Einstellungen zum anwendungsbasierten Routing bzw. der Layer-7-Applikationskontrolle finden Sie unter **Firewall / Qos** > **Allgemein** > **Application Routing / Layer 7-Applikationskontrolle**.

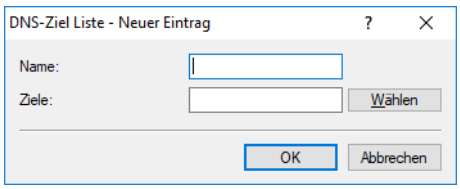


DNS-Ziele

Defninieren Sie in LANconfig unter **Konfiguration** > **Firewall/QoS** > **Allgemein** > **Applikations-Definitionen** (Siehe auch *Applikationsdefinitionen für die Layer-7-Erkennung und die Layer-7-Applikationskontrolle* auf Seite 661.) die Namen und Wildcardausdrücke für die DNS-Ziele, die Sie in der Firewall gesondert behandeln wollen.

DNS-Ziel-Liste

Defninieren Sie in LANconfig unter **Firewall / Qos** > **Allgemein** > **Anwendungsbasiertes Routing** > **DNS-Ziel-Liste** die DNS-Ziele in einer Liste, die Sie in der Firewall gemeinsam als ein Objekt referenzieren wollen.



Name

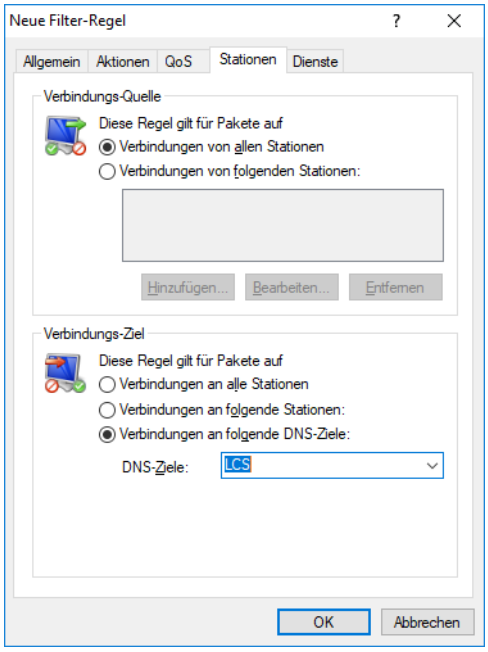
Name der Liste aus DNS-Zielen

Ziele

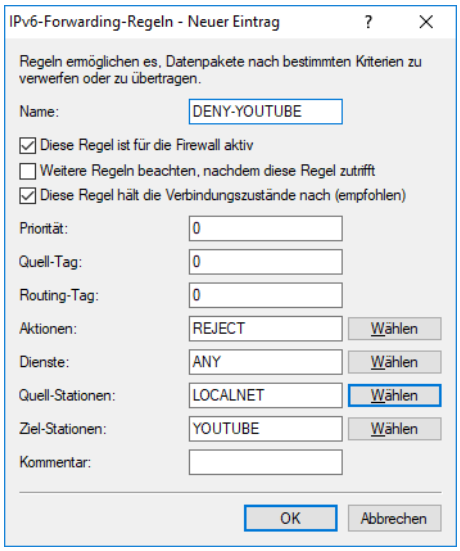
Enthält eine mittels Kommata oder Leerzeichen separierte Liste von Namen der DNS-Ziele.

Referenzierung in den Firewall-Regeln

In **Firewall / Qos** > **IPv4-Regeln** > **Regeln** können Sie eine neue Filter-Regel anlegen und dort auf dem Reiter **Stationen** unter **Verbindungen an folgende DNS-Ziele** aus den konfigurierten DNS-Zielen auswählen.



In **Firewall / Qos** > **IPv6-Regeln** > **IPv6-Forwarding-Regeln** können Sie eine neue Regel anlegen. Als **Ziel-Stationen** können Einträge aus den Tabellen **DNS-Ziele** bzw. **DNS-Ziel-Liste** verwendet werden.



8.3.4 Die Parameter der Firewall-Regeln

In diesem Abschnitt stellen wir vor, aus welchen Komponenten eine Firewall-Regel besteht und welche Optionen zur Einstellung der verschiedenen Parameter zur Verfügung stehen.

8.3.4.1 Die Komponenten einer Firewall-Regel

Eine Firewall-Regel wird zunächst bestimmt durch ihren Namen und einige weitere Optionen:

- **Ein-/Ausschalter**: Ist die Regel aktiv?

- Verknüpfung: Sollen weitere Firewall-Regeln beachtet werden, wenn diese Regel für ein Datenpaket zutrifft? *Verknüpfung* auf Seite 665
- **Priorität**: Mit welcher Priorität wird die Regel bearbeitet? *Priorität* auf Seite 665
- **Quell-Tag**: Über ein Quell-Tag ergänzen Sie das Routing-Tag um die Angabe, auf welches Quell-Netzwerk das Gerät die Firewall-Regel anwendet. Geben Sie ein Quell-Tag an, um eine eindeutige Beziehung zwischen Quell- und Ziel-Hosts in ARF-Kontexten festzulegen: Das Gerät leitet nur dann Datenpakete an ein ARF-Netzwerk weiter, wenn diese von Hosts aus einem ARF-Netzwerk mit dem angegeben Quell-Tag stammen.
- **Routing-Tag**: Mit dem Einsatz des Routing-Tags können über die Ziel-IP-Adressen weitere Informationen wie z. B. der verwendete Dienst oder das verwendete Protokoll für die Auswahl der Zielroute genutzt werden. Durch das so realisierte Policy-based Routing ist eine deutlich feinere Steuerung des Routing-Verhaltens möglich.

  Das Routing-Tag 0 bedeutet hier 'nicht markieren'. Wenn das Gerät Datenpakete in ein mit 0 getaggtes Netz leiten soll, tragen Sie hier bitte 65535 ein.

8.3.4.2 Priorität

Das Gerät nimmt beim Aufbau der Filterliste aus den Firewall-Regeln eine automatische Sortierung der Einträge vor. Dabei wird der "Detallierungsgrad" berücksichtigt: Zunächst werden alle speziellen Regeln beachtet, danach die allgemeinen (z. B. Deny-All).

Wenn sich durch die automatische Sortierung nicht das gewünschte Verhalten der Firewall einstellt, kann die Priorität von Hand verändert werden. Je höher die Priorität der Firewall-Regel, desto eher wird der zugehörige Filter in der Filterliste platziert.

Prüfen Sie bei komplexen Regelwerken die Filterliste, wie im Abschnitt *Firewall-Diagnose* auf Seite 680 beschrieben.

8.3.4.3 Verknüpfung

Es gibt Anforderungen an die Firewall, die mit einer einzelnen Regel nicht abgedeckt werden können. Wenn die Firewall dazu eingesetzt wird, den Internet-Traffic verschiedener Abteilungen (in eigenen IP-Subnetzen) zu begrenzen, können einzelne Regeln z. B. nicht gleichzeitig die gemeinsame Obergrenze abbilden. Soll jeder von z. B. drei Abteilungen eine Bandbreite von maximal 512 kBit/s zugestanden werden, die gesamte Datenrate der drei Abteilungen aber ein Limit von 1024 kBit/s nicht überschreiten, so muss eine mehrstufige Prüfung der Datenpakete eingerichtet werden:

- In der ersten Stufe wird geprüft, ob die aktuelle Datenrate der einzelnen Abteilung die Grenze von 512 kBit/s nicht übersteigt.
- In der zweiten Stufe wird geprüft, on die Datenrate aller Abteilungen zusammen die Grenze von 1024 kBit/s nicht übersteigt.

Normalerweise wird die Liste der Firewall-Regeln der Reihe nach auf ein empfangenes Datenpaket angewendet. Trifft eine Regel zu, wird die entsprechende Aktion ausgeführt. Die Prüfung durch die Firewall ist damit beendet, es werden keine weiteren Regeln auf das Paket angewendet.

Um eine zwei- oder mehrstufige Prüfung eines Datenpaketes zu erreichen, wird die "Verknüpfungsoption" für die Regeln aktiviert. Wenn eine Firewall-Regel mit aktivierter Verknüpfungsoption auf ein Datenpaket zutrifft, wird zunächst die entsprechende Aktion ausgeführt, anschließend wird die Prüfung in der Firewall jedoch fortgesetzt. Trifft eine der weiteren Regeln auch auf dieses Paket zu, wird auch die in dieser Regel definierte Aktion ausgeführt. Ist auch bei dieser folgenden Regel die Verknüpfungsoption aktiviert, wird die Prüfung solange fortgesetzt, bis

- entweder eine Regel auf das Paket zutrifft, bei der die Verknüpfung nicht aktiviert ist
- oder die Liste der Firewall-Regeln ganz durchgearbeitet ist, ohne das eine weitere Regel auf das Paket zutrifft.

Zur Realisierung dieses Szenarios wird also für jedes Subnetz eine Firewall-Regel eingerichtet, die ab einer Datenrate von 512 kBit/s zusätzliche Pakete der Protokolle FTP und HTTP verwirft. Für diese Regeln wird die Verknüpfungsoption aktiviert. In einer weiteren Regel für alle Stationen im LAN werden alle Pakete verworfen, die über 1024 kBit/s hinausgehen.

8.3.4.4 Anwendung der Firewall-Regel

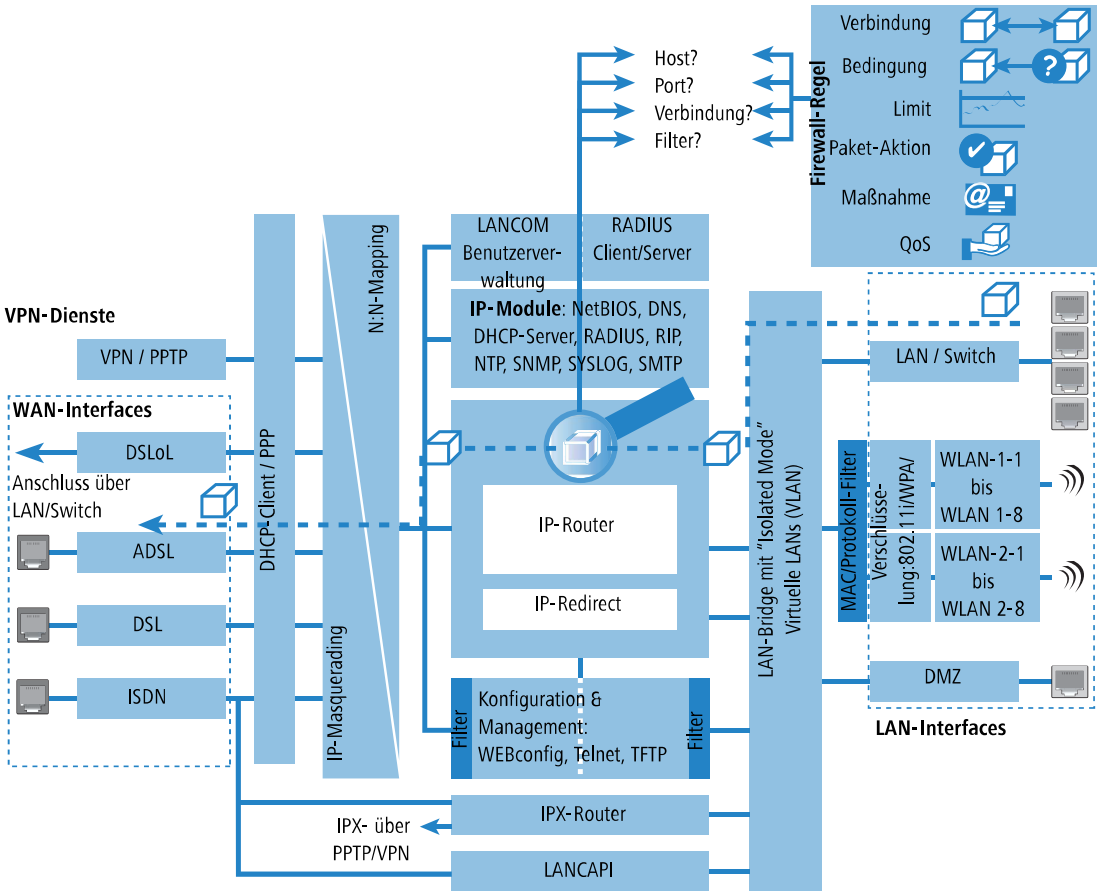
Neben diesen Basisinformationen beantwortet eine Firewall-Regel die Fragen, wann bzw. worauf sie angewendet werden soll und welche Aktionen ggf. ausgeführt werden:

- Verbindung: Auf welche Stationen / Netzwerke und Dienste / Protokolle bezieht sich die Regel? *Verbindung* auf Seite 667
- Bedingung: Ist die Wirksamkeit der Regel durch Bedingungen eingeschränkt? *Bedingung* auf Seite 667
- Limit (Trigger): Beim Erreichen welcher Schwellenwerte soll die Regel anspringen? *Limit (Trigger)* auf Seite 667
- Paket-Aktion: Was soll mit den Datenpaketen passieren, wenn die Bedingung erfüllt und das Limit erreicht sind? *Paket-Aktion* auf Seite 668
- Sonstige Maßnahmen: Sollen neben der Paket-Aktion noch weitere Maßnamen eingeleitet werden? *Sonstige Maßnahmen* auf Seite 668
- Quality of Service (QoS): Werden Datenpakete bestimmter Anwendungen oder mit entsprechenden Markierungen durch die Zusicherung von speziellen Dienstgüten besonders bevorzugt? *Quality of Service (QoS)* auf Seite 668

Bedingung, Limit, Paket-Aktion und sonstige Maßnahmen bilden zusammen ein so genanntes "Aktionen-Set". Jede Firewall-Regel kann mehrere Aktionen-Sets beinhalten. Wenn für mehrere Aktionen-Sets das gleiche Limit verwendet wird, kann die Reihenfolge der Aktionen-Sets eingestellt werden.

Im Abschnitt *So prüft die Firewall im Gerät die Datenpakete* auf Seite 655 wurde bereits dargestellt, dass die Listen zur Prüfung der Datenpakete letztlich aus den Firewall-Regeln gebildet werden. Die Erweiterung der Grafik stellt sich damit wie folgt dar:

Aufbau der Firewall-Regeln



8.3.4.5 Verbindung

Mit der Verbindung in der Firewall-Regel legen Sie fest, auf welche Datenpakete sich die Vorschrift bezieht. Eine Verbindung wird definiert durch die Quelle, das Ziel und den verwendeten Dienst. Zur Bezeichnung von Quelle oder Ziel können die folgenden Angaben verwendet werden:

- Alle Stationen
- Das gesamte lokale Netz (LAN)
- Bestimmte Gegenstellen (bezeichnet durch den Namen aus der Gegenstellenliste)
- Bestimmte Stationen im LAN (bezeichnet durch den Hostnamen)
- Bestimmte MAC-Adressen

  MAC steht für Media Access Control und ist Dreh- und Angelpunkt für die Kommunikation innerhalb eines LAN. In jedem Netzwerkadapter ist eine MAC-Adresse fest eingespeichert. MAC-Adressen sind weltweit eindeutig und unverwechselbar, ähnlich zu Seriennummern von Geräten. Über die MAC-Adressen lassen sich die PCs im LAN zuverlässig auswählen, um ihnen gezielt Rechte auf IP-Paketebene zu gewähren oder zu versagen. MAC-Adressen werden häufig außen auf den Netzwerkgeräten in hexadezimaler Darstellung (z. B. 00:A0:57:01:02:03) angebracht.
- Bereiche von IP-Adressen
- Komplette IP-Netzwerke
- DNS-Ziele für anwendungsbasiertes Routing

Hostnamen können nur dann verwendet werden, wenn das Gerät die Namen in IP-Adressen auflösen kann. Dafür muss das Gerät die Namen über DHCP gelernt haben, oder die Zuordnung muss statisch in der DNS- oder IP-Routing-Tabelle eingetragen sein. Ein Eintrag in der IP-Routing-Tabelle kann dabei einem Hostnamen ein ganzes Netz zuordnen.

Werden die Quelle oder Ziel für eine Firewall-Regel nicht näher bestimmt, gilt die Regel generell für Datenpakete „von allen Stationen“ bzw. „an alle Stationen“.

Der Dienst wird bestimmt durch die Kombination eines IP-Protokolls mit entsprechenden Quell- und / oder Zielports. Für häufig verwendete Dienste (WWW, Mail etc.) sind die entsprechenden Verknüpfungen im Gerät schon vordefiniert, andere können je nach Bedarf zusätzlich angelegt werden.

8.3.4.6 Bedingung

Mit den zusätzlichen Bedingungen schränkt man die Wirksamkeit einer Firewall-Regel weiter ein. Folgende Bedingungen stehen zur Auswahl:

- Nur für Pakete mit bestimmten ToS- bzw. DiffServ-Markierungen
- Nur wenn Verbindung noch nicht besteht
- Nur für Defaultroute (Internet)
- Nur für VPN-Routen

8.3.4.7 Limit (Trigger)

Das Limit (oder auch Trigger) bezeichnet einen quantifizierten Schwellenwert, der auf der definierten Verbindung überschritten werden muss, bevor der Filter ein Datenpaket erfasst. Ein Limit setzt sich zusammen aus folgenden Eckwerten:

- Einheit (kBit, kByte oder Pakete)
- Betrag, also Datenrate oder Anzahl
- Bezugsgröße (pro Sekunde, pro Minute, pro Stunde oder absolut)

Zusätzlich kann für das Limit vereinbart werden, ob es sich auf eine logische Verbindung bezieht oder auf alle Verbindungen gemeinsam, die zwischen den festgelegten Ziel- und Quell-Stationen über die zugehörigen Dienste bestehen. So wird gesteuert, ob der Filter greift, wenn z. B. alle HTTP-Verbindungen der User im LAN in Summe das Limit überschreiten oder ob es ausreicht, wenn eine einzige der parallel aufgebauten HTTP-Verbindungen den Schwellenwert durchbricht.

Bei absoluten Werten kann außerdem definiert werden, dass der zugehörige Zähler beim Überschreiten des Limits zurückgesetzt wird.

Die Daten werden bis zum Erreichen des Limits auf jeden Fall übertragen! Mit einem Betrag von "0" wird die Regel sofort aktiv, wenn auf der definierten Verbindung Datenpakete zur Übertragung anstehen.

8.3.4.8 Paket-Aktion

Die Firewall hat drei Möglichkeiten, ein gefiltertes Paket zu behandeln:

- **Übertragen**: Das Paket wird normal übertragen.
- **Verwerfen**: Das Paket wird stillschweigend verworfen.
- **Zurückweisen**: Das Paket wird zurückgewiesen, der Empfänger erhält eine entsprechende Nachricht über ICMP.

8.3.4.9 Sonstige Maßnahmen

Die Firewall dient nicht nur dazu, die gefilterten Datenpakete zu verwerfen oder durchzulassen, sie kann auch zusätzliche Maßnahmen ergreifen, wenn ein Datenpaket durch den Filter erfasst wurde. Die Maßnahmen gliedern sich dabei in die beiden Bereiche "Protokollierung / Benachrichtigung" und "Verhindern weiterer Angriffe":

- Syslog-Nachricht senden: Sendet eine Nachricht über das SYSLOG-Modul an einen SYSLOG-Client, wie im Konfigurationsbereich "Meldungen" festgelegt.
- E-Mail-Nachricht senden: Sendet eine E-Mail-Nachricht an den Administrator, der im Konfigurationsbereich "Meldungen" festgelegt ist.
- SNMP senden: Sendet einen SNMP-Trap, der z. B. vom LANmonitor ausgewertet wird.

  Jede dieser drei Benachrichtigungsmaßnahmen führt automatisch zu einem Eintrag in der Firewall-Ereignisstabelle.
- Verbindung trennen: Trennt die Verbindung, über die das gefilterte Paket empfangen wurde.

  Dabei wird die physikalische Verbindung getrennt (also z. B. die Internetverbindung), nicht nur die logische Verbindung zwischen den beiden beteiligten Rechnern!
- Absender-Adresse sperren: Sperrt die IP-Adresse, von der das gefilterte Paket empfangen wurde, für eine einstellbare Zeit.
- Ziel-Port sperren: Sperrt den Ziel-Port, an den das gefilterte Paket gesendet wurde, für eine einstellbare Zeit.

8.3.4.10 Quality of Service (QoS)

Neben den Beschränkungen für die Übertragung von Datenpaketen kann die Firewall auch für bestimmte Anwendungen eine "Sonderbehandlung" einräumen. Die QoS-Einstellungen nutzen dabei die Möglichkeiten der Firewall, Datenpakete gezielt Verbindungen oder Diensten zuordnen zu können.

8.3.5 Die Alarmierungsfunktionen der Firewall

In diesem Abschnitt werden die Meldungen, die von der Firewall bei sicherheitsrelevanten Ereignissen verschickt werden, im Detail beschrieben. Es stehen die folgenden Meldungstypen zur Verfügung:

- E-Mail-Benachrichtigung
- SYSLOG-Meldung
- SNMP-Trap

Benachrichtigungen können dabei jeweils getrennt entweder durch die Intrusion Detection, die Denial-of-Service Protection oder durch frei einstellbare Maßnahmen in der Firewall ausgelöst werden. Die spezifischen Parameter für die verschiedenen Benachrichtigungsarten (wie z. B. das zu benutzende E-Mail-Konto) können Sie an folgenden Stellen angeben:

LANconfig: **Meldungen** > **SMTP-Konto** bzw. **Meldungen** > **Systemereignisse**

Konsole: **Setup** > **Mail** bzw. **Setup** > **SYSLOG**

Ein Beispiel:

Es sei ein Filter namens 'BLOCKHTTP' definiert, der den Zugriff auf einen HTTP-Server (192.168.200.10) abblockt, und für den Fall, dass doch jemand auf den Server zugreifen wollte, jeden Traffic von und zu diesem Rechner unterbindet und den Administrator über SYSLOG informiert.

8.3.5.1 Benachrichtigung per SYSLOG

Wenn die Portfilter-Firewall ein entsprechendes Paket verwirft, wird über Syslog eine Meldung ausgegeben, z. B.:

```
PACKET_ALERT: Dst: 192.168.200.10:80 {}, Src: 10.0.0.37:4353 {} (TCP): port filter
```

Die Ports werden dabei nur bei portbehafteten Protokollen ausgegeben. Zusätzlich werden Rechnernamen dann ausgegeben, wenn das Gerät diese direkt (d. h. ohne weitere DNS-Anfrage) auflösen kann.

Werden für einen Filter die Syslog-Meldungen aktiviert (`%s`-Aktion), so wird diese Meldung ausführlicher. Dann werden

Name des Filters, überschrittenes Limit, sowie ausgeführte Aktionen zusätzlich mit ausgegeben. Für das obige Beispiel könnte die Meldung dann so aussehen:

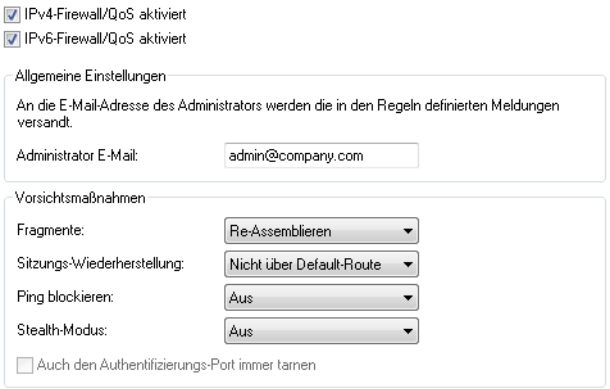
```
PACKET_ALERT: Dst: 192.168.200.10:80 {}, Src: 10.0.0.37:4353 {} (TCP): port filter
PACKET_INFO:
matched filter: BLOCKHTTP
exceeded limit: more than 0 packets transmitted or received on a connection
actions: drop; block source address for 1 minutes; send syslog message;
```

8.3.5.2 Benachrichtigung per E-Mail

Ist das E-Mail-System des Gerätes aktiviert, so können Sie die bequeme Benachrichtigung per E-Mail nutzen. Das Gerät sendet dann eine E-Mail in der folgenden Form an den Administrator, sobald die entsprechende Aktion der Firewall ausgeführt wurde:

```
FROM: device@company.com
TO: admin@company.com
SUBJECT: packet filtered
Date: 9/24/2002 15:06:46
The packet below
Src: 10.0.0.37:4353 {cs2} Dst: 192.168.200.10:80 {ntserver} (TCP)
45 00 00 2c ed 50 40 00 80 06 7a a3 0a 00 00 25 | E..,.P@. ..z....%
c0 a8 c8 0a 11 01 00 50 00 77 5e d4 00 00 00 00 | .......P .w^.....
60 02 20 00 74 b2 00 00 02 04 05 b4 | `. .t... ....
matched this filter rule: BLOCKHTTP
and exceeded this limit: more than 0 packets transmitted or received on a connection
because of this the actions below were performed:
drop
block source address for 1 minutes
send syslog message
send SNMP trap
send email to administrator
```

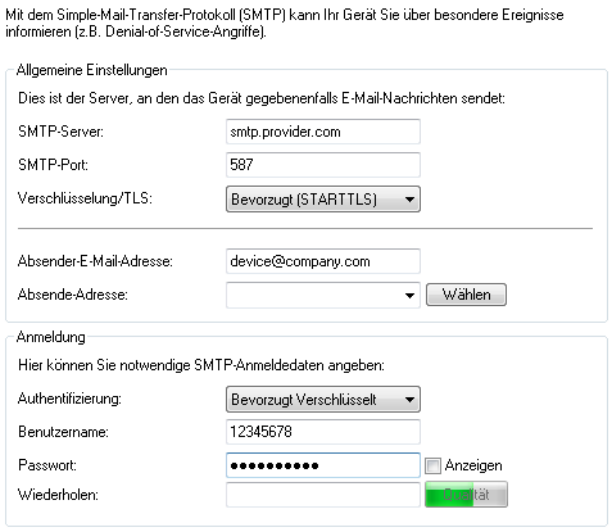
Damit der Mailversand an den Administrator funktioniert, muss die E-Mailadresse des Empfängers richtig eingetragen sein.



LANconfig: **Firewall/QoS** > **Allgemein**

Konsole: **Setup** > **IP-Router** > **Firewall**

Außerdem muss ein Mail-Postfach eingerichtet sein, über das die E-Mail verschickt werden kann.



LANconfig: **Meldungen** > **SMTP-Konto**

Konsole: **Setup** > **SMTP** > **Firewall**

8.3.5.3 Benachrichtigung per SNMP-Trap

Wenn als Benachrichtigungsmethode das Versenden von SNMP-Traps aktiviert wurde, so wird die erste Zeile der Logging-Tabelle als Enterprise-Specific Trap 26 verschickt. Dieser Trap enthält zusätzlich noch den System-Descriptor und den System-Namen aus der MIB-2.

Für das Beispiel wird ein SNMP-Trap erzeugt, aus dem man u. a. folgende Informationen ablesen kann:

```
SNMP: SNMPv1; community = public; SNMPv1 Trap; Length = 443 (0x1BB)
SNMP: Message type = SNMPv1
SNMP: Version = 1 (0x0)
SNMP: Community = public
SNMP: PDU type = SNMPv1 Trap
SNMP: Enterprise = 1.3.6.1.4.1.2356.400.1.6021
SNMP: Agent IP address = 10.0.0.43
SNMP: Generic trap = enterpriseSpecific (6)
SNMP: Specific trap = 26 (0x1A)
SNMP: Time stamp = 1442 (0x5A2)
```

- System-Descriptor:

```
SNMP: OID = 1.3.6.1.2.1.1.1.0 1.
SNMP: String Value = LANCOM Business 6021 2.80.0001 / 23.09.2002 8699.000.036
```

- Device-String:

```
SNMP: OID = 1.3.6.1.2.1.1.5.0 2. System-Name
SNMP: String Value = LANCOM Business 6021
```

- Time-Stamp:

```
SNMP: OID = 1.3.6.1.4.1.2356.400.1.6021.1.10.26.1.2.1 3.
SNMP: String Value = 9/23/2002 17:56:57
```

- Quell-Adresse:

```
SNMP: OID = 1.3.6.1.4.1.2356.400.1.6021.1.10.26.1.3.1 3.
SNMP: IP Address = 10.0.0.37
```

- Ziel-Adresse:

```
SNMP: OID = 1.3.6.1.4.1.2356.400.1.6021.1.10.26.1.4.1 4.
SNMP: IP Address = 192.168.200.10
```

- Protokoll (6 = TCP):

```
SNMP: OID = 1.3.6.1.4.1.2356.400.1.6021.1.10.26.1.5.1 5.
SNMP: Integer Value = 6 (0x6) TCP
```

- Quell-Port:

```
SNMP: OID = 1.3.6.1.4.1.2356.400.1.6021.1.10.26.1.6.1 6.
SNMP: Integer Value = 4353 (0x1101)
```

- Ziel-Port (80 = HTTP):

```
SNMP: OID = 1.3.6.1.4.1.2356.400.1.6021.1.10.26.1.7.1 7.
SNMP: Integer Value = 80 (0x50)
```

- Name der Filterregel:

```
SNMP: OID = 1.3.6.1.4.1.2356.400.1.6021.1.10.26.1.8.1 8.
SNMP: String Value = BLOCKHTTP
```

Dieser Trap und alle anderen im Gerät generierten Traps werden sowohl an alle manuell konfigurierten Trap-Empfänger gesendet, ebenso wie auch an jeden angemeldeten LANmonitor, welcher diesen und u. U. auch alle anderen Traps auswerten kann.

8.3.6 Strategien für die Einstellung der Firewall

Firewalls bilden die Schnittstelle zwischen Netzwerken und schränken dort den ungehinderten Datenaustausch mehr oder weniger deutlich ein. Damit stehen die Firewalls den Zielsetzungen der Netzwerke, zu denen sie selbst gehören, entschieden entgegen: Netzwerke sollen Rechner verbinden, Firewalls sollen die Verbindung verhindern.

Aus diesem Widerspruch lässt sich das Dilemma der verantwortlichen Administratoren erkennen, die in der Folge verschiedene Strategien zur Lösung entwickelt haben.

8.3.6.1 Allow-All

Die Allow-All-Strategie stellt die ungehinderte Kommunikation der Mitarbeiter in den Netzwerken über die Sicherheit. Dabei wird zunächst jede Kommunikation erlaubt, das LAN steht für Angreifer weiter offen. Erst durch die Konfiguration des Admins wird das LAN sukzessive sicherer, in dem nach und nach neue Regeln aufgebaut werden, die Teile der Kommunikation einschränken oder verhindern.

8.3.6.2 Deny-All

Bei der Deny-All-Strategie wird zunächst nach der Methode “Alles sperren!” verfahren, die Firewall blockt die Kommunikation zwischen dem zu schützenden Netzwerk und dem Rest der Welt vollständig ab. Im zweiten Schritt öffnet der Administrator dann die Adressbereiche oder Ports, die für die tägliche Kommunikation mit dem Internet etc. erforderlich sind.

Dieser Ansatz ist für die Sicherheit des LANs besser als die Allow-All-Strategie, führt aber in der Anfangsphase oft zu Schwierigkeiten mit den Benutzern. Einige Dinge laufen eben nach Einschalten der Deny-All-Firewall vielleicht nicht mehr so wie vorher, bestimmte Rechner können ggf. nicht mehr erreicht werden etc.

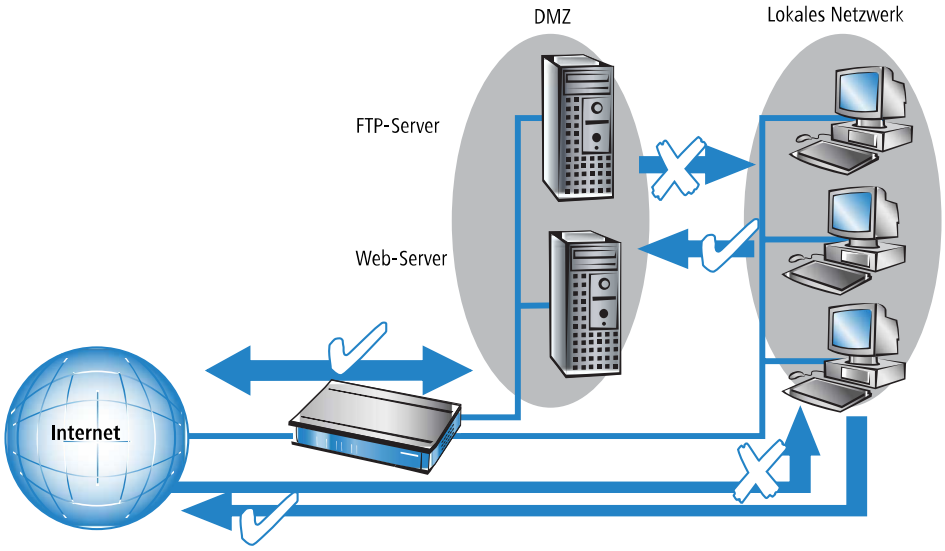
8.3.6.3 Firewall mit DMZ

Die demilitarisierte Zone (DMZ) stellt einen speziellen Bereich des lokalen Netzes dar, der durch eine Firewall sowohl gegen das Internet als auch gegen das eigentliche LAN abgeschirmt ist. In diesem Netzabschnitt werden alle Rechner positioniert, auf die aus dem unsicheren Netz (Internet) direkt zugegriffen werden soll. Dazu gehören z. B. die eigenen FTP- und Web-Server.

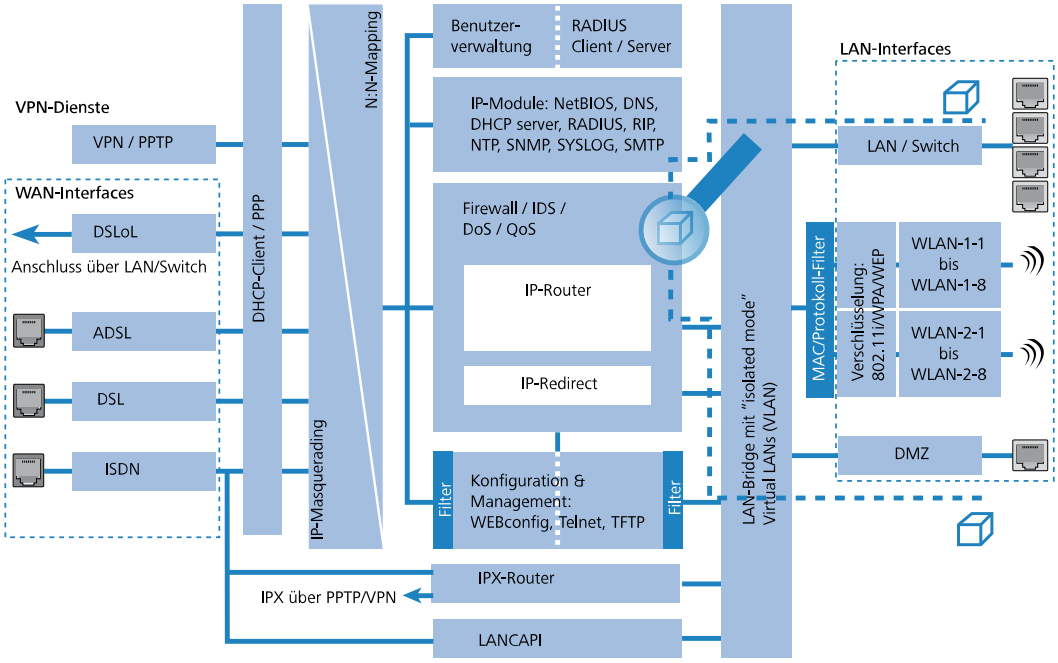
Die Firewall schützt dabei zunächst die DMZ gegen Angriffe aus dem Internet. Zusätzlich schützt die Firewall aber auch das LAN gegen die DMZ. Die Firewall wird dazu so konfiguriert, dass nur folgende Zugriffe möglich sind:

- Stationen aus dem Internet können auf die Server in der DMZ zugreifen, der Zugriff aus dem Internet auf das LAN ist jedoch nicht möglich.
- Die Stationen aus dem LAN können auf das Internet und auf die Server in der DMZ zugreifen.

› Die Server aus der DMZ können nicht auf die Stationen im LAN zugreifen. damit ist sichergestellt, dass auch ein „gehackter" Server aus der DMZ nicht zu einem Sicherheitsrisiko für das LAN wird.



Einige Router-Modelle unterstützen diesen Aufbau durch eine separate LAN-Schnittstelle, die nur für die DMZ verwendet wird. Betrachtet man den Weg der Daten durch das Gerät, dann wird die Funktion der Firewall für die Abschirmung des LANs gegenüber der DMZ deutlich.



Der direkte Datenaustausch zwischen LAN und DMZ ist über die LAN-Bridge nicht möglich, wenn ein DMZ-Port verwendet wird. Der Weg vom LAN in die DMZ und umgekehrt geht also nur über den Router, und damit auch über die Firewall! Die wiederum schirmt das LAN gegen Anfragen aus der DMZ genau so ab wie gegenüber dem Internet.

Das Abschirmen der DMZ gegenüber dem Internet auf der einen und dem LAN auf der anderen Seite wird in vielen Netzstrukturen mit zwei separaten Firewalls gelöst. Beim Einsatz eines Geräts mit DMZ-Port benötigt man für diesen Aufbau nur ein Gerät, was u. a. den Vorteil einer deutlich vereinfachten Konfiguration mit sich bringt.

8.3.7 Tipps zur Einstellung der Firewall

Mit der Geräte-Firewall steht ein extrem flexibles und leistungsfähiges Werkzeug zur Verfügung. Um Ihnen bei der Erstellung individuell angepasster Firewall-Regeln behilflich zu sein, finden Sie im folgenden Hinweise zur optimalen Einstellung für Ihre spezifische Anwendung.

Bei Geräten mit integrierter oder nachträglich über Software-Option freigeschalteter VoIP-Funktion werden die für die Voice-Verbindungen benötigten Ports automatisch freigeschaltet!

8.3.7.1 Die Default-Einstellung der Firewall

Im Auslieferungszustand befindet sich mit der "WINS-Regel" genau ein Eintrag in der Firewall-Regeltabelle. Diese Regel verhindert unerwünschte Verbindungsaufbauten auf der Default-Route (i.d.R. zum Internet) durch das NetBIOS-Protokoll. Windows Netzwerke senden in regelmäßigen Intervallen Anfragen in das Netzwerk um herauszufinden, ob die bekannten Stationen noch verfügbar sind. Dies führt bei zeitbasierter Abrechnung einer Netzwerkkopplung zu unerwünschten Verbindungsaufbauten.

8.3.7.2 Sicherheit durch NAT und Stateful-Inspection

Sofern keine weitere Firewall-Regel eingetragen wird, wird das lokale Netz durch das Zusammenspiel von Network Address Translation und Stateful-Inspection geschützt: Nur Verbindungen aus dem lokalen Netz heraus erzeugen einen Eintrag in der NAT-Tabelle, woraufhin das Gerät einen Kommunikationsport öffnet. Die Kommunikation über diesen Port wird durch die Stateful-Inspection überwacht: Nur Pakete, die genau zu dieser Verbindung gehören, dürfen über diesen Port kommunizieren. Für Zugriff von außen auf das lokale Netzwerk ergibt sich somit eine implizite "Deny-All"-Strategie.

Sofern Sie in Ihrem LAN einen Server betreiben, der über Einträge in der Servicetabelle für Zugriffe aus dem Internet freigegeben ist, können Stationen aus dem Internet von außen Verbindungen zu diesem Server aufbauen. Das inverse Masquerading hat in diesem Fall Vorrang vor der Firewall, solange keine explizite "Deny-All"-Regel eingerichtet wurde.

Firewall-Regeln mit Scripten übertragen

Firewall-Regeln können einfach und komfortabel mittels Scripten über Geräte- und Softwareversionen hinweg übertragen werden. Explizite Beispielscripte finden sich in der LANCOM KnowledgeBase.

8.3.7.3 Aufbau einer expliziten „Deny-All"-Strategie

Für einen maximalen Schutz und bestmögliche Kontrolle über den Datenverkehr wird empfohlen, zunächst einmal jeglichen Datentransfer durch die Firewall zu unterbinden. Danach werden dann selektiv nur genau die benötigten Funktionen und Kommunikationspfade freigeschaltet. Dies bietet z. B. Schutz vor sog. 'Trojanern' bzw. E-Mail-Viren, die aktiv eine abgehende Verbindung auf bestimmten Ports aufbauen.

Die „Deny-All"-Regel ist mit Abstand die wichtigste Regel zum Schutz des lokalen Netzwerks. Mit dieser Regel verfährt die Firewall nach dem Prinzip: „Alles, was nicht ausdrücklich erlaubt ist, bleibt verboten!" Nur mit dieser Strategie kann der Administrator sicher sein, dass er nicht irgendwo eine Zugangsmöglichkeit übersehen hat, denn es gibt nur die Zugänge, die er selbst geöffnet hat.

Wir empfehlen die Einrichtung der Deny-All-Regel, bevor das LAN über ein Gerät mit dem Internet verbunden wird. Anschließend kann man in der Logging-Tabelle (z. B. über LANmonitor zu starten) sehr komfortabel nachvollziehen, welche Verbindungsaufbauten von der Firewall verhindert werden. Mit diesen Informationen wird dann sukzessive die Firewall mit „Allow-Regeln" erweitert.

Einige typische Anwendungsfälle sind im Folgenden aufgezeigt.

Alle hier beschriebenen Filter können sehr komfortabel mit dem Firewall-Assistenten eingerichtet werden, um danach bei Bedarf mit z. B. LANconfig weiter verfeinert zu werden.

› Beispielkonfiguration „Basic Internet"

Regel	Quelle	Ziel	Aktion	Dienst (Zielport)
ALLOW_HTTP	Lokales Netzwerk	Alle Stationen	Übertragen	HTTP, HTTPS
ALLOW_FTP	Lokales Netzwerk	Alle Stationen	Übertragen	FTP
ALLOW_EMAIL	Lokales Netzwerk	Alle Stationen	Übertragen	MAIL, NEWS
ALLOW_DNS_FORWARDING	Lokales Netzwerk	IP-Adresse des Routers (alternativ: Lokales Netzwerk)	Übertragen	DNS
DENY_ALL	Alle Stationen	Alle Stationen	Zurückweisen	ANY

› Sofern Sie VPN-Einwahl auf ein Gerät als VPN-Gateway gestatten wollen, benötigen Sie eine Firewall-Regel, die die Kommunikation des Clients mit dem lokalen Netz erlaubt:

Regel	Quelle	Ziel	Aktion	Dienst
ALLOW_VPN_DIAL_IN	Gegenstellenname	Lokales Netzwerk	Übertragen	ANY

› Für den Fall, dass ein VPN nicht vom Gerät selbst terminiert wird (z. B. VPN-Client im lokalen Netz, oder das Gerät als Firewall vor einem zusätzlichen VPN-Gateway), so müssen Sie zusätzlich IPSec bzw. PPTP (für das 'IPSec over PPTP' des LANCOM VPN Clients) freischalten:

Regel	Quelle	Ziel	Aktion	Dienst (Zielport)
ALLOW_VPN	VPN-Client	VPN-Server	Übertragen	IPSEC, PPTP

› Für eine Netzwerkkopplung gestatten Sie zusätzlich die Kommunikation zwischen den beteiligten Netzwerken:

Regel	Quelle	Ziel	Aktion	Dienst
ALLOW_LAN1_TO_LAN2	LAN1	LAN2	Übertragen	ANY
ALLOW_LAN2_TO_LAN1	LAN2	LAN1	Übertragen	ANY

› Wenn Sie z. B. einen eigenen Webserver betreiben, so schalten Sie selektiv den Server frei:

Regel	Quelle	Ziel	Aktion	Dienst (Zielport)
ALLOW_WEBSERVER	ANY	Webserver	Übertragen	HTTP, HTTPS

› Für Diagnosezwecke empfiehlt sich ferner die Freischaltung des ICMP-Protokolls (z. B. für den Befehl ping):

Regel	Quelle	Ziel	Aktion	Dienst
ALLOW_PING	Lokales Netzwerk	Alle Stationen	Übertragen	ICMP

Diese Regeln können jetzt beliebig verfeinert werden – z. B. durch die Angabe von Mindest- und Maximalbandbreiten für den Serverzugriff, oder aber durch die feinere Einschränkung auf bestimmte Dienste, Stationen oder Gegenstellen.

Das Gerät nimmt beim Aufbau der Filterliste eine automatische Sortierung der Firewall-Regeln vor. Dies geschieht dadurch, dass die Regeln anhand ihres Detaillierungsgrades sortiert in die Filterliste eingetragen werden. Zunächst werden alle spezifischen Regeln beachtet, danach die allgemeinen (z. B. Deny-All). Prüfen Sie bei komplexen Regelwerken die Filterliste, wie im nachfolgenden Abschnitt beschrieben.

8.4 Konfiguration der Firewall mit LANconfig

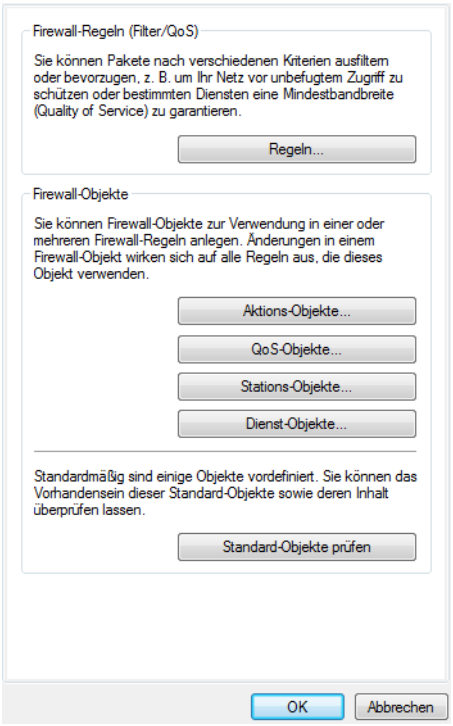
Sie finden die jeweiligen Konfigurationen nun unter **Firewall/QoS** > **IPv4-Regeln** bzw. **Firewall/QoS** > **IPv6-Regeln**.

8.4.1 Definition der Firewall-Objekte

Bei der Konfiguration der Firewall mit LANconfig können verschiedene Objekte definiert werden, die in den Firewall-Regeln verwendet werden. Auf diese Weise müssen häufig benutzte Definitionen (z. B. eine bestimmte Aktion) nicht bei jeder Regel neu eingegeben werden, sondern können einmal an einem zentralen Ort abgelegt werden.

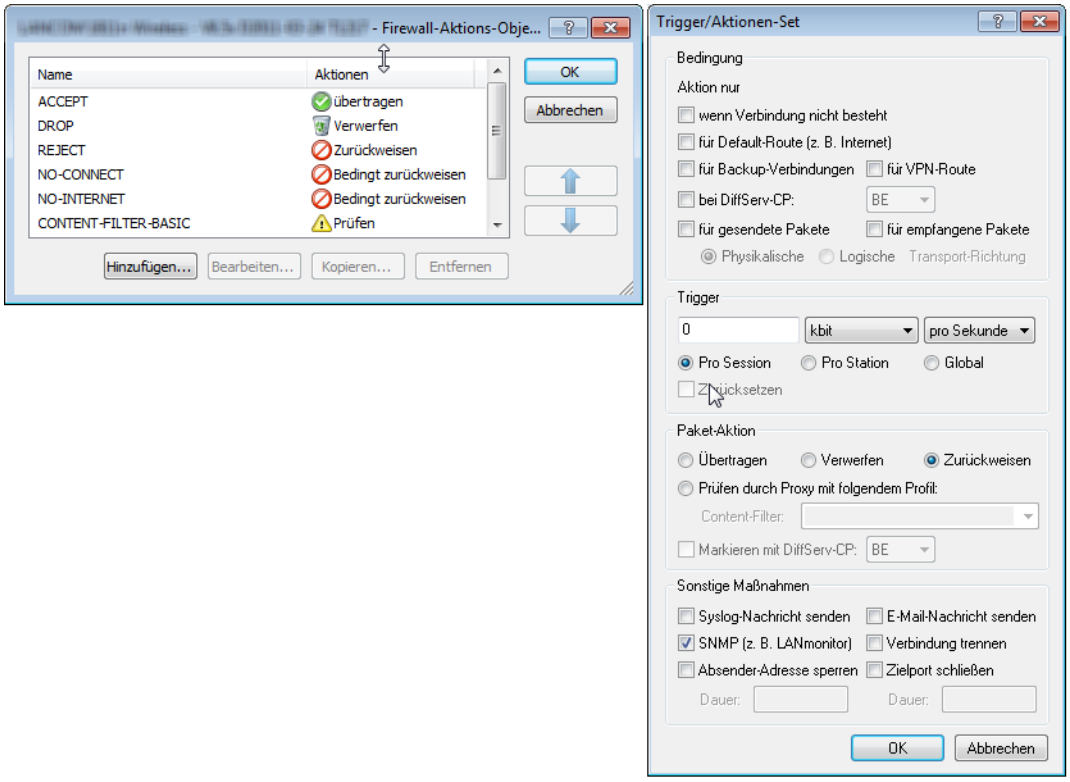
Bitte beachten Sie, dass sich eine Änderung der Firewall-Objekte auf alle Firewall-Regeln auswirkt, die dieses Objekt verwenden. Daher werden beim Ändern von Firewall-Objekten alle Firewall-Regeln angezeigt, die ebenfalls diese Objekte verwenden.

Existierende Firewalls (in der %-Schreibweise) werden beim Öffnen der Konfiguration mit LANconfig nicht automatisch auf die objektorientierte Form umgestellt. In der LANCOM KnowledgeBase finden Sie vorgefertigte Firewalleinstellungen, welche die neuen Objekte benutzen.



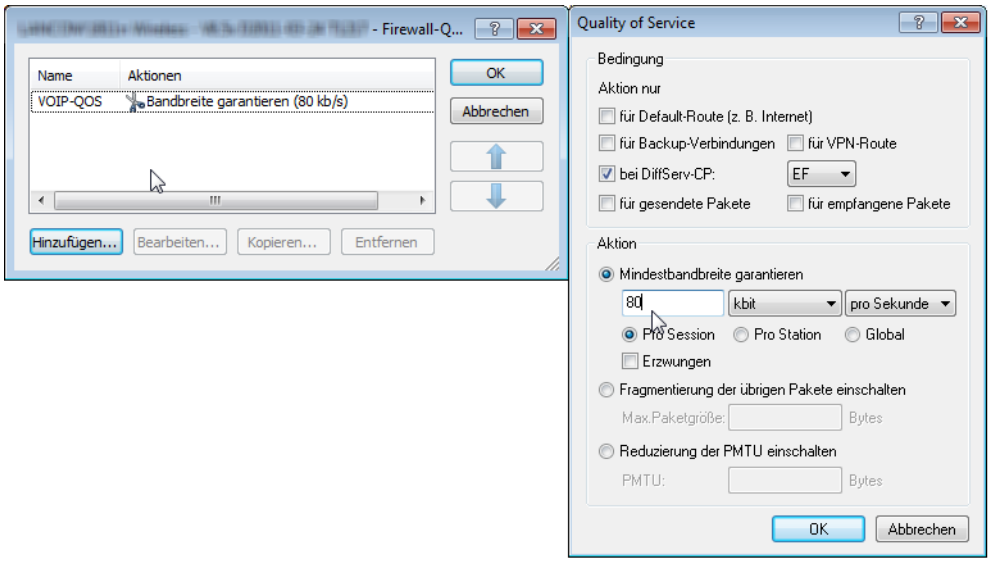
8.4.1.1 Aktions-Objekte

Hier legen Sie die Firewall-Aktion fest, bestehend aus Bedingung, Limit, Paket-Aktion und sonstigen Maßnahmen, die durch die Firewall-Regeln verwendet werden sollen.



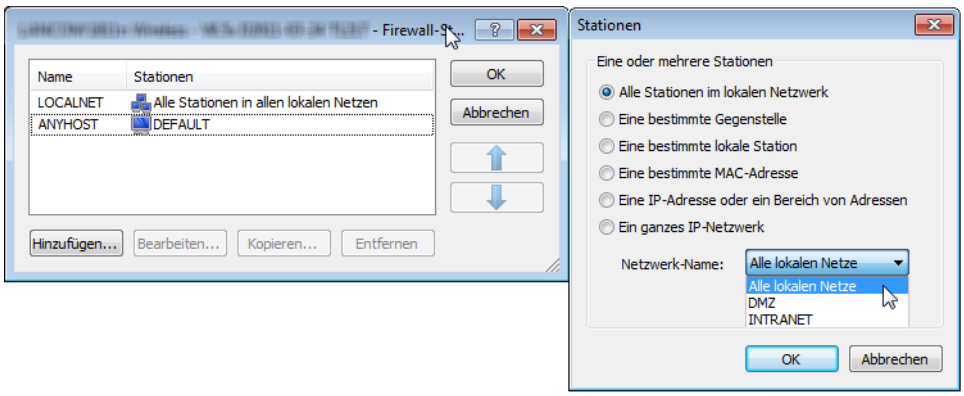
8.4.1.2 QoS-Objekte

Hier können Sie die Mindestbandbreiten für die Datenpakete zur Verfügung stellen, die durch die Firewall-Regeln verwendet werden sollen.



8.4.1.3 Stations-Objekte

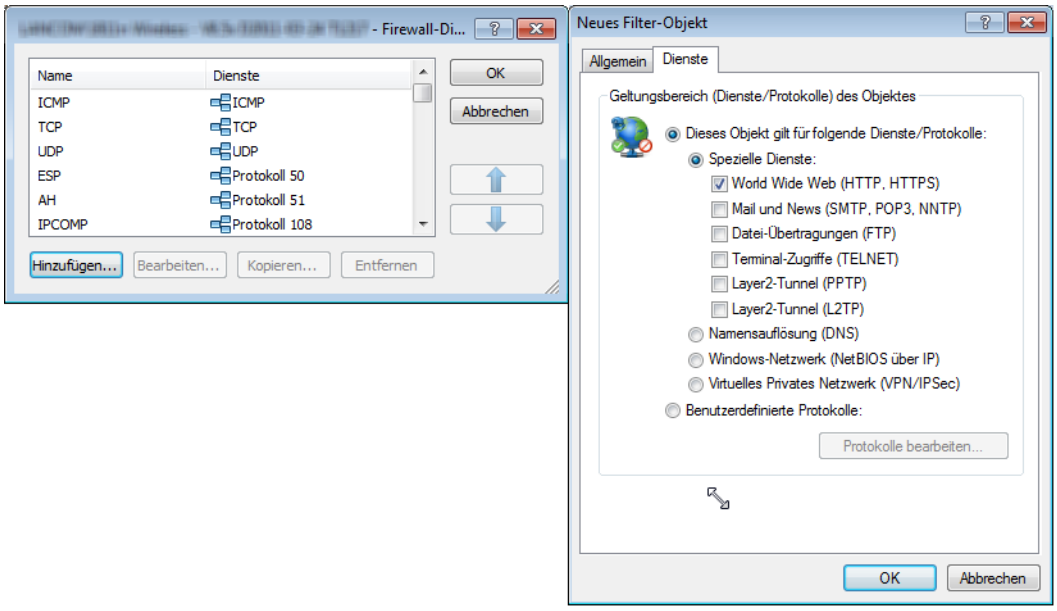
Hier werden die Stationen festgelegt, die als Absender oder Adressat der Pakete durch die Firewall-Regeln verwendet werden sollen. Die Stations-Objekte sind dabei nicht auf Quelle oder Ziel festgelegt, sondern können in den Firewall-Regeln je nach Bedarf verwendet werden. Im Zusammenhang mit ARF ist es z. B. möglich, eine bestimtmes IP-Netzwerk als Stations-Objekt zu definieren.



MAC-Adressen werden als Ziel in einer Firewall-Regel nicht unterstützt.

8.4.1.4 Dienst-Objekte

Hier werden die IP-Protokolle, Quell- und Zielports definiert, die durch die Firewall-Regeln verwendet werden sollen.

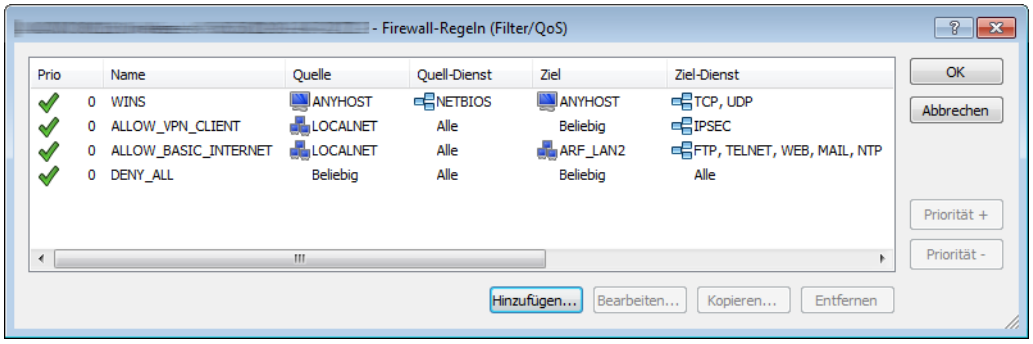


8.4.2 Definition der Firewall-Regeln

Die Firewall-Regeln werden in einer übersichtlichen Tabelle mit folgenden Informationen dargestellt:

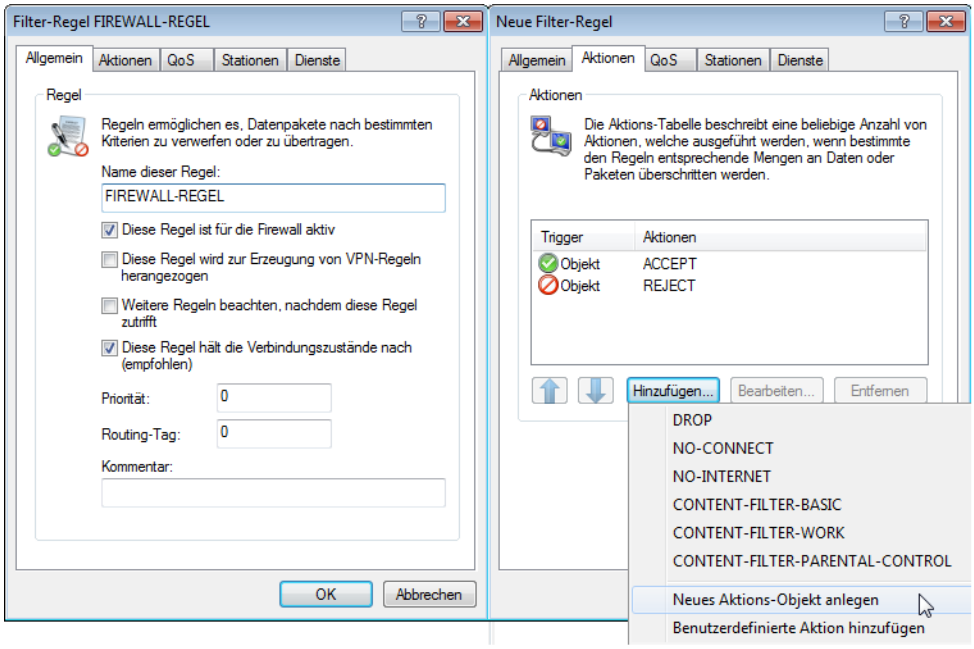
- In der Spalte äußerst links zeigen Symbole den Zustand der Firewall-Regel an:
  - Grünes Häkchen: Firewall-Regel ist aktiv.
  - Rotes Kreuzchen: Firewall-Regel ist nicht aktiv.
  - Schloss: Firewall-Regel wird zur manuellen Erzeugung von VPN-Regeln verwendet.
  - Zwei verkettete Pfeile: Wenn diese Firewall-Regel zutrifft, weitere Regeln beachten.

- Name der Firewall-Regel
- Quelle
- Ziel
- Quell- und Ziel-Dienst
- Aktion/QoS
- Kommentar



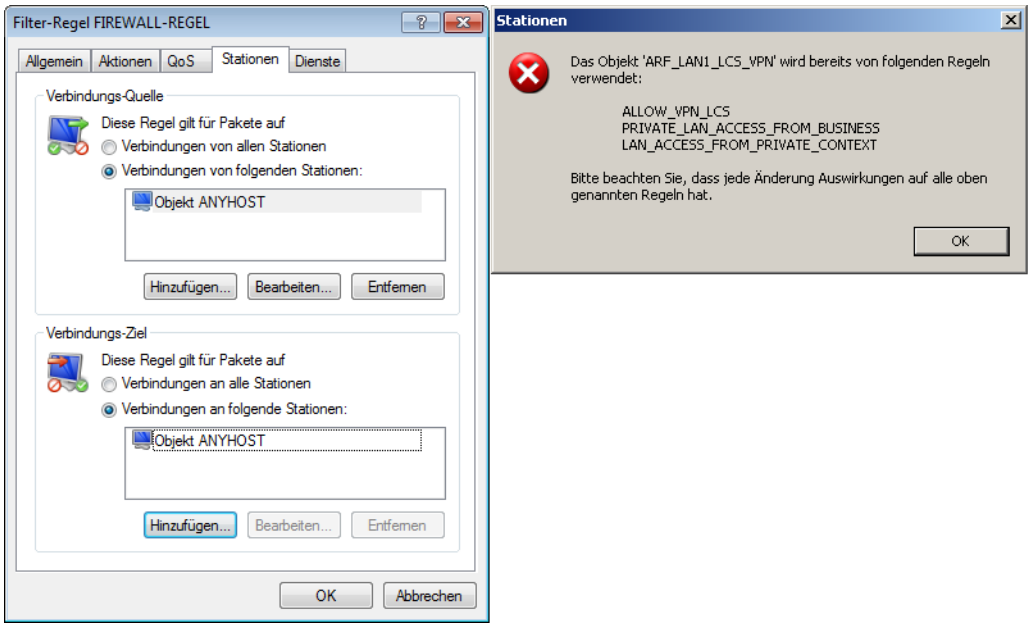
8.4.2.1 Neue Firewall-Regel hinzufügen

Beim Anlegen einer neuen Firewall-Regel werden zunächst die allgemeinen Daten erfasst. Auf den folgenden Registerkarten für Aktionen, QoS, Stationen oder Dienste werden die schon definierten Objekte zur direkten Verwendung angeboten. Alternativ können von dieser Stelle aus neue Objekte angelegt werden, die auch in anderen Regeln verwendet werden können oder benutzerdefinierte Einträge, die nur in der aktiven Firewall-Regel zum Einsatz kommen.



8.4.2.2 Firewall-Regel bearbeiten

Beim Bearbeiten einer bestehenden Firewall-Regel wird angezeigt, ob Aktionen, QoS, Stationen oder Dienste als vordefiniertes Objekt eingefügt wurden. Wenn ein referenziertes Objekt bearbeitet werden soll, das schon in anderen Firewall-Regeln verwendet wird, wird ein entsprechender Hinweis ausgegeben.



8.5 Konfiguration der Firewall-Regeln über die Konsole

8.5.1 Regel-Tabelle

Konsole: **Setup** > **IP-Router** > **Firewall** > **Regel-Tabelle**

In der Regel-Tabelle werden verschiedene Informationen zu einer Firewall-Regel verknüpft. Die Regel enthält das zu filternde Protokoll, die Quelle, das Ziel sowie die auszuführende Firewall-Aktion. Zusätzlich gibt es für jede Firewall-Regel einen Ein-/Ausschalter, eine Priorität, die Option für eine Verknüpfung mit anderen Regeln und eine Aktivierung der Regel für VPN-Verbindungen.

Das Routing-Tag 0 bedeutet hier 'nicht markieren'. Wenn das Gerät Datenpakete in ein mit 0 getaggtes Netz leiten soll, tragen Sie hier bitte 65535 ein.

Die Konfiguration der Firewall wird mit Hilfe von Objekten vorgenommen. Die im folgenden beschriebene %-Schreibweise ist nur bei der Definition von Objekten oder Aktionen erforderlich.

Existierende Firewalls in der %-Schreibweise werden nicht automatisch auf die objektorientierte Form umgestellt. Allerdings stehen in der LANCOM KnowledgeBase vorgefertigte Firewalleinstellungen bereit, die die neuen Objekte verwenden.

Bei Geräten mit einer Firmware-Version 7.6 oder neuer sind automatisch die wichtigsten Objekte in der Firewall vordefiniert. Bei der Bearbeitung von älteren Konfigurationen mit LANconfig werden die Standard-Objekte der Firewall automatisch ergänzt.

Zur Beschreibung der Firewall-Regeln gibt es in der Firmware eine spezielle Syntax. Diese Syntax erlaubt es, auch komplexe Zusammenhänge für die Prüfung und Behandlung von Datenpaketen in der Firewall mit wenigen Zeichen darzustellen. Die Regeln werden in der Regel-Tabelle definiert. Damit häufig verwendete Objekte nicht jedesmal wieder neu in der

Firmware-Syntax eingetragen werden müssen, können in zwei weiteren Tabellen vordefinierte Objekte gespeichert werden:

- In der Aktionstabelle sind die Firewall-Aktionen enthalten
- In der Objekttabelle sind die Stationen und Dienste enthalten

Die Objekte aus diesen Tabellen können bei der Regeldefinition verwendet werden, müssen es aber nicht! Sie erleichtern lediglich die Verwendung von häufiger verwendeten Objekten.

Die Definition der Firewall-Regeln kann sowohl aus Einträgen der Objekttabelle für Protokolle, Dienste, Stationen und der Aktionstabelle für die Firewall-Aktionen bestehen, als auch direkte Beschreibungen in der entsprechenden Firmware-Syntax enthalten (z. B. %P6 für TCP).

Bei der direkten Eingabe der Pegel-Parameter in der Firmware-Syntax gelten die gleichen Regeln, wie sie für Protokolle, Quelle und Ziel sowie die Firewall-Aktionen angegeben sind.

8.5.2 Objekttabelle

Konsole: **Setup** > **IP-Router** > **Firewall** > **Objekt-Tabelle**

In der Objekttabelle werden diejenigen Elemente bzw. Objekte definiert, die in der Regeltabelle der Firewall verwendet werden sollen. Objekte können sein:

- einzelne Rechner (MAC- oder IP-Adresse, Hostname)
- ganze Netze
- Protokolle
- Dienste (Ports oder Port-Bereiche, z. B. HTTP, Mail&News, FTP, …)

Diese Elemente lassen sich beliebig kombinieren und hierarchisch strukturieren. So können z. B. zunächst Objekte für die Protokolle TCP und UDP definiert werden. Später kann man darauf aufbauend Objekte z. B. für FTP (= TCP + Ports 20 und 21), HTTP (= TCP + Port 80) und DNS (= TCP, UDP + Port 53) anlegen. Diese können dann wiederum zu einem Objekt zusammengefasst werden, das alle Definitionen der Einzelobjekte enthält.

8.5.3 Aktionstabelle

Konsole: **Setup** > **IP-Router** > **Firewall** > **Aktions-Tabelle**

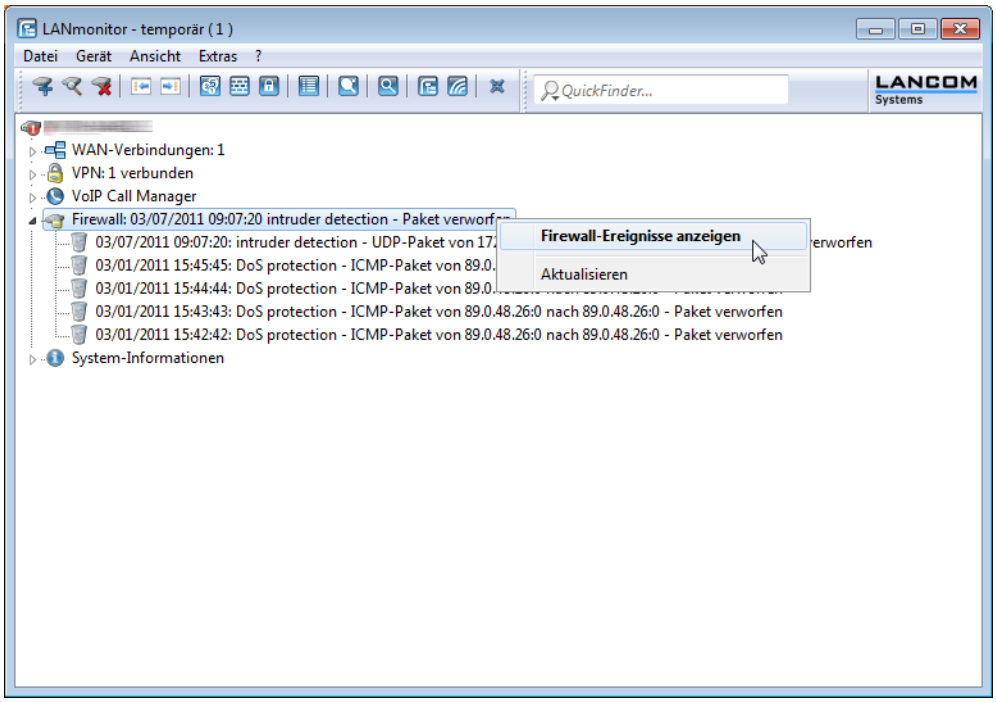
Eine Firewall-Aktion besteht aus einer Bedingung, einem Limit, einer Paket-Aktion und sonstigen Maßnahmen.

Die Firewall-Aktionen können wie bereits die Elemente der Objekt-Tabelle mit einem Namen versehen und beliebig rekursiv miteinander kombiniert werden, wobei die maximale Rekursionstiefe auf 16 beschränkt ist. Sie können aber auch direkt in das Aktionsfeld der Regeltabelle eingetragen werden.

8.6 Firewall-Diagnose

Alle Ereignisse, Zustände und Verbindungen der Firewall können detailliert protokolliert und überwacht werden.

Die komfortabelste Überwachung ergibt sich mit der Anzeige der Logging-Tabelle (s. u.) durch den LANmonitor. Im LANmonitor werden im Bereich 'Firewall' die letzten fünf Ereignisse angezeigt, die durch eine Firewall-Regel, das DoS- oder IDS-System mit aktivierter 'SNMP'-Option ausgelöst wurden.



Mit einem Klick der rechten Maustaste auf diese Rubrik öffnet sich im Kontextmenü unter dem Eintrag Firewall-Ereignisanzeige ein neues Fenster mit der vollständigen Logging-Tabelle *Die Firewall-Tabelle* auf Seite 681.

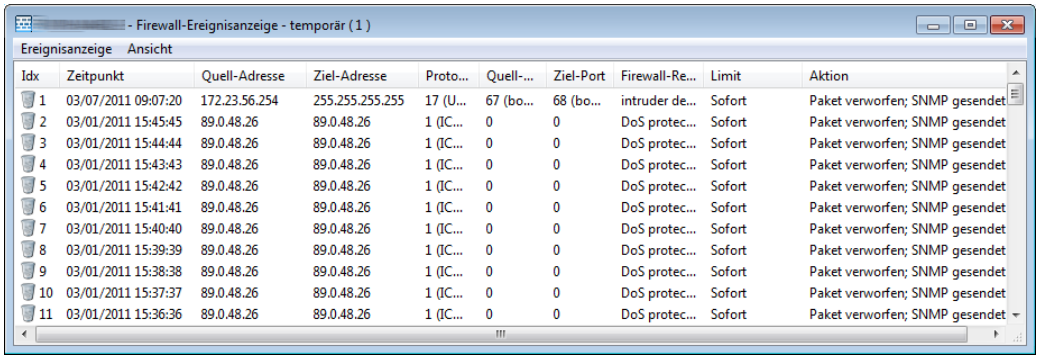
Alle in diesem Abschnitt beschriebenen Listen und Tabellen finden Sie unter folgenden Menüpunkten:

WEBconfig: **Extras** > **LCOS-Menübaum** > **Status** > **IP-Router-Statistik**

8.6.1 Die Firewall-Tabelle

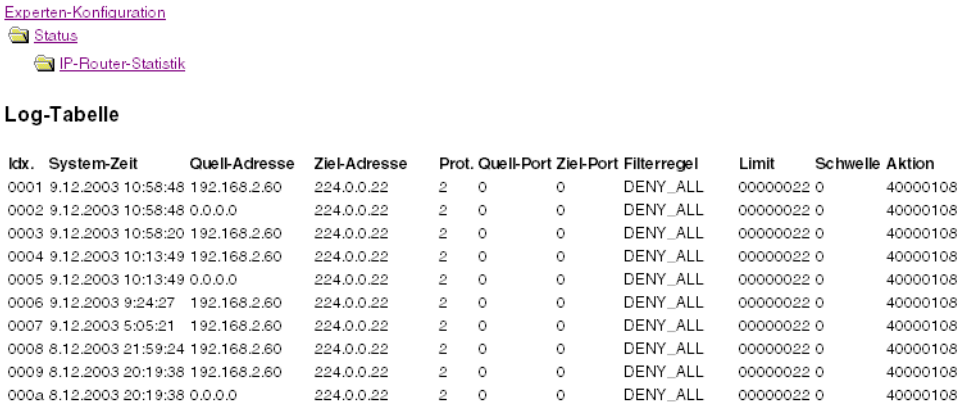
Wenn ein zu loggendes Ereignis eingetreten ist, d. h. als auszuführende Aktion beim Empfang eines Paketes ist eine Mitteilung per E-Mail, Syslog oder SNMP gefordert, so wird dieses Ereignis in einer Logging-Tabelle festgehalten.

Wird die Logging-Tabelle über den LANmonitor aufgerufen, präsentiert sie sich in folgender Darstellung:



Idx	Zeitpunkt	Quell-Adresse	Ziel-Adresse	Proto...	Quell-...	Ziel-Port	Firewall-Re...	Limit	Aktion
1	03/07/2011 09:07:20	172.23.56.254	255.255.255.255	17 (U...	67 (bo...	68 (bo...	intruder de...	Sofort	Paket verworfen; SNMP gesendet
2	03/01/2011 15:45:45	89.0.48.26	89.0.48.26	1 (IC...	0	0	DoS protec...	Sofort	Paket verworfen; SNMP gesendet
3	03/01/2011 15:44:44	89.0.48.26	89.0.48.26	1 (IC...	0	0	DoS protec...	Sofort	Paket verworfen; SNMP gesendet
4	03/01/2011 15:43:43	89.0.48.26	89.0.48.26	1 (IC...	0	0	DoS protec...	Sofort	Paket verworfen; SNMP gesendet
5	03/01/2011 15:42:42	89.0.48.26	89.0.48.26	1 (IC...	0	0	DoS protec...	Sofort	Paket verworfen; SNMP gesendet
6	03/01/2011 15:41:41	89.0.48.26	89.0.48.26	1 (IC...	0	0	DoS protec...	Sofort	Paket verworfen; SNMP gesendet
7	03/01/2011 15:40:40	89.0.48.26	89.0.48.26	1 (IC...	0	0	DoS protec...	Sofort	Paket verworfen; SNMP gesendet
8	03/01/2011 15:39:39	89.0.48.26	89.0.48.26	1 (IC...	0	0	DoS protec...	Sofort	Paket verworfen; SNMP gesendet
9	03/01/2011 15:38:38	89.0.48.26	89.0.48.26	1 (IC...	0	0	DoS protec...	Sofort	Paket verworfen; SNMP gesendet
10	03/01/2011 15:37:37	89.0.48.26	89.0.48.26	1 (IC...	0	0	DoS protec...	Sofort	Paket verworfen; SNMP gesendet
11	03/01/2011 15:36:36	89.0.48.26	89.0.48.26	1 (IC...	0	0	DoS protec...	Sofort	Paket verworfen; SNMP gesendet

Wird die Logging-Tabelle über WEBconfig aufgerufen, präsentiert sie sich in folgender Darstellung:



Diese Tabelle enthält die folgenden Werte:

Element	Bedeutung
Idx.	laufender Index (damit die Tabelle auch über SNMP abgefragt werden kann)
System-Zeit	System-Zeit in UTC Kodierung (wird bei der Ausgabe der Tabelle in Klartext umgewandelt)
Quell-Adresse	Quell-Adresse des gefilterten Pakets
Ziel-Adresse	Zieladresse des gefilterten Pakets
Prot.	Protokoll (TCP, UDP etc.) des gefilterten Pakets
Quell-Port	Quell-Port des gefilterten Pakets (nur bei portbehafteten Protokollen)
Ziel-Port	Ziel-Port des gefilterten Pakets (nur bei portbehafteten Protokollen)
Filterregel	Name der Regel, die den Eintrag erzeugt hat.
Limit	Bitfeld, dass das überschrittene Limit beschreibt, durch welches das Paket gefiltert wurde. Folgende Werte sind zur Zeit definiert: › 0x01 Absolute Anzahl › 0x02 Anzahl pro Sekunde › 0x04 Anzahl pro Minute › 0x08 Anzahl pro Stunde › 0x10 globales Limit › 0x20 Bytelimit (wenn nicht gesetzt, handelt es sich um ein Paket-Limit) › 0x40 Limit gilt nur in Empfangsrichtung › 0x80 Limit gilt nur in Senderichtung
Schwelle	überschrittener Grenzwert des auslösenden Limits
Aktion	Bitfeld, das alle ausgeführten Aktionen aufführt. Folgende Werte sind zur Zeit definiert: › 0x00000001 Accept › 0x00000100 Reject › 0x00000200 Aufbaufilter › 0x00000400 Internet- (Defaultrouten-) Filter › 0x00000800 Drop › 0x00001000 Disconnect › 0x00004000 Quell-Adresse sperren › 0x00020000 Zieladresse und -port sperren › 0x20000000 Sende Syslog-Benachrichtigung › 0x40000000 Sende SNMP-Trap › 0x80000000 Sende E-Mail

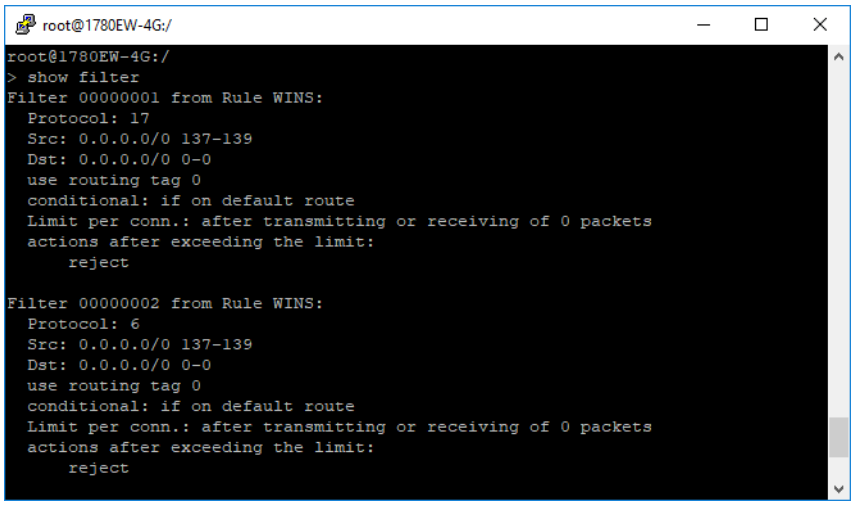
Alle Firewall-Aktionen werden ebenfalls im IP-Router-Trace angezeigt. Einige Modelle verfügen ferner über eine Firewall-LED, welche jedes gefilterte Paket signalisiert.

8.6.1.1 Die Filterliste

Über die Filterliste können die aus den in der Aktions-, Objekt- und Regeltabelle definierten Regeln erzeugten Filter ermittelt werden.

Bei einer manuellen Filter-Definition über Kommandozeile oder WEBconfig wird kein Eintrag in der Filterliste angelegt, wenn die Definition Fehler in der Syntax enthält. In diesem Fall wird auch keine Fehlermeldung ausgegeben! Wenn Sie die Filter manuell konfigurieren, sollten Sie in jedem Fall anhand der Filterliste überprüfen, ob die gewünschten Filter erzeugt wurden.

Auf der Kommandozeile können die konfigurierten Filter mit dem Kommando `show filter` angezeigt werden:



Unter WEBconfig rufen Sie die Filterliste unter **Extras** > **LCOS-Menübaum** > **Status** > **IP-Router** > **Filterliste**auf Sie hat den folgenden Aufbau:

Filter-Liste

Idx.	Prot.	Quelle	Q-Von	Q-Bis	Ziel	Z-Von	Z-Bis	Aktion	verknuepft	Prio	Quell-Tag	Rtg-Tag
00000001	17	0.0.0.0/0	137	139	0.0.0.0/0	0	0	inet: reject	nein	0	0	0
00000002	6	0.0.0.0/0	137	139	0.0.0.0/0	0	0	inet: reject	nein	0	0	0

Die einzelnen Felder in der Filterliste haben folgende Bedeutung:

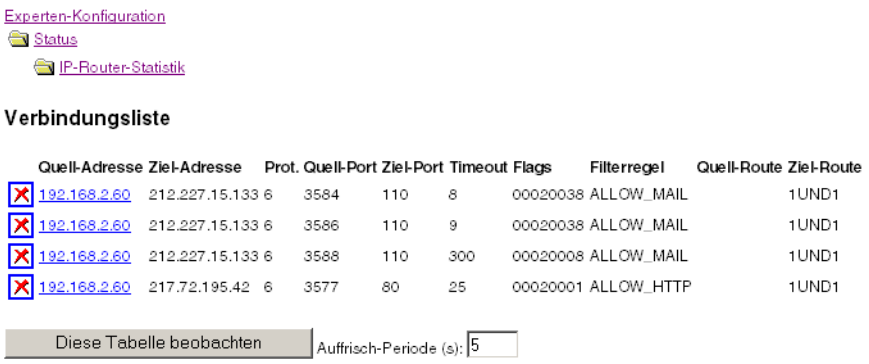
Eintrag	Beschreibung
Idx.	laufender Index
Prot	zu filterndes Protokoll, also z. B. 6 für TCP oder 17 für UDP
Quelle	Diese Spalte zeigt entweder die MAC-Adresse oder das Netzwerk als Adresse mit Präfixlänge an.
Q-von	Start-Quell-Port der zu filternden Pakete.
Q-bis	End-Quell-Port der zu filternden Pakete. Spannt zusammen mit dem Start-Quell-Port einen Portbereich auf, in dem der Filter wirksam ist. Sind Start und Endport 0, so gilt der Filter für alle Quell-Ports.
Ziel	Diese Spalte zeigt entweder die MAC-Adresse oder das Netzwerk als Adresse mit Präfixlänge oder das DNS-Ziel an.
Z-von	Start-Zielport der zu filternden Pakete.
Z-bis	End-Zielport der zu filternden Pakete. Spannt zusammen mit dem Start-Zielport einen Portbereich auf, in dem der Filter wirksam ist. Sind Start und Endport 0, so gilt der Filter für alle Zielports.

Eintrag	Beschreibung
Aktion	In dieser Spalte wird die “Hauptaktion”, also die Aktion textuell ausgegeben, die bei überschreiten des ersten Limits ausgeführt wird. Das erste Limit kann auch ein implizites Limit sein, so z. B. wenn nur ein Limit zur Beschränkung des Durchsatzes konfiguriert wurde, so wird ein implizites Limit eingefügt, das mit einer “accept” Aktion verknüpft ist. Als Hauptaktion wird in diesem Fall “accept” ausgegeben. Die vollständigen Aktionen lassen sich über das Kommando `show filter` anzeigen.
verknüpft	Gibt an, ob es sich bei dieser Regel um eine “First Match”-Regel handelt (verknüpft = Nein). Nur bei verknüpften Regeln werden im Falle des Zutreffens dieser Regel auch weitere Regeln ausgewertet.
Prio	Priorität der Regel, durch die der Eintrag erzeugt wurde.
Quell-Tag	Ursprüngliches Routing Tag.
Rtg-Tag	Zugewiesenes Routing Tag nach Anwendung des Filters.

8.6.1.2 Die Verbindungsliste

In der Verbindungstabelle werden Quell-Adresse, Ziel-Adresse, Protokoll, Quell-Port, Ziel-Port, etc. einer Verbindung nachgehalten sowie mögliche Aktionen gespeichert. Diese Tabelle ist sortiert nach Quell-Adresse, Ziel-Adresse, Protokoll, Quell-Port und Ziel-Port des Pakets, das den Eintrag in der Tabelle hervorgerufen hat.

Unter WEBconfig hat die Filterliste den folgenden Aufbau:



Die Tabelle enthält die folgenden Elemente:

Element	Bedeutung
Quell-Adresse	Quell-Adresse der Verbindung
Ziel-Adresse	Ziel-Adresse der Verbindung
Prot.	verwendetes Protokoll (TCP/UDP etc.) Das Protokoll wird dezimal angegeben
Quell-Port	Quell-Port der Verbindung. Der Port wird nur bei portbehafteten Protokollen (TCP/UDP) oder Protokollen, die ein vergleichbares Feld besitzen (ICMP/GRE) angegeben
Ziel-Port	Ziel-Port der Verbindung (bei UDP-Verbindungen wird dieser erst mit der ersten Antwort besetzt)
Timeout	Jeder Eintrag altert mit der Zeit aus dieser Tabelle heraus, damit die Tabelle bei „gestorbenen“ Verbindungen nicht überläuft.
Flags	In den Flags wird der Zustand der Verbindung und weitere (interne) Informationen in einem Bitfeld gespeichert. Als Zustände sind folgende Werte möglich: new, establish, open, closing, closed, rejected (entsprechend der TCP-Flags: SYN, SYN ACK, ACK, FIN, FIN ACK und RST) UDP-Verbindungen kennen die Zustände new, open und closing (letzteren nur, wenn die UDP-Verbindung mit einem zustandsbehafteten Steuerkanal verknüpft ist.
Quell-Route	Name der Gegenstelle, über die das erste Paket empfangen wurde.
Ziel-Route	Name der Gegenstelle, auf die das erste Paket gesendet wird.

Element	Bedeutung
Filterregel	Name der Regel, die den Eintrag erzeugt hat. Diese bestimmt auch die auszuführenden Aktionen, wenn ein passendes Paket empfangen wird.

Bedeutung der Flags in der Verbindungsliste

Flag	Bedeutung
00000001	TCP: SYN gesendet
00000002	TCP: SYN/ACK empfangen
00000004	TCP: warte auf ACK des Servers
00000008	alle: Verbindung offen
00000010	TCP: FIN empfangen
00000020	TCP: FIN gesendet
00000040	TCP: RST gesendet oder empfangen
00000080	TCP: Sitzung wird wiederhergestellt
00000100	FTP: passive FTP-Verbindung wird aufgebaut
00000400	H.323: zugehörige T.120-Verbindung
00000800	Verbindung über Loopback-Interface
00001000	prüfe verkettete Regeln
00002000	Regel ist verkettet
00010000	Ziel ist auf "lokaler Route"
00020000	Ziel ist auf Default-Route
00040000	Ziel ist auf VPN-Route
00080000	physikalische Verbindung ist nicht aufgebaut
00100000	Quelle ist auf Default-Route
00200000	Quelle ist auf VPN-Route
00800000	keine Route zum Ziel
01000000	enthält globale Aktion mit Bedingung

8.6.1.3 Portsperrliste

Wenn als Aktion die Sperrung des Zielports auf dem Zielrechner ausgewählt wurde, so werden Adresse, Protokoll und Port des Zielrechners in der Portsperrtabelle abgelegt. Diese Tabelle ist ebenfalls eine sortierte halbdynamische Tabelle. Die Sortierung erfolgt nach Adresse, Protokoll und Port. Die Tabelle enthält die folgenden Elemente:

Element	Bedeutung
Address	Adresse des Rechners, für den die Sperre gelten soll.
Protocol	Verwendetes Protokoll (TCP/UDP etc.) Das Protokoll wird dezimal angegeben.
Port	Zu sperrender Port auf dem Rechner. Wenn das jeweilige Protokoll nicht portbehaftet ist, dann wird das gesamte Protokoll für diesen Rechner gesperrt.
Timeout	Dauer der Sperre in Minuten.
Filterregel	Name der Regel, die den Eintrag erzeugt hat. Diese bestimmt auch die auszuführenden Aktionen, wenn ein passendes Paket empfangen wird.

8.6.1.4 Hostsperrliste

Wenn als Aktion eines Filters die Sperrung des Absenders ausgewählt wurde, dann wird die Adresse des Rechners in der Hostsperrtabelle abgelegt. Diese Tabelle ist eine nach der Absenderadresse sortierte halbdynamische Tabelle und enthält die folgenden Elemente:

Element	Bedeutung
Address	Adresse des Rechners, der gesperrt werden soll
Timeout	Dauer der Sperre in Minuten
Filter-Regel	Name der Regel, die den Eintrag erzeugt hat. Diese bestimmt auch die auszuführenden Aktionen, wenn ein passendes Paket empfangen wird.

8.7 Grenzen der Firewall

Neben dem Verständnis der Funktionsweise der Firewall ist es auch sehr wichtig, ihre Grenzen zu erkennen und sie ggf. weiter zu ergänzen. So schützt die Firewall grundsätzlich nicht vor bösartigen Inhalten, die auf den zugelassenen Wegen in das lokale Netzwerk gelangen. Die Auswirkungen einiger Viren und Würmer werden zwar unterbunden, weil die Kommunikation über die benötigten Ports gesperrt ist, aber einen echten Schutz vor Viren bietet die Firewall allein nicht.

Auch das Abhören von sensiblen Daten im Internet wird durch die Firewall nicht verhindert. Sind die Daten erst einmal über die Firewall hinaus in das unsichere Netz gelangt, stehen sie dort weiterhin den bekannten Gefahren gegenüber. Vertrauliche Informationen wie Verträge, Passwörter, Entwicklungsinformationen etc. sollten daher auch bei Einsatz einer Firewall nur geschützt übertragen werden, z. B. durch den Einsatz geeigneter Verschlüsselungsverfahren oder über VPN-Verbindungen.

8.8 Abwehr von Einbruchsversuchen: Intrusion Detection

Die Firewall hat die Aufgabe, den Datenverkehr über die Grenzen zwischen den Netzwerken hinweg zu prüfen und diejenigen Datenpakete, die keine Erlaubnis für die Übertragung mitbringen, zurückzuweisen bzw. zu verwerfen. Neben dem Ansatz, direkt auf einen Rechner im geschützten Netzwerk zuzugreifen, gibt es aber auch Angriffe auf die Firewall selbst oder Versuche, die Firewall mit gefälschten Datenpaketen zu überlisten.

Solche Versuche werden über ein Intrusion-Detection-System (IDS) erkannt, abgewehrt und protokolliert. Dabei kann zwischen Protokollierung im Gerät (Logging), E-Mail-Benachrichtigung, SNMP-Traps oder SYSLOG-Alarmen gewählt werden. Das IDS prüft den Datenverkehr auf bestimmte Eigenschaften hin und erkennt so auch neue Angriffe, die nach auffälligen Mustern ablaufen.

8.8.1 Beispiele für Einbruchsversuche

Als typische Einbruchsversuche kann man gefälschte Absender-Adressen (IP-Spoofing) und Portscans ansehen, sowie den Missbrauch spezieller Protokolle wie z. B. FTP, um einen Port im angegriffenen Rechner und der davor hängenden Firewall zu öffnen.

8.8.1.1 IP-Spoofing

Beim IP-Spoofing gibt sich der Absender eines Pakets als ein anderer Rechner aus. Dies geschieht entweder, um Firewalls zu überlisten, die Paketen aus dem eigenen Netz mehr Vertrauen schenken als Paketen aus fremden Netzen, oder um den Urheber eines Angriffs zu verschleiern.

Die Geräte-Firewall schützt sich davor durch Routenprüfung, d. h. sie überprüft, ob das Paket überhaupt über das Interface empfangen werden durfte, von dem es empfangen wurde.

8.8.1.2 Portscan-Erkennung

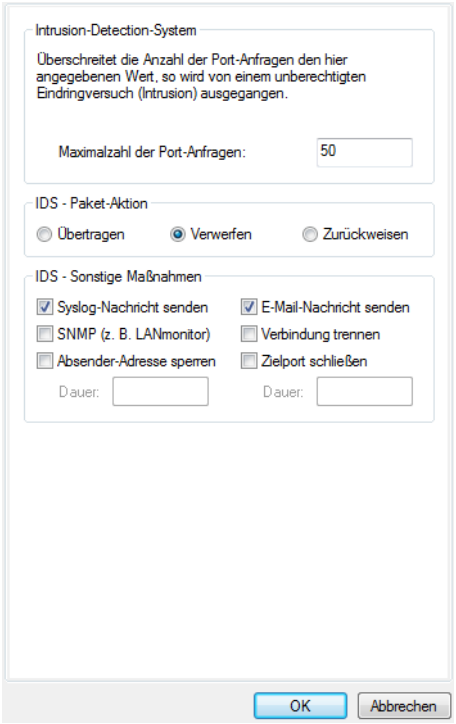
Das Intrusion-Detection System versucht Portscans zu erkennen, zu melden und geeignet auf den Angriff zu reagieren. Dies geschieht ähnlich der Erkennung eines 'SYN Flooding'-Angriffs (siehe *SYN Flooding* auf Seite 689): Es werden auch hier die "halboffenen" Verbindungen gezählt, wobei ein TCP-Reset, das vom gescannten Rechner gesendet wird, die "halboffene" Verbindung weiterhin offen lässt.

Wenn eine bestimmte Anzahl von halboffenen Verbindungen zwischen dem gescannten und dem scannenden Rechner existiert, so wird dies als Portscan gemeldet.

Ebenso wird der Empfang von leeren UDP-Paketen als versuchter Portscan interpretiert.

8.8.2 Konfiguration des IDS

Hier finden Sie die Einstellungen des IDS.



LANconfig: **Firewall/QoS** > **IDS**

Konsole: **Setup** > **IP-Router** > **Firewall**

Neben der Maximalzahl der Portanfragen, der Paket-Aktion und den möglichen Meldemechanismen gibt es hier noch weitergehende Reaktionsmöglichkeiten:

- Die Verbindung wird getrennt
- Die Adresse des Absenders wird für eine einstellbare Zeit gesperrt
- Der Zielport des Scans wird für eine einstellbare Zeit gesperrt

8.9 Schutz vor „Denial-of-Service"-Angriffen

Angriffe aus dem Internet können neben Einbruchsversuchen auch Angriffe mit dem Ziel sein, die Erreichbarkeit und Funktionstüchtigkeit einzelner Dienste zu blockieren. Diese Angriffe nennt man auch „Denial-of-Service" (DoS). Die Geräte

sind mit entsprechenden Schutzmechanismen ausgestattet, die bekannte Hacker-Angriffe erkennen und die Funktionstüchtigkeit erhalten.

Distributed-Denial-Of-Service (DDoS) ist ein Spezialfall von DoS, bei dem die Angriffe von einer Vielzahl von Rechnern ausgeht. Dieser Spezialfall wird durch diesen Schutzmechanismus auch abgedeckt.

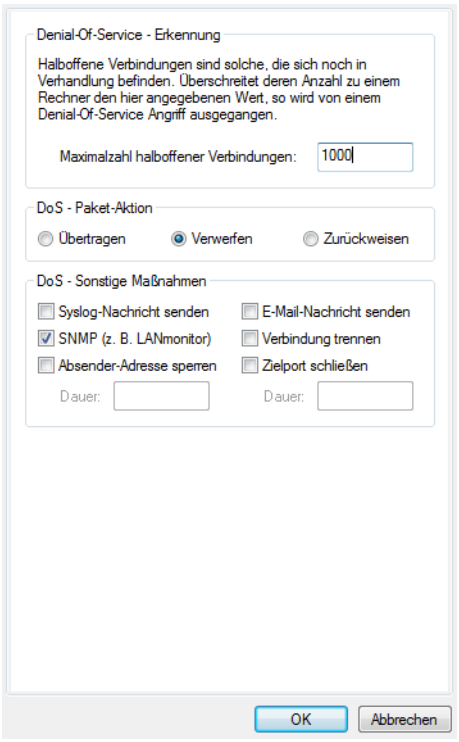
8.9.1 Erhöhter DoS-Schwellenwert für Zentralgeräte

Denial-Of-Service Angriffe nutzen prinzipielle Schwächen der TCP/IP-Protokolle sowie fehlerhafte Implementationen aus.

- Zu den Angriffen, die prinzipielle Schwächen ausnutzen, gehören z. B. SYN-Flood und Smurf.
- Zu den Angriffen, die fehlerhafte Implementationen zum Ziel haben, gehören alle Angriffe, die mit fehlerhaft fragmentierten Paketen operieren (z. B. Teardrop) oder mit gefälschten Absenderadressen arbeiten (z. B. Land).

Ihr Gerät erkennt die meisten dieser Angriffe und kann mit gezielten Gegenmaßnahmen reagieren. Für diese Erkennung wird die Anzahl der Verbindungen ermittelt, die sich noch in Verhandlung befinden (halboffene Verbindungen). Überschreitet die Anzahl der halboffenen Verbindungen einen Schwellenwert, geht das Gerät von einem DoS-Angriff aus. Die dann resultierenden Aktionen und Maßnahmen können wie bei Firewall-Regeln definiert werden.

Für Zentralgeräte befinden sich aufgrund der zumeist höheren Anzahl der angeschlossenen Benutzer auch ohne DoS-Angriff eine große Zahl von Verbindungen im halboffenen Zustand. Aus diesem Grund verwenden diese Geräte einen höheren Standard-Schwellenwert für die Erkennung der DoS-Angriffe.



LANconfig: **Firewall/QoS** > **DoS**

Konsole: **Setup** > **IP-Router** > **Firewall**

- **Maximalzahl halboffene Verbindungen**

  Legen Sie hier fest, ab welcher Anzahl von halboffenen Verbindungen die Aktionen zur Abwehr von DoS-Angriffen ausgelöst werden sollen.

  Mögliche Werte:

  - 0 bis 9999

Default:

- 100
- 1000 für Zentralgeräte

8.9.2 Beispiele für Denial-of-Service-Angriffe

Denial-Of-Service-Angriffe nutzen prinzipielle Schwächen der TCP/IP-Protokolle sowie fehlerhafte Implementationen von TCP/IP-Protokollstacks aus. Zu den Angriffen, die prinzipielle Schwächen ausnutzen, gehören z. B. SYN-Flood und Smurf. Zu den Angriffen, die fehlerhafte Implementationen zum Ziel haben, gehören alle Angriffe, die mit fehlerhaft fragmentierten Paketen operieren (z. B. Teardrop), oder die mit gefälschten Absenderadressen arbeiten (z. B. Land). Im folgenden werden einige dieser Attacken, deren Auswirkungen und mögliche Gegenmaßnahmen beschrieben.

8.9.2.1 SYN Flooding

Beim SYN-Flooding schickt der Angreifer in kurzen zeitlichen Abständen TCP-Pakete mit gesetztem SYN-Flag und sich ständig ändernden Quell-Ports auf offene Ports seines Opfers. Der angegriffene Rechner richtet darauf hin eine TCP-Verbindung ein, sendet dem Angreifer ein Paket mit gesetzten SYN- und ACK-Flags und wartet nun vergeblich auf die Bestätigung des Verbindungsaufbaus. Dadurch bleiben dann hunderte "halboffener" TCP-Verbindungen zurück, und verbrauchen Ressourcen (z. B. Speicher) des angegriffenen Rechners. Das ganze kann letztendlich so weit gehen, dass das Opfer keine TCP-Verbindung mehr annehmen kann oder gar aufgrund von Speichermangel abstürzt.

Als Gegenmaßnahme in einer Firewall hilft nur, die Anzahl "halboffener" TCP-Verbindungen, die zwischen zwei Rechnern bestehen zu überwachen und zu beschränken, d. h. falls weitere TCP-Verbindungen zwischen diesen Rechnern aufgebaut werden, dann müssen diese von der Firewall abgeblockt werden.

8.9.2.2 Smurf

Der Smurf-Angriff arbeitet zweistufig und legt gleich zwei Netze lahm. Im ersten Schritt wird mit gefälschter Absenderadresse ein Ping (ICMP Echo-Request) an die Broadcastadresse des ersten Netzes gesendet, worauf alle Rechner in diesem Netz mit einem ICMP-Echo-Reply an die gefälschte Absenderadresse (die im zweiten Netz liegt) antworten. Wenn die Rate der einkommenden Echo-Requests sowie die Anzahl der antwortenden Rechner hoch genug ist, dann wird zum einen der gesamte einkommende Traffic des zweiten Netzes für die Dauer der Attacke blockiert, zum anderen kann der Besitzer der gefälschten Adresse für die Dauer der Attacke keine normalen Daten mehr annehmen. Ist die gefälschte Absenderadresse die Broadcastadresse des zweiten Netzes, so sind sogar alle Rechner in diesem Netz blockiert.

In diesem Fall blockiert die DoS-Erkennung des Gerätes das Weiterleiten von Paketen, die an die lokale Broadcastadresse gerichtet sind.

8.9.2.3 LAND

Beim LAND-Angriff handelt es sich um ein TCP-Paket, dass mit gesetztem SYN-Flag und gefälschter Absender-Adresse an den Opferrechner geschickt wird. Das Pikante dabei ist, dass die gefälschte Absenderadresse gleich der Adresse des Opfers ist. Bei einer unglücklichen Implementierung des TCP wird das auf dieses Paket gesendete SYN-ACK vom Opfer wieder als SYN interpretiert und ein neues SYN-ACK gesendet. Dies führt zu einer Endlosschleife, die den Rechner einfrieren lässt.

Bei einer neueren Variante wird als Absenderadresse des Pakets nicht die Adresse des angegriffenen Rechners eingesetzt, sondern die Loopback-Adresse 127.0.0.1. Sinn dieser Täuschung ist es, Personal Firewalls zu überlisten, die zwar auf die klassische Variante (Absenderadresse = Zieladresse) reagieren, die neue Form aber ungehindert durchlassen. Diese Form wird vom Gerät ebenfalls erkannt und geblockt.

8.9.2.4 Ping of Death

Der Ping of Death gehört zu den Angriffen, die Fehler bei der Re-assemblierung von fragmentierten Paketen ausnutzen. Dies funktioniert wie folgt:

Im IP-Header befindet sich das Feld Fragment-Offset das angibt, an welcher Stelle das empfangene Fragment in das IP-Paket eingebaut werden soll. Dieses Feld hat eine Länge von 13 Bit und gibt die Einfügeposition in jeweils 8 Byte

grossen Schritten an. Die Einfügeposition kann daher zwischen 0 und 65528 Bytes liegen. Bei einer MTU auf dem Ethernet von 1500 Bytes kann somit ein bis zu 65528 + 1500 - 20 = 67008 Byte großes IP-Paket erzeugt werden, was zu Überläufen von internen Zählern führen oder gar Pufferüberläufe provozieren kann und es somit dem Angreifer gar die Möglichkeit eröffnet, eigenen Code auf dem Opferrechner auszuführen.

Hier bieten sich der Firewall zwei Möglichkeiten: Entweder, die Firewall re-assembliert das gesamte einkommende Paket und prüft dessen Integrität, oder aber es wird nur das Fragment, das über die maximale Paketgröße hinaus geht, verworfen. Im ersten Fall kann die Firewall bei einer fehlerhaften Implementation selbst zum Opfer werden, im zweiten Fall sammeln sich beim Opfer teilweise re-assemblierte Pakete an, die erst nach einer gewissen Zeit verworfen werden, wodurch sich ein neuer Denial-Of-Service Angriff ergeben kann, wenn dem Opfer dadurch der Speicher ausgeht.

8.9.2.5 Teardrop

Der Teardrop-Angriff arbeitet mit überlappenden Fragmenten. Dabei wird nach dem ersten Fragment ein weiteres geschickt, das komplett innerhalb des ersten liegt, d. h. das Ende des zweiten Fragments liegt vor dem Ende des ersten. Wird nun aus Bequemlichkeit des Programmierers des IP-Stack bei der Ermittlung der Länge der zur Re-assemblierung zu kopierenden Bytes einfach "neues Ende" - "altes Ende" gerechnet, so ergibt sich ein negativer Wert, bzw. ein sehr großer positiver Wert, durch den bei der Kopieroperation Teile des Speichers des Opfers überschrieben werden und der Rechner daraufhin abstürzt.

Auch hier hat die Firewall wieder zwei Möglichkeiten: Entweder sie re-assembliert selbst und verwirft ggf. das gesamte Paket, oder sie hält nur minimalen Offset und maximales Ende des Pakets nach und verwirft alle Fragmente, deren Offset oder Ende in diesen Bereich fallen. Im ersten Fall muss die Implementation innerhalb der Firewall korrekt sein, damit diese nicht selbst Opfer wird, im anderen Fall sammeln sich wieder teilweise re-assemblierte Pakete beim Opfer.

8.9.2.6 Bonk / Fragrouter

Bonk ist eine Variante des Teardrop-Angriffs, die jedoch nicht zum Ziel hat den angegriffenen Rechner zum Absturz zu bringen, sondern einfache Portfilter-Firewalls, die auch fragmentierte Pakete akzeptieren, auszutricksen und somit in das zu schützende Netz einzudringen. Bei diesem Angriff wird nämlich durch geschickte Wahl des Fragment-Offsets der UDP- oder TCP-Header des ersten Fragments überschrieben. Hierdurch akzeptieren einfache Portfilter-Firewalls das erste Paket und die dazugehörenden Fragmente. Durch das Überschreiben des Headers im zweiten Fragment, wird so ganz plötzlich aus einem erlaubten Paket ein Paket, das eigentlich in der Firewall geblockt werden sollte.

Auch hier gilt, die Firewall kann entweder selbst Re-assemblieren, oder nur das falsche Fragment (und alle nachfolgenden) filtern, mit den bereits oben angedeuteten Problemen der einen oder anderen Lösung.

In der Default-Einstellung sind alle Einstellungen auf "sicher" konfiguriert, d. h. maximal 100 zulässige halboffene Verbindungen von verschiedenen Rechnern (vgl. SYN-Flooding), maximal 50 halboffene Verbindungen von einem Rechner (vgl. Portscan), fragmentierte Pakete werden re-assembliert.

8.9.3 Konfiguration der DoS-Abwehr

LANconfig: **Firewall/QoS** > **DoS**

Konsole: **Setup** > **IP-Router** > **Firewall**

Um die Anfälligkeit des Netzes vor DoS-Attacken schon im Vorfeld drastisch zu reduzieren, dürfen Pakete aus entfernten Netzen nur dann angenommen werden, wenn entweder eine Verbindung vom internen Netz aus initiiert wurde, oder die einkommenden Pakete durch einen expliziten Filtereintrag (Quelle: entferntes Netz, Ziel: lokales Netz) zugelassen werden. Diese Maßnahme blockiert bereits eine Vielzahl von Angriffen.

Für alle erlaubten Zugriffe werden im Gerät explizit Verbindungszustand, Quell-Adressen und Korrektheit von Fragmenten überprüft. Dies geschieht sowohl für einkommende als auch für ausgehende Pakete, da ein Angriff auch aus dem lokalen Netz heraus gestartet werden kann.

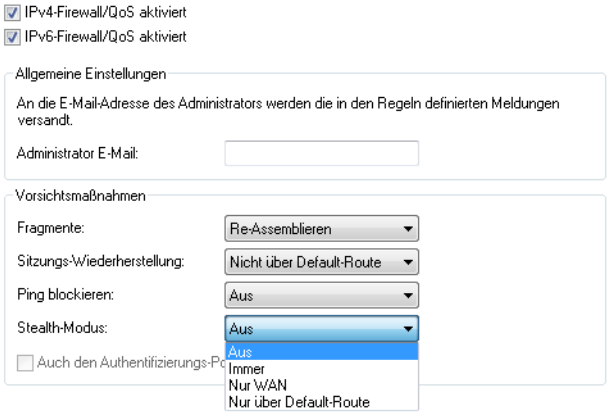
Um nicht durch fehlerhafte Konfiguration der Firewall ein Tor für DoS-Angriffe zu öffnen, wird dieser Teil zentral konfiguriert. Neben der Maximalzahl der halboffenen Verbindungen, der Paket-Aktion und den möglichen Meldemechanismen gibt es hier noch weitergehende Reaktionsmöglichkeiten:

- Die Verbindung wird getrennt
- Die Adresse des Absenders wird für eine einstellbare Zeit gesperrt
- Der Zielport des Scans wird für eine einstellbare Zeit gesperrt

Immer aktiv hingegen sind folgende Schutzmechanismen:

- Adressüberprüfung (gegen IP-Spoofing)
- Abblocken von Broadcasts in lokale Netz (gegen Smurf und Co)

8.9.4 Konfiguration von ping-Blocking und Stealth-Modus



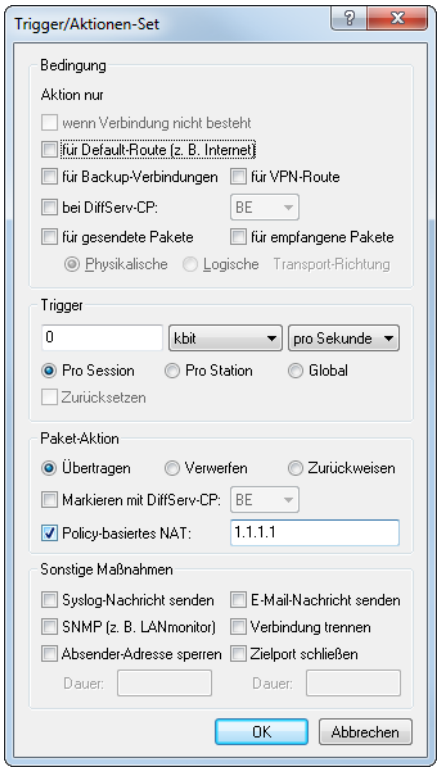
LANconfig: **Firewall/QoS** > **Allgemein**

Konsole: **Setup** > **IP-Router** > **Firewall**

8.10 WAN Policy-Based NAT

WAN Policy-Based NAT ermöglicht die Adressumsetzung (Maskierung) von Verbindungen basierend auf Firewall-Regeln. Es kann konfiguriert werden, hinter welcher vom Provider zugewiesenen WAN-IPv4-Adresse interne Adressen umgesetzt (maskiert) werden sollen. Ideal für Szenarien, in denen der Provider mehrere statische IPv4-Adressen zugewiesen hat, z. B. für den Betrieb von Mailservern und Webservern mit verschiedenen WAN-Adressen.

In der Firewall gibt es dazu die neue Paket-Option **Policy-basiertes NAT** unter **Firewall/QoS** > **IPv4-Regeln** > **Aktions-Objekte**. Diese Aktion ist zusammen mit der Option **Übertragen** verwendbar und ermöglicht das maskieren bzw. NAT hinter eine definierten IPv4-Adresse.



Der Parameter muss als feste IP-Adresse eingetragen werden. Dynamische IP-Adressen werden nicht unterstützt.

NAT ist nur möglich, falls eine WAN-Schnittstelle beteiligt ist. NAT zwischen zwei LAN-Schnittstellen wird nicht unterstützt.

Auf der Konsole (`/Setup/IP-Router/Firewall/Aktions-Tabelle`) kann dazu die Variable `%Y` als Aktion verwendet werden.

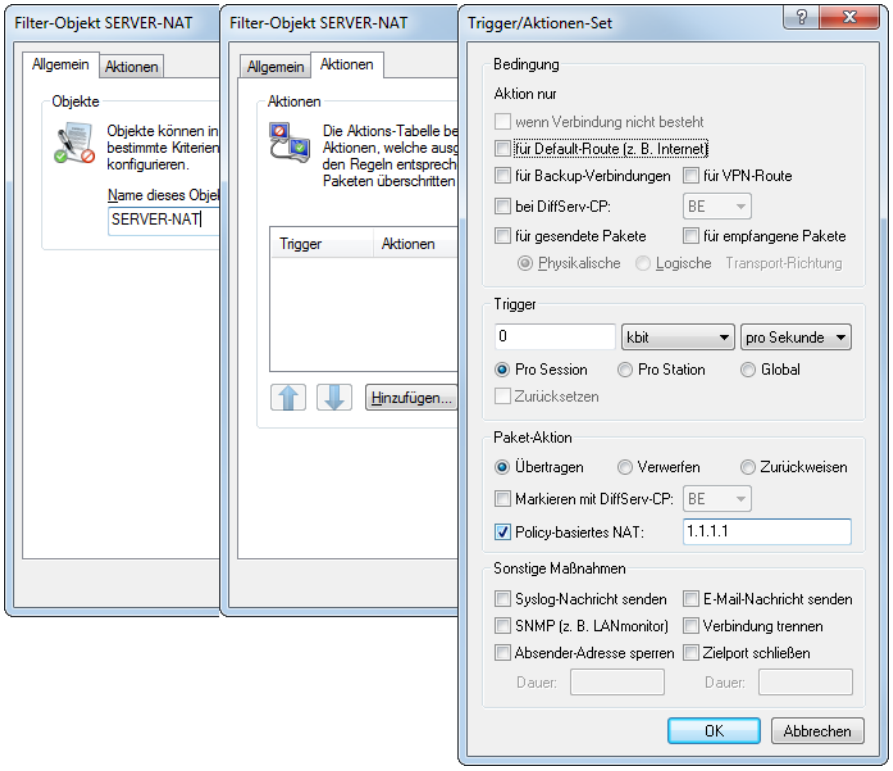
8.10.1 Konfiguration eines Policy-basierten NATs mit Firewall-Regeln

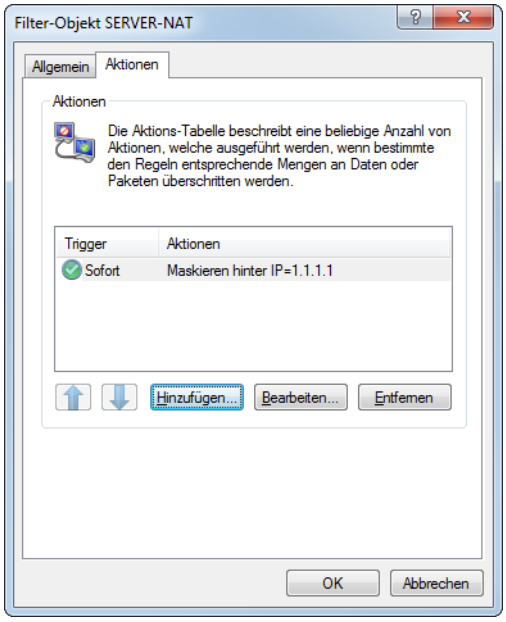
In dem folgenden Beispiel ist ein IPv4-Netzwerk (Intranet) mit Subnetz 192.168.80.0/24 konfiguriert. Der Internetprovider hat mehrere öffentliche IP-Adressen zugewiesen. Der Internetzugang ist mit dem Setup-Assistenten eingerichtet worden. Die Clients aus dem Intranet werden automatisch hinter der öffentlichen IP-Adresse, die mit dem Assistenten angelegt wurde, maskiert.

Aus diesem Netzwerk soll nun ein Server mit der internen IP-Adresse 192.168.80.21 hinter der öffentlichen IP-Adresse 1.1.1.1 maskiert werden.

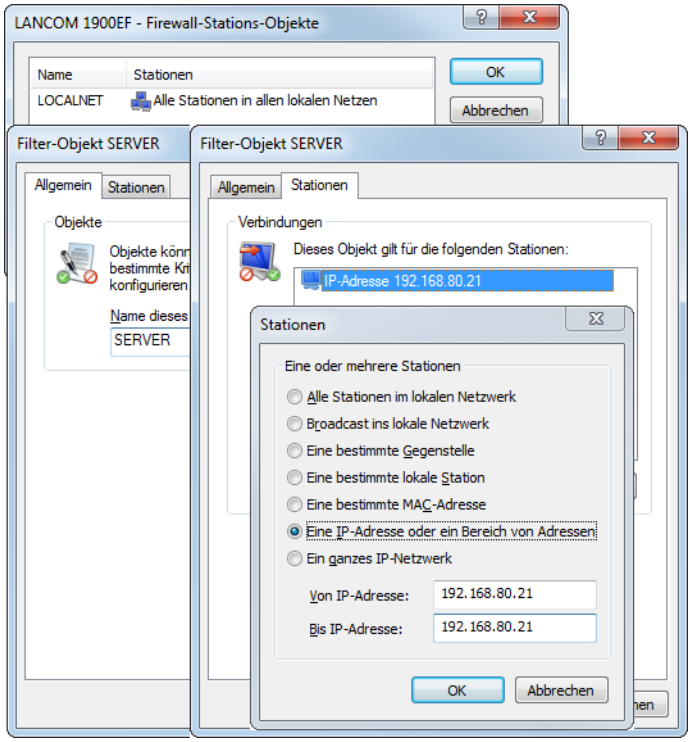
Die „Rückwärtsrichtung" der Maskierung bzw. Erreichbarkeit des Servers von außen, wird über einen Portforwarding-Eintrag realisiert, der nicht Teil dieses Beispiels ist.

1. Legen Sie unter **Firewall/QoS** > **IPv4-Regeln** > **Aktions-Objekte** ein neues Firewall-Aktionsobjekt an. Setzen Sie unter Aktion die Paket-Aktion auf **Übertragen** und dann **Policy-basiertes NAT** auf 1.1.1.1.

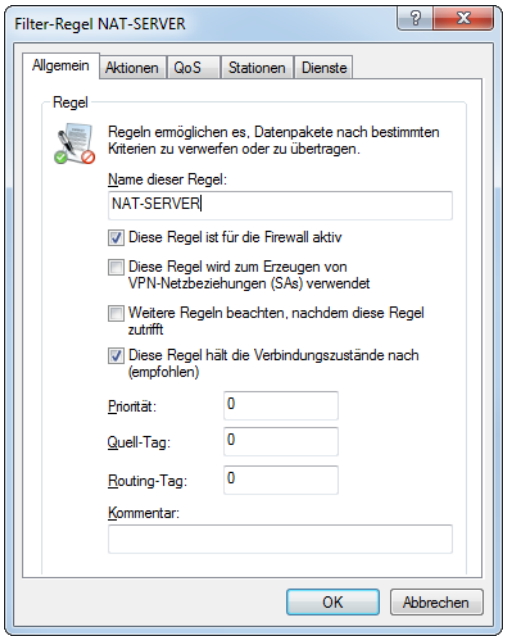




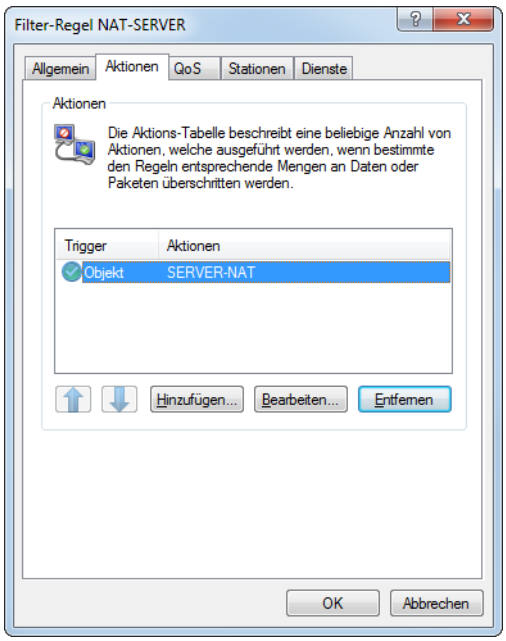
2. Legen Sie unter **Firewall/QoS** > **IPv4-Regeln** > **Stations-Objekte** ein neues Stationsobjekt an, das für die IP-Adresse 192.168.80.21 definiert wird.



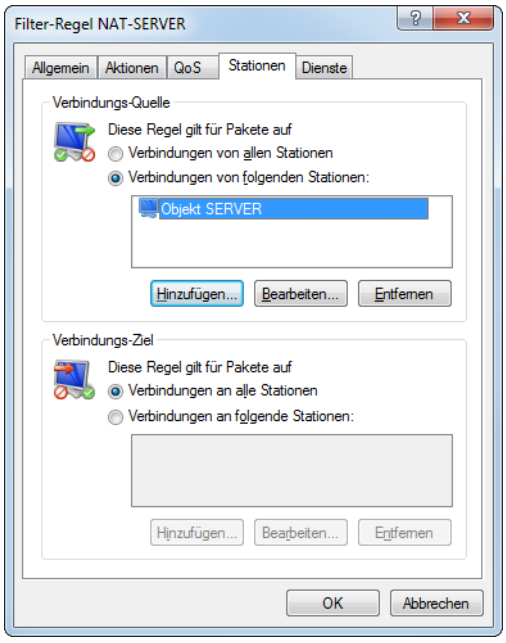
3. Als nächstes legen Sie unter **Firewall/QoS** > **IPv4-Regeln** > **Firewall-Regeln** eine Filter-Regel an.

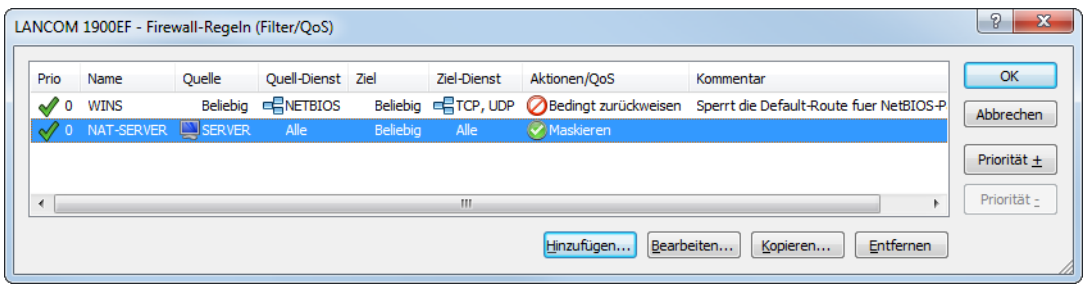


4. In dieser Filter-Regel geben Sie unter **Aktionen** die weiter oben neu definierte Aktion „SERVER-NAT“ an.



5. Danach noch in dieser Filter-Regel unter **Stationen** das neu angelegte Stationsobjekt verwenden. Ggfs. können Sie bei Bedarf als **Verbindungsziel** noch die Internetleitung angeben.





9 Quality-of-Service

Dieses Kapitel widmet sich dem Thema Quality-of-Service (kurz: QoS). Unter diesem Oberbegriff sind die Funktionen des LCOS zusammengefasst, die sich mit der Sicherstellung von bestimmten Dienstgüten befassen.

9.1 Wozu QoS?

Generell möchte man mit dem Quality-of-Service erreichen, dass bestimmte Datenpakete entweder besonders sicher oder möglichst sofort übertragen werden.

- Bei der Datenübertragung kann es durchaus vorkommen, dass Datenpakete gar nicht beim Empfänger ankommen. Für manche Anwendungen ist es aber sehr wichtig, dass alle abgeschickten Pakete auch wirklich ankommen. Eine in mehrere kleine Datenpakete aufgeteilte E-Mail kann z. B. beim Empfänger nur dann wieder zusammengebaut werden, wenn alle Teile vollständig angekommen sind. Ob das eine oder andere Paket dabei mit kleinen Zeitverzögerungen eintrifft, ist jedoch weniger wichtig. Diese Anwendungen setzen meistens auf das verbindungsorientierte Transmission Control Protocol (TCP). Dieses Protokoll stellt sicher, dass die Daten korrekt und in der richtigen Reihenfolge über das Netz transportiert werden. Es regelt dabei die Senderate selbst herunter, wenn die Bestätigungen der verschickten Datenpakete länger auf sich warten lassen, und sorgt im Falle eines Paketverlustes automatisch für ein erneutes Übertragen.
- Bei anderen Anwendungen wie z. B. der Telefonie über das Internet (Voice-over-IP, VoIP) ist es im Gegenteil dazu sehr wichtig, dass die Datenpakete nur mit geringer zeitlicher Verzögerung beim Empfänger eintreffen. Ob dabei einmal ein Datenpaket verloren geht, ist hier weniger wichtig. Der Teilnehmer am anderen Ende der Verbindung versteht den Anrufer auch dann, wenn kleine Teile der Sprache verloren gehen. Bei dieser Anwendung steht also der Wunsch im Vordergrund, dass die zu versendenden Datenpakete möglichst sofort verschickt werden. Für diese Anwendungen wird oft das verbindungslose User Datagram Protocol (UDP) eingesetzt. Bei diesem Protokoll ist der Overhead für die Verwaltung sehr gering. Allerdings ist die Zustellung der Pakete in der richtigen Reihenfolge nicht garantiert, die Datenpakete werden einfach losgeschickt. Da es keine Empfangsbestätigung gibt, werden verlorene Pakete auch nicht erneut zugestellt.

9.2 Welche Datenpakete bevorzugen?

Die Notwendigkeit für das QoS-Konzept entsteht erst durch die Tatsache, dass die verfügbare Bandbreite nicht immer ausreicht, um alle anstehenden Datenpakete zuverlässig und rechtzeitig zu übertragen. Werden über die Datenleitung gleichzeitig große FTP-Downloads gefahren, E-Mails ausgetauscht und IP-Telefone verwendet, kommt es sehr schnell zu Belastungsspitzen. Um auch in diesen Situationen die Anforderungen an die gewünschte Datenübertragung sicher zu stellen, müssen bestimmte Datenpakete bevorzugt behandelt werden. Dazu muss ein Gerät zunächst einmal erkennen, welche Datenpakete denn überhaupt bevorzugt werden sollen.

Es gibt zwei Möglichkeiten, den Bedarf für eine bevorzugte Behandlung von Datenpaketen im Gerät zu signalisieren:

- Die Applikation, wie z. B. die Software von einigen IP-Telefonen, kann die Datenpakete selbst entsprechend kennzeichnen. Diese Kennzeichnung, das „Tag", wird in den Header der IP-Pakete eingefügt. Die beiden verschiedenen Varianten dieser Kennzeichnung „ToS" und „DiffServ" können vereinfacht dargestellt folgende Zustände annehmen:
  - ToS "Low Delay"
  - ToS "High Reliability"
  - DiffServ "Expedited Forwarding"
  - DiffServ "Assured Forwarding"

Die IP-Header-Bits des ToS- bzw. DiffServ-Feldes werden im Falle einer VPN-Strecke auch in den umgebenden IP-Header des IPSec-VPN-Paketes kopiert. Somit steht QoS auch für VPN-Strecken über das Internet zur Verfügung, sofern der Provider entsprechende Pakete auch im WAN bevorzugt behandelt.

- Wenn die Applikation selbst nicht die Möglichkeit hat, die Datenpakete entsprechend zu kennzeichnen, kann das Gerät für die richtige Behandlung sorgen. Dazu werden die vorhandenen Funktionen der Firewall genutzt, die Datenpakete z. B. nach Subnetzen oder Diensten (Anwendungen) klassifizieren kann. Mit diesen Funktionen ist es z. B. möglich, die Datenpakete einer FTP-Verbindung oder die einer bestimmten Abteilung (in einem separaten Subnetz) gesondert zu behandeln.

  Für die Behandlung von Datenpaketen, die über die Firewall klassifiziert werden, stehen die beiden folgenden Möglichkeiten zur Auswahl:

  - Garantierte Mindestbandbreite
  - Limitierte Maximalbandbreite

9.2.1 Was ist DiffServ?

DiffServ steht für „Differentiated Services" und stellt ein Modell dar, die Priorität der Datenpakete zu signalisieren. DiffServ basiert auf dem Type-of-Service(ToS)-Feld und nutzt das gleiche Byte im IP-Header.

ToS verwendet die ersten drei Bits zur Kennzeichnung der Prioritäten (Precedence) 0 bis 7 und vier weitere Bits (die ToS-Bits) zur Optimierung des Datenflusses (u. a. "Low Delay" und "High Reliability"). Dieses Modell ist recht unflexibel und wurde daher in der Vergangenheit eher selten verwendet.

Das DiffServ-Modell nutzt die ersten 6 Bits zur Unterscheidung verschiedener Klassen. Damit sind bis zu 64 Abstufungen (Differentiated Services Code Point, DSCP) möglich, die eine feinere Priorisierung des Datenflusses ermöglichen:

- Um die Abwärtskompatibilität zur ToS-Implementation sicherzustellen, können mit den „Class Selectors" (CS0 bis CS7) die bisherigen Precedence-Stufen abgebildet werden. Die Stufe CS0 wird dabei auch als „Best Effort" (BE) bezeichnet und steht für die normale Übertragung der Datenpakete ohne besondere Behandlung.
- Die „Assured Forwarding"-Klassen werden für die gesicherte Übertragung von Datenpaketen eingesetzt. Die erste Ziffer der AF-Klasse steht jeweils für die Priorität der Übertragung (1 bis 4), die zweite Ziffer für „Drop-Wahrscheinlichkeit" (1 bis 3). Pakete mit AFxx-Kennzeichnung werden „gesichert" übertragen, also nicht verworfen.

Mit der Klasse „Expedited Forwarding" schließlich werden die Pakete markiert, die vor allen anderen Paketen (bevorzugt) übertragen werden sollen.

Codepoint	DSCP Bits	Dez.	Codepoint	DSCP Bits	Dez.	Codepoint	DSCP Bits	Dez.
CS0 (BE)	000000	0	AF11	001010	10	AF33	011110	30
CS1	001000	8	AF12	001100	12	AF41	100010	34
CS2	010000	16	AF13	001110	14	AF42	100100	36
CS3	011000	24	AF21	010010	18	AF43	100110	38
CS4	100000	32	AF22	010100	20	EF	101110	46
CS5	101000	40	AF23	010110	22			
CS6	110000	48	AF31	011010	26			
CS7	111000	56	AF32	011100	28			

9.2.2 Garantierte Mindestbandbreiten

Hiermit geben Sie Vorfahrt für sehr wichtige Applikationen, Voice-over-IP (VoIP)-TK-Anlagen oder bestimmte Benutzergruppen.

Bei Geräten mit integrierter oder nachträglich über Software-Option freigeschalteter VoIP-Funktion werden die QoS-Einstellungen für SIP-Gespräche automatisch vorgenommen!

9.2.2.1 Volldynamisches Bandbreitenmanagement beim Senden

Das Bandbreitenmanagement erfolgt in Senderichtung dynamisch. Dies bedeutet, dass z. B. eine garantierte Mindestbandbreite nur solange zur Verfügung gestellt wird, wie auch tatsächlich entsprechender Datentransfer anliegt.

Ein Beispiel:

Zur Übertragung von VoIP-Daten eines entsprechenden VoIP-Gateways soll immer eine Bandbreite von 256 kBit/s garantiert werden. Ein einzelne VoIP-Verbindung benötigt 32 kBit/s.

Solange niemand telefoniert, steht die gesamte Bandbreite anderen Diensten zur Verfügung. Mit jeder neu aufgebauten VoIP-Verbindung stehen den anderen Anwendungen jeweils 32 kBit/s weniger zur Verfügung, bis 8 VoIP-Verbindungen aktiv sind. Sobald eine VoIP-Verbindung beendet ist, steht die entsprechende Bandbreite wieder allen anderen Anwendungen zur Verfügung.

Für das korrekte Funktionieren dieses Mechanismus darf die Summe der konfigurierten Mindestbandbreiten die effektiv zur Verfügung stehende Sendebandbreite nicht übersteigen.

9.2.2.2 Dynamisches Bandbreitenmanagement auch beim Empfang

Zur empfangsseitigen Bandbreitensteuerung können Pakete zwischengespeichert und erst verzögert bestätigt werden. Dadurch regeln sich TCP/IP-Verbindungen selbständig auf eine geringere Bandbreite ein.

Jedem WAN-Interface ist eine maximale Empfangsbandbreite zugeordnet. Diese Bandbreite wird durch jede QoS-Regel, die eine minimale Empfangsbandbreite auf diesem Interface garantiert, entsprechend reduziert.

- Ist die QoS-Regel verbindungsbezogen definiert, wird die reservierte Bandbreite direkt nach dem Beenden der Verbindung wieder freigegeben, und die maximal auf dem WAN-Interface verfügbare Bandbreite steigt entsprechend an.
- Ist die QoS-Regel global definiert, wird die reservierte Bandbreite erst nach dem Beenden der letzten Verbindung wieder freigegeben.

9.2.3 Limitierte Maximalbandbreiten

Hiermit schränken Sie z. B. die gesamte oder verbindungsbezogene Maximalbandbreite für Serverzugriffe ein.

Ein Beispiel:

Sie betreiben einen Webserver und ein lokales Netzwerk an einem gemeinsamen Internetzugang.

Um zu verhindern, dass Ihr Produktivnetz (LAN) von vielen Internetzugriffen auf Ihren Webserver lahmgelegt wird, limitieren Sie alle Serverzugriffe auf die Hälfte der Ihnen zur Verfügung stehenden Bandbreite. Um ferner sicherzustellen, dass Ihre Serverdienste vielen Benutzern gleichzeitig und gleichberechtigt zugute kommen, setzen Sie pro Verbindung zum Server eine bestimmte Maximalbandbreite.

9.2.3.1 Kombination möglich

Minimal- und Maximalbandbreiten können kombiniert zusammen verwendet werden. Somit kann die zur Verfügung stehende Bandbreite speziell nach Ihren Erfordernissen z. B. auf bestimmte Benutzergruppen oder Anwendungen verteilt werden.

9.3 Das Warteschlangenkonzept

9.3.1 Sendeseitige Warteschlangen

Die Anforderungen an die Dienstgüte werden im LCOS durch den Einsatz mehrerer Warteschlangen (Queues) für die Datenpakete realisiert. Auf der Sendeseite kommen folgende Queues zum Einsatz:

- Urgent-Queue I

  Diese Queue wird immer vor allen anderen abgearbeitet. Hier landen folgende Datenpakete:

  - Pakete mit ToS "Low Delay"
  - Pakete mit DiffServ "Expedited Forwarding"
  - Alle Pakete, denen eine bestimme Mindestbandbreite zugewiesen wurde, solange die garantierte Minimalbandbreite nicht überschritten wird
  - TCP-Steuerungspakete können ebenfalls durch diese Queue bevorzugt versendet werden

- Urgent Queue II

  Hier landen alle Pakete, die eine garantierte Mindestbandbreite zugewiesen bekommen haben, deren Verbindung diese aber überschritten hat.

  Solange das Intervall für die Mindestbandbreite läuft (z. B. bis zum Ende der laufenden Sekunde) werden alle Pakete in dieser Queue ohne weitere besondere Priorität behandelt. Alle Pakete in dieser Queue, der "gesicherten Queue" und der "Standard-Queue" teilen sich von nun an die vorhandene Bandbreite. Die Pakete werden beim Senden in der Reihenfolge aus den Queues geholt, in der sie auch in die Queues gestellt wurden. Läuft das Intervall ab, werden alle Blöcke, die sich zu diesem Zeitpunkt noch in der Urgent Queue II befinden, bis zum Überschreiten der jeweils zugeteilten Mindestbandbreite wieder in die Urgent Queue I gestellt, der Rest verbleibt in der Urgent Queue II.

  Mit diesem Verfahren wird sichergestellt, dass priorisierte Verbindungen den restlichen Datenverkehr nicht erdrücken.

- gesicherte Queue

  Diese Warteschlange hat keine gesonderte Priorität. Jedoch werden Pakete in dieser Queue niemals verworfen (garantierte Übertragung). Hier landen folgende Datenpakete:

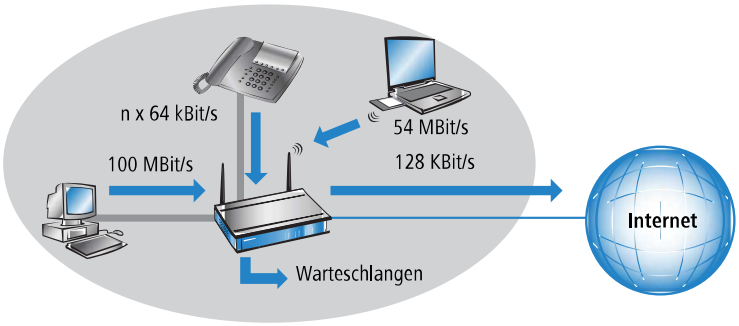
  - Pakete mit ToS "High Reliability"
  - Pakete mit DiffServ "Assured Forwarding"

- Standard-Queue

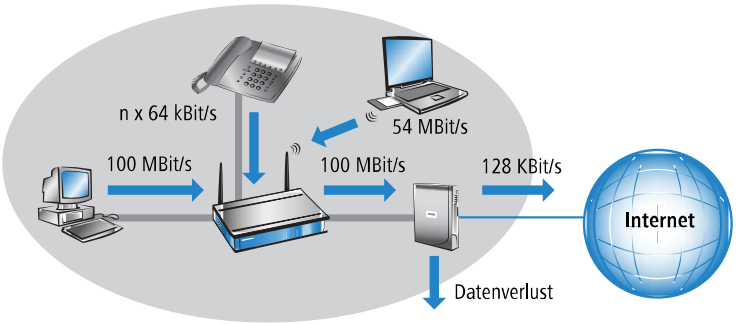
  Die Standard-Warteschlange enthält alle nicht klassifizierten Datenpakete. Pakete in dieser Queue werden zuerst verworfen, sofern die Datenpakete nicht schnell genug abgeliefert werden können.

  Das Konzept der Warteschlangen funktioniert natürlich nur, wenn sich an der Schnittstelle vom LAN zum WAN ein Stau von Datenpaketen bildet. Dieser Stau bildet sich dann, wenn das Interface im Gerät weniger Daten an das WAN abgeben kann, als aus dem LAN in den Spitzenzeiten angeliefert werden. Das ist z. B. dann der Fall, wenn die Schnittstelle zum WAN ein integriertes ADSL Interface mit vergleichsweiser geringer Sendegeschwindigkeit (Upstream)

ist. Das integrierte ADSL-Modem meldet selbständig an das Gerät zurück, wie viele Datenpakete es noch aufnehmen kann und bremst so den Datenfluss schon im Router. Dabei werden dann automatisch die Warteschlangen gefüllt.



Anders sieht das aus, wenn ein Ethernet-Interface die Verbindung ins WAN darstellt. Aus Sicht des Geräts sieht die Verbindung ins Internet über ein externes DSL-Modem wie ein Ethernet-Abschnitt aus. Auf der Strecke vom Gerät zum DSL-Modem werden die Daten auch mit der vollen LAN-Geschwindigkeit von 10, 100, 1000 oder mehr MBit/s übertragen. Hier bildet sich also kein natürlicher Stau, da die Ein- und Ausgangsgeschwindigkeiten gleich sind. Außerdem meldet das Ethernet zwischen Gerät und DSL-Modem nichts über die Kapazität der Verbindung zurück. Die Folge: erst im DSL-Modem kommt es zum Stau. Da hier keine Warteschlangen mehr vorhanden sind, gehen die überschüssigen Daten verloren. Eine Priorisierung der bevorzugten Daten ist also nicht möglich.



Um dieses Problem zu lösen, wird die Übertragungsrate des WAN-Interfaces im Gerät künstlich gedrosselt. Die Schnittstelle wird dabei auf die Übertragungsrate eingestellt, die für den Transport der Daten ins WAN zur Verfügung stehen.

Bei der von den Providern angegebenen Datenrate handelt es sich meistens um die Nettodatenrate. Die für das Interface nutzbare Bruttodatenrate liegt etwas höher als die vom Provider garantierte Nettodatenrate. Wenn Sie die Bruttodatenrate Ihres Providers kennen, können Sie diesen Wert für das Interface eintragen und damit den Datendurchsatz leicht steigern. Mit der Angabe der Nettodatenrate sind Sie aber auf jeden Fall auf der sicheren Seite!

9.3.2 Empfangsseitige Warteschlangen

Neben der Übertragungsrate in Senderichtung gilt die gleiche Überlegung auch für die Empfangsrichtung. Hier bekommt das WAN-Interface des Geräts vom DSL-Modem deutlich weniger Daten angeliefert, als eigentlich aufgrund der Geschwindigkeit des Ethernet-Interfaces möglich wäre. Alle auf dem WAN-Interface empfangenen Datenpakete werden gleichberechtigt in das LAN übertragen.

Um die eingehenden Daten priorisieren zu können, muss also auch in dieser Richtung eine künstliche Bremse eingeschaltet werden. Wie schon bei der Senderichtung wird daher die Übertragungsrate der Schnittstelle in Empfangsrichtung an das Angebot des Providers angepasst, also z. B. auf eine Downstreamrate von 16 MBit/s. Auch hier kann wie bei der Upstreamrate die Bruttodatenrate eingetragen werden, wenn bekannt.

Das Reduzieren der Empfangsbandbreite macht es nun möglich, die empfangenen Datenpakete angemessen zu behandeln. Die bevorzugten Datenpakete werden bis zur garantierten Mindestbandbreite direkt in das LAN weitergegeben, die restlichen Datenpakete laufen in einen Stau. Dieser Stau führt in der Regel zu einer verzögerten Bestätigung der Pakete. Bei einer TCP-Verbindung wird der sendende Server auf diese Verzögerungen reagieren, seine Sendefrequenz herabsetzen und sich so der verfügbaren Bandbreite anpassen.

Auf der Empfangsseite kommen folgende Queues zum Einsatz:

- Deferred Acknowledge Queue

  Jedes WAN-Interface erhält zusätzlich eine QoS-Empfangsqueue, welche die Pakete aufnimmt, die ausgebremst werden sollen. Die Verweildauer jedes einzelnen Pakets richtet sich nach der Länge des Pakets und der aktuell zulässigen Empfangsbandbreite. Pakete, für die über eine QoS-Regel eine empfangsseitige Mindestbandbreite definiert ist, werden ungebremst durchgelassen, solange die Mindestbandbreite nicht überschritten wurde.

- normale Empfangsqueue

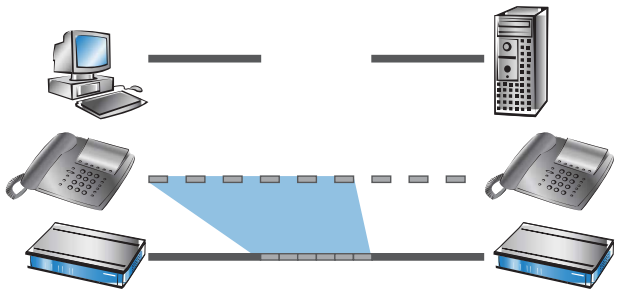
  Hier landen alle Pakete, die nicht aufgrund einer empfangsseitig aktiven QoS-Regel gesondert behandelt werden müssen. Pakete in dieser Queue werden direkt weitergeleitet bzw. bestätigt, ohne Maximalbandbreiten zu berücksichtigen.

9.4 Reduzierung der Paketlänge

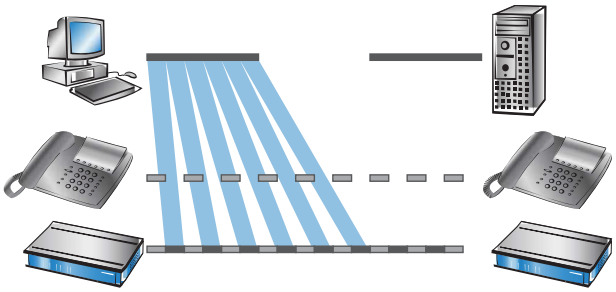
Die bevorzugte Behandlung von Datenpaketen einer wichtigen Applikation kann je nach Situation durch extrem lange Datenpakete anderer Anwendungen gefährdet werden. Das ist z. B. dann der Fall, wenn IP-Telefonie und ein FTP-Datentransfer gleichzeitig auf der WAN-Verbindung aktiv sind.



Der FTP-Transfer setzt recht große Datenpakete von 1500 Byte ein, während die Voice-over-IP-Verbindung Pakete von z. B. netto 24 Byte in relativ kurzen Takten verschickt. Wenn sich in dem Moment, in dem ein VoIP-Paket übertragen werden soll, z. B. schon FTP-Pakete in der Sendequeue des Gerätes befinden, kann das VoIP-Paket erst dann verschickt werden, wenn die Leitung wieder frei ist. Je nach Übertragungsrate der Verbindung kann das zu einer merklichen Verzögerung der Sprachübertragung führen.



Dieses störende Verhalten kann ausgeglichen werden, wenn alle Datenpakete, die nicht zu der über QoS bevorzugten Verbindung gehören, eine bestimmte Länge nicht überschreiten. Auf der FTP-Verbindung werden dann z. B. nur so kleine Pakete verschickt, dass die zeitkritische VoIP-Verbindung die Pakete in der benötigten Taktung ohne zeitliche Verzögerung zustellen kann. Für die TCP-gesicherte FTP-Übertragung wirkt sich die sich möglicherweise einstellende Verzögerung nicht nachteilig aus.



Zur Beeinflussung der Paketlänge gibt es zwei verschiedene Verfahren:

- Das Gerät kann die Teilnehmer der Datenverbindung informieren, dass sie nur Datenpakete bis zu einer bestimmten Länge verschicken sollen. Dabei wird eine passende PMTU (Path Maximum Transmission Unit) auf der Sendeseite erzwungen, das Verfahren bezeichnet man als „PMTU-Reduzierung".

  Die PMTU-Reduzierung kann dabei sowohl in Sende- als auch in Empfangsrichtung eingesetzt werden. Für die Senderichtung werden die Absender im eigenen LAN mit der PMTU-Reduzierung auf eine geringere Paketgröße eingestellt, für die Empfangsrichtung die Absender im WAN, z. B. Web- oder FTP-Server im Internet.

  Sofern die Datenverbindung schon besteht, wenn die VoIP-Verbindung gestartet wird, regeln die Absender die Paketlänge sehr schnell auf den zulässigen Wert zurück. Beim Aufbau von neuen Datenverbindungen, während die VoIP-Verbindung schon steht, wird während der Verbindungsverhandlung direkt die maximal zulässige Paketlänge vereinbart.

  Die reduzierte Paketlänge auf der Datenverbindung bleibt auch nach dem Beenden der VoIP-Verbindung bestehen, bis der Absender den PMTU-Wert erneut überprüft.

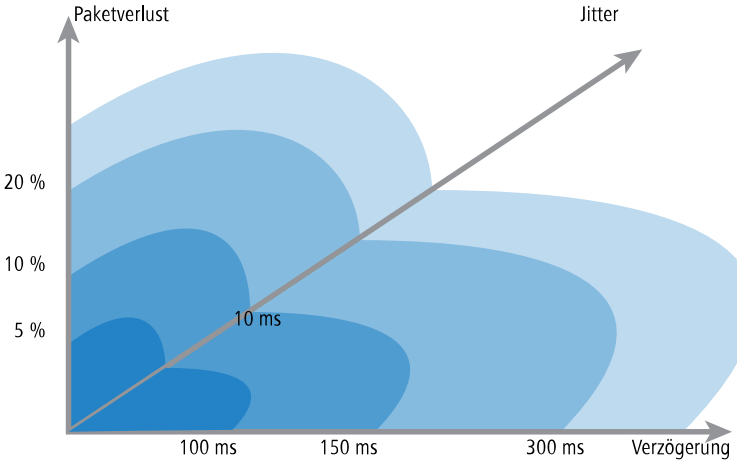
- Das Gerät kann die zu sendenden Pakete oberhalb einer einstellbaren Maximalgröße (z. B. 256 Byte) selbst in kleinere Einheiten aufteilen. Dieses als „Fragmentieren" bezeichnete Verfahren wird jedoch nicht von allen Servern im Internet unterstützt, da die Verarbeitung von fragmentierten Paketen als Sicherheitsrisiko betrachtet wird und in vielen Servern ausgeschaltet ist. Dadurch kann es zu Störungen z. B. beim Datendownload oder bei der Übertragung von Webseiten kommen.

  Dieses Verfahren ist daher nur für solche Verbindungen zu empfehlen, bei denen keine unbekannten Server im Internet beteiligt sind, z. B. bei der direkten Anbindung von Filialen an eine Zentrale über eine VPN-Verbindung, über die nicht gleichzeitig der Internet-Traffic läuft.

9.5 QoS-Parameter für Voice-over-IP-Anwendungen

Eine wichtige Aufgabe bei der Konfiguration von VoIP-Systemen ist die Sicherstellung einer ausreichenden Sprachqualität. Zwei Faktoren beeinflussen die Sprachqualität einer VoIP-Verbindung wesentlich: Die Verzögerung der Sprache auf dem Weg vom Sender zum Empfänger sowie der Verlust von Datenpaketen, die nicht oder nicht rechtzeitig beim Empfänger eintreffen. Die International Telecommunication Union (ITU) hat in umfangreichen Tests untersucht, was der Mensch als ausreichende Sprachqualität empfindet, und als Resultat die Empfehlung der ITU G.114 veröffentlicht.

Bei Geräten mit integrierter oder nachträglich über Software-Option freigeschalteter VoIP-Funktion werden die QoS-Einstellungen für SIP-Gespräche automatisch vorgenommen!



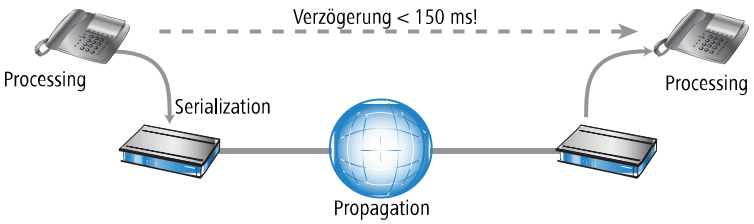
Bei einer Verzögerung von nicht mehr als 100 ms und einem Paketverlust von weniger als 5 % wird die Qualität wie bei einer normalen Telefonverbindung empfunden, bei nicht mehr als 150 ms Verzögerung und weniger als 10 % Paketverlust empfindet der Telefonteilnehmer immer noch eine sehr gute Qualität. Bis zu 300 ms bei 20 % schließlich empfinden manche Hörer die Qualität noch als brauchbar, darüber hinaus gilt die Verbindung als nicht mehr brauchbar für die Sprachübertragung.

Neben der mittleren Verzögerungszeit wird auch die Schwankung in dieser Verzögerung vom menschlichen Ohr wahrgenommen. Die Unterschiede in der Laufzeit der Sprachinformationen vom Sender zum Empfänger (Jitter) werden bis zu 10 ms noch toleriert, darüber hinaus als störend empfunden.

Die Konfiguration einer VoIP-Verbindung soll dementsprechend so erfolgen, dass die Randwerte für eine gute Sprachqualität eingehalten werden: Paketverlust bis 10 %, Verzögerung bis 150 ms, Jitter bis 10 ms.

- Der Jitter kann beim Empfänger durch einen entsprechenden Puffer ausgeglichen werden. In diesem Puffer (Jitter-Buffer) werden einige Pakete zwischengespeichert und mit konstantem Abstand an den Empfänger weitergegeben. Durch diese Zwischenspeicherung können die Schwankungen in der Übertragungszeit zwischen den einzelnen Pakete ausgeglichen werden.
- Die Verzögerung wird von mehren Komponenten beeinflusst:
  - Zum fixen Anteil der Verzögerung tragen die Zeit der Verarbeitung (Processing: Paketierung, Kodierung und Kompression beim Absender sowie beim Empfänger), die Dauer für Übergabe des Pakets von der Anwendung an das Interface (Serialization) und die Zeit für die Übertragung über die WAN-Strecke (Propagation) bei.
  - Der variable Anteil wird vom Jitter bzw. dem eingestellen Jitter-Buffer bestimmt.

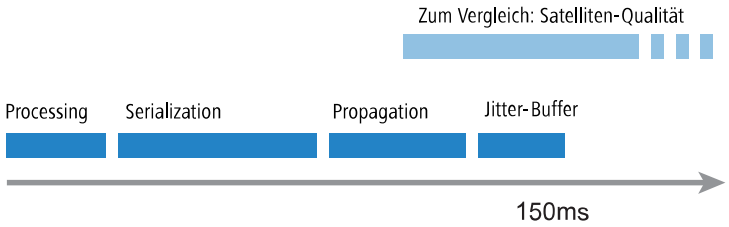
  Diese beiden Anteile ergeben zusammen die Verzögerung, die idealerweise nicht mehr als 150 ms betragen sollte.



- Der Paketverlust schließlich wird neben dem allgemeinen Verlust durch die Netzübertragung maßgeblich durch den Jitter-Buffer beeinflusst. Wenn Pakete mit einer größeren Verzögerung ankommen als durch den Jitter-Buffer ausgeglichen werden kann, werden die Pakete verworfen und erhöhen den Paketverlust. Je größer also der Jitter-Buffer, desto kleiner der Verlust. Umgekehrt steigt mit dem Jitter-Buffer auch die gesamte Verzögerung, so dass bei der

Konfiguration der Jitter-Buffer so klein gewählt werden sollte, dass die Qualität noch als ausreichend betrachtet werden kann.

Die Verzögerung wird im Detail vor allem durch den verwendeten Codec, die daraus resultierende Paketgröße und die verfügbare Bandbreite bestimmt:



- Die Zeit für die Verarbeitung wird durch den verwendeten Codec festgelegt. Bei einer Samplingzeit von 20 ms wird genau alle 20 ms ein neues Paket gebildet. Die Zeiten für die Komprimierung etc. können meistens vernachlässigt werden.
- Die Zeit für die Übergabe der Pakete an das Interface wird durch den Quotient aus Paketgröße und verfügbarer Bandbreite definiert:

	Paketgröße in Byte						
	1	64	128	256	512	1024	1500
56 Kbit/s	0,14	9	18	36	73	146	215
64 Kbit/s	0,13	8	16	32	64	128	187
128 Kbit/s	0,06	4	8	16	32	64	93
256 Kbit/s	0,03	2	4	8	16	32	47
512 Kbit/s	0,016	1	2	4	8	16	23
768 Kbit/s	0,010	0,6	1,3	2,6	5	11	16
1536 Kbit/s	0,005	0,3	0,6	1,3	3	5	8

- Ein 512 Byte großes Paket einer FTP-Verbindung belegt auf einer 128 Kbit/s-Upstream-Leitung also für mindestens 32 ms die Leitung.

  Die Pakete der VoIP-Verbindung selbst sind außerdem oft deutlich größer als die reine Nutzlast. Zu den Nutzdaten müssen die zusätzlichen IP-Header sowie ggf. die IPSec-Header addiert werden. Die Nutzlast ergibt sich aus dem Produkt von Nutzdatenrate und Samplingzeit des verwendeten Codecs. Dazu kommen für alle Codecs jeweils 40 Byte für IP-, RTP- und UDP-Header und mindestens 20 Byte für den IPSec-Header (RTP- und IPSec-Header können allerdings je nach Konfiguration auch größer sein).

ohne IPSec	Payload	IP-Payload	Ethernet / PPPoE	ATMNetto Bit/s	ATMBrutto Bit/s
Code	20 ms	20 ms	20 ms	20 ms	20 ms
G711-64	160	200	222	96000,0	106000,0
G722-64	160	200	222	96000,0	106000,0
G726-40	100	140	162	76800,0	84800,0
G726-32	80	120	142	76800,0	84800,0
G726-24	60	100	122	57600,0	63600,0
G726-16	40	80	102	57600,0	63600,0
G729-8	20	60	82	57600,0	63600,0

ohne IPSec	Payload	IP-Payload	Ethernet / PPPoE	ATMNetto Bit/s	ATMBrutto Bit/s
Code	30 ms	30 ms	30 ms	30 ms	30 ms
G711-64	240	280	302	89600,0	98933,3
G722-64	240	280	302	89600,0	98933,3
G726-40	150	190	212	64000,0	70666,7
G726-32	120	160	182	64000,0	70666,7
G726-24	90	130	152	51200,0	56533,3
G726-16	60	100	122	38400,0	42400,0
G729-8	30	70	92	38400,0	42400,0
G723-6,3	24	64	86	38400,0	42400,0

mit IPSec	Payload	IP-Payload	IPSec-Payload	Ethernet / PPPoE	ATMNetto Bit/s	ATMBrutto Bit/s
Code	20 ms	20 ms	20 ms	20 ms	20 ms	20 ms
G711-64	160	200	260	282	134400,0	148400,0
G722-64	160	200	260	282	134400,0	148400,0
G726-40	100	140	200	222	96000,0	106000,0
G726-32	80	120	180	202	96000,0	106000,0
G726-24	60	100	160	182	96000,0	106000,0
G726-16	40	80	140	162	76800,0	84800,0
G729-8	20	60	120	142	76800,0	84800,0

mit IPSec	Payload	IP-Payload	IPSec-Payload	Ethernet / PPPoE	ATMNetto Bit/s	ATMBrutto Bit/s
Code	30 ms	30 ms	30 ms	30 ms	30 ms	30 ms
G711-64	240	280	340	362	102400,0	113066,7
G722-64	240	280	340	362	102400,0	113066,7
G726-40	150	190	250	272	89600,0	98933,3
G726-32	120	160	220	242	76800,0	84800,0
G726-24	90	130	190	212	64000,0	70666,7
G726-16	60	100	160	182	64000,0	70666,7
G729-8	30	70	130	152	51200,0	56533,3
G723-6,3	24	64	124	146	51200,0	56533,3

- IP-Payload: Voice Payload + 40 Byte Header (12 Byte RTP; 8 Byte UDP; 20 Byte IP-Header)
- IPSec-Payload: IP-Paket + Padding + 2 Byte (Padding Length u. Next Header) = Vielfaches vom IPSec-Initialisierungsvektor

Die Werte in der Tabelle gelten für die Verwendung von AES. Bei anderen Verschlüsselungsverfahren kann sich die resultierende Paketgröße in geringem Umfang ändern.

Weitere Informationen über die Bandbreiten beim Zusammenspiel von Voice over IP und IPSec entnehmen Sie bitte dem LANCOM Techpaper „Performance-Analyse der Router".

- Die Zeit für die Übertragung über das Internet ist abhängig von der Entfernung (ca. 1 ms pro 200 km) und von den dabei passierten Routern (ca. 1 ms pro Hop). Diese Zeit kann als Hälfte des Mittelwertes einer Reihe von Ping-Zeiten auf die Gegenstelle angenähert werden.
- Der Jitter-Buffer kann an vielen IP-Telefonen direkt eingestellt werden, z. B. als feste Anzahl von Paketen, die für die Zwischenspeicherung verwendet werden sollen. Die Telefone laden dann bis zu 50% der eingestellten Pakete und beginnen dann mit der Wiedergabe. Der Jitter-Buffer entspricht damit der Hälfte der eingestellten Paketanzahl multipliziert mit der Samplingzeit des Codecs.
- Fazit: Die gesamte Verzögerung ergibt sich bei der entsprechenden Bandbreite, einer Ping-Zeit von 100 ms zur Gegenstelle und einem Jitter-Buffer von 4 Paketen für die beiden Codecs im Beispiel zu:

Codec	Processing	Serialization	Propagation	Jitter-Buffer	Summe
G.723.1	30 ms + 7,5 ms look ahead	32 ms	50 ms	60 ms	179,5 ms
G.711	20 ms	32 ms	50 ms	40 ms	142 ms

- Die Übertragungszeit der Pakete auf das Interface (Serialization) geht dabei von einer PMTU von 512 Byte für eine 128 Kbit-Verbindung aus. Für langsamere Interfaces oder andere Codecs müssen ggf. andere Jitter-Buffer und / oder PMTU-Werte eingestellt werden.

Bitte beachten Sie, dass die benötigten Bandbreiten jeweils in Sende- und Empfangsrichtung sowie für eine einzelne Verbindung gelten.

Diese Erläuterungen beziehen sich auf Internet-Verbindungen mit sehr geringer Bandbreite. Wenn eine hohe Bandbreite zur Verfügung steht, bewirkt die Verkleinerung der PMTU nur noch kaum wahrnehmbare Leistungsunterschiede.

9.6 QoS in Sende- oder Empfangsrichtung

Bei der Steuerung der Datenübertragung mit Hilfe der QoS kann man auswählen, ob die entsprechende Regel für die Sende- oder Empfangsrichtung gilt. Welche Richtung bei einer konkreten Datenübertragung jetzt aber Sende- und welche Empfangsrichtung ist, hängt vom Blickwinkel der Betrachtung ab. Es gibt dabei die beiden folgenden Varianten:

- Die Richtung entspricht dem logischen Verbindungsaufbau
- Die Richtung entspricht der physikalischen Datenübertragung über das jeweilige Interface

Die Betrachtung eines FTP-Transfers macht die Unterschiede deutlich. Ein Client im LAN ist über ein Gerät mit dem Internet verbunden.

- Bei einer aktiven FTP-Session sendet der Client dem Server über den PORT-Befehl die Informationen, auf welchem Port er die DATA-Verbindung erwartet. Der Server baut daraufhin die Verbindung zum Client auf und sendet in der gleichen Richtung die Daten. Hier gehen also sowohl die logische Verbindung als auch der tatsächliche Datenstrom über das Interface vom Server zum Client, das Gerät wertet beides als Empfangsrichtung.
- Anders sieht es aus bei einer passiven FTP-Session. Dabei baut der Client selbst die Verbindung zum Server auf. Der logische Verbindungsaufbau geht hierbei also vom Client in Richtung Server, die Datenübertragung über das physikalische Interface jedoch in umgekehrter Richtung vom Server zum Client.

In der Standardeinstellung bewertet ein Gerät die Sende- oder Empfangsrichtung anhand des logischen Verbindungsaufbaus. Weil diese Sichtweise in manchen Anwendungsszenarien nicht einfach zu durchschauen ist, kann der Blickwinkel alternativ auf die Betrachtung des physikalischen Datenstroms umgestellt werden.

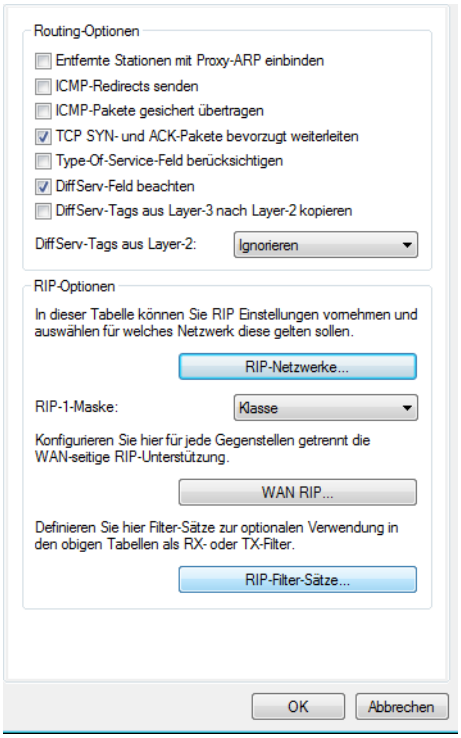
Die Unterscheidung von Sende- und Empfangsrichtung gilt nur für die Einrichtung von Maximalbandbreiten. Bei einer garantierten Mindestbandbreite sowie bei Fragmentierung und PMTU-Reduzierung gilt immer die physikalische Datenübertragung über das jeweilige Interface als Richtung!

9.7 QoS-Konfiguration

9.7.1 ToS- und DiffServ-Felder auswerten

9.7.1.1 ToS- oder DiffServ?

Wählen Sie bei der Konfiguration mit LANconfig den Konfigurationsbereich **IP-Router**. Auf der Registerkarte **Allgemein** wird eingestellt, ob das Type-of-Service-Feld oder alternativ das DiffServ-Feld bei der Priorisierung der Datenpakete berücksichtigt wird. Werden beide Optionen ausgeschaltet, wird das ToS / DiffServ-Feld ignoriert.



Bei der Konfiguration über die Konsole wird die Entscheidung für die Auswertung der ToS- oder DiffServ-Felder hier eingetragen: **Setup** > **IP-Router** > **Routing-Methode**

Die Einstellmöglichkeiten des Wertes Routing-Methode sind folgende:

Normal

Das ToS / DiffServ-Feld wird ignoriert.

TOS

Das ToS / DiffServ-Feld wird als ToS-Feld betrachtet, es werden die Bits „Low-Delay" und „High-Reliability" ausgewertet.

DiffServ

Das ToS / DiffServ-Feld wird als DiffServ-Feld betrachtet und wie folgt ausgewertet:

DSCP Codepoints	Übertragungsweise
CSx (inklusive CS0 = BE)	normal übertragen
AFxx	gesichert übertragen

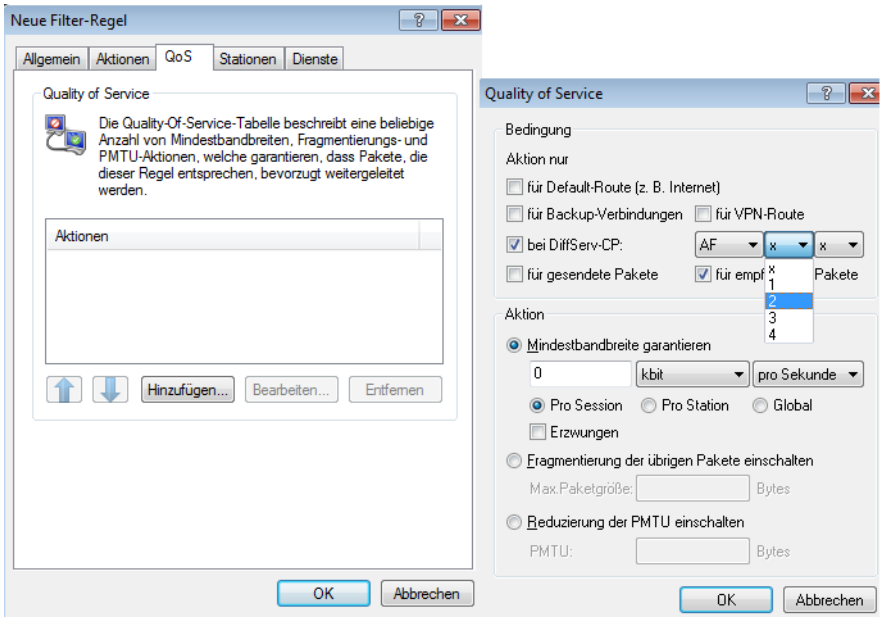
DSCP Codepoints	Übertragungsweise
EF	bevorzugt übertragen

Die DSCP-Markierung kann für einige interne LCOS-Anwendungen konfiguriert werden. Dies geht über die Konsole unter **Setup** > **Config** > **DCSP-Markierung**.

9.7.1.2 DiffServ in den Firewall-Regeln

In den Firewall-Regeln können die Code Points aus dem DiffServ-Feld ausgewertet werden, um weitere QoS-Parameter wie Mindestbandbreiten oder PMTU-Reduzierung zu steuern.

Die Parameter für die Auswertung der DiffServ-Felder werden im LANconfig beim Definieren der QoS-Regel festgelegt:



Je nach Auswahl des DSCP-Typs (BE, CS, AF, EF) können in zusätzlichen Drop-Down-Listen die gültigen Werte eingestellt werden. Alternativ kann auch der DSCP-Dezimalwert direkt eingetragen werden. Eine Tabelle mit den gültigen Werten findet sich unter *Was ist DiffServ?* auf Seite 697.

Bei der Konfiguration über die Konsole werden diese Parameter hier eingetragen: **Setup** > **IP-Router** > **Firewall** > **Regel-Liste**

Die Regel in der Firewall wird dabei um die Bedingung "@d" und den DSCP (Differentiated Services Code Point) erweitert. Der Code Point kann entweder über seinen Namen (CS0 - CS7, AF11 bis AF 43, EF oder BE) oder seine dezimale bzw. hexadezimale Darstellung angegeben werden. "Expedited Forwarding" kann somit als "@dEF", "@d46" oder "@d0x2e" angegeben werden. Desweiteren sind Sammelnamen (CSx bzw. AFxx) möglich.

Beispiele:

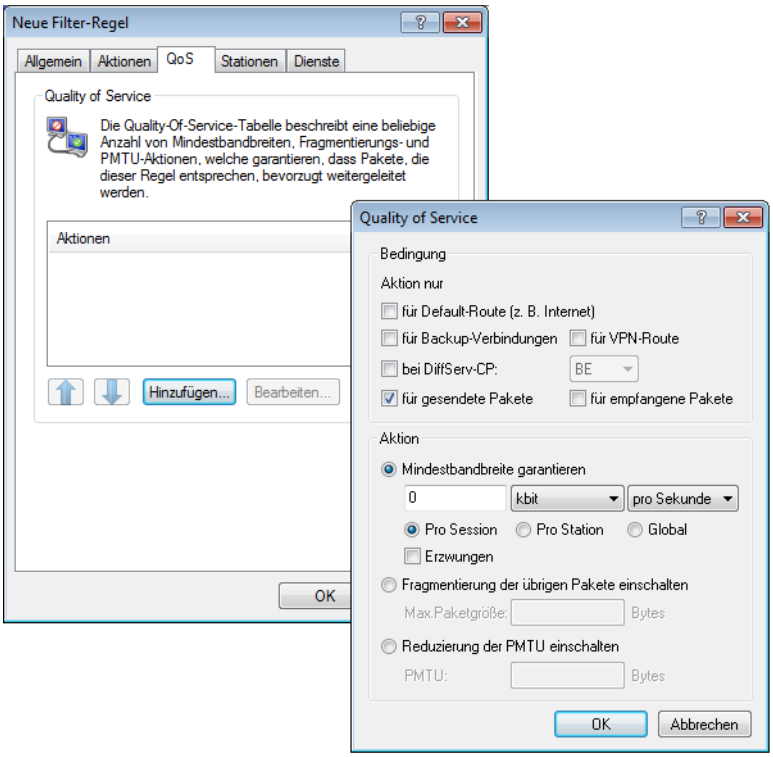
- **%Lcds0 @dAFxx %A**: Akzeptieren (gesichert Übertragen) bei DiffServ "AF", Limit "0"
- **%Qcds32 @dEF**: Mindestbandbreite für DiffServ EF von 32 kBit/s
- **%Fprw256 @dEF**: PMTU-Reduzierung beim Empfang für DiffServ EF auf 256 Bytes)

Mit den hier aufgeführten Beispielen kann man für Voice-over-IP-Telefonate die gewünschte Bandbreite freihalten. Der erste Baustein "%Lcds0 @dAFxx %A" akzeptiert die mit dem DSCP AFxx markierten Pakete zur Signalisierung eines Anrufs. Die mit EF gekennzeichneten Sprachdaten werden durch den Eintrag "%Qcds32 @dEF" priorisiert übertragen, dabei wird eine Bandbreite von 32 KBit/s garantiert. Parallel dazu wird mit "%Fprw256 @dEF" die PMTU auf 256 Byte festgelegt, was eine Sicherung der erforderlichen Bandbreite in Empfangsrichtung erst möglich macht.

9.7.2 Minimal- und Maximalbandbreiten definieren

Eine Mindestbandbreite für eine bestimmte Anwendung wird im LANconfig über eine Firewallregel nach den folgenden Randbedingungen definiert:

- Die Regel benötigt keine Aktion, da für die QoS-Regeln immer implizit das „Übertragen“ als Aktion vorausgesetzt wird.
- Auf der Registerkarte **QoS** wird die garantierte Bandbreite festgelegt.



- Mit der Option **Aktion nur für Default-Route** beschränkt man die Regel auf Pakete, die über die Defaultroute gesendet oder empfangen werden.
  - Mit der Option **Aktion nur für VPN-Route** beschränkt man die Regel auf Pakete, die über einen VPN-Tunnel gesendet oder empfangen werden.
  - Mit der Option **Erzwungen** wird eine statische Bandbreitenreservierung definiert. Die so reservierte Bandbreite bleibt für alle anderen Verbindungen auch dann gesperrt, wenn die bevorzugte Verbindung die Bandbreite zur Zeit nicht in Anspruch nimmt.
  - Mit der Option **Pro Verbindung** bzw. **Global** wird festgelegt, ob die hier eingestellte Mindestbandbreite für jede einzelne Verbindung gilt, die dieser Regel entspricht (Pro Verbindung), oder ob es sich dabei um die Obergrenze für die Summe aller Verbindungen gemeinsam handelt (Global).
- Auf den Registerkarten **Stationen** und **Dienste** wird wie bei anderen Firewallregeln vereinbart, für welche Stationen im LAN / WAN und für welche Protokolle diese Regel gilt.

Bei der Konfiguration über die Konsole werden die Minimal- bzw. Maximalbandbreiten in eine neue Firewallregel hier eingetragen: **Setup** > **IP-Router** > **Firewall** > **Regel-Liste**

Eine geforderte Mindestbandbreite wird in den Regeln mit dem Bezeichner “%Q” eingeleitet. Dabei wird implizit angenommen, dass es sich bei der entsprechenden Regel um eine „Accept“-Aktion handelt, die Pakete also übertragen werden.

Für eine Maximalbandbreite wird eine einfache Limit-Regel definiert, die mit einer „Drop“-Aktion alle Pakete verwirft, die über die eingestellte Bandbreite hinausgehen.

Beispiele:

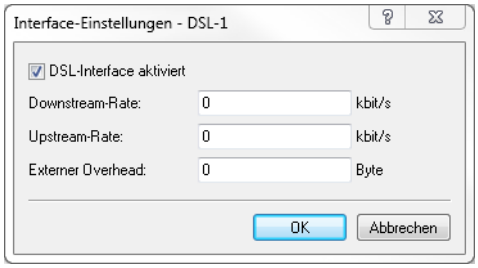
- **%Qcds32**: Mindestbandbreite von 32 kBit/s für jede Verbindung
- **%Lgds256 %d**: Maximalbandbreite von 256 kBit/s für alle Verbindungen (global)

9.7.3 Übertragungsraten für Schnittstellen festlegen

Die Beschränkungen der Datenübertragungsrate für Ethernet-, DSL und DSLoL-Schnittstellen werden in LANconfig unter **Schnittstellen** > **WAN** über die Schaltfläche **Interface-Einstellungen** festgelegt.

Die Werte für die Upstream-Rate und die Downstream-Rate werden in kbit/s angegeben, die Werte für den externen Overhead in Bytes/Paket.

Ethernet-, DSL und DSLoL-Schnittstellen



- Ein DSL-Interface kann in diesem Dialog vollständig ausgeschaltet werden.
- Als Upstream- und Downstream-Rate werden hier die Bruttodatenraten angegeben, die üblicherweise etwas über den Nettodatenraten liegen, die der Provider als garantierte Datenrate angibt (siehe auch *Das Warteschlangenkonzept* auf Seite 699).
- Der „externe Overhead" berücksichtigt Informationen, die bei der Datenübertragung den Paketen zusätzlich angehängt werden. Bei Anwendungen mit eher kleinen Datenpaketen (z. B. Voice-over-IP) macht sich dieser Extra-Overhead durchaus bemerkbar. Beispiele für den externen Overhead:

Übertragung	externer Overhead	Bemerkung
T-DSL	36 Bytes	zusätzliche Header, Verluste durch nicht vollständig genutzte ATM-Zellen
PPTP	24 Bytes	zusätzliche Header, Verluste durch nicht vollständig genutzte ATM-Zellen
IPoA (LLC)	22 Bytes	zusätzliche Header, Verluste durch nicht vollständig genutzte ATM-Zellen
IPoA (VC-MUX)	18 Bytes	zusätzliche Header, Verluste durch nicht vollständig genutzte ATM-Zellen
Kabelmodem	0	direkte Übertragung von Ethernet-Paketen

Über die Konsole können die Beschränkungen der Datenübertragungsrate für Ethernet-, DSL und DSLoL-Interfaces an folgender Stelle eingetragen werden: **Setup** > **Schnittstellen** > **DSL-Schnittstellen**

VDSL- und ADSL-Schnittstellen

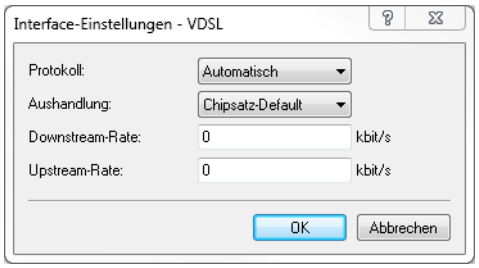
Für die ordnungsgemäße Funktion von Quality of Service ist es erforderlich, dass die tatsächliche Bandbreite der WAN-Verbindung bekannt ist. Es kann vorkommen, dass die vom DSL-Modem ausgehandelte Bandbreite nicht mit der tatsächlichen Datenübertragungsrate übereinstimmt. In diesem Fall ist es erforderlich, die Geschwindigkeit der DSL-Verbindung manuell auf den tatsächlichen Wert zu korrigieren.

Gilt nur für Geräte mit integriertem ADSL- / VDSL-Modem.

Beispiel:

Die ausgehandelte Bandbreite der DSL-Synchronisierung ergibt 100 MBit/s. Tatsächlich steht nur eine Übertragungsgeschwindigkeit von 50 MBit/s zur Verfügung.

Einstellungen für Geräte mit integriertem VDSL-Modem



Protokoll

Wählen Sie das Protokoll aus, welches an Ihrem DSL-Anschluss verwendet wird. Informationen dazu erhalten Sie bei Ihrem Internet-Provider.

Folgende Optionen stehen zur Auswahl:

Automatisch

Automatische Auswahl des Betriebsmodus.

VDSL2 (G.993.2)

Betriebsmodus VDSL2 für Übertragungsraten für bis zu 100 MBit/s im Up- und Downstream.

ADSL

Betriebsmodus ADSL mit bis zu 8 MBit/s Downstream und 0,6 MBit/s Upstream.

ADSL2+ (G.992.5)

Betriebsmodus ADSL2+ mit bis zu 24 MBit/s Downstream und 1 MBit/s Upstream.

ADSL2 (G.992.3)

Betriebsmodus ADSL2 mit bis zu 12 MBit/s Downstream und 1,2 MBit/s Upstream.

ADSL1 (G.992.1/G.DMT)

Betriebsmodus ADSL (G.DMT) mit bis zu 8 MBit/s Downstream und 1 MBit/s Upstream.

ADSL2+ (Annex J)

Betriebsmodus All Digital ADSL2+ mit bis zu 24 MBit/s Downstream und 3,5 MBit/s Upstream.

ADSL2 (Annex J)

Betriebsmodus All Digital Mode ADSL2 mit bis zu 12 MBit/s Downstream und 3,5 MBit/s Upstream.

Aus

Die Schnittstelle ist nicht aktiv.

Aushandlung

Wählen Sie für diese Schnittstelle zwischen folgenden Aushandlungsmethoden aus:

Chipsatz-Default

Die Aushandlung erfolgt nach dem Standard des jeweiligen Geräte-Chipsatzes.

V43 wenn benötigt

Zur Aushandlung wird, falls erforderlich, der Trägersatz V43 verwendet.

V43 aktiviert

Für die Aushandlung wird der Trägersatz V43 aktiviert.

V43 deaktiviert

Für die Aushandlung wird der Trägersatz V43 deaktiviert.

Downstream-Rate

Geben Sie die Downstream-Rate (RX) an. Die tatsächliche Bandbreite entspricht dem Minimum des ausgehandelten und des hier gesetzten Wertes.

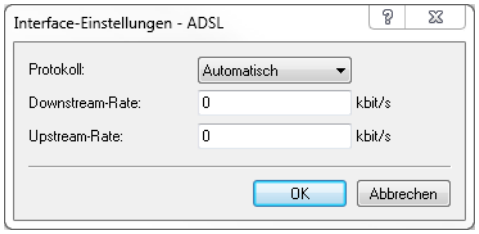
Beim Defaultwert 0 wird der automatisch ausgehandelte Wert verwendet.

Upstream-Rate

Geben Sie die Upstream-Rate (TX) an. Die tatsächliche Bandbreite entspricht dem Minimum des ausgehandelten und des hier gesetzten Wertes.

Beim Defaultwert 0 wird der automatisch ausgehandelte Wert verwendet.

Einstellungen für Geräte mit integriertem ADSL-Modem



Protokoll

Wählen Sie das Protokoll aus, welches an Ihrem DSL-Anschluss verwendet wird. Informationen dazu erhalten Sie bei Ihrem Internet-Provider.

Folgende Optionen stehen zur Auswahl:

Automatisch

Automatische Auswahl des Betriebsmodus.

ADSL1 (autom. Annex A/B)

Betriebsmodus ADSL over POTS / ISDN für Übertragungsraten für bis zu 10 MBit/s Downstream und 1 MBit/s Upstream.

ADSL2 (autom. Annex A/B)

Betriebsmodus ADSL2 over POTS / ISDN für Übertragungsraten für bis zu 12 MBit/s Downstream und 1 MBit/s Upstream.

ADSL2+ (autom. Annex A/B)

Betriebsmodus ADSL2+ over POTS / ISDN für Übertragungsraten für bis zu 24 MBit/s Downstream und 1 MBit/s Upstream.

Auto-POTS (autom. Annex A/I/L/M)

Betriebsmodus ADSL over POTS für Übertragungsraten von 10 bis zu 24 MBit/s Downstream und bis zu 3,5 MBit/s Upstream.

ADSL1 (Annex A)

Betriebsmodus ADSL over POTS für Übertragungsraten bis zu 10 MBit/s Downstream und 1 MBit/s Upstream.

ADSL2 (Annex A)

Betriebsmodus ADSL2 over POTS mit bis zu 12 MBit/s Downstream und 1 MBit/s Upstream.

ADSL2+ (Annex A)

Betriebsmodus ADSL2+ over POTS mit bis zu 24 MBit/s Downstream und 1 MBit/s Upstream.

ADSL2 (Annex I)

Betriebsmodus All Digital Mode ADSL2 mit bis zu 12 MBit/s Downstream und 3,2 MBit/s Upstream.

ADSL2+ (Annex I)

Betriebsmodus All Digital ADSL2+ mit bis zu 24 MBit/s Downstream und 3,2 MBit/s Upstream.

ADSL2 (Annex L)

Betriebsmodus RE-ADSL2 mit bis zu 6 MBit/s Downstream und 1,2 MBit/s Upstream.

ADSL2 (Annex M)

Betriebsmodus ADSL2 mit bis zu 24 MBit/s Downstream und 3,5 MBit/s Upstream.

ADSL2+ (Annex M)

Betriebsmodus ADSL2+ mit bis zu 24 MBit/s Downstream und 3,7 MBit/s Upstream.

Auto-ISDN (autom. Annex B/J)

Betriebsmodus ADSL over ISDN für Übertragungsraten von 10 bis zu 24 MBit/s Downstream und bis zu 3,5 MBit/s Upstream.

ADSL1 (Annex B)

Betriebsmodus ADSL over ISDN für Übertragungsraten bis zu 10 MBit/s Downstream und 1 MBit/s Upstream.

ADSL2 (Annex B)

Betriebsmodus ADSL over ISDN für Übertragungsraten bis zu 12 MBit/s Downstream und 1 MBit/s Upstream.

ADSL2+ (Annex B)

Betriebsmodus ADSL over ISDN für Übertragungsraten bis zu 24 MBit/s Downstream und 1 MBit/s Upstream.

ADSL2 (Annex J)

Betriebsmodus ADSL over ISDN für Übertragungsraten bis zu 12 MBit/s Downstream und 3,5 MBit/s Upstream.

ADSL2+ (Annex J)

Betriebsmodus ADSL over ISDN für Übertragungsraten bis zu 24 MBit/s Downstream und 3,5 MBit/s Upstream.

Aus

Die Schnittstelle ist nicht aktiv.

Downstream-Rate

Geben Sie die Downstream-Rate (RX) an. Die tatsächliche Bandbreite entspricht dem Minimum des ausgehandelten und des hier gesetzten Wertes.

Beim Defaultwert 0 wird der automatisch ausgehandelte Wert verwendet.

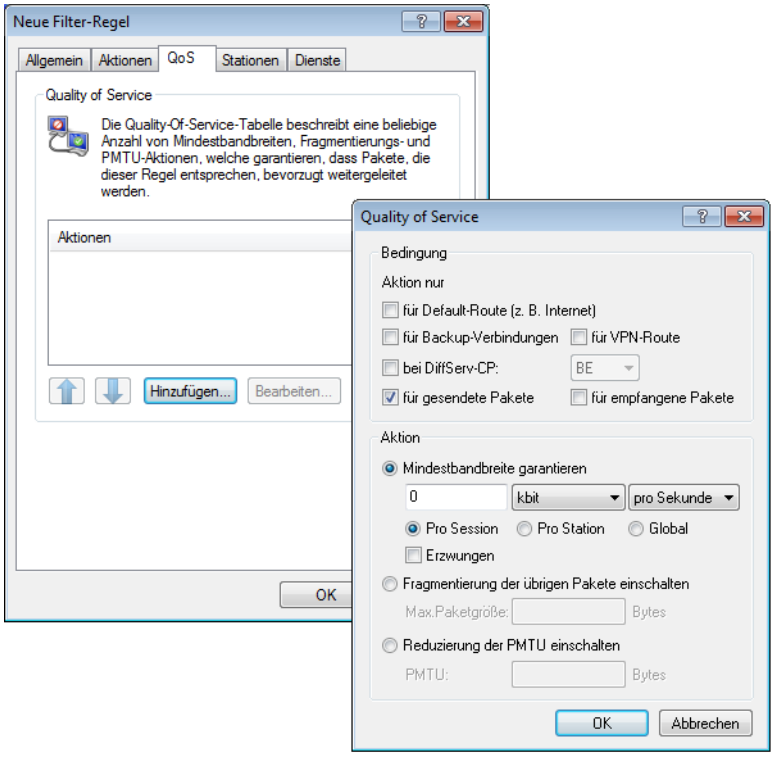
Upstream-Rate

Geben Sie die Upstream-Rate (TX) an. Die tatsächliche Bandbreite entspricht dem Minimum des ausgehandelten und des hier gesetzten Wertes.

Beim Defaultwert 0 wird der automatisch ausgehandelte Wert verwendet.

9.7.4 Sende- und Empfangsrichtung

Die Bedeutung der Datenübertragungsrichtung wird im LANconfig beim Definieren der QoS-Regel festgelegt:



Bei der Konfiguration über die Konsole wird die Bedeutung der Datenübertragungsrichtung über die Parameter "R" für receive (Empfangen), "T" für transmit (Senden) und "W" für den Bezug zum WAN-Interface an folgenden Stellen in eine neue Regel der Firewall eingetragen: **Setup** > **IP-Router** > **Firewall** > **Regel-Liste**

Die Beschränkung der Datenübertragung auf 16 KBit/s in Senderichtung bezogen auf das physikalische WAN-Interface wird also z. B. durch die folgende Regel in der Firewall erreicht:

- %Lcdstw16%d

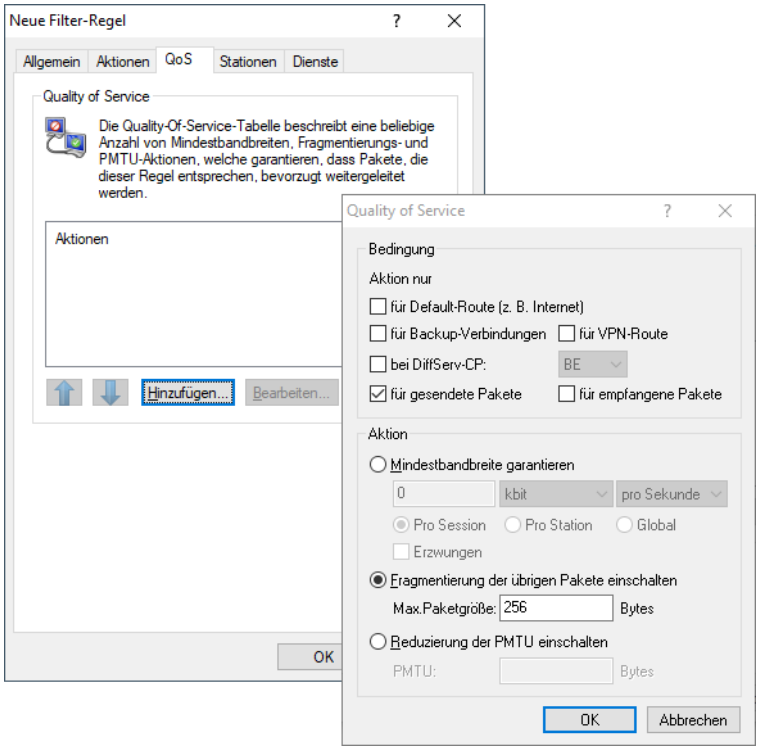
9.7.5 Reduzierung der Paketlänge

Die Längenreduzierung der Datenpakete wird definiert über eine Regel in der Firewall nach den folgenden Randbedingungen:

- Die Reduzierung bezieht sich auf **alle** Pakete, die auf das Interface gesendet werden und **nicht** der Regel entsprechen.
- Es werden nicht bestimmte Protokolle reduziert, sondern global alle Pakete auf dem Interface.

Bei Geräten mit integrierter oder nachträglich über Software-Option freigeschalteter VoIP-Funktion können Fragmentierung und PMTU-Reduzierung separat für SIP-Gespräche eingestellt werden!

Die Längenreduzierung der Datenpakete wird im LANconfig beim Definieren der QoS-Regel festgelegt:



Bei der Konfiguration über die Konsole wird die Reduzierung über die Parameter "P" für die Reduzierung der PMTU (Path MTU, MTU = Maximum Transmission Unit) und "F" für die Größe der Fragmente an folgender Stelle in eine neue Firewallregel eingetragen: **Setup** > **IP-Router** > **Firewall** > **Regel-Liste**

PMTU-Reduzierung und Fragmentierung beziehen sich immer auf die physikalische Verbindung. Die Angabe des Parameters "W" für die WAN-Senderichtung ist also hier nicht erforderlich und wird ignoriert, falls vorhanden.

Das folgende Beispiel zeigt eine Einstellung für Voice-over-IP-Telefonie:

Regel	Quelle	Ziel	Aktion	Protokoll
VOIP	IP-Adressen der IP-Telefone im LAN, alle Ports	IP-Adressen der IP-Telefone im LAN, alle Ports	%Qcds32 %Fpt256	UDP

Diese Regel setzt die Mindestbandbreite für Senden und Empfang auf 32 KBit/s, erzwingt und verringert die PMTU beim Senden auf 256 Byte große Pakete. Für die TCP-Verbindungen wird die Maximum Segment Size des lokalen Rechners auf 216 gesetzt, damit der Server maximal 256 Bytes große Pakete sendet (Verringerung der PMTU in Senderichtung).

9.8 Quality-of-Service (QoS) mit 8 Queues

Im Folgenden soll konzeptionell die Funktionsweise des Quality-of-Service mit acht Queues erklärt werden. Grundlegend sollen Pakete vom Router auf Basis des DSCP-Wertes im IP-Header priorisiert werden können. Hierfür stehen insgesamt acht **Queues** zur Verfügung, die strikt priorisiert werden. Das bedeutet, dass Pakete nach Verfügbarkeit von der **Queue** mit der höchsten Priorität bis zur **Queue** mit der niedrigsten Priorität versendet werden. Die Zuordnung eines Paketes zu einer **Queue** geschieht auf Basis des DSCP-Werts im IP-Header oder der Zuweisung zu einer Queue über eine Firewall-Regel. Von den acht zur Verfügung stehenden **Queues** sind zwei reserviert, einmal für die **Urgent-Queue** (höchste Priorität, für interne Dienste wie VCM und Protokollpakete) und zum anderen für die **Best-Effort-Queue** (niedrigste Priorität, für alle nicht-priorisierten Pakete). Die verbleibenden sechs **Queues** stehen dem Nutzer zur freien

Verfügung. Um die Prioritätsstufen der einzelnen **Queues** festzulegen werden sie in eine **Queue-List** nach absteigender Priorität verkettet. Die interne **Urgent-Queue** und **Best-Effort-Queue** werden an diese **Queue-List** vorne und hinten eingefügt. Die fertige **Queue-List** muss dann einem physischen **WAN-Interface** zugeordnet werden. Danach werden Pakete, die dieses **WAN-Interface** zum Ziel haben, auf Basis der konfigurierten **Queues** priorisiert.

QoS basiert darauf, dass die Bandbreiten bzw. Raten einer Schnittstelle bekannt sind, damit das QoS die korrekte Verteilung übernehmen kann, z. B. in dem Fall, dass prozentual Bandbreiten zugewiesen werden. Die Bandbreiten werden in der Regel aus der Upstream- bzw. Downstream-Datenrate aus den internen DSL-Modems übernommen oder aus der übermittelten Bandbreite im PPP durch den Provider.

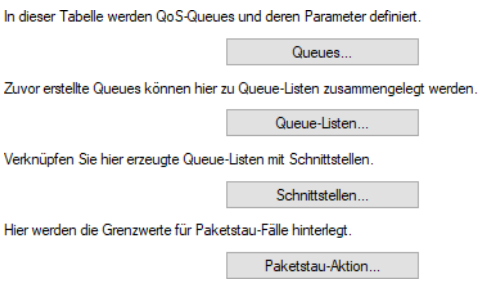
Bei WAN-Verbindungen über externe Modems oder reine Ethernet-Verbindungen müssen die tatsächlichen Bandbreiten in der Tabelle **Schnittstellen** > **WAN** > **Interface-Einstellungen** bei **Downstream-Rate** sowie **Upstream-Rate** für das entsprechende Interface eingetragen werden.



Bitte beachten Sie, dass bestimmte eigene Pakete automatisch vom LCOS in die Urgent-Queue sortiert werden. Dazu zählen wichtige Verhandlungspakete wie IKEv2, BGP oder Keepalive-Pakete.

Darüber hinaus werden weitergeleitete TCP SYN- und ACK-Pakete bevorzugt behandelt und ebenfalls in die Urgent-Queue einsortiert. Das Verhalten kann konfiguriert werden unter **IP-Router** > **Allgemein** > **Routing-Optionen** > **TCP SYN- und ACK-Pakete bevorzugt weiterleiten**.

Die Konfiguration dieser **Queues** erfolgt in LANconfig unter **Firewall/QoS** > **QoS**.

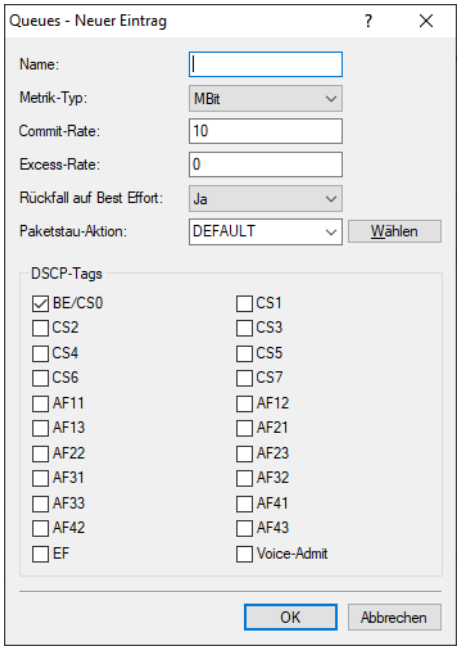


9.8.1 Queues

In dieser Tabelle werden **Queue-Vorlagen** konfiguriert. Das bedeutet, dass nicht jeder Eintrag in dieser Tabelle auch eine Queue erzeugt. Eine **Queue** wird erst dann erzeugt, wenn sie in einer **Queue-List** verwendet und diese einem **WAN-Interface** zugeordnet wurde. Das bedeutet, dass auf Basis einer hier erstellten Vorlage beliebig viele oder auch keine **Queues** erzeugt werden können.

Beispiel: Wenn in diese Tabelle ein Eintrag mit Namen „Test“ angelegt wird und dieser Eintrag dann in zwei **Queue-List**-Objekten genutzt und diese zwei verschiedenen **WAN-Interfaces** zugeordnet werden, dann gibt es zwei **Queues** mit Namen „Test“, die aber voneinander völlig unabhängig sind.

Die Konfiguration der Queues und deren Parameter erfolgt in LANconfig unter **Firewall/QoS** > **QoS** > **Queues**.



Name

Hier wird der Name der **Queue-Vorlage** eingetragen. Die Vorlage wird mit diesem Namen in anderen Tabellen referenziert. Der Name muss innerhalb der Tabelle eindeutig sein.

Metrik-Typ

Hier wird die Metrik der Spalten **Commit-Rate** und **Excess-Rate** festgelegt.

Commit-Rate

Hier wird eingetragen, wieviel Bandbreite dieser **Queue** zur Verfügung steht. Der Wert wird allgemein auch als CIR (Committed Information Rate) bezeichnet. Die Einheit der Eingabe wird in der Spalte **Metrik-Typ** festgelegt. Es gelten folgende Wertebereiche:

- *Prozent:* 1 < x < 100
- *KBit:* 1 < x < 4294967295
- *MBit:* 1 < x < 4294967295

Excess-Rate

Hier wird eingetragen, wieivel Bandbreite die **Queue** zusätzlich zu ihrer **Commit-Rate** nutzen darf. Der Wert wird allgemein auch als EIR (Excess Information Rate) bezeichnet. Damit höher priorisierte **Queues** sich nicht die **Commit-Rate** der niedriger priorisierten **Queues** nehmen können, wurde folgendes Konzept verwendet:

Das QoS operiert in Zeitscheiben, in denen jede **Queue** ihre **Commit-Rate** zur Verfügung hat. Am Ende der Zeitscheibe wird die nicht genutzte **Commit-Rate** aller **Queues** bestimmt und als Pool für die **Excess-Rate** in die nächste Zeitscheibe mitgenommen. Dieser Pool limitiert dann, wie ivel Bandbreite mit der **Excess-Rate** genutzt werden darf. Damit sind zwei wichtige Punkte erfüllt, nämlich erstens wird die **Excess-Rate** einer Queue nicht von der aktuellen **Commit-Rate** einer anderen Queue genommen, sondern von der ungenutzten Rate der letzten Zeitscheibe. Zweitens wird der Pool für die **Excess-Rate** am Anfang jeder Zeitscheibe neu gesetzt und nicht aufaddiert, womit die ungenutzte **Commit-Rate** einer Zeitscheibe nur in der darauf folgenden Zeitscheibe genutzt werden kann. Damit wird ein Ansparen verhindert, was dafür sorgen könnte, dass **Queues** mit konfigurierter Excess-Rate die niedriger priorisierten Queues aushungern lassen.

Beispiel: Es werden zwei **Queues** konfiguriert, in eine **Queue-List** verkettet und einem **WAN-Interface** zugewiesen. **Queue A** hat eine **Commit-Rate** von 10 MBit/s und eine **Excess-Rate** von 4 MBit/s. **Queue B**

hat eine **Commit-Rate** von 5 MBit/s und eine **Excess-Rate** von 0. Wenn jetzt in Zeitscheibe 1 **Queue A** 9 MBit/s und **Queue B** 4 MBit/s nutzt, dann werden 2 MBit/s als ungenutzte Rate in den Pool der **Excess-Rate** für die Zeitscheibe 2 mitgenommen. In dieser Zeitscheibe könnte **Queue A** dann seine 10 MBit/s **Commit-Rate** und zusätzlich 2 MBit/s aus dem Pool im Rahmen seiner **Excess-Rate** nutzen. Wichtig ist, dass nur soviel **Excess-Rate** genutzt werden kann wie der Pool zur Verfügung stellt.

Die Einheit der Eingabe wird in der Spalte **Metrik-Typ** festgelegt. Es gelten folgende Wertebereiche:

- *Prozent:* 0 < x < 100
- *KBit:* 0 < x < 4294967295
- *MBit:* 0 < x < 4294967295

Rückfall auf Best Effort

Dieser Schalter bestimmt, was mit Paketen passiert, die weder im Rahmen der Commit-Rate noch Excess-Rate versendet werden können. Bei **Ja** werden die Pakete über die Best-Effort-Queue versendet, sonst verworfen.

Paketstau-Aktion

Hier wird ein Objekt aus der Tabelle *Paketstau-Aktion* auf Seite 719 referenziert, welches bestimmt wann Pakete wegen voller werdender Sendequeues verworfen werden.

DSCP-Tags

Hier wedern die DSCP-Tags (Differentiated Services Code Point) eingetragen, die dieser Queue zugeordnet werden sollen. Es können mehrere Werte übergeben werden.

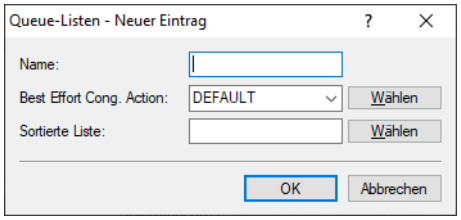
9.8.2 Queue-Listen

Die konfigurierten **Queue-Vorlagen** werden hier zu einer **Queue-Liste** verkettet. Dafür wird eine komma-separierte Liste verwendet, wobei die Reihenfolge die Priorisierung vorgibt, von hoch nach niedrig.

Es ist bei der Erstellung einer **Queue-Liste** darauf zu achten, dass die **Commit-Raten** der **Queues** die Bandbreite des **WAN-Interfaces** nicht überbuchen. Ansonsten kann es zu einem Aushungern der niedrig priorisierten **Queues** kommen.

Es ist außerdem darauf zu achten, dass **DSCP-Tags** nicht mehrfach zugewiesen werden. Sollte das passieren, wird implementierungsbedingt der niedrigst priorisierten **Queue** das Tag zugeordnet.

Zuvor erstellte Queues können in LANconfig unter **Firewall/QoS** > **QoS** > **Queue-Listen** zusammengelegt werden.



Name

Mit diesem Namen wird die **Queue-Liste** in anderen Tabellen referenziert. Er muss innerhalb der Tabelle eindeutig sein.

Best Effort Cong. Action

Hier kann eine **Paketstau-Aktion** aus der Paketstau-Aktion-Tabelle referenziert werden, um der **Best-Effort-Queue** eine **Paketstau-Aktion** zuzuweisen. Im Default wird der DEFAULT-Eintrag genutzt.

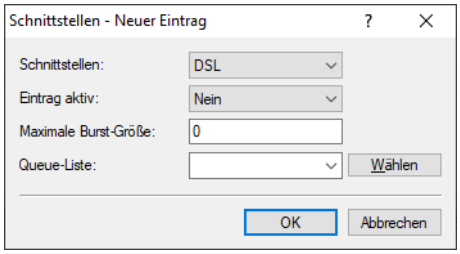
Sortierte Liste

Hier wird eine komma-separierte Liste aus **Queue-Vorlagen** eingetragen, deren Priorisierung sich aus der Reihenfolge von hoch nach niedrig ergibt. Es können bis zu sechs eigene **Queue-Vorlagen** verkettet werden, da zwei Plätze für die interne **Urgent-Queue** und **Best-Effort-Queue** reserviert sind.

Beispiel für eine Liste: Gold, Silber, Bronze. Die Priorität der Queues beginnt mit Gold über Silber bis zu Bronze.

9.8.3 Schnittstellen

In LANconfig unter **Firewall/QoS** > **QoS** > **Schnittstellen** verknüpfen Sie Queue-Listen mit Schnittstellen.



Schnittstellen

Hier wird der Name der physischen **WAN-Schnittstelle** eingetragen. Die Eingabe ist auf ein Inputset der auf dem Gerät verfügbaren **WAN-Schnittstellen** begrenzt.

Eintrag aktiv

Hier wird das konfigurierte QoS auf der **WAN-Schnittstelle** ein- und ausgeschaltet.

Maximale Burst-Größe

Die Maximum Burst Size (MBS) reguliert die Anzahl der Bytes, die in einem kurzen Zeitraum (Burst) gesendet werden können. Dieser Parameter gewährleistet, dass ein massiv oder kontinuierlich überbuchter Datenverkehr die verfügbaren Pufferressourcen, z. B. auf vorgeschalteten Provider-Routern, nicht vollständig ausschöpft. Der Defaultwert 0 bedeutet, dass das Betriebssystem den Parameter intern automatisch verwaltet. In der Regel entspricht der Wert intern der MTU der verwendeten WAN-Verbindung. Der Wert sollte auf die Vorgaben des Providers für den gebuchten Anschluss gesetzt werden.

Queue-Liste

Referenziert einen Eintrag aus der Queue-Listen-Tabelle.

9.8.4 Paketstau-Aktion

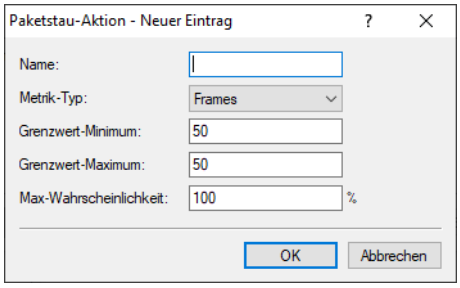
Die Paketstau-Aktion bestimmt, wie mit einer sich anstauenden Sendequeue umgegangen wird. Da diese Queue nicht unbegrenzt lang werden kann, müssen ab einem Punkt Pakete verworfen werden. Dafür stehen zwei Mechanismen zur Verfügung: **Taildrop** und **Random Early Detection (RED)** oder auch als **Random Early Discard** bezeichnet. Bei Taildrop wird eine Grenze bestimmt, ab der alle weiteren eingehenden Pakete verworfen werden. Bei RED werden zwei Grenzen bestimmt. Ab der ersten werden Pakte mit einer Wahrscheinlichkeit P verworfen. P steigt dabei an, je näher man an die zweite Grenze kommt. Wenn die zweite Grenze überschritten wird, werden alle eingehenden Pakete verworfen, wie beim Taildrop.

Die Tabelle **Paketstau-Aktion** ist so definiert, dass darin sowohl **RED** als auch **Taildrop** passiv konfiguriert werden kann. Ein **Taildrop** wird daran erkannt, dass der **Grenzwert-Minimum** gleich **Grenzwert-Maximum** ist. **Max-Wahrscheinlichkeit** erfüllt bei einem **Taildrop** keinen Zweck, sollte aber mit 100 eingetragen werden, um zu definieren, dass oberhalb der Grenze alles verworfen wird.

Man gibt nur den **Metrik-Typ** und **Grenzwert-Minimum** an, die weiteren Werte werden passend so gesetzt, dass ein **Taildrop** konfiguriert wird.

Für ein **RED** ist **Grenzwert-Minimum** ungleich **Grenzwert-Maximum**. Ab **Grenzwert-Minimum** wird beginnend mit Wahrscheinlichkeit P=0 das Paket verworfen, wobei sich P linear **Max-Wahrscheinlichkeit** annähert, je weiter man sich **Grenzwert-Max** annähert.

In LANconfig werden die Grenzwerte für Paketstau-Fälle unter **Firewall/QoS** > **QoS** > **Paketstau-Aktion** hinterlegt.



Name

Hier wird der Name der **Paketstau-Aktion** eingetragen, mit dem der Eintrag in anderen Tabellen referenziert wird. Der Name muss eindeutig innerhalb dieser Tabelle sein.

Metrik-Typ

Hier wird angegeben, welche Metrik die Werte in den Spalten **Commit-Rate** und **Excess-Rate** haben.

Grenzwert-Minimum

Gibt die untere Grenze der **Paketstau-Aktion** an.

Grenzwert-Maximum

Gibt die obere Grenze der **Paketstau-Aktion** an. Ab hier werden alle Pakete verworfen.

Max.-Wahrscheinlichkeit

Gibt die maximale Drop-Wahrscheinlichkeit bei einem konfigurierten **RED** an. Wird bei einem **Taildrop** ignoriert und sollte dort auf 100 gesetzt werden.

9.8.5 Beispiel 1: Konfiguration eines QoS-Konzepts mit vier Klassen

Im folgenden Beispiel soll ein Router für einen Kunden bereitgestellt werden, der dem Kunden am Anschluss ein QoS-Konzept mit vier QoS-Klassen ermöglicht. Die Klassen sind definiert als VoIP, Gold, Silber und Best Effort.

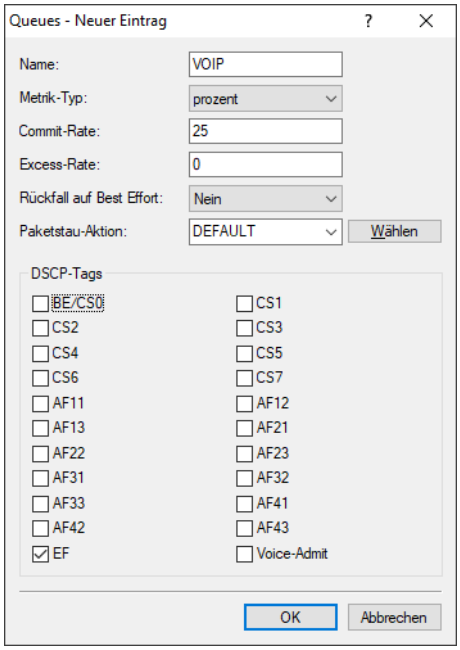
Jeder Serviceklasse wird 25% der Bandbreite zugeteilt. Der Kunde markiert seine Pakete per DSCP, so dass die Pakete der korrekten Queue im Router zugewiesen werden können.

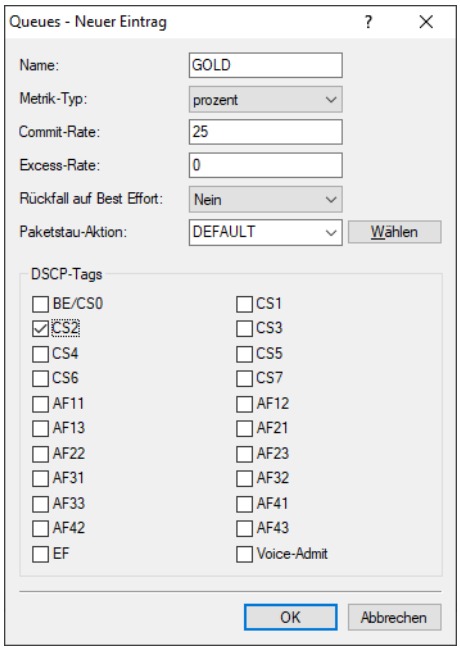
Werden in der definierten Serviceklasse mehr Daten übertragen als Bandbreite vorhanden ist, so werden diese Daten verworfen. Ein Rückfall in die Serviceklasse Best Effort wird nicht erlaubt. Die Definition ist wie folgt:

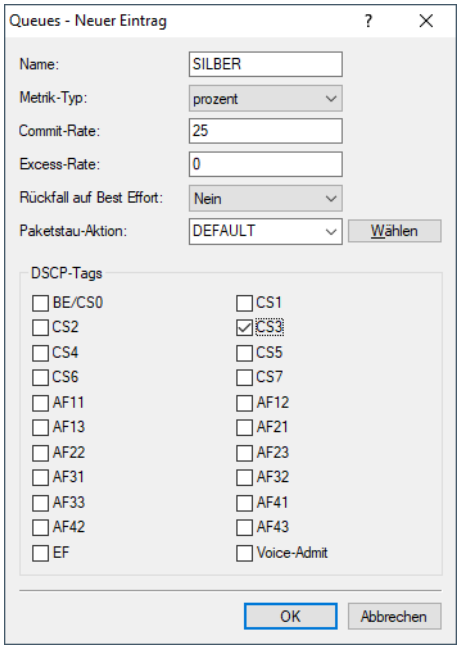
Klasse	DSCP
VOIP	EF
Gold	CS3
Silber	CS2
Best Effort	0

1. Starten Sie LANconfig und öffnen Sie den Konfigurationsdialog für das Gerät.

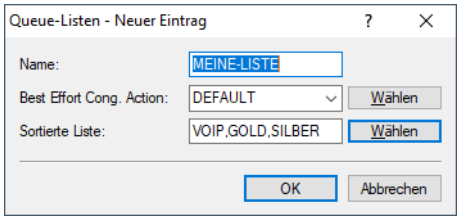
2. Wechseln Sie in den Dialog **Firewall/QoS** > **QoS** > **Queues**.
3. Legen Sie die drei Vorlagen für die Serviceklassen VOIP, GOLD und SILBER an. Die Klasse Best Effort muss nicht manuell konfiguriert werden, da diese automatisch vorhanden ist.



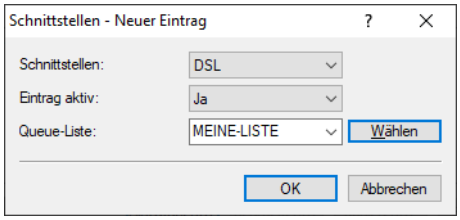




4. Wechseln Sie in den Dialog **Firewall/QoS** > **QoS** > **Queue-Listen**.
5. Legen Sie eine Liste an, mit der Sie eine strikte Reihenfolge für die angelegten Klassen vorgeben. Die erste Klasse in der Liste hat die höchste Priorität.

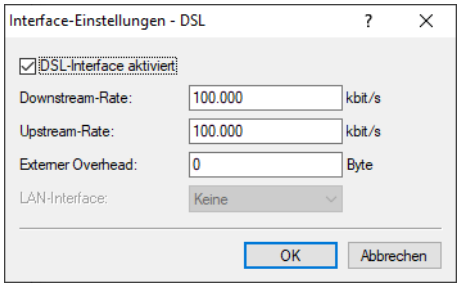


6. Als letztes muss die konfigurierte Liste einer WAN-Schnittstelle zugewiesen werden. In diesem Beispiel nehmen wir DSL. Wechseln Sie in den Dialog **Firewall/QoS** > **QoS** > **Schnittstellen**.



7. (Optional): Je nach verwendeter WAN-Schnittstelle muss noch die verfügbare Datenrate im Fall einer Ethernet-Verbindung konfiguriert werden. Dies ist nicht nötig, falls ein internes xDSL-Modem verwendet wird. In

diesem Fall wird die synchronisierte DSL-Datenrate verwendet. Wechseln Sie in den Dialog **Schnittstellen** > **WAN** > **Interface-Einstellungen**.



Die Paket-Statistiken und die Verteilung in die Queues können auf der CLI unter `/status/WAN/QoS/Statistik` abgerufen werden (hier gekürzte Darstellung):

```
root@:/
> ls /Status/WAN/QoS/Statistik/

Interface  Prioritaet  Queue-Name          Vorab-klassifiziert   DSCP-klassifiziert    Gesamt-klassifiziert
=======================-------------------------------------------------------------------------------------
DSL-1      0           #urgent               0                     0                     0

DSL-1      1           VOIP                  0                     0                     0

DSL-1      2           GOLD                  0                     0                     0

DSL-1      3           SILBER                0                     0                     0

DSL-1      4           #best-effort          0                     0                     0
```

9.8.6 Beispiel 2: Konfiguration eines QoS-Konzepts am VDSL-Anschluss mit zwei QoS-Klassen

Im folgenden Beispiel soll ein Router für einen Kunden bereitgestellt werden, der dem Kunden am VDSL-Anschluss ein QoS-Konzept mit zwei QoS-Klassen ermöglicht. Die Klassen sind definiert als VoIP und Best Effort. Als Gerät wird ein Router mit internem xDSL-Modem verwendet.

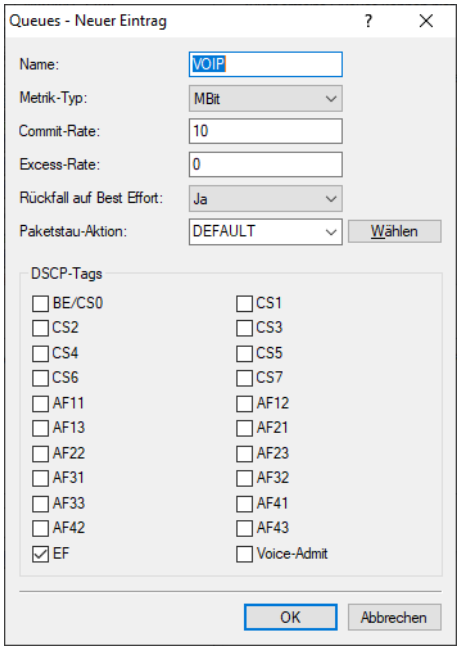
Der Serviceklasse VoIP wird eine absolute Bandbreite von 10 Mbit/s zugewiesen. Der Kunde markiert seine Pakete per DSCP, so dass die Pakete der korrekten Queue im Router zugewiesen werden können.

Werden in der definierten Serviceklasse mehr Daten übertragen als Bandbreite vorhanden ist, so werden diese Daten der Klasse Best Effort zugewiesen. Die Definition ist wie folgt:

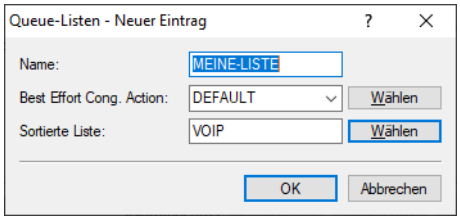
Klasse	DSCP
VOIP	EF

1. Starten Sie LANconfig und öffnen Sie den Konfigurationsdialog für das Gerät.
2. Wechseln Sie in den Dialog **Firewall/QoS** > **QoS** > **Queues**.

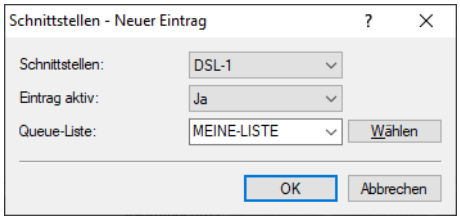
3. Legen Sie die Vorlage für die Serviceklasse VOIP an. Die Klasse Best Effort muss nicht manuell konfiguriert werden, da diese automatisch vorhanden ist.



4. Wechseln Sie in den Dialog **Firewall/QoS** > **QoS** > **Queue-Listen**.
5. Legen Sie eine Liste an, mit der Sie eine strikte Reihenfolge für die angelegten Klassen vorgeben. Die erste Klasse in der Liste hat die höchste Priorität.



6. Als letztes muss die konfigurierte Liste einer WAN-Schnittstelle zugewiesen werden. In diesem Beispiel nehmen wir DSL-1. Wechseln Sie in den Dialog **Firewall/QoS** > **QoS** > **Schnittstellen**.



Die Paket-Statistiken und die Verteilung in die Queues können auf der CLI unter `/status/WAN/QoS/Statistik` abgerufen werden (hier gekürzte Darstellung):

```
root@:/
> ls /Status/WAN/QoS/Statistik/

Interface  Prioritaet  Queue-Name          Vorab-klassifiziert   DSCP-klassifiziert    Gesamt-klassifiziert
=========================-------------------------------------------------------------------------------------
DSL-1      0           #urgent               0                     0                     0

DSL-1      1           VOIP                  0                     0                     0

DSL-1      2           #best-effort          0                     0                     0
```

9.8.7 Queue-Nutzung in der Firewall

In der Firewall ist es möglich, die im QoS konfigurierten Queues regelbasiert zuzuweisen. Diese Zuweisung ist unabhängig vom DSCP-Wert im IP-Header. Die Zuweisung erfolgt über Aktionen, die einer Regel zugewiesen werden. Wenn eine Regel mit einer solchen Aktion übereinstimmt und in der Firewall eine Session erzeugt wird, dann wird geprüft, ob dem Ziel- oder Quell-Interface der Session eine solche Queue zugewiesen wurde und die Zuweisung in der Aktion vermerkt. Wenn Daten über die Session laufen und die Aktion ausgeführt wird, wird das jeweilige Paket mit der Zuweisung markiert und wird dadurch vom DSCP-Classifier ignoriert und in der QoS-Statistik für die jeweilige Queue als „Pre-Classifed" gezählt.

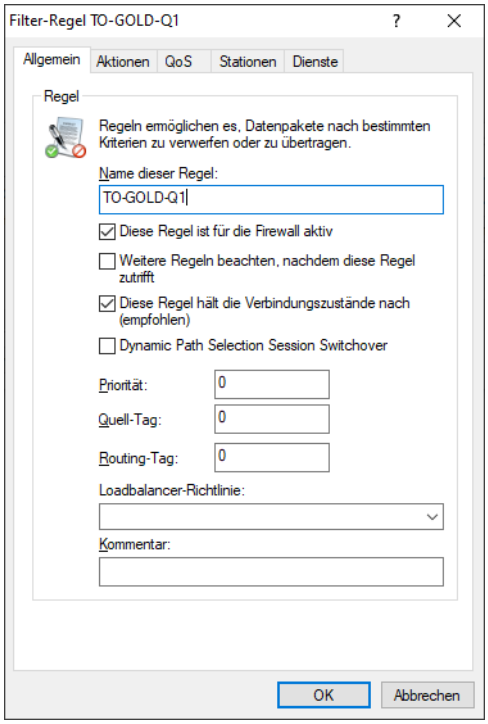
Die Queue-Zuweisung bezieht sich auf Queues, die physikalischen Interfaces zugewiesen wurden, wird aber auf darüber gestapelte Interfaces vererbt, d. h. wenn z. B. das Ziel-Interface einer Session ein VPN-Interface ist, dann propagiert sich die Queue-Zuweisung bis zum physikalischen Interface (WAN) durch und nutzt dieses dann zur Zuweisung.

Da sich die IPv4- und die IPv6-Firewall in ihrer Konfiguration unterscheiden, werden sie im Folgenden getrennt aufgeführt.

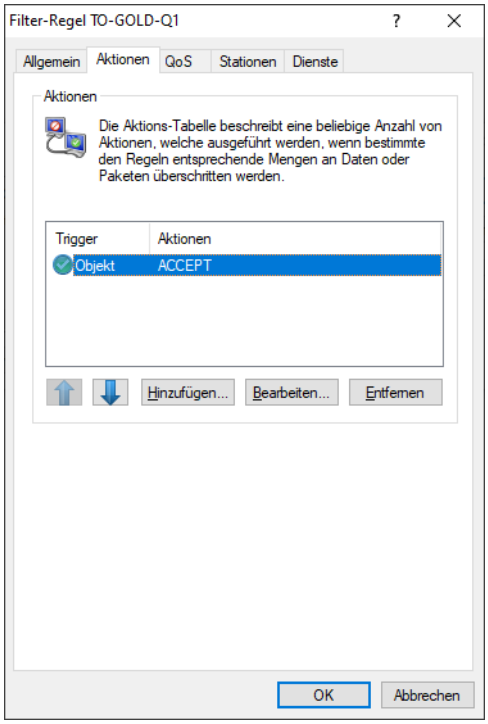
9.8.7.1 IPv4-Firewall

Im Folgenden ein Beispiel für die Vorgehensweise für eine Queuezuweisung:

1. Eine Queuezuweisung erfolgt über eine Firewall-Regel, d. h. sie wird unter **Firewall/QoS** > **IPv4-Regeln** > **Firewall-Regeln (Filter/QoS)** > **Regeln** hinzugefügt. Als erstes geben Sie der Regel auf dem Reiter **Allgemein** einen Namen.

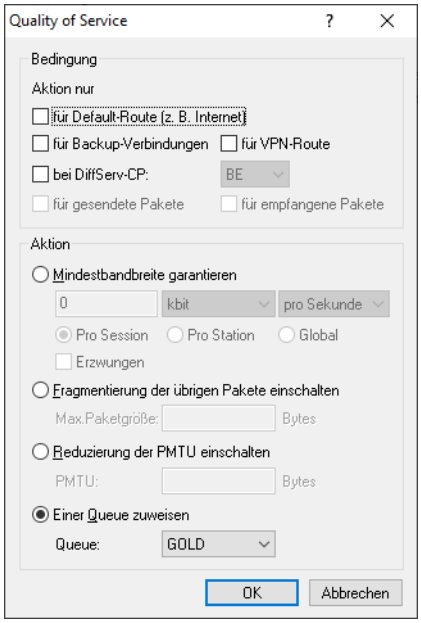


2. Danach fügen Sie auf dem Reiter **Aktionen** eine „ACCEPT"-Aktion hinzu und entfernen die voreingestellte „REJECT"-Aktion.

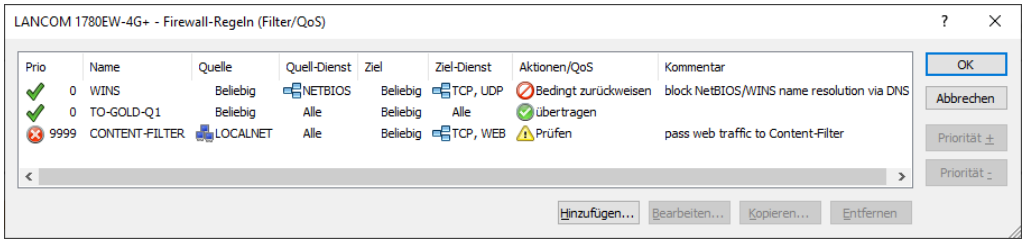


3. Als nächstes fügen Sie auf dem Reiter **QoS** ein neues QoS-Objekt an. Geben Sie diesem auf dem Reiter **Allgemein** einen Namen und weisen Die dann auf dem Reiter **Qos** diesem die gewünschte Queue zu.

   Die Aktion kann mit Bedingungen eingeschränkt werden, z. B. wenn die Zuweisung nur in einer bestimmten Richtung oder nur für einen bestimmten DSCP-Wert gelten soll.



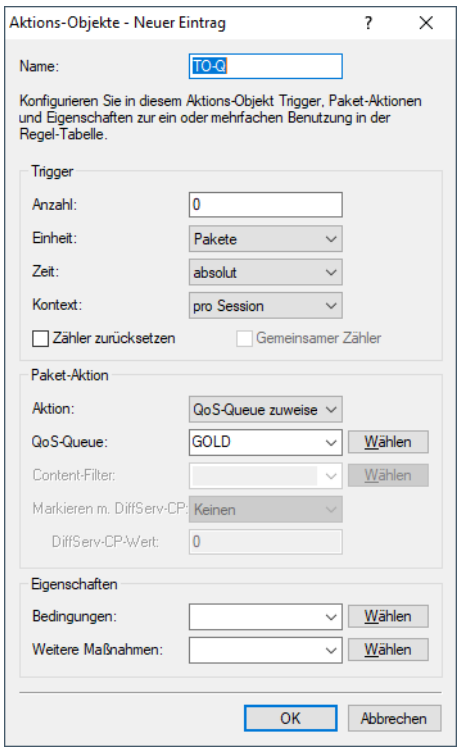
4. Als Ergebnis erhalten Sie eine Regel, welche die gewünschten Pakete einer Queue – in diesem Beispiel „GOLD" – zuweist.



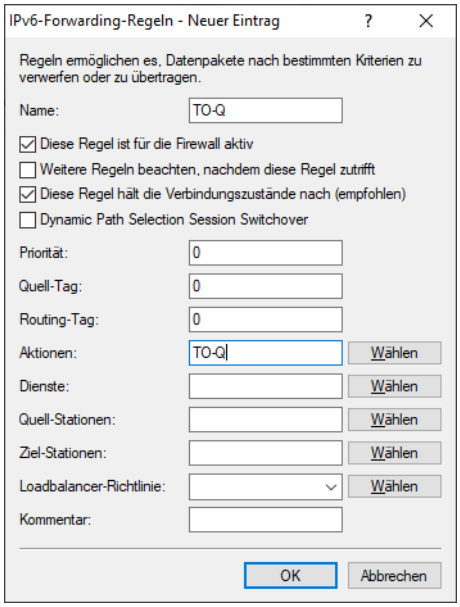
9.8.7.2 IPv6-Firewall

Im Folgenden ein Beispiel für die Vorgehenswweise für eine Queuezuweisung:

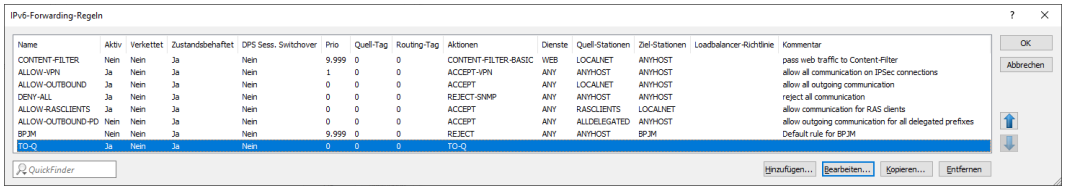
1. Eine Queuezuweisung erfolgt über ein in einer IPv6-Forwarding-Regel zugewiesenes Aktions-Objekt. Legen Sie als erstes ein Aktions-Objekt unter **Firewall/QoS** > **IPv6-Regeln** > **Firewall-Objekte** > **Aktions-Objekte** an, in dem Sie die gewünschte Queue zuweisen.



2. Danach erstellen Sie unter **Firewall/QoS** > **IPv6-Regeln** > **IPv6-Forwarding-Regeln** eine neue Regel, in der dieses Aktions-Objekt verwendet wird.



3. Als Ergebnis erhalten Sie eine Regel, welche die gewünschten Pakete einer Queue – in diesem Beispiel „GOLD" – zuweist.



9.9 QoS für WLANs nach IEEE 802.11e (WMM/WME)

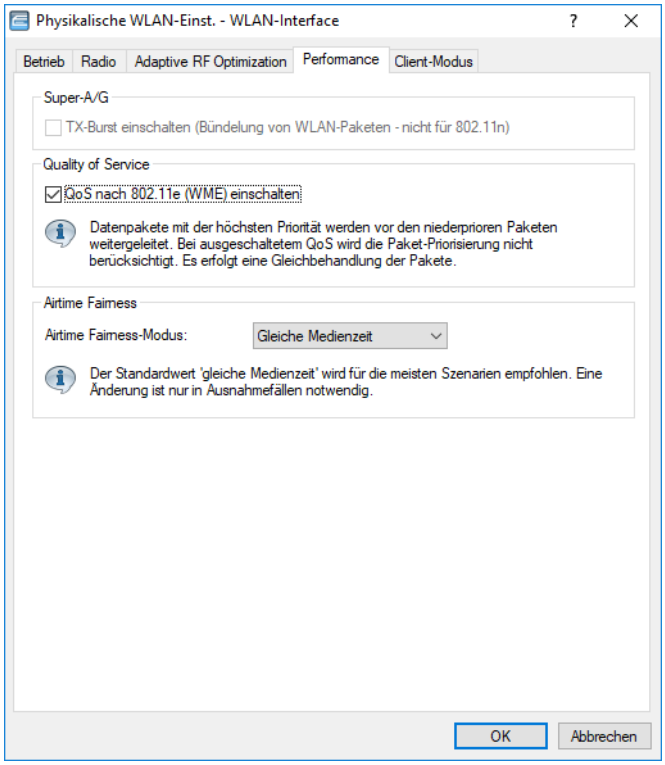
Mit der Erweiterung der 802.11-Standards um 802.11e können auch für WLAN-Übertragungen definierte Dienstgüten angeboten werden (Quality of Service). 802.11e unterstützt u. a. eine Priorisierung von bestimmten Datenpaketen. Die Erweiterung stellt damit eine wichtige Basis für die Nutzung von Voice-Anwendungen im WLAN dar (Voice over WLAN – VoWLAN).

Die Wi-Fi-Alliance zertifiziert Produkte, die Quality of Service nach 802.11e unterstützen, unter dem Namen WMM (Wi-Fi Multimedia, früher WME für Wireless Multimedia Extension). WMM definiert vier Kategorien (Sprache, Video, Best Effort und Hintergrund), die in Form separater Warteschlangen zur Prioritätensteuerung genutzt werden.

Der 802.11e-Standard nutzt zur Steuerung der Prioritäten die VLAN-Tags bzw. die DiffServ-Felder von IP-Paketen, wenn keine VLAN-Tags vorhanden sind. Die Verzögerungszeiten (Jitter) bleiben mit weniger als zwei Millisekunden in einem Bereich, der vom menschlichen Gehör nicht wahrgenommen wird. Zur Steuerung des Zugriffs auf das Übertragungsmedium nutzt der 802.11e-Standard die Enhanced Distributed Coordination Function (EDCF).

Die Steuerung der Prioritäten ist nur möglich, wenn sowohl der WLAN-Client als auch der Access Point den 802.11e-Standard bzw. WMM unterstützen und die Anwendungen die Datenpakete mit den entsprechenden Prioritäten kennzeichnen.

Die Verwendung von 802.11e kann in einem Access Point für jedes physikalische WLAN-Netzwerk getrennt aktiviert werden.



LANconfig: **Wireless-LAN** > **Allgemein** > **Physikalische WLAN-Einstellungen** > **Performance**

Konsole: **Setup** > **Schnittstellen** > **WLAN** > **Leistung**

10 Multicast Routing

In der Datenkommunikation unterscheidet man grundsätzlich vier Kategorien von Kommunikationsbeziehungen: Unicast, Broadcast, Multicast und Anycast. Unter Unicast versteht man die 1:1-Kommunikation, d. h. ein Sender kommuniziert mit einem Empfänger. Bei Broadcast sendet ein Sender Daten an alle angeschlossenen Geräte (1:n-Beziehung, bzw. „einer an alle"). Diese Kommunikationsmethode ist für bestimmte Dienste wie IPTV ineffizient, da alle Clients die Daten erhalten würden, also auch die Clients die kein Interesse daran haben. Daher gibt es mit Multicast eine weitere Methode, um Sender / Empfänger-Beziehungen herzustellen.. Multicast ist eine effiziente Kommunikationsmethode bei der ein Sender die Daten nur an die Geräte sendet, die Interesse an den Daten haben (1:m Beziehung, bzw. „einer an viele"). Empfänger müssen daher, bevor sie Daten empfangen, ihr Interesse durch Signalisierungsnachrichten bekunden. Bei der Kommunikationsbeziehung Anycast sendet ein Sender die Daten an einen beliebigen Empfänger aus einer Gruppe. In diesem Kapitel wird das Thema Multicast weiter behandelt.

Bei Multicast unterscheidet man grundsätzlich zwischen den folgenden Rollen: Sender und Empfänger. Ein Empfänger ist beispielsweise ein IPTV-Receiver oder ein mobiles Endgerät / PC. Unter einem Sender versteht man die Multicast-Quelle, z. B. einen IPTV-Sender. Wenn ein Client Multicast-Daten erhalten möchte, z. B. einen IPTV-Kanal, so bekundet er sein Interesse durch das Senden eines IGMP (Internet Group Management Protocol) Membership Reports bzw. bei IPv6 eines MLD (Multicast Listener Discovery) Membership Reports. Ein Multicast-Router erzeugt daraufhin automatisch einen Multicast-Routing Eintrag für diese Gruppe. Die Daten fließen dann „rückwärts" von der Quelle zum Empfänger. Besteht beim Client kein Interesse mehr an den Multicast-Daten, so sendet dieser eine entsprechen Membership Report zum Verlassen der Gruppe.

Der IP-Adressbereich für Multicast ist definiert von 224.0.0.0 bis 239.255.255.255 bei IPv4 bzw. als Präfix FF00::/8 bei IPv6. Man unterscheidet bei Multicast grundsätzlich in verschiedene Gültigkeitsbereiche, z. B. Link Local, Source Specific Multicast (232.0.0.0 bis 232.255.255.255) oder Organization-Local Scope (239.0.0.0 bis 239.255.255.255).

Weiterhin unterscheidet man zwei Kategorien von Multicast: Any Source Multicast (ASM) sowie Source Specific Multicast (SSM). Bei Any Source Multicast, dargestellt als (*,G), gibt der Empfänger nur die Multicast-Gruppe G an, und akzeptiert diese von beliebigen Quellen *. Any Source Multicast ist die ältere Variante der beiden Verfahren. Source Specific Multicast ist die moderne Variante bei der ein Empfänger neben der gewünschten Gruppe auch eine oder mehrere Quellen S anfordert. SSM setzt allerdings IGMPv3 bzw. MLDv2 voraus. Nach Möglichkeit sollte grundsätzlich SSM mit IGMPv3 eingesetzt werden, da dies besser skaliert. In der Regel basieren IPTV-Architekturen auf SSM.

Multicast-Routen werden nicht in der normalen (Unicast-)Routing-Tabelle verwaltet, sondern in einer separaten Multicast-Routing-Tabelle. Die Routing-Einträge dort werden in der Regel nicht statisch konfiguriert, sondern von Multicast-Routing-Protokollen wie PIM (Protocol Independent Multicast) oder einem Proxy, z. B. IGMP-Proxy, dynamisch erzeugt. Grundsätzlich setzt Multicast eine funktionierende Unicast-Routing-Tabelle voraus, da beim Reverse Path Forward Check (RPF-Check) geprüft wird, ob es eine Route zur Multicast-Quelle gibt. In der Regel wird neben einem Multicast Routing Protokoll wie PIM auch immer ein Unicast Routing-Protokoll verwendet, beispielsweise OSPF.

Für ein Szenario mit Multicast-Routing stehen drei Ansätze zur Verfügung:

1. Für ein einfaches Multicast-Routing-Szenario: Einsatz des IGMP- / MLD-Proxies.
2. Für ein komplexes Multicast-Routing-Szenario: PIM SSM.
3. Konfiguration von statischen Gruppeneinträgen wird nur empfohlen, wenn Clients kein IGMP / MLD beherrschen.

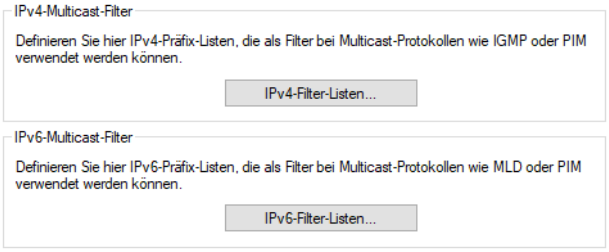
PIM Sparse Mode kann ebenfalls statt PIM SSM zum Einsatz kommen, allerdings muss sowohl die Rolle des Rendezvous Points als auch die des First-Hop-Routers direkt vor der Multicast-Quelle von einem Dritthersteller übernommen werden.

10.1 Allgemeine Multicast Show-Kommandos

- `show IPv4-mfib` / `show IPv4-mfib` (als alias gibt es `ipv4-mroute` / `ipv6-mroute`): Zeigt den Inhalt der Multicast Forwarding Information Base / Routing-Tabelle an.
- `show iPv4-tib` / `show iPv6-tib`: Zeigt den Inhalt der Tree Information Base an. Enthält Informationen über den Multicast Gruppenstatus sowie zusätzliche Informationen aus PIM.
- `show igmp-groups`: Zeigt Informationen über Multicast-Gruppen, bei denen der Router selbst beigetreten ist.

10.2 Allgemeine Einstellungen

Um allgemeine Einstellungen zu Multicast mit LANconfig zu konfigurieren, wechseln Sie in die Ansicht **Multicast** > **Allgemein**.

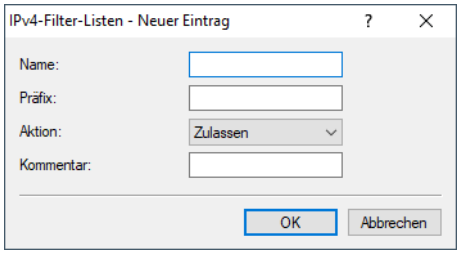


10.2.1 IPv4-Filter-Listen

In LANconfig konfigurieren Sie die IPv4-Filter-Listen für Muilticast unter **Multicast** > **Allgemein** > **IPv4-Multicast-Filter** über **IPv4-Filter-Listen**.

In dieser Tabelle können Listen von gewünschten oder unerwünschten IPv4 Multicast-Adressen bzw. Präfixen definiert werden. Verschiedene einzelne Filterregeln können durch einen gleichen Namen zu einer Regelliste zusammengefasst werden. In einer Regelliste können sowohl Präfixe verboten als auch erlaubt werden.

Die Namen der Filterlisten können an verschiedenen Stellen referenziert werden und über diese Tabelle global verwaltet werden.



Name

Geben Sie diesem Eintrag einen Namen. Eine Liste wird durch mehrere Einträge mit gleichem Namen definiert.

Präfix

Geben Sie hier die IPv4-Adresse des Netzwerkes gefolgt von der Präfix-Länge des Netzwerkes an (CIDR-Notation). Diese legt fest, wie viele höchstwertige Bits (Most Significant Bit, MSB) der IP-Adresse für eine Übereinstimmung notwendig sind.

Aktion

Geben Sie an, ob die Präfixe dieses Filtereintrags zugelassen oder abgewiesen werden sollen.

Kommentar

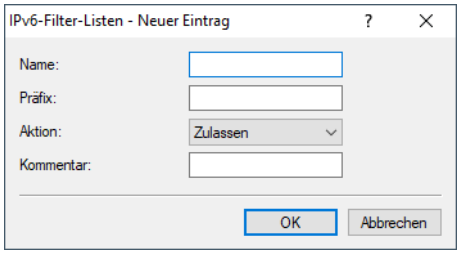
Kommentar zu diesem Eintrag.

10.2.2 IPv6-Filter-Listen

In LANconfig konfigurieren Sie die IPv4-Filter-Listen für Muilticast unter **Multicast** > **Allgemein** > **IPv6-Multicast-Filter** über **IPv6-Filter-Listen**.

In dieser Tabelle können Listen von gewünschten oder unerwünschten IPv6 Multicast-Adressen bzw. Präfixen definiert werden. Verschiedene einzelne Filterregeln können durch einen gleichen Namen zu einer Regelliste zusammengefasst werden. In einer Regelliste können sowohl Präfixe verboten als auch erlaubt werden.

Die Namen der Filterlisten können an verschiedenen Stellen referenziert werden und über diese Tabelle global verwaltet werden.



Name

Geben Sie diesem Eintrag einen Namen. Eine Liste wird durch mehrere Einträge mit gleichem Namen definiert.

Präfix

Geben Sie hier die IPv6-Multicast-Adresse bzw. das Präfix an.

Aktion

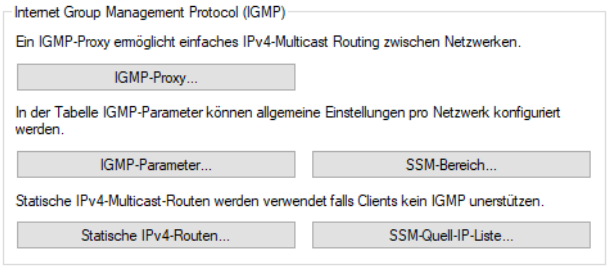
Geben Sie an, ob die Präfixe dieses Filtereintrags zugelassen oder abgewiesen werden sollen.

Kommentar

Kommentar zu diesem Eintrag.

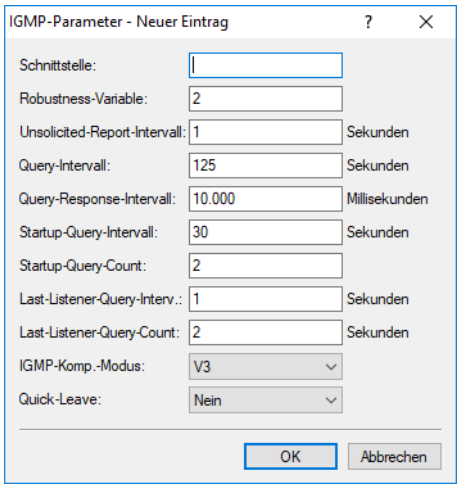
10.3 IGMP (Internet Group Management Protocol)

Um IGMP mit LANconfig zu konfigurieren, wechseln Sie in die Ansicht **Multicast** > **IGMP / MLD** > **Internet Group Management Protocol (IGMP)**.



10.3.1 IGMP-Parameter

In LANconfig konfigurieren Sie die allgemeinen IGMP-Parameter unter **Multicast** > **IGMP / MLD** > **Internet Group Management Protocol (IGMP)** über **IGMP-Parameter**.



Schnittstelle

Schnittstellenname, für den die IGMP-Konfiguration gilt. Der Eintrag mit dem Namen DEFAULT gilt für alle Schnittstellen, die keinen spezifischen Eintrag haben. Falls der Eintrag DEFAULT nicht vorhanden ist, gelten interne Default-Werte die den Werten des DEFAULT-Eintrags entsprechen. Mögliche Werte sind DEFAULT, IPv4-Netzwerke, z. B. INTRANET oder IPv4-(WAN)-Gegenstellen. Ebenfalls sind Wildcard-Einträge mit * für RAS-Interfaces erlaubt, z. B. „VPN*“.

Robustness-Variable

Anzahl der Wiederholungen von IGMP-Nachrichten. (1-10; Default: 2)

Unsolicited-Report-Intervall

Definiert die Zeit zwischen den Wiederholungen von Membership-Reports nach dem das Gerät in der Host-Rolle den erstmaligen Membership-Report in einer Gruppe gesendet hat. (1-25 Sekunden; Default: 2)

Query-Intervall

Intervall zwischen IGMP General-Query-Nachrichten. (2-99999 Sekunden; Default: 125)

Query-Response-Intervall

Maximale Antwortzeit. Aus dieser wird der Wert Maximum Response Time berechnet, der in periodischen General-Query-Nachrichten gesetzt wird. Der Wert Query-Response-Intervall muss kleiner als der Wert für Query-Intervall sein. (1-999999 Millisekunden; Default: 10000)

Startup-Query-Intervall

Intervall zwischen IGMP General-Query-Nachrichten beim Start des IGMP-Queriers. (1-99998 Sekunden; Default: 30)

Startup-Query-Count

Anzahl an IGMP General-Query-Nachrichten, die beim Start gesendet werden, unterbrochen bzw. zeitlich verzögert vom Startup-Query-Intervall. (1-10; Default: 2)

Last-Listener-Query-Intervall

Definiert den Wert der Maximum Response Time in Multicast-Address-Specific Queries, die als Antwort auf Done-Nachrichten gesendet werden. Der Parameter definiert ebenso die Zeit zwischen Multicast-Address-Specific-Query-Nachrichten. (1-25 Sekunden; Default: 2)

Last-Listener-Query-Count

Anzahl von gesendeten Nachrichten vom Typ Multicast-Address-Specific Query bevor der Router annimmt, dass es keine lokalen Empfänger mehr gibt. Definiert ebenso die Anzahl an gesendeten Nachrichten vom Typ Multicast-Address-Specific-Query bevor der Router annimmt, dass es keine weiteren Empfänger für eine spezielle Quelle gibt. (1-10; Default: 2)

IGMP-Kompatibilitäts-Modus

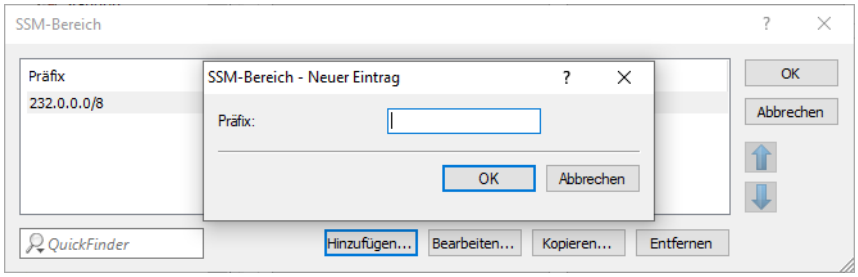
IGMP-Version, in der das Gerät in der Rolle als Multicast-Router arbeitet. Mögliche Werte: Aus, V1, V2, V3. (Default: V3)

Quick-Leave

Erlaubt das schnelle Verlassen von Multicast Gruppen. Sollte nur verwendet werden, falls es nur einen Empfänger pro Gruppe auf dem Interface gibt. Intern wird der Parameter Last-Listener-Query-Count auf 1 und das Last-Listener-Query-Intervall auf 20 ms gesetzt. Mögliche Werte: Ja, Nein (Default: Nein)

10.3.2 SSM-Bereich

In LANconfig konfigurieren Sie die SSM-Bereiche unter **Multicast** > **IGMP / MLD** > **Internet Group Management Protocol (IGMP)** über **SSM-Bereich**.



Präfix

Definiert den IP-Adressbereich in Präfixschreibweise, der für SSM verwendet wird.

10.3.3 IGMP-Proxy

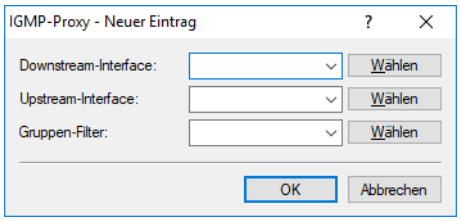
Ein IGMP-Proxy wird in der Regel bei Interzugängen mit Multicast IPTV verwendet. Dabei senden Clients bzw. IPTV Set-Top-Boxen (STBs) im lokalen Netz IGMP-Nachrichten, um einen bestimmten TV-Kanal zu empfangen. Dazu treten

sie bestimmten Multicast-Gruppen bei und verlassen diese auch wieder. Der Router bzw. die IGMP-Proxy-Funktionalität empfängt die IGMP-Nachrichten und leitet sie an das Provider-Netzwerk weiter bzw. filtert die Gruppen bei Bedarf. Der IGMP-Proxy arbeitet dabei als Stellvertreter für das lokale Netzwerk mit seinen Clients.

Ein IGMP-Proxy kann auch in einfachen Multicast-Routing Szenarien beispielsweise über VPN verwendet werden ohne dass PIM verwendet werden muss. Durch die Konfiguration des IGMP-Proxies wird eine statische (Baum-)Struktur ohne alternative Pfade bzw. Redundanz sowie Loop-Verhinderung erzeugt. IGMP-Proxies können durch eine Reihenschaltung mehrerer Router „kaskadiert" werden.

Der IGMP-Proxy unterstützt kein BiDirectional Multicast. Daher dürfen die Interfaces im IGMP-Proxy nicht über Kreuz angelegt werden.

In LANconfig konfigurieren Sie den IGMP-Proxy unter **Multicast** > **IGMP / MLD** > **Internet Group Management Protocol (IGMP)** über **IGMP-Proxy**.



Downstream-Interface

Interface-Name auf dem IGMP-Clients Gruppen beitreten können und IGMP-Nachrichten vom Proxy empfangen werden. Mögliche Werte sind IPv4-Netzwerke, z. B. INTRANET, IPv4-(WAN)-Gegenstellen. Ebenfalls sind Wildcard-Einträge mit * für RAS-Interfaces erlaubt, z. B. „VPN*".

Bei Provider-basierten IPTV-Szenarien muss hier das lokale Netzwerk, z. B. INTRANET, konfiguriert werden.

Upstream-Interface

Interface Name auf dem IGMP-Nachrichten vom Proxy stellvertretend für Clients gesendet werden. Die Quelle der Multicast-Nachrichten muss über dieses Interface erreicht werden. Mögliche Werte sind IPv4-Netzwerke, z. B. INTRANET sowie IPv4-(WAN)-Gegenstellen.

Bei Provider-basierten IPTV-Szenarien muss hier die WAN-Gegenstelle, z. B. INTERNET, konfiguriert werden.

Gruppenfilter

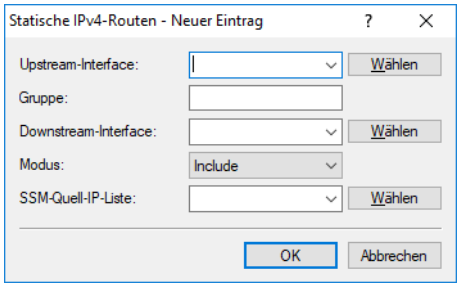
Name des Gruppenfilters der für diesen Proxy gelten soll. Referenziert die Tabelle IPv4-Filter-Listen unter **Multicast** > **Allgemein**. Standardmäßig ist der Filtereintrag leer bzw. verweist auf die Filterliste „ANY", die alle Multicast-Gruppen erlaubt. Mit Hilfe des Gruppenfilters können die möglichen Multicast-Gruppen für Clients eingeschränkt werden.

10.3.4 Statisches IPv4-Multicast Routing

Statisches Multicast Routing kann verwendet werden, wenn Multicast Clients kein IGMP beherrschen bzw. für Szenarien, in dem Multicast-Datenverkehr immer fließen muss, ohne dass Clients die entsprechende Gruppe anfordern. Der Router erzeugt ab dem Anlegen des Eintrags auf dem Upstream-Interface IGMP Joins bzw. Gruppenreporte.

Bitte beachten Sie, dass ein statisches Multicast Routing hohen Datenverkehr und Last verursachen kann, da die Multicast-Daten immer weitergeleitet werden.

In LANconfig konfigurieren Sie die statischen IPv4-Multicast-Routen unter **Multicast** > **IGMP / MLD** > **Internet Group Management Protocol (IGMP)** über **Statische IVv4-Routen**.



Upstream-Interface

Interface Name auf dem die Multicast-Pakete den Router erreichen. Mögliche Werte sind IPv4-Netzwerke, z. B. INTRANET sowie IPv4-(WAN)-Gegenstellen.

Gruppe

Multicast-Gruppe für die das statische Weiterleiten von Multicast-Daten angelegt werden soll, z. B. 239.0.0.1.

Downstream-Interface

Interface Name auf dem die Multicast-Pakete den Router verlassen sollen. Mögliche Werte sind IPv4-Netzwerke, z. B. INTRANET sowie IPv4-(WAN)-Gegenstellen.

Modus

Falls SSM verwendet werden soll: Steuert, über welche Methode Quelladressen der Multicast-Quellen in einem IGMP-Membership-Report angefordert werden sollen. Mögliche Werte:

Include

Es wird ein IGMP-Membership Report mit Record-Type „Change to Include Mode“ gesendet. Die Einträge aus der SSM-Quell-IP-Liste werden als gewünschte Quelladressen gesendet. Eine Kombination mit Einstellung „Include“ und SSM-Quell-IP-Liste mit Eintrag „ANY“ führt zu keinem sinnvollen Ergebnis und wird als Konfiguration intern nicht akzeptiert, da alle Quell-IP-Adressen abgelehnt werden würden.

Exclude

Es wird ein IGMP-Membership Report mit Record-Type „Change to Exclude Mode“ gesendet. Wenn die Quell-Liste den Eintrag „ANY“ bzw. „0.0.0.0“ enthält, d. h. alle Quellen erlaubt, so wird ein IGMP-Membership Report mit Join Group für „any sources“ gesendet. Wenn die Liste einen anderen Eintrag als 0.0.0.0 enthält wird ein IGMP Membership Report „block sources“ mit der entsprechenden IP-Adresse gesendet.

Wenn eine SSM-Gruppe mit beliebigen Quelladressen verwendet werden soll, so muss bei Modus „Exclude“ und SSM-Quell-IP-Liste „ANY“ verlinkt werden.

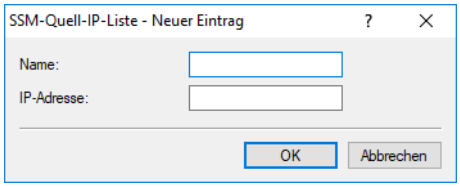
SSM-Quell-IP-Liste

Falls SSM verwendet werden soll, kann hier eine Liste von gewünschten Quellen zusätzlich zur Multicast-Gruppe definiert werden. Sollen alle Quellen zugelassen werden, kann die vordefinierte Liste „ANY“ mit dem Eintrag „0.0.0.0“ verwendet werden.

10.3.5 SSM-Quell-IP-Liste

In dieser Tabelle können Listen von gewünschten oder unerwünschten (Unicast) Quell-IP-Adressen definiert werden. Diese können an verschiedenen Stellen referenziert werden und über diese Tabelle global verwaltet werden. Eine Liste wird durch den mehrere Einträge mit gleichem Namen definiert.

In LANconfig konfigurieren Sie die SSM-Quell-IP-Liste unter **Multicast** > **IGMP / MLD** > **Internet Group Management Protocol (IGMP)** über **SSM-Quell-IP-Liste**.



Name

Vergeben Sie einen Namen für den Eintrag. Eine Liste wird durch den mehrere Einträge mit gleichem Namen definiert.

IP-Adresse

Unicast Quell-IPv4-Adresse. Multicast-Adressen sind an dieser Stelle keine gültige Eingabe, da hier die Quell-IP-Adressen (Source) eines Multicast-Eintrag (S,G) definiert werden.

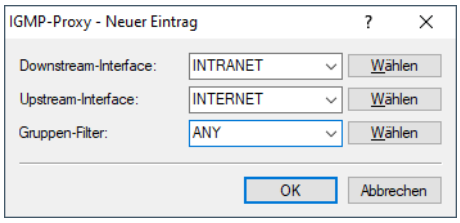
10.3.6 Tutorial: IGMP-Proxy einrichten

Im folgenden Tutorial werden die notwendigen Schritte zur Einrichtung eines IGMP-Proxies für Multicast-Routing beschrieben.

In diesem Beispiel befinden sich Multicast-Clients im Netzwerk „INTRANET", die Multicast-Quellen sind über die WAN-Gegenstelle „INTERNET" zu erreichen. Der IGMP-Proxy leitet IGMP-Nachrichten vom INTRANET ins INTERNET stellvertretend für die Clients weiter. Zusätzlich ist es möglich, dass bestimmte Multicast-Gruppen gefiltert werden können.

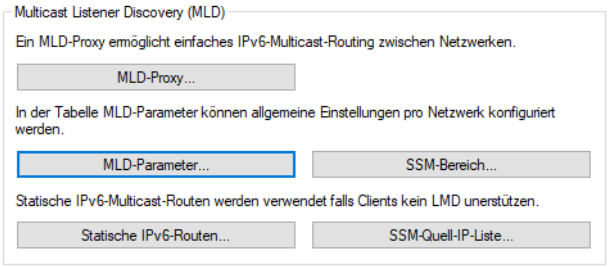
1. Neuen Tabelleneintrag erstellen unter **Multicast** > **IGMP / MLD** > **Internet Group Management Protocol (IGMP)** > **IGMP-Proxy** erstellen:
   - **Downstream-Interface**: Interface-Name, auf dem IGMP-Clients Gruppen beitreten können und IGMP-Nachrichten vom Proxy empfangen werden. Konfigurieren Sie hier den Namen des Client-Netzwerks, z. B. „INTRANET".
   - **Upstream-Interface**: Interface Name, auf dem IGMP-Nachrichten vom Proxy stellvertretend für Clients gesendet werden. Die Quelle der Multicast-Nachrichten muss über dieses Interface erreicht werden. Konfigurieren Sie hier den Namen der Gegenstelle der Internetverbindung, z. B. „INTERNET".
   - **Gruppen-Filter**: Name des Gruppenfilters der für diesen Proxy gelten soll. Referenziert die Tabelle **IPv4-Filter-Listen** unter **Multicast** > **Allgemein**. Mit Hilfe des Gruppenfilters können die möglichen Multicast-Gruppen für Clients eingeschränkt werden. Eintrag „ANY" auswählen, dieser erlaubt alle Multicast-Gruppen.

Weitere Einstellungen, z. B. in der Firewall sind ab LCOS 10.40 nicht mehr erforderlich.



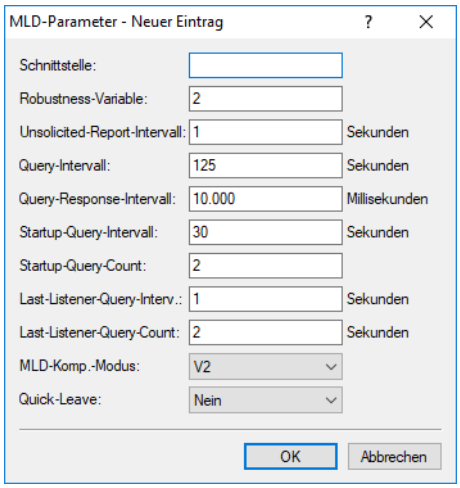
10.4 MLD (Multicast Listener Discovery)

Um MLD mit LANconfig zu konfigurieren, wechseln Sie in die Ansicht **Multicast** > **IGMP / MLD** > **Multicast Listener Discovery (MLD)**.



10.4.1 MLD-Parameter

In LANconfig konfigurieren Sie die allgemeinen MLD-Parameter unter **Multicast** > **IGMP / MLD** > **Multicast Listener Discovery (MLD)** über **MLD-Parameter**.



Schnittstelle

Schnittstellenname, für den die MLD-Konfiguration gilt. Der Eintrag mit dem Namen DEFAULT gilt für alle Schnittstellen, die keinen spezifischen Eintrag haben. Falls der Eintrag DEFAULT nicht vorhanden ist, gelten interne Default-Werte, die den Werten des DEFAULT-Eintrags entsprechen. Mögliche Werte sind DEFAULT, IPv6-Netzwerke, z. B. INTRANET, IPv6-(WAN)-Gegenstellen oder IPv6 RAS-Templates.

Robustness-Variable

Anzahl der Wiederholungen von MLD-Nachrichten. (1-10; Default: 2)

Unsolicited-Report-Intervall

Definiert die Zeit zwischen den Wiederholungen von Membership-Reports nach dem das Gerät in der Host-Rolle den erstmaligen Membership-Report in einer Gruppe gesendet hat. (1-25 Sekunden; Default: 2)

Query-Intervall

Intervall zwischen MLD General-Query-Nachrichten. (2-99999 Sekunden; Default: 125)

Query-Response-Intervall

Maximale Antwortzeit aus der der Wert Maximum Response Code berechnet wird, der in periodischen MLD General-Query-Nachrichten gesetzt wird. Der Wert Query-Response-Intervall muss kleiner als der Wert für Query-Intervall sein. (1-999999 Millisekunden; Default: 10000)

Startup-Query-Intervall

Intervall zwischen MLD General-Query-Nachrichten beim Start des MLD-Queriers. (1-99998 Sekunden; Default: 30)

Startup-Query-Count

Anzahl an MLD-General-Nachrichten die beim Start gesendet werden, unterbrochen bzw. zeitlich verzögert vom Startup-Query-Intervall. (1-10; Default: 2)

Last-Listener-Query-Intervall

Definiert den Wert des Maximum Response Code (bei IPv6) in Multicast-Address-Specific Queries, die als Antwort auf Done-Nachrichten gesendet werden. Der Parameter definiert ebenso die Zeit zwischen Multicast-Address-Specific-Query-Nachrichten. (1-25 Secunden; Default: 2)

Last-Listener-Query-Count

Anzahl von gesendeten Nachrichten vom Typ Multicast-Address-Specific Query bevor der Router annimmt, dass es keine lokalen Empfänger mehr gibt. Definiert ebenso die Anzahl an gesendeten Nachrichten vom Typ Multicast-Address-Specific-Query bevor der Router annimmt, dass es keine weiteren Empfänger für eine spezielle Quelle gibt. (1-10; Default: 2)

MLD-Kompatibilitäts-Modus

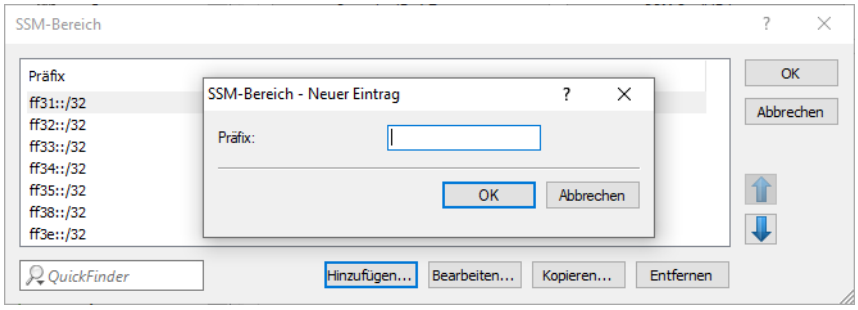
MLD-Version, in der das Gerät in der Rolle als Multicast-Router arbeitet. Mögliche Werte: Aus, V1, V2 (Default: V2)

Quick-Leave

Erlaubt das schnelle Verlassen von Multicast Gruppen. Sollte nur verwendet werden, falls es nur einen Empfänger pro Gruppe auf dem Interface gibt. Intern wird der Parameter Last-Listener-Query-Count auf 1 und das Last-Listener-Query-Intervall auf 20 ms gesetzt. Mögliche Werte: Ja, Nein (Default: Nein)

10.4.2 SSM-Bereich

In LANconfig konfigurieren Sie die SSM-Bereiche unter **Multicast** > **IGMP / MLD** > **Multicast Listener Discovery (MLD)** über **SSM-Bereich**.



Präfix

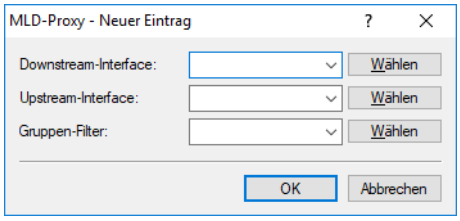
Definiert den IP-Adressbereich in Präfixschreibweise, der für SSM verwendet wird.

10.4.3 MLD-Proxy

Ein MLD-Proxy wird in der Regel bei Interzugängen mit Multicast IPTV über IPv6 verwendet. Dabei senden Clients bzw. IPTV Set-Top-Boxen (STBs) im lokalen Netz MLD-Nachrichten um einen bestimmten TV-Kanal zu empfangen. Dazu treten sie bestimmten Multicast-Gruppen bei und verlassen diese auch wieder. Der Router bzw. die MLD-Proxy-Funktionalität empfängt die MLD-Nachrichten und leitet sie an das Provider-Netzwerk weiter bzw. filtert die Gruppen bei Bedarf. Der MLD-Proxy arbeitet dabei als Stellvertreter für das lokale Netzwerk mit seinen Clients.

Ein MLD-Proxy kann auch in einfachen Multicast-Routing Szenarien beispielsweise über VPN verwendet werden ohne dass PIM verwendet werden muss. Durch die Konfiguration des MLD-Proxies wird eine statische (Baum-)Struktur ohne alternative Pfade bzw. Redundanz sowie Loop-Verhinderung erzeugt. MLD-Proxies können durch eine Reihenschaltung mehrerer Router „kaskadiert" werden.

In LANconfig konfigurieren Sie den MLD-Proxy unter **Multicast** > **IGMP / MLD** > **Multicast Listener Discovery (MLD)** über **MLD-Proxy**.



Downstream-Interface

Interface-Name auf dem MLD-Clients Gruppen beitreten können und MLD-Nachrichten vom Proxy empfangen werden. Mögliche Werte sind IPv6-Netzwerke, z. B. INTRANET, IPv6-(WAN)-Gegenstellen oder RAS-Templates.

Bei Provider-basierten IPTV-Szenarien muss hier das lokale Netzwerk, z. B. INTRANET, konfiguriert werden.

Upstream-Interface

Interface Name auf dem MLD-Nachrichten vom Proxy stellvertretend für Clients gesendet werden. Die Quelle der Multicast-Nachrichten muss über dieses Interface erreicht werden. Mögliche Werte sind IPv6-Netzwerke, z. B. INTRANET sowie IPv6-(WAN)-Gegenstellen.

Bei Provider-basierten IPTV-Szenarien muss hier die WAN-Gegenstelle, z. B. INTERNET, konfiguriert werden.

Gruppenfilter

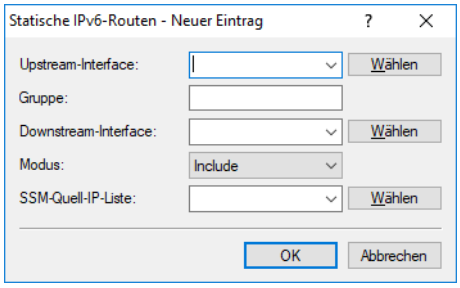
Name des Gruppenfilters, der für diesen Proxy gelten soll. Referenziert die Tabelle IPv6-Filter-Listen unter **Multicast** > **Allgemein**. Standardmäßig ist der Filtereintrag leer bzw. verweist auf die Filterliste „ANY", die alle Multicast-Gruppen erlaubt. Mit Hilfe des Gruppenfilters können die möglichen Multicast-Gruppen für Clients eingeschränkt werden.

10.4.4 Statisches IPv6-Multicast Routing

Statisches Multicast Routing kann verwendet werden, wenn Multicast Clients kein MLD beherrschen bzw. für Szenarien, in dem Multicast-Datenverkehr immer fließen muss, ohne dass Clients die entsprechende Gruppe anfordern. Der Router erzeugt ab dem Anlegen des Eintrags auf dem Upstream-Interface MLD Gruppenreporte.

Bitte beachten Sie, dass ein statisches Multicast Routing hohen Datenverkehr und Last verursachen kann, da die Multicast-Daten immer weitergeleitet werden.

In LANconfig konfigurieren Sie die statischen IPv6-Multicast-Routen unter **Multicast** > **IGMP / MLD** > **Multicast Listener Discovery (MLD)** über **Statische IVv6-Routen**.



Upstream-Interface

Interface Name auf dem die Multicast-Pakete den Router erreichen. Mögliche Werte sind IPv6-Netzwerke, z. B. INTRANET sowie IPv6-(WAN)-Gegenstellen.

Gruppe

Multicast-Gruppe für die das statische Weiterleiten von Multicast-Daten angelegt werden soll, beispielsweise „ff09::1".

Downstream-Interface

Interface Name auf dem die Multicast-Pakete den Router verlassen sollen. Mögliche Werte sind IPv6-Netzwerke, z. B. INTRANET sowie IPv6-(WAN)-Gegenstellen.

Modus

Falls SSM verwendet werden soll: Steuert, über welche Methode Quelladressen der Multicast-Quellen in einem MLD-Membership-Report angefordert werden sollen. Mögliche Werte:

Include

Es wird ein MLD-Membership Report mit Record-Type „Change to Include Mode" gesendet. Die Einträge aus der SSM-Quell-IP-Liste werden als gewünschte Quelladressen gesendet. Eine Kombination mit Einstellung „Include" und SSM-Quell-IP-Liste mit Eintrag „ANY" führt zu keinem sinnvollen Ergebnis und wird als Konfiguration intern nicht akzeptiert, da alle Quell-IP-Adressen abgelehnt werden würden.

Exclude

Es wird ein MLD-Membership Report mit Record-Type „Change to Exclude Mode" gesendet. Wenn die Quell-Liste den Eintrag „ANY" bzw. „::" enthält, d. h. alle Quellen erlaubt, so wird ein MLD-Membership Report mit Join Group für „any sources" gesendet. Wenn die Liste einen anderen Eintrag als „::" enthält wird ein MLD Membership Report „block sources" mit der entsprechenden IP-Adresse gesendet.

Wenn eine SSM-Gruppe mit beliebigen Quelladressen verwendet werden soll, so muss bei Modus „Exclude" und SSM-Quell-IP-Liste „ANY" verlinkt werden.

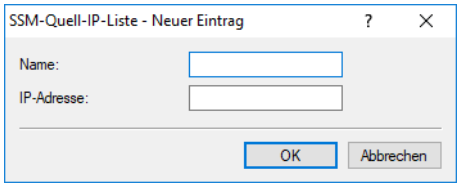
SSM-Quell-IP-Liste

Falls SSM verwendet werden soll, kann hier eine Liste von gewünschten Quellen zusätzlich zur Multicast-Gruppe definiert werden. Sollen alle Quellen zugelassen werden, kann die vordefinierte Liste „ANY" mit dem Eintrag „::" verwendet werden.

10.4.5 SSM-Quell-IP-Liste

In dieser Tabelle können Listen von gewünschten oder unerwünschten (Unicast) Quell-IPv6-Adressen definiert werden. Diese können an verschiedenen Stellen referenziert werden und über diese Tabelle global verwaltet werden. Eine Liste wird durch mehrere Einträge mit gleichem Namen definiert.

In LANconfig konfigurieren Sie die SSM-Quell-IP-Liste unter **Multicast** > **IGMP / MLD** > **Multicast Listener Discovery (MLD)** über **SSM-Quell-IP-Liste**.



Name

Vergeben Sie einen Namen für den Eintrag. Eine Liste wird durch den mehrere Einträge mit gleichem Namen definiert.

IP-Adresse

Unicast Quell-IPv6-Adresse. Multicast-Adressen sind an dieser Stelle keine gültige Eingabe, da hier die Quell-IPv6-Adressen (Source) eines Multicast-Eintrag (S,G) definiert werden.

10.5 PIM (Protocol Independent Multicast)

PIM (*RFC 7761*) ermöglicht dynamisches Routing von Multicast-Paketen. Dabei nutzt PIM die Routinginformationen des im Router aktiven Unicast-Routing-Protokolls mit, funktioniert aber grundsätzlich unabhängig von dem verwendeten Routingprotokoll wie z. B. RIP, OSPF oder BGP.

Für ein PIM-Szenario mit ausschließlich LANCOM Router wird nur die Betriebsart PIM SSM (Source Specific Multicast) vollständig unterstützt. Für den Betrieb des PIM Sparse Mode werden Router bzw. Komponenten von Drittherstellern benötigt. PIM SSM hat den Vorteil, dass es dank einfacherer Architektur deutlich besser skaliert und ideal geeignet ist für moderne Multicast-Anwendungen wie etwa IPTV. PIM SSM setzt auf der Clientseite IGMPv3 bzw. MLDv2 (bei IPv6) voraus und kommt ohne zusätzlichen Rendezvous Point (RP) aus, da Clients neben der gewünschten Multicast Gruppe (G) auch die Multicast Source (S) direkt anfragen.

Grundsätzlich wird bei PIM SSM zwischen zwei Router-Rollen unterschieden: First-Hop-Router und Last-Hop-Router. Ein First-Hop-Router ist definiert als Router, der direkt mit Multicast IGMP- bzw. MLD-Clients bzw. Empfängern verbunden ist. Ein Last-Hop-Router ist definiert als Router, der direkt mit der Multicast-Quelle verbunden ist. Darüber hinaus gibt es noch Router, die zwischen den beiden anderen Router-Rollen geschaltet sein können. PIM muss grundsätzlich auf allen Interfaces aktiviert werden, auf denen Multicast-Routing durchgeführt werden soll. Auf Client-Interfaces muss IGMP bzw. MLD aktiviert sein.

Die folgenden PIM-Funktionen werden vom LCOS unterstützt:

- PIM Sparse Mode (ASM) mit externem RP von einem Dritthersteller
- Statische Konfiguration des RPs bei PIM Sparse Mode
- PIM SSM in den Rollen als Last-Hop-Router sowie First-Hop-Router
- Unterstützung von IPv4 und IPv6 PIM
- SSM Mapping, wobei aus IGMPv2- bzw. MLD-Nachrichten PIM SSM-Joins erzeugt werden
- PIM nativ über IPSec VPN ohne GRE-Tunnel

Die folgenden PIM-Funktionen werden nicht unterstützt:

- Rolle als Rendezvous Point (RP)
- Rolle als First-Hop-Router bei PIM Sparse, der einen automatischen Register-Unicast-Tunnel erzeugt, um beim RP eine Multicast-Quelle zu registrieren
- Dense Mode, Bi-Dir Mode
- Dynamische RP-Konfiguration, z. B. über Bootstrap Router (BSR) Funktion

PIM Show-Kommandos

Die folgenden Show Kommandos stehen für PIM zur Verfügung:

- PIM IPv4-Groups: Zeigt Informationen über beigetretene IPv4 Multicast Gruppen
- PIM IPv6-Groups: Zeigt Informationen über beigetretene IPv6 Multicast Gruppen
- PIM IPv4-Hello: Zeigt erweiterte Informationen über PIM-Nachbarn und PIM Hello-State auf IPv4-Interfaces
- PIM IPv6-Hello: Zeigt erweiterte Informationen über PIM-Nachbarn und PIM Hello-State auf IPv6-Interfaces
- PIM IPv4-Neighbors: Zeigt einen kompakten Überblick über PIM-Nachbarn auf IPv4-Interfaces. Optional kann über den Parameter `[-s] [--skip-own-info]` die Ausgabe des eigenen Interfaces in der Ausgabe weggelassen werden.
- PIM IPv6-Neighbors: Zeigt einen kompakten Überblick über PIM-Nachbarn auf IPv6-Interfaces. Optional kann über den Parameter `[-s] [--skip-own-info]` die Ausgabe des eigenen Interfaces in der Ausgabe weggelassen werden.

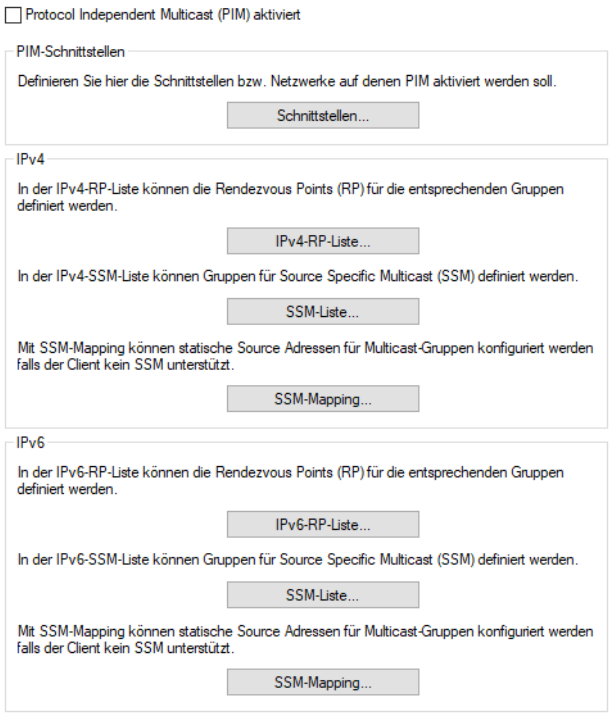
Beispiel für notwendige Konfigurationsschritte

Für ein einfaches Szenario mit PIM SSM sind folgende Konfigurationsschritte notwendig:

1. PIM global aktivieren
2. Für alle Interfaces, die am Multicast-Routing beteiligt sind, inkl. Client-Interfaces und Source-Interface, muss ein Eintrag in der PIM-Schnittstellen-Tabelle erfolgen. Die Default-Werte können übernommen werden.
3. Um SSM zu aktivieren, muss ein Eintrag in der IPv4- bzw. IPv6-SSM-Tabelle angelegt werden. Die Default-Werte können übernommen werden.

Konfiguration

Um PIM mit LANconfig zu konfigurieren, wechseln Sie in die Ansicht **Multicast** > **PIM**.

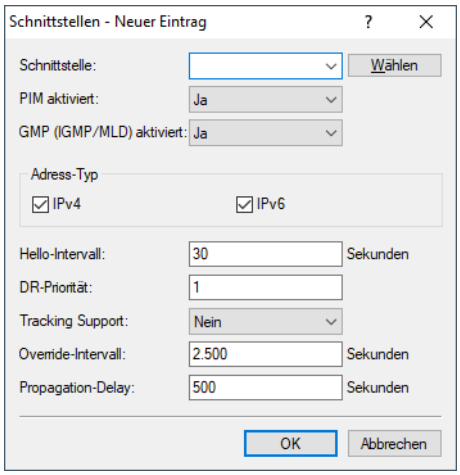


Protocol Independent Multicast (PIM) aktiviert

Aktiviert bzw. deaktiviert PIM auf dem Gerät.

10.5.1 Schnittstellen

In LANconfig konfigurieren Sie die Schnittstellen unter **Multicast** > **PIM** > **PIM-Schnittstellen** über **Schnittstellen**. In dieser Tabelle werden die Interfaces bzw. logischen Netzwerke definiert, auf denen PIM aktiviert werden soll. Ebenso werden die Interfaces definiert, auf denen Clients per IGMP bzw. MLD Multicast-Gruppen beitreten können. Für alle Interfaces, die am Multicast-Routing beteiligt sind, inkl. Client-Interfaces und Source-Interface, muss ein Eintrag in der PIM-Schnittstellen-Tabelle erfolgen.



Schnittstelle

Name des logischen Interfaces auf dem PIM bzw. GMP (Group Management Protokoll wie IGMP oder MLD) aktiviert werden soll. Mögliche Werte sind IPv4-Netzwerke, z. B. INTRANET, WAN-Gegenstellen, Wildcard-Einträge mit * für IPv4-RAS-Interfaces, z. B. „VPN*“. Weitere mögliche Werte sind IPv6-Interfaces sowie IPv6 RAS-Templates.

PIM aktiviert

Aktiviert PIM sowie das Senden und Empfangen von PIM-Nachrichten auf diesem logischen Interface. Wenn nur IGMP- / MLD-Clients bzw. Multicast-Empfänger auf dieser Schnittstelle vorhanden sind, kann somit das Senden bzw. Empfangen von PIM-Nachrichten explizit deaktiviert werden. In diesem Fall muss nur GMP (IGMP / MLD) aktiviert sein.

GMP (IGMP / MLD) aktiviert

Aktiviert die IGMP- bzw. MLD-Routerrolle auf diesem logischen Interface. In diesem Fall werden IGMP- bzw. MLD-Joins von Clients akzeptiert. Auf Interfaces bei denen keine Clients im Netzwerk, sondern nur PIM-Nachbar-Router vorhanden sind, kann GMP deaktiviert werden. IGMP- / MLD-Joins werden in diesem Fall dann nicht akzeptiert.

Adress-Typ

Hier definieren Sie, für welche Adressfamilie PIM bzw. GMP auf diesem Interface aktiviert werden soll. Bei Bedarf können Sie auch beide Adressfamilienn gleichzeitig aktivieren. Mögliche Werte: IPv4, IPv6

Hello-Intervall

Definiert die Zeit in Sekunden zwischen der Wiederholung von regelmäßigen PIM Hello-Nachrichten. Die Haltezeit ist automatisch das 3,5-fache des PIM-Hello-Intervalls und nicht separat konfigurierbar.

Mögliche Werte: 0-255 Sekunden, Default: 30. Der Wert 0 deaktiviert das Senden von Hello-Nachrichten.

DR-Priorität

Definiert die Priorität als Designated Router (DR) im Prozess der DR-Wahl von PIM. Ein höherer Wert bedeutet eine höhere Priorität im DR-Wahlverfahren zum Designated Router (DR). Haben mehrere Router die gleiche (höchste) Priorität, so wird der Router mit der höchsten numerischen IP-Adresse DR.

Mögliche Werte: 0 bis 2^{32}, Default: 1.

Tracking Support

Beeinflusst das Setzen des „T-Bits“ in der LAN-Prune-Delay-Option in ausgehenden Hello-Nachrichten.

Mögliche Werte: Ja, Nein, Default: Nein.

Override Intervall

Beeinflusst das Setzen des Override-Intervall-Felds in der LAN-Prune-Delay-Option in ausgehenden Hello-Nachrichten. Definiert die maximale Verzögerung für die Übertragung von Override-Join-Nachrichten für Multicast-Netzwerke, die Join-Supression aktiviert haben.

Mögliche Werte: 0 bis 2^{32}, Default: 0.

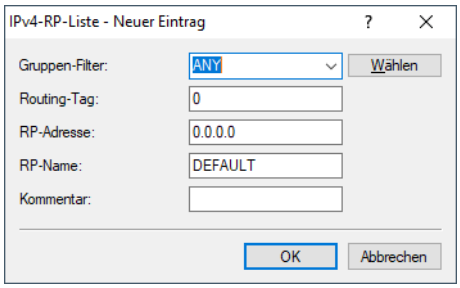
Propagation-Delay

Konfiguriert das Setzen des Propagation-Delay-Felds in gesendeten Hello-Nachrichten der LAN-Prune-Delay-Option. Definiert die Verzögerung für das Versenden von PIM Prune-Nachrichten auf dem Upstream-Router in einem Multicast-Netzwerk, in dem Join-Unterdrückung aktiviert ist.

Mögliche Werte: 250-2000 Millisekunden, Default: 500.

10.5.2 IPv4-RP-Liste

In LANconfig konfigurieren Sie die IPv4-RP-Liste unter **Multicast** > **PIM** > **IPv4** über **IPv4-RP-Liste**. In dieser Tabelle werden die IPv4 Rendezvous Points (RPs) sowie die zugehörigen Multicastgruppen für den PIM Sparse Mode konfiguriert.



Gruppen-Filter

Definiert die Multicast-Gruppen, für die der Rendezvous Points zuständig sein soll. Adressen, die auf den Gruppen-Filter passen, werden von diesem Rendezvous Point verwaltet. Referenziert eine Filterliste aus der Tabelle **Multicast** > **Allgemein** > **IPv4-Filterlisten**.

Routing-Tag

Routing-Tag, das verwendet werden soll um diesen Rendezvous Point zu erreichen.

RP-Adresse

IPv4-Adresse des externen Rendezvous Points. Das Gerät selbst unterstützt nicht die Rolle eines Rendezvous Points.

RP-Name

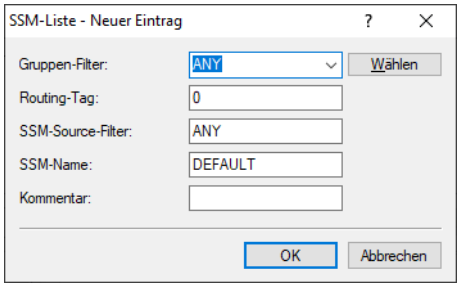
Name des Rendezvous Points.

Kommentar

Vergeben Sie optional einen sinnvollen Kommentar als Beschreibung.

10.5.3 IPv4-SSM-Liste

In LANconfig konfigurieren Sie die IPv4-SSM-Liste unter **Multicast** > **PIM** > **IPv4** über **SSM-Liste**. In dieser Tabelle werden die Parameter für PIM SSM (Source Specific Multicast) Mode konfiguriert.



Gruppen-Filter

Definiert die Multicast-Gruppen, für die diese SSM-Konfiguration gelten soll. Adressen, die auf den Gruppen-Filter passen, werden auf diese SSM-Konfiguration angewendet. Referenziert eine Filterliste aus der Tabelle **Multicast** > **Allgemein** > **IPv4-Filterlisten**.

Routing-Tag

Routing-Tag, für den diese Konfiguration gelten soll.

SSM-Source-Filter

Definiert den SSM-Source-Filter für diesen Tabellen-Eintrag. Nur Multicast-Quell-Adressen, die auf den SSM-Source-Filter passen, werden auf diese SSM-Konfiguration angewendet. Referenziert eine Filterliste aus der Tabelle **Multicast** > **IGMP / MLD** > **Internet Group Management Protocol (IGMP)** > **SSM-Quell-IP-Liste**.

SSM-Name

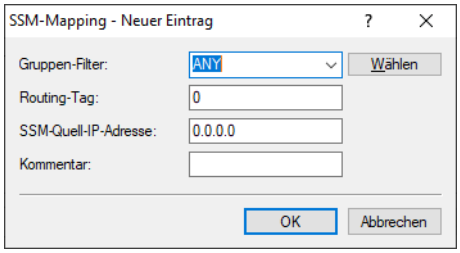
Name dieser SSM-Konfiguration.

Kommentar

Vergeben Sie optional einen sinnvollen Kommentar als Beschreibung.

10.5.4 IPv4-SSM-Mapping

In LANconfig konfigurieren Sie das IPv4-SSM-Mapping unter **Multicast** > **PIM** > **IPv4** über **SSM-Mapping**. In dieser Tabelle können IPv4 Multicast Quell-Adressen (S) konfiguriert werden, die automatisch in PIM-Join-Nachrichten eingefügt werden sollen, falls in empfangenen IGMP-Nachrichten keine Quell-Adressen (S) vorhanden sind. Somit werden (*,G)-Einträge vom Router automatisch zu (S,G)-Einträgen ergänzt.



Gruppen-Filter

Definiert die Multicast-Gruppen (G) für die dieses SSM-Mapping durchgeführt werden soll. Referenziert eine Filterliste aus der Tabelle **Multicast** > **Allgemein** > **IPv4-Filterlisten**.

Routing-Tag

Routing-Tag für das diese Konfiguration gelten soll.

SSM-Quell-IP-Adresse

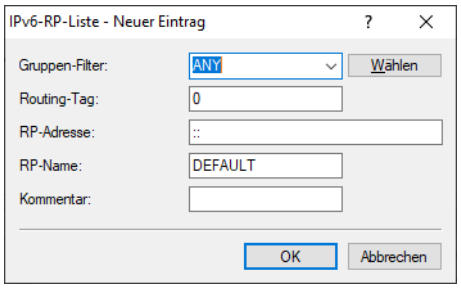
Definiert eine Quell-IPv4-Adresse (S), die automatisch in PIM-Join-Nachrichten für (*,G)-Einträge eingefügt werden soll und automatisch zu (S,G)-Einträge ergänzt werden soll.

Kommentar

Vergeben Sie optional einen sinnvollen Kommentar als Beschreibung.

10.5.5 IPv6-RP-Liste

In LANconfig konfigurieren Sie die IPv6-RP-Liste unter **Multicast** > **PIM** > **IPv6** über **IPv6-RP-Liste**. In dieser Tabelle werden die Rendezvous Points (RPs) sowie die zugehörigen Multicastgruppen für den PIM Sparse Mode konfiguriert.



Gruppen-Filter

Definiert die Multicast-Gruppen, für die der Rendezvous Points zuständig sein soll. Adressen, die auf den Gruppen-Filter passen, werden von diesem Rendezvous Point verwaltet. Referenziert eine Filterliste aus der Tabelle **Multicast** > **Allgemein** > **IPv6-Filterlisten**.

Routing-Tag

Routing-Tag, das verwendet werden soll um diesen Rendezvous Point zu erreichen.

RP-Adresse

IPv6-Adresse des externen Rendezvous Points. Das Gerät selbst unterstützt die Rolle eines Rendezvous Points nicht.

RP-Name

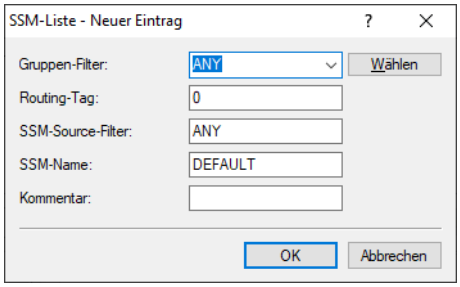
Name des Rendezvous Points.

Kommentar

Vergeben Sie optional einen sinnvollen Kommentar als Beschreibung.

10.5.6 IPv6-SSM-Liste

In LANconfig konfigurieren Sie die IPv6-SSM-Liste unter **Multicast** > **PIM** > **IPv6** über **SSM-Liste**. In dieser Tabelle werden die Parameter für PIM IPv6 SSM (Source Specific Multicast) Mode konfiguriert.



Gruppen-Filter

Definiert die Multicast-Gruppen, für die diese SSM-Konfiguration gelten soll. Adressen, die auf den Gruppen-Filter passen, werden auf diese SSM-Konfiguration angewendet. Referenziert eine Filterliste aus der Tabelle **Multicast** > **Allgemein** > **IPv6-Filterlisten**.

Routing-Tag

Routing-Tag, für den diese Konfiguration gelten soll.

SSM-Source-Filter

Definiert den SSM-Source-Filter für diesen Tabellen-Eintrag. Nur Multicast-Quell-Adressen, die auf den SSM-Source-Filter passen, werden auf diese SSM-Konfiguration angewendet. Referenziert eine Filterliste aus der Tabelle **Multicast** > **IGMP / MLD** > **Internet Group Management Protocol (IGMP)** > **SSM-Quell-IP-Liste**.

SSM-Name

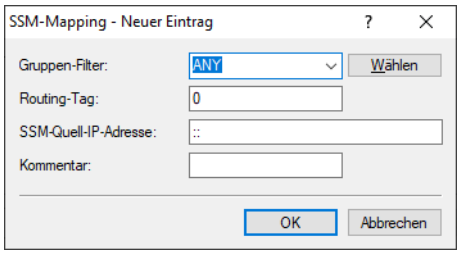
Name dieser SSM-Konfiguration.

Kommentar

Vergeben Sie optional einen sinnvollen Kommentar als Beschreibung.

10.5.7 IPv6-SSM-Mapping

In LANconfig konfigurieren Sie das IPv6-SSM-Mapping unter **Multicast** > **PIM** > **IPv6** über **SSM-Mapping**. In dieser Tabelle können IPv6 Multicast Quell-Adressen (S) konfiguriert werden, die automatisch in PIM-Join-Nachrichten eingefügt werden sollen, falls in empfangenen MLD-Nachrichten keine Quell-Adressen vorhanden sind. Somit werden (*,G) Einträge vom Router automatisch zu (S,G) ergänzt.



Gruppen-Filter

Definiert die Multicast-Gruppen (G) für die dieses SSM-Mapping durchgeführt werden soll. Referenziert eine Filterliste aus der Tabelle **Multicast** > **Allgemein** > **IPv6-Filterlisten**.

Routing-Tag

Routing-Tag für das diese Konfiguration gelten soll.

SSM-Quell-IP-Adresse

Definiert eine Quell-IPv6-Adresse (S), die automatisch in PIM-Join-Nachrichten für (*,G)-Einträge eingefügt werden soll und automatisch zu (S,G)-Einträge ergänzt werden soll.

Kommentar

Vergeben Sie optional einen sinnvollen Kommentar als Beschreibung.

10.6 Weitere Multicast-Protokolle

10.6.1 Bonjour-Proxy

Mit Apple Bonjour haben Endgeräte die Möglichkeit, freigegebene Dienste innerhalb eines lokalen Netzwerkes automatisch und ohne vorherige Konfiguration zu finden und zu verwenden. Dieses Verfahren ist auch bekannt als "Zero Configuration Networking" (ZeroConf).

Zu den gängigsten Diensten zählen z. B.:

- Druckerdienste (mit oder ohne Apple Airprint Unterstützung)
- Dateidienste (Ordner- oder Dateifreigaben)
- Apple Airplay
- iTunes

10.6.1.1 Bonjour-Grundlagen

Bonjour nutzt zum Informationsaustausch einzelne Multicast-DNS-Pakete (mDNS) laut *RFC 6762* und DNS-Based Service Discovery (DNS-SD) laut *RFC 6763*. Dabei tauschen Clients die Bonjour-Informationen über die Multicast-Adresse `224.0.0.251` (IPv4) oder `ff02::fb` (IPv6) auf dem Port 5353 aus. Bonjour-Pakete werden nicht geroutet (Multicast Paket, TTL = 1), was die Nutzung auf das aktuelle lokale Netzwerk beschränkt.

Bitte beachten Sie, dass der Bonjour-Proxy lediglich zum Auffinden von Bonjour-Diensten dient. Für das entsprechende Routing zwischen den Kommunikationspartnern erfolgt eine separate Konfiguration oder Limitierung, z. B. über Routing- oder Firewall-Einträge.

Oft ist es nicht sinnvoll, alle Dienste in einem einzelnen Netzwerk bereitzustellen. Daher werden größere Netzwerke oft in mehrere Subnetze unterteilt. In diesem Fall kann Bonjour allerdings nicht eingesetzt werden.

Anwendungsbeispiel mit zwei Netzwerken

In einer Schule haben Schüler über ein eigenes IP-Netzwerk Zugang zum WLAN. Parallel dazu stehen in einem zweiten internen IP-Netzwerk die lokalen Drucker zur Verfügung. Generell wäre es einem Schüler durch das Routing und die Restriktionen möglich, von seinem Smartphone auf die lokalen internen Drucker zuzugreifen. Weil mDNS allerdings nur Link-Lokal definiert ist, ist es dem Schüler mit seinem Mobiltelefon allerdings nicht möglich, den gewünschten Drucker mit Bonjour zu ermitteln. Der LANCOM Bonjour Proxy fungiert als Vermittler zwischen zwei Netzwerken und ermöglicht es den Schülern somit, Drucker in anderen Netzwerken zu finden.

Grundsätzlich existieren zur Realisierung eines solchen Szenarios zwei Lösungsmöglichkeiten:

Multicast-Routing

Ein Router leitet Suchanfragen und Dienstankündigungen zwischen den Netzwerken weiter.

Diese Option verursacht unnötig Traffic und ist daher wenig effizient.

Caching von Diensten

Der Router speichert entdeckte mDNS-Service-Ankündigungen in seinem lokalen Cache. Erfolgt eine mDNS-Anfrage beim Router, antwortet dieser stellvertretend für den ursprünglichen Dienst. Vor der Verarbeitung der Ankündigung und bevor er aus dem Cache sendet, überprüft der Router anhand von definierten Richtlinien, ob der Dienst akzeptiert (freigegeben) oder verworfen (gesperrt) wird. Die Policies steuern dabei, zwischen welchen Netzen welche Dienste gefunden werden dürfen.

Bitte beachten Sie, dass das Auslesen des mDNS-Cache-Inhalts über das SNMP-Protokoll nicht unterstützt wird.

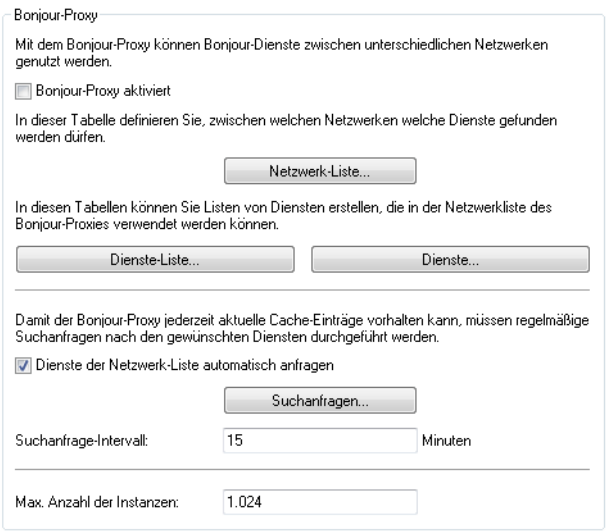
Der Bonjour-Proxy unterstützt einen mDNS-Query-Client, der in festgelegten Zeitintervallen auf einer Schnittstelle bestimmte Dienste abfragt. Diese Abfrage stellt die Aktualität bestimmter Cache-Einträge von freigegebenen Diensten sicher. Damit der Cache stets aktuell gehalten werden kann, ist es sinnvoll, automatische Suchanfragen für die permanent bereitzustellenden Dienste zu aktivieren (z. B. Druckdienste).

Falls Sie für häufig benötigte Dienste keine automatischen Suchanfragen konfigurieren, kann das dazu führen, dass der Bonjour-Proxy entsprechende Suchanfragen nicht beantworten kann, obwohl diese Dienstanbieter aktiviert sind.

Die Verwendung des Bonjour-Proxies ist nur auf logischen LAN / WLAN-Schnittstellen oder in logischen Netzwerken mit einer IP-Adresse möglich. WAN-Schnittstellen / Gegenstellen oder Tunnel (außer WLC L3-Tunnel) sowie VLANs ohne Adressbindung werden nicht unterstützt.

10.6.1.2 Konfiguration mit LANconfig

Die Konfiguration des Bonjour-Proxies nehmen Sie in LANconfig unter **Multicast** > **Bonjour** vor.



In dieser Ansicht stehen Ihnen folgende Einstellungen zur Verfügung:

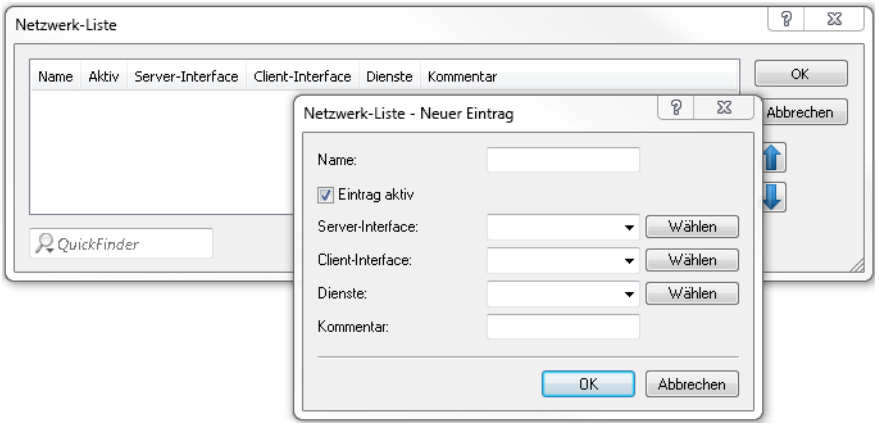
Bonjour-Proxy aktiviert

Aktivieren oder deaktivieren Sie mit dieser Checkbox den Bonjour-Proxy.

Netzwerk-Liste

In dieser Tabelle definieren Sie, zwischen welchen Netzwerken welche Bonjour-Dienste gefunden werden dürfen. Für die ordnungsgemäße Funktionalität ist es erforderlich, dass die Netzwerke oder Schnittstellen mit

einer entsprechenden IPv4- oder IPv6-Adresse konfiguriert sind. Innerhalb der Tabelle haben Sie weitere Einstellungsmöglichkeiten:



Name

Legen Sie einen eindeutigen Namen für diesen Tabelleneintrag fest.

Eintrag aktiv

Aktivieren oder deaktivieren Sie diesen Tabelleneintrag.

Server-Interface

Definieren Sie einen IPv4-Netzwerknamen oder einen IPv6-Interface-Namen, über den Server Bonjour-Dienste (z. B. Druckerdienste) anbieten.

Client-Interface

IPv4-Netzwerkname oder IPv6-Schnittstellen-Name über den Bonjour-Clients Dienste aus dem Server-Netzwerk finden dürfen

Dienste

Referenziert einen Eintrag aus der Dienste-Liste. Clients können nur diese Dienste aus dieser Liste finden. Nicht gelistete Dienste werden abgelehnt.

Wird kein Eintrag konfiguriert, so sind alle Dienste erlaubt.

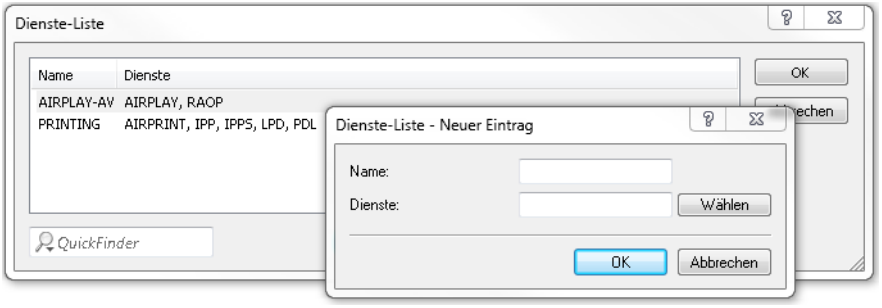
Kommentar

Geben Sie einen Kommentar für diesen Tabelleneintrag ein.

Dienste-Liste

Erstellen Sie in dieser Tabelle eine Liste aus Bonjour-Diensttypen, die in der Bonjour-Netzwerkliste verwendet werden kann.

Hierfür stehen Ihnen folgende Einstellungsmöglichkeiten zur Verfügung:



Name

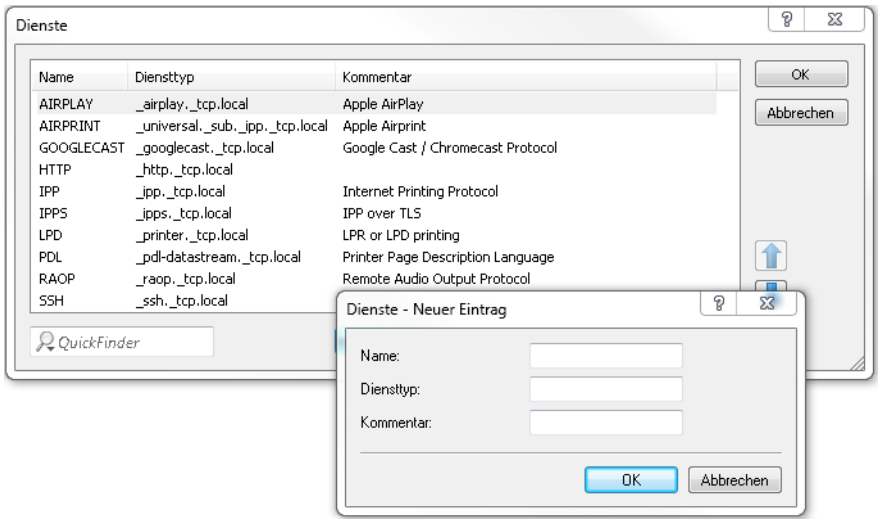
Definieren Sie einen eindeutigen Namen für diesen Tabelleneintrag.

Dienste

Definieren Sie mit einer kommaseparierten Liste die Dienste, die aus der Tabelle **Dienste** verwendet werden sollen.

Dienste

In dieser Tabelle definieren Sie die Typen von Bonjour-Diensten, die in der Dienste-Liste verwendet werden können. Es stehen Ihnen folgende weitere Einstellungsmöglichkeiten zur Verfügung:



Name

Legen Sie einen eindeutigen Namen für diesen Tabelleneintrag fest.

Diensttyp

Geben Sie den Bonjour-Diensttyp als DNS SRV Record an, z. B. `_http._tcp.local`.

Kommentar

Geben Sie einen Kommentar für diesen Tabelleneintrag ein.

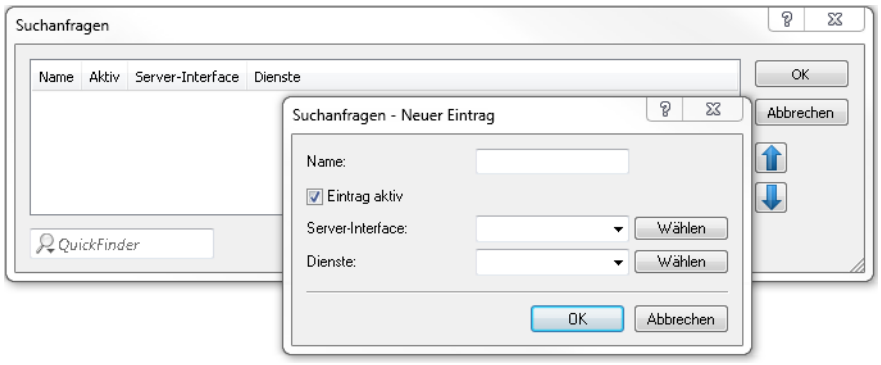
Dienste der Netzwerk-Liste automatisch anfragen

Dieser Eintrag aktiviert das Senden von regelmäßigen Suchanfragen nach den erlaubten Diensten der Netzwerk-Liste auf der entsprechenden Server-Schnittstelle. Als Standardwert ist diese Option aktiviert. Diese Einstellung wird zugleich empfohlen.

Sollte diese Einstellung deaktiviert sein, ist es erforderlich, die abzufragenden Dienste manuell in die Tabelle **Suchanfragen** einzutragen.

Suchanfragen

Damit der Bonjour-Proxy jederzeit aktuelle Dienste im Cache vorhalten kann, ist es erforderlich, dass Sie regelmäßige Suchanfragen nach gewünschten Diensten konfigurieren. Der Query Client fragt in regelmäßigen Abständen die konfigurierten Diensttypen nach deren Verfügbarkeit ab.



Name

Definieren Sie einen eindeutigen Namen für den entsprechenden Eintrag.

Eintrag aktiv

Aktiviert oder deaktiviert diesen Tabelleneintrag.

Server-Interface

Definieren Sie einen IPv4-Netzwerknamen oder einen IPv6-Interface-Namen, über den Server Bonjour-Dienste (z. B. Druckerdienste) anbieten und auf dem regelmäßig durch den Router Suchanfragen durchgeführt werden sollen.

Dienste

Referenziert einen Eintrag aus der Dienste-Liste. Diese Dienste werden regelmäßig durch den Router auf dem Server-Interface angefragt. Dieser Eintrag darf nicht leer sein.

Suchanfrage-Intervall

Legen Sie das Intervall in Minuten fest, in dem der Query-Client die in der Tabelle **Suchanfragen** konfigurierten Bonjour-Dienste abfragt. Als Default sind 15 Minuten definiert.

Max. Anzahl der Instanzen

Definieren Sie die maximale Anzahl an Dienstinstanzen, die der Bonjour-Proxy gleichzeitig speichert.

11 Virtual Private Networks – VPN

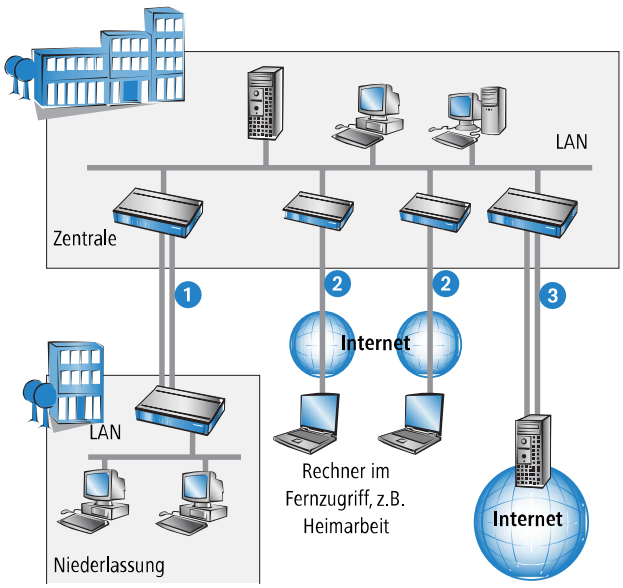
11.1 Welchen Nutzen bietet VPN?

Mit einem VPN (Virtual Private Network) können sichere Datenverkehrsverbindungen über kostengünstige, öffentliche IP-Netze aufgebaut werden, beispielsweise über das Internet.

Was sich zunächst unspektakulär anhört, hat in der Praxis enorme Auswirkungen. Zur Verdeutlichung schauen wir uns zunächst ein typisches Unternehmensnetzwerk ohne VPN-Technik an. Im zweiten Schritt werden wir dann sehen, wie sich dieses Netzwerk durch den Einsatz von VPN optimieren lässt.

11.1.1 Herkömmliche Netzwerkstruktur

Blicken wir zunächst auf eine typische Netzwerkstruktur, die in dieser oder ähnlicher Form in vielen Unternehmen anzutreffen ist:



Das Unternehmensnetz basiert auf einem internen Netzwerk (LAN) in der Zentrale. Dieses LAN ist über folgende Wege mit der Außenwelt verbunden:

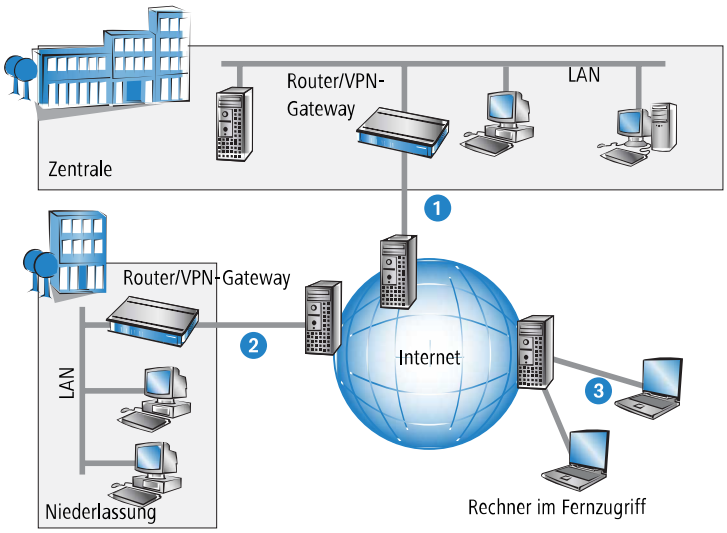
1. Eine Niederlassung ist (typischerweise über eine Standleitung) angeschlossen.
2. Rechner wählen sich über das Internet ins zentrale Netzwerk ein (Remote Access Service – RAS).
3. Es existiert eine Verbindung ins Internet, um den Benutzern des zentralen LAN den Zugriff auf das Web und die Möglichkeit zum Versand und Empfang von E-Mails zu geben.

Alle Verbindungen zur Außenwelt basieren auf dedizierten Leitungen, d. h. Wähl- oder Standleitungen. Dedizierte Leitungen gelten einerseits als zuverlässig und sicher, andererseits aber auch als teuer. Ihre Kosten sind in aller Regel von der Verbindungsdistanz abhängig. So hat es gerade bei Verbindungen über weite Strecken Sinn, nach preisgünstigeren Alternativen Ausschau zu halten.

In der Zentrale muss für jeden verwendeten Zugangs- und Verbindungsweg entsprechende Hardware betrieben werden. Neben den Investitionskosten für diese Ausrüstung fallen auch kontinuierliche Administrations- und Wartungskosten an.

11.1.2 Vernetzung über Internet

Bei Nutzung des Internets anstelle direkter Verbindungen ergibt sich folgende Struktur:



Alle Teilnehmer sind (fest oder per Einwahl) mit dem Internet verbunden. Es gibt keine teuren dedizierten Leitungen zwischen den Teilnehmern mehr.

1. Nur noch die Internet-Verbindung des LANs der Zentrale ist notwendig. Spezielle Einwahlgeräte oder Router für dedizierte Leitungen zu einzelnen Teilnehmern entfallen.
2. Die Niederlassung ist ebenfalls mit einer eigenen Verbindung ans Internet angeschlossen.
3. Die RAS-Rechner wählen sich über das Internet in das LAN der Zentrale ein.

Das Internet zeichnet sich durch geringe Zugangskosten aus. Insbesondere bei Verbindungen über weite Strecken sind gegenüber Wähl- oder Standverbindungen deutliche Einsparungen zu erzielen.

Die physikalischen Verbindungen bestehen nicht mehr direkt zwischen zwei Teilnehmern, sondern jeder Teilnehmer hat selber nur einen Zugang ins Internet. Die Zugangstechnologie spielt dabei keine Rolle: Idealerweise kommen Breitbandtechnologien wie DSL (Digital Subscriber Line) in Verbindung mit Flatrates zum Einsatz.

Die Technologien der einzelnen Teilnehmer müssen nicht kompatibel zueinander sein, wie das bei herkömmlichen Direktverbindungen erforderlich ist. Über einen einzigen Internet-Zugang können mehrere gleichzeitige logische Verbindungen zu verschiedenen Gegenstellen aufgebaut werden.

Niedrige Verbindungskosten und hohe Flexibilität machen das Internet (oder jedes andere IP-Netzwerk) zu einem hervorragenden Übertragungsmedium für ein Unternehmensnetzwerk.

Zwei technische Eigenschaften des IP-Standards stehen allerdings der Nutzung des Internets als Teil von Unternehmensnetzwerken entgegen:

- Die Notwendigkeit öffentlicher IP-Adressen für alle Teilnehmer
- Fehlende Datensicherheit durch ungeschützte Datenübertragung

11.1.3 Private IP-Adressen im Internet?

Der IP-Standard definiert zwei Arten von IP-Adressen: öffentliche und private. Eine öffentliche IP-Adresse hat weltweite Gültigkeit, während eine private IP-Adresse nur in einem abgeschotteten LAN gilt.

Öffentliche IP-Adressen müssen weltweit eindeutig und daher einmalig sein. Private IP-Adressen dürfen weltweit beliebig häufig vorkommen, innerhalb eines abgeschotteten Netzwerkes jedoch nur einmal.

Normalerweise haben Rechner im LAN nur private IP-Adressen, lediglich der Router mit Anschluss ans Internet verfügt auch über eine öffentliche IP-Adresse. Die Rechner hinter diesem Router greifen über dessen öffentliche IP-Adresse auf das Internet zu (IP-Masquerading). In einem solchen Fall ist nur der Router selber über das Internet ansprechbar. Rechner hinter dem Router sind aus dem Internet heraus ohne Vermittlung durch den Router nicht ansprechbar.

11.1.3.1 Routing auf IP-Ebene mit VPN

Soll das Internet zur Kopplung von Netzwerken eingesetzt werden, müssen deshalb IP-Strecken zwischen Routern mit jeweils öffentlicher IP-Adresse eingerichtet werden. Diese Router stellen die Verbindung zwischen mehreren Teilnetzen her. Schickt ein Rechner ein Paket an eine private IP-Adresse in einem entfernten Netzwerksegment, dann setzt der eigene Router dieses Paket über das Internet an den Router des entfernten Netzwerksegments ab.

Das „Einpacken" der Datenpakete mit privaten IP-Adressen in Pakete mit öffentlichen IP-Adressen übernimmt das VPN-Gateway. Ohne VPN können Rechner ohne eigene öffentliche IP-Adresse nicht über das Internet miteinander kommunizieren.

11.1.4 Sicherheit des Datenverkehrs im Internet?

Es existiert Skepsis gegenüber der Idee, Teile der Unternehmenskommunikation über das Internet abzuwickeln. Der Grund für die Skepsis ist die Tatsache, dass sich das Internet dem direkten Einflussbereich des Unternehmens entzieht. Anders als bei dedizierten Verbindungen laufen die Daten durch fremde Netzstrukturen, deren Eigentümer dem Unternehmen häufig unbekannt sind.

Das Internet basiert außerdem nur auf einer simplen Form der Datenübertragung in Form unverschlüsselter Datenpakete. Dritte, durch deren Netze diese Pakete laufen, können sie mitlesen und möglicherweise sogar manipulieren. Der Zugang zum Internet ist für jedermann möglich. Dadurch ergibt sich die Gefahr, dass sich auch Dritte unbefugt Zugang zu den übertragenen Daten verschaffen.

11.1.4.1 VPN – Sicherheit durch Verschlüsselung

Zur Lösung dieses Sicherheitsproblems wird der Datenverkehr zwischen zwei Teilnehmern im VPN verschlüsselt. Während der Übermittlung sind die Daten für Dritte unlesbar.

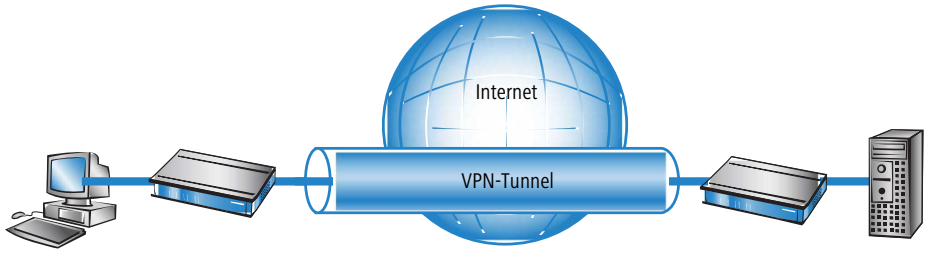
Für die Verschlüsselung kommen die modernsten und sichersten Kryptografieverfahren zum Einsatz. Aus diesem Grund übertrifft die Übertragungssicherheit im VPN das Sicherheitsniveau dedizierter Leitungen bei weitem.

Für die Datenverschlüsselung werden Codes zwischen den Teilnehmern vereinbart, die man üblicherweise als „Schlüssel" bezeichnet. Diese Schlüssel kennen nur die Beteiligten im VPN. Ohne gültigen Schlüssel können Datenpakete nicht entschlüsselt werden. Die Daten bleiben Dritten unzugänglich, sie bleiben „privat".

11.1.4.2 Schicken Sie Ihre Daten in den Tunnel – zur Sicherheit

Jetzt wird auch klar, warum VPN ein virtuelles privates Netz aufbaut: Es wird zu keinem Zeitpunkt eine feste, physikalische Verbindung zwischen den Geräten aufgebaut. Die Daten fließen vielmehr über geeignete Routen durchs Internet. Dennoch ist es unbedenklich, wenn Dritte die übertragenen Daten während der Übertragung abfangen und aufzeichnen. Da die Daten durch VPN verschlüsselt sind, bleibt ihr eigentlicher Inhalt unzugänglich. Experten vergleichen diesen Zustand mit

einem Tunnel: Offen nur am Anfang und am Ende, dazwischen perfekt abgeschirmt. Die sicheren Verbindungen innerhalb eines öffentlichen IP-Netzes werden deshalb auch „Tunnel“ genannt.

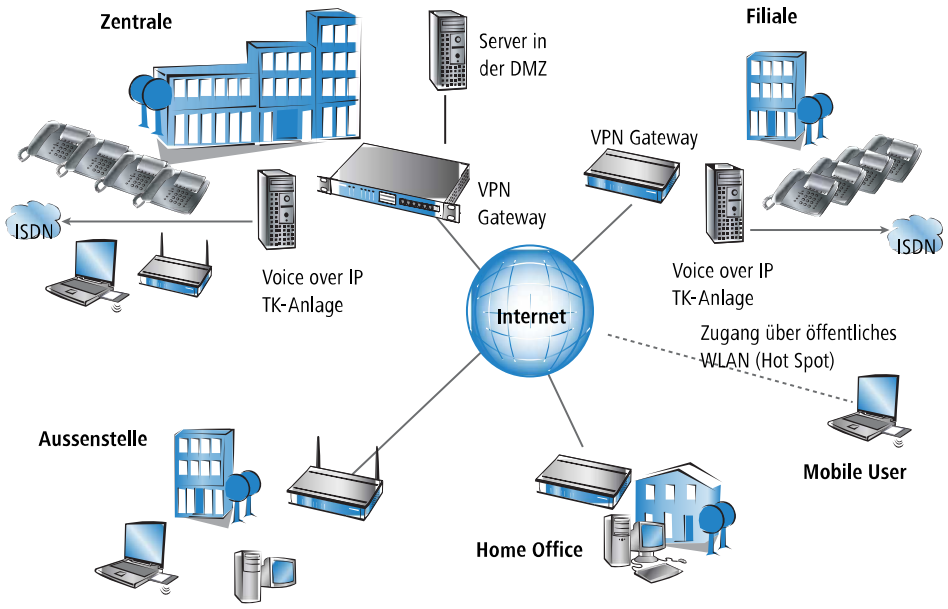


Damit ist das Ziel moderner Netzwerkstrukturen erreicht: Sichere Verbindungen über das größte und kostengünstigste aller öffentlichen IP-Netze: das Internet.

11.2 Das VPN-Modul im Überblick

11.2.1 VPN-Anwendungsbeispiel

VPN-Verbindungen werden in sehr unterschiedlichen Anwendungsgebieten eingesetzt. Meistens kommen dabei verschiedene Übertragungstechniken für Daten und auch Sprache zum Einsatz, die über VPN zu einem integrierten Netzwerk zusammenwachsen. Das folgende Beispiel zeigt eine typische Anwendung, die so oder ähnlich in der Praxis oft anzutreffen ist.



Die wesentlichen Komponenten und Merkmale dieser Anwendungen:

- Kopplung von Netzwerken z. B. zwischen Zentrale und Filiale
- Anbindung von Aussenstellen ohne feste IP-Adressen über VPN-Router
- Anbindung von Home Offices ohne feste IP
- Anbindung an Voice-over-IP-Telefonanlagen
- Anbindung von mobilen Usern, z. B. über öffentliche WLAN-Zugänge

11.2.2 Funktionen des VPN-Moduls

In diesem Abschnitt sind alle Funktionen und Eigenschaften des LCOS-VPN-Moduls aufgelistet. Experten im Bereich VPN bietet er eine stark komprimierte Zusammenfassung über die Leistungsfähigkeit der Funktion. Das Verständnis der verwendeten Fachtermini setzt allerdings solide Kenntnisse über die technischen Grundlagen von VPN voraus. Für die Inbetriebnahme und den Normalbetrieb von VPN sind diese Informationen jedoch nicht erforderlich.

- VPN-Tunnel über Festverbindung, Wählverbindung und IP-Netzwerk
- VPN nach dem IPSec-Standard
- IPSec im Tunnelmodus
- Hash-Algorithmen:
  - HMAC-MD5-96, Hashlänge 128 Bits
  - HMAC-SHA-1-96, Hashlänge 160 Bits
  - HMAC-SHA-256, Hashlänge 256 Bits
  - HMAC-SHA-384, Hashlänge 384 Bits
  - HMAC-SHA-512, Hashlänge 512 Bits
- Schlüsselmanagement nach ISAKMP (IKEv1, IKEv2)
- Symmetrische Verschlüsselungsverfahren
  - AES, Schlüssellänge 128, 192 und 256 Bits
  - Triple-DES (3DES), Schlüssellänge 168 Bits
- IKEv1 Main- und Aggressive-Modus
- IKEv1 / IKEv2 Config Mode
- IKEv1 mit Preshared Keys und IKEv2
- IKEv1 und IKEv2 mit RSA-Signature und digitalen Zertifikaten (X.509)
- Schlüsselaustausch über Oakley, Diffie-Hellman-Algorithmus mit folgenden DH-Gruppen:
  - DH-1 (768-Bit Modulus)
  - DH-2 (1024-Bit Modulus)
  - DH-5 (1536-Bit Modulus)
  - DH-14 (2048-Bit Modulus)
  - DH-15 (3072-Bit Modulus)
  - DH-16 (4096-Bit Modulus)
  - DH-19 (256-bit random ECP group)
  - DH-20 (384-bit random ECP group)
  - DH-21 (521-bit random ECP group)
  - DH-28 (brainpoolP256r1)
  - DH-29 (brainpoolP384r1)
  - DH-30 (brainpoolP512r1)

11.3 VPN-Verbindungen im Detail

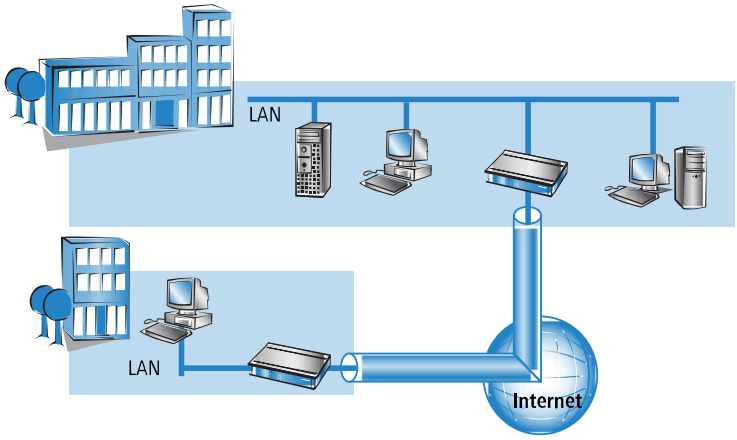
Es existieren zwei Arten von VPN-Verbindungen:

- VPN-Verbindungen zur Kopplung zweier lokaler Netzwerke. Diese Verbindungsart wird auch „LAN-LAN-Kopplung“ genannt.
- Den Anschluss eines einzelnen Rechners mit einem Netzwerk, in der Regel über Einwahlzugänge (Remote Access Service – RAS).

11.3.1 LAN-LAN-Kopplung

Als „LAN-LAN-Kopplung“ wird die Verbindung von zwei entfernten Netzen bezeichnet. Besteht eine solche Verbindung, dann können die Geräte in dem einen LAN auf Geräte des entfernten LANs zugreifen (sofern sie die notwendigen Rechte besitzen).

LAN-LAN-Kopplungen werden in der Praxis häufig zwischen Firmenzentrale und -niederlassungen oder zu Partnerunternehmen aufgebaut.



Auf jeder Seite des Tunnels befindet sich ein VPN-fähiger Router (VPN-Gateway). Die Konfiguration beider VPN-Gateways muss aufeinander abgestimmt sein.

Für die Rechner und sonstigen Geräte in den lokalen Netzwerken ist die Verbindung transparent, d. h., sie erscheint ihnen wie eine gewöhnliche direkte Verbindung. Nur die beiden Gateways müssen für die Benutzung der VPN-Verbindung konfiguriert werden.

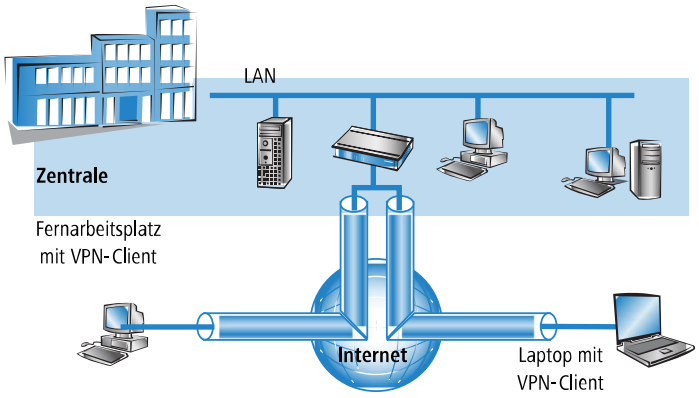
11.3.1.1 Parallele Internet-Nutzung

Die Internet-Verbindung, über die eine VPN-Verbindung aufgebaut wurde, kann weiterhin parallel für herkömmliche Internet-Anwendungen (Web, Mail etc.) verwendet werden. Aus Sicherheitsgründen kann die parallele Internet-Nutzung allerdings auch unerwünscht sein. So beispielsweise, wenn auch die Filiale nur über die zentrale Firewall auf das Internet zugreifen können soll. Für solche Fälle kann die parallele Internet-Nutzung auch gesperrt werden.

11.3.2 Einwahlzugänge (Remote Access Service)

Über Einwahlzugänge erhalten einzelne entfernte Rechner (Clients) Zugriff auf die Ressourcen eines LANs. Beispiele in der Praxis sind Heimarbeitsplätze oder Außendienstmitarbeiter, die sich in das Firmennetzwerk einwählen.

Soll die Einwahl eines einzelnen Rechners in ein LAN über VPN erfolgen, dann wählt sich der einzelne Rechner ins Internet ein. Eine spezielle VPN-Client-Software baut dann auf Basis dieser Internetverbindung einen Tunnel zum VPN-Gateway in der Zentrale auf.



Das VPN-Gateway in der Zentrale muss den Aufbau von VPN-Tunneln mit der VPN-Client-Software des entfernten Rechners unterstützen.

11.4 Was ist LANCOM Dynamic VPN?

LANCOM Dynamic VPN ist eine Technik, die den Aufbau von VPN-Tunneln auch zu solchen Gegenstellen ermöglicht, die keine statische, sondern nur eine dynamische IP-Adresse besitzen.

Wer benötigt LANCOM Dynamic VPN und wie funktioniert es? Die Antwort erfolgt in zwei Schritten: Zunächst zeigt ein Blick auf die Grundlagen der IP-Adressierung das Problem dynamischer IP-Adressen. Der zweite Schritt zeigt die Lösung durch LANCOM Dynamic VPN.

11.4.1 Ein Blick auf die IP-Adressierung

Im Internet benötigt jeder Teilnehmer eine eigene IP-Adresse. Er benötigt sogar eine besondere Art von IP-Adresse, nämlich eine öffentliche IP-Adresse. Die öffentlichen IP-Adressen werden von zentralen Stellen im Internet verwaltet. Jede öffentliche IP-Adresse darf im gesamten Internet nur ein einziges Mal existieren.

Innerhalb lokaler Netzwerke auf IP-Basis werden keine öffentlichen, sondern private IP-Adressen verwendet. Für diesen Zweck wurden einige Nummernbereiche des gesamten IP-Adressraums als private IP-Adressen reserviert.

Einem Rechner, der sowohl an ein lokales Netzwerk als auch direkt an das Internet angeschlossen ist, sind deshalb zwei IP-Adressen zugeordnet: Eine öffentliche für die Kommunkation mit dem Rest des Internets und eine private, unter der er in seinem lokalen Netzwerk erreichbar ist.

11.4.1.1 Statische und dynamische IP-Adressen

Öffentliche IP-Adressen müssen beantragt und verwaltet werden, was mit Kosten verbunden ist. Es gibt auch nur einen begrenzten Vorrat an öffentlichen IP-Adressen. Aus diesem Grund verfügt auch nicht jeder Internet-Benutzer über eine eigene feste (statische) IP-Adresse.

Die Alternative zu statischen IP-Adressen sind die sogenannten dynamischen IP-Adressen. Eine dynamische IP-Adresse wird dem Internet-Benutzer von seinem Internet Service Provider (ISP) bei der Einwahl für die Dauer der Verbindung zugewiesen. Der ISP verwendet dabei eine beliebige unbenutzte Adresse aus seinem IP-Adress-Pool. Die zugewiesene IP-Adresse ist dem Benutzer nur temporär zugewiesen, nämlich für die Dauer der aktuellen Verbindung. Wird die Verbindung gelöst, so wird die zugewiesene IP-Adresse wieder freigegeben, und der ISP kann sie für den nächsten Benutzer verwenden.

Auch bei vielen Flatrate-Verbindungen handelt es sich oftmals um dynamische IP-Adressen. Dabei findet z. B. alle 24h eine Zwangstrennung der Verbindung statt. Nach dieser Zwangstrennung bekommt der Anschluss i.d.R. eine neue, andere IP-Adresse zugewiesen.

11.4.1.2 Vor- und Nachteile dynamischer IP-Adressen

Dieses Verfahren hat für den ISP einen wichtigen Vorteil: Er benötigt nur einen relativ kleinen IP-Adress-Pool. Auch für den Benutzer sind dynamische IP-Adressen günstig: Er muss nicht zuerst eine statische IP-Adresse beantragen, sondern kann sich sofort ins Internet einwählen. Auch die Verwaltung der IP-Adresse entfällt. Dadurch erspart er sich Aufwand und Gebühren. Die Kehrseite der Medaille: Ein Benutzer ohne statische IP-Adresse lässt sich aus dem Internet heraus nicht direkt adressieren.

Für den Aufbau von VPNs ergibt sich daraus ein erhebliches Problem. Möchte beispielsweise Rechner A einen VPN-Tunnel zu Rechner B über das Internet aufbauen, so benötigt er dessen IP-Adresse. Besitzt B nur eine dynamische IP-Adresse, so kennt A sie nicht, er kann B deshalb nicht ansprechen.

Hier bietet die Technik von LANCOM Dynamic VPN die Patentlösung.

11.4.2 So funktioniert LANCOM Dynamic VPN

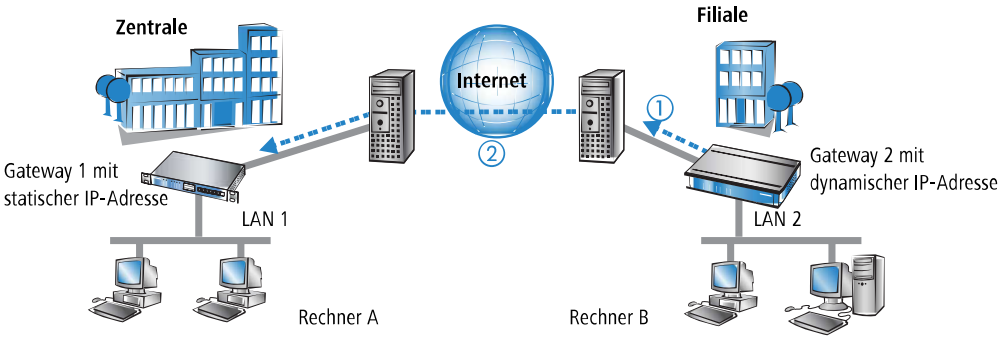
Verdeutlichen wir die Funktionsweise von LANCOM Dynamic VPN an Hand des folgenden Beispiels (Bezeichnungen beziehen sich auf die IP-Adressart der beiden VPN-Gateways):

› dynamisch – statisch

11.4.2.1 Dynamisch – Statisch

Möchte ein Benutzer an Rechner B im LAN 2 eine Verbindung zu Rechner A im LAN 1 aufbauen, dann erhält Gateway 2 die Anfrage und versucht, einen VPN-Tunnel zu Gateway 1 aufzubauen. Gateway 1 verfügt über eine statische IP-Adresse und kann daher direkt über das Internet angesprochen werden.

Problematisch ist, dass die IP-Adresse von Gateway 2 dynamisch zugeteilt wird, und Gateway 2 seine aktuelle IP-Adresse beim Verbindungsaufruf an Gateway 1 übermitteln muss. In diesem Fall sorgt LANCOM Dynamic VPN für die Übertragung der IP-Adresse beim Verbindungsaufbau.



1. Gateway 2 baut eine Verbindung zu seinem Internet-Anbieter auf und erhält eine dynamische IP-Adresse zugewiesen.
2. Gateway 2 spricht Gateway 1 über dessen öffentliche IP-Adresse an. Über Funktionen von LANCOM Dynamic VPN erfolgen Identifikation und Übermittlung der IP-Adresse an Gateway 2. Schließlich baut Gateway 1 den VPN-Tunnel auf.

Der große Vorteil der Geräte bei dieser Anwendung: an Stelle des „Aggressive Mode“, der normalerweise für die Einwahl von VPN-Clients in eine Zentrale verwendet wird, kommt hier der wesentlich sicherere „Main Mode“ zum Einsatz. Beim Main Mode werden in der IKE-Verhandlungsphase deutlich mehr Nachrichten ausgetauscht als im Aggressive Mode.

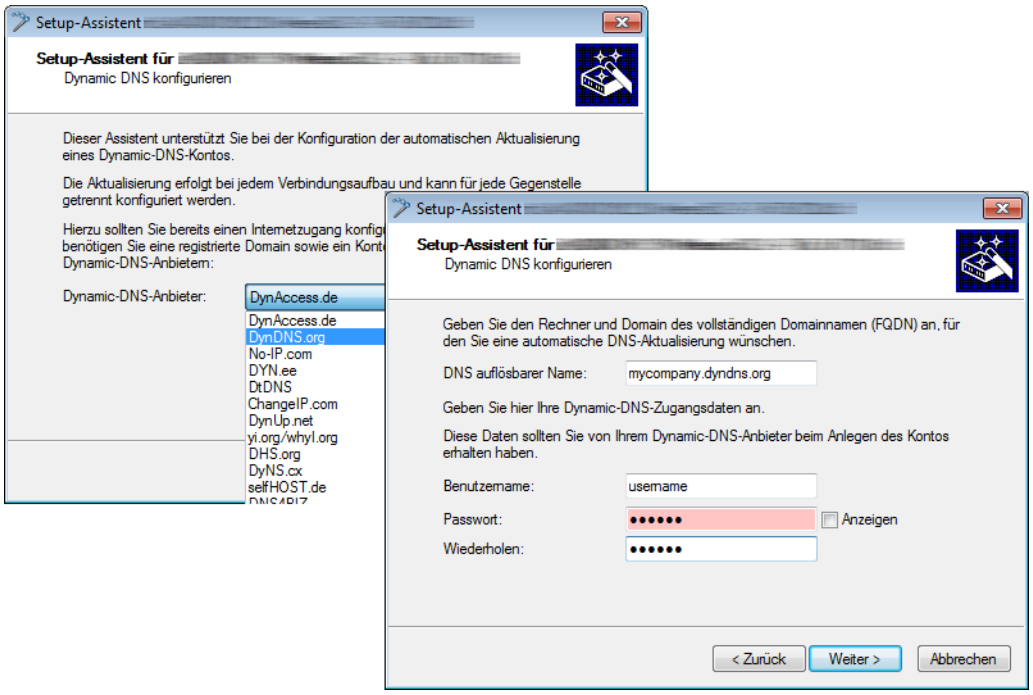
Die dynamische Seite übermittelt ihre IP-Adresse verschlüsselt über das Internet-Protokoll ICMP (alternativ auch über UDP).

11.4.2.2 Dynamische IP-Adressen und DynDNS

Der Verbindungsaufbau zwischen zwei Stationen mit dynamischen IP-Adressen ist ebenfalls unter Verwendung eines so genannten Dynamic-DNS-Dienstes (DynDNS) möglich. Dazu wird die Tunnel-Endpunktadresse nicht in Form einer IP-Adresse angegeben (die ja dynamisch ist und häufig wechselt), sondern in Form eines statischen Namens (z. B. MyDevice@DynDNS.org).

Für die Namensauflösung zu einer jeweils aktuellen IP-Adresse werden zwei Dinge benötigt: Ein Dynamic-DNS-Server und ein Dynamic-DNS-Client:

- Ersterer ist ein Server, wie er von vielen Dienstleistern im Internet angeboten wird und der mit Internet-DNS-Servern in Verbindung steht.
- Der Dynamic-DNS-Client ist im Gerät integriert. Er kann zu einer Vielzahl von Dynamic-DNS-Serviceanbietern Kontakt aufnehmen und bei jeder Änderung seiner IP-Adresse automatisch ein vorher angelegtes Benutzerkonto zur DNS-Namensauflösung beim Dynamic-DNS-Anbieter aktualisieren. Die Einrichtung geschieht komfortabel mit einem Assistenten unter LANconfig:



11.5 Konfiguration von VPN-Verbindungen

Bei der Konfiguration von VPN-Verbindungen werden drei Fragen beantwortet:

- Zwischen welchen VPN-Gateways (Gegenstellen) wird die Verbindung aufgebaut?
- Mit welchen Sicherheitsparametern wird der VPN-Tunnel zwischen den beiden Gateways gesichert?
- Welche Netzwerke bzw. Rechner können über diesen Tunnel miteinander kommunizieren?

In diesem Abschnitt werden die grundsätzlichen Überlegungen zur Konfiguration von VPN-Verbindungen vorgestellt. Dabei bezieht sich die Beschreibung zunächst auf die einfache Verbindung von zwei lokalen Netzwerken. Sonderfälle wie die Einwahl in LANs mit einzelnen Rechnern (RAS) oder die Verbindung von strukturierten Netzwerken werden im weiteren Verlauf dargestellt.

11.5.1 VPN-Tunnel: Verbindungen zwischen den VPN-Gateways

In virtuellen privaten Netzwerken (VPNs) werden lokale Netzwerke über das Internet miteinander verbunden. Dabei werden die privaten IP-Adressen aus den LANs über eine Internet-Verbindung zwischen zwei Gateways mit öffentlichen IP-Adressen geroutet.

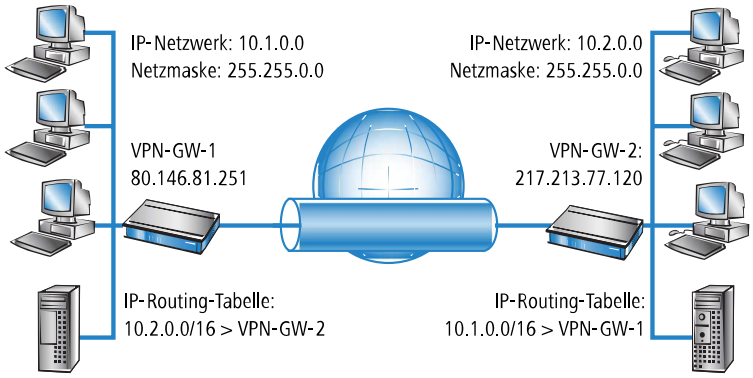
Um das gesicherte Routing der privaten IP-Adressbereiche über die Internet-Verbindung zu ermöglichen, wird zwischen den beiden LANs eine VPN-Verbindung etabliert, die auch als VPN-Tunnel bezeichnet wird.

Der VPN-Tunnel hat zwei wichtige Aufgaben:

- Abschirmen der transportierten Daten gegen den unerwünschten Zugriff von Unbefugten
- Weiterleiten der privaten IP-Adressen über eine Internet-Verbindung, auf der eigentlich nur öffentliche IP-Adressen geroutet werden können.

Die VPN-Verbindung zwischen den beiden Gateways wird durch die folgenden Parameter definiert:

- Die Endpunkte des Tunnels, also die VPN-Gateways, die jeweils über eine öffentliche IP-Adresse (statisch oder dynamisch) erreichbar sind
- Die IP-Verbindung zwischen den beide Gateways
- Die privaten IP-Adressbereiche, die zwischen den VPN-Gateways geroutet werden sollen
- Sicherheitsrelevante Einstellungen wie Passwörter, IPSec-Schlüssel etc. für die Abschirmung des VPN-Tunnels

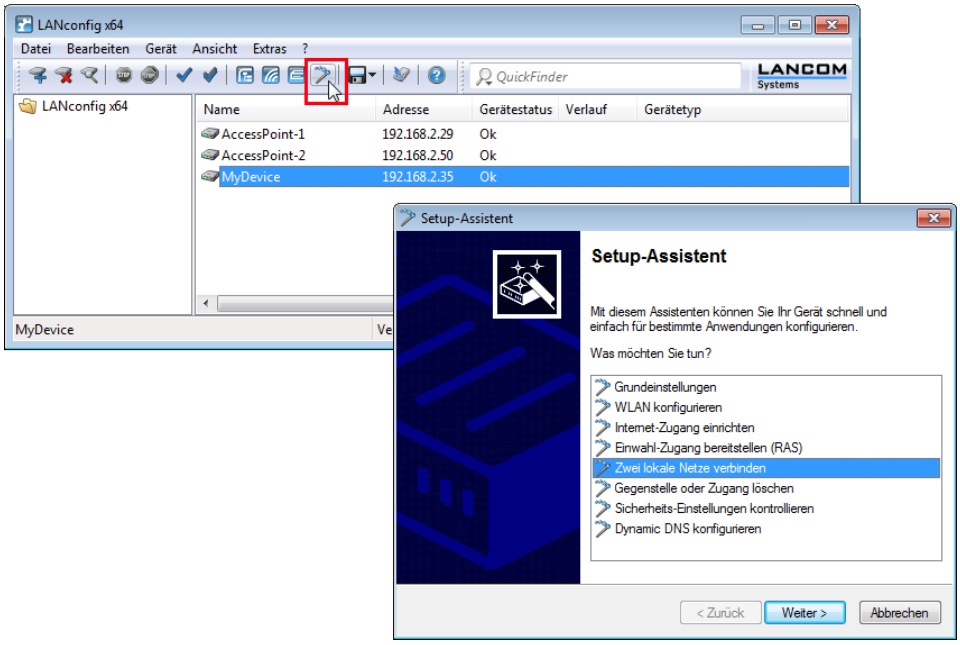


Diese Informationen sind in den so genannten VPN-Regeln enthalten.

11.5.2 VPN-Verbindungen einrichten mit den Setup-Assistenten

Verwenden Sie für die Einrichtung der VPN-Verbindungen zwischen den lokalen Netzen nach Möglichkeit die Setup-Assistenten von LANconfig. Die Assistenten leiten Sie durch die Konfiguration und nehmen alle benötigten Einstellungen vor. Führen Sie die Konfiguration nacheinander an beiden Routern durch.

1. Markieren Sie Ihr Gerät im Auswahlfenster von LANconfig und wählen Sie die Schaltfläche **Setup Assistent** oder aus der Menüleiste den Punkt **Extras** > **Setup Assistent**.



2. Folgen Sie den Anweisungen des Assistenten und geben Sie die notwendigen Daten ein. Der Assistent meldet, sobald ihm alle notwendigen Angaben vorliegen. Schließen Sie den Assistenten dann mit **Fertig stellen** ab.
3. Nach Abschluss der Einrichtung an beiden Routern können Sie die Netzwerkverbindung testen. Versuchen Sie dazu, einen Rechner im entfernten LAN (z. B. mit `ping`) anzusprechen. Das Gerät sollte automatisch eine Verbindung zur Gegenstelle aufbauen und den Kontakt zum gewünschten Rechner herstellen.

Mit diesem Assistenten werden für eine normale LAN-LAN-Kopplung alle notwendigen VPN-Verbindungen automatisch angelegt. Die manuelle Konfiguration der VPN-Verbindungen ist in den folgenden Fällen erforderlich:

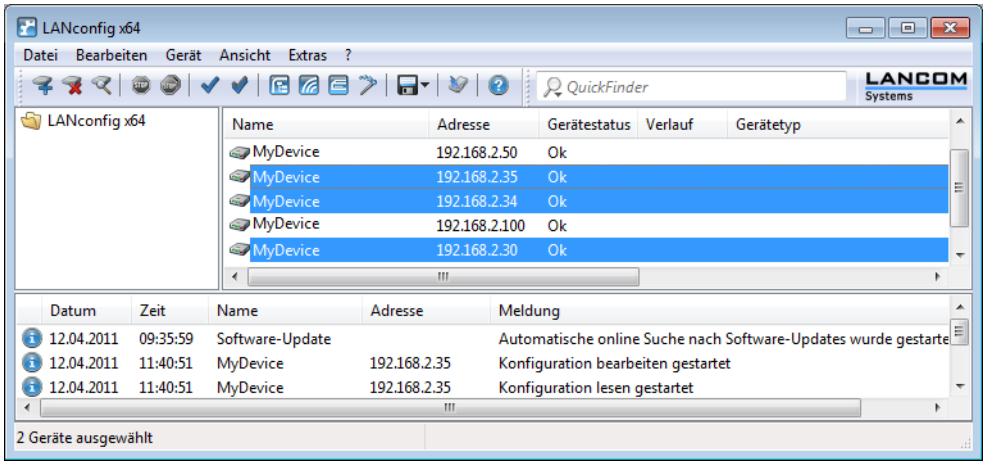
- Wenn kein Windows-Rechner mit LANconfig zur Konfiguration verwendet werden kann. In diesem Fall nehmen Sie die Einstellung der erforderlichen Parameter über WEBconfig oder die Konsole vor.
- Wenn nicht das komplette lokale LAN (Intranet) über die VPN-Verbindung mit anderen Rechnern kommunizieren soll. Das ist z. B. dann der Fall, wenn an das Intranet weitere Subnetze mit Routern angeschlossen sind, oder wenn nur Teile des Intranets auf die VPN-Verbindung zugreifen können sollen. In diesen Fällen werden die Parameter der Setup-Assistenten nachträglich um weitere Einstellungen ergänzt.
- Wenn VPN-Verbindungen zu Fremdgeräten konfiguriert werden sollen.

11.5.3 1-Click-VPN für Netzwerke (Site-to-Site)

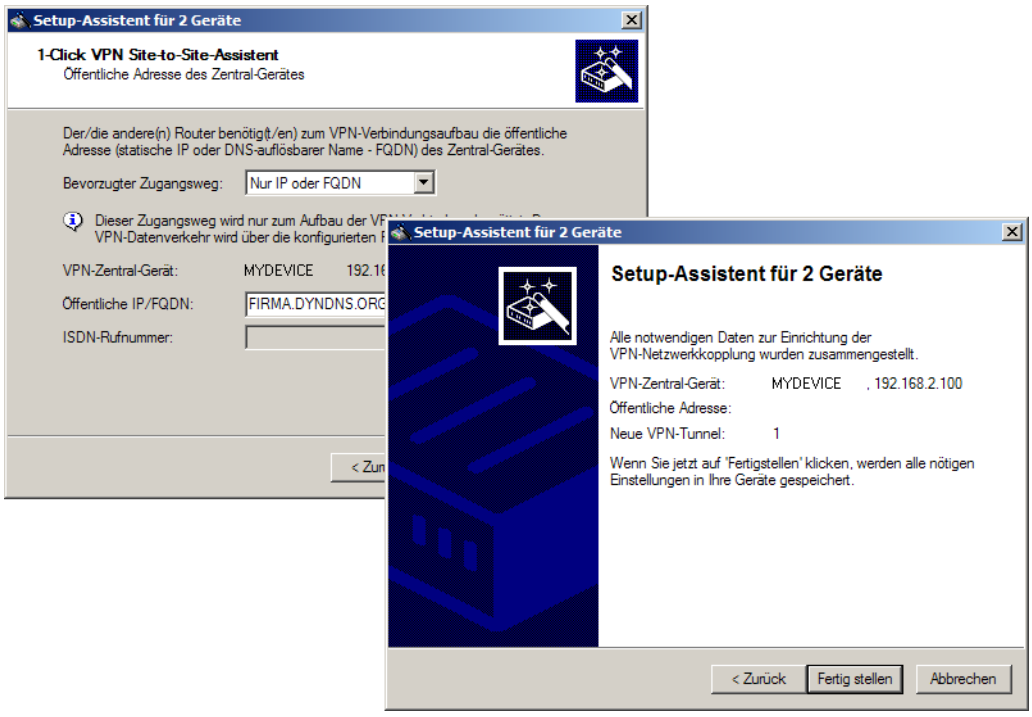
Die Einstellungen für die Kopplung von Netzwerken können sehr komfortabel über den 1-Click-VPN-Assistenten vorgenommen werden. Dabei können sogar mehrere Router gleichzeitig an ein zentrales Netzwerk gekoppelt werden.

1. Markieren Sie in LANconfig die Router der Filialen, für die Sie eine VPN-Kopplung zu einem zentralen Router einrichten möchten.

2. Ziehen Sie die Geräte mit der Maus auf den Eintrag für den zentralen Router.



3. Der 1-Click-VPN Site-to-Site-Assistent startet. Geben Sie den Namen für diesen Zugang ein und wählen Sie aus, über welche Adresse der Router aus dem Internet erreichbar ist.



4. Wählen Sie aus, ob der Verbindungsaufbau über den Namen bzw. die IP-Adresse des zentralen Routers erfolgen soll. Geben Sie dazu die Adresse bzw. den Namen des zentralen Routers an.
5. Im letzten Schritt legen Sie fest, wie die verbundenen Netzwerke untereinander kommunizieren können:
   - Nur das INTRANET der Zentrale wird für die Außenstellen verfügbar gemacht werden.
   - Alle privaten Netze der Außenstellen können ebenfalls über die Zentrale untereinander verbunden werden.

Alle Eingaben werden nur einmal für das Zentralgerät vorgenommen und dann in den Geräteeigenschaften hinterlegt.

11.5.4 1-Click-VPN für LANCOM Advanced VPN Client

VPN-Zugänge für Mitarbeiter, die sich mit Hilfe des LANCOM Advanced VPN Client in ein Netzwerk einwählen, lassen sich sehr einfach mit dem Setup-Assistenten erstellen und in eine Datei exportieren, die vom LANCOM Advanced VPN Client als Profil eingelesen werden kann. Dabei werden die erforderlichen Informationen der aktuellen Konfiguration des VPN-Routers entnommen und mit zufällig ermittelten Werten ergänzt (z. B. für den Preshared Key).

1. Starten Sie über LANconfig den Setup-Assistenten **Zugang bereitstellen** und wählen Sie die **VPN-Verbindung**.
2. Aktivieren Sie die Optionen **LANCOM Advanced VPN Client** und **Beschleunigen Sie das Konfigurieren mit 1-Click-VPN**.
3. Geben Sie den Namen für diesen Zugang ein und wählen Sie aus, über welche Adresse der Router aus dem Internet erreichbar ist.
4. Im letzten Schritt können Sie wählen, wie die neuen Zugangsdaten ausgegeben werden sollen:
   - Profil als Importdatei für den LANCOM Advanced VPN Client speichern
   - Profil per E-Mail versenden
   - Profil ausdrucken

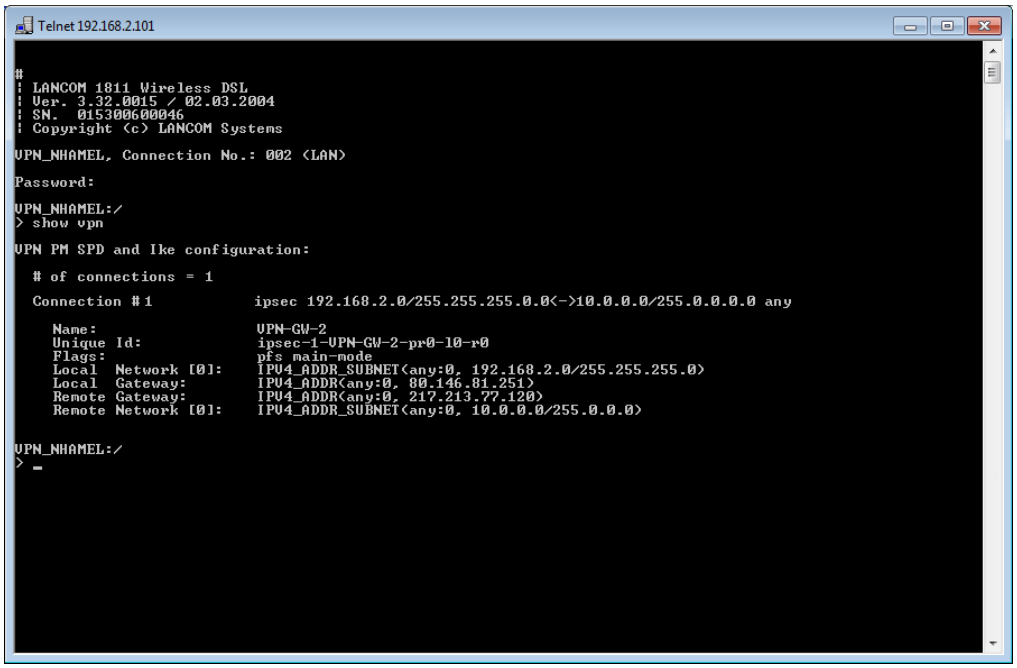
   Das Versenden der Profildatei per E-Mail stellt ein Sicherheitsrisiko dar, weil die E-Mail unterwegs ggf. abgehört werden könnte! Zum Versenden der Profildatei per E-Mail muss in der Konfiguration des Geräts ein SMTP-Konto mit den erforderlichen Zugangsdaten eingerichtet sein. Außerdem muss auf dem Konfigurationsrechner ein E-Mail-Programm als Standard-Mail-Anwendung eingerichtet sein, über die auch andere Anwendungen E-Mails versenden dürfen.

Beim Erstellen des VPN-Zugangs werden Einstellungen verwendet, die optimal auf die Verwendung im LANCOM Advanced VPN Client abgestimmt sind, darunter z. B.:

- Gateway: Sofern im VPN-Router definiert, wird hier ein DynDNS-Name verwendet, ansonsten die IP-Adresse.
- FQUN: Kombination aus dem Namen der Verbindung, einer fortlaufenden Nummer und der internen Domäne im VPN-Router.
- Domäne: Sofern im VPN-Router definiert, wird hier die interne Domäne verwendet, ansonsten ein DynDNS-Name oder die IP-Adresse.
- VPN IP-Netze: Alle im Gerät definierten IP-Netzwerke vom Typ 'Intranet'.
- Preshared Key: Zufällig generierter Schlüssel mit einer Länge von 16 ASCII-Zeichen.
- Verbindungsmedium: Für den Verbindungsaufbau wird das LAN genutzt.
- VoIP-Priorisierung: Die VoIP-Priorisierung ist voreingestellt.
- Exchange Mode: Als Exchange-Mode wir der 'Aggressive Mode' verwendet.
- IKE-Config-Mode: Der IKE-Config-Mode ist aktiviert, die IP-Adress-Informationen für den LANCOM Advanced VPN Client werden automatisch vom VPN-Router zugewiesen.

11.5.5 VPN-Regeln einsehen

Die Informationen über die aktuellen VPN-Regeln im Gerät können Sie über die Telnet-Konsole abrufen. Stellen Sie dazu eine Telnet-Verbindung zu dem VPN-Gateway her und geben Sie an der Konsole den Befehl `show vpn` ein:



In der Ausgabe finden Sie die Informationen über die Netzbeziehungen, die für den Aufbau von VPN-Verbindungen zu anderen Netzwerken in Frage kommen.

In diesem Fall wird das lokale Netzwerk einer Filiale (Netzwerk `192.168.2.0` mit der Netzmaske `255.255.255.0`) und das Netz der Zentrale (Netzwerk `10.0.0.0` mit der Netzmaske `255.0.0.0`) angebunden. Die öffentliche IP-Adresse des eigenen Gateways lautet `80.146.81.251`, die des entfernten VPN-Gateways ist die `217.213.77.120`.

Die Angabe `any:0` zeigt die über die Verbindung erlaubten Protokolle und Ports an.

Eine erweiterte Ausgabe wird über den Befehl `show vpn long` aufgerufen. Hier finden Sie neben den Netzbeziehungen auch die Informationen über die sicherheitsrelevanten Parameter wie IKE- und IPSec-Proposals.

11.5.6 Manuelles Einrichten der VPN-Verbindungen

Beim manuellen Einrichten der VPN-Verbindungen fallen die schon beschriebenen Aufgaben an:

- Definition der Tunnelendpunkte
- Definition der sicherheitsrelevanten Parameter (IKE und IPSec)
- Definition der VPN-Netzbeziehungen, also der zu verbindenden IP-Adressbereiche. Bei überschneidenden IP-Netzbereichen auf den beiden Seiten der Verbindung bitte auch den Abschnitt beachten.
- Bei Nutzung von LANCOM Dynamic VPN: Eintrag für die entsprechende Gegenstelle in der PPP-Liste mit einem geeigneten Passwort für die Dynamic VPN Verhandlung. Als Benutzername ist derjenige VPN-Verbindungsname einzutragen, unter dem das Gerät in der VPN-Verbindungsliste der entfernten Gegenstelle angesprochen wird. Aktivieren Sie das „IP Routing“.

Als Tunnelendpunkt wird neben dem eigenen, lokalen VPN-Gateway jeweils eine VPN-Gegenstelle in der VPN-Verbindungsliste eingetragen.

Die manuelle Konfiguration der VPN-Verbindungen umfasst die folgenden Schritte:

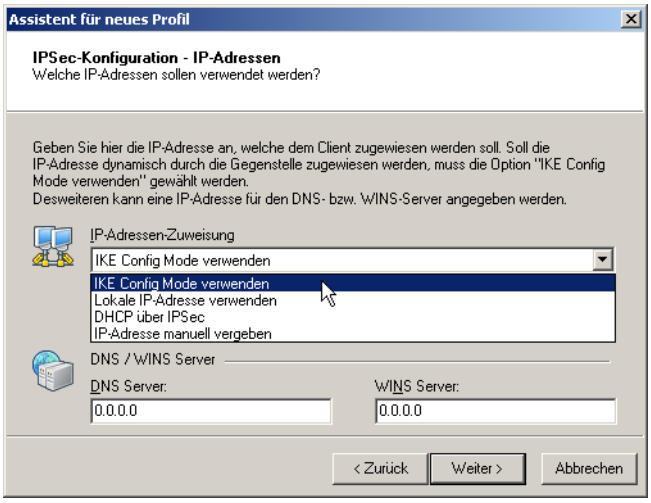
1. Legen Sie das entfernte VPN-Gateway in der Verbindungsliste an und tragen Sie dabei die öffentlich erreichbare Adresse ein.
2. Die Sicherheitsparameter für die VPN-Verbindung werden in der Regel aus den vorbereiteten Listen entnommen, hier besteht neben der Definition eines IKE-Schlüssels kein weiterer Handlungsbedarf.
3. Bei einer Dynamic VPN-Verbindung erzeugen Sie einen neuen Eintrag in der PPP-Liste mit dem Namen des entfernten VPN-Gateways als Gegenstelle, mit dem Namen des lokalen VPN-Gateways als Benutzername und einem geeigneten Passwort. Für diese PPP-Verbindung aktivieren Sie auf jeden Fall das IP-Routing. Die restlichen PPP-Parameter wie das Verfahren für die Überprüfung der Gegenstelle können analog zu anderen PPP-Verbindungen definiert werden.
4. Die Hauptaufgabe bei der Einrichtung von VPN-Verbindungen liegt schließlich in der Definition der Netzbeziehungen: Welche IP-Adressbereiche sollen auf den beiden Seiten des VPN-Tunnels in die gesicherte Verbindung einbezogen werden?

11.5.7 IKE Config Mode

Bei der Konfiguration von VPN-Einwahlzugängen kann alternativ zur festen Vergabe der IP-Adressen für die einwählenden Gegenstellen auch ein Pool von IP-Adressen angegeben werden. In den Einträgen der Verbindungsliste wird dazu der „IKE-CFG"-Modus angegeben. Dieser kann die folgenden Werte annehmen:

- **Server**: In dieser Einstellung fungiert das Gerät als Server für diese VPN-Verbindung. Für die Zuweisung der IP-Adresse an den Client gibt es zwei Möglichkeiten:
  - Wenn die Gegenstelle in der Routing-Tabelle eingetragen ist, wird ihr die dort konfigurierte IP-Adresse zugewiesen.
  - Wenn die Gegenstelle nicht in der Routing-Tabelle eingetragen ist, wird eine freie IP-Adresse aus dem IP-Pool für die Einwahlzugänge entnommen.

  Die Gegenstelle muss dabei als IKE-CFG-Client konfiguriert sein und so vom Server eine IP-Adresse für die Verbindung anfordern. Für die Einwahl mit einem LANCOM Advanced VPN Client aktivieren Sie im Verbindungsprofil die Option **IKE Config Mode verwenden**.



- **Client**: In dieser Einstellung fungiert das Gerät als Client für diese VPN-Verbindung und fordert eine IP-Adresse für die Verbindung von der Gegenstelle (Server) an. Das Gerät verhält sich also so ähnlich wie ein VPN-Client.

- **Aus**: Ist der IKE-CFG-Modus ausgeschaltet, werden keine IP-Adressen für die Verbindung zugewiesen. Auf beiden Seiten der VPN-Strecke muss fest konfiguriert sein, welche IP-Adressen für diese Verbindung zu verwenden sind.



LANconfig: **VPN** > **IKE/IPSec** > **Verbindungs-Liste**

Konsole: **Setup** > **VPN** > **VPN-Gegenstellen**

11.5.8 Diagnose der VPN-Verbindungen

Wenn die VPN-Verbindungen nach der Konfiguration der entsprechenden Parameter nicht wie gewünscht zustande kommen, stehen folgende Möglichkeiten zur Diagnose zur Verfügung:

- Mit dem Befehl `show vpn spd` an der Konsole rufen Sie die „Security Policy Definitions“ auf.
- Mit dem Befehl `show vpn sadb` rufen Sie die Informationen über die ausgehandelten „Security Associations“ (SAs) auf.
- Mit dem Befehl `trace + vpn` [status, packet] können Sie die Status- und Fehlermeldungen der aktuellen VPN-Verhandlung aufrufen.
  - Die Fehlermeldung „No proposal chosen“ deutet auf einen Fehler in der Konfiguration der Gegenstelle hin.
  - Die Fehlermeldung „No rule matched“ deutet hingegen auf einen Fehler in der Konfiguration des lokalen Gateways hin.

In der Standardeinstellung behält das Gerät VPN-Fehlermeldungen in der Statustabelle. Nach einiger Zeit zeigt der LANmonitor je nach Installation sehr viele offene Fehlermeldungen an, was die Anzeige unübersichtlich macht. Sie haben deshalb an der Konsole unter **Setup** > **Config** > **Error-Aging-Minutes** die Möglichkeit, eine Zeitspanne in Minuten zu definieren, nach der das Gerät diese Fehlermeldungen automatisch aus der Statustabelle entfernt.

Um sporadisch auftretende Fehler zu dokumentieren, deaktivieren Sie diese Option mit dem Eintrag `0`.

11.6 Einsatz von digitalen Zertifikaten

Die Sicherheit der Kommunikation über VPN erfüllt im Kern drei Anforderungen:

- Vertraulichkeit: Die übertragenen Daten können durch Verschlüsselung von keinem Unbefugten gelesen werden.
- Integrität: Die Daten können während der Übertragung nicht unbemerkt verändert werden (über Authentifizierung).
- Authentizität: Der Empfänger kann sicher sein, dass die empfangenen Daten auch tatsächlich vom vermuteten Absender stammen (über Authentifizierung).

Für die Verschlüsselung und Authentifizierung von Daten stehen zahlreiche Verfahren zur Verfügung, mit denen die beiden ersten Aspekte – Vertraulichkeit und Integrität – ausreichend abgedeckt werden können. Der Einsatz von digitalen Zertifikaten verfolgt das Ziel, auch die Authentizität der Kommunikationspartner zu sichern.

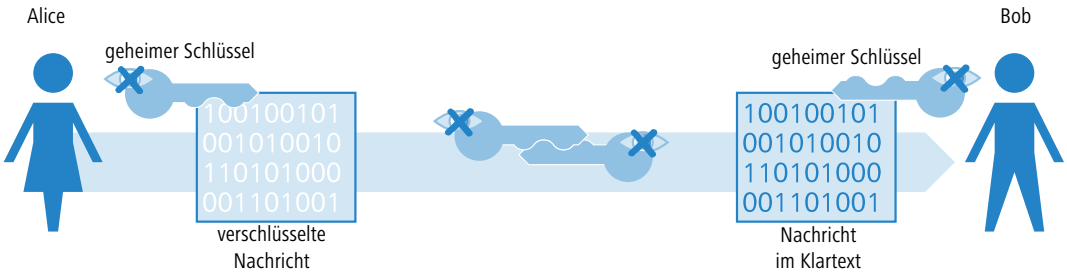
11.6.1 Grundlagen

Verschlüsselungsverfahren kann man in zwei Kategorien einteilen: Die symmetrische und die asymmetrische Verschlüsselung.

11.6.1.1 Die symmetrische Verschlüsselung

Die symmetrische Verschlüsselung ist seit Jahrtausenden bekannt und basiert darauf, dass sowohl der Sender als auch der Empfänger einer Nachricht über einen gemeinsamen, geheimen Schlüssel verfügen. Dieser Schlüssel kann sehr unterschiedliche Gestalt haben: Die Römer verwendeten zum Ver- und Entschlüsseln z. B. einen Stab mit einem ganz bestimmten Durchmesser.

In der heutigen digitalen Kommunikation handelt es sich bei dem Schlüssel meist um ein besonderes Passwort. Mit Hilfe dieses Passwortes und eines Verschlüsselungsalgorithmus werden die Daten vom Sender verändert. Der Empfänger verwendet den gleichen Schlüssel und einen passenden Entschlüsselungsalgorithmus, um die Daten wieder lesbar zu machen. Jede andere Person, die den Schlüssel nicht kennt, kann die Daten nicht lesen. Ein übliches symmetrisches Verschlüsselungsverfahren ist z. B. 3DES.



Beispiel:

1. Alice möchte Bob eine vertrauliche Nachricht zukommen lassen. Dazu verschlüsselt sie die Nachricht mit einem geheimen Schlüssel und einem geeigneten Verfahren, z. B. 3DES. Die verschlüsselte Nachricht schickt sie an Bob und teilt ihm dabei mit, welches Verschlüsselungsverfahren sie verwendet hat.
2. Bob verfügt über den gleichen Schlüssel wie Alice. Da er von Alice nun auch das Verschlüsselungsverfahren kennt, kann er die Nachricht entschlüsseln und in den Klartext zurückverwandeln.

Die symmetrische Verschlüsselung ist sehr einfach und effizient in der Handhabung, hat aber zwei gravierende Nachteile:

- Für jede geheime Kommunikationsbeziehung wird ein eigener Schlüssel benötigt. Wenn neben Alice und Bob noch Carol dazukommt, werden schon drei Schlüssel benötigt, um die jeweiligen Datenübertragungen untereinander

abzusichern, bei vier Teilnehmern sechs Schlüssel, bei 12 Teilnehmern 66 und bei 1000 Teilnehmern schon fast 500.000! In einem weltweiten Netz mit immer höheren Anforderungen an die gesicherte Kommunikation zahlreicher Teilnehmer wird das schon zu einem ernsthaften Problem.

- Während der erste Nachteil mit Hilfe der Technik evtl. zu lösen wäre, ist der Zweite ein Kernproblem der symmetrischen Verschlüsselung: Der geheime Schlüssel muss auf beiden Seiten der Datenübertragung bekannt sein und darf nicht in unbefugte Hände geraten. Alice kann den Schlüssel also nicht einfach per E-Mail an Bob schicken, bevor die Datenverbindung ausreichend gesichert ist, wozu genau dieser Schlüssel beitragen soll. Sie müsste den Schlüssel schon persönlich an Bob übergeben oder ihn zumindest über ein *abhörsicheres* Verfahren übermitteln. Diese Aufgabe ist in Zeiten weltweiter dynamischer Datenkommunikation kaum zu bewältigen.

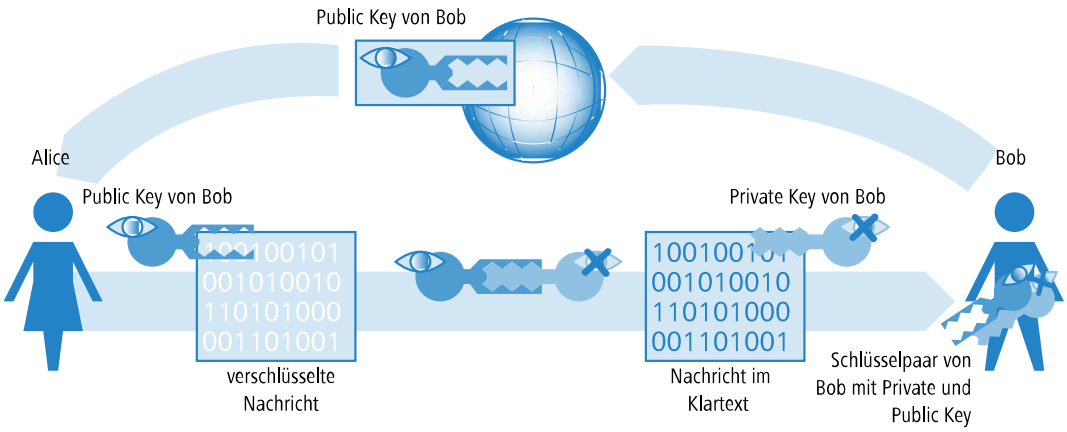
11.6.1.2 Das Verfahren der asymmetrischen Verschlüsselung

Als grundlegend neuer Ansatz wurde in den 1970er Jahren die asymmetrische Verschlüsselung entwickelt. Diese Variante setzt nicht mehr auf einen Schlüssel, der auf beiden Seiten bekannt und dabei geheim ist, sondern auf ein Schlüsselpaar:

- Der erste Teil des Schlüsselpaares wird zum **Ver**schlüsseln der Daten verwendet, die zum Eigentümer des Schlüssels gesendet werden. Dieser öffentliche Schlüssel (oder im Folgenden Public Key genannt) darf weltweit allen Interessenten öffentlich zur Verfügung gestellt werden.
- Der zweite Teil des Schlüsselpaares ist der private Schlüssel Private Key), der nur zum **Ent**schlüsseln der empfangenen Botschaften verwendet wird. Dieser Schlüssel ist geheim und darf nicht in die Hände Unbefugter geraten.

Der große Unterschied gegenüber den symmetrischen Verschlüsselungen: Es wird ein öffentlich bekannter Schlüssel verwendet, daher spricht man hier auch vom „Public-Key-Verfahren". Ein bekanntes asymmetrisches Verschlüsselungsverfahren ist z. B. RSA.

Sehen wir uns wieder das Beispiel von Alice und Bob an:



- Bob erzeugt für die gesicherte Kommunikation zunächst ein Schlüsselpaar mit einem Private Key und einem Public Key, die genau zueinander passen. Beim Erstellen dieser Schlüssel wird ein Verfahren verwendet, mit dem der Private Key nicht aus dem Public Key zurückgerechnet werden kann. Den Public Key kann Bob jetzt unbedenklich öffentlich bekannt machen. Er kann ihn per Mail an Alice schicken oder einfach auf seinem Webserver ablegen.
- Alice verschlüsselt nun die Nachricht an Bob mit dessen Public Key. Die so unkenntlich gemachte Botschaft kann nur noch mit dem Private Key von Bob entschlüsselt werden. Selbst wenn die Daten auf dem Weg von Alice zu Bob mitgehört werden, kann niemand außer Bob den Klartext entziffern!

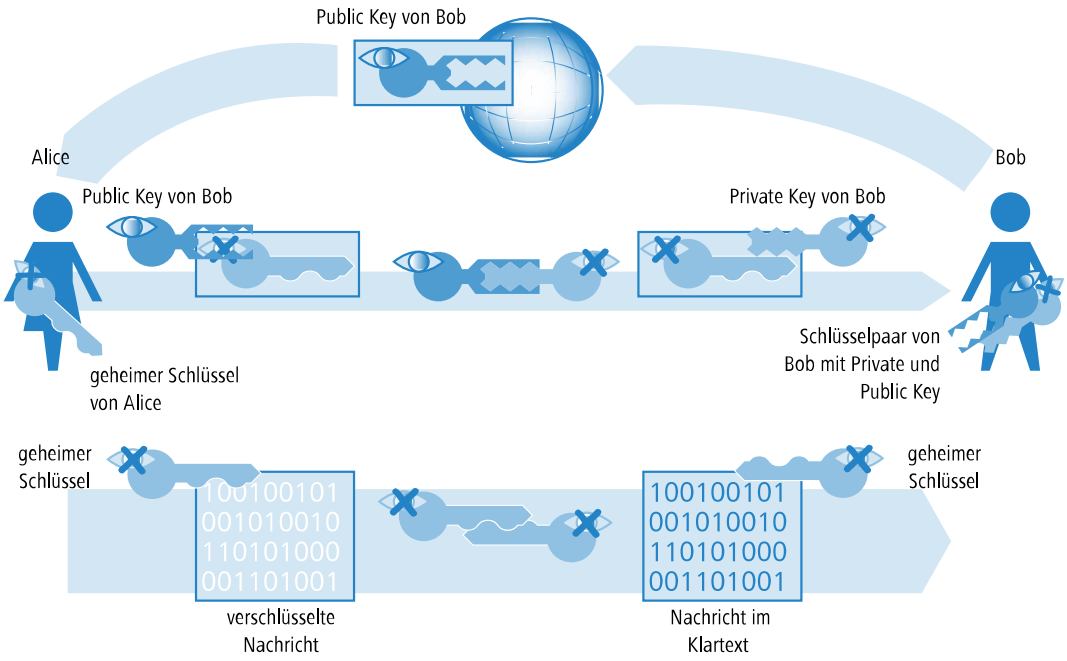
Die asymmetrische Verschlüsselung bietet gegenüber der symmetrischen Variante folgende Vorteile:

- Es wird nicht für jede Kommunikationsbeziehung ein Schlüsselpaar benötigt, sondern nur für jeden Teilnehmer. Bei 1000 Teilnehmern benötigt jeder nur sein eigenes Schlüsselpaar, von dem er den Public Key öffentlich zur Verfügung stellt. Anstelle der 500.000 geheimen Schlüssel werden beim Public Key-Verfahren also nur 1000 Schlüsselpaare verwendet.
- Die unsichere Übertragung des geheimen Schlüssels an die Kommunikationspartner entfällt, da nur der Public Key auf der jeweils anderen Seite der Kommunikationsbeziehung bekannt sein muss. Damit wird ein wesentliches Problem bei der dynamischen Verschlüsselung von Daten zwischen vielen Teilnehmern gelöst.

11.6.1.3 Kombination von symmetrischer und asymmetrischer Verschlüsselung

Aufgrund Ihrer Sicherheit konnten sich asymmetrische Verschlüsselungsverfahren schnell etablieren. Doch hat die Sicherheit auch Ihren Preis: Asymmetrische Verschlüsselungsverfahren sind langsam. Die mathematischen Verfahren zum Ver- und Entschlüsseln von Nachrichten sind sehr viel aufwändiger als bei symmetrischen Verschlüsselungsverfahren und brauchen daher auch mehr Rechenzeit, was bei der Übertragung von großen Datenmengen zum Ausschlusskriterium wird.

Die Vorteile von symmetrischer und asymmetrischer Verschlüsselung können in einer geeigneten Kombination ausgenutzt werden. Dabei wird die sichere asymmetrische Verschlüsselung dazu verwendet, die Übertragung des geheimen Schlüssels zu schützen. Die eigentlichen Nutzdaten der Verbindung werden anschließend mit den schnelleren symmetrischen Verfahren verschlüsselt.



1. Bob erstellt im ersten Schritt sein Schlüsselpaar und stellt den Public Key öffentlich bereit.
2. Alice verwendet den Public Key, um damit einen geheimen, symmetrischen Schlüssel zu **ver**schlüsseln und schickt ihn an Bob. Dieser geheime Schlüssel wird bei jeder Übertragung durch ein Zufallsverfahren neu bestimmt.
3. Nur Bob kann den geheimen Schlüssel nun wieder mit Hilfe seines Private Keys **ent**schlüsseln.
4. Alice und Bob verwenden dann den geheimen Schlüssel zum **Ver**- und **Ent**schlüsseln der deutlich größeren Nutzdaten-Volumina.

11.6.1.4 Public-Key-Infrastruktur

Die Kombination von symmetrischen und asymmetrischen Verschlüsselungsverfahren erlaubt es, auch über zunächst ungesicherte Verbindungen eine sichere Datenkommunikation aufzubauen. Dabei wurde bisher der Aspekt der Authentizität nicht beleuchtet: Woher weiß Alice, dass der verwendete Public Key auch tatsächlich von Bob stammt? Die Verwendung von Public-Keys hängt also vom Vertrauen an die Authentizität der Kommunikationspartner ab.

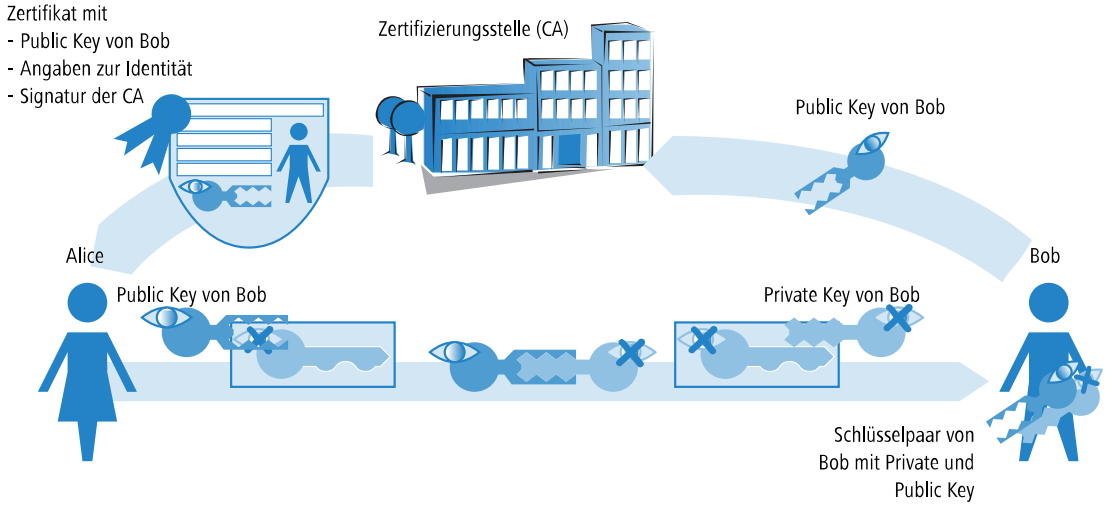
Um dieses Vertrauen zu sichern, können die verwendeten Schlüsselpaare der asymmetrischen Verschlüsselung von öffentlich anerkannten, vertrauenswürdigen Stellen bestätigt werden. So ist z. B. in Deutschland die Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen die oberste vertrauenswürdige Instanz bei der Bestätigung von digitalen Schlüsseln. Diese wiederum vergibt Akkreditierungen an geeignete Dienstleister, die ebenfalls als vertrauenswürdig angesehen werden.

Auf der Webseite der Bundesnetzagentur (*www.bundesnetzagentur.de*) finden Sie ständig aktuelle Listen mit akkreditierten Zertifizierungsdiensteanbietern sowie Hinweise auf widerrufene Akkreditierungen. Unter den akkreditierten Dienstleistern befinden sich z. B. zahlreiche Steuerberater und Anwaltskammern.

Die Aufgabe dieser Stellen ist es, einen Public Key genau einer Person oder Organisation zuzuordnen. Diese Zuordnung wird in einem bestimmten Dokument – einem Zertifikat – festgehalten und öffentlich bekannt gemacht. Diese Anbieter werden daher auch als Zertifizierungsstellen bezeichnet, im Englischen als „Certification Authority" oder kurz CA bezeichnet. Die oberste Zertifizierungsstelle gilt als die Stamm oder Wurzel-CA bzw. Root-CA.

An eine solche CA kann sich Bob nun wenden, wenn er seinen Public Key für seine eigene Person zertifizieren lassen möchte. Dazu reicht er seinen Public Key bei der CA ein, die die Zugehörigkeit des Schlüssels zu Bob bestätigt.

Die CA stellt über diese Bestätigung ein Zertifikat aus, das neben dem Public Key von Bob auch weitere Angaben u. a. über seine Identität enthält.



Das Zertifikat selbst wird von der CA wiederum signiert, damit auch die Bestätigung nicht angezweifelt werden kann. Da das Zertifikat nur aus einer kleinen Datenmenge besteht, kann dazu ein asymmetrisches Verfahren verwendet werden. Bei der Signatur wird das asymmetrische Verfahren jedoch in umgekehrter Richtung eingesetzt:

1. Auch die CA verfügt über ein Schlüsselpaar aus Private und Public Key. Als vertrauenswürdige Stelle kann ihr eigenes Schlüsselpaar als zuverlässig angesehen werden.
2. Die CA berechnet einen Hash-Wert über das Zertifikat, verschlüsselt diesen und signiert damit das Zertifikat von Bob. Dadurch wird die Zuordnung von Bobs Public Key zu seiner Identität bestätigt.

   Dieser Vorgang verhält sich genau umgekehrt wie bei der normalen asymmetrischen Verschlüsselung. Hier hat die Verschlüsselung aber nicht die Aufgabe, die Daten vor Unbefugten zu sichern, sondern die Signatur der CA zu bestätigen.
3. Jeder Teilnehmer einer Datenkommunikation weltweit ist nun mit dem Public Key der CA in der Lage, das so signierte Zertifikat zu überprüfen.

   Nur die CA kann mit ihrem eigenen Private Key Signaturen erzeugen, die mit dem Public Key der CA wieder entschlüsselt werden können. Durch diese Signatur ist sichergestellt, dass das Zertifikat tatsächlich von der ausstellenden CA stammt.

11.6.2 Vorteile von Zertifikaten

Die Verwendung von Zertifikaten zur Absicherung von VPN-Verbindungen bietet sich in manchen Fällen als Alternative zum sonst eingesetzten Preshared-Key-Verfahren (PSK-Verfahren) an:

- Sicherere VPN-Client-Verbindungen (mit IKE Main Mode)

  Beim PSK-Verbindungsaufbau von Peers mit dynamischen IP-Adressen kann der Main Mode nicht eingesetzt werden. Hier muss der Aggressive Mode mit geringerer Sicherheit verwendet werden. Der Einsatz von Zertifikaten erlaubt auch bei Peers mit dynamischen IP-Adressen wie z. B. Einwahlrechnern mit LANCOM Advanced VPN Client die Verwendung des Main Mode und damit eine Steigerung der Sicherheit.
- Höhere Sicherheit der verwendeten Schlüssel bzw. Kennwörter

Preshared Keys sind genau so anfällig wie alle anderen Kennwörter auch. Der Umgang der Anwender mit diesen Kennwörtern („menschlicher Faktor") hat also erheblichen Einfluss auf die Sicherheit der Verbindungen. Bei einem zertifikatsbasierten VPN-Aufbau werden die in den Zertifikaten verwendeten Schlüssel automatisch mit der gewünschten Schlüssellänge erstellt. Darüber hinaus sind die von Rechnern erstellten, zufälligen Schlüssel auch bei gleicher Schlüssellänge sicherer gegen Angriffe (z. B. Wörterbuchangriffe) als die von Menschen erdachten Preshared Keys.

- Prüfung der Authentizität der Gegenseite möglich

  Beim VPN-Verbindungsaufbau über Zertifikate müssen sich die beiden Gegenstellen authentifizieren. In den Zertifikaten können dabei weitere Info-Elemente enthalten sein, die zur Prüfung der Gegenstellen herangezogen werden. Die zeitliche Befristung der Zertifikate gibt zusätzlichen Schutz z. B. bei der Vergabe an Anwender, die nur vorübergehend Zugang zu einem Netzwerk erhalten sollen.

- Unterstützung von Tokens und Smartcards

  Mit der Auslagerung der Zertifikate auf externe Datenträger gelingt auch die Integration in „Strong Security"-Umgebungen, das Auslesen von Kennwörtern aus Computern wird verhindert.

Den Vorteilen von Zertifikaten steht allerdings der höhere Aufwand für die Einführung und Pflege einer Public Key Infrastructure (PKI) gegenüber.

11.6.3 Aufbau von Zertifikaten

11.6.3.1 Inhalte

Um seinen Aufgaben gerecht werden zu können, enthält ein Zertifikat diverse Informationen. Einige davon sind verpflichtend, andere sind optional. Es gibt verschiedene Formate, in denen ein Zertifikat gespeichert werden kann. Ein Zertifikat nach dem X.509-Standard beinhaltet z. B. folgende Informationen:

- Version: Dieser Eintrag enthält die Version des X.509-Standards. Z. B. war 06/2005 die Version 'v3' aktuell.
- Serial Number: Eine eindeutige Seriennummer, über die ein Zertifikat identifiziert werden kann.
- Signature Algorithm: Identifiziert den Algorithmus, mit dem der Aussteller das Zertifikat unterschreibt. Außerdem findet sich hier die digitale Unterschrift des Ausstellers.
- Validity: Zertifikate sind zeitlich begrenzt gültig. Validity enthält Informationen über die Dauer.
- Issuer: Daten zur Identifizierung des Ausstellers, z. B. Name, E-Mail-Adresse, Nationalität etc.
- Subject: Daten zur Identifizierung des Eigentümers des Zertifikates, z. B. Name, Institution, E-Mail-Adresse, Nationalität, Stadt etc.
- Subject Public Key: Informationen, welches Verfahren zum Generieren des öffentlichen Schlüssels des Zertifikatsinhabers verwendet wurde. Außerdem findet sich unter diesem Punkt der Public Key des Eigentümers.

11.6.3.2 Zielanwendung

Bei der Erstellung der Zertifikate wird üblicherweise ausgewählt, für welchen Zweck die Zertifikate eingesetzt werden können. Manche Zertifikate sind gezielt nur für Webbrowser oder E-Mail-Übertragung gedacht, andere sind allgemein für beliebige Zwecke einsetzbar.

Achten Sie bei der Erstellung der Zertifikate darauf, dass sie für den gewünschten Zweck ausgestellt werden.

11.6.3.3 Formate

Für die Form der Zertifikate ist der ITU-Standard X.509 weit verbreitet. In Textdarstellung sieht ein solches Zertifikat z. B. wie folgt aus:

```
Certificate:
 Data:
 Version: 3 (0x2)
 Serial Number: 1 (0x1)
 Signature Algorithm: md5WithRSAEncryption
 Issuer: CN=CA/Email=ca@trustme.dom, OU=Certificate Authority, O=TrustMe Ltd, ST=Austria, L=Graz, C=XY,
 Validity
 Not Before: Oct 29 17:39:10 2000 GMT
```

```
Not After : Oct 29 17:39:10 2001 GMT
Subject: CN=anywhere.com/Email=xyz@anywhere.com, OU=Web Lab, O=Home, L=Vienna, ST=Austria, C=DE
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public Key: (1024 bit)
Modulus (1024 bit):
00:c4:40:4c:6e:14:1b:61:36:84:24:b2:61:c0:b5:
d7:e4:7a:a5:4b:94:ef:d9:5e:43:7f:c1:64:80:fd:
9f:50:41:6b:70:73:80:48:90:f3:58:bf:f0:4c:b9:
90:32:81:59:18:16:3f:19:f4:5f:11:68:36:85:f6:
1c:a9:af:fa:a9:a8:7b:44:85:79:b5:f1:20:d3:25:
7d:1c:de:68:15:0c:b6:bc:59:46:0a:d8:99:4e:07:
50:0a:5d:83:61:d4:db:c9:7d:c3:2e:eb:0a:8f:62:
8f:7e:00:e1:37:67:3f:36:d5:04:38:44:44:77:e9:
f0:b4:95:f5:f9:34:9f:f8:43
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Subject Alternative Name:
email:xyz@anywhere.com
Netscape Comment:
mod_ssl generated test server certificate
Netscape Cert Type:
SSL Server
Signature Algorithm: md5WithRSAEncryption
12:ed:f7:b3:5e:a0:93:3f:a0:1d:60:cb:47:19:7d:15:59:9b:
3b:2c:a8:a3:6a:03:43:d0:85:d3:86:86:2f:e3:aa:79:39:e7:
82:20:ed:f4:11:85:a3:41:5e:5c:8d:36:a2:71:b6:6a:08:f9:
cc:1e:da:c4:78:05:75:8f:9b:10:f0:15:f0:9e:67:a0:4e:a1:
4d:3f:16:4c:9b:19:56:6a:f2:af:89:54:52:4a:06:34:42:0d:
d5:40:25:6b:b0:c0:a2:03:18:cd:d1:07:20:b6:e5:c5:1e:21:
44:e7:c5:09:d2:d5:94:9d:6c:13:07:2f:3b:7c:4c:64:90:bf:
ff:8e
```

11.6.3.4 Dateitypen

Digitale Zertifikate und Private Keys liegen je nach Aussteller mit verschiedenen Dateiendungen vor. Üblich sind z. B. die Endungen:

- *.pfx und *.p12: PKCS#12-Dateien
- *.pem, *.cer und *.crt: BASE-64-codierte Zertifikate
- *.cer, *.crt und *.der: DER-codierte Zertifikate
- *.key: BASE64- oder DER-codierte Schlüssel
- *.pvk: Microsoft-spezifisches Schlüsselformat

Im Umfeld der zertifikatsgesicherten VPN-Verbindungen ist neben den reinen Zertifikaten noch ein weiterer Dateityp von großer Bedeutung: die PKCS#12-Dateien, in denen mehrere Komponenten enthalten sein können, u. a. ein Zertifikat und ein Private Key. Zur Verarbeitung der PKCS#12-Dateien ist ein Kennwort erforderlich, das beim Exportieren der Zertifikate festgelegt wird.



BASE64-codierte Zertifikate tragen im Header üblicherweise die Zeile:

```
----- BEGIN CERTIFICATE -----
```

11.6.3.5 Gültigkeit

Darüber hinaus kann optional ein Verweis auf eine so genannte Certificate Revocation List (CRL) eingefügt werden. In CRL's sind Zertifikate aufgelistet, die ungültig geworden sind, z. B. weil ein Mitarbeiter eine Firma verlassen hat und sein Zertifikat deshalb zurückgezogen wurde. Mit dieser Angabe kann bei der Prüfung der Zertifikate die richtige CRL verwendet werden.

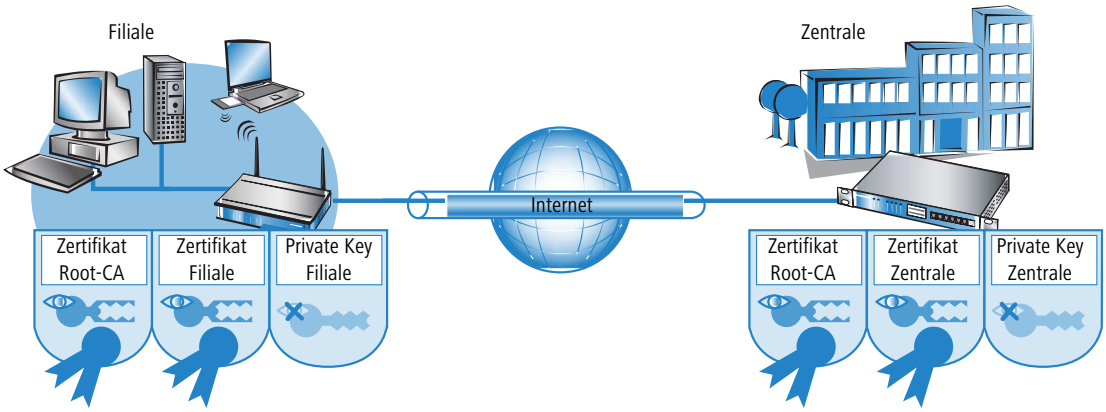
11.6.4 Sicherheit

Auch beim Umgang mit Zertifikaten sind bestimmte Sicherheitsaspekte zu beachten:

- Übertragen Sie die Private Keys nur über sichere Verbindungen, z. B. mit HTTPS.
- Verwenden Sie als Kennwörter für Schlüssel oder PKCS#12-Dateien nur ausreichend lange und sichere Passphrasen.

11.6.5 Zertifikate beim VPN-Verbindungsaufbau

Neben den grundlegenden Informationen zum Thema Zertifikate betrachten wir in diesem Abschnitt die konkrete Anwendung beim VPN-Verbindungsaufbau. Für einen solchen Verbindungsaufbau mit Zertifikatsunterstützung müssen auf beiden Seiten der Verbindung (z. B. Anbindung einer Filiale an das Netzwerk der Zentrale über einen Router) bestimmte Informationen vorhanden sein:



- Die Filiale verfügt über folgende Komponenten:
  - Zertifikat der Root-CA mit dem Public Key der CA
  - Eigenes Geräte-Zertifikat mit dem eigenen Public Key und der Bestätigung der Identität. Die Prüfsumme dieses Zertifikats ist mit dem Private Key der CA signiert.
  - Eigener Private Key
- Die Zentrale verfügt über folgende Komponenten:
  - Zertifikat der Root-CA mit dem Public Key der CA
  - Eigenes Geräte-Zertifikat mit dem eigenen Public Key und der Bestätigung der Identität. Die Prüfsumme dieses Zertifikats ist mit dem Private Key der CA signiert.
  - Eigener Private Key

Beim VPN-Verbindungsaustausch laufen vereinfacht dargestellt im Main Mode folgende Vorgänge ab (in beide Richtungen symmetrisch):

1. In einem ersten Paketaustausch handeln die Peers z. B. die verwendeten Verschlüsselungsmethoden und die Verfahren zur Authentifizierung aus. In dieser Phase haben beide Seiten noch keine gesicherte Kenntnis darüber, mit wem sie gerade verhandeln, das ist jedoch bis zu diesem Zeitpunkt nicht notwendig.
2. Im nächsten Schritt wird ein gemeinsames Schlüsselmaterial für die weitere Verwendung ausgehandelt, darin u. a. symmetrische Schlüssel und asymmetrische Schlüsselpaare. Auch in diesem Zustand können beide Seiten noch nicht sicher sein, mit wem sie die Schlüssel ausgehandelt haben.
3. Im nächsten Schritt wird mit Hilfe der Zertifikate geprüft, ob der Peer aus der Verhandlung des Schlüsselmaterials auch tatsächlich der beabsichtigte Kommunikationspartner ist:
   - Die Filiale errechnet aus dem Schlüsselmaterial der aktuellen Verhandlung eine Prüfsumme (Hash), die lediglich die beiden beteiligten Peers (Filiale und Zentrale) berechnen können, und dies auch nur, während diese Verbindung besteht.
   - Diesen Hash verschlüsselt die Filiale mit dem eigenen Private Key und erzeugt damit eine Signatur.
   - Diese Signatur übermittelt die Filiale zusammen mit dem eigenen Zertifikat dem Peer in der Zentrale.
   - Die Zentrale prüft dann die Signatur für das empfangene Zertifikat der Filiale. Das kann sie mit Hilfe des Public Keys im Root-CA, welcher in beiden Peers identisch vorhanden ist. Kann die Signatur aus dem Filialen-Zertifikat (erstellt mit dem Private Key der CA) mit dem Public Key der CA entschlüsselt werden, dann ist die Signatur gültig und dem Zertifikat kann vertraut werden.

- Im nächsten Schritt prüft die Zentrale dann die Signatur der verschlüsselten Prüfsumme. Der Public Key der Filiale aus dem entsprechenden Zertifikat wurde im vorigen Schritt für gültig befunden. Daher kann die Zentrale prüfen, ob die signierte Prüfsumme mit dem Public Key der Filiale entschlüsselt werden kann. Die Zentrale kann die gleiche Prüfsumme aus dem Schlüsselmaterial der aktuellen Verbindung berechnen wie die Filiale. Wenn diese Prüfung erfolgreich ist, kann der Peer „Filiale" als authentifiziert angesehen werden.

11.6.6 Zertifikate von Zertifikatsdiensteanbietern

Die von öffentlichen Zertifikatsstellen angebotenen Zertifikate können in der Regel in verschiedenen Sicherheitsklassen beantragt werden. Mit höherer Sicherheit steigt dabei jeweils der Aufwand des Antragstellers, sich gegenüber der CA mit seiner Identität zu authentifizieren. Die Trustcenter AG in Hamburg verwendet z. B. die folgenden Klassen:

- Class 0: Diese Zertifikate werden ohne Prüfung der Identität ausgestellt und dienen nur zu Testzwecken für Geschäftskunden.
- Class 1: Hier wird nur die Existenz einer E-Mail-Adresse geprüft. Diese Stufe eignet sich für private Anwender, die z. B. Ihre E-Mails signieren möchten.
- Class 2: Auch in dieser Stufe findet keine persönliche Identitätsprüfung statt. Die Übersendung eines Antrags mit einer Kopie z. B. eines Handelsregisterauszugs ist ausreichend. Diese Stufe eignet sich daher für die Kommunikation zwischen Unternehmen, die vorher untereinander bekannt sind.
- Class 3: In dieser Stufe wird die Person oder das Unternehmen persönlich überprüft. Dabei werden die Angaben in dem ausgestellten Zertifikat mit denen im Pass bzw. einer beglaubigten Kopie des Handelsregisterauszugs verglichen. Diese Stufe eignet sich für fortgeschrittene Anwendungen z. B. im e-Business oder Online-Banking.

Wenn Sie mit einem öffentlichen Zertifikatsdiensteanbieter zusammenarbeiten, prüfen Sie genau die angebotenen Sicherheitsstufen bzgl. der Prüfung der Identität. Nur so können Sie feststellen, ob die verwendeten Zertifikate auch tatsächlich Ihrer Sicherheitsanforderung entsprechen.

11.6.7 Aufbau einer eigenen CA

Die Nutzung von öffentlichen CAs ist für die sichere Unternehmenskommunikation nur bedingt empfehlenswert:

- Die Ausstellung von neuen Zertifikaten ist aufwändig und manchmal nicht schnell genug.
- Die verwendeten Schlüssel werden über unzureichend gesicherte Verbindungen übertragen.
- Die Kommunikation basiert auf dem Vertrauen gegenüber der CA.

Als Alternative eignet sich daher für die Unternehmenskommunikation der Aufbau einer eigenen CA. Hierfür bieten sich z. B. die Microsoft CA auf einem Microsoft Windows Server oder OpenSSL als OpenSource-Variante an. Mit einer eigenen CA können Sie ohne Abhängigkeit von fremden Stellen alle benötigten Zertifikate zur Sicherung des Datenaustauschs selbst erstellen und verwalten.

Der Einsatz einer eigenen CA ist für Unternehmen sicherlich eher zu empfehlen als die Nutzung öffentlicher Anbieter für Zertifizierungsdienste. Allerdings sind schon bei der Planung einer CA einige wichtige Punkte zu beachten. So werden z. B. schon bei der Installation einer Windows-CA die Gültigkeitszeiträume für die Root-CAs festgelegt, die nachträglich nicht mehr geändert werden können. Weitere Aspekte der Planung sind u. a.:

- Die Zertifikats-Policy, also die Sicherheitsstufe, die mit Hilfe der Zertifikate erreicht werden soll
- Der verwendete Namensraum
- Die Schlüssellängen
- Die Lebensdauer der Zertifikate
- Die Verwaltung von Sperrlisten

Eine genaue Planung zahlt sich auf jedem Fall aus, da spätere Korrekturen teilweise nur mit hohem Aufwand zu realisieren sind.

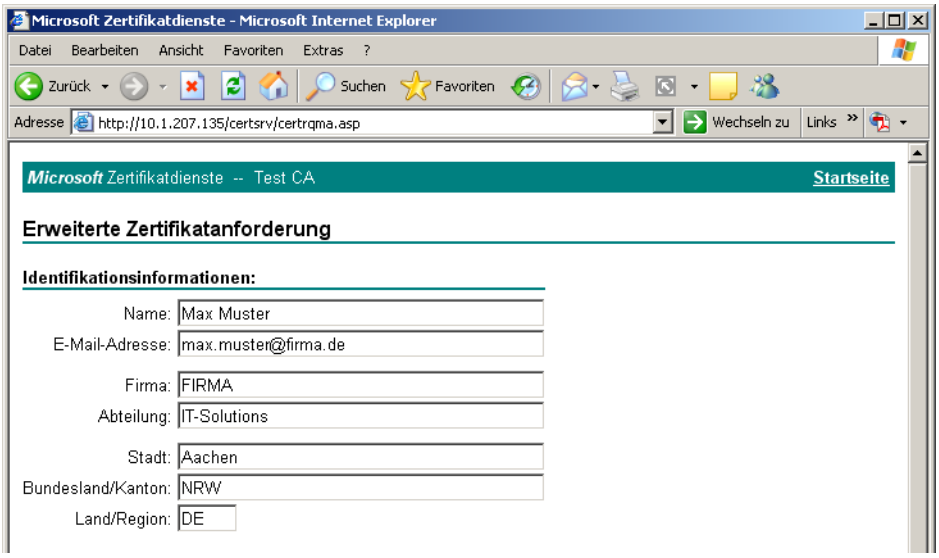
11.6.8 Anfordern eines Zertifikates mit der Stand-alone Windows CA

Für die Verwendung in einem Router leistet eine Kombination aus PKCS#12-Datei mit Root-Zertifikat, eigenem Geräte-Zertifikat und Public Key des Gerätes die besten Dienste.

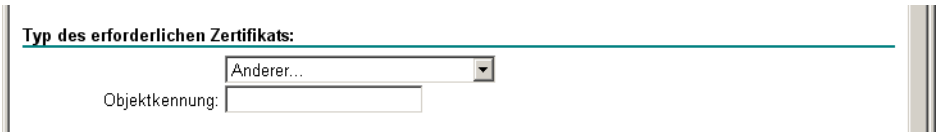
1. Rufen Sie in Ihrem Browser die Startseite des Microsoft Zertifikatsdienstes auf.
2. Wählen Sie als Zertifikatstyp die 'erweiterte Zertifikatanforderung'.
3. Wählen Sie im nächsten Schritt die Option 'Eine Anforderung an diese Zertifikatsstelle erstellen und einreichen'.

   Nur wenn das Root-Zertifikat schon in einer separaten Datei vorliegt, wählen Sie hier die Option 'BASE64'.

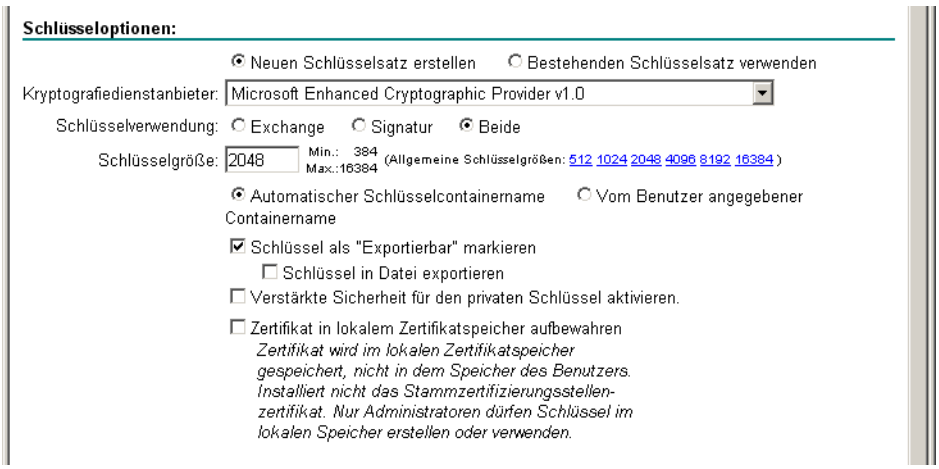
4. Im nächsten Schritt werden die Daten zur Identifikation eingetragen.



5. Wählen Sie im gleichen Dialog als Typ des Zertifikats die Option 'Anderer...' und löschen Sie den daraufhin erscheinenden Wert für die 'Objektkennung'.



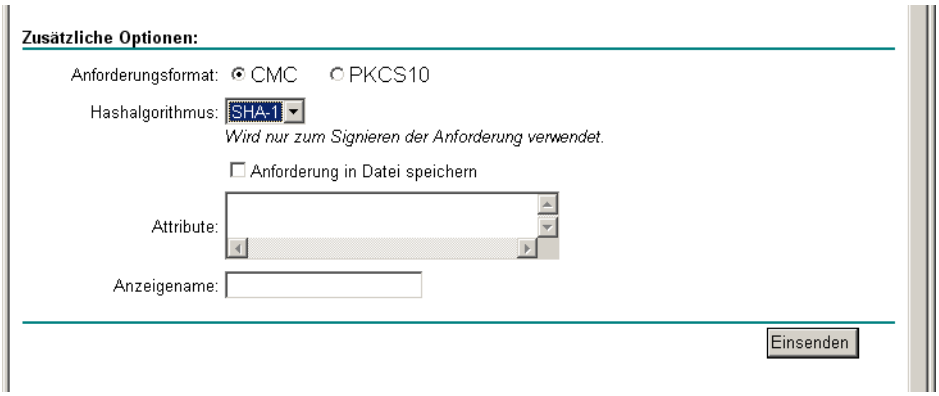
6. Markieren Sie die 'Automatische Schlüsselerstellung'. Damit werden Public und Private Key für den aktuellen Benutzer automatisch von der CA erstellt.



7. Wählen Sie eine geeignete Schlüssellänge (passend zur Zertifikats-Policy), aktivieren Sie die Option für exportierbare Schlüssel.

   Der Schlüssel wird an dieser Stelle nicht exportiert, daher muss auch kein Dateiname angegeben werden. Beim Exportieren würde eine Datei im Microsoft-spezifischen *.pvk-Format angelegt werden, die für die Weiterverarbeitung unter LCOS ungeeignet ist.

8. Wählen Sie zuletzt als Hash-Algorithmus 'SHA-1' und reichen Sie die Zertifikatanforderung mit **Einsenden** ein.



   Den Status der eingereichten Zertifikatanforderungen können Sie jederzeit über die Startseite der Windows-CA einsehen. Sie können die Zertifikatanforderungen nur vom gleichen Rechner aus einsehen, mit dem Sie die Anforderung eingereicht haben.

9. Sobald der Administrator der CA die Zertifikatanforderung geprüft und das Zertifikat erstellt hat, können Sie dieses auf Ihrem Rechner installieren.

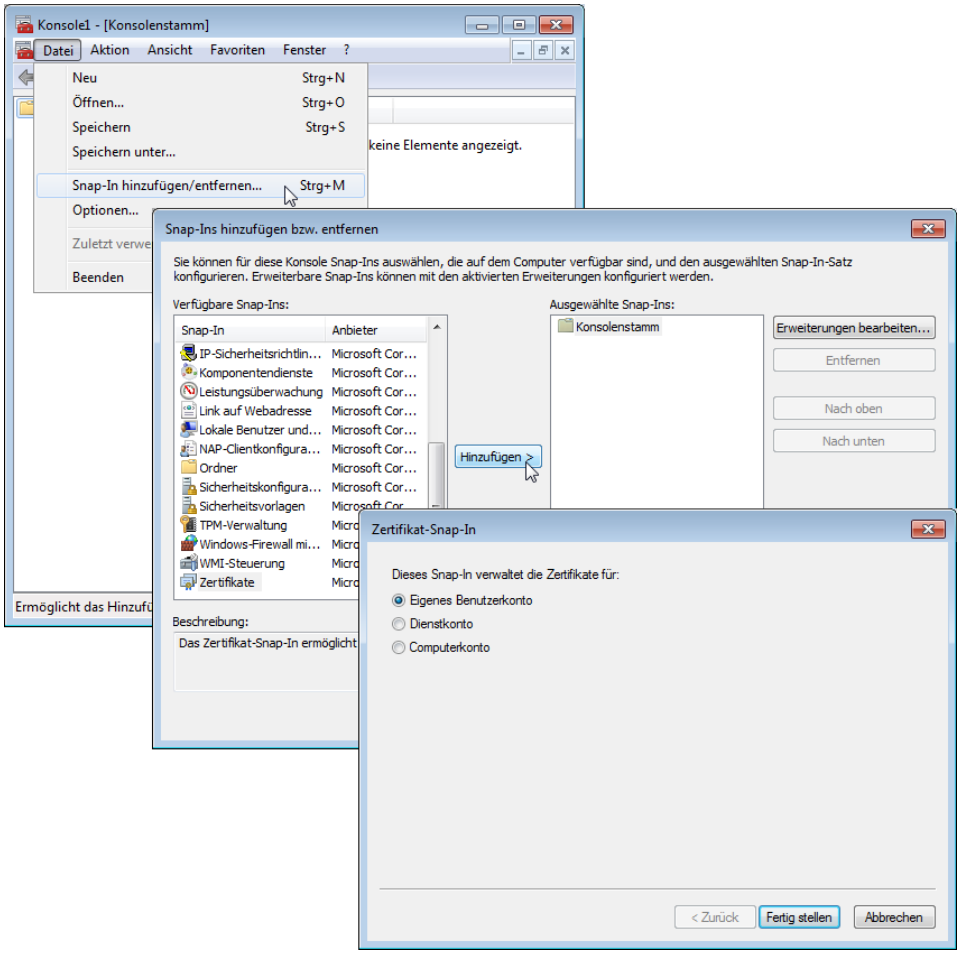
Sie können die Zertifikate nur auf dem gleichen Rechner installieren, mit dem Sie die Anforderung eingereicht haben.

11.6.9 Zertifikat in eine PKCS#12-Datei exportieren

Mit der Installation wird das Zertifikat in Ihrem Betriebssystem gespeichert, es liegt noch nicht als separate Datei vor. Diese benötigen Sie jedoch für die Installation im Gerät. Um zu einem Zertifikat in Dateiform zu gelangen, müssen Sie es zunächst exportieren.

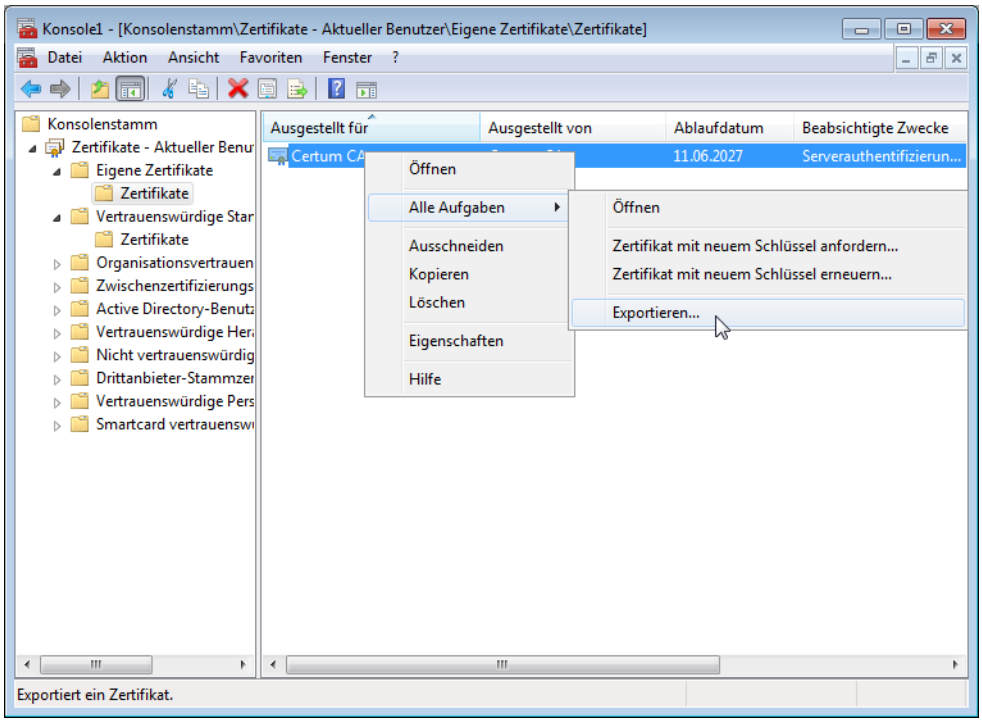
11.6.9.1 Export über den Windows-Konsolenstamm

1. Öffnen Sie dazu die Management-Konsole über den Befehl `mmc` an der Eingabeaufforderung und wählen Sie den Menüpunkt **Datei** > **Snap-In hinzufügen/entfernen**.

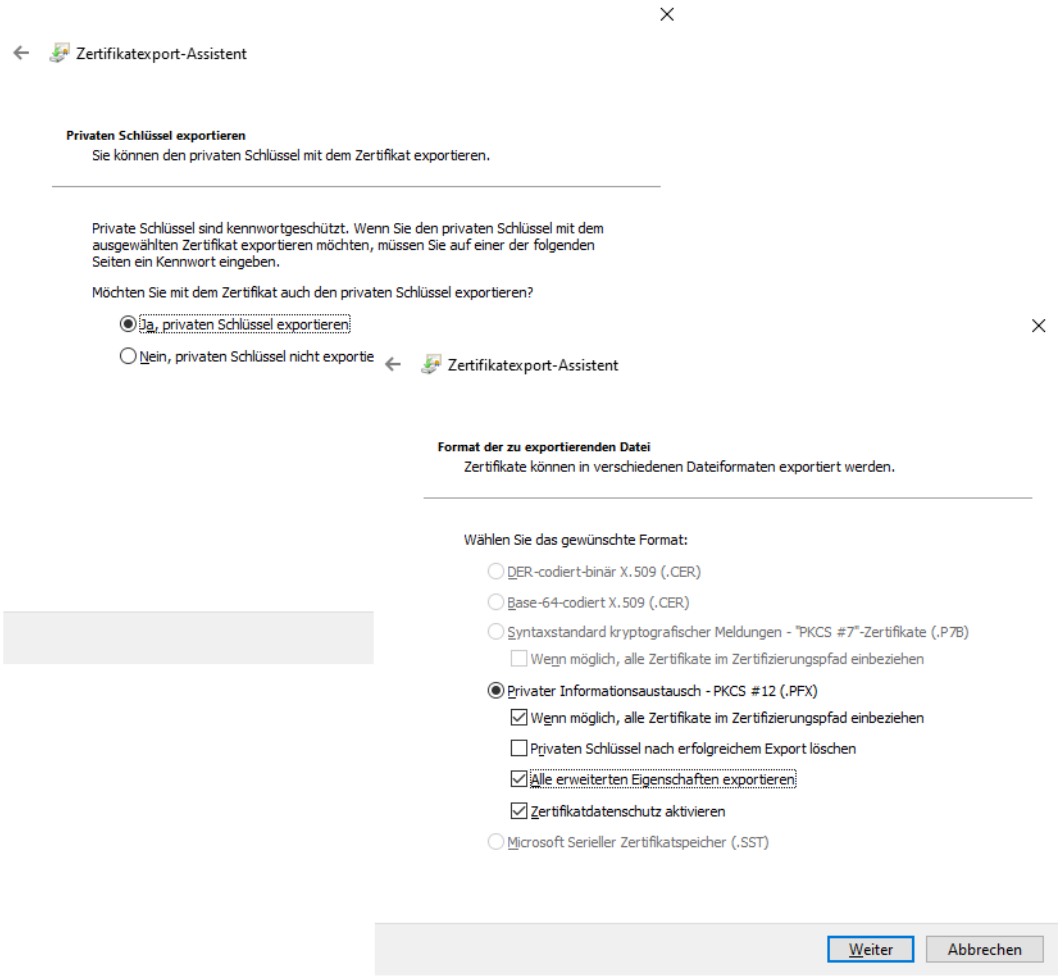


2. Klicken Sie auf **Hinzufügen** und wählen Sie den Eintrag „Zertifikate“. Bestätigen Sie mit **Hinzufügen**, markieren Sie anschließend „Eigenes Benutzerkonto“ und klicken Sie auf **Fertig stellen**.

3. Um das gewünschte Zertifikat in eine Datei zu exportieren, klicken Sie anschließend in der Managementkonsole in der Gruppe **Zertifikate - Aktueller Benutzer** > **Eigene Zertifikate** > **Zertifikate** mit der rechten Maustaste und wählen im Kontextmenü den Eintrag **Alle Aufgaben** > **Exportieren**.



4. Aktivieren Sie im Verlaufe des Zertifikatsexportassistenten die Option zum Exportieren des privaten Schlüssels. Optional können Sie den privaten Schlüssel nach dem Export aus dem System löschen.



Die Option „Wenn möglich, alle Zertifikate im Zertifizierungspfad einbeziehen" muss aktiviert sein, damit das Root-Zertifikat mit in die PKCS#12-Datei exportiert wird.

5. Beim Export werden Sie aufgefordert, ein Kennwort zum Schutz des privaten Schlüssels einzugeben. Wählen Sie hier ein sicheres Kennwort ausreichender Länge (Passphrase). Dieses Kennwort werden Sie bei der Installation der Zertifikate im Gerät wieder benötigen.

Für das Kennwort werden je nach Umgebung auch die synonymen Begriffe „Passwort" oder „PIN" verwendet.

11.6.10 Zertifikate mit OpenSSL erstellen

Mit OpenSSL steht eine weitere Möglichkeit zur Verfügung, eigene Zertifikate zu erstellen und Zertifikats-Verbindungen zu testen. OpenSSL ist als Open Source-Projekt kostenlos für Linux und Windows erhältlich, als Kommandozeilen-Tool jedoch auch weniger anwenderfreundlich als andere CA-Varianten.

Die Konfigurations-Datei openssl.cnf muss dabei an Ihre spezifischen Bedürfnisse angepasst werden. Nähere Informationen dazu finden Sie in der Dokumentation zu OpenSSL.

11.6.10.1 OpenSSL installieren

1. Laden Sie eine aktuelle OpenSSL-Version von *https://www.slproweb.com/products/Win32OpenSSL.html*.

Eine Übersicht der Downloadserver finden Sie unter *https://wiki.openssl.org/index.php/Binaries*.

2. Installieren Sie das Paket und erstellen Sie im Verzeichnis `./bin/PEM/demoCA` zusätzlich die Unterverzeichnisse:
   - `/certs`
   - `/newcerts`
   - `/crl.`
3. Ändern Sie in der Datei openssl.cnf den Pfad in der Gruppe `[CA_default]` auf: `dir=./PEM/demoCA`
4. Starten Sie OpenSSL durch einen Doppelklick auf die `openssl.exe` im Verzeichnis `./bin`.

11.6.10.2 Zertifikat für Root-CA ausstellen

1. Erstellen Sie einen Schlüssel für die CA mit dem Befehl:

   ```
   genrsa -aes256 -out ca.key 2048
   ```

   Merken Sie sich das Kennwort, das Sie nach der Aufforderung für den CA-Schlüssel eingeben, es wird später wieder benötigt!

   Dieser Befehl erstellt die Datei 'ca.key' im aktuellen Verzeichnis.
2. Erstellen Sie eine Zertifikatsanforderung (Request) für die CA mit dem Befehl:

   ```
   req -key ca.key -new -subj /CN="Test_CA" -out ca.req
   ```

   Hier werden Sie wieder zur Eingabe des Kennwortes für den CA-Schlüssel aufgefordert.

   Dieser Befehl erstellt die Datei 'ca.req' im aktuellen Verzeichnis.
3. Erstellen Sie ein Zertifikat aus der Zertifikatsanforderung mit dem Befehl:

   ```
   x509 -req -in ca.req -signkey ca.key -days 365 -out ca.crt
   ```

   Auch hier werden Sie wieder zur Eingabe des Kennwortes für den CA-Schlüssel aufgefordert.

   Dieser Befehl signiert die Zertifikatsanforderung 'ca.req' mit dem Schlüssel 'ca.key' und stellt damit das Zertifikat 'ca.crt' aus.

11.6.10.3 Zertifikat für Benutzer oder Geräte ausstellen

1. Erstellen Sie einen Schlüssel für das Gerät oder den Benutzer mit dem Befehl:

   ```
   genrsa -out device.key 2048
   ```

   Dieser Befehl erstellt die Datei 'device.key' im aktuellen Verzeichnis.
2. Erstellen Sie eine Zertifikatsanforderung (Request) für das Gerät oder den Benutzer mit dem Befehl:

   ```
   req -key device.key -new -subj /CN=DEVICE -out device.req
   ```

   Dieser Befehl erstellt die Datei 'device.req' im aktuellen Verzeichnis.

   Neben diesem Befehl sind noch weitere Änderungen in der Datei „openssl.cnf“ zur Definition einer Extension notwendig.
3. Erstellen Sie ein Zertifikat aus der Zertifikatsanforderung mit dem Befehl:

```
x509 -extfile openssl.cnf -req -in device.req -CAkey ca.key -CA ca.crt
-CAcreateserial -days 90 -out device.crt
```

Dieser Befehl signiert die Zertifikatsanforderung 'device.req' mit dem Schlüssel 'ca.key' und stellt damit das Zertifikat 'device.cert' aus. Zusätzlich wird dabei die Konfigurationsdatei openssl.cnf verwendet.

4. Exportieren Sie das Zertifikat für das Gerät oder den Benutzer mit dem Befehl:

```
pkcs12 -export -inkey device.key -in device.crt -certfile ca.crt
-out device.p12
```

Dieser Befehl fasst den Schlüssel 'device.key', das Geräte-Zertifikat 'device.crt' und das Root-Zertifikat 'ca.crt' zusammen und speichert sie gemeinsam in der Datei 'device.p12'. Diese PKCS#12-Datei können Sie direkt in das gewünschte Gerät laden.

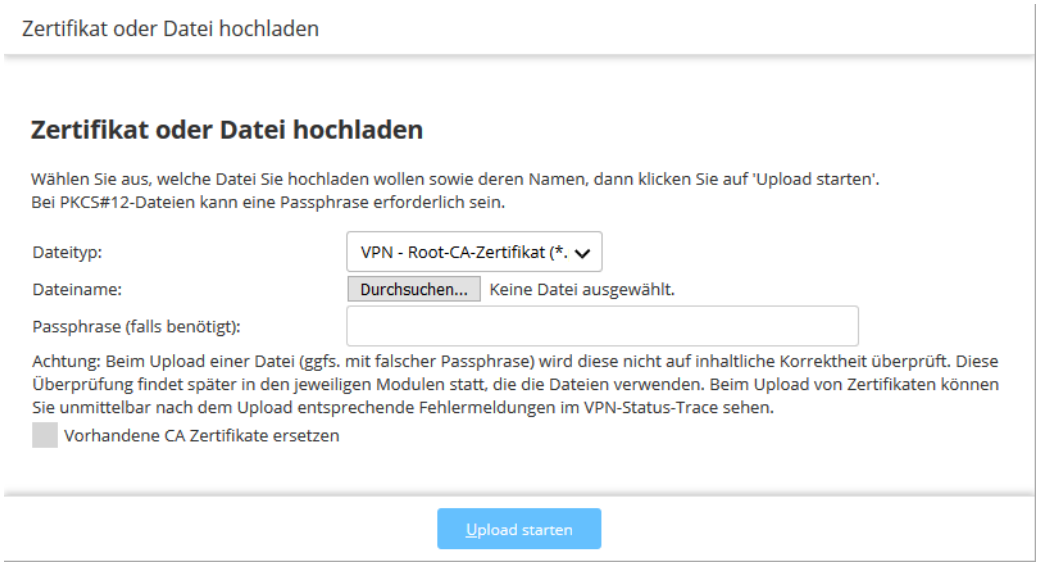
11.6.11 Zertifikate in das Gerät laden

Für den zertifikatgesicherten VPN-Verbindungsaufbau müssen in einem Gerät die folgenden Komponenten vorhanden sein:

- Zertifikat der Root-CA mit dem Public Key der CA
- Eigenes Geräte-Zertifikat mit dem eigenen Public Key und der Bestätigung der Identität. Die Prüfsumme dieses Zertifikats ist mit dem Private Key der CA signiert.
- Eigener Private Key

Sofern Sie die Anleitungen zur Ausstellung der Zertifikate über eine Windows-CA und den Export befolgt haben, liegen diese Informationen nun in Form einer gemeinsamen PKCS#12-Datei vor. Alternativ haben Sie ein anderes Verfahren verwendet und die einzelnen Komponenten liegen in separaten Dateien vor.

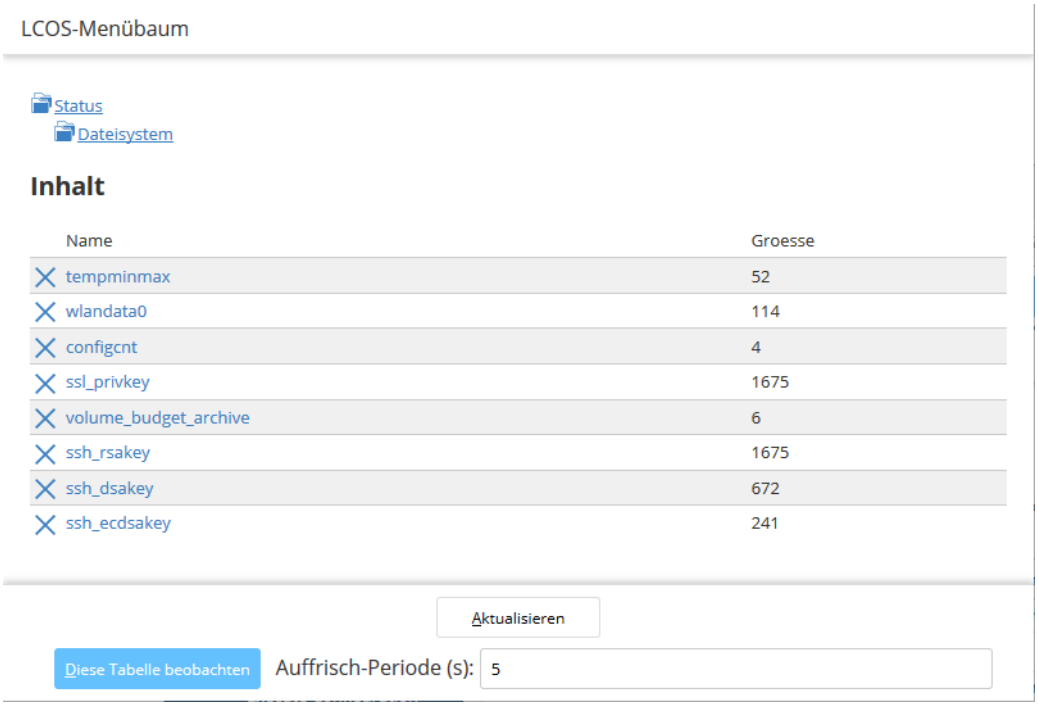
1. Melden Sie sich mit Administratorrechten über WEBconfig an dem gewünschten Gerät an.
2. Wählen Sie den Eintrag **Extras** > **Dateimanagement** > **Zertifikat oder Datei hochladen**.



3. Wählen Sie aus, welche Komponenten Sie in das Gerät laden wollen:
   - Root-Zertifikat
   - Geräte-Zertifikat
   - Private Key des Gerätes
   - PKCS#12-Datei mit einer Kombination aus Root-Zertifikat, Geräte-Zertifikat und Private Key

Je nach Typ der hochgeladenen Datei muss ggf. das entsprechende Kennwort eingegeben werden.

Die hochgeladenen Dateien können anschließend in einer Liste unter **Extras** > **LCOS-Menübaum** > **Status** > **Dateisystem** > **Inhalt** eingesehen werden.



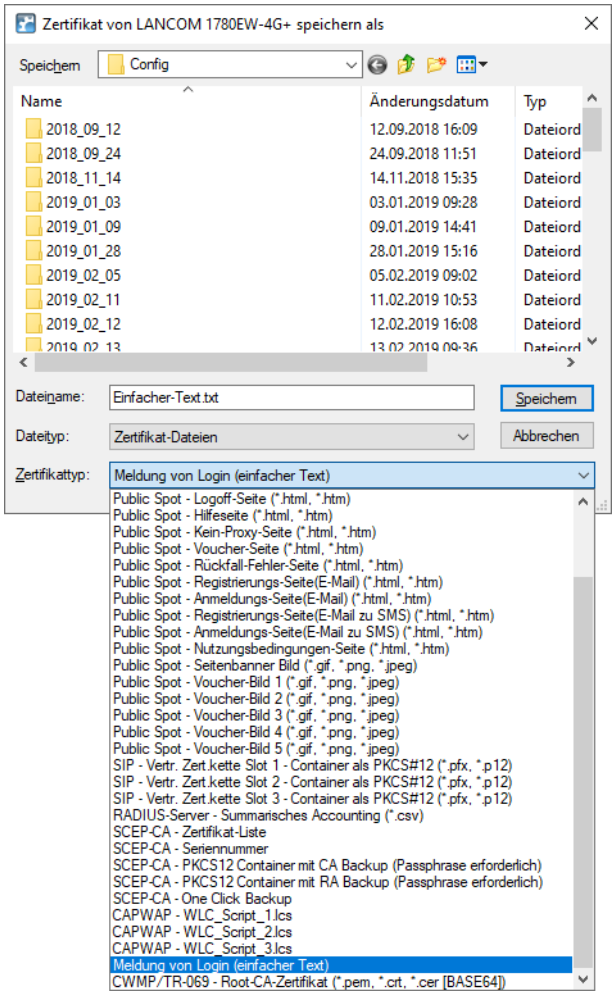
Eine kombinierte PKCS#12-Datei wird beim Upload automatisch in die benötigten Teile zerlegt.

11.6.12 Zertifikate sichern und hochladen mit LANconfig

In einem Gerät können unterschiedliche Zertifikate zur Verschlüsselung bestimmter Dienste verwendet werden. Diese Zertifikate können über LANconfig in die Geräte geladen werden. Außerdem können die im Gerät vorhandenen Zertifikate auch über LANconfig ausgelesen und in eine Datei gesichert werden.

1. Wählen Sie das Gerät aus, in das Sie ein Zertifikat einspielen bzw. aus dem Sie ein Zertifikat sichern wollen.

2. Klicken Sie die Auswahl mit der rechten Maustaste und wählen Sie im Kontextmenü **Konfigurations-Verwaltung** entweder **Zertifikat als Datei sichern** oder **Zertifikat als Datei hochladen**.



3. Wählen Sie Speicherort und den Typ des Zertifikats aus, der gesichert oder hochgeladen werden soll und bestätigen Sie die Auswahl mit **Speichern** > **Öffnen**.

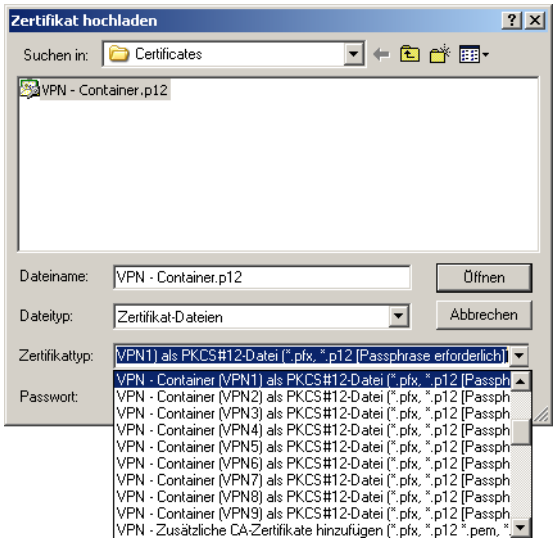
Mit der Auswahl von mehreren Geräten kann durchaus eine Zertifikatsdatei in mehrere Geräte gleichzeitig hochgeladen werden. das gleichzeitige Sichern von Zertifikaten aus mehreren Geräten ist hingegen nicht möglich. Je nach Typ der Zertifikatsdatei ist beim Hochladen ggf. ein Passwort (Passphrase) notwendig.

11.6.13 Erweiterte Zertifkats-Unterstützung

11.6.13.1 Mehrere Zertifikatshierarchien

Zur Unterstützung von mehreren Zertifikatshierarchien können bis zu neun PKCS#12-Dateien in das Gerät geladen werden. Darüber hinaus können weitere Dateien mit zusätzlichen CA-Zertifikaten hochgeladen werden, in denen die Zertifikate einzeln oder als PKCS#12-Container enthalten sein können. Alle Zertifikatshierarchien können manuell oder per SCEP verwaltet werden und können CRLs verwenden.

LANconfig: **Gerät** > **Konfigurations-Verwaltung** > **Zertifikat als Datei hochladen**



Die im Gerät vorhandenen Zertifikate können im Statusbereich eingesehen werden:

WEBconfig: **Extras** > **LCOS-Menübaum** > **Status** > **Zertifikate** > **Geraetezertifikate**

Die Gerätezertifikate werden im internen Dateisystem der Geräte den Verwendungszwecken “VPN1” bis “VPN9” zugeordnet.

Zur Nutzung der Zertifikate kann in den IKE-Schlüsseln mit dem Typ ASN.1-Distinguished Name als „lokale Identität“ entweder das Subject des Zertifikats oder diese Kurzbezeichnung verwendet werden.

Durch die Referenzierung der Zertifikate über die Kurzbezeichnung können auch Subjects mit deutschen Umlauten oder anderen Sonderzeichen verwendet werden, die ansonsten aufgrund der Einschränkungen der CLI-Konfiguration nicht angesprochen werden können.

Die Kurzbezeichnung wird bei der Konfiguration der Zertifikate für den SCEP-Client als “Verwendung” eingetragen.

11.6.13.2 Einstellbare Trace-Stufe für den SCEP-Client

Für den SCEP-Client-Trace kann die Ausgabe von Tracemeldungen auf einen bestimmten Inhalt beschränkt werden. Dazu wird ein Wert angegeben, bis zu welcher Stufe die Pakete im Trace ausgegeben werden sollen.

Konsole: **Setup** > **Zertifikate** > **SCEP-Client** > **Trace-Stufe**

Trace-Stufe

Mögliche Werte:

alles (Default)

Alle Tracemeldungen, auch reine Info- und Debug-Meldungen.

reduziert

Nur Fehler- und Warnmeldungen.

nur-Fehler

Nur Fehlermeldungen

11.6.14 VPN-Verbindungen auf Zertifikatsunterstützung einstellen

VPN-Verbindungen mit Zertifikatsunterstützung können nur aufgebaut werden, wenn das Gerät über die korrekte Uhrzeit verfügt. Wenn das Gerät keine aktuelle Uhrzeit hat, kann die Gültigkeit der Zertifikate nicht richtig beurteilt werden, die Zertifikate werden dann abgelehnt und es kommt keine Verbindung zustande.

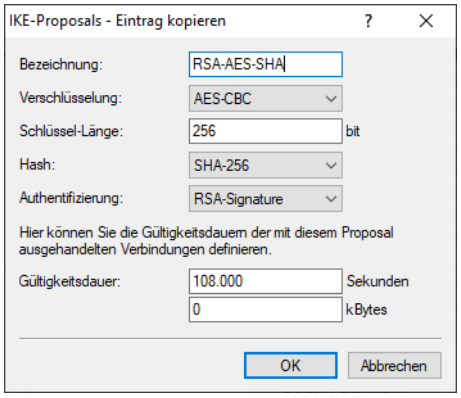
Um VPN-Verbindungen auf die Unterstützung von Zertifikaten einzustellen, müssen verschiedene Teile der Konfiguration entsprechend vorbereitet werden:

- IKE-Proposals
- IKE-Proposal-Listen
- IKE-Schlüssel
- VPN-Parameter
- Verbindungs-Parameter

Je nach Firmwarestand sind die benötigten Werte teilweise schon in Ihrem Gerät vorhanden. Prüfen Sie in diesem Fall nur die Werte auf richtige Einstellung.

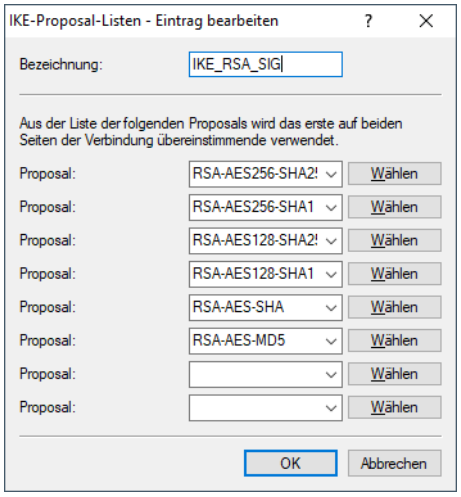
Wenn Sie ein entferntes Gerät auf die nachfolgende beschriebene Weise auf Zertifikatsunterstützung umstellen wollen, das nur über einen VPN-Tunnel erreichbar ist, müssen Sie auf jeden Fall zuerst das entfernte Gerät umstellen, bevor Sie die Verbindung des lokalen Geräts ändern. Durch die Änderung der lokalen Konfiguration ist das entfernte Gerät ansonsten nicht mehr erreichbar!

1. In den Listen der Proposals werden zwei neue Proposals mit den exakten Bezeichnung 'RSA-AES-MD5' und 'RSA-AES-SHA' benötigt, die beide als Verschlüsselung 'AES-CBC' und als Authentifizierungsmodus 'RSA-Signature' verwenden und sich nur im Hash-Verfahren unterscheiden.



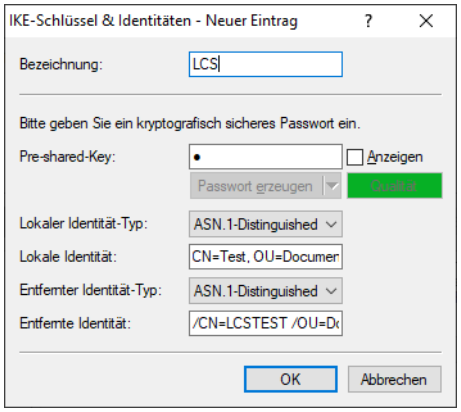
LANconfig: **VPN** > **IKE/IPSec** > **IKE-Proposals** > **IKE-Proposals**

2. In den Proposal-Listen wird eine neue Liste benötigt mit der exakten Bezeichnung 'IKE_RSA_SIG', in der die beiden neuen Proposals 'RSA-AES-MD5' und 'RSA-AES-SHA' aufgeführt sind.



LANconfig: **VPN** > **IKE/IPSec** > **IKE-Proposals** > **IKE-Proposal-Listen**

3. In der Liste der IKE-Schlüssel müssen für alle Zertifikats-Verbindungen die entsprechenden Identitäten eingestellt werden.



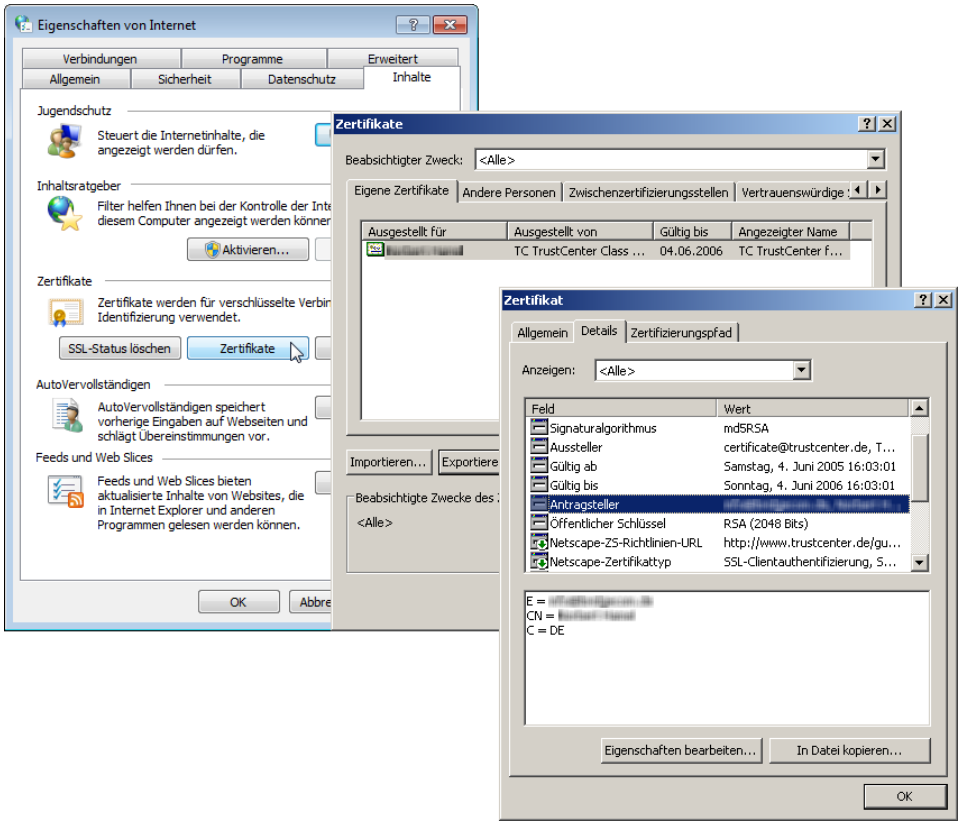
LANconfig: **VPN** > **IKE/IPSec** > **IKE-Schlüssel & Identitäten**

- Der Preshared Key kann ggf. gelöscht werden, wenn er endgültig nicht mehr benötigt wird.
- Der Typ der Identitäten wird auf ASN.1 Distinguished Names umgestellt (lokal und remote).
- Die Identitäten werden exakt so eingetragen wie in den Zertifikaten. Die einzelnen Werte z. B. für 'CN', 'O' oder 'OU' können durch Kommata oder Slashes getrennt werden.

Es müssen alle in den Zertifikaten eingetragenen Werte aufgeführt werden, in der gleichen Reihenfolge. Prüfen Sie ggf. über die Systemsteuerung den Inhalt der Zertifikate. Geben Sie dazu in der Windows-Suche **Internetoptionen** ein und öffnen diese. Dort auf der Registerkarte **Inhalte** die Schaltfläche **Zertifikate** anklicken.

Öffnen Sie das gewünschte Zertifikat und wählen Sie auf der Registerkarte **Details** den entsprechenden Wert aus. Für den Antragsteller finden Sie hier z. B. die benötigten ASN.1 Distinguished Names mit den zugehörigen

Kurzzeichen. Die in den Zertifikaten von oben nach unten aufgeführten Werte müssen in den IKE-Schlüssel von links nach rechts eingetragen werden. Beachten Sie auch die Groß- und Kleinschreibung!

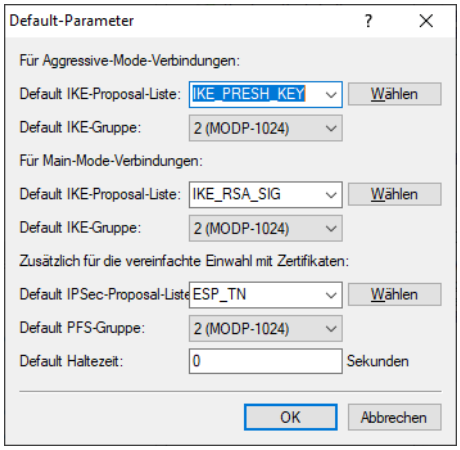


Die Anzeige von Zertifikaten unter Microsoft Windows zeigt für manche Werte ältere Kurzformen an, beispielweise 'S' anstelle von 'ST' für 'stateOrProvinceName' (Bundesland) oder 'G' anstelle von 'GN' für 'givenName' (Vorname). Verwenden Sie hier ausschließlich die aktuellen Kurzformen 'ST' und 'GN'.

Sonderzeichen in den ASN.1 Distinguished Names können durch die Angabe der ASCII-Codes in Hexadezimaldarstellung mit einem vorangestellten Backslash eingetragen werden. „\61" entspricht z. B. einem kleinen „a".

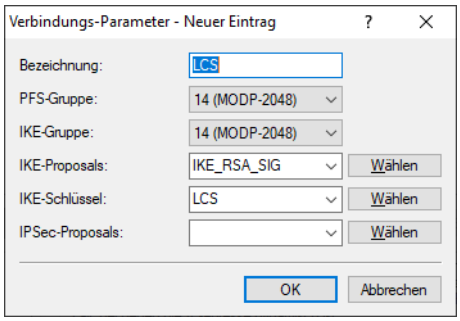
4. In den IKE-Verbindungs-Parametern müssen die Default-IKE-Proposal-Listen für eingehende Aggressive-Mode- und Main-Mode-Verbindungen auf die Proposal-Liste 'IKE_RSA_SIG' eingestellt sein. Beachten Sie außerdem die Einstellung der Default-IKE-Gruppe, die im nächsten Schritt ggf. angepasst werden muss.

Die Default-IKE-Proposal-Listen und Default-IKE-Gruppen finden Sie in LANconfig unter **VPN** > **IKE/IPSec** > **Default-Parameter**:



In den VPN-Verbindungs-Parametern müssen zum Schluss die VPN-Verbindungen auf die Verwendung der richtigen IKE-Proposals eingestellt werden ('IKE_RSA_SIG'). Dabei müssen die Werte für 'PFS-Gruppe' und 'IKE-Gruppe' mit den in den IKE-Verbindungs-Parametern eingestellten Werten übereinstimmen.

Die VPN-Verbindungs-Parameter finden Sie in LANconfig unter **VPN** > **IKE/IPSec** > **VPN-Verbindungen** > **Verbindungs-Parameter**:



11.6.15 Zertifikatsbasierte VPN-Verbindungen mit dem Setup-Assistenten erstellen

Mit dem Setup-Assistenten von LANconfig können Sie schnell und bequem zertifikatsbasierte LAN-Kopplungen oder RAS-Zugänge über VPN einrichten.

VPN-Verbindungen mit Zertifikatsunterstützung können nur aufgebaut werden, wenn das Gerät über die korrekte Uhrzeit verfügt und die entsprechenden Zertifikate in das Gerät geladen wurden.

11.6.15.1 LAN-Kopplungen

1. Wählen Sie den Assistenten „Zwei lokale Netze verbinden (VPN)“ zum Verbinden von Netzwerken über VPN. Wählen Sie dann im entsprechenden Dialog die VPN-Verbindungsauthentifizierung über Zertifikate (RSA-Signature).
2. Tragen Sie die Identitäten aus dem lokalen und entfernten Geräte-Zertifikat ein. Übernehmen Sie dabei die vollständigen Angaben aus den jeweiligen Zertifikaten in der richtigen Reihenfolge: die in den Zertifikaten unter Windows von oben nach unten aufgeführten ASN.1-Distinguished Names werden in LANconfig von links nach rechts eingetragen.

   Die Anzeige von Zertifikaten unter Microsoft Windows zeigt für manche Werte ältere Kurzformen an, beispielweise 'S' anstelle von 'ST' für 'stateOrProvinceName' (Bundesland) oder 'G' anstelle von 'GN' für 'givenName' (Vorname). Verwenden Sie hier ausschließlich die aktuellen Kurzformen 'ST' und 'GN'.

Der Konsolenbefehl `show vpn cert` zeigt die Inhalte des Geräte-Zertifikates in einem Gerät, u. a. die eingetragenen Relative Distinguished Names (RDN) unter „Subject“.

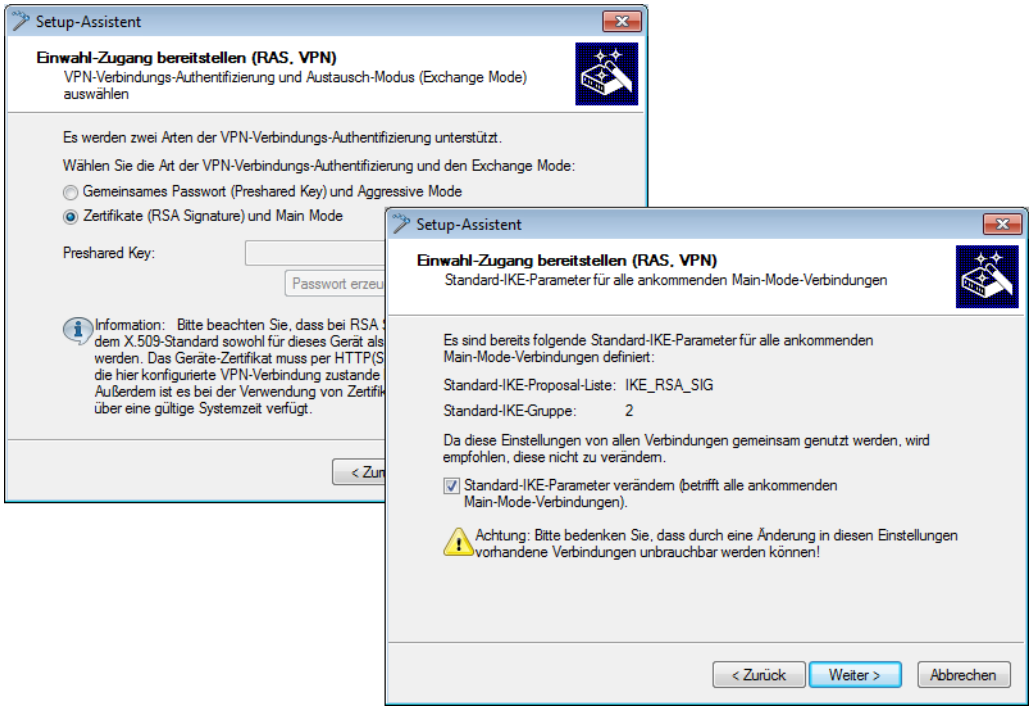
3. Wählen Sie nach Möglichkeit den optimierten Verbindungsaufbau mit IKE- und PFS-Gruppe 14. Wählen Sie nur dann die Gruppe 5 für IKE und PFS, wenn dies von der Gegenstelle verlangt wird.
4. Tragen Sie den Namen der VPN-Gegenstelle, die IP-Adresse und die Netzmaske des entfernten Netzes sowie die ggf. verwendeten Domain für die DNS-Weiterleitung ein. Aktivieren Sie je nach Bedarf die „Extranet“-Funktion.

11.6.15.2 RAS-Zugänge

RAS-Zugänge mit Zertifikatsunterstützung können für den LANCOM Advanced VPN Client oder für einen anderen VPN-Client mit benutzerdefinierten Parametern eingerichtet werden. Der Standard VPN-Client bietet keine Unterstützung für Zertifikate an.

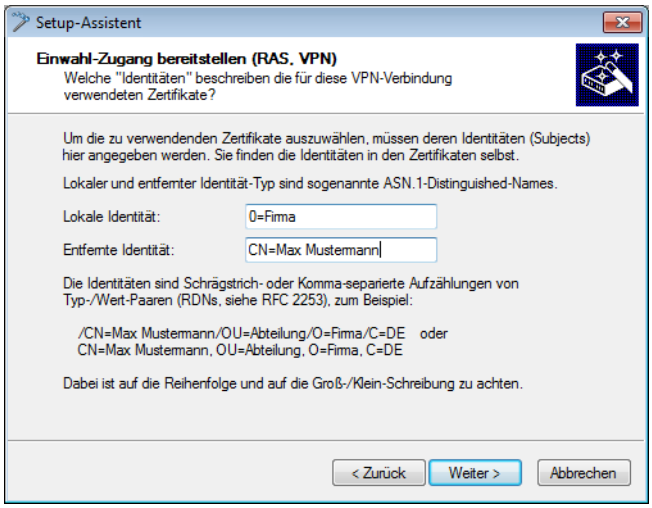
Die abgefragten Parameter unterscheiden sich je nach Auswahl des Clients bzw. der Optionen während der Dialoge. Diese Beschreibung zeigt vollständig alle evtl. auftretenden Dialoge des Assistenten, von denen nicht alle für Ihre Anwendung relevant sein müssen.

1. Wählen Sie den Assistenten zum Bereitstellen von Zugängen über VPN. Wählen Sie dann im entsprechenden Dialog die VPN-Verbindungsauthentifizierung über Zertifikate (RSA-Signature). Als „Exchange Mode“ wird dabei automatisch der Main Mode verwendet.



2. In der Konfiguration sind üblicherweise bereits Standard-IKE-Parameter für ankommende Main-Mode-Verbindungen in der Standard-IKE-Proposal-Liste 'IKE_RSA_SIG' definiert. Verwenden Sie nach Möglichkeit diese Liste mit den vorbereiteten IKE-Parametern.
3. Wenn Sie gezielt andere Parameter für die ankommenden Main-Mode-Verbindungen nutzen möchten, können Sie die Standard-IKE-Parameter an Ihre Bedürfnisse anpassen. Sie können entweder über die Abfrage der benötigten Parameter eine neue Liste 'WIZ-IKE-MAIN-MODE' erstellen oder eine der vorhandenen IKE-Proposal-Listen als neue „Standard-IKE-Proposal-Liste“ auswählen. Die hier definierte Liste wird in Zukunft von allen ankommenden Main-Mode-Verbindungen verwendet. Für eine neue IKE-Proposal-Liste können Sie auswählen, welche Verschlüsselungsverfahren und Authentifizierungsverfahren der Client während der IKE-Verhandlung verwenden kann.

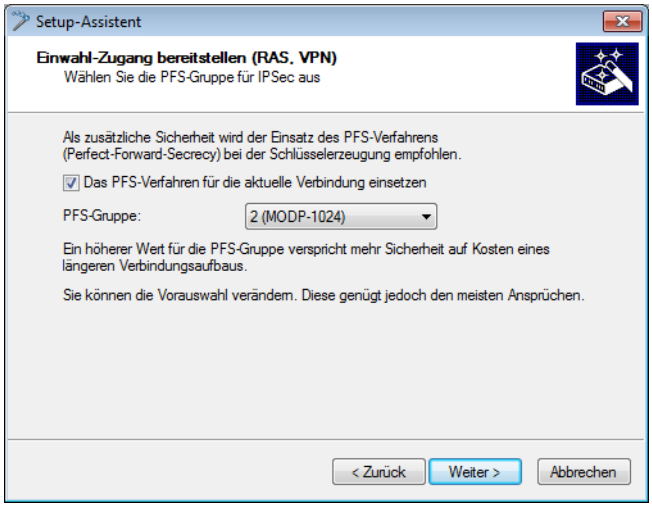
4. Tragen Sie die Identitäten aus dem lokalen und entfernten Geräte-Zertifikat ein. Übernehmen Sie dabei die vollständigen Angaben aus den jeweiligen Zertifikaten in der richtigen Reihenfolge: die in den Zertifikaten unter Windows von oben nach unten aufgeführten ASN.1-Distinguished Names werden in LANconfig von links nach rechts eingetragen.



Die Anzeige von Zertifikaten unter Microsoft Windows zeigt für manche Werte ältere Kurzformen an, beispielweise 'S' anstelle von 'ST' für 'stateOrProvinceName' (Bundesland) oder 'G' anstelle von 'GN' für 'givenName' (Vorname). Verwenden Sie hier ausschließlich die aktuellen Kurzformen 'ST' und 'GN'.

Der Konsolenbefehl `show vpn cert` zeigt die Inhalte des Geräte-Zertifikates in einem Gerät, u. a. dabei die eingetragenen Relative Distinguished Names (RDN) unter „Subject“.

5. Wählen Sie nach Möglichkeit den optimierten Verbindungsaufbau mit PFS-Gruppe 2. Wählen Sie nur dann die Gruppe 5 als PFS-Gruppe, wenn dies vom Client verlangt wird.

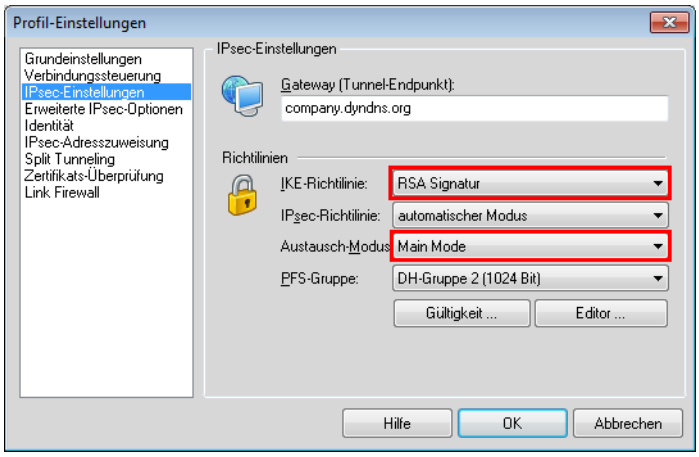


6. Für die Übertragung der Nutzdaten mit IPSec können in den folgenden Dialogen die Verschlüsselungs- und Authentifizierungsverfahren sowie die „Authentication Header“ und die Datenkompression festgelegt werden, die der Client verwenden kann. Verwenden Sie nach Möglichkeit die voreingestellten Werte, sofern der Client keine anderen Einstellungen erwartet.
7. Tragen Sie die IP-Adresse für den Client und den für den Zugriff erlaubten Adress-Bereich im lokalen Netzwerk ein.

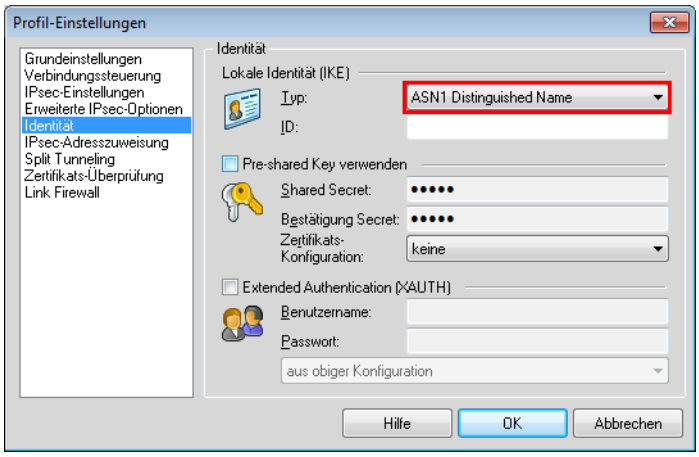
11.6.16 LANCOM Advanced VPN Client auf Zertifikatsverbindungen einstellen

Bei der Einwahl mit dem LANCOM Advanced VPN Client in einen Router müssen die entsprechenden Profil-Einstellungen an die Verwendung von Zertifikaten angepasst werden.

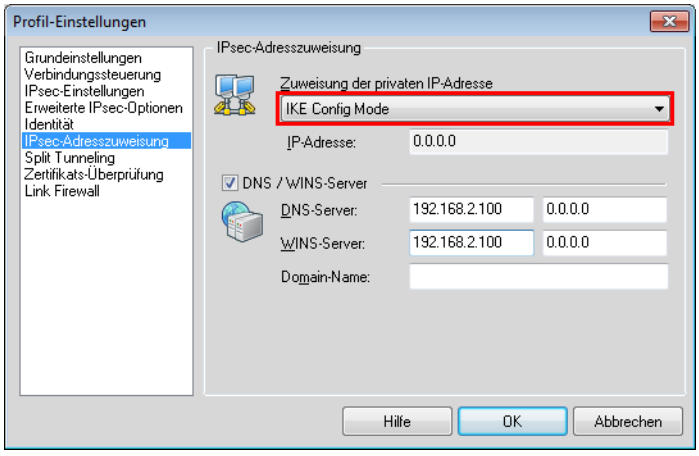
1. Stellen Sie in den IPSec-Einstellungen des Profils die IKE-Richtlinie auf 'RSA-Signatur' um.



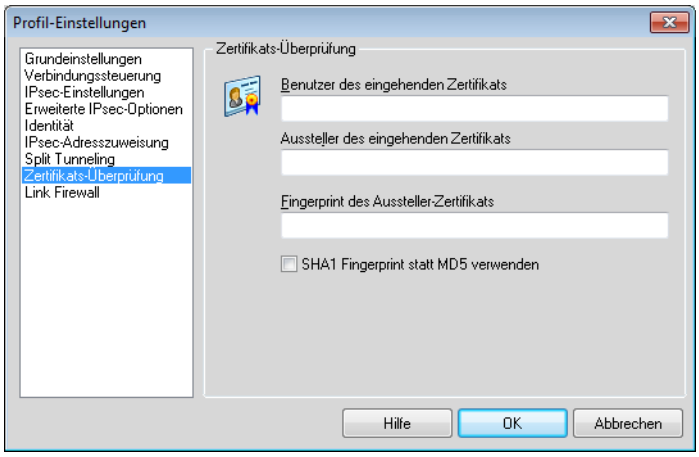
2. Stellen Sie die Identität auf 'ASN1 Distinguished Names' um. Die 'Identität' kann frei bleiben, da diese Information aus dem Zertifikat ausgelesen wird.



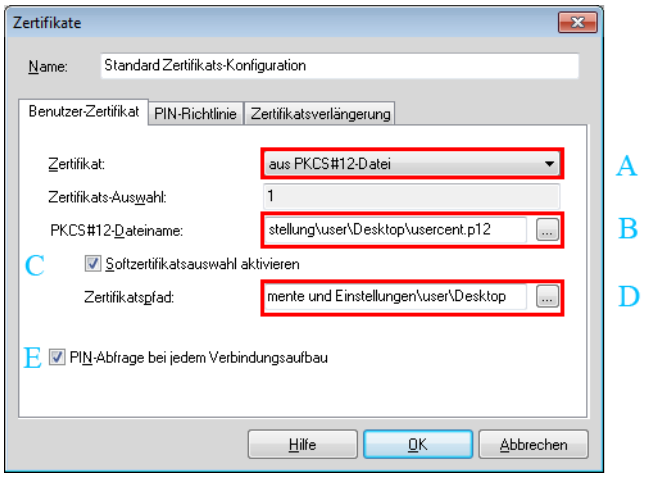
3. Verwenden Sie bei der IP-Adress-Zuweisung den 'IKE Config Mode'.



4. Bei der Zertifikatsüberprüfung können Sie optional die Zertifikate einschränken, die der LANCOM Advanced VPN Client akzeptiert. Dazu geben Sie den Benutzer und / oder den Aussteller des eingehenden Zertifikats und ggf. den zugehörigen „Fingerprint" an.



5. Nachdem Sie das geänderte Verbindungsprofil gespeichert haben, öffnen Sie über den Menüpunkt **Konfiguration** / **Zertifikate** die Einstellungen für die Benutzerzertifikate.



6. Wählen Sie als Zertifikatetyp die 'PKCS#12-Datei aus und geben Sie die gewünschte Zertifikatsdatei an.

   - Wenn Sie mit verschiedenen Zertifikaten arbeiten möchten, aktivieren Sie die Option 'Softzertifikatsauswahl' und geben den Pfad zum Ordner an, in dem die Zertifikatsdateien abgelegt sind.
   - Wählen Sie aus, ob die PIN (das Kennwort) für das Zertifikat bei jedem Verbindungsaufbau abgefragt werden soll. Alternativ können Sie die PIN über den Menüpunkt **Verbindung** > **PIN eingeben** fest im LANCOM Advanced VPN Client speichern.



› Bei aktivierter Softzertifikatsauswahl können Sie beim Verbindungsaufbau im Hauptfenster des LANCOM Advanced VPN Client jeweils das gewünschte Zertifikat aus der Liste auswählen, passend zum gewählten Profil.



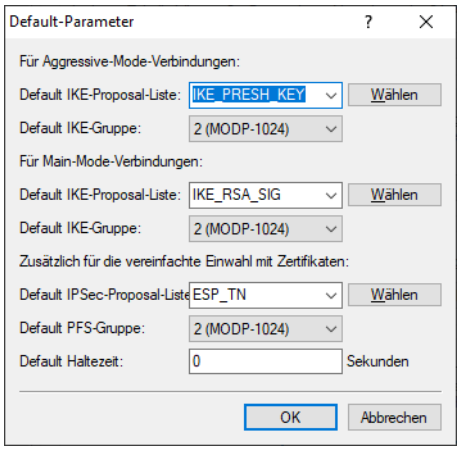
11.6.17 Vereinfachte Einwahl mit Zertifikaten

Bei der Einwahl von Rechnern mit wechselnden IP-Adressen ist zu Beginn der IKE-Verhandlung (Phase 1) die Identität der Gegenstelle noch nicht bekannt. Zur Kommunikation werden Defaultwerte für IKE-Proposal-Listen und IKE-Proposal-Gruppen verwendet. Während der Verhandlung wird die Identität übermittelt, anhand derer die Parameter für die Phase 2 bestimmt werden können (IPSec-Proposal-Liste und PFS-Gruppe). Um diese Zuordnung zu ermöglichen, muss allerdings jeder einzelne Benutzer separat in der Konfiguration des VPN-Routers eingetragen werden.

Bei der zertifikatsbasierten Einwahl wird über das Zertifikat eine Identität übermittelt. Um nicht jeweils eigene Benutzereinträge in der Router-Konfiguration anlegen zu müssen, können für alle über Zertifikate identifizierbaren Benutzer gemeinsame Parameter für Phase 2 definiert werden. Bei dieser vereinfachten Einwahl muss der Benutzer nur über ein gültiges Zertifikat verfügen, das vom Herausgeber des im Gerät befindlichen Root-Zertifikats signiert ist. Darüber hinaus müssen die vom Client bei der Einwahl verwendeten Parameter mit den Defaultwerten des VPN-Routers übereinstimmen.

Informationen über die Konfiguration des VPN-Clients entnehmen Sie bitte der entsprechenden Dokumentation des Software-Herstellers.

Zur Konfiguration der vereinfachten Einwahl wird diese Funktion in LANconfig unter **VPN** > **Allgemein** > **Vereinfachte Einwahl mit Zertifikaten aktiviert** eingeschaltet. Die Default-Parameter können bei Bedarf unter **VPN** > **IKE/IPSec** > **Default-Parameter** verändert werden.



Durch das Aktivieren der vereinfachten Zertifikate-Einwahl können sich **alle** Clients mit einem gültigen Zertifikat, das vom Herausgeber des im Gerät befindlichen Root-Zertifikats signiert ist, in das entsprechende Netzwerk einwählen. Es ist keine weitere Konfiguration des Routers erforderlich! Unerwünschte Einwahlen können ausschließlich über das Sperren der Zertifikate und die Verwendung einer Certificate Revocation List (CRL) verhindert werden.

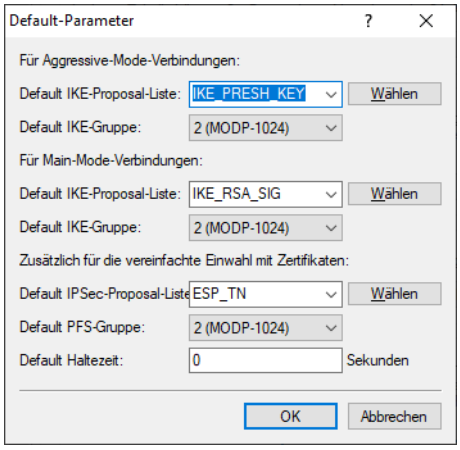
11.6.18 Vereinfachte Netzwerkanbindung mit Zertifikaten – Proadaptives VPN

Bei VPN-Kopplung von großen Netzwerkstrukturen ist oft gewünscht, dass der Konfigurationsaufwand bei der Einrichtung eines neuen Teilnetzwerks auf den dortigen VPN-Router beschränkt wird und die Konfiguration der zentralen Einwahl-Router unverändert bleiben kann. Um diese vereinfachte Netzwerkanbindung zu erreichen, übermitteln die einwählenden Geräte ihre Identität mit Hilfe eines Zertifikates.

Wenn die vereinfachte Einwahl mit Zertifikaten für den Router in der Zentrale aktiviert ist, können die entfernten Router während der IKE-Verhandlung in Phase 2 selbst ein Netzwerk vorschlagen, dass für die Anbindung verwendet werden soll. Dieses Netzwerk wird z. B. bei der Einrichtung der VPN-Verbindung in den entfernten Router eingetragen. Der Router in der Zentrale akzeptiert das vorgeschlagene Netzwerk, wenn zusätzlich zur vereinfachten Einwahl über **VPN** > **Allgemein** > **Vereinfachte Einwahl mit Zertifikaten aktiviert** die Option **VPN** > **Allgemein** > **Gegenstelle die Auswahl des entfernten Netzwerks erlauben** aktiviert ist. Darüber hinaus müssen die vom Client bei der Einwahl verwendeten Parameter mit den Defaultwerten des VPN-Routers übereinstimmen.

Achten Sie bei der Konfiguration der einwählenden Gegenstellen darauf, dass jede Gegenstelle ein spezielles Netzwerk anfordert, damit es nicht zu Konflikten der Netzwerkadressen kommt.

Die Default-Parameter können bei Bedarf unter **VPN** > **IKE/IPSec** > **Default-Parameter** verändert werden.



Durch das Aktivieren der vereinfachten Zertifikate-Einwahl können sich **alle** entfernten Router mit einem gültigen Zertifikat, das vom Herausgeber des im Gerät befindlichen Root-Zertifikats signiert ist, in das entsprechende Netzwerk einwählen. Es ist keine weitere Konfiguration des Routers erforderlich! Unerwünschte Einwahlen können ausschließlich über das Sperren der Zertifikate und die Verwendung einer CRL verhindert werden. Die vereinfachte Anbindung von Netzwerken mit Zertifikaten ist daher auf Router beschränkt, die Certificate Revocation Lists (CRL) unterstützen.

11.6.19 Anfrage von Zertifikaten mittels CERTREQ

Einige VPN Gateways erwarten bei einer mittels RSA-Signature authentifizierten IPSec-Aushandlung, dass die zu übermittelnden Zertifikate über einen „Certificate Request" (CERTREQ) von der Gegenstelle angefragt werden. Dies ermöglicht unter anderem eine Auswahl des zu verwendenden Zertifikats, sofern das Gateway mehreren CAs vertraut.

Um den Aufbau zu solchen VPN-Gateways zu ermöglichen, senden VPN-Router beim Verbindungsaufbau einen entsprechenden CERTREQ, der den Herausgeber des im Router gespeicherten Root-Zertifikates enthält.

11.6.20 Certificate Revocation List – CRL

Zertifikate für VPN-Verbindungen enthalten eine Gültigkeitsdauer in Form von Start- und Enddatum. Während dieser Zeit kann über dieses Zertifikat eine VPN-Verbindung aufgebaut werden. Scheidet ein Mitarbeiter aus dem Unternehmen aus, der ein solches Zertifikat z. B. für einen mobilen VPN-Zugang verwendet, möchte man in der Regel das Zertifikat vorzeitig für ungültig erklären, damit der Zugang zum Firmennetzwerk auch bei unveränderter Konfiguration der VPN-Router nicht mehr möglich ist.

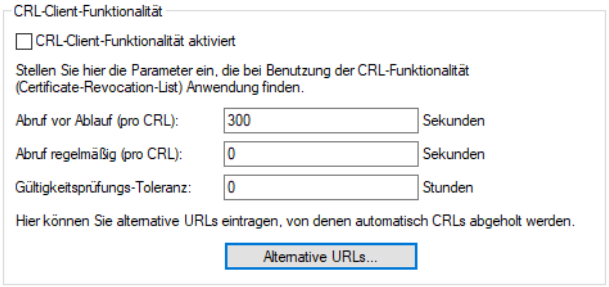
Da sich das Zertifikat selbst beim Mitarbeiter befindet und nicht verändert werden kann, wird eine Zertifikatsperrliste verwendet. In einer solchen Zertifikatsperrliste (Certificate Revocation List – CRL), wie sie z. B. von der Microsoft CA oder von OpenSSL unterstützt werden, sind die ungültigen Zertifikate eingetragen. Die CRL wird auf einem geeigneten Server bereitgestellt. Die URL, von der ein Router die CRL in seinen Speicher laden kann, wird im Root-Zertifikat des VPN-Routers und / oder in der Konfiguration des Geräts selbst eingetragen.

Die CRL wird von der CA regelmäßig erneuert, damit Änderungen in der CRL durch zurückgezogene Zertifikate von den VPN-Routern rechtzeitig erkannt werden können. Beim Aufsetzen der CA wird üblicherweise eine Zeitspanne festgelegt, nach der die CRL regelmäßig erneuert werden soll. Nach dem Erneuern der CRL und der Ablage der CRL auf dem Server (manuell oder automatisiert) muss der VPN-Router diese neuen Informationen aktualisieren. Dazu liest der Router die Gültigkeitsdauer der CRL aus und versucht kurz vor deren Ablauf eine aktuelle CRL zu laden. Alternativ kann auch ein regelmäßiges Update – unabhängig von der Gültigkeitsdauer der CRL – in einem Router definiert werden.

Beim Verbindungsaufbau prüft der VPN-Router, ob das Zertifikat der Gegenstelle in der aktuellen CRL enthalten ist. So können Verbindungen zu Gegenstellen mit ungültigen Zertifikaten abgelehnt werden.

11.6.20.1 Konfiguration der CRL-Funktion

Die Adresse, von der eine Certificate Revocation List (CRL) abgeholt werden kann, wird normalerweise innerhalb der Zertifikate (als crlDistributionPoint) angegeben. Bei der Konfiguration der CRL-Funktion können zusätzliche Parameter wie das Update-Intervall angegeben werden.



Konfigurationstool	Aufruf
LANconfig	**Zertifikate** > **CRL-Client**
Konsole	**Setup** > **Zertifikate** > **CRLs**

CRL-Client-Funktionalität aktiviert

Bei der Prüfung der Gültigkeit eines Zertifikats wird eine ggf. vorhandene CRL herangezogen.

Wenn die CRL-Funktionalität aktiviert ist, werden bei Systemstart zunächst neue (zertifikatsbasierte) Verbindungen immer blockiert, bis es eine gültige CRL im System gibt, die zum Zertifikat passt. Wenn die CRL-Funktionalität aktiviert wird, bleiben bereits bestehende Verbindungen erhalten, ein nachfolgendes Rekeying der Phase 1 scheitert aber.

Abruf vor Ablauf (pro CRL)

Dieser Wert wird immer um eine Zufallskomponente von 0 bis 59 Sekunden erhöht, um gehäufte Anfragen an den Server zu vermeiden. Zu Beginn dieses Zeitraums wird ein eventuell laufendes regelmäßiges Abrufen gestoppt.

Wenn das Abrufen der CRL scheitert, so wird es alle 30 Sekunden erneut versucht.

Abruf regelmäßig (pro CRL)

Das Intervall zwischen regelmäßigen Versuchen, eine neue CRL herunterzuladen.

Falls die CA neue CRLs außer der Reihe (mitten im Gültigkeitszeitraum der aktuellen CRL) herausgibt, kann ein Intervall definiert werden, in dem nach dem Herunterladen der aktuellen CRL regelmäßig versucht wird, eine neue CRL herunterzuladen. Dadurch kann die neue CRL frühzeitig verwendet werden und nicht erst kurz vor Ablauf der Gültigkeit der aktuellen CRL. Ein Intervall von 0 schaltet diese Funktionalität aus.

Wenn die CRL bei regelmäßigen Update nicht geladen werden kann, werden keine Versuche bis zum nächsten regelmäßigen Termin gestartet.

Gültigkeitsprüfungs-Toleranz

Zertifikatsbasierte Verbindungen werden auch nach Ablauf der CRL-Gültigkeit noch innerhalb des hier eingetragenen Zeitraums zugelassen. Mit dieser Toleranz-Zeit kann verhindert werden, dass z. B. bei kurzfristig nicht erreichbarem CRL-Server die Verbindungen abgelehnt oder getrennt werden.

Innerhalb des hier eingestellten Zeitraums kann mit Hilfe der in der CRL bereits gesperrten Zertifikate weiterhin eine Verbindung aufrecht erhalten bzw. eine neue Verbindung aufgebaut werden.

Alternative URLs

Die Adresse, von der eine Certificate Revocation List (CRL) abgeholt werden kann, wird normalerweise innerhalb der Zertifikate (als crlDistributionPoint) angegeben. In der Firmware können in einer Tabelle alternative URLs angegeben werden. Nach dem Systemstart werden die entsprechenden CRLs automatisch von diesen URLs abgeholt und zusätzlich zu den in den Zertifikaten angegebenen Listen verwendet.

11.6.20.2 Anzeige des CRL-Status im LANmonitor

Informationen über die Gültigkeitsdauer und den Herausgeber der aktuellen CRL im Router können im LANmonitor unter **Zertifikate** > **CRLs** eingesehen werden.

11.6.21 Wildcard Matching von Zertifikaten

11.6.21.1 Einleitung

Bei zertifikatsbasierten VPN-Verbindungen werden in der Regel die Subjects (Antragsteller) der verwendeten Zertifikate als lokale und entfernte Identität verwendet. Diese werden in der VPN-Konfiguration in Form von (oftmals komplexen) ASN.1 Distinguished Names (DN) hinterlegt. In der VPN-Verhandlung wird dann die konfigurierte lokale Identität zur Auswahl des eigenen Zertifikates benutzt und an die Gegenstelle übermittelt, während die konfigurierte entfernte Identität mit der empfangenen Identität der Gegenstelle und mit dem Subject des empfangenen Zertifikates verglichen wird.

Die lokale und die entfernte Identität müssen in der VPN-Konfiguration bisher immer vollständig angegeben werden. Dies ist zum einen fehleranfällig, und zum anderen ist es manchmal gewünscht, nur einen Teil des Subjects angeben zu müssen. Praktisch ist dies beispielsweise, um bei einem Zertifikatswechsel oder bei gleichzeitiger Verwendung mehrerer paralleler Zertifikatshierarchien verschiedene Zertifikate mit ähnlichem Subject automatisch zu akzeptieren.

Um dies zu ermöglichen, kann ein flexiblerer Identitätsvergleich verwendet werden. Die in den konfigurierten Identitäten enthaltenen Komponenten eines ASN.1-Distinguished Name (DN) (Relative Distinguished Names – RDNs) müssen in den relevanten Subjects dabei nur enthalten sein. Die Reihenfolge der RDNs ist dabei beliebig. Darüber hinaus können

die Werte der RDNs die Wildcards „?“ und „*“ beinhalten. Werden die Wildcards als Teil des RDNs benötigt, müssen sie in Form von „\?“ bzw. „*“ angegeben werden. Beispiele:

- Subject = '/CN=Max Mustermann/O=*ACME*', DN = '/CN=Max?Muster*'
- Subject = '/CN=Max Mustermann/O=*ACME*', DN = '/O=*ACME*'

11.6.21.2 Konfiguration

Der flexible Identitätsvergleich kann in der VPN-Konfiguration aktiviert bzw. deaktiviert werden.

Konsole: **Setup** > **VPN** > **Flexibler-ID-Vergleich**

Mögliche Werte:

- Ja, Nein
- Default: Nein

Der flexible Identitätsvergleich wird sowohl bei der Prüfung der (empfangenen) entfernten Identität als auch bei der Zertifikatsauswahl durch die lokale Identität eingesetzt.

11.6.22 Diagnose der VPN-Zertifikatsverbindungen

Die folgenden Befehle an der Konsole können hilfreiche Aufschlüsse geben, sollte der VPN-Verbindungsaufbau nicht wie gewünscht funktionieren:

- `trace + vpn-status`

  Zeigt einen Trace der aktuellen VPN-Verbindungen.

- `show vpn long`

  Zeigt die Inhalte der VPN-Konfiguration, u. a. dabei die eingetragenen Distinguished Names (DN).

- `show vpn ca`

  Zeigt den Inhalt des Root-Zertifikats.

- `show vpn cert`

  Zeigt den Inhalt des eigenen Geräte-Zertifikats.

Die Relative Distinguished Names werden in dieser Darstellung bis Firmware-Version 6.00 in umgekehrter Reihenfolge, ab Firmware-Version 6.10 in der üblichen Reihenfolge angezeigt!

11.6.23 OCSP Client zur Zertifikatsüberprüfung

11.6.23.1 Einleitung

Das Online Certificate Status Protocol (OCSP) bietet eine Möglichkeit, den Status von Zertifikaten z. B. für den Aufbau von VPN-Verbindungen zu prüfen. Die Geräte nutzen dieses Protokoll, um zu untersuchen, ob der Herausgeber das verwendete Zertifikat evtl. schon vor dem Ablauf der Gültigkeit gesperrt und damit als ungültig markiert hat.

Der Herausgeber der Zertifikate pflegt den Status aller herausgegebenen Zertifikate auf einem speziellen Server, dem OCSP-Responder. Der OCSP-Client (also z. B. ein VPN-Router, der eine Verbindung aufbauen möchte) sendet einen OCSP-Request über das HTTP-Protokoll an den Responder, um den Status des Zertifikats zu ermitteln. Der Responder beantwortet diese Anfrage mit einer signierten Antwort, die der OCSP-Client auf ihre Gültigkeit hin prüft. Die Antwort des OCSP-Responders beschreibt einen der folgenden Zustände:

- good: Das überprüfte Zertifikat ist nicht gesperrt.
- evoked: Das überprüfte Zertifikat ist gesperrt und darf für den Aufbau von VPN-Verbindungen nicht mehr genutzt werden.

- unknown: Der OCSP-Responder kann den Status des Zertifikats nicht ermitteln, z. B. weil der OCSP-Responder den Herausgeber des Zertifikates nicht kennt oder weil das Zertifikat gefälscht und damit nicht in der Datenbasis des OCSP-Responders eingetragen ist.

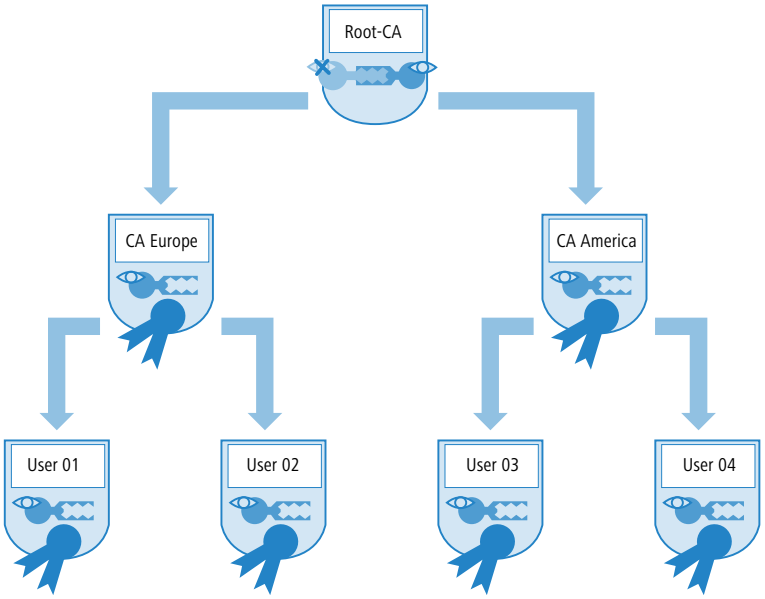
Sie können das OCSP als Ergänzung oder als Ersatz für die Überprüfung der Zertifikate mit Zertifikatfsrückruflisten (Certificate Revocation Lists – CRL) verwenden. OCSP bietet gegenüber dem Ansatz der CRL folgende Vorteile:

- Die Herausgeber erstellen die CRLs in bestimmten zeitlichen Intervallen und sorgen idealerweise für die Verteilung der CRLs in die Geräte, welche die Zertifikate für den Aufbau der VPN-Verbindungen einsetzen. Die Zuverlässigkeit dieser Überprüfung ist daher an die zeitliche Aktualisierung der CRLs in den Geräten gekoppelt. Die Überprüfung der Zertifikate mit Hilfe eines OCSP-Responders ist dagegen immer „online", also automatisch auf dem aktuellen Stand. Der Betreiber des OCSP-Responders kann die dort vorgehaltenen Daten z. B. über eine automatische Synchronisierung mit den Daten der CA oder CAs abgleichen und so für einen jederzeit aktuellen Stand sorgen.
- Die Prüfung der Zertifikate gegen die Zertifikatfsrückruflisten belastet insbesondere bei großen CRLs den Speicher der Geräte. Die Abfrage des Zertifikatsstatus von einem OCSP-Responder ist dagegen unabhängig von der Anzahl der verwendeten CAs und Zertifikate und daher besser skalierbar.
- Das CRL-Verfahren liefert bei unbekannten Zertifikaten kein Ergebnis – damit kann dieses Verfahren keine gefälschten Zertifikate erkennen. Der OCSP-Responder beantwortet je nach Konfiguration die Anfrage nach unbekannten Zertifikaten mit einer negativen Bewertung.

11.7 Mehrstufige Zertifikate für SSL/TLS

11.7.1 Einleitung

Bei großen oder räumlich verteilten Organisationen werden häufig mehrstufige Zertifikatshierarchien genutzt, bei der Endzertifikate durch eine oder mehrere Zwischen-CAs herausgegeben werden. Die Zwischen-CAs selbst sind dabei durch Root CA zertifiziert.



Für die Authentifizierung der Endzertifikate muss die Prüfung der gesamten Zertifikatshierarchie möglich sein.

11.7.2 SSL / TLS mit mehrstufigen Zertifikaten

Bei Anwendungen, die auf SSL / TLS basieren, (z. B. EAP / 802.1X, HTTPS oder RADSEC) wird das SSL-(Server-)Zertifikat samt privatem Schlüssel und den CA-Zertifikat(en) der Zwischenstufen als PKCS#12-Container in das Gerät geladen.

Die Gegenstellen müssen dann beim Verbindungsaufbau nur das eigene Gerätezertifikat an das Gerät senden. Die Zertifikatskette wird im Gerät auf Gültigkeit geprüft.

11.7.3 VPN mit mehrstufigen Zertifikaten

Für den zertifikatsbasierten Aufbau von VPN-Verbindungen werden im Dateisystem des Gerätes ein privater Schlüssel, ein Gerätezertifikat und das Zertifikat der CA abgelegt. Bei einstufigen Zertifikatslösungen können dazu sowohl die einzelnen Dateien, als auch eine PKCS#12-Datei verwendet werden. Nach dem Hochladen und der Eingabe des Kennworts wird ein solcher Container in die drei genannten Bestandteile zerlegt.

Bei einer mehrstufigen Zertifikatshierarchie muss hingegen ein PKCS#12-Container mit den Zertifikaten der CAs aller Stufen in der Zertifikatskette verwendet werden. Hier wird nach dem Hochladen und der Eingabe des Kennworts neben dem privaten Schlüssel und dem Gerätezertifikat das Zertifikat der nächsten CA „oberhalb" des Gerätes entpackt – die restlichen Zertifikate verbleiben im PKCS#12-Container. Beim Aktualisieren der VPN-Konfiguration werden die entpackten Zertifikate und die Zertifikate aus dem Container eingelesen. Beim Aufbau einer VPN-Verbindung übermittelt die Gegenstelle dann nur das eigene Geräte-Zertifikat, nicht jedoch die ganze Kette. Das Gerät kann dieses Zertifikat dann gegen die vorhandene Hierarchie prüfen.

Die Zertifikatsstrukturen müssen bei beiden Gegenstellen zueinander passen, d. h. die Hierarchie des anfragenden VPN-Gerätes darf keine Zertifikate erfordern, die in der Hierarchie des anderen VPN-Gerätes nicht enthalten sind.

11.8 Zertifikatsenrollment über SCEP

Zur Sicherung der Kommunikation über öffentlich zugängliche Netzwerke werden immer mehr zertifikatsbasierte VPN-Verbindungen eingesetzt. Dem hohen Sicherheitsanspruch der digitalen Zertifikate steht dabei ein deutlicher Mehraufwand für die Verwaltung und Verteilung der Zertifikate gegenüber. Dieser Aufwand entsteht dabei überwiegend in den Filialen oder Home-Offices einer verteilten Netzwerkstruktur.

Zum Aufbau einer zertifikatsbasierten VPN-Verbindung von einer Außenstelle zum Netzwerk einer Zentrale benötigt ein VPN-Router die folgenden Komponenten:

- Zertifikat der Root-CA mit dem Public Key der CA. In der Zentrale muss ebenfalls ein Zertifikat vorliegen, welches von derselben CA ausgestellt worden ist.
- Eigenes Geräte-Zertifikat mit dem eigenen Public Key. Dieses Zertifikat ist mit dem Private Key der CA signiert und stellt die Bestätigung der Identität dar.
- Eigenen privaten Schlüssel (Private Key).

Der SCEP-Client unterstützt ein Zertifikat pro Verwendungszweck (VPN, WLAN-Controller). Bei den CAs kann neben dem konkreten Verwendungszweck auch die Einstellung „Allgemein" gewählt werden. Wenn eine allgemeine CA eingetragen wird, wird diese CA für alle Zertifikate verwendet.

Beim herkömmlichen Aufbau einer VPN-Struktur mit Zertifikaten müssen die Schlüssel und Zertifikate manuell in die einzelnen Geräte geladen werden und rechtzeitig vor Ablauf getauscht werden. Das Simple Certificate Enrollment Protocol (SCEP) erlaubt die sichere und automatisierte Verteilung von Zertifikaten über einen entsprechenden Server und reduziert so den Aufwand für den Roll-Out und die Pflege von zertifikatsbasierten Netzwerkstrukturen. Dabei wird u. a. das Schlüsselpaar für das Gerät nicht in einer externen Anwendung erstellt und später in das Gerät übertragen, sondern das Schlüsselpaar wird direkt im VPN-Router selbst erzeugt – der private Teil des Schlüssels muss also niemals das Gerät verlassen, was einen deutlichen Sicherheitsgewinn darstellt. Sowohl das Root-Zertifikat der CA als auch das eigene Geräte-Zertifikat kann ein VPN-Router über SCEP automatisiert von einer zentralen Stelle abrufen.

11.8.1 SCEP-Server und SCEP-Client

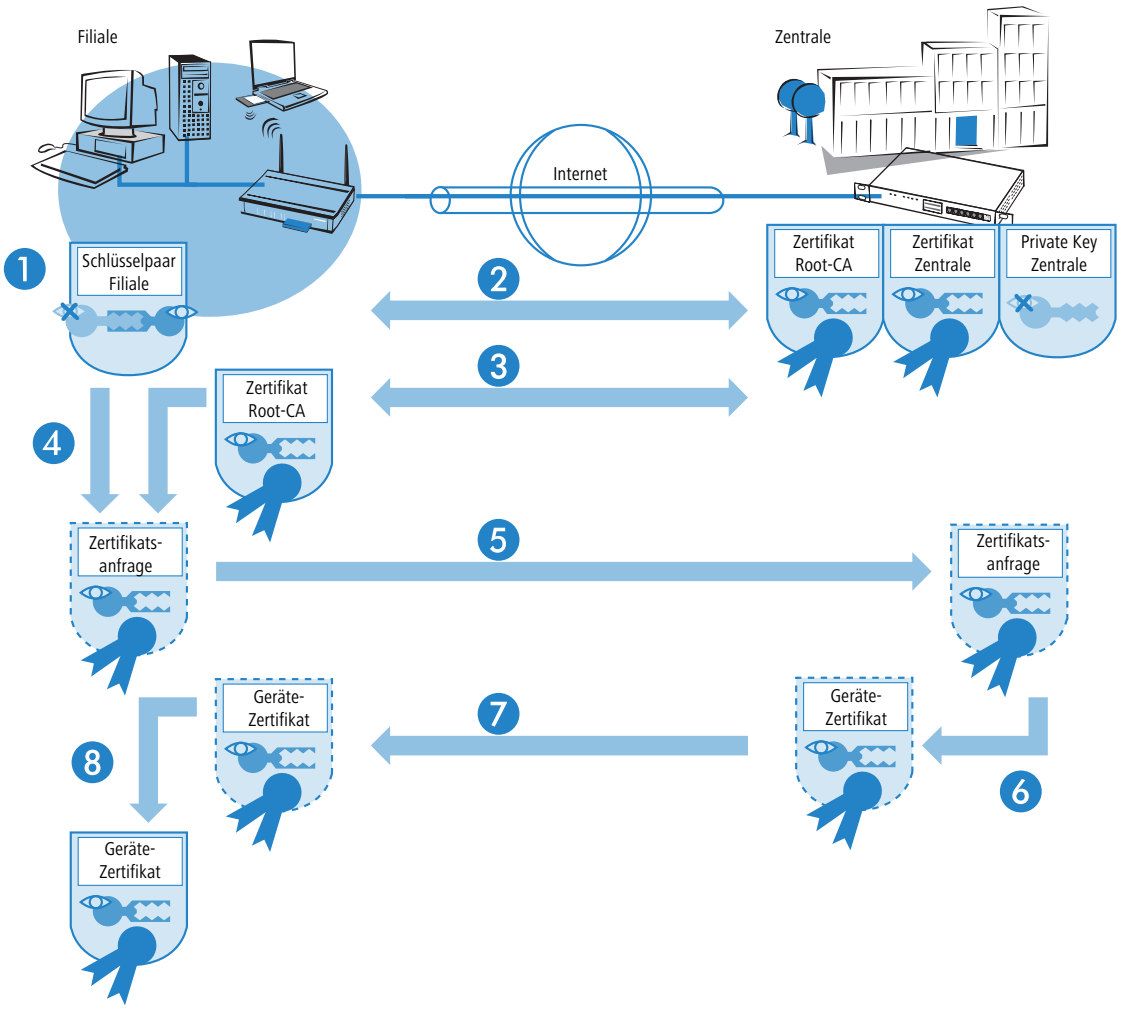
Die Bereitstellung und Verwaltung der Zertifikate wird von einem SCEP-Server vorgenommen, der neben der Funktion einer üblichen Certification Authority (CA) um die SCEP-Funktionalität erweitert ist. Dieser Server kann z. B. als Windows Server CA mit einem speziellen Plug-In (der mscep.dll) realisiert werden. Es existieren daneben eine Vielzahl von CA-Lösungen die SCEP beherrschen, so beispielsweise die OpenSource-Lösung OpenCA (www.openca.org).

Die SCEP-Erweiterung, also z. B. die mscep.dll, bildet eine zusätzliche Instanz auf dem Server, welche die Anfragen der SCEP-Clients bearbeitet und an die eigentliche CA weiterreicht. Diese Instanz wird als Registration Authority (RA) bezeichnet.

Als SCEP-Clients treten die VPN-Router auf, die vom zentralen Server die benötigten Zertifikate automatisiert abrufen wollen. Für den SCEP-Vorgang werden i.d.R. auch die von der CA signierten Zertifikate der RA (Registration Authority) benötigt. Für den eigentlichen VPN-Betrieb benötigen die VPN-Router dabei vor allem gültige Systemzertifikate (Gerätezertifikate). Die anderen ggf. genutzten Zertifikate werden nur für den SCEP-Vorgang benötigt.

11.8.2 Der Ablauf einer Zertifikatsverteilung

Im Überblick verläuft die Verteilung von Zertifikaten über SCEP nach folgendem Schema ab:



1. Schlüsselpaar im VPN-Router erzeugen.

   Im VPN-Router wird ein Schlüsselpaar erzeugt. Der öffentliche Teil dieses Schlüsselpaares wird später zusammen mit der Anfrage an den SCEP-Server übermittelt. Der private Teil des Schlüsselpaares verbleibt im SCEP-Client (VPN-Router).

Die Tatsache, dass der private Schlüssel das Gerät zu keiner Zeit verlassen muss, stellt einen Sicherheitsgewinn gegenüber der manuellen Zertifikatsverteilung über z. B. PKCS#12-Container dar.

2. CA- und RA-Zertifikate abrufen.

   Zur Kommunikation mit der RA/CA müssen im VPN-Router die entsprechenden RA- und CA-Zertifikate vorhanden sein. Bei einem Abruf des CA-Zertifikates über SCEP kann mit dem im Vorfeld konfigurierten Fingerprint automatisch geprüft werden, ob die abgerufenen Zertifikate auch tatsächlich von der gewünschten CA stammen. SCEP bietet selbst keinen Mechanismus zur automatischen Authentifizierung der CA-Zertifikate auf Seiten des SCEP-Clients. Wenn der Administrator der VPN-Router nicht selbst Zugriff auf die CA hat, muss er den Fingerprint z. B. per Telefon mit dem CA-Admin überprüfen.

3. Request für ein Geräte-Zertifikat erstellen und verschlüsseln.

   Für die Beantragung eines System- bzw. Gerätezertifikats stellt der SCEP-Client die konfigurierten Informationen zusammen, u. a. die Identität des anfragenden Gerätes (Requester) und ggf. die „Challenge Phrase", das Kennwort für die automatische Bearbeitung der Anfrage auf dem SCEP-Server. Diese Anfrage wird mit dem privaten Teil des Schlüsselpaares signiert.

4. Request an den SCEP-Server übermitteln.

   Anschließend übermittelt der SCEP-Client die Anfrage mitsamt seinem öffentlichen Schlüssel an den SCEP-Server.

5. Prüfen der Zertifikatsanfrage auf dem SCEP-Server und Ausstellen des Geräte-Zertifikats.

   Der SCEP-Server kann die erhaltene Anfrage entschlüsseln und daraufhin ein System- bzw. Gerätezertifikat für den Requester ausstellen. SCEP unterscheidet dabei folgende Methoden für die Bearbeitung der Anfragen:

   - Bei der automatischen Bearbeitung muss die Authentizität des Requesters über die Challenge Phrase sichergestellt sein. Die Challenge Phrase wird z. B. auf einem Windows CA-Server mit mscep.dll automatisch erzeugt und ist für eine Stunde gültig. Stimmt die Challenge Phrase in der Zertifikatsanfrage mit dem aktuell gültigen Wert auf dem Server überein, kann das Systemzertifikat automatisch ausgestellt werden.
   - Im manuellen Fall stellt der SCEP-Server die Zertifikatsanfrage in einen Wartezustand, bis die Bewilligung oder Ablehnung des CA-Administrators feststeht. Während dieser Wartezeit prüft der SCEP-Client regelmäßig ab, ob inzwischen beim SCEP-Server das angeforderte Systemzertifikat ausgestellt wurde.
   - Bei RA-AutoApprove wird der Client über ein gültiges von der CA ausgestelltes Zertifikat authentifiziert.

6. Geräte-Zertifikat vom SCEP-Server abrufen

   Sobald das Zertifikat ausgestellt ist, stellt der Client durch regelmäßiges Polling fest, dass er das Zertifikat abrufen kann.

7. Geräte-Zertifikat prüfen und für VPN-Betrieb bereitstellen

11.8.3 Konfiguration von SCEP

Zur Konfiguration von SCEP werden globale Parameter für den SCEP-Betrieb und die CAs definiert, von denen die Geräte-Zertifikate abgerufen werden können.

Neben der Konfiguration des SCEP-Parameter ist ggf. eine Anpassung der VPN-Konfigurationen erforderlich.

Konfigurationstool	Aufruf
WEBconfig, CLI	LCOS-Menübaum > Setup > Zertifikate > SCEP-Client

11.8.3.1 Globale SCEP-Parameter

- Aktiv

  Schaltet die Nutzung von SCEP ein oder aus.

  - Mögliche Werte: Ja, Nein
  - Default: Nein

- Wiederholen-Nach-Fehler-Intervall

  Intervall in Sekunden für Wiederholungen nach jeglicher Art von Fehler.

  - Default: 22

- Ausstehende-Anfragen-Prüfen-Intervall

  Intervall in Sekunden für das Prüfen von ausstehenden Zertifikatsanfragen.

  - Default: 101

- Systemzertifikate-Aktualisieren-Vor-Ablauf

  Vorlaufzeit in Tagen zur rechtzeitigen Beantragung neuer Systemzertifikate (Gerätezertifikate).

  - Default: 2

- CA-Zertifikate-Aktualisieren-Vor-Ablauf

  Vorlaufzeit in Tagen zur rechtzeitigen Abholung neuer RA/CA-Zertifikate.

  - Default: 1

11.8.3.2 Aktionen

- Reinit

  Startet die manuelle Re-Initialisierung der SCEP-Parameter. Dabei werden wie bei der gewöhnlichen SCEP-Initialisierung auch die notwendigen RA- und CA-Zertifikate von der CA abgerufen und so im Dateisystem des VPN-Routers abgelegt, dass sie noch **nicht** für die Nutzung im VPN-Betrieb bereit stehen.

  - Sofern das vorhandene Systemzertifikat zum abgerufenen CA-Zertifikat passt, können Systemzertifikat, CA-Zertifikat und privater Geräteschlüssel für den VPN-Betrieb genutzt werden.
  - Sofern die vorhandenen Systemzertifikate **nicht** zum abgerufenen CA-Zertifikat passen, muss zunächst eine neue Zertifikatsanfrage beim SCEP-Server gestellt werden. Erst wenn so ein neues, zum CA-Zertifikat passendes Systemzertifikat ausgestellt und abgerufen wurde, können Systemzertifikat, CA-Zertifikat und privater Geräteschlüssel für den VPN-Betrieb genutzt werden.

- Aktualisieren

  Startet manuell die Anfrage nach einem neuen Systemzertifikat, unabhängig von der verbleibenden Gültigkeitsdauer. Dabei wird ein neues Schlüsselpaar erzeugt.

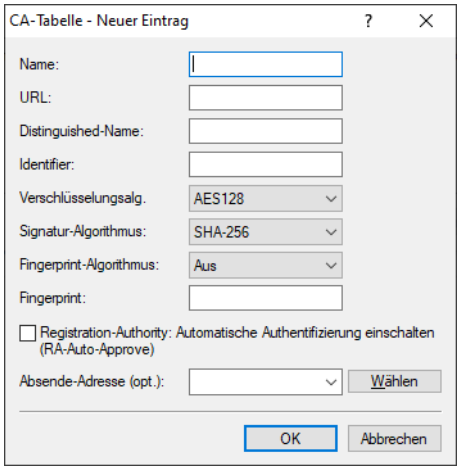
- Bereinige-SCEP-Dateisystem

  Startet die Bereinigung des SCEP-Dateisystems.

  - gelöscht werden: RA-Zertifikate, ausstehende Zertifikatsanfragen, neue und inaktive CA-Zertifikate, neue und inaktive private Schlüssel.
  - erhalten bleiben: aktuell im VPN-Betrieb genutzte Systemzertifikate, private Schlüssel dazu und die aktuell im VPN-Betrieb genutzten CA-Zertifikate.

11.8.3.3 Konfiguration der CAs

Die Konfiguration erfolgt in LANconfig unter **Zertifikate** > **SCEP-Client** mit der Schaltfläche **CA-Tabelle**.



Name

Konfigurationsname der CA.

URL

URL der CA.

Distinguished-Name

Distinguished Name der CA. Über diesen Parameter erfolgt einerseits die Zuordnung von CAs zu Systemzertifikaten (und umgekehrt). Andererseits spielt dieser Parameter auch eine Rolle bei der Bewertung, ob erhaltene oder vorhandene Zertifikate der Konfiguration entsprechen.

Durch die Verwendung eines vorangestellten Backslash („\") können Sie auch reservierte Zeichen benutzen. Diese unterstützten reservierten Zeichen sind:

- Komma („,")
- Slash („/")
- Plus („+")
- Semikolon („;")
- Gleich („=")

Außerdem lassen sich die folgenden internen Firmware-Variablen nutzen:

- %% fügt ein Prozentzeichen ein.
- %f fügt die Version und das Datum der aktuellen im Gerät aktiven Firmware ein.
- %r fügt die Hardware-Release des Gerätes ein.
- %v fügt die Version des aktuellen im Gerät aktiven Loaders ein.
- %m fügt die MAC-Adresse des Gerätes ein.
- %s fügt die Seriennummer des Gerätes ein.
- %n fügt den Namen des Gerätes ein.
- %l fügt den Standort des Gerätes ein.
- %d fügt den Typ des Gerätes ein.

Identifier

CA-Identifier (wird von manchen Webservern benötigt, um die CA zuordnen zu können).

Encryption-Algorithmus

Mit diesem Algorithmus wird die Nutzlast des Zertifikatsantrages verschlüsselt. Mögliche Werte sind:

- 3-DES
- AES128 (Default)
- AES192
- AES256

Signatur-Algorithmus

Mit diesem Algorithmus wird der Zertifikatsantrag signiert. Mögliche Werte sind:

- MD5
- SHA1
- SHA256 (Default)
- SHA384
- SHA512

Fingerprint-Algorithmus

Algorithmus zum Signieren der Fingerprints. Legt fest, ob eine Überprüfung der CA-Zertifikate anhand des Fingerprints vorgenommen wird und mit welchem Algorithmus. Der CA-Fingerprint muss mit der Prüfsumme übereinstimmen, die sich bei Verwendung des Algorithmus ergibt. Mögliche Werte sind:

- Aus (Default)
- MD5
- SHA1
- SHA256
- SHA384
- SHA512

Fingerprint

Anhand der hier eingetragenen Prüfsumme (Fingerprint) kann die Authentizität des erhaltenen CA-Zertifikates überprüft werden (entsprechend des eingestellten CA-Fingerprintalgorithmus).

RA-Autoapprove

Manche CAs bieten die Möglichkeit, ein bereits von dieser CA ausgestelltes Zertifikat als Nachweis der Authentizität für nachfolgende Anträge zu benutzen. Mit dieser Option wird festgelegt, ob bei bereits vorliegendem Systemzertifikat Neuanträge mit dem vorhandenen Systemzertifikat unterschrieben werden. Mögliche Werte sind:

- Ja
- Nein (Default)

Absende-Adresse

Hier konfigurieren Sie optional eine Absendeadresse, die statt der ansonsten automatisch für die Zieladresse gewählten Absendeadresse verwendet wird. Falls Sie z. B. Loopback-Adressen konfiguriert haben, können Sie diese hier als Absendeadresse angeben.

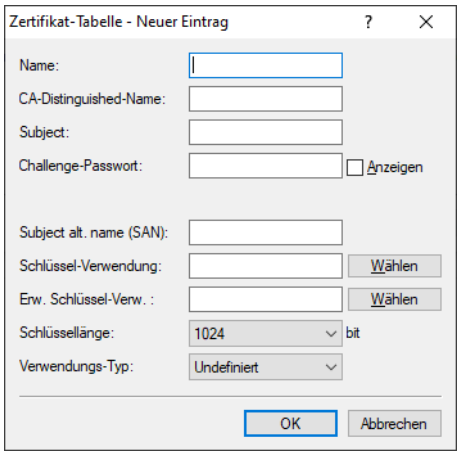
Als Adresse werden verschiedene Eingabeformen akzeptiert:

- Name des IP-Netzwerkes (ARF-Netz), dessen Adresse eingesetzt werden soll.
- "INT" für die Adresse des ersten Intranets.
- "DMZ" für die Adresse der ersten DMZ (Achtung: wenn es eine Schnittstelle Namens "DMZ" gibt, dann wird deren Adresse genommen).
- LB0 ... LBF für eine der 16 Loopback-Adressen oder deren Name.
- Des Weiteren kann eine beliebige IP-Adresse in der Form x.x.x.x angegeben werden.

Sofern die hier eingestellte Absendeadresse eine Loopback-Adresse ist, wird diese auch auf maskiert arbeitenden Gegenstellen unmaskiert verwendet.

11.8.3.4 Konfiguration der Zertifikat-Tabellen

Die Konfiguration erfolgt in LANconfig unter **Zertifikate** > **SCEP-Client** mit der Schaltfläche **Zertifikat-Tabelle**.



Name

Konfigurationsname des Zertifikats.

CA-Distinguished-Name

Distinguished Name der CA. Über diesen Parameter erfolgt einerseits die Zuordnung von CAs zu Systemzertifikaten (und umgekehrt). Andererseits spielt dieser Parameter auch eine Rolle bei der Bewertung, ob erhaltene bzw. vorhandene Zertifikate der Konfiguration entsprechen.

Durch die Verwendung eines vorangestellten Backslash („\") können Sie auch reservierte Zeichen benutzen. Diese unterstützten reservierten Zeichen sind:

- Komma („,")
- Slash („/")
- Plus („+")
- Semikolon („;")
- Gleich („=")

Außerdem lassen sich die folgenden internen Firmware-Variablen nutzen:

- %% fügt ein Prozentzeichen ein.
- %f fügt die Version und das Datum der aktuellen im Gerät aktiven Firmware ein.
- %r fügt die Hardware-Release des Gerätes ein.
- %v fügt die Version des aktuellen im Gerät aktiven Loaders ein.
- %m fügt die MAC-Adresse des Gerätes ein.
- %s fügt die Seriennummer des Gerätes ein.
- %n fügt den Namen des Gerätes ein.
- %l fügt den Standort des Gerätes ein.
- %d fügt den Typ des Gerätes ein.

Subject

Distinguished Name des Subjects des Antragstellers.

Challenge-Passwort

Kennwort (für das automatische Ausstellen der Geräte-Zertifikate auf dem SCEP-Server).

Subject alt. name (SAN)

Weitere Angaben zum Requester, z. B. Domain oder IP-Adresse.

Schlüssel-Verwendung

Beliebige kommaseparierte Kombination aus:

- digitalSignature
- nonRepudiation
- keyEncipherment
- dataEncipherment
- keyAgreement
- keyCertSign
- cRLSign
- encipherOnly
- decipherOnly
- critical (möglich aber nicht empfohlen)

Erw. Schlüssel-Verw.

Beliebige kommaseparierte Kombination aus:

- critical
- serverAuth
- clientAuth
- codeSigning
- emailProtection
- timeStamping
- msCodeInd
- msCodeCom
- msCTLSign
- msSGC
- msEFS
- nsSGC
- 1.3.6.1.5.5.7.3.18 für WLAN-Controller
- 1.3.6.1.5.5.7.3.19 für Access Points im Managed-Modus

Schlüssellänge

Die Schlüssellänge in Bits. Mögliche Werte:

- 1024
- 2048
- 4096
- 8192

Verwendungs-Typ

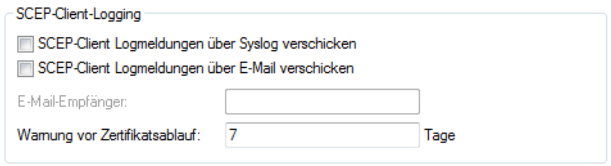
Gibt den Verwendungszweck der eingetragenen Zertifikate an. Die hier eingetragenen Zertifikate werden dann nur für den entsprechenden Verwendungszweck abgefragt. Mögliche Werte:

- VPN
- WLAN-Controller
- EAP/TLS
- CA

› Default Zertifikat

11.8.3.5 SCEP-Client-Logging

LANconfig: **Zertifikate** > **SCEP-Client** > **SCEP-Client-Logging**



SCEP-Client Logmeldungen über Syslog verschicken

Aktiviert / deaktiviert das Verschicken der Logmeldung über SYSLOG.

SCEP-Client Logmeldungen über E-Mail verschicken

Aktiviert / deaktiviert das Verschicken der Logmeldung per E-Mail.

Hierzu tragen Sie bitte eine E-Mail-Adresse in das folgende Eingabefenster ein.

E-Mail-Empfänger

E-Mail-Adresse zum Empfang der Logmeldung.

Um eine Eintragung vorzunehmen, muss zuvor **SCEP-Client Logmeldungen über E-Mail verschicken** aktiviert worden sein.

Warnung vor Zertifikatsablauf

Zeitintervall bis zum Ablauf des Zertifikates in Tagen.

11.8.4 Verwendung digitaler Zertifikate (Smart Certificate)

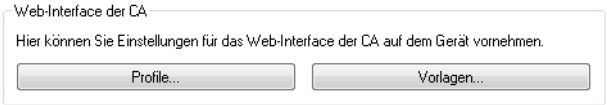
Die Konfiguration des SCEP-Clients für die Erstellung und Verteilung von Zertifikaten wird in einer komplexen und ausgedehnten Netz-Infrastruktur schnell aufwändig. Durch vordefinierte, auswählbare Profile und den Zugriff über eine Web-Schnittstelle lässt sich dieser Aufwand reduzieren.

Mit einem LANCOM Router haben Sie die Möglichkeit, hochsichere Zertifikate zu generieren und zuzuweisen. Sie verwalten die Zertifikate bequem über die WEBconfig-Oberfläche des entsprechenden Gerätes. Eine externe Zertifizierungsstelle ist somit nicht mehr erforderlich, was gerade bei kleineren Infrastrukturen vorteilhaft ist.

Mit dem Zertifikats-Wizard von LANCOM können selbst Anwender ohne Zertifikats-Knowhow in wenigen Schritten Zertifikate erstellen.

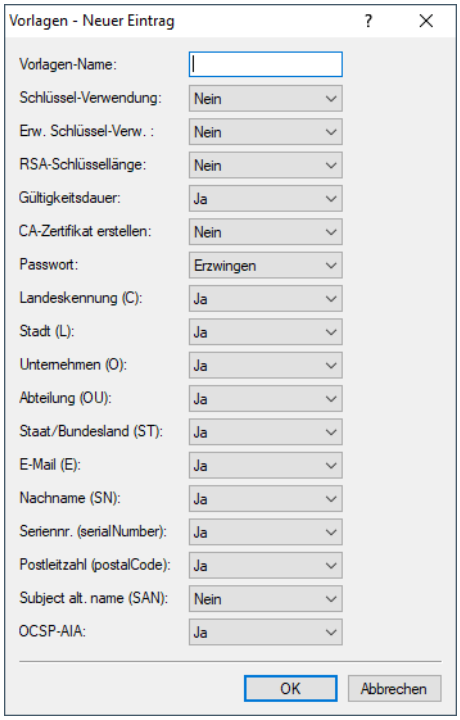
Der Geräte-Administrator erstellt das Profil als Sammlung von Zertifikats-Eigenschaften. Es enthält einerseits die Konfiguration des Zertifikates sowie eine eindeutige Zertifikats-ID. Statt also alle Zertifikats-Parameter einzugeben, genügt es von da an, eines der angezeigten Profile auszuwählen, um ein Zertifikat zu erstellen und zu verteilen.

Die Verwaltung von Profilen erfolgt auch im LANconfig unter **Zertifikate** > **Zertifikatsbehandlung** im Abschnitt **Web-Interface der CA**.



11.8.4.1 Vorlagen für Zertifikats-Profile erstellen

In LANconfig erfolgt die Profil-Erstellung unter **Zertifikate** > **Zertifikatsbehandlung** > **Vorlagen**.



Standardmäßig ist bereits eine Vorlage „DEFAULT“ angelegt.

Der Adminstrator legt fest, welche der Profileigenschaften erforderlich und welche durch den Anwender zu editieren sind. Die folgenden Optionen stehen zur Auswahl:

- Nein: Das Feld ist unsichtbar, der eingetragene Wert gilt als Defaultwert.
- Fest: Das Feld ist sichtbar, aber nicht durch den Anwender änderbar.
- Ja: Das Feld ist sichtbar und durch den Anwender änderbar.
- Erzwingen: Das Feld ist sichtbar, der Anwender muss einen Wert eintragen.

Diese Zugriffsrechte gelten für die folgenden Profil- und ID-Felder:

Profilfelder

- Schlüssel-Verwendung
- weit. Verwendungszweck
- RSA-Schlüssellänge
- Gültigkeitsdauer
- CA-Zertifikat erstellen
- Passwort

Identifier

- Landeskennung (C)
- Stadt (L)
- Unternehmen (O)
- Abteilung (OU)
- Staat / Bundesland (ST)
- E-Mail (E)

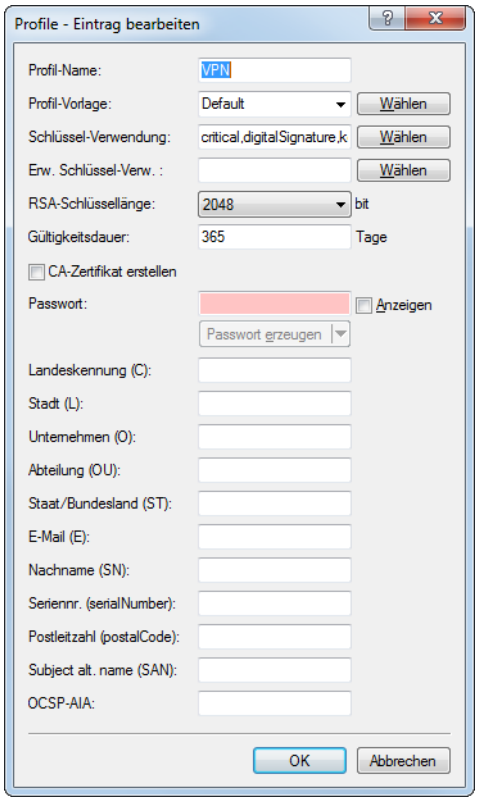
- Nachname (SN)
- Seriennr. (serialNumber)
- Postleitzahl (postalCode)
- Subject alt. name
- OCSP-AIA

Bei leerer Vorlagen-Tabelle sieht der Anwender nur Eingabefelder für die Profilnamen, die allgemeinen Namen (CN) sowie das Passwort. Die restlichen Profilfelder behalten die vom Geräte-Administrator festgelegten Defaultwerte.

11.8.4.2 Erstellen eines Profils in LANconfig

Der Anwender benötigt für Erstellung, Auswahl, Änderung und Zuweisung der Profile die entsprechenden Zugriffsrechte.

In LANconfig erfolgt die Profil-Erstellung unter **Zertifikate** > **Zertifikatsbehandlung** > **Profile**.



Standardmäßig sind bereits drei Profile für gängige Anwendungsszenarien angelegt.

Profil-Name

Der eindeutige Name des Profils.

Profil-Vorlage

Wählen Sie hier ggf. eine passende Profil-Vorlage aus.

In der Profil-Vorlage ist festgelegt, welche Zertifikatsangaben notwendig und welche änderbar sind. Die Vorlagen-Erstellung erfolgt unter **Zertifikate** > **Zertifikats-Behandlung** > **Vorlagen**.

Schlüssel-Verwendung

Gibt an, für welche Verwendung das Profil einzusetzen ist. Die folgenden Verwendungen stehen über die Schaltfläche **Wählen** zur Auswahl:

Tabelle 26: Zur Verfügung stehende Schlüssel-Verwendungen

Wert	Bedeutung
critical	Ist diese Einschränkung gesetzt, ist es immer erforderlich, die Schlüsselverwendungs-Erweiterung zu beachten. Wird die Erweiterung nicht unterstützt, wird das Zertifikat als nicht gültig abgelehnt.
digitalSignature	Ist diese Option gesetzt, wird der öffentliche Schlüssel für digitale Signaturen verwendet.
nonRepudiation	Ist diese Option gesetzt, wird der Schlüssel für digitale Signaturen eines Nichtabstreitbarkeitsservice verwendet. D. h., dass dieser eher einen langfristigen Charakter besitzt, wie z. B. ein Notariatsservice.
keyEncipherment	Ist diese Option gesetzt, wird der Schlüssel für die Verschlüsselung von anderen Schlüsseln oder Sicherheitsinformation verwendet. Es ist möglich, die Verwendung mit **encipher only** und **decipher only** einzuschränken.
dataEncipherment	Ist diese Option gesetzt, wird der Schlüssel zur Verschlüsselung von Benutzerdaten (außer andere Schlüssel) verwendet.
keyAgreement	Ist diese Option gesetzt, wird der "Diffie-Hellman" Algorithmus für die Schlüsselvereinbarung verwendet.
keyCertSign	Ist diese Option gesetzt, wird der Schlüssel für die Verifikation von Signaturen auf Zertifikaten verwendet. Dies ist z. B. für CA-Zertifikate sinnvoll.
cRLSign	Ist diese Option gesetzt, wird der Schlüssel für die Verifikation von Signaturen auf CRLs verwendet. Dies ist z. B. für CA-Zertifikate sinnvoll.
encipherOnly	Ist nur mit der Schlüsselvereinbarung nach Diffie Hellman (keyAgreement) sinnvoll.
decipherOnly	Ist nur mit der Schlüsselvereinbarung nach Diffie Hellman (keyAgreement) sinnvoll.

Eine kommagetrennte Mehrfachauswahl ist möglich.

Erw. Schlüssel-Verw.

Gibt an, für welche erweiterte Verwendung das Profil einzusetzen ist. Die folgenden Verwendungen stehen über die Schaltfläche **Wählen** zur Auswahl:

Tabelle 27: Erweiterte Verwendungen

Wert	Bedeutung
critical	
serverAuth	SSL/TLS-Web-Server-Authentifizierung
clientAuth	SSL/TLS-Web-Client-Authentifizierung
codeSigning	Signierung von Programmcode
emailProtection	E-Mail-Schutz (S/MIME)
timeStamping	Daten mit zuverlässigen Zeitstempeln versehen
msCodeInd	Microsoft Individual Code Signing (authenticode)
msCodeCom	Microsoft Commercial Code Signing (authenticode)
msCTLSign	Microsoft Trust List Signing
msSGC	Microsoft Server Gated Crypto

Wert	Bedeutung
msEFS	Microsoft Encrypted File System
nsSGC	Netscape Server Gated Crypto

Eine kommagetrennte Mehrfachauswahl ist möglich.

RSA-Schlüssellänge

Gibt die Länge des Schlüssels an.

Gültigkeitsdauer

Gibt die Zeitdauer in Tagen an, für die der Schlüssel gültig ist. Nach Ablauf dieser Frist verliert der Schlüssel seine Gültigkeit, falls der Anwender ihn nicht vorher erneuert.

CA-Zertifikat erstellen

Gibt an, ob es sich um ein CA-Zertifikat handelt.

Passwort

Passwort, um die PKCS12-Zertifikatsdatei abzusichern.

Die folgenden Eingaben dienen zur Erstellung einer Zertifikats-ID. Zur Auswahl stehen die folgenden Optionen:

Landeskennung (C)

Geben Sie die Staatenkennung ein (z. B. „DE" für Deutschland).

Im Subject oder Issuer des Zertifikates erscheint dieser Eintrag unter `C=` (**C**ountry).

Stadt (L)

Geben Sie den Ort ein.

Im Subject oder Issuer des Zertifikates erscheint dieser Eintrag unter `L=` (**L**ocality).

Unternehmen (O)

Geben Sie das Unternehmen an, welches das Zertifikat ausstellt.

Im Subject oder Issuer des Zertifikates erscheint dieser Eintrag unter `O=` (**O**rganization).

Abteilung (OU)

Geben Sie die Abteilung an, die das Zertifikat ausstellt.

Im Subject oder Issuer des Zertifikates erscheint dieser Eintrag unter `OU=` (**O**rganization **U**nit).

Staat / Bundesland (ST)

Geben Sie das Bundesland ein.

Im Subject oder Issuer des Zertifikates erscheint dieser Eintrag unter `ST=` (**ST**ate).

E-Mail (E)

Geben Sie eine E-Mail-Adresse ein.

Im Subject oder Issuer des Zertifikates erscheint dieser Eintrag unter `emailAddress=`.

Nachname (SN)

Geben Sie einen Nachnamen ein.

Im Subject oder Issuer des Zertifikates erscheint dieser Eintrag unter `SN=` (**S**ur**N**ame).

Seriennr. (serialNumber)

Geben Sie eine Seriennummer ein.

Im Zertifikat erscheint dieser Eintrag unter `serialNumber=`.

Postleitzahl (postalCode)

Geben Sie die Postleitzahl des Ortes ein.

Im Subject oder Issuer des Zertifikates erscheint dieser Eintrag unter `postalCode=`.

Subject alt. Name (SAN)

Mit dem „Subject-Alternative-Name“ (SAN) verknüpfen Sie weitere Daten mit diesem Zertifikat. Die folgenden Daten sind möglich:

- E-Mail-Adressen
- IPv4- oder IPv6-Adressen
- URIs
- DNS-Namen
- Verzeichnis-Namen
- Beliebige Namen

Im Subject oder Issuer des Zertifikates erscheint dieser Eintrag unter `subjectAltName=` (z. B. `subjectAltName=IP:192.168.7.1`).

OCSP-AIA

Dieses Feld wird für den OCSP-Server benötigt. Es enthält den Namen oder die IP-Adresse, unter dem der OCSP-Server für die OCSP-Clients erreichbar ist. Siehe *OCSP-Server* auf Seite 820.

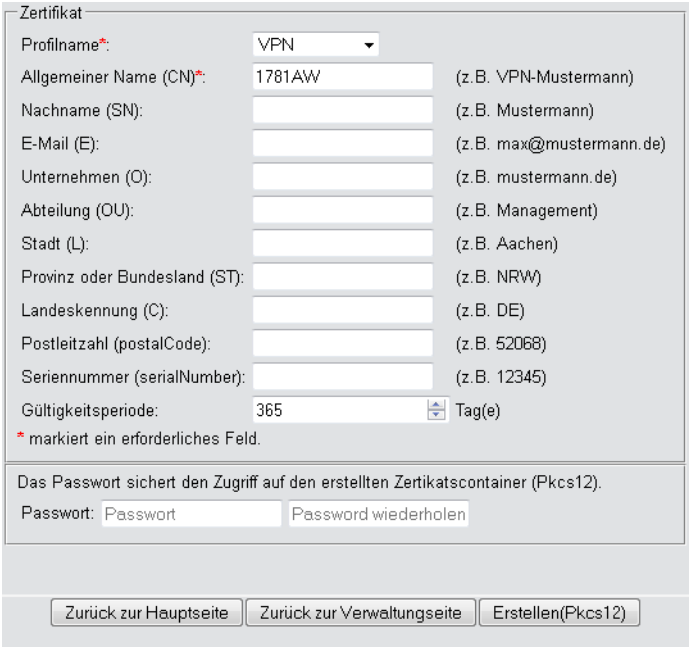
Der Zertifikatersteller vergibt den allgemeinen Namen "CN". Die Angabe des "CN" ist mindestens erforderlich.

11.8.4.3 Zertifikaterstellung über WEBconfig

Sie benötigen für Auswahl, Änderung und Zuweisung der Profile die entsprechenden Zugriffsrechte.

Zur Zertifikaterstellung wechseln Sie in die WEBconfig des LANCOM-Gerätes.

1. Um über die Webschnittstelle ein Zertifikat zu erstellen, wechseln Sie in die Ansicht **Setup-Wizards** > **Zertifikate verwalten** und wählen Sie **Neues Zertifikat erstellen**.



2. Wählen Sie im Dropdown-Menü **Profilname** das Profil aus, auf dem das Zertifikat beruhen soll.

   Leere Vorlagen enthalten nur Felder mit der Auswahl „Nein“. Wählt der Anwender ein Profil aus, das auf einer leeren Vorlage basiert, erscheint in der Eingabemaske nur der allgemeine Name (Common-name). Die restlichen Profilfelder behalten die vom Geräte-Administrator festgelegten Defaultwerte.

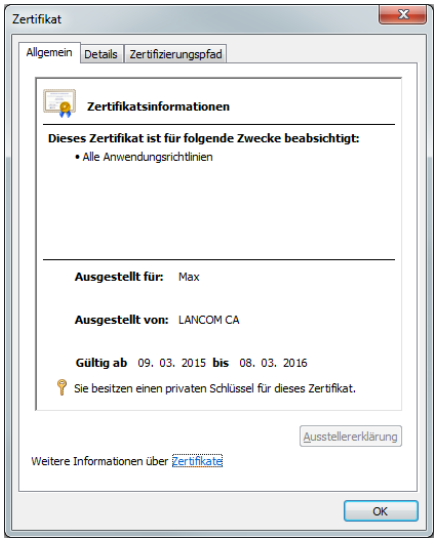
3. Füllen Sie das Feld **Allgemeiner Name (CN)** aus. Definieren Sie eine Gültigkeitsperiode für das Zertifikat und vergeben Sie ein sicheres Passwort (PIN). Die übrigen Felder wie **E-Mail**, **Unternehmen** etc. sind optionale Informationen. Sie erleichtern jedoch ggf. die schnellere Suche des Zertifikat-Empfängers, wenn es zu Problemen mit dem Zertifikat kommen sollte.

   Für das Passwort sind folgende Zeichen zulässig: [A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

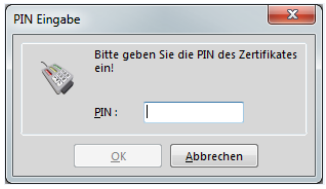
4. Zum Abschluss der Änderungen klicken Sie auf die Schaltfläche **Erstellen (PKCS12)**. Im darauf folgenden Speicherdialog haben Sie die Möglichkeit, den Namen und Speicherort der Datei festzulegen.

   Die so neu erstellten Zertifikate erscheinen in der Zertifikate-Status-Tabelle unter **Status** > **Zertifikate** > **SCEP-CA** > **Zertifikate**.

5. Übergeben Sie dem Empfänger das erstellte Zertifikat zusammen mit dem Zugangspasswort, das Sie in Schritt 3 vergeben haben.



6. Der Empfänger hat jetzt die Möglichkeit einer sicheren VPN-Einwahl. Für eine erfolgreiche Einwahl ist die Eingabe des Zugangspasswortes (PIN) erforderlich, das Sie in Schritt 3 vergeben haben.



11.8.4.4 Zertifikatverwaltung über die WEBconfig

Sie benötigen für die Verwaltung der Zertifikate die entsprechenden Zugriffsrechte.

Um über die Webschnittstelle ein Zertifikat zu verwalten, wechseln Sie in die Ansicht **Setup-Wizards** > **Zertifikate verwalten**. Hier erhalten Sie eine Übersicht der erstellten Zertifikate und können diese auch widerrufen.



Die Tabellenspalten haben die folgenden Bedeutungen:

Seite

In dieser Spalte markieren Sie den Eintrag.

Index

Zeigt den fortlaufenden Index des Eintrages an.

Name

Zeigt den Namen des Zertifikates an.

Seriennummer

Enthält die Seriennummer des Zertifikates.

Status

Zeigt den aktuellen Status des Zertifikates an. Mögliche Werte sind:

- V: Gültig (valid)
- R: Widerrufen (revoked)
- P: Angefragt (pending)

Erstellungszeitpunkt

Zeigt den Zeitpunkt der Zertifikaterstellung an (Datum, Uhrzeit).

Ablaufzeit

Gibt den Zeitpunkt mit Datum und Uhrzeit an, zu dem das Zertifikat regulär abläuft.

Rückrufzeit

Gibt den Zeitpunkt mit Datum und Uhrzeit an, zu dem das Zertifikat vorzeitig widerrufen wurde.

Rückrufgrund

Gibt den Grund für einen vorzeitigen Widerruf an. Die Auswahl erfolgt über eine Drop-Down-Auswahlliste.

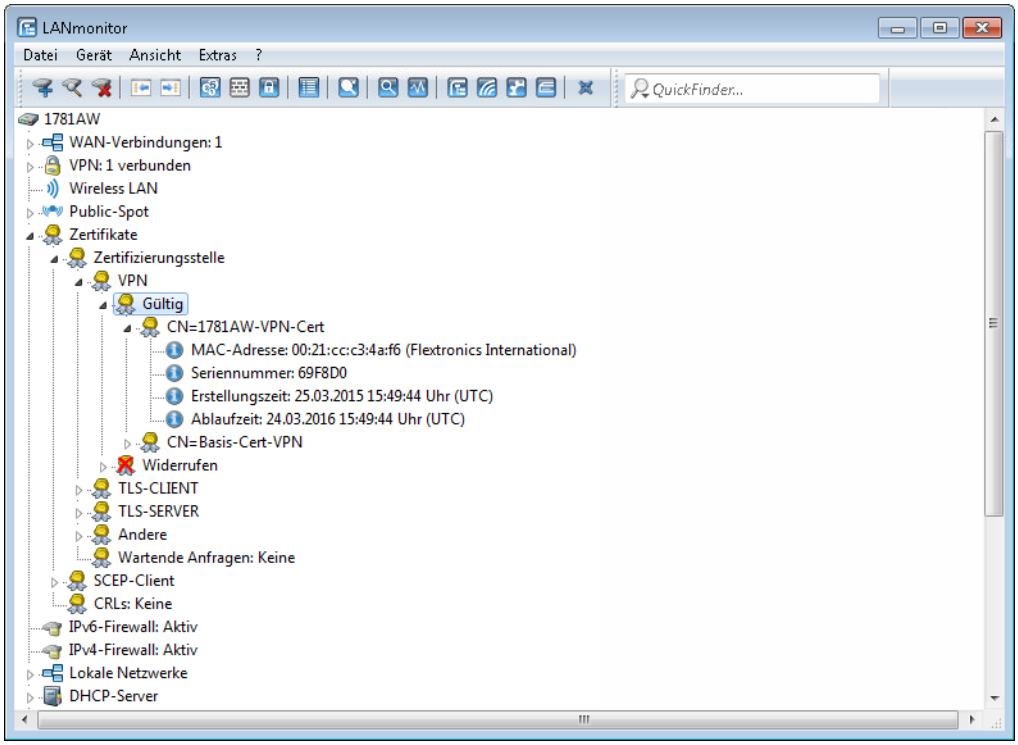
Um ein Zertifikat zu widerrufen, markieren Sie es in der Spalte **Seite**, geben in der Spalte **Rückrufgrund** an, warum Sie das Zertifikat widerrufen und klicken auf **Widerrufen**.

Die Spalteneinträge von **Status**, **Rückrufzeit** und **Rückrufgrund** ändern sich entsprechend.

Um ein zuvor widerrufenes Zertifikat wieder für gültig zu erklären, markieren Sie es wieder in der ersten Spalte und klicken auf **Als gültig erklären**.

11.8.4.5 Zertifikate verwalten im LANmonitor

Der LANmonitor zeigt die aktiven und widerrufenen Zertifikate sowie die Zertifikatsanfragen der SCEP-Clients an.



Um ein Zertifikat zu widerrufen, klicken Sie mit der rechten Maustaste auf das entsprechende Zertifikat und wählen Sie im Kontextdialog den Punkt **Zertifikat widerrufen** aus.

Eine Übersicht aller widerrufenen Zertifikate sehen Sie im Abschnitt **Widerrufen**.

Zertifikatanfragen von SCEP-Clients sehen Sie im Abschnitt **Wartende Anfragen**. Klicken Sie mit der rechten Maustaste auf die entsprechende Anfrage und wählen Sie im Kontextdialog entweder **Ablehnen** oder **Akzeptieren** aus.

11.8.4.6 Zertifikate über URL-API erstellen

Die Erstellung von Zertifikaten ist in einer komplexen und ausgedehnten Netz-Infrastruktur komfortabel über eine spezielle API möglich.

Durch den Aufruf einer URL mit angehängten Parametern lässt sich die Erstellung z. B. über ein Skript automatisieren. Die folgenden Parameter sind möglich:

- `a`: Gibt den Profilnamen an.
- `b`: Gibt den allgemeinen Namen (common name) an.
- `c`: Gibt den Familiennamen (surname) an.
- `d`: Gibt die E-Mail (email) an.
- `e`: Gibt die Organisation an.
- `f`: Gibt die Organisations-Einheit (organization unit) an.
- `g`: Gibt den Ort (locality) an.
- `h`: Gibt das Bundesland (state) an.
- `i`: Gibt den Staat (country) an.
- `j`: Gibt die Postleitzahl (postal code) an.

- `k`: Gibt die Seriennummer an.
- `l`: Gibt den Subject-Alternative-Name an.
- `m`: Gibt die Verwendung (key usage) an.
- `n`: Gibt die erweiterte Verwendung (extended key usage) an.
- `o`: Gibt die Schlüssellänge (key length) an.
- `p`: Gibt die Gültigkeitsdauer (validity period) in Tagen an.
- `q`: Gibt das Passwort für die PKCS12-Datei an.
- `r`: Gibt an, ob es sich um ein CA-Zertifikat handelt.
  - 1: CA-Zertifikat
  - 0: kein CA-Zertifikat

Der Wizard verarbeitet nur die Parameter, für die in der Presets-Tabelle die entsprechenden Zugriffsrechte gesetzt sind.

Der Aufruf der URL mit den entsprechenden Parametern sieht wie folgt aus:

```
192.168.10.74/scepwiz/a=VPN&b=iPhone&q=company
```

11.8.4.7 OCSP-Server

Online Certificate Status Protocol (OCSP) ist ein in RFC 6960 definiertes Verfahren zur Prüfung der Gültigkeit eines Zertifikats bei einer zentralen Instanz. Im Gegensatz zu Zertifikatssperrlisten (CRLs) muss bei der Verwendung nicht regelmäßig die komplette CRL heruntergeladen werden; stattdessen wird on-demand beim Verbindungsaufbau eine OCSP-Anfrage an den OCSP-Server gestellt, sodass die Information über die Gültigkeit des Zertifikats immer aktuell ist. Da hierbei nur die Gültigkeitsinformation für ein Zertifikat übertragen wird, müssen weniger Daten übertragen werden. Somit sind die Gültigkeitsinformationen im Vergleich zum CRL-basierten Verfahren stets aktuell und die Überprüfung passiert schneller.

Der OCSP-Server kann nur in Zusammenhang mit einer Zertifizierungsstelle (CA) auf dem selben Gerät eingesetzt werden (LANCOM Smart Certificate). Es ist nicht möglich, Gültigkeitsinformationen für Zertifikate anderer CAs über den OCSP-Server bereitzustellen.

Damit der OCSP-Server bei der Erzeugung von Zertifikaten per LANCOM Smart Certificate verwendet wird, muss diesem ein Zertifikat zugewiesen werden und das Profil zur Erstellung von Zertifikaten um einen Eintrag erweitert werden, damit diese den OCSP-Server kennen.

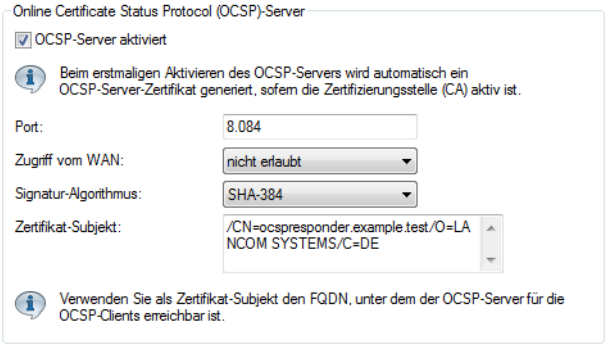
OCSP-Server konfigurieren

Um den OCSP-Server zu konfigurieren, sind folgende Schritte erforderlich:

1. Aktivieren Sie den OCSP-Server unter **Zertifikate** > **OCSP** > **Online Certificate Status Protocol (OCSP)-Server** > **OCSP-Server aktiviert**.
2. Weisen Sie dem OCSP-Server ein Zertifikat zu.

   Für den Betrieb des OCSP-Server ist es erforderlich, dass dieser ein Zertifikat von der CA erhält, über deren Zertifikate er Auskunft geben soll. Mit diesem Zertifikat werden die OCSP-Antworten signiert.

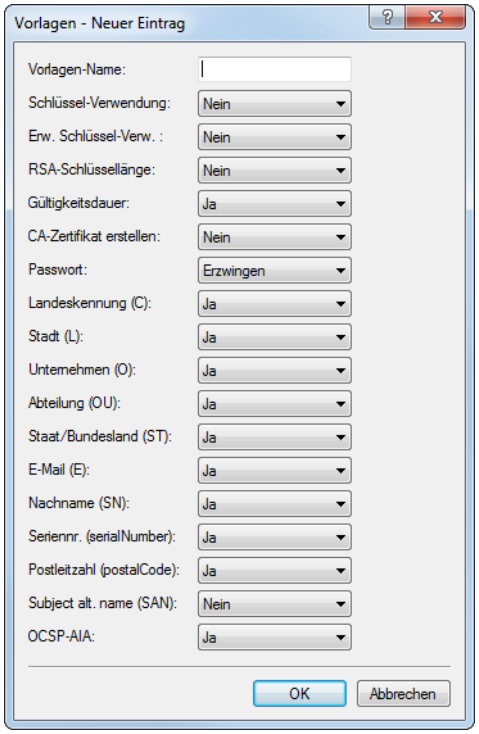
Hierzu ist unter **Zertifikate** > **OCSP** > **Online Certificate Status Protocol (OCSP)-Server** das **Zertifikat-Subject** für den OCSP-Server zu konfigurieren. Aus dieser Information wird dann beim erstmaligen Aktivieren das Zertifikat für den OCSP-Server automatisch erzeugt.



Geben Sie im Zertifikat-Subject als CN den FQDN an, unter dem der OCSP-Server für die OCSP-Clients erreichbar ist.

3. Erweitern Sie die Smart Certificate-Vorkonfiguration um Informationen zum OCSP-Server

   a) Unter **Zertifikate** > **Zertifikatsbehandlung** > **Web-Interface der CA** > **Vorlagen** konfigurieren Sie, dass bei der Erzeugung eines Zertifikats mittels Smart Certificate CA das Feld "OCSP-AIA" (Authority Information Access) konfiguriert werden kann. Verwenden Sie die "Default"-Vorlage, ist dies bereits automatisch der Fall. Verwenden Sie eine benutzerdefinierte Vorlage, dann schalten Sie das Feld „OCSP-AIA“ aktiv.

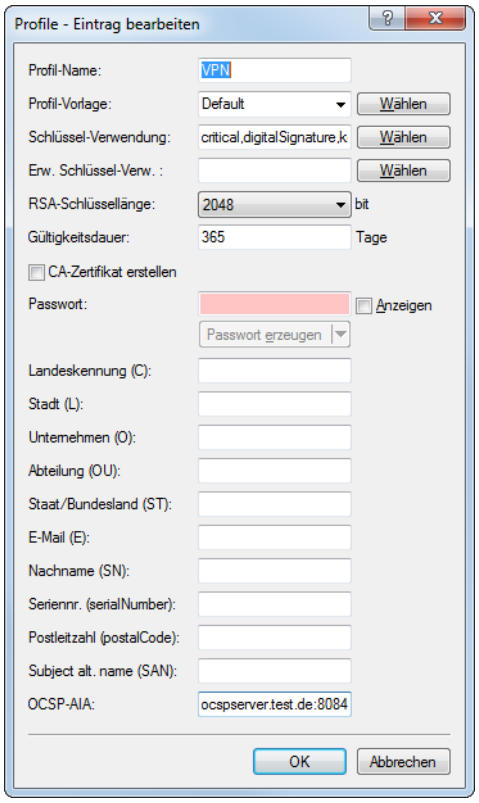


   b) Unter **Zertifikate** > **Zertifikatsbehandlung** > **Web-Interface der CA** > **Profile** legen Sie als nächstes einen Default-Wert für das Feld OCSP-AIA im gewünschten Smart-Certificate-Profil fest.

Dieser Schritt ist optional. Wenn Sie hier keinen Default-Wert festlegen, dann müssen Sie manuell einen Wert bei der Erzeugung eines Zertifikats angeben.

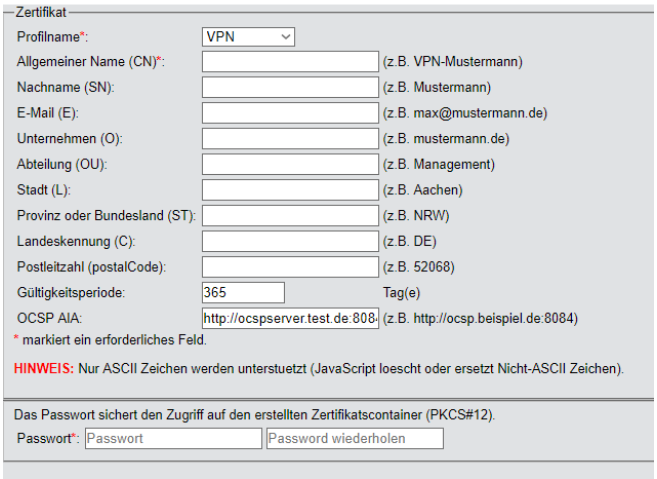
Konfigurieren Sie hier den Namen oder die IP-Adresse, unter dem der OCSP-Server für die OCSP-Clients erreichbar ist. Dieser wurde bereits oben bei der Erzeugung des OCSP-Server-Zertifikats verwendet. Fügen Sie auch die Portnummer an, unter der der OCSP-Server erreichbar ist. Standardmäßig ist der Port 8084.

Im Beispiel wird der Default-Wert für das Profil „VPN“ auf „ocspserver.test.de:8084“ angepasst:



Die Konfiguration des OCSP-Servers ist damit abgeschlossen.

Wird nun wie in *Zertifikaterstellung über WEBconfig* auf Seite 815 beschrieben über WEBconfig ein Zertifikat mittels Smart Certificate erzeugt, dann wird diesem automatisch die OCSP-AIA angefügt, sodass der Client beim Verbindungsaufbau zur Gültigkeitsprüfung den OCSP-Server kontaktiert.



Zur Prüfung der Gültigkeit zieht der OCSP-Server wiederum die geräteinterne Zertifikatsliste heran, so dass Zertifikate über die Smart Certificate-Weboberfläche bequem zurückgezogen oder wieder für gültig erklärt werden können.

11.9 NAT Traversal (NAT-T)

Die nicht ausreichende Anzahl von öffentlich gültigen IP-Adressen hat zur Entwicklung von Verfahren wie IP-Masquerading oder NAT (Network Address Translation) geführt, bei denen ein ganzes lokales Netzwerk hinter einer einzigen, öffentlich gültigen IP-Adresse maskiert wird. Auf diese Weise nutzen alle Clients in einem LAN die gleiche IP-Adresse beim Datenaustausch mit öffentlichen Netzwerken wie dem Internet. Die Zuordnung der ein- und ausgehenden Datenpakete zu den verschiedenen Teilnehmern im Netz wird dabei über eine Verbindung der internen IP-Adressen zu entsprechenden Port-Nummern gewährleistet.

Dieses Verfahren hat sich bewährt und ist mittlerweile Standard in nahezu allen Internet-Routern. Neue Schwierigkeiten in der Verarbeitung der maskierten Datenpakete treten jedoch bei der Verwendung von VPN auf. Da Datenverbindungen über VPN sehr stark gesichert sind, kommen Mechanismen wie Authentifizierung und Verschlüsselung hier hohe Bedeutung zu.

Die Umsetzung der internen IP-Adressen auf die zentrale, öffentlich gültige IP-Adresse des Gateways sowie die Umsetzung von Quell- und Zielports kann in manchen Anwendungen zu Problemen führen, weil dabei z. B. der üblicherweise während der IKE-Verhandlung verwendete UDP-Port 500 verändert wird und die IKE-Verhandlung somit nicht mehr erfolgreich abgeschlossen werden kann. Die Adressänderung über NAT wird also von einem VPN-Gateway als sicherheitskritische Veränderung der Datenpakete gewertet, die VPN-Verhandlung scheitert, es kommt keine Verbindung zustande. Konkret treten diese Probleme z. B. bei der Einwahl über manche Mobilfunknetze auf, bei denen die Server des Netzbetreibers die Adress-Umsetzung in Verbindung mit IPSec-basierten VPNs nicht unterstützen.

Um auch in diesen Fällen eine VPN-Verbindung erfolgreich aufbauen zu können, steht mit NAT-T (NAT Traversal) ein Verfahren bereit, die beschriebenen Probleme bei der Behandlung von Datenpaketen mit geänderten Adressen zu überwinden.

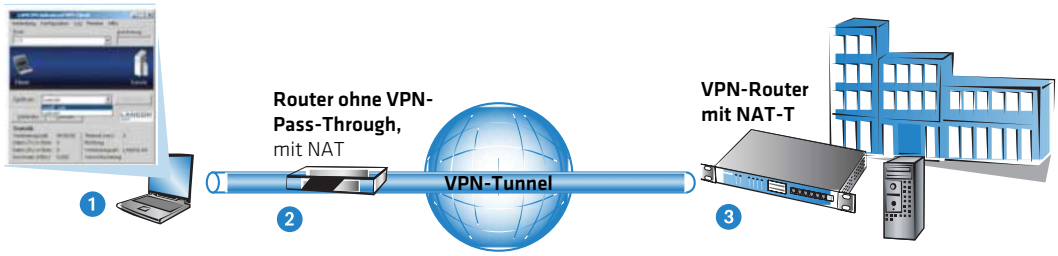
NAT-T kann nur bei VPN-Verbindungen eingesetzt werden, die zur Authentifizierung ESP (Encapsulating Security Payload) verwenden. ESP berücksichtigt im Gegensatz zu AH (Authentication Header) bei der Ermittlung des Hashwertes zur Authentifizierung nicht den IP-Header der Datenpakete. Der vom Empfänger berechnete Hashwert entspricht daher dem in den Paketen eingetragenen Hashwert.

Setzt die VPN-Verbindung zur Authentifizierung AH ein, kann grundsätzlich keine Verbindung über Strecken mit Network Address Translation aufgebaut werden, da sich die AH-Hashwerte bei der Änderung der IP-Adressen ebenfalls ändern und der Empfänger die Datenpakete als nicht vertrauenswürdig einstufen würde.

Das Verfahren von NAT Traversal überwindet die Probleme beim VPN-Verbindungsaufbau an den Endpunkten der VPN-Tunnel. Folgende Szenarien lassen sich daher unterscheiden:

- Ein Aussendienstmitarbeiter wählt sich mit einem LANCOM Advanced VPN-Client über einen Router **ohne** „VPN-Pass-Through"-Unterstützung (d. h. IPSec-Maskierung), aber **mit** Network Address Translation in den VPN-Router seiner Firma ein.

LANCOM Advanced VPN Client mit NAT-T

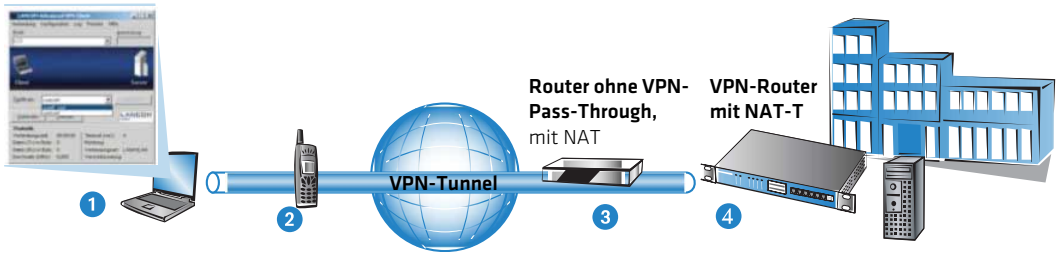


- Die beiden Tunnelendpunkte LANCOM Advanced VPN-Client **1** und VPN-Router **3** unterstützen das NAT-T-Verfahren und können so auch über den zwischengeschalteten Router eine VPN-Verbindung aufbauen.

- Der Router **2** macht als NAT-Gerät zwischen den VPN-Endpunkten eine reine Adress-Umsetzung. In diesem Router wird kein NAT-T benötigt, hier müssen jedoch die Ports 500 und 4500 in der Firewall freigeschaltet sein, um die NAT-T-Kommunikation der beiden Tunnelendpunkte zu ermöglichen.

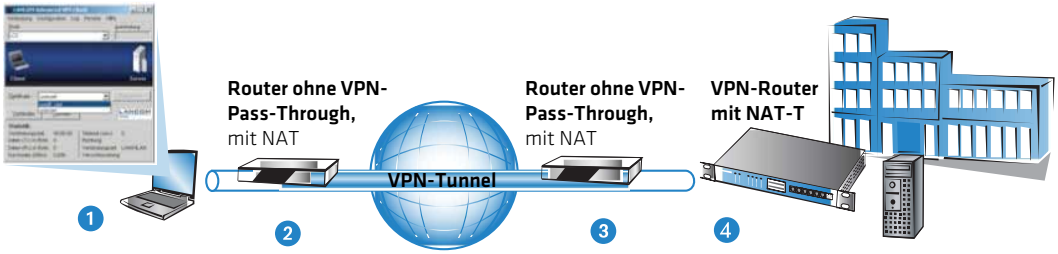
- Im zweiten Anwendungsbeispiel wählt sich der Außendienstmitarbeiter von unterwegs über sein Notebook **1** und ein Mobiltelefon oder Modem **2** in das Netzwerk der Zentrale ein.

LANCOM Advanced VPN Client mit NAT-T



- Dabei steht in der Zentrale der VPN-Router **4** hinter einem Abschlussrouter **3**, der nur den Internetzugang mit der Adressumsetzung bereitstellt.
- Die beiden Tunnelendpunkte LANCOM Advanced VPN-Client **1** und VPN-Router **4** können über das NAT-T-Verfahren wie im ersten Beispiel eine VPN-Verbindung aufbauen.
- Im Abschlussrouter **2** müssen jedoch die Ports 500 und 4500 in der Firewall freigeschaltet sein, zusätzlich muss das Port-Forwarding in diesem Router aktiviert werden.

- In der Kombination der beiden vorhergehenden Fälle stehen auf beiden Seiten der Verbindung reine NAT-Router **2** und **3**. Die VPN-Strecke wird zwischen dem LANCOM Advanced VPN-Client **1** und VPN-Router **4** aufgebaut.



Die beiden Router **2** und **3** müssen über die Firewallfreischaltung der Ports 500 und 4500 die NAT-T-Verbindung zwischen den Tunnelendpunkten zulassen, im Abschlussrouter der Zentrale muss zusätzlich das Port-Forwarding aktiviert werden.

Um dieses Verfahren zu ermöglichen, müssen beide Seiten der VPN-Verbindung NAT-T beherrschen. Der Ablauf des VPN-Verbindungsaufbaus sieht (reduziert auf die NAT-T-relevanten Vorgänge) so aus:

1. In einer frühen Phase der IKE-Verhandlung wird daher überprüft, ob die beiden Seiten der VPN-Verbindung NAT-T-fähig sind.
2. Im zweiten Schritt wird dann geprüft, ob auf der Strecke zwischen den beiden Tunnelendpunkten eine Adressumsetzung nach NAT stattfindet und an welcher Stelle der Verbindung sich die NAT-Geräte befinden.
3. Um die Probleme mit den möglicherweise veränderten Ports zu umgehen, werden anschließend alle Verhandlungs- und Datenpakete nur noch über den UDP-Port 4500 verschickt, sofern ein NAT-Gerät gefunden wurde.

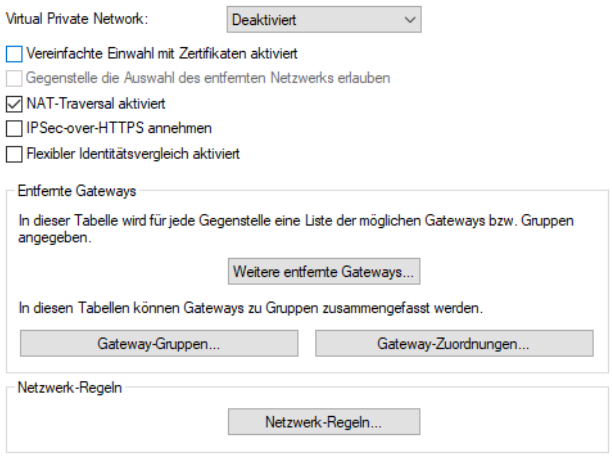
Achten Sie darauf, dass neben dem UDP-Port 500 auch der UDP-Port 4500 bei Verwendung von NAT-T in der Firewall freigeschaltet ist, wenn das Gerät als NAT-Router zwischen den VPN-Endpunkten fungiert! Bei Verwendung des Firewall-Assistenten in LANconfig wird dieser Port automatisch freigeschaltet.

Sofern die VPN-Verbindungen erstmals auf Geräten mit einer Firmware-Version 5.20 oder neuer mit dem VPN-Assistenten und anschließend dem Firewall-Assistenten von LANconfig angelegt werden, sind für die NAT-Router keine zusätzlichen Einstellungen an der Firewall erforderlich.

4. Im folgenden werden die Datenpakete noch einmal in UDP-Pakete verpackt (UDP-Encapsulation) und ebenfalls über den Port 4500 versendet. Durch diese zusätzliche Kapselung ist die Veränderung der IP-Adressen für die VPN-Verhandlung nicht mehr relevant, der VPN-Tunnel kann ohne Probleme aufgebaut werden. Auf der Gegenseite der Verbindung werden die IP-Daten wieder vom zusätzlichen UDP-Header befreit und können ohne weiteres vom Router verarbeitet werden.

Zur Verwendung dieses Verfahrens müssen beide Seiten der VPN-Verbindung NAT-T verwenden.

Den Schalter zur Aktivierung von NAT-T finden Sie in LANconfig unter **VPN** > **Allgemein**.



Unter Telnet oder SSH-Client finden Sie die Aktivierung von NAT-T unter **Setup** > **VPN** > **NAT-T-Aktiv**.

11.10 Extended Authentication Protocol (XAUTH)

11.10.1 Einleitung

Bei der Einwahl von Gegenstellen über WAN-Verbindungen (z. B. über PPP) werden oft RADIUS-Server eingesetzt, um die Benutzer zu authentifizieren. Die üblichen WAN-Verbindungen wurden im Laufe der Zeit dann immer mehr von sichereren (verschlüsselten) und kostengünstigeren VPN-Verbindungen verdrängt. Der Aufbau von VPN-Verbindungen über IPSec mit IKE erlaubt jedoch keine unidirektionale Authentifizierung von Benutzern über RADIUS o ä.

Das Extended Authentication Protocol (XAUTH) bietet eine Möglichkeit, die Authentifizierung bei der Verhandlung von IPSec-Verbindungen um eine zusätzliche Stufe zu erweitern, in der die Benutzerdaten authentifiziert werden können. Dazu wird zwischen der ersten und der zweiten IKE-Verhandlungsphase eine zusätzliche Authentifizierung mit XAUTH-Benutzernamen und XAUTH-Kennwort durchgeführt, welche durch die zuvor ausgehandelte Verschlüsselung geschützt ist. Diese Authentifizierung kann über einen RADIUS-Server erfolgen und so die Weiterverwendung der vorhandenen RADIUS-Datenbanken bei der Migration auf VPN-Verbindungen für die Einwahl-Clients ermöglichen. Alternativ kann die Authentifizierung eine interne Benutzertabelle des Gerätes verwenden.

Um die Verwendung von XAUTH besonders sicher zu gestalten, sollten Sie nach Möglichkeit anstelle des Preshared-Key-Verfahrens (PSK) die Einwahl über RSA-SIG (Zertifikate) verwenden. Stellen Sie dabei sicher, dass das VPN-Gateway nur das Zertifikat der jeweils richtigen Gegenstelle akzeptiert (und nicht alle von der gleichen CA ausgestellten Zertifikate).

11.10.2 XAUTH in der Firmware

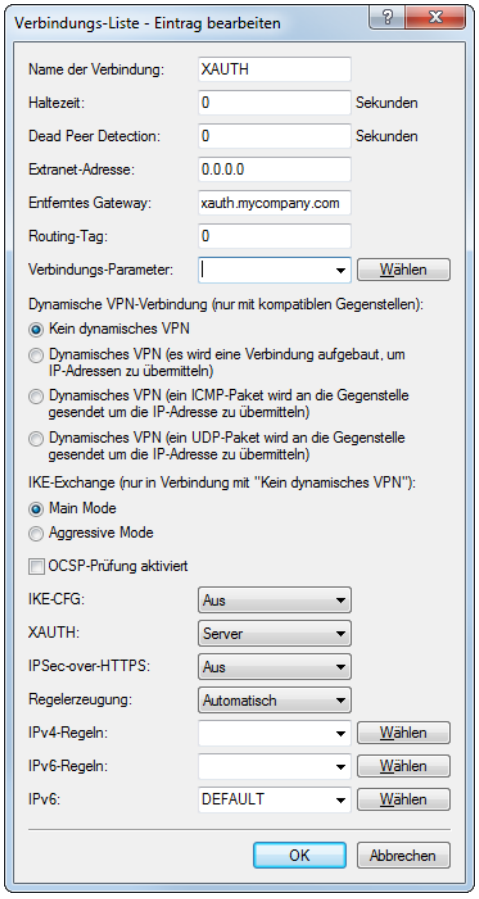
Im Gerät nutzt das XAUTH-Protokoll die Einträge in der PPP-Tabelle zur Authentifizierung der Gegenstelle. Die Verwendung der Einträge in der PPP-Tabelle ist dabei von der Richtung des Verbindungsaufbaus abhängig, also von der XAUTH-Betriebsart:

XAUTH-Betriebsart	Server	Client
XAUTH-Benutzername	Gegenstelle aus der PPP-Tabelle. Es wird dabei der Eintrag aus der PPP-Tabelle gewählt, bei dem die PPP-Gegenstelle dem übermittelten XAUTH-Benutzernamen entspricht. Die PPP-Gegenstelle muss dabei auch der verwendeten VPN-Gegenstelle entsprechen.	Benutzername aus der PPP-Tabelle. Es wird dabei der Eintrag aus der PPP-Tabelle gewählt, bei dem die PPP-Gegenstelle der verwendeten VPN-Gegenstelle entspricht.
XAUTH-Kennwort	Kennwort aus der PPP-Tabelle.	Kennwort aus der PPP-Tabelle.

11.10.3 Konfiguration von XAUTH

Die Verwendung des XAUTH-Protokolls wird für jede VPN-Gegenstelle separat vorgenommen. Dabei wird lediglich der XAUTH-Betriebsmodus festgelegt.

LANconfig: **VPN** > **IKE/IPSec** > **Verbindungs-Liste**



CLI: **Setup** > **VPN** > **VPN-Gegenstellen**

› XAUTH

Aktiviert die Verwendung von XAUTH für die gewählte VPN-Gegenstelle.

Mögliche Werte:

Client

In der Betriebsart als XAUTH-Client startet das Gerät die erste Phase der IKE-Verhandlung (Main Mode oder Aggressive Mode) und wartet dann auf den Authentifizierungs-Request vom XAUTH-Server. Auf diesen Request antwortet der XAUTH-Client mit dem Benutzernamen und dem Kennwort aus dem Eintrag der PPP-Tabelle, in dem die PPP-Gegenstelle der hier definierten VPN-Gegenstelle entspricht. Zu der VPN-Gegenstelle muss es also eine gleichnamige PPP-Gegenstelle geben. Der in der PPP-Tabelle definierte Benutzername weicht üblicherweise von dem Gegenstellennamen ab.

Server

In der Betriebsart als XAUTH-Server startet das Gerät nach erfolgreicher Verhandlung der ersten IKE-Verhandlung die Authentifizierung mit einem Request an den XAUTH-Client, der daraufhin mit seinem Benutzernamen und Kennwort antwortet. Der XAUTH-Server sucht den übermittelten Benutzernamen in den Gegenstellennamen der PPP-Tabelle und prüft bei Übereinstimmung das Kennwort. Der Benutzername für diesen Eintrag in der PPP-Tabelle wird nicht verwendet.

Aus (Default)

Bei der Verbindung zu dieser Gegenstelle wird keine XAUTH-Authentifizierung durchgeführt.

Wenn die XAUTH-Authentifizierung für eine VPN-Gegenstelle aktiviert ist, muss die Option IKE-CFG auf den gleichen Wert eingestellt werden.

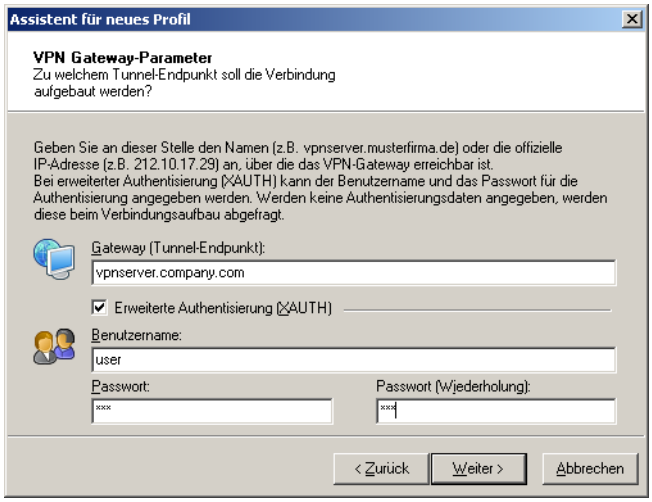
11.10.4 XAUTH mit externem RADIUS-Server

Seit der Firmware-Version 7.60 kann ein Router die Gegenstelle auch über das Extended Authentication Protocol (XAUTH) identifizieren und authentifizieren. Zur Authentifizierung wurden dabei die Benutzerdaten aus der PPP-Liste herangezogen.

Ab der Firmware-Version 7.80 kann die XAUTH-Authentifizierung auch an einen (externen) RADIUS-Server weitergereicht werden. So können z. B. die auf dem RADIUS-Server schon vorhandenen RAS-Benutzerdaten komfortabel weiter genutzt werden, wenn die RADIUS-authentifizierte Einwahl über PPP auf VPN mit XAUTH umgestellt wird.

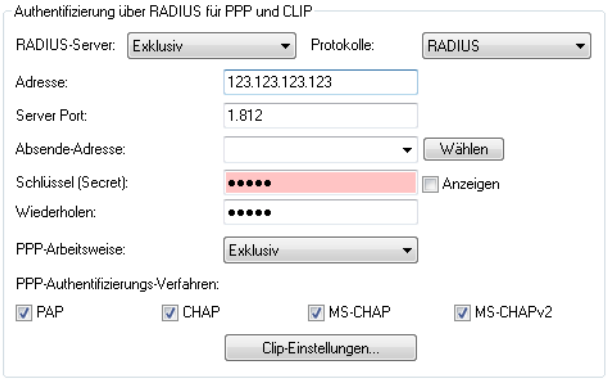
Um einen Einwahlzugang über VPN zusätzlich mit XAUTH zu authentifizieren, gehen Sie folgendermaßen vor:

1. Richten Sie einen VPN-Einwahlzugang ein, z. B. mit dem Setup-Assistenten von LANconfig.
2. Aktivieren Sie im VPN-Client der einwählenden Station die Verwendung von XAUTH. Tragen Sie als Benutzernamen und Kennwort die Werte ein, die auch im RADIUS-Server hinterlegt sind.



3. Aktivieren Sie die Authentifizierung der Einwahlgegenstellen über das XAUTH-Protokoll an einem externen RADIUS-Server. Aktivieren Sie unter LANconfig im Konfigurationsbereich **Kommunikation** > **RADIUS** für den

RADIUS-Server die Betriebsart "Exklusiv". In dieser Einstellung werden die eingehenden XAUTH-Anfragen ausschließlich über den RADIUS-Server authentifiziert.



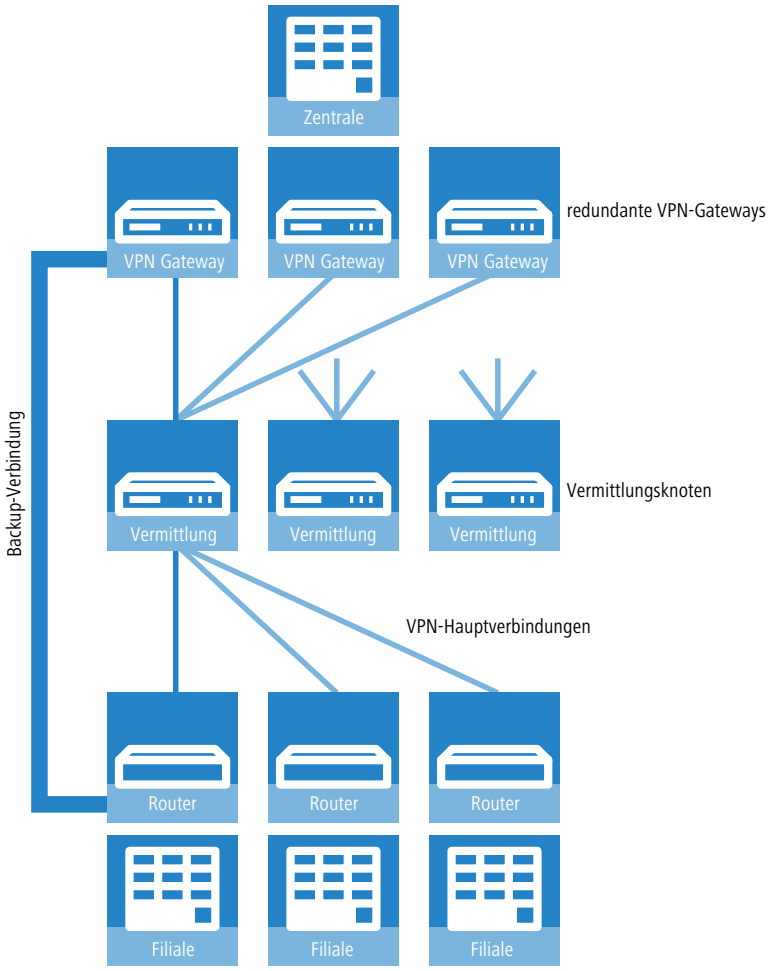
4. Geben Sie außerdem für den externen RADIUS-Server die IP-Adresse, den Port, das Protokoll und den Schlüssel an.
5. Stellen Sie auch die PPP-Arbeitsweise auf "Exklusiv" ein, damit die eingehenden XAUTH-Anfragen ausschließlich über den RADIUS-Server authentifiziert werden.

11.11 Backup über alternative VPN-Verbindung

11.11.1 Einleitung

Das Thema der Backup-Verbindungen ist gerade in verteilten Standorten mit mehreren Filialen, die über VPN an die Zentrale angebunden sind, ein zentrales Thema für die Verfügbarkeit von unternehmenskritischen Anwendungen. Bei einer direkten Beziehung von Routern in den Filialen zu redundanten Routern in der Zentrale ist das Backup einfach zu lösen: Ist ein Router in der Zentrale nicht über Internet erreichbar, kann sich die Filiale in einen anderen Router der Zentrale einwählen. Die Kommunikation der Geräte über die verfügbaren Routen läuft dabei über RIP.

In sehr großen Netzstrukturen sind die Filialen jedoch oft nicht direkt mit der Zentrale verbunden mehrere Standorte laufen zunächst in einem Vermittlungsknoten zusammen, die Vermittlungsknoten sind dann an die Zentrale angebunden. Ist der Vermittlungsknoten für die Filiale vorübergehend nicht erreichbar, könnte die Filiale eine Backup-Verbindung direkt in die Zentrale aufbauen.



Das gelingt allerdings nur über eine Mobilfunk-Verbindung, die aus Kostengründen und wegen der meist geringen Bandbreite oft nicht erwünscht ist. Eine parallele Backup-Verbindung direkt über VPN führt aus folgenden Gründen nicht zum Ziel:

- In der Zentrale sind nur die Vermittlungsknoten als VPN-Gegenstellen definiert, alle Routen zu den Filialen laufen über diese Vermittlungsknoten. Versucht eine Filiale eine direkte Verbindung zur Zentrale aufzubauen, so wird dieser Aufbau abgelehnt. Und selbst wenn diese Verbindung zustande kommen würde, bleiben in der Zentrale die Routen zu den Filialen über die Vermittlungsknoten bestehen, denn der Vermittlungsknoten ist ja aus Sicht der Zentrale noch erreichbar.
- Der Vermittlungsknoten erfährt nichts über eine evtl. vorhandene Direktverbindung der Filiale an die Zentrale, er kann also die Ziele im Netz der Filiale nicht über den Umweg der Zentrale erreichen.
- Von der Zentrale aus ist über die reguläre VPN-Verbindung, sowohl das Netz des Vermittlungsknotens, als auch das Netz der Filiale erreichbar. Über eine direkte VPN-Verbindung der Filiale in die Zentrale ist aber nur das Filialnetz erreichbar. Der Router in der Zentrale kann aufgrund dieser unterschiedlichen Eigenschaften die direkte Verbindung nicht als Backup für die reguläre Verbindung akzeptieren.
- Die Filiale kann die reguläre Verbindung zum Vermittlungsknoten nicht mehr aufbauen, weil der Eindeutigkeitsgrundsatz der IPsec-Regeln keine zweite Verbindung mit gleichem Regelsatz zulässt. Die IPSec-Regeln enthalten neben den Angaben zur Verschlüsselung auch die sogenannten Netzbeziehungen, also die IP-Adressen der Netzwerke auf beiden Seiten der Verbindung. Diese Netzbeziehungen dürfen nur einmal im VPN-Regelsatz vorkommen. Im Backupfall müssten aber zwei Regeln für dieselbe Netzbeziehung existieren – einmal für die Backup-Verbindung und einmal für die neu aufzubauende Hauptverbindung.

11.11.2 Backup-fähige Netzstruktur

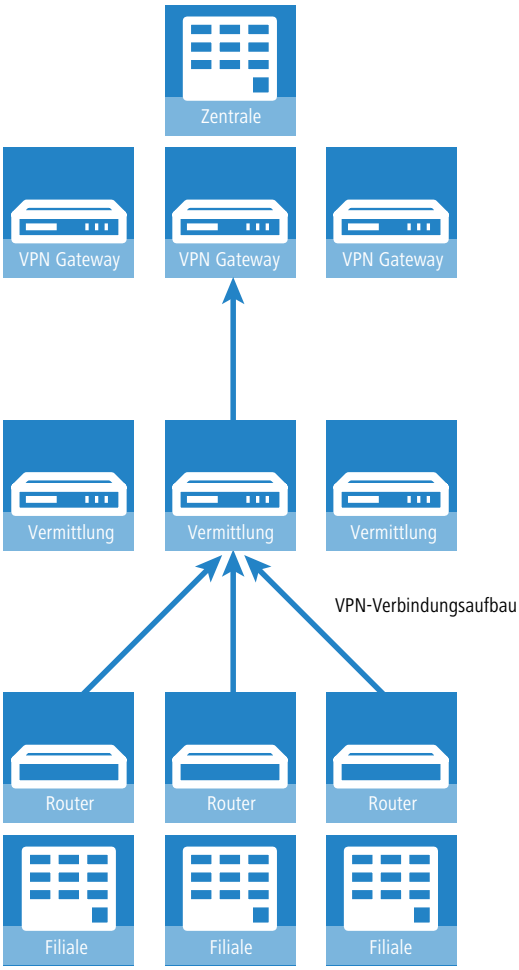
Um auch für diese Anwendungen ein funktionsfähiges Backup aufbauen zu können, müssen die in den folgenden Abschnitten beschriebenen Aspekte erfüllt sein.

11.11.2.1 Grundvorraussetzungen

Grundvoraussetzung für die hier beschriebene Backup-Funktion ist die Einrichtung einer „Dynamic VPN"-Verbindung zwischen Filialen und Vermittlungsknoten sowie die Aktivierung der Funktionen „vereinfachte Einwahl mit Zertifikaten" und „Gegenstelle die Auswahl des entfernten Netzes erlauben" in den VPN-Gateways der Zentrale.

11.11.2.2 Hierarchie beim VPN-Verbindungsaufbau

Damit die Filialen im Backup-Fall eine Verbindung zum Netz der Zentrale aufbauen können, muss eine definierte Hierarchie für den Verbindungsaufbau eingehalten werden. Dabei werden die Verbindungen immer nur von den „unteren" zu den „oberen" Netzen hergestellt, also von der Filiale zum Vermittlungsknoten, vom Vermittlungsknoten zur Zentrale.



In der Zentrale müssen alle Verbindungen also nur passiv angenommen werden. Die Vermittlungsknoten nehmen ebenfalls die Verbindungen der Filialen passiv an, bauen aber die Verbindungen zur Zentrale aktiv auf. Diese Hierarchie ist Voraussetzung für die spätere Definition der VPN-Regeln.

11.11.2.3 Netzwerkdefinitionen

Die Filialen bauen Netzbeziehungen zu den Vermittlungsknoten und zur Zentrale auf, was durch die entsprechenden Regeln abgedeckt sein muss. Dazu müssen entweder alle denkbaren Netzbeziehungen einzeln hinterlegt werden oder

aber die Netzwerke werden so definiert, dass mit einer Regel alle erforderlichen Netzbeziehungen erlaubt werden können. Das gelingt, wenn die Netzwerke z. B. die folgende Struktur von IP-Adressen verwenden:

- Zentralnetz 10.1.1.0/255.255.255.0
- Vermittlungsknoten 10.x.1.0/255.255.255.0
- Filialen 10.x.y.0/255.255.255.0

Mit der folgenden VPN-Regel in den VPN-Gateways der Zentrale können alle erforderlichen Netzbeziehungen zugelassen werden, d. h. alle Gegenstellen aus dem gesamten 10er-Adressraum können Verbindungen zu allen Gateways aufbauen:

- Quelle 10.0.0.0/255.0.0.0
- Ziel 10.0.0.0/255.0.0.0

Da die Filialen über die Zwischenstufe der Vermittlungsknoten mit der Zentrale kommunizieren, müssen auch in den Vermittlungsknoten entsprechende VPN-Regeln angelegt werden. Wenn dabei auch eine Kommunikation mit anderen Unterknoten und Filialen möglich sein soll, werden mit der folgenden VPN-Regel in den Vermittlungsknoten alle erforderlichen Netzbeziehungen zugelassen:

- Quelle 10.x.0.0/255.255.0.0
- Ziel 10.0.0.0/255.0.0.0

11.11.2.4 Routing-Informationen

Die Routen aus der Zentrale zu den einzelnen Filialen laufen im Normalbetrieb über die Vermittlungsknoten. Im Backup-Fall müssen diese Routen angepasst werden. Damit diese Anpassung automatisch vorgenommen werden kann, wird in den VPN-Gateways der Zentrale die „vereinfachte Einwahl mit Zertifikaten" aktiviert. Damit kann für alle ankommenden Verbindungen eine gemeinsame Konfiguration vorgenommen werden (über die Default-Einstellungen), wenn die Zertifikate der Gegenstellen mit dem Root-Zertifikat der VPN-Gateways in der Zentrale signiert wurden. Zusätzlich wird dabei den Gegenstellen die Auswahl des entfernten Netzwerks ermöglicht. So können die Router der Filialen während der IKE-Verhandlung in Phase 2 selbst ein Netzwerk vorschlagen, das für die Anbindung verwendet werden soll.

Die Aktivierung der beiden Funktionen „vereinfachte Einwahl mit Zertifikaten" und „Gegenstelle die Auswahl des entfernten Netzes erlauben" ist eine notwendige Voraussetzung für die hier beschriebene Backup-Funktion.

Auch für die Vermittlungsknoten müssen die Routing-Informationen im Backup-Fall angepasst werden. Normalerweise werden die Vermittlungsknoten von den Filialen aus direkt erreicht. Im Backup-Fall müssen die Vermittlungsknoten die Daten aus den Filialen über den Umweg der Zentrale empfangen können. Das wird ermöglicht durch eine Route, die das gesamte zusammengefasste Netz (im Beispiel also 10.x.0.0/255.255.0.0 oder, wenn auch eine Kommunikation mit anderen Unterknoten möglich sein soll: 10.0.0.0/255.0.0.0) zur Zentrale überträgt.

Damit die Routen automatisch umgeschaltet werden können, muss auch in den Vermittlungsknoten die Auswahl des entfernten Netzes durch die Gegenstelle erlaubt werden.

Daraus ergibt sich folgender Ablauf beim Aufbau der VPN-Verbindungen:

- Der Vermittlungsknoten baut die Verbindung zur Zentrale auf und fordert alle Netzbeziehungen zu den Filialen an (d. h. er fordert das 10.x.0.0/255.255.0.0 Netz an).
- Die Filale baut die Verbindung zum Vermittlungsknoten auf und fordert ihr Netz (10.x.y.0/255.255.255.0) an.

  Damit können nun Daten von der Filiale über den Vermittlungsknoten zur Zentrale übertragen werden.

Wenn nun die VPN-Verbindung zwischen Filiale und Zentrale abbricht, passiert Folgendes:

- Der Vermittlungsknoten bemerkt den Abbruch aufgrund eines konfigurierten Pollings (DPD) und entfernt die Route zur Filiale.
- Die Filiale baut irgendwann die Backupverbindung zur Zentrale auf und fordert ihr Netz (10.x.y.0/255.255.255.0) an.

  Damit können nun Daten von der Filiale zur Zentrale übertragen werden.

Wenn die Netze zusammengefasst wurden und die Vermittlungsknoten immer das zusammengefasste Netz (hier im Beispiel also das Netz 10.x.0.0/255.255.0.0 bzw. 10.0.0.0/255.0.0.0) zur Zentrale routen, dann ist sogar eine Datenübertragung von der Filiale zum Vermittlungsknoten über die Zentrale möglich.

Wenn der Backup-Fall beendet wird, baut die Filiale die Haupverbindung zum Vermittlungsknoten wieder auf:

- Die Filiale baut die Backup-Verbindung wieder ab, wodurch die Zentrale die Route zur Filiale wieder löscht.
- Die Filiale fordert ihr Netz (10.x.y.0/255.255.255.0) wieder beim Vermittlungsknoten an.

Nun ist wieder problemlos die Kommunikation zwischen Filiale und Vermittlungsknoten möglich.

Da das Filialnetz ein Subnetz des Netzes im Vermittlungsknoten ist, ist auch sofort wieder die Kommunikation zwischen Filiale und Zentrale über den Vermittlungsknoten möglich. Die Zentrale hat keine eigene Route mehr zur Filiale und überträgt die Daten für die Filiale daher wieder zum Vermittlungsknoten.

Wenn die Struktur der Netzwerkadressen nicht wie oben beschrieben gestaltet werden kann, muss in der Zentrale die Route zur Filiale statisch konfiguriert werden und auf den Vermittlungsknoten verweisen. Wenn dann die Filiale die Backup-Verbindung aufbaut, dann wird die statische durch die dynamisch angemeldete Route überschrieben. Wird die Backup-Verbindung wieder abgebaut, dann wird die dynamische Route gelöscht und die statische Route erneut aktiv. Soll in diesem Fall die Kommunikation zwischen Filialen und Vermittlungsknoten auch im Backup-Fall gewährleistet werden, müssen auch in den Vermittlungsknoten die Routen zu den Filialen statisch konfiguriert werden.

11.11.2.5 Aufbau der Backupverbindung

Um dem Grundsatz der eindeutigen IPSec-Regeln zu entsprechen, werden im Backup-Fall zunächst die VPN-Regeln für die Hauptverbindung gelöscht und dann neue Regeln für die Backup-Verbindung angelegt.

Wenn der Aufbau der Backupverbindung scheitert, wählt das Backup-Modul die nächste Backupverbindung aus, wenn mehrere konfiguriert wurden.

11.11.2.6 Wiederaufbau der Hauptverbindung

Während die Backup-Verbindung aufgebaut wurde, versucht das Gerät die Hauptverbindung wieder herzustellen. Bei diesem Aufbauversuch darf der VPN-Regelsatz zunächst nicht wieder neu erstellt werden, da sonst der Aufbau der Backup-Verbindung scheitert bzw. eine bestehende VPN-Verbindung einfach abreißen würde.

Um das zu verhindern, wird zunächst eine „Dynamic VPN"-Verhandlung mit der Gegenstelle der Hauptverbindung durchgeführt. Verläuft diese Verhandlung erfolgreich, kann die Hauptverbindung wieder aufgebaut werden. Dazu wird zunächst die Backup-Verbindung getrennt und zusätzlich der Backup-Status zurückgesetzt. So wird verhindert, dass die Backup-Verbindung sofort wieder aufgebaut wird. Erst danach wird die Hauptverbindung mit den ursprünglichen VPN-Regeln wieder etabliert.

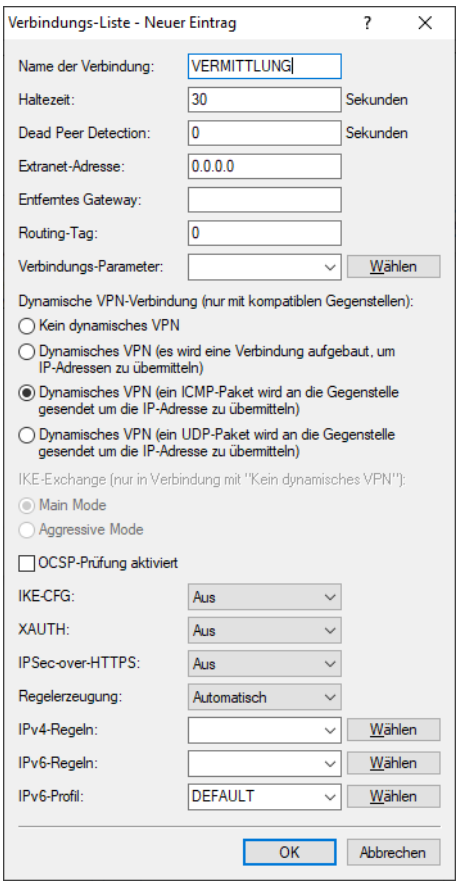
Die Nutzung der „Dynamic VPN"-Verbindung zwischen Filiale und Vermittlungsknoten ist eine notwendige Voraussetzung für die hier beschriebene Backup-Funktion.

11.11.3 Konfiguration des VPN-Backups

Bei der Konfiguration des VPN-Backups müssen die Filial-, Zentral- und Vermittlungsknoten-Geräte separat betrachtet werden.

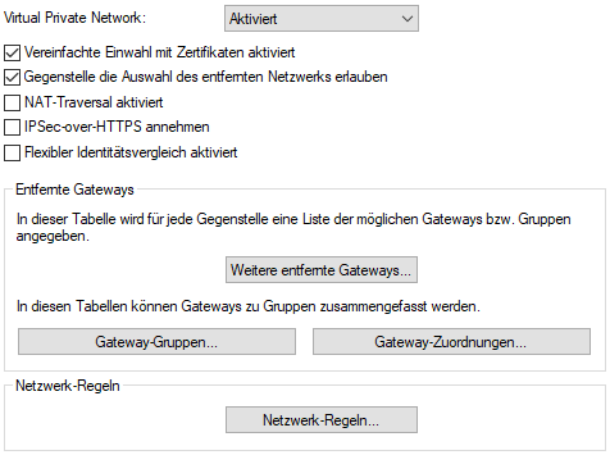
- Filiale

- Für die Hauptverbindung muss „Dynamic VPN“ über ICMP/UDP konfiguriert werden.



- Für die Backupverbindung bestehen keine Anforderungen bezüglich „Dynamic VPN“.
- In der Filiale muss die Zentrale als Backupgegenstelle konfiguriert sein.

- Zentrale
  - Die vereinfachte Einwahl mit Zertifikaten muss eingeschaltet sein.
  - Die Auswahl der entfernten Netzwerke durch die Gegenstelle muss aktiviert werden.
  - Eine Konfiguration in der Backup-Tabelle ist hier nicht notwendig.



- Vermittlungsknoten
  - Die VPN-Verbindung zur Zentrale muss vollständig konfiguriert werden.

- Die vereinfachte Einwahl mit Zertifikaten muss eingeschaltet sein.
- Die Auswahl der entfernten Netzwerke durch die Gegenstelle muss aktiviert werden.

Wenn nicht mit „zusammengefassten Netzen“ (d. h. das Filialnetz ist ein Subnetz des Vermittlungsknotens und das Vermittlungsknoten-Netz ist ein Subnetz des Zentralnetzes) gearbeitet wird, dann muss im Vermittlungsknoten die Route zur Filiale auf die Zentrale zeigen, damit die Filiale den Vermittlungsknoten auch im Backupfall erreichen kann. Im Normalbetrieb wird diese Route durch die von der Filiale im VPN übermittelte Route überschrieben (weil die Gegenstellen Netzbeziehungen vorgeben dürfen) und kommt somit nur zum Einsatz, wenn die direkte Verbindung abreißt und die Filiale die Backupverbindung aufbaut.

11.12 Automatischer Konfigurationsabgleich (Config-Sync) mit der LANCOM VPN High Availability Clustering XL Option

Anwendungsbeispiel VPN:

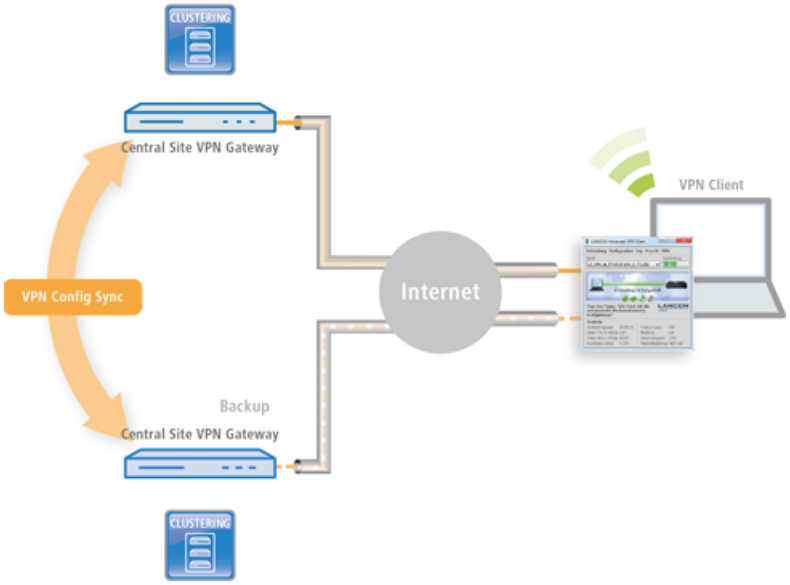
VPN-Infrastrukturen sind seit langer Zeit Bestandteil von Unternehmensnetzwerken. Die Ansprüche an die Verfügbarkeit von VPN-Gateways sind in den letzten Jahren enorm gestiegen. Wurden VPN-Lösungen im Unternehmensbereich in der Vergangenheit häufig temporär z. B. von Außendienstmitarbeitern mit VPN-Client genutzt, so werden heute Home Offices oder Zweigniederlassungen dauerhaft per VPN-Tunnel an die Zentrale angebunden. Genutzt werden dann beispielsweise Sprachdienste (VoIP), Datenbankanwendungen oder Dateidienste. Mit zunehmender Abhängigkeit von VoIP-Diensten oder kritischen Unternehmensanwendungen steigt auch der Bedarf an zuverlässigen Backup- und Hochverfügbarkeitslösungen ("High Availability") der VPN-Lösung.

Um VPN-Dienste in größeren kritischen Netzwerkinfrastrukturen hochverfügbar zu gestalten, ist der Einsatz eines oder mehrerer Backup-VPN-Gateways neben dem primären VPN-Gateway empfehlenswert. So kann bei Ausfall oder Wartung eines Central-Site-VPN-Gateways ein anderes Gerät als Backup dienen. Die VPN-Verbindung wird automatisch über das erreichbare Backup-Central-Site-VPN-Gateway aufgebaut.

Hierfür ist auf dem Backup-Central-Site-VPN-Gateway die gleiche Konfiguration wie auf dem primären Central-Site-VPN-Gateway erforderlich. Speziell die VPN-Benutzerdaten oder die Firewall-Konfiguration müssen auf beiden Geräten vorhanden sein, damit ein Benutzer authentifiziert werden kann und seine Dienste korrekt bereitgestellt werden können. Dies erfordert eine manuelle Einrichtung jedes einzelnen Gerätes – für den Administrator ein enormer Aufwand.

Neu mit der LANCOM VPN High Availability Clustering XL Option: Diese Option ermöglicht die Gruppierung von mehreren Central Site VPN Gateways zu einem Cluster. Damit können Konfigurationsänderungen, Funktionen und Erweiterungen, die an einem Central-Site-VPN-Gateway vorgenommen werden, automatisch auf die anderen übertragen werden, ohne dass jedes einzelne Gerät manuell gemanagt werden muss. Gemeinsame Parameter in einem Cluster (z. B.

VPN-Benutzerdatenbank und Firewall) werden hierbei synchronisiert, individuelle Parameter (wie z. B. die IP-Adresse) werden nicht untereinander ausgetauscht.



Die Voraussetzungen für eine gültige Gruppenmitgliedschaft eines Gerätes sind:

- Es muss eine LANCOM VPN High Availability Clustering XL Option vorhanden sein.
- Es muss eine IP-Kommunikation zu allen anderen Geräten möglich sein, z. B. über LAN, WAN oder VPN.
- Es muss in der Gruppenliste aufgeführt sein, die in jedem Gerät gespeichert ist.
- Es muss ein gültiges Zertifikat vorhanden sein.
- Es muss sich als Gruppenmitglied per Zertifikat authentifizieren können.

11.13 IPSec over HTTPS

11.13.1 Einleitung

In manchen Umgebungen ist es nicht möglich, über eine vorhandene Internetverbindung eine geschützte VPN-Verbindung aufzubauen, weil in den Einstellungen einer vorgeschalteten Firewall die von IPSec genutzten Ports gesperrt sind. Um auch in einer solchen Situation eine IPSec-geschützte VPN-Verbindung aufbauen zu können, unterstützen VPN-Router die IPSec over HTTPS-Technologie.

Dabei wird zunächst eine Datenübertragung über Standard-IPSec versucht. Kommt diese Verbindung nicht zustande (z. B. weil der IKE Port 500 in einem Mobilfunknetz gesperrt ist), so wird automatisch ein Verbindungsaufbau versucht, bei dem das IPSec-VPN mit einem zusätzlichen SSL-Header (Port 443, wie bei https) gekapselt wird.

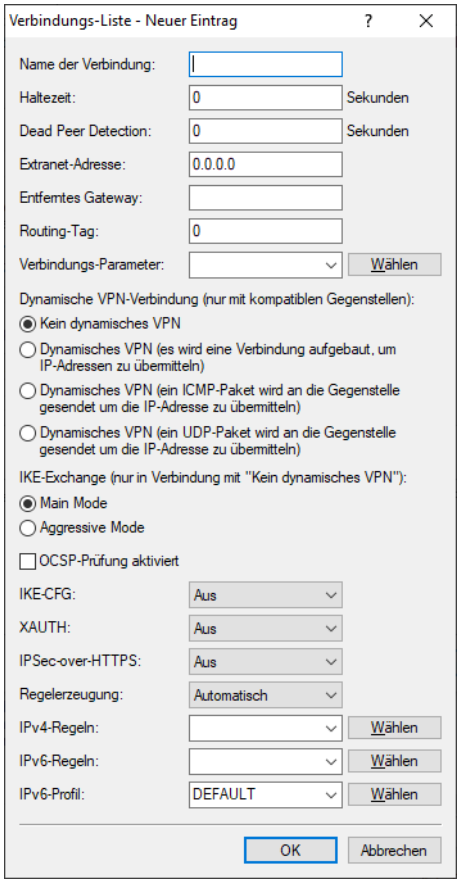
Bitte beachten Sie, dass die IPSec over HTTPS-Technologie nur genutzt werden kann, wenn beide Gegenstellen diese Funktion unterstützen und die entsprechenden Optionen aktiviert sind. IPSec over HTTPS ist verfügbar ab LCOS 8.0 sowie im LANCOM Advanced VPN Client 2.22 oder höher.

11.13.2 Konfiguration der IPSec over HTTPS-Technologie

Für den aktiven Verbindungsaufbau eines VPN-Geräts zu einer anderen VPN-Gegenstelle mit Hilfe der IPSec over HTTPS-Technologie aktivieren Sie die Option im entsprechenden Eintrag für die Gegenstelle in der VPN-Namenliste.

LANconfig: **VPN** > **IKE/IPSec** > **Verbindungsliste**

CLI: **Setup** > **VPN** > **VPN-Gegenstellen**



IPsec-over-HTTPS

Mit dieser Option aktivieren Sie die Nutzung der IPSec over HTTPS-Technologie beim aktiven Verbindungsaufbau zu dieser Gegenstelle.

Mögliche Werte:

- Ein, Aus

Default:

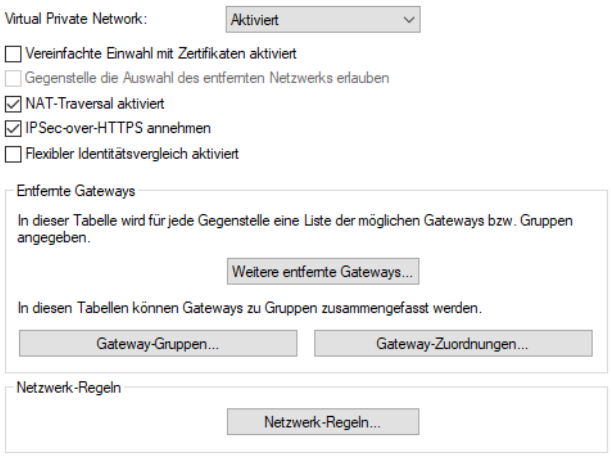
- Aus

Bitte beachten Sie, dass bei eingeschalteter IPSec over HTTPS-Option die VPN-Verbindung nur aufgebaut werden kann, wenn die Gegenstelle diese Technologie ebenfalls unterstützt und die Annahme von passiven VPN-Verbindungen mit IPSec over HTTPS bei der Gegenstelle aktiviert ist.

Für den passiven Verbindungsaufbau zu einem VPN-Gerät von einer anderen VPN-Gegenstelle mit Hilfe der IPSec over HTTPS-Technologie (VPN-Gerät oder LANCOM Advanced VPN-Client) aktivieren Sie die Option in den allgemeinen VPN-Einstellungen.

LANconfig: **VPN** > **Allgemein**

CLI: **Setup** > **VPN**



IPsec-over-HTTPS annehmen

Mit dieser Option aktivieren Sie die Annahme von passiven Verbindungsaufbauten, wenn die Gegenstelle die IPSec over HTTPS-Technologie nutzt.

Mögliche Werte:

- Ein, Aus

Default:

- Aus

Der LANCOM Advanced VPN Client unterstützt einen automatischen Fallback auf IPSec over HTTPS. In dieser Einstellung versucht der VPN-Client zunächst eine Verbindung **ohne** die zusätzliche SSL-Kapselung aufzubauen. Falls diese Verbindung nicht aufgebaut werden kann, versucht das Gerät im zweiten Schritt eine Verbindung **mit** der zusätzlichen SSL-Kapselung aufzubauen.

11.13.3 Statusanzeigen der IPSec-over-HTTPS-Technologie

Die Statusanzeigen zu jeder aktiven VPN-Verbindung zeigen an, ob für die jeweilige Verbindung die IPSec-over-TTPS-Technologie (SSL-Encapsulation) genutzt wird.

WEBconfig: **LCOS-Menübaum** > **Status** > **VPN** > **Verbindungen**

Verbindungen

Gegenstelle	Status	Letzter-Fehler	Mode	SH-Zeit	phys.-Verb.	B1-HZ	Entferntes-Gw	Nat-Erkennung	SSL-Encaps.	Krypt-Alg	Krypt-Laenge	Hash-Alg	Hash-Laenge	Hmac-Alg	Hmac-Laenge	Kompr-Alg	Client-SN	Verb.-Zeit
CLIENT_0004	Verbindung	(none)	passiv	0	NETCOLOGN	9999	91.114.240.66	no-nat	nein	AES	128	HMAC_MD5	128	(none)	0	(none)	nicht-vorhanden	00:46:45
LCS	Verbindung	(none)	aktiv	9999	NETCOLOGN	9999	213.217.69.77	no-nat	nein	AES	128	HMAC_MD5	128	(none)	0	(none)	nicht-vorhanden	05:58:55

11.14 MPPE für PPTP-Tunnel

Das Verschlüsselungsprotokoll MPPE (Microsoft Point-To-Point Encryption) sichert die Datenübertragung über PPP- und VPN-Verbindungen mit Schlüssellängen von bis zu 128 Bit.

MPPE benutzt zur Verschlüsselung den sogenannten „Stateless Mode“, um die Synchronisierung beider Kommunikationspartner sicherzustellen. In diesem Modus ändert sich der Sitzungs-Schlüssel mit jedem zu übertragenden

Datenpaket. Außerdem synchronisieren beide Stationen jedesmal ihre Verschlüsselungs-Tabellen, in denen die Schlüssel zur Datenverschlüsselung gespeichert sind.

VPN-fähige Geräte nutzen MPPE als Möglichkeit zur Verschlüsselung der Datenübertragung über PPTP-Tunnel.

In LANconfig finden Sie diese Einstellung unter **Kommunikation** > **Gegenstellen** > **PPTP** > **PPTP-Liste**.

Haben Sie das Verschlüsselungsprotokoll MPPE aktiviert, kommen Verbindungen von Clients ausschließlich unter folgenden Voraussetzungen zustande:

- Der Client baut eine MPPE-gesicherte Verbindung auf. Bei anderen Protokollen lehnt der Router eine Verbindung ab.
- Der Client verwendet mindestens die im Router vorgegebene Schlüssellänge. Bei geringerer Schlüssellänge lehnt der Router eine Verbindung ab, bei stärkerer Verschlüsselung schaltet der Router auf die entsprechende Schlüssellänge um.

11.15 Layer 2 Tunneling Protocol (L2TP)

LCOS unterstützt L2TP in Version 2 und 3.

Bei L2TPv2 tunnelt ein sogenannter L2TP Access Concentrator (LAC) die PPP-Anfrage eines Clients über eine öffentliche Verbindung (z. B Internet, ATM, Frame Relay) zu einem L2TP Network Server (LNS). Der LNS dient als Gateway zum entfernten Netzwerk. Bei Bedarf authentifiziert dort zunächst ein angeschlossener RADIUS-Server den Client. Anschließend sendet der LNS die zu verwendende IP-Adresse an den LAC und startet den L2TP-Tunnel. Der LAC gibt die IP-Adresse an den Client weiter. Ab diesem Zeitpunkt ist der Client über eine L2TP-Verbindung Teil des entfernten Netzwerkes.

Innerhalb der Firmware sind der LAC und der PPP-Client in einer Rolle zusammengefasst. Ein Gerät als LAC startet also sowohl den Kontrollkanal als auch die PPP-Sitzung. Im Rahmen der Netzwerkvirtualisierung werden mehrere PPP-Sitzungen in einem L2TP-Tunnel unterstützt. Ein L2TP-fähiges Gerät ist sowohl als LAC als auch als LNS einsetzbar.

Bei L2TPv3 wird Ethernet-Traffic (Layer 2) getunnelt über UDP übertragen. Hiermit können also LANs über Netzwerk- und Standortgrenzen hinweg verbunden werden.

Insbesondere bietet es sich an, WLAN-Traffic auf Seiten der Access Points in einen L2TPv3 Ethernet-Tunnel einzukoppeln und an einem zentralen Konzentrator wieder auszukoppeln. Dies erforderte ohne L2TPv3 immer einen WLAN-Controller, der dieses mittels CAPWAP Layer-3-Tunnel realisiert hat. Nun ist dies mit L2TPv3 losgelöst von WLAN-Controllern möglich, so dass der WLAN-Traffic getunnelt übertragen und zentral ausgekoppelt werden kann.

Datentypen

L2TP verwendet zwei Typen von Daten:

Steuerdaten

Die Steuerdaten dienen dem Aufbau, der Aufrechterhaltung und dem Abbau von Tunnel-Verbindungen. Die Steuerdaten enthalten eine Datenfluss-Kontrolle, um sicherzustellen, dass Sender und Empfänger die Steuerdaten korrekt austauschen.

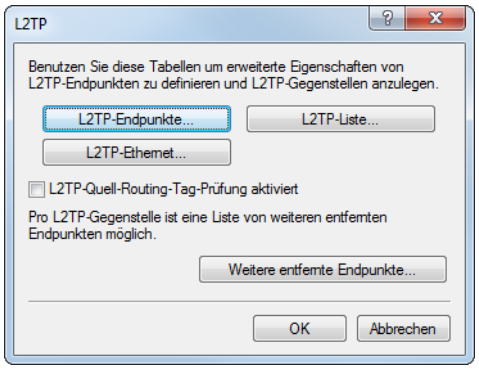
Nutzdaten

Die Nutzdaten kapseln die PPP-Frames, die der LAC und der LNS über den Tunnel austauschen. Im Gegensatz zu den Steuerdaten enthalten die Nutzdaten keine Datenfluss-Kontrolle. Es ist also nicht sichergestellt, dass Sender und Empfänger die Daten fehlerfrei austauschen.

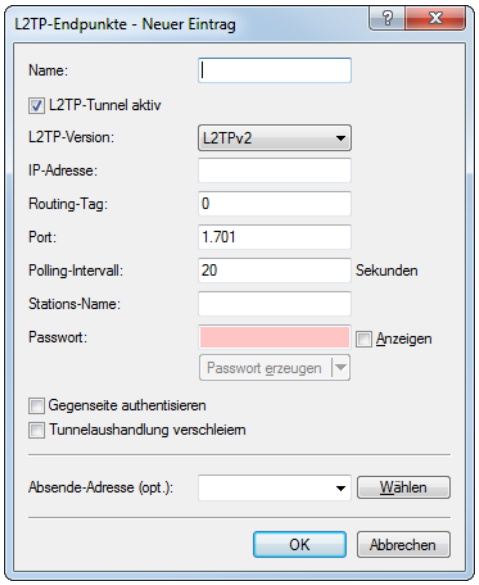
Im Gegensatz zu PPTP, welches Steuer- und Nutzdaten mit unterschiedlichen Protokollen (TCP und GRE) überträgt, nutzt L2TP für beide Datentypen ausschließlich UDP. Sie haben hierbei die Möglichkeit, mehrere logische Nutzdaten-Kanäle je Steuerdaten-Kanal zu betreiben.

11.15.1 Konfiguration der L2TP-Tunnel

Mit LANconfig konfigurieren Sie L2TP unter **Kommunikation** > **Gegenstellen** > **L2TP**.



Die Tunnel-Konfiguration für die Steuerdaten eines L2TP-Tunnels zu einem Tunnelendpunkt erfolgt unter **L2TP-Endpunkte**.



Name

Name des Tunnelendpunktes.

L2TP-Tunnel aktiv

Aktiviert den konfigurierten L2TP-Tunnel.

L2TP-Version

Die verwendete L2TP-Protokollversion, entweder Version 2 oder 3.

Ethernet-Tunnel sind nur mit Version 3 möglich. Achten Sie darauf, für diesen Fall hier das Protokoll „L2TPv3" auszuwählen.

L2TPv3 wird im LCOS immer in UDP gekapselt. Dadurch ist eine problemlose Übertragung durch NAT-Gateways hindurch möglich.

IP-Adresse

IP-Adresse des Tunnelendpunktes (IPv4, IPv6, FQDN).

Falls dieses Feld bei Auswahl des Protokolls L2TPv3 leer gelassen wird, dann handelt es sich um einen „Wildcard"-Eintrag, der Verbindungen von beliebigen Gegenstellen annehmen kann.

Routing-Tag

Routing-Tag der Route zum Tunnelendpunkt.

Wenn für die Absende-Adresse eine Loopback-Adresse eingetragen ist und das Routing-Tag den Wert "0" besitzt, verwendet das Gerät das Routing-Tag der Loopback-Adresse.

Port

UDP-Port

Polling-Intervall

Poll-Intervall in Sekunden

Stations-Name

Name, mit dem sich das Gerät am Tunnelendpunkt authentifiziert

Passwort

Passwort, mit dem sich das Gerät am Tunnelendpunkt authentifiziert

Gegenseite authentisieren

Wenn zwei Tunnelendpunkte (LAC und LNS) sich gegenseitig authentifizieren sollen, um einen Tunnel aufzubauen, ist diese Option aktiv. In diesem Fall sind im Tunnelendpunkt Stations-Name und Passwort dieses Gerätes als Tunnelendpunkt konfiguriert und ebenfalls die Option **Gegenseite authentisieren** aktiv.

Tunnelaushandlung verschleiern

Wenn bereits die Aushandlung eines Tunnels zwischen LAC und LNS verschlüsselt erfolgen soll, ist diese Option aktiv. Hierbei ver- und entschlüsseln beide L2TP-Partner mit Hilfe eines gemeinsamen "preshared Secrets" bestimmte AVPs (Attribute Value Pair) der L2TP-Nachrichten.

Absende-Adresse

Hier können Sie optional eine Absende-Adresse konfigurieren, die das Gerät statt der ansonsten automatisch für die Zieladresse gewählten Absende-Adresse verwendet. Mögliche Werte sind:

- Name der IP-Netzwerke, deren Adresse eingesetzt werden soll.
- "INT" für die Adresse des ersten Intranets
- "DMZ" für die Adresse der ersten DMZ
- LB0 bis LBF für die 16 Loopback-Adressen
- Beliebige gültige IP-Adresse

Wenn in der Liste der IP-Netzwerke oder in der Liste der Loopback-Adressen ein Eintrag mit dem Namen „DMZ" vorhanden ist, verwendet das Gerät die zugehörige IP-Adresse.

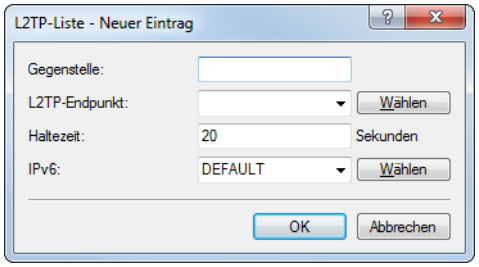
Sofern die hier eingestellte Absende-Adresse eine Loopback-Adresse ist, wird diese auch auf maskiert arbeitenden Gegenstellen unmaskiert verwendet.

Ab LCOS 10.20 sind Layer-3-Ethernet-Tunnel mit L2TPv3 konfigurierbar. Die Konfiguration erfolgt in der soeben beschriebenen L2TP-Endpunkte-Tabelle und in der weiter unten beschriebenen L2TP-Ethernet-Tabelle. Für ein entsprechendes Szenario siehe *Konfiguration eines WLAN-Szenarios mit zentraler Auskopplung der Nutzdaten* auf Seite 851. Falls Sie eine IP-Adresse oder einen Hostnamen angeben, dann wird versucht, eine Verbindung aufzubauen. Wird das entsprechende Feld leer gelassen, wird keine Verbindung aufgebaut, es können aber Verbindungen angenommen werden. Konfigurierte Eigenschaften wie Stations-Name oder Passwort werden beim Verbindungsaufbau durch die Gegenseite geprüft; beim Annehmen von Verbindungen werden diese entsprechend geprüft.

Da die verschiedenen impliziten Abhängigkeiten bei der Verbindungsannahme und der Authentisierung nicht direkt offensichtlich sind, hier einige Erläuterungen dazu:

- Es wird geprüft, ob der von der Gegenseite übermittelte Hostname einem konfigurierten L2TP-Endpunkt entspricht. Der Hostname kann in der L2TP-Endpunktetabelle der Gegenseite unter **Stations-Name** konfiguriert werden. Wird dieses Feld leer gelassen, wird der Gerätename zur Authentifizierung verwendet.
- Ist dies der Fall, wird für den Verbindungsaufbau mit der Konfiguration für eben diesen L2TP-Endpunkt fortgefahren.
- Ist dies nicht der Fall, wird geschaut ob ein „Wildcard"-Eintrag in der L2TP-Endpunkte-Tabelle existiert. Dies ist ein Eintrag ohne konfigurierten Hostnamen / Stations-Namen und ohne Routing-Tag. Es wird für den Verbindungsaufbau dann mit der Konfiguration dieses „Wildcard"-Eintrages fortgefahren.
- Ist für den passenden Eintrag der L2TP-Endpunkte-Tabelle die Authentisierung eingeschaltet, wird die Authentisierung anhand des konfigurierten Passworts gemacht.
- Ist das Passwort leer und die Authentisierung eingeschaltet, wird eine RADIUS-Authentisierung durchgeführt. Siehe *Authentifizierung über RADIUS* auf Seite 843.
- Ist die Authentisierung ausgeschaltet wird mit einem „Wildcard"-Eintrag dementsprechend jeder eingehende Tunnel akzeptiert.

Unter **L2TP-Liste** verknüpfen Sie die L2TP-Gegenstellen mit einem zuvor konfigurierten Tunnelendpunkt.



Ein Eintrag in dieser Tabelle ist nur für die folgenden Bedingungen notwendig:

- abgehende Verbindungen,
- ankommende Verbindungen mit einem Idle-Timeout ungleich „20" oder
- wenn ankommende Verbindungen nur einen bestimmten Tunnel nutzen sollen.

Gegenstelle

Name der L2TP-Gegenstelle

L2TP-Endpunkt

Name des Tunnelendpunktes, den diese Gegenstelle verwendet.

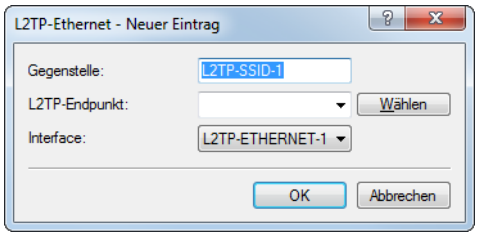
Haltezeit

Bestimmt, wie lange der L2TP-Tunnelendpunkt den Tunnel bei Inaktivität offen hält.

IPv6

Dieser Eintrag gibt den Namen der IPv6-WAN-Schnittstelle an. Ein leerer Eintrag schaltet IPv6 für dieses Interface ab. Die IPv6-Gegenstellen konfigurieren Sie unter **IPv6** > **Allgemein** > **WAN-Schnittstellen**.

Unter **L2TP-Ethernet** verknüpfen Sie L2TPv3-Sessions mit einer der 16 virtuellen L2TP-Ethernet-Schnittstellen. Die virtuellen L2TP-Ethernet-Schnittstellen können anschließend an anderer Stelle in der Konfiguration verwendet werden, z. B. in der LAN-Bridge zur Verknüpfung mit WLAN- oder LAN-Schnittstellen.



Gegenstelle

Konfigurieren Sie hier den Namen, anhand dessen der Ethernet-Tunnel auf der Gegenseite zugeordnet werden soll. Je Ethernet-Tunnel muss dieser Name also auf aufbauender und annehmender Seite gleich lauten.

L2TP-Endpunkt

Konfigurieren Sie hier den Namen des in der L2TP-Endpunkte-Tabelle konfigurierten L2TP-Endpunkts. Somit wird eine Ethernet-Tunnel-Session über diesen Endpunkt aufgebaut. Wenn nur Verbindungen angenommen, aber nicht selber aufgebaut werden sollen, kann durch leer lassen des Feldes erwirkt werden, dass beliebige Sessions angenommen werden. Natürlich müssen diese trotzdem über einen akzeptierten / aufgebauten Endpunkt aus der L2TP-Endpunkte-Tabelle „laufen“. Dies kann in Szenarien, in denen nicht jeder Endpunkt auf der annehmenden Seite separat konfiguriert werden soll, sinnvoll sein.

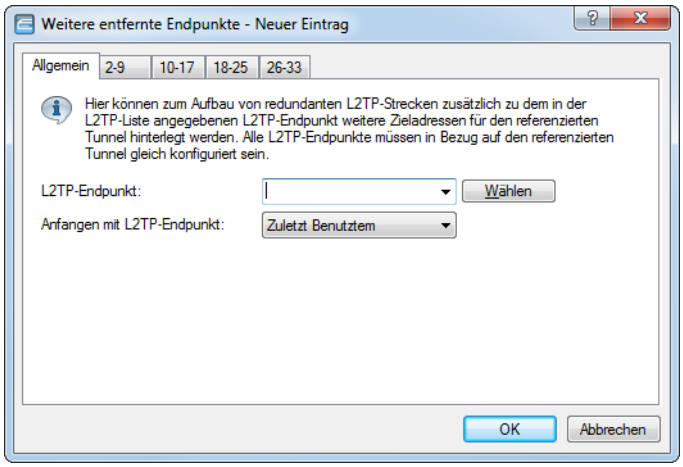
Interface

Die für die L2TPv3-Session zu verwendende virtuelle L2TP-Ethernet-Schnittstelle.

Bei ankommenden Tunnel-Anfragen erfolgt eine Prüfung entweder über RADIUS oder über einen Eintrag des anfragenden Hostes in der L2TP-Endpunkte-Tabelle. Existiert ein Tabellen-Eintrag mit identischer IP-Adresse (oder ist für diesen Eintrag keine IP-Adresse definiert), lässt das Gerät diesen Host für einen Tunnelaufbau zu.

Als zusätzliche Sicherung, um z. B. eine Verschlüsselung der L2TP-Sessions über IPSec zu ermöglichen, kann das Gerät darüber hinaus auch das Routing-Tag der Gegenstelle prüfen, über die es die Daten empfangen hat. Diese Option aktivieren Sie unter **L2TP-Quell-Routing-Tag-Prüfung aktiviert**.

Um bis zu 32 zusätzliche Gateways je Tunnelendpunkt zu konfigurieren, klicken Sie auf **Weitere entfernte Endpunkte**.



Achten Sie darauf, dass alle zusätzlich angegebenen L2TP-Endpunkte identisch zum referenzierten Tunnel-Endpunkt konfiguriert sind.

L2TP-Endpunkt

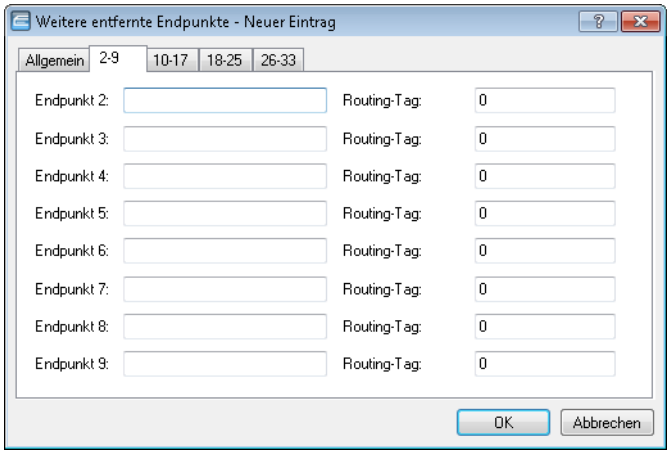
Name des Tunnelendpunktes, wie er in der Tabelle **L2TP-Endpunkte** konfiguriert ist.

Anfangen mit L2TP-Endpunkt

Option zur Auswahl des nächsten Gateways. Folgende Auswahl ist möglich:

- **Zuletzt Benutztem**: Auswahl der zuletzt erfolgreichen Adresse
- **Erstem**: Auswahl des ersten Gateways in der Liste
- **Zufall**: Zufällige Auswahl eines Gateways aus der Liste

Auf den folgenden Reitern konfigurieren Sie die Namen sowie die jeweiligen Routing-Tags der alternativen Gateways.



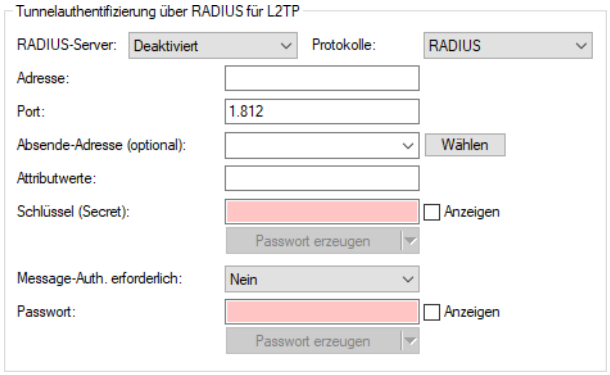
11.15.2 Authentifizierung über RADIUS

Eine RADIUS-Authentifizierung ist bei L2TP in zwei Anwendungsfällen möglich:

- Tunnel-Authentifizierung: Der RADIUS-Server prüft, ob ein LAC eine L2TP-Verbindung aufbauen darf.
- PPP-Session: Der RADIUS-Server prüft die Benutzerdaten der jeweiligen PPP-Session.

Deshalb erfolgt die Konfiguration des RADIUS-Servers für die Authentifizierung des L2TP-Tunnels und der PPP-Benutzerdaten unabhängig voneinander.

Bei einer Tunnel-Authentifizierung über RADIUS konfigurieren Sie die Einstellungen im LANconfig unter **Kommunikation** > **RADIUS** im Abschnitt **Tunnel-Authentifizierung über RADIUS für L2TP**.



RADIUS-Server

Aktiviert bzw. deaktiviert den RADIUS-Server für die Authentifizierung des Tunnelendpunktes, unabhängig von einer Authentifizierung einer PPP-Session. Die folgende Auswahl ist möglich:

- **Deaktiviert**: Der RADIUS-Server ist nicht aktiv für die Authentifizierung eines Tunnelendpunktes.
- **Aktiviert**: Der RADIUS-Server übernimmt die Authentifizierung eines Tunnelendpunktes.
- **Exklusiv**: Aktiviert die Nutzung des externen RADIUS-Servers als ausschließliche Möglichkeit für die Authentifizierung von PPP-Gegenstellen. Die PPP-Liste wird nicht berücksichtigt.

Protokolle

Protokoll für die Kommunikation zwischen dem internen RADIUS-Server und dem Tunnelendpunkt.

Adresse

IP-Adresse oder DNS-Name des RADIUS-Servers.

Port

Port des RADIUS-Servers

Absende-Adresse

Optionale Absende-Adresse des Gerätes. Falls Sie z. B. Loopback-Adressen konfiguriert haben, ist deren Eingabe hier ebenfalls möglich. Folgende Eingabeformate sind erlaubt:

- Name des IP-Netzwerkes (ARF-Netz), dessen Adresse stattdessen zu verwenden ist
- "INT" für die Adresse des ersten Intranets
- "DMZ" für die Adresse der ersten DMZ
- LB0 bis LBF für die 16 Loopback-Adressen
- Beliebige gültige IP-Adresse

Attributwerte

LCOS ermöglicht es, die RADIUS-Attribute für die Kommunikation mit einem RADIUS-Server (sowohl Authentication als auch Accounting) zu konfigurieren.

Die Angabe der Attribute erfolgt als semikolon-separierte Liste von Attribut-Nummern oder -Namen und einem entsprechenden Wert in der folgenden Form:

`<Attribut_1>=<Wert_1>;<Attribut_2>=<Wert_2>`

Da die Anzahl der Zeichen begrenzt ist, lässt sich der Name abkürzen. Das Kürzel muss dabei eindeutig sein. Beispiele:

- `NAS-Port=1234` ist nicht erlaubt, da das Attribut nicht eindeutig ist (`NAS-Port`, `NAS-Port-Id` oder `NAS-Port-Type`).
- `NAS-Id=ABCD` ist erlaubt, da das Attribut eindeutig ist (`NAS-Identifier`).

Als Attribut-Wert ist die Angabe von Namen oder RFC-konformen Nummern möglich. Für das Gerät sind die Angaben `Service-Type=Framed` und `Service-Type=2` identisch.

Die Angabe eines Wertes in Anführungszeichen (`"<Wert>"`) ist möglich, um Sonderzeichen wie Leerzeichen, Semikolon oder Gleichheitszeichen mit angeben zu können. Das Anführungszeichen erhält einen umgekehrten Schrägstrich vorangestellt (`\"`), der umgekehrte Schrägstrich ebenfalls (`\\`).

Als Werte sind auch die folgenden Variablen erlaubt:

`%n`

Gerätename

`%e`

Seriennummer des Gerätes

`%%`

Prozentzeichen

`%{name}`

Original-Name des Attributes, wie ihn die RADIUS-Anwendung überträgt. Damit lassen sich z. B. Attribute mit originalen RADIUS-Attributen belegen: `Called-Station-Id=%{NAS-Identifier}` setzt das Attribut `Called-Station-Id` auf den Wert, den das Attribut `NAS-Identifier` besitzt.

Schlüssel (Secret)

Shared-Secret zwischen dem RADIUS-Server und dem Gerät

Passwort

Dummy-Passwort für die Tunnel-Authentifizierung

Trifft von einem entfernten Host eine L2TP-Tunnelanfrage ein (Start Control Connection Request), schickt das Gerät eine Anfrage an den für L2TP aktivierten RADIUS-Server. Diese Anfrage enthält u. a. den Namen des Hostes, das Dummy-Passwort, die IP-Adresse des Gerätes sowie den Service-Typ "Outbound-User". Der RADIUS-Server authentifiziert den Host und schickt ein "RADIUS-Accept" an das Gerät zusammen mit dem zu verwendenden Tunnel-Passwort, dem Tunnel-Typ "L2TP" mit dem Tag "0" sowie der Tunnel-Client-Auth-ID, die dem zuvor vom Gerät übermittelten Stationsnamen entsprechen muss. Das Gerät prüft diese Daten und übernimmt bei positivem Ergebnis das Tunnel-Passwort, um den einwählenden Client zu authentifizieren und ggf. die L2TP-Tunnelaushandlung zu verschleiern.

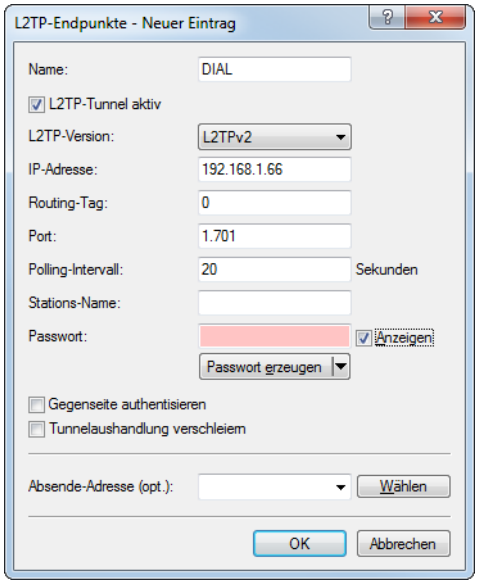
Die Konfiguration des RADIUS-Servers zur Authentifizierung von PPP-Sessions erfolgt, wie es im Abschnitt **Weitere Dienste** > **RADIUS** > **Konfiguration von RADIUS als Authenticator bzw. NAS** > **Einwahl über PPP und RADIUS** beschrieben ist.

11.15.3 Betrieb als L2TP Access Concentrator (LAC)

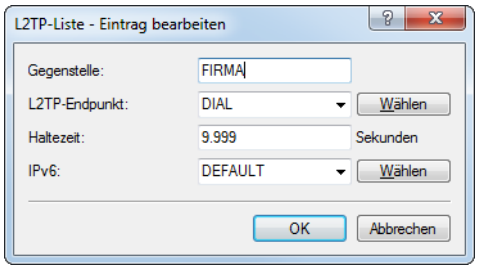
Im folgenden Beispiel baut das Gerät als L2TP Access Concentrator (LAC) einen L2TP-Tunnel zu einem L2TP Network Server (LNS) mit der IP-Adresse 192.168.1.66 auf.

Um das Gerät als LAC zu konfigurieren, gehen Sie wie folgt vor:

1. Erstellen Sie unter **Kommunikation** > **Gegenstellen** > **L2TP** in der Tabelle **L2TP-Endpunkte** einen Eintrag für einen LNS als entferntes L2TP-Gateway.

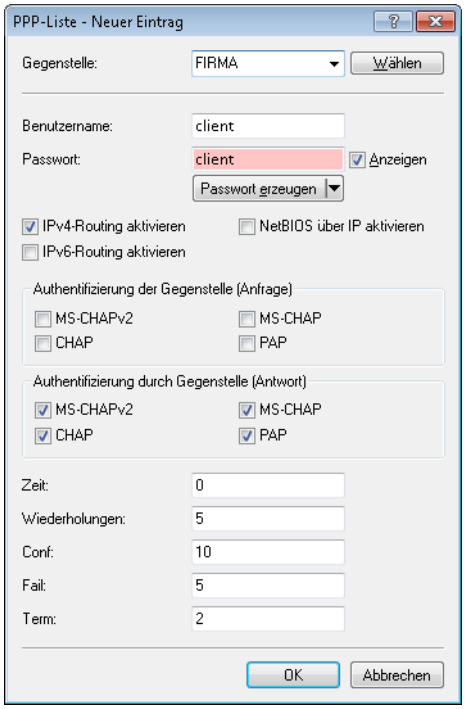


2. Vergeben Sie unter **Kommunikation** > **Gegenstellen** > **L2TP** in der Tabelle **L2TP-Liste** einen Namen für diese Gegenstelle und verbinden Sie sie mit dem zuvor angelegten L2TP-Endpunkt.

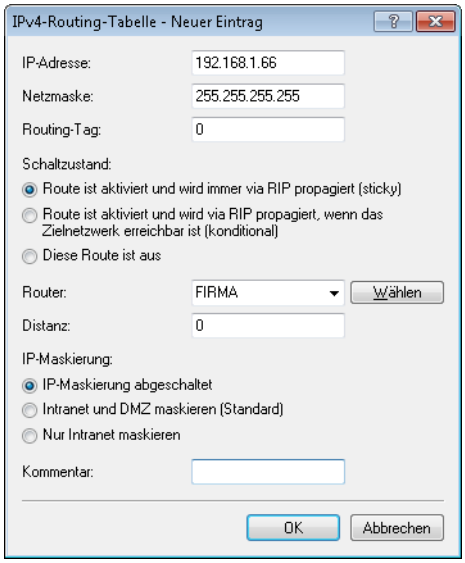


Es ist möglich, mehrere Gegenstellen mit einem L2TP-Tunnel zu verbinden. Dadurch lassen sich mehrere PPP-Sessions durch einen L2TP-Tunnel transportieren. Konfigurieren Sie hierfür in dieser Tabelle mehrere Gegenstellen mit dem gleichen L2TP-Endpunkt.

3. Erstellen Sie unter **Kommunikation** > **Protokolle** in der Tabelle **PPP-Liste** einen Eintrag für den L2TP-Tunnel.



4. Legen Sie unter **Konfiguration** > **IP-Router** > **Routing** in der entsprechenden IPv4- oder IPv6-Routing-Tabelle einen Eintrag für diese Gegenstelle an.

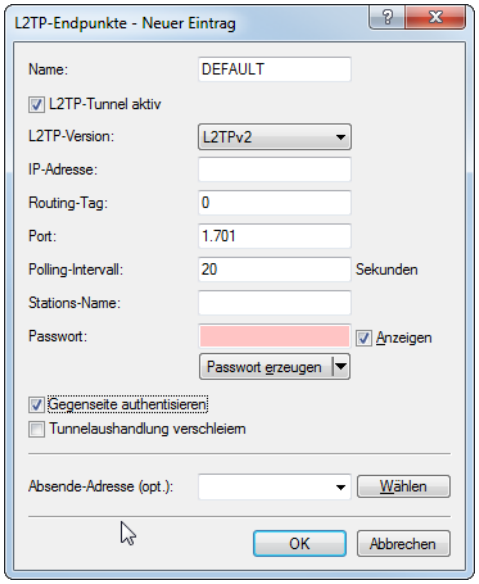


11.15.4 Betrieb als L2TP Network Server (LNS) mit Authentifizierung über RADIUS

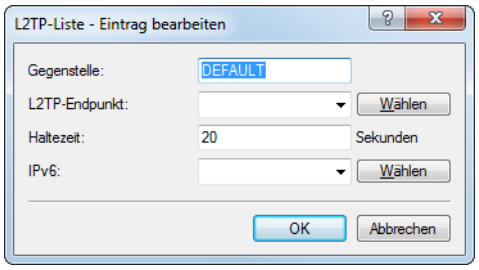
Im folgenden Beispiel arbeitet das Gerät als L2TP Network Server (LNS). Die Authentifizierung der eingehenden L2TP-Tunnel sowie der PPP-Sessions erfolgt über RADIUS.

Um das Gerät als LNS zu konfigurieren, gehen Sie wie folgt vor:

1. Erstellen Sie unter **Kommunikation** > **Gegenstellen** > **L2TP** in der Tabelle **L2TP-Endpunkte** einen Eintrag „DEFAULT“.

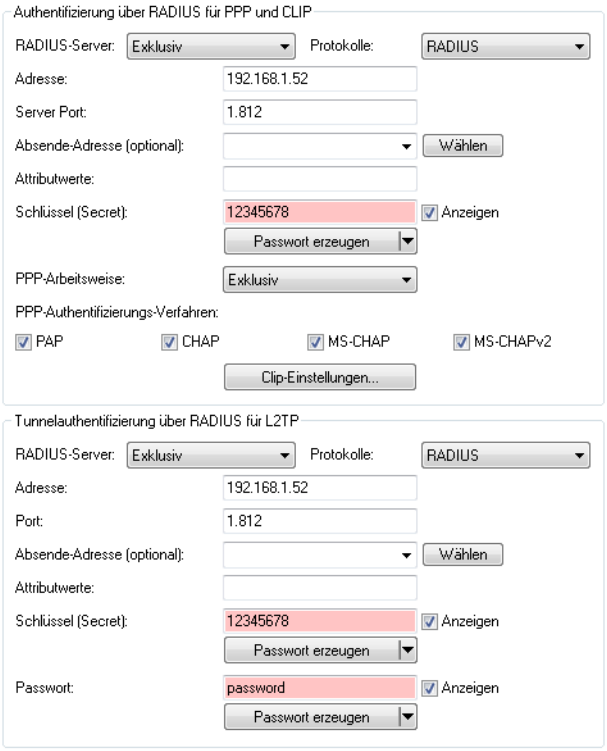


2. Konfigurieren Sie anschließend unter **Kommunikation** > **Gegenstellen** > **L2TP** in der Tabelle **L2TP-Liste** einen Eintrag „DEFAULT“.



Falls der L2TP-Tunnel dauerhaft verbunden sein soll, setzen Sie die Haltezeit auf „9999“.

3. Konfigurieren Sie unter **Kommunikation** > **RADIUS** den RADIUS-Server.



Den unteren Abschnitt **RADIUS-Server-Einstellungen für L2TP** konfigurieren Sie nur, wenn eine L2TP-Tunnel-Authentifizierung über den RADIUS-Server erfolgen soll.

4. Konfigurieren Sie den RADIUS-Server entsprechend, damit er die Authentifizierung des L2TP-Tunnels und der PPP-Sessions durchführen kann.

   Möchte sich ein LAC mit dem Stationsnamen "router1" und dem Passwort "abcde" für den L2TP-Tunnel authentifizieren lassen, konfigurieren Sie den entsprechenden Eintrag im RADIUS-Server (z. B. FreeRADIUS) wie folgt:

```
router1 Cleartext-Password := "password"
        Service-Type := Outbound-User,
        Tunnel-Type  := L2TP,
        Tunnel-Password := "abcde",
        Tunnel-Client-Auth-ID := "router1"
```

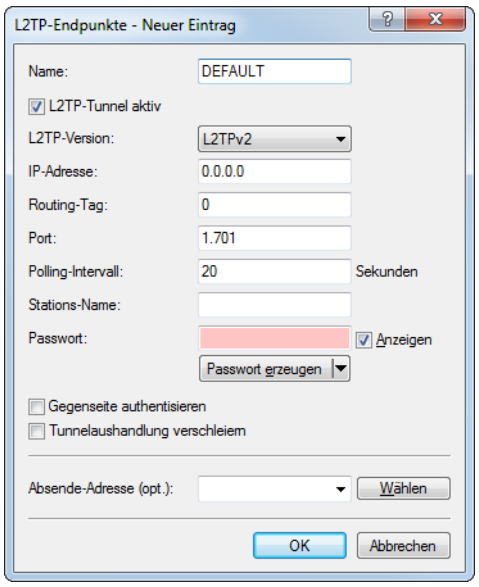
   Für die Authentifizierung der PPP-Session eines Benutzers mit dem Benutzernamen "test" und dem Passwort "1234" lautet der entsprechende Eintrag im RADIUS-Server wie folgt:

```
test Cleartext-Password := "1234"
     Service-Type := Framed-User,
     Framed-Protocol := PPP
```

11.15.5 Betrieb als L2TP Network Server (LNS) für RAS-Clients

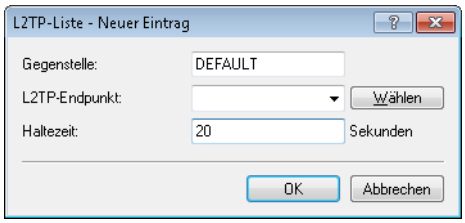
Um das Gerät als L2TP Network Server (LNS) für die Anmeldung von RAS-Clients zu konfigurieren, ohne einen RADIUS-Server im Gerät zu konfigurieren, haben Sie zwei Möglichkeiten:

1. Erstellen Sie unter **Kommunikation** > **Gegenstelle** > **L2TP** in der Tabelle **L2TP-Endpunkte** einen Eintrag "DEFAULT".



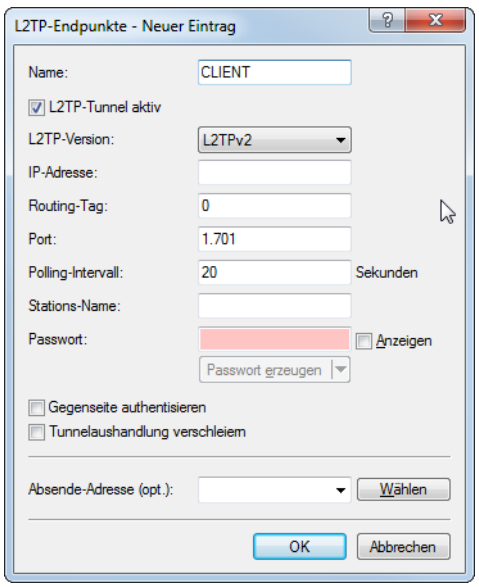
Der Eintrag für die IP-Adresse lautet "0.0.0.0", da die IP-Adresse des L2TP-LACs dem Gerät unbekannt ist.

2. Konfigurieren Sie anschließend unter **Kommunikation** > **Gegenstellen** > **L2TP** in der Tabelle **L2TP-Liste** einen Eintrag "DEFAULT".

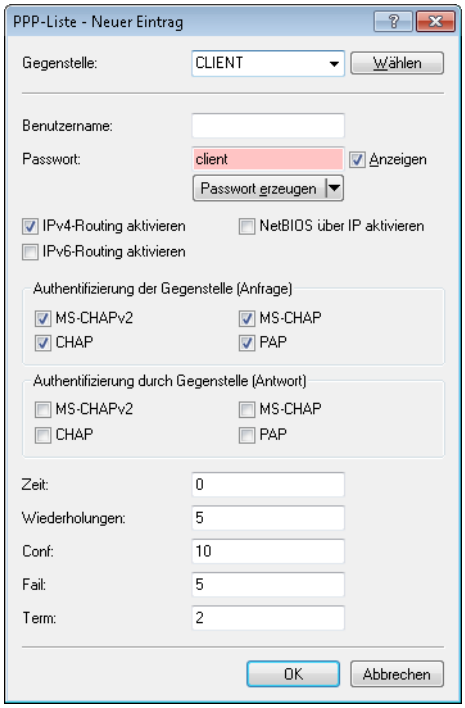


Soll der L2TP-Tunnel dauerhaft verbunden sein, setzen Sie die Haltezeit auf "9999".

3. Alternativ legen Sie unter **Kommunikation** > **Gegenstellen** > **L2TP** in der Tabelle **L2TP-Endpunkte** für den RAS-Client einen separaten Eintrag (z. B. "CLIENT") an.



4. Anschließend konfigurieren Sie unter **Kommunikation** > **Protokolle** in der **PPP-Liste** für den Client einen neuen Eintrag.



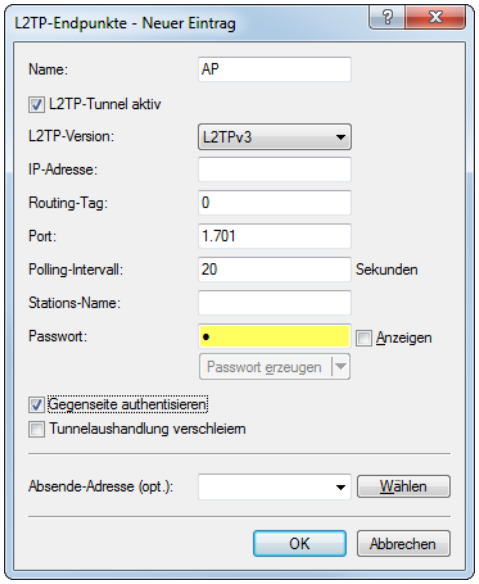
11.15.6 Konfiguration eines WLAN-Szenarios mit zentraler Auskopplung der Nutzdaten

Hier wird exemplarisch beschrieben, wie mittels L2TPv3 ein Szenario umgesetzt werden kann, in dem mehrere Access Points ihre Nutzdaten zu einem zentralen Router (hier „Konzentrator" genannt) übertragen, wo diese über einen separaten Ethernet-Port ausgekoppelt werden.

Vor LCOS 10.20 wurde für dieses Szenario ein WLAN-Controller benötigt.

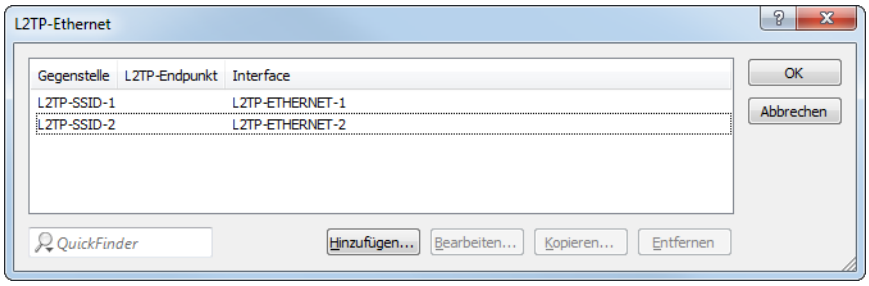
1. Bereiten Sie die WLAN-Konfiguration auf den Access Points vor. Um Roaming zu ermöglichen, sollten SSID-Namen und Verschlüsselungseinstellungen identisch konfiguriert sein.
2. Konfigurieren Sie nun den Konzentrator, der die L2TPv3-Ethernet-Sessions der einzelnen Access Points annehmen soll.
   a) Erstellen Sie unter **Kommunikation** > **Gegenstellen** > **L2TP** in der Tabelle L2TP-Endpunkte einen neuen Eintrag. Vergeben Sie einen aussagekräftigen Namen für den neuen Eintrag. Setzen Sie die **L2TP-Version** auf „L2TPv3". Geben Sie keine **IP-Adresse** an. Setzen Sie ein Passwort, um die Sicherheit zu erhöhen und wählen Sie „Gegenseite

authentisieren", damit das Passwort beim Verbindungsaufbau zur Authentisierung verwendet wird. Belassen Sie die restlichen Einstellungen auf ihren Standardwerten.



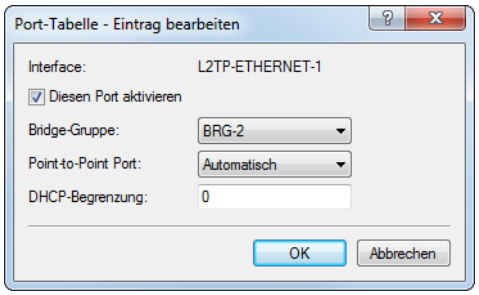
Die **IP-Adresse** ist leer. Es handelt sich daher um einen „Wildcard"-Eintrag, der Verbindungen von beliebigen Gegenstellen annehmen kann.

b) Erstellen Sie unter **Kommunikation** > **Gegenstellen** > **L2TP** in der Tabelle L2TP-Ethernet einen neuen Eintrag. Vergeben Sie unter **Gegenstelle** einen Namen, der den Ethernet-Tunnel identifiziert, z. B. den Namen der SSID, mit der der Tunnel auf den Access Points verknüpft werden soll. Lassen Sie das Feld **L2TP-Endpunkt** leer, um beliebige (authentisierte) Sessions anzunehmen. Auf diese Weise müssen Sie nicht noch für jeden Access Point einen Eintrag in der L2TP-Endpunkte-Tabelle anlegen – stattdessen genügt der im vorherigen Schritt erzeugte Wildcard-Eintrag. Konfigurieren Sie nun noch unter **Interface**, mit welchem virtuellen Interface der L2TP-Ethernet-Tunnel verbunden werden soll. Falls Sie auf den Access Points mehr als eine SSID verwenden, die zentral ausgekoppelt werden sollen, können Sie in dieser Tabelle je SSID einen weiteren Eintrag anlegen, der unter **Gegenstelle** einen eindeutigen Namen aufweist.



In unserem Szenario werden die Nutzdaten aller verbundener Access Points in das hier konfigurierte virtuelle Interface geleitet. Auch werden die Nutzdaten aller mit diesem virtuellen Interface verbundener Access Points untereinander gebridged – ähnlich dem Verfahren mit WLAN-Controller-gestütztem Layer-3-Tunnel.

c) Verknüpfen Sie unter **Schnittstellen** > **LAN** > **LAN-Bridge-Einstellungen** > **Port-Tabelle** das oben gewählte virtuelle L2TP-Interface mit einem LAN-Interface, in dem Sie die selbe Bridge-Gruppe setzen. Wiederholen Sie dies für eventuelle weitere virtuelle L2TP-Interfaces für weitere SSIDs.

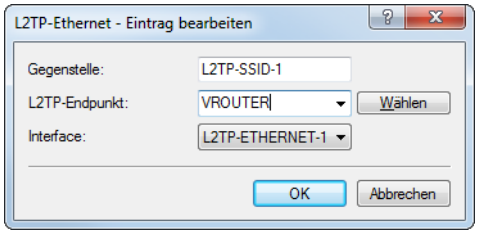


d) Die Konfiguration des Konzentrators ist damit abgeschlossen.

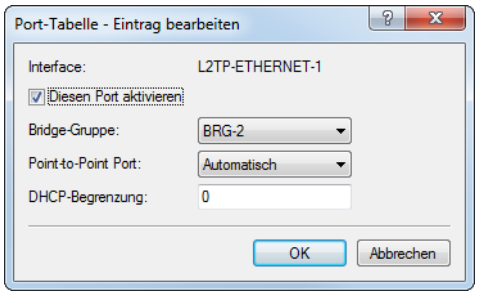
3. Konfigurieren Sie nun exemplarisch einen Access Point, der Nutzdaten an den Konzentrator leiten soll.

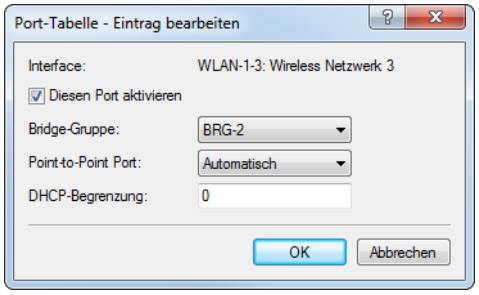
a) Erstellen Sie unter **Kommunikation** > **Gegenstellen** > **L2TP** in der Tabelle L2TP-Endpunkte einen neuen Eintrag. Vergeben Sie einen aussagekräftigen Namen für den neuen Eintrag. Setzen Sie die **L2TP-Version** auf „L2TPv3". Geben Sie die IP-Adresse oder den Hostnamen an, unter dem der Access Point den Konzentrator kontaktieren soll. Setzen Sie das bei der Konfiguration des Konzentrators vergebene Passwort und wählen Sie „Gegenseite authentisieren", damit das Passwort zur Authentisierung verwendet wird. Belassen Sie die restlichen Einstellungen auf ihren Standardwerten.

b) Erstellen Sie unter **Kommunikation** > **Gegenstellen** > **L2TP** in der Tabelle L2TP-Ethernet einen neuen Eintrag. Vergeben Sie unter **Gegenstelle** einen Namen, der den Ethernet-Tunnel identifiziert. Dieser muss gleich dem Namen lauten, der für diesen Ethernet-Tunnel auf dem Konzentrator vergeben wurde. Tragen Sie im Feld **L2TP-Endpunkt** den im vorherigen Schritt erzeugten Eintrag der L2TP-Endpunkte-Tabelle ein – über diesen Endpunkt wird der Ethernet-Tunnel dann aufgebaut. Konfigurieren Sie nun noch unter **Interface**, mit welchem virtuellen Interface der L2TP-Ethernet-Tunnel verbunden werden soll.



c) Verknüpfen Sie unter **Schnittstellen** > **LAN** > **LAN-Bridge-Einstellungen** > **Port-Tabelle** das oben gewählte virtuelle L2TP-Interface mit einem WLAN-Interface, in dem Sie die selbe Bridge-Gruppe setzen. Wiederholen Sie dies für eventuelle weitere virtuelle L2TP-Interfaces für weitere SSIDs.



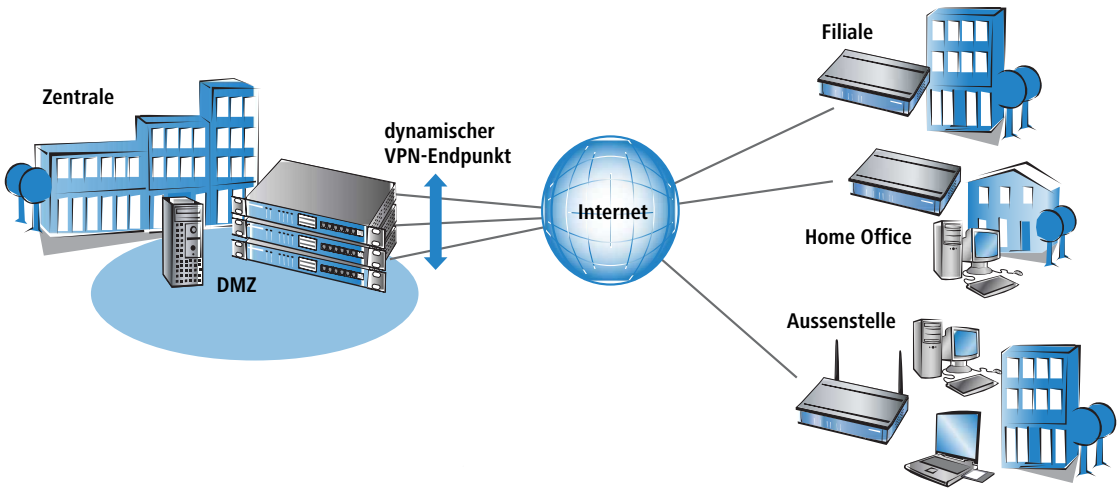


d) Führen Sie die Konfiguration wie hier beschrieben für weitere Access Points durch. Wenn Sie die Konfiguration auf diese Weise durchgeführt haben, dann kann auf allen Access Points die identische Konfiguration verwendet werden und es sind keine Access-Point-spezifischen Anpassungen notwendig.

11.16 VPN-Verbindungen: hohe Verfügbarkeit mit „Lastenausgleich“

11.16.1 Mehrere VPN-Gateway-Adressen

In verteilten Unternehmensstrukturen, die auf Vernetzung der Standorte über VPN setzen, kommt der Verfügbarkeit der zentralen VPN-Gateways eine besondere Bedeutung zu. Nur wenn diese zentralen Einwahlknoten einwandfrei funktionieren, kann die betriebliche Kommunikation reibungslos ablaufen.



Mit der Möglichkeit, mehrere „Remote-Gateway"-Adressen als „dynamischer VPN-Endpunkt" für eine VPN-Verbindung zu konfigurieren, bieten VPN-Gateways eine hohe Verfügbarkeit durch den Einsatz redundanter Geräte. Dabei werden in der Zentrale mehrere Gateways mit gleicher VPN-Konfiguration eingesetzt. In den Außenstellen werden alle vorhandenen Gateways als mögliche Gegenstellen für die gewünschte VPN-Verbindung eingetragen. Falls eines der Gateways nicht erreichbar ist, weicht der entfernte Router automatisch auf eine der anderen Gegenstellen aus.

Damit die Rechner im LAN der Zentrale auch wissen, welche Aussenstelle gerade über welches VPN-Gateway erreicht werden kann, werden die jeweils aktuellen Outband-Routen zu den verbundenen Gegenstellen über RIPv2 im Netzwerk der Zentrale propagiert.

Wenn die Außenstellen so konfiguriert werden, dass sie beim Aufbau der VPN-Verbindung die Gegenstelle zufällig auswählen, wird mit diesem Mechanismus die Hochverfügbarkeit mit gleichmäßiger Lastverteilung zwischen den VPN-Gateways in der Zentrale realisiert („Load-Balancing").

11.16.2 Gruppierung und Priorisierung von alternativen Gateways

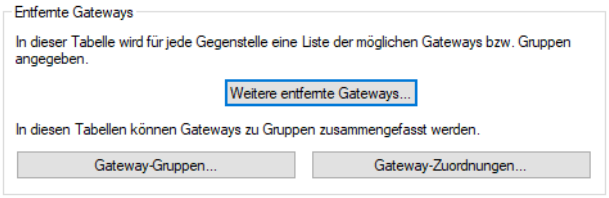
Zusätzlich unterstützt Ihr Gerät die Möglichkeit der Gruppierung und Priorisierung von alternativen VPN-Gateways. Dies erweitert die bereits vorhandene Möglichkeit, bis zu 32 zusätzliche Gateways zu konfigurieren, die alternativ nach einem konfigurierbaren Schema (Erstes, Zuletzt benutzt, Zufall) als Einwahlpunkt verwendet wurden, sobald das primäre VPN-Gateway nicht erreichbar war.

Nun können Gateways optional in Gruppen zusammengefasst werden, wobei Gruppen gleicher Priorität auf einer Ebene nebeneinander angesiedelt werden. Die höchste Priorität ist 0, die niedrigste 65535. Der primäre Gateway wird automatisch in einer eigenen Gruppe mit Priorität 0 angelegt. Wenn der primäre Gateway selbst eine Gateway-Gruppe referenziert, so wird diese Gruppe unabhängig von ihrer konfigurierten Priorität mit der Priorität 0 der Ebenenstruktur hinzugefügt. Alle Gateways aus der Tabelle der **weiteren entfernten Gateways**, die keinen Gruppennamen referenzieren, werden ebenfalls der Gruppe der primären Gateways hinzugefügt. Die Auswahl-Strategie innerhalb der Gruppe der primären Gateways wird durch die folgenden Regeln definiert:

- Gibt es zusätzliche Gateways, so wird die Auswahl-Strategie durch die Spalte **Anfangen mit** aus der Tabelle der **weiteren entfernten Gateways** festgelegt.
- Gibt es keine zusätzlichen Gateways:
  - Gibt es nur einen primären Gateway, so ist die Auswahl-Strategie „Erstes".
  - Ist der primäre Gateway eine Gateway-Gruppe, so wird die Auswahl-Strategie der Gruppe verwendet.

Alle definierten Gruppen werden dann in der Reihenfolge der Gateways aus der Tabelle der **weiteren entfernten Gateways** der Ebenenstruktur mit ihrer in der Tabelle **Gateway-Gruppen** hinterlegten Priorität hinzugefügt. Die Auswahl-Strategie zwischen den Gruppen gleicher Priorität wird durch die Spalte **Anfangen mit** aus der Tabelle **Weitere entfernte Gateways** festgelegt, die Auswahl-Strategie innerhalb einer Gruppe durch die Spalte **Beginne mit** in der Tabelle **Gateway-Gruppen**. Die verschiedenen Ebenen werden immer in aufsteigender Reihenfolge ihrer Priorität nach beginnend mit 0 verwendet.

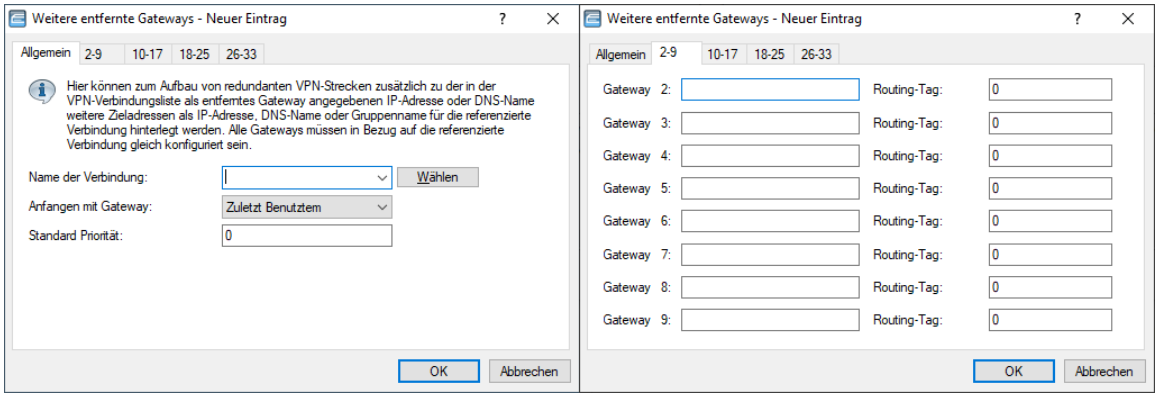
Die Konfiguration erfolgt unter **VPN** > **Allgemein** > **Entfernte Gateways**.



11.16.2.1 Weitere entfernte Gateways

Unter **Weitere entfernte Gateways** können zum Aufbau von redundanten VPN-Strecken zusätzlich zu der in der VPN-Verbindungsliste als entferntes Gateway angegebenen IP-Adresse oder DNS-Name weitere Zieladressen als IP-Adresse,

DNS-Name oder Gruppenname für die referenzierte Verbindung hinterlegt werden. Alle Gateways müssen in Bezug auf die referenzierte Verbindung gleich konfiguriert sein.



Name der Verbindung

Wählen Sie aus der Liste der definierten VPN-Verbindungen den Namen der VPN-Verbindung aus, für welche die hier definierten zusätzlichen Gateways gelten sollen.

Anfangen mit Gateway

Auswahl des Gateways, über das zuerst der Aufbau der VPN-Verbindung versucht werden soll. Mögliche Werte:

Zuletzt Benutztem

Beginnt mit dem Gateway, über den zuletzt eine Verbindung erfolgreich aufgebaut werden konnte.

Erstem

Beginnt mit dem ersten Eintrag in der Liste.

Zufall

Wählt zufällig einen Eintrag aus der Liste.

Standard-Priorität

Dies ist die Standard-Priorität für alle hier definierten Gateways. Die höchste Priorität ist 0, die niedrigste 65535. Alle Gateways werden jeweils in Gruppen zusammengefasst, wobei Gruppen gleicher Priorität auf einer Ebene nebeneinander angesiedelt werden.

Der primäre Gateway wird automatisch in einer eigenen Gruppe mit Priorität 0 angelegt. Wenn der primäre Gateway selbst eine Gateway-Gruppe referenziert, so wird diese Gruppe unabhängig von ihrer konfigurierten Priorität mit der Priorität 0 der Ebenenstruktur hinzugefügt. Werden hier alternative Gateways definiert, die keine Gateway-Gruppe referenzieren, dann werden diese ebenfalls der Gruppe der primären Gateways hinzugefügt.

Gateway 2-33

Für jeden der bis zu 32 alternativen Gateways können Sie drei mögliche Einträge vornehmen:

1. Der Name einer Gateway-Gruppe
2. Der DNS-Name eines Gateways
3. Die IP-Adresse eines Gateways

Beim Auswerten der Tabelle wird nun zuerst geprüft, ob der eingetragene Gateway der Name einer Gruppe ist, die in der Tabelle **Gateway-Grupen** definiert ist. In diesem Fall werden alle Gateways, die über die Tabelle **Gateway-Zuordnungen** dieser Gruppe zugeordnet sind, in die Gateway-Liste aufgenommen.

Routing-Tag

Geben Sie hier das jeweilige Routing-Tag an, mit dem die Route zum zugehörigen entfernten Gateway ermittelt wird.

Wenn Sie hier kein Routing-Tag angeben (d. h. das Routing-Tag ist 0), dann wird für den zugehörigen Gateway das in der VPN-Verbindungs-Liste für diese Gegenstelle konfigurierte Routing-Tag verwendet.

Beispiel eines alternativen Gateways

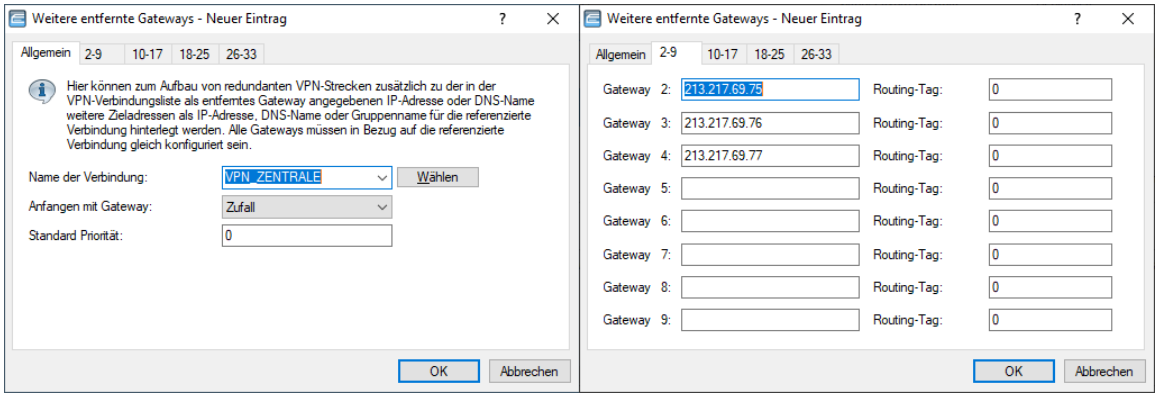
Unter **Weitere entfernte Gateways** tragen Sie in der Liste zusätzliche Ziele für eine VPN-Verbindung ein. Die Liste besteht aus den folgenden Einträgen:

- Name der Gegenstelle aus der VPN-Verbindungsliste, das „Ziel" der VPN-Verbindung.
- Gateway 2 bis Gateway 33, die Adressen der alternativen Gateways, als IP-Adresse oder auflösbarer DNS-Name.
- Definition der Reihenfolge, in der die Gateway-Adressen versucht werden.

Der Eintrag für das Gateway in der VPN-Verbindungsliste kann frei bleiben, wenn alle möglichen Gateways in der Liste **Weitere entfernte Gateways** eingetragen sind.

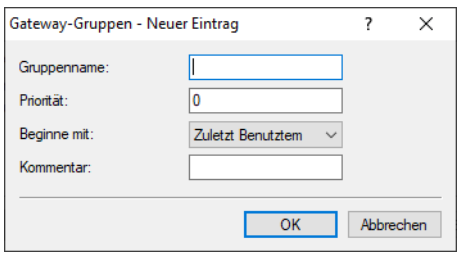
Beispiel:

Mit dem folgenden Einträgen legen Sie drei Gateways (213.217.69.75, 213.217.69.76, 213.217.69.77) als Ziel in der Zentrale fest, die zufällig ausgewählt werden:



11.16.2.2 Gateway-Gruppen

Unter **Gateway-Gruppen** können Sie Gateway-Gruppen einrichten, die Sie dann unter *Weitere entfernte Gateways* referenzieren können.



Gruppenname

Geben Sie dieser Gateway-Gruppe einen eindeutigen Namen, über den Sie diese Gruppe referenzieren können.

Priorität

Die Priorität dieser Gruppe. Die höchste Priorität ist 0, die niedrigste 65535.

Beginne mit

Auswahl-Strategie innerhalb der Gruppe. Mögliche Werte:

Zuletzt Benutztem

Beginnt mit dem Gateway in der Gruppe, über den zuletzt eine Verbindung erfolgreich aufgebaut werden konnte.

Erstem

Beginnt mit dem ersten Eintrag in der Liste.

Zufall

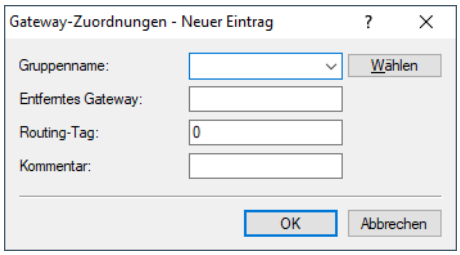
Wählt zufällig einen Eintrag aus der Liste.

Kommentar

Vergeben Sie optional einen sinnvollen Kommentar als Beschreibung.

11.16.2.3 Gateway-Zuordnungen

Unter **Gateway-Zuordnungen** können Sie Gateway-Gruppen einrichten, die Sie dann unter *Weitere entfernte Gateways* referenzieren können. **Entferntes Gateway** und **Gruppenname** bilden zusammen den Primärschlüssel der Tabelle, d. h. die Kombination aus beiden muss innerhalb der Tabelle eindeutig sein. Damit kann ein einzelner Gateway aber auch mehreren Gruppen zugeordnet werden, insofern das gewünscht ist.



Gruppenname

Name der Gruppe, zu dem der Gateway gehört.

Entferntes Gateway

DNS-Name oder IP-Adresse eines Gateways.

Routing-Tag

Routing-Tag des Gateways.

Kommentar

Vergeben Sie optional einen sinnvollen Kommentar als Beschreibung.

11.16.2.4 Beispiel eines alternativen Gateways mit priorisierten Gruppen

Der Kunde „Telekom“ nutze den primären Gateway 1.1.1.1 und den zusätzlichen Gateway 1.1.1.2 ohne spezielle Gruppenzugehörigkeit. Darüber hinaus werden unter **VPN** > **Allgemein** > **Entfernte Gateways** die folgenden weiteren entfernten Gateways, Gateway-Gruppen und Gateway-Zuordnungen angegeben:

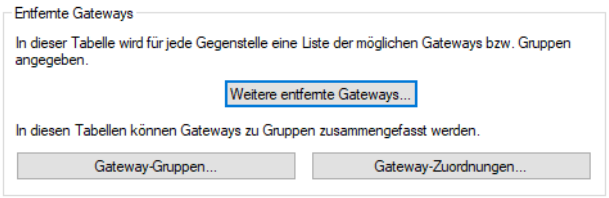


Abbildung 2: Entfernte Gateways

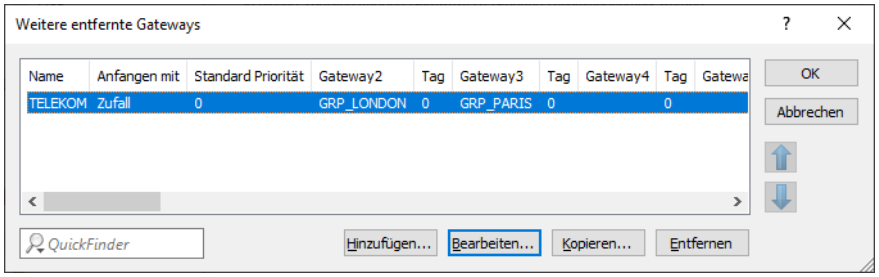


Abbildung 3: Weitere entfernte Gateways

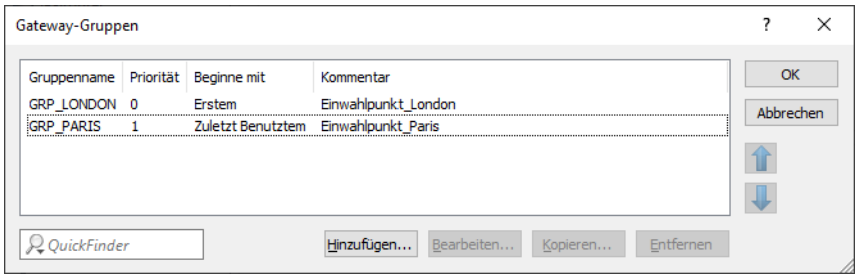


Abbildung 4: Gateway-Gruppen

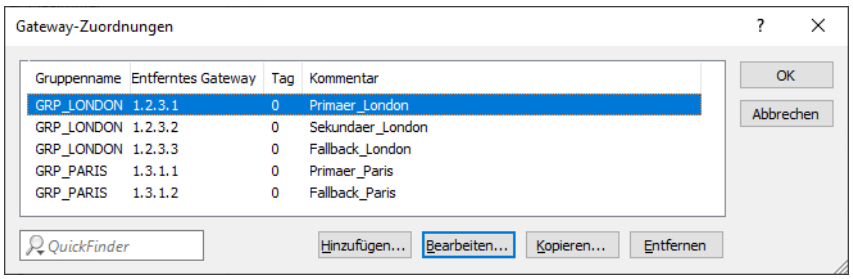


Abbildung 5: Gateway-Zuordnungen

Dadurch würde sich die folgende Ebenenstruktur ergeben:

Priorität	Gruppe 1	Gruppe 2
0	1.1.1.1, 1.1.1.2	GRP_LONDON
1	GRP_PARIS	

Die Gateways würden dann in der folgenden Reihenfolge angesprochen:

1. Priorität 0: Es wird nach dem Zufallsprinzip eine Gruppe ausgewählt, weil in der Tabelle **Weitere entfernte Gateways** die Spalte **Anfangen** mit auf „Zufall" gesetzt ist:
   - 1.1.1.1, 1.1.1.2 (Primärer Gateway sowie zusätzlicher Gateway, der keiner Gruppe angehört)
   - 1.2.3.1, 1.2.3.2, 1.2.3.3 (GRP_LONDON) beginnend mit dem ersten Gateway in dieser Gruppe
2. Priorität 1: Es wird nach dem Zufallsprinzip eine Gruppe ausgewählt, weil in der Tabelle **Weitere entfernte Gateways** die Spalte **Anfangen mit** auf „Zufall" gesetzt ist:
   - 1.3.1.1, 1.3.1.2 (GRP_PARIS) beginnend mit dem letzten Gateway in dieser Gruppe, der zuvor erreicht werden konnte.

11.17 Wie funktioniert VPN?

Ein VPN muss in der Praxis einer Reihe von Ansprüchen gerecht werden:

- Unbefugte Dritte dürfen die Daten nicht lesen können (Verschlüsselung)
- Ausschluss von Datenmanipulationen (Datenintegrität)
- Zweifelsfreie Feststellung des Absenders der Daten (Authentizität)
- Einfache Handhabung der Schlüssel
- Kompatibilität mit VPN-Geräten verschiedener Hersteller

Diese fünf wichtigen Ziele erreicht VPN durch die Verwendung des weitverbreiteten IPSec-Standards.

11.17.1 IPSec – Die Basis für VPN

Das ursprüngliche IP-Protokoll enthält keinerlei Sicherheitsvorkehrungen. Erschwerend kommt hinzu, dass Pakete unter IP nicht gezielt an den Empfänger gesendet werden, sondern über das gesamte Netzwerksegment an alle angeschlossenen Rechner gestreut werden. Wer auch immer möchte, bedient sich und liest die Pakete mit. Datenmissbrauch ist so möglich.

Deshalb wurde IP weiterentwickelt und es gibt IP inzwischen auch in einer sicheren Variante: IPSec. VPN basiert auf IPSec.

IPSec steht für „**IPSec**urity Protocol" und ist ursprünglich der Name einer Arbeitsgruppe innerhalb des Interessenverbandes IETF, der **I**nternet **E**ngineering **T**ask **F**orce. Diese Arbeitsgruppe hat über die Jahre ein Rahmenwerk für ein gesichertes IP-Protokoll entwickelt, das heute allgemein als IPSec bezeichnet wird.

Wichtig ist, dass IPSec selbst kein Protokoll ist, sondern nur der Standard für ein Protokoll-Rahmenwerk. IPSec besteht in der Tat aus verschiedensten Protokollen und Algorithmen für die Verschlüsselung, die Authentifizierung und das Schlüssel-Management. Diese Standards werden in den folgenden Abschnitten vorgestellt.

11.17.1.1 Sicherheit im IP-Gewand

IPSec ist (nahezu) vollständig innerhalb der Ebene 3 des OSI-Modells implementiert, also in der Vermittlungsebene (dem Network Layer). Auf Ebene 3 wird in IP-Netzwerken der Verkehr der Datenpakete auf Basis des IP-Protokolls abgewickelt.

Damit ersetzt IPSec das IP-Protokoll. Die Pakete werden unter IPSec intern anders aufgebaut als IP-Pakete. Ihr äußerer Aufbau bleibt dabei aber vollständig kompatibel zu IP. IPSec-Pakete werden deshalb weitgehend problemlos innerhalb bestehender IP-Netze transportiert. Die für den Transport der Pakete zuständigen Geräte im Netzwerk können IPSec-Pakete mit Blick aufs Äußere nicht von IP-Paketen unterscheiden.

Ausnahmen sind bestimmte Firewalls und Proxy-Server, die auch auf den Inhalt der Pakete zugreifen. Die Probleme resultieren dabei aus (teilweise funktionsbedingten) Inkompatibilitäten dieser Geräte mit dem geltenden IP-Standard. Diese Geräte müssen entsprechend an IPSec angepasst werden.

In der nächsten Generation des IP-Standards (IPv6) wird IPSec fest implementiert werden. Man kann deshalb davon ausgehen, dass IPSec auch in Zukunft der wichtigste Standard für virtuelle private Netzwerke sein wird.

11.17.2 Alternativen zu IPSec

IPSec ist ein offener Standard. Er ist unabhängig von einzelnen Herstellern und wird innerhalb der IETF unter Einbezug der interessierten Öffentlichkeit entwickelt. Die IETF steht jedermann offen und verfolgt keine wirtschaftlichen Interessen. Aus dieser offenen Gestaltung zur Zusammenführung verschiedener technischer Ansätze resultiert die breite Anerkennung von IPSec.

Dennoch gab und gibt es andere Ansätze zur Verwirklichung von VPNs. Nur die beiden wichtigsten seien hier erwähnt. Sie setzen nicht auf der Netzwerkebene wie IPSec an, sondern auf Verbindungs- und auf Anwendungsebene.

11.17.2.1 Sicherheit auf Verbindungsebene – PPTP, L2F, L2TP

Bereits auf der Verbindungsebene (Level 2 des OSI-Modells) können Tunnel gebildet werden. Microsoft und Ascend entwickelten frühzeitig das **P**oint-to-**P**oint **T**unneling **P**rotocol (PPTP). Cisco stellte ein ähnliches Protokoll mit **L**ayer **2** **F**orwarding (L2F) vor. Beide Hersteller einigten sich auf ein gemeinsames Vorgehen und in der IETF wurde daraus das **L**ayer **2** **T**unnel **P**rotocol (L2TP).

Der Vorteil dieser Protokolle gegenüber IPSec liegt vor allem darin, dass beliebige Netzwerk-Protokolle auf eine solche sichere Netzwerkverbindung aufgesetzt werden können, insbesondere NetBEUI.

Ein wesentlicher Nachteil der beschriebenen Protokolle ist die fehlende Sicherheit auf Paketebene. Außerdem wurden die Protokolle speziell für Einwahlverbindungen entwickelt.

11.17.2.2 Sicherheit auf höherer Ebene – SSL, S/MIME, PGP

Auch auf höheren Ebenen des OSI-Modells lässt sich die Kommunikation durch Verschlüsselung absichern. Bekannte Beispiele für Protokolle dieser Art sind SSL (**S**ecure **S**ocket **L**ayer) vornehmlich für Webbrowser-Verbindungen, S/MIME (**S**ecure **M**ultipurpose **I**nternet **M**ail **E**xtensions) für E-Mails und PGP (**P**retty **G**ood **P**rivacy) für E-Mails und Dateien.

Bei allen obengenannten Protokollen übernimmt eine Anwendung die Verschlüsselung der übertragenen Daten, beispielsweise der Webbrowser auf der einen Seite und der HTTP-Server auf der anderen Seite.

Ein Nachteil dieser Protokolle ist die Beschränkung auf bestimmte Anwendungen. Für verschiedene Anwendungen werden zudem in aller Regel verschiedene Schlüssel benötigt. Die Verwaltung der Konfiguration wird auf jedem einzelnen Rechner vorgenommen und kann nicht komfortabel nur auf den Gateways erfolgen, wie das bei IPSec möglich ist. Zwar sind Sicherungsprotokolle auf Anwendungsebene intelligenter, schließlich kennen sie die Bedeutung der übertragenen Daten, aber zumeist sind sie auch deutlich komplexer.

Alle diese Layer-2-Protokolle erlauben nur Ende-zu-Ende-Verbindungen, sind also (ohne Ergänzungen) ungeeignet für die Kopplung ganzer Netzwerke.

Andererseits benötigen diese Mechanismen nicht die geringsten Änderungen der Netzwerkgeräte oder der Zugangssoftware. Zudem können sie im Unterschied zu Protokollen in unteren Netzwerkebenen auch dann noch wirken, wenn die Dateninhalte schon in den Rechner gelangt sind.

11.17.2.3 Die Kombination ist möglich

Alle genannten Alternativen sind verträglich zu IPSec und daher auch parallel anzuwenden. Auf diese Weise kann das Sicherheitsniveau erhöht werden. Es ist beispielsweise möglich, sich mit einer L2TP-Verbindung ins Internet einzuwählen, einen IPSec-Tunnel zu einem Web-Server aufzubauen und dabei die HTTP-Daten zwischen Webserver und Browser im gesicherten SSL-Modus auszutauschen.

Allerdings beeinträchtigt jede zusätzlich eingesetzte Verschlüsselung den Datendurchsatz. Der Anwender wird im Einzelfall entscheiden, ob ihm die Sicherheit alleine über IPSec ausreicht oder nicht. Nur in seltenen Fällen wird eine höhere Sicherheit tatsächlich notwendig sein. Zumal sich der verwendete Grad an Sicherheit auch innerhalb von IPSec noch einstellen lässt.

11.18 Die Standards hinter IPSec

IPSec basiert auf verschiedenen Protokollen für die verschiedenen Teilfunktionen. Die Protokolle bauen aufeinander auf und ergänzen sich. Die durch dieses Konzept erreichte Modularität ist ein wichtiger Vorteil von IPSec gegenüber anderen Standards. IPSec ist nicht auf bestimmte Protokolle beschränkt, sondern kann jederzeit um zukünftige Entwicklungen ergänzt werden. Die bisher integrierten Protokolle bieten außerdem schon jetzt ein so hohes Maß an Flexibilität, dass IPSec perfekt an nahezu jedes Bedürfnis angepasst werden kann.

11.18.1 Module von IPSec und ihre Aufgaben

IPSec hat eine Reihe von Aufgaben zu erfüllen. Für jede dieser Aufgaben wurde eines oder mehrere Protokolle definiert.

- Sicherung der Authentizität der Pakete
- Verschlüsselung der Pakete
- Übermittlung und Management der Schlüssel

11.18.2 Security Associations – nummerierte Tunnel

Eine logische Verbindung (Tunnel) zwischen zwei IPSec-Geräten wird als SA (**S**ecurity **A**ssociation) bezeichnet. SAs werden selbstständig vom IPSec-Gerät verwaltet. Eine SA besteht aus drei Werten:

- **Security Parameter Index (SPI)**

  Kennziffer zur Unterscheidung mehrerer logischer Verbindungen zum selben Zielgerät mit denselben Protokollen.
- **IP-Ziel-Adresse**
- **Verwendetes Sicherheitsprotokoll**

  Kennzeichnet das bei der Verbindung eingesetzte Sicherheitsprotokoll, im Normalfall ESP.

Eine SA gilt dabei nur für eine Kommunikationsrichtung der Verbindung (simplex). Für eine vollwertige Sende- und Empfangsverbindung werden zwei SAs benötigt. Außerdem gilt eine SA nur für ein eingesetztes Protokoll.

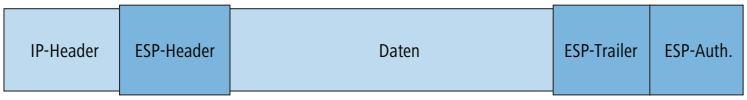
Die SAs werden im IPSec-Gerät in einer internen Datenbank verwaltet, in der auch die erweiterten Verbindungsparameter abgelegt werden. Zu diesen Parametern gehören beispielsweise die verwendeten Algorithmen und Schlüssel.

11.18.3 Verschlüsselung der Pakete – das ESP-Protokoll

Das ESP-Protokoll (**E**ncapsulating **S**ecurity **P**ayload) verschlüsselt die Pakete zum Schutz vor unbefugtem Zugriff. Diese ehemals einzige Funktion von ESP wurde in der weiteren Entwicklung des Protokolls um Möglichkeiten zum Schutz der Integrität und zur Feststellung der Authentizität erweitert. Zudem verfügt ESP auch über einen wirksamen Schutz gegen die Wiedereinspielung von Paketen.

11.18.3.1 Arbeitsweise von ESP

ESP fügt einen Header hinter den IP-Header ein, zusätzlich auch noch einen eigenen Trailer und einen Block mit ESP-Authentifizierungsdaten.



11.18.3.2 Transport- und Tunnel-Modus

ESP kann in zwei Modi verwendet werden: Im Transport-Modus und im Tunnel-Modus.

Im Transport-Modus wird der IP-Header des ursprünglichen Paketes unverändert gelassen und es werden ESP-Header, die verschlüsselten Daten und die beiden Trailer eingefügt.

Der IP-Header enthält die unveränderte IP-Adresse. Der Transport-Modus kann daher nur zwischen zwei Endpunkten verwendet werden, beispielsweise zur Fernkonfiguration eines Routers. Zur Kopplung von Netzen über das Internet kann der Transport-Modus nicht eingesetzt werden – hier wird ein neuer IP-Header mit der öffentlichen IP-Adresse des Gegenübers benötigt. In diesen Fällen kommt ESP im Tunnel-Modus zum Einsatz.

Im Tunnel-Modus wird das gesamte Paket inkl. dem ursprünglichen IP-Header am Tunnel-Eingang verschlüsselt und authentifiziert und mit ESP-Header und -Trailern versehen. Diesem neuen Paket wird ein neuer IP-Header vorangesetzt, diesmal mit der öffentlichen IP-Adresse des Empfängers am Tunnel-Ende.

11.18.3.3 Verschlüsselungs-Algorithmen

IPSec setzt als übergeordnetes Protokoll keine bestimmten Verschlüsselungs-Algorithmen voraus. In der Wahl der angewandten Verfahren sind die Hersteller von IPSec-Produkten daher frei. Üblich sind folgende Standards:

- AES – Advanced Encryption Standard

  AES ist der offizielle Verschlüsselungsstandard für die Verwendung in US-amerikanischen Regierungsbehörden und damit die wichtigste Verschlüsselungstechnik weltweit. Im Jahr 2000 entschied sich das **N**ational **I**nstitute of **S**tandards and **T**echnology (NIST) nach einem weltweiten Wettbewerb zwischen zahlreichen Verschlüsselungsalgorithmen für den Rijndael-Algorithmus (gesprochen: „Reindoll“) und erklärte ihn 2001 zum AES.

  Beim Rijndael-Algorithmus handelt es sich um ein symmetrisches Verschlüsselungsverfahren, das mit variablen Block- und Schlüssellängen arbeitet. Es wurde von den beiden belgischen Kryptografen Joan Daemen und Vincent Rijmen entwickelt und zeichnet sich durch hohe Sicherheit, hohe Flexibilität und hervorragende Effizienz aus.
- Triple-DES (auch 3-DES)

  Ist eine Weiterentwicklung des DES. Der herkömmliche DES-Algorithmus wird dreimal hintereinander angewendet. Dabei werden zwei verschiedene Schlüssel mit jeweils 56 Bits Länge eingesetzt, wobei der Schlüssel des ersten Durchlaufs beim dritten Durchlauf wiederverwendet wird. Es ergibt sich eine nominale Schlüssellänge von 168 Bit bzw. eine effektive Schlüssellänge von 112 Bit.

  Triple-DES kombiniert die ausgeklügelte Technik des DES mit einem ausreichend langen Schlüssel und gilt daher als sicher. Triple-DES arbeitet allerdings langsamer als andere Verfahren.

Die Verschlüsselung kann über die Kommandozeile angepasst werden. Eingriffe dieser Art sind in der Regel nur dann erforderlich, wenn VPN-Verbindungen zwischen Geräten unterschiedlicher Hersteller aufgebaut werden sollen.

11.18.4 Management der Schlüssel – IKE

Das **I**nternet **K**ey **E**xchange Protocol (IKE) ist ein Protokoll, das Unterprotokolle zum Aufbau der SAs (Security Associations) und für das Schlüsselmanagement beinhalten kann.

Innerhalb von IKE werden zwei Unterprotokolle verwendet: Oakley für die Authentifizierung der Partner und den Schlüsselaustausch sowie ISAKMP für die Verwaltung der SAs.

11.18.4.1 Aufbau der SA mit ISAKMP / Oakley

Jeder Aufbau einer SA erfolgt in mehreren Schritten (bei dynamischen Internet-Verbindungen erfolgen diese Schritte, nachdem die öffentliche IP-Adresse übertragen wurde):

1. Per ISAKMP sendet der Initiator an die Gegenstelle eine Meldung im Klartext mit der Aufforderung zum Aufbau einer SA und Vorschlägen (Proposals) für die Sicherheitsparameter dieser SA.
2. Die Gegenstelle antwortet mit der Annahme eines Vorschlags.
3. Beide Geräte erzeugen nun Zahlenpaare (bestehend aus öffentlichem und privatem Zahlenwert) für das Diffie-Hellman-Verfahren.
4. In zwei weiteren Mitteilungen tauschen beide Geräte ihre öffentlichen Zahlenwerte für Diffie-Hellman aus.

5. Beide Seiten erzeugen aus übertragenem Zahlenmaterial (nach dem Diffie-Hellman-Verfahren) und Shared Secret einen gemeinsamen geheimen Schlüssel, mit dem die weitere Kommunikation verschlüsselt wird. Außerdem authentifizieren sich beide Seiten gegenseitig anhand von Hash-Codes ihres gemeinsamen Shared Secrets. Die sogenannte Phase 1 des SA-Aufbaus ist damit beendet.
6. Phase 2 basiert auf der verschlüsselten und authentifizierten Verbindung, die in Phase 1 aufgebaut wurde. In Phase 2 werden die Sitzungsschlüssel für die Authentifizierung und die symmetrische Verschlüsselung des eigentlichen Datentransfers erzeugt und übertragen.

Für die Verschlüsselung des eigentlichen Datentransfers werden symmetrische Verfahren eingesetzt. Asymmetrische Verfahren (auch bekannt als Public-Key-Verschlüsselung) sind zwar sicherer, da keine geheimen Schlüssel übertragen werden müssen. Zugleich erfordern sie aber aufwändige Berechnungen und sind daher deutlich langsamer als symmetrische Verfahren. In der Praxis wird Public-Key-Verschlüsselung meist nur für den Austausch von Schlüsselmaterial eingesetzt. Die eigentliche Datenverschlüsselung erfolgt anschließend mit schnellen symmetrischen Verfahren.

11.18.4.2 Der regelmäßige Austausch neuer Schlüssel

ISAKMP sorgt während des Bestehens der SA dafür, dass regelmäßig neues Schlüsselmaterial zwischen den beiden Geräten ausgetauscht wird. Dieser Vorgang geschieht automatisch und kann über die Einstellung der Gültigkeitsdauer in LANconfig konfiguriert werden.

11.18.5 Replay-Detection

Mit der Replay-Detection beinhaltet der IPsec-Standard eine Möglichkeit, sogenannte Replay-Attacken zu erkennen. Bei einer Replay-Attacke sendet eine Station die zuvor unberechtigt protokollierten Daten an eine Gegenstelle, um eine andere als die eigene Identität vorzutäuschen.

Die Idee der Replay-Detection besteht darin, eine bestimmte Anzahl von aufeinander folgenden Paketen zu definieren (ein „Fenster" mit der Länge „n"). Da der IPSec-Standard die Pakete mit einer fortlaufenden Sequenznummer versieht kann das empfangende VPN-Gerät feststellen, ob ein Paket eine Sequenznummer aus dem zulässigen Fenster trägt. Wenn z. B. die aktuell höchste empfangene Sequenznummer 10.000 lautet bei einer Fensterbreite von 100, dann liegt die Sequenznummer 9.888 außerhalb des erlaubten Fensters.

Die Replay-Detection verwirft emfpangene Pakete dann, wenn sie entweder:

- eine Sequenznummer vor dem aktuellen Fenster tragen, in diesem Fall betrachtet die Replay-Detection diese als zu alt, oder
- eine Sequenznummer tragen, welche das VPN-Gerät zuvor schon einmal empfangen hat, in diesem Fall wertet die Replay-Detection dieses Paket als Teil einer Replay-Attacke

Bitte beachten Sie bei der Konfiguration des Fensters für die Replay-Detection folgende Aspekte:

- wenn Sie das Fenster zu groß wählen, übersieht die Replay-Detection möglicherweise eine aktuell von einem Angreifer ausgeführte Replay-Attacke
- wenn Sie das Fenster zu klein wählen, verwirft die Replay-Detection aufgrund einer während der Datenübertragung geänderten Paketreihenfolge möglicherweise rechtmäßige Pakete und erzeugt so Störungen in der VPN-Verbindung

Wägen Sie den Einsatz der Replay-Detection in Ihrem speziellen Anwendungsfall ab. Aktivieren Sie die Replay-Detection nur dann, wenn Sie die Sicherheit der VPN-Verbindung höher bewerten als die störungsfreie Datenübertragung.

11.19 IKEv2

Der VPN-Aufbau ist mit LANCOM Geräten sowohl über IKEv1 als auch über IKEv2 möglich.

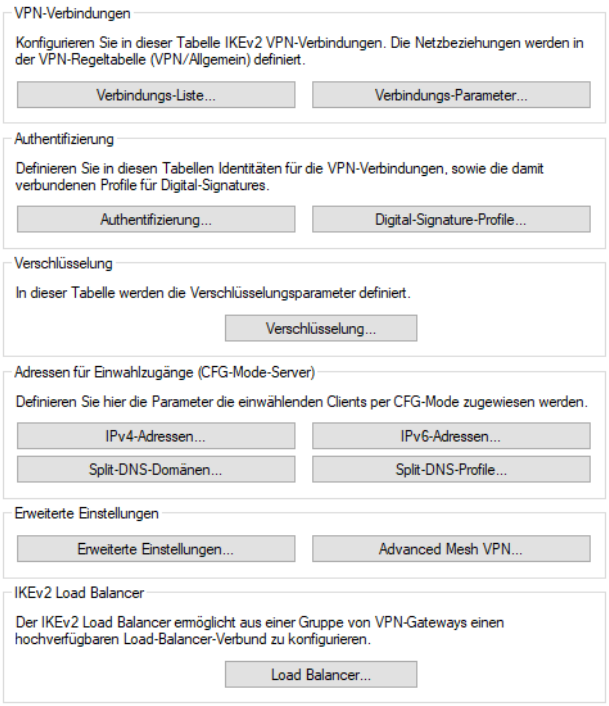
IKEv2 ermöglicht einen schnelleren und sichereren Verbindungsaufbau von VPN-Tunneln. Erstmals ist zudem die VPN-verschlüsselte Vernetzung von IPv6-basierten Standorten auch im Mischbetrieb mit IPv4 möglich.

Die Einrichtung einer VPN-Verbindung über IKEv1 ist bei manueller Konfiguration komplex und fehleranfällig, so dass viele Implementationen von IPSec inkompatibel zueinander konfiguriert sein können und damit eine VPN-Verbindung zwischen den Geräten durch fehlerhafte Konfigurationsvorgänge scheitern kann. Die IKEv2-Konfiguration im LCOS ermöglicht es dem Administrator, zuverlässig eine Übereinstimmung der Konfiguration mit der Gegenstelle einzurichten. Der Administrator hat z. B. die Möglichkeit, mehrere Diffie-Hellman-Gruppen anzuwählen. Damit erhält das Gerät über die überarbeitete Benutzeroberfläche an vielen Konfigurationsparametern empfohlene Default-Werte. Dieser vereinfachte Konfigurationsablauf mit IKEv2 beseitigt folglich Fehlerquellen, was wiederum zu einem geringeren Administrationsaufwand führt. Zusätzlich ist der VPN-Verbindungsaufbau bei IKEv2 performanter, denn IKEv2 nutzt für den Informationsaustausch bei der Aushandlung eines VPN-Tunnels nur 4 Pakete (je VPN-Partner ein `REQUEST` und ein `REPLY`), anstatt wie bei IKEv1 zwischen 6 (im „aggressive/quick mode“) und 12 (im „main mode“) Paketen. Der Sicherheitsstandard ist bei IKEv2 genauso hoch wie bei IKEv1.

Bei der Verwendung von IKEv2 werden *RFC 7296*, *RFC 7427* und im IKEv2-Client-Betrieb *RFC 5685* unterstützt.

11.19.1 IKEv2 mit LANconfig konfigurieren

IKEv2 konfigurieren Sie unter **VPN** > **IKEv2 / IPSec**.



VPN-Verbindungen

In diesem Abschnitt konfigurieren Sie die IKEv2-VPN-Verbindungen und Verbindungsparameter.

Authentifizierung

Definieren Sie in dieser Tabelle die Identitäten für die VPN-Verbindungen.

Digitale Signatur-Profile

Definieren Sie in dieser Tabelle die Authentifizierungs-Methode für die VPN-Verbindungen.

Verschlüsselung

Definieren Sie in dieser Tabelle die Verschlüsselungsparameter.

Adressen für Einwahlzugänge (CFG-Mode-Server)

Definieren Sie in diesen Tabellen die Parameter, die das Gerät den einwählenden Clients per CFG-Mode zuweist.

Zudem können Sie hier IKEv2 Split-DNS unter **Split-DNS-Domänen** und **Split-DNS-Profile** konfigurieren.

Erweiterte Einstellungen

Konfigurieren Sie in diesem Abschnitt die Einstellungen zur Authentifizierung weiterer entfernter Identitäten, die IKEv2-Rekeying-Parameter und die Präfixe für das IKEv2-Routing.

Load Balancer

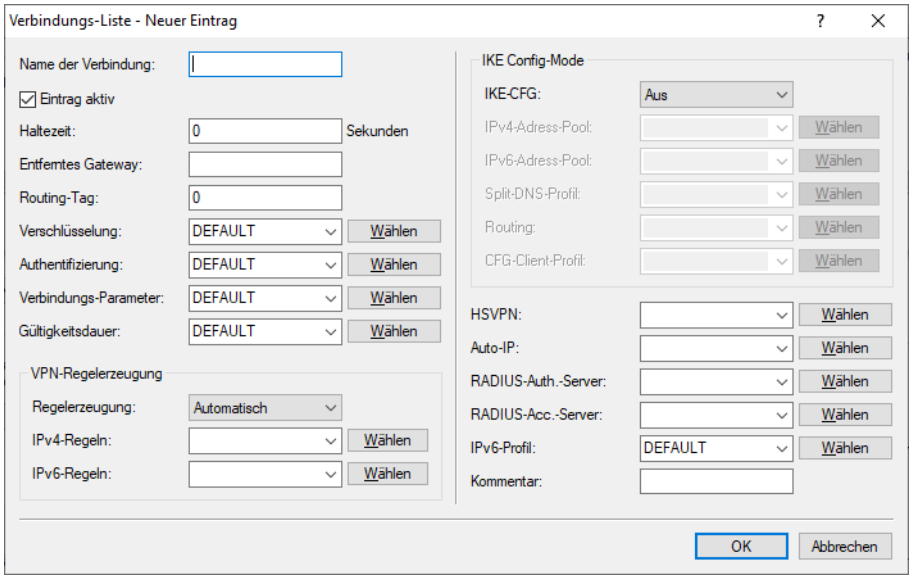
Konfigurieren Sie in diesem Abschnitt die Einstellungen zum IKEv2 Load-Balancer.

Um eine IKEv2-Verbindung zu konfigurieren, ist zunächst ein Eintrag in der **Verbindungs-Liste** erforderlich. Um den Konfigurationsaufwand gering zu halten, enthält LCOS Default-Einträge, die die meisten Parameter mit den gängigen Einstellungen für starke Verschlüsselungsalgorithmen, Dead-Peer-Detection oder Gültigkeitszeiträume vorbelegen. Lediglich die Angabe der VPN-Gegenstellen-Adresse, der Authentifizierungs-Parameter (unter **Authentifizierung**) sowie der VPN-Regeln (unter **VPN** > **Allgemein** > **Netzwerk-Regeln**) ist erforderlich.

Der Konsolenbefehl `show vpn` zeigt, ob die so eingerichtete VPN-Verbindung erfolgreich erstellt wurde.

11.19.1.1 Verbindungs-Liste

In dieser Tabelle konfigurieren Sie die IKEv2-Verbindungen zu VPN-Partnern.



Name der Verbindung

Enthält den Namen der Verbindung zur Gegenstelle.

Eintrag aktiv

Aktiviert oder deaktiviert die Verbindung zu dieser VPN-Gegenstelle.

Haltezeit

Gibt die Haltezeit in Sekunden an, die das Gerät eine Verbindung ohne Datenfluss aufrecht erhält.

Entferntes Gateway

Enthält die Adresse (IPv4- oder IPv6-Adresse, FQDN) des VPN-Partners. Wird der Wert leer gelassen, so findet keine zusätzliche Prüfung der IP-Adresse der Gegenseite statt. Dies ist erforderlich, wenn die Gegenseite beispielsweise eine dynamische IP-Adresse besitzt.

Über ein Suffix können Sie bei Angabe eines FQDN die DNS-Auflösung steuern. Siehe hierzu *Konfigurationsmöglichkeit für IPv4/IPv6-Auflösung bei DNS-Auflösungen* auf Seite 172.

Routing-Tag

Enthält das Routing-Tag für diese VPN-Verbindung.

Verschlüsselung

Bestimmt die Verschlüsselung der VPN-Verbindung. Der entsprechende Eintrag steht in der Tabelle **Verschlüsselung**.

Authentifizierung

Bestimmt die Authentifizierung der VPN-Verbindung. Der entsprechende Eintrag steht in der Tabelle **Authentifizierung**.

Verbindungs-Parameter

Bestimmt die allgemeinen Parameter der VPN-Verbindung. Der entsprechende Eintrag steht in der Tabelle **Verbindungs-Parameter**.

Gültigkeitsdauer

Bestimmt die Lebensdauer der Schlüssel einer VPN-Verbindung. Der entsprechende Eintrag steht in der Tabelle **VPN** > **IKEv2/IPSec** > **Erweiterte Einstellungen** > **Gültigkeitsdauer**.

VPN-Regelerzeugung

Regelerzeugung

Bestimmt, wie VPN-Regeln erstellt werden.

Mögliche Werte:

Automatisch

Als Quellnetz wird das lokale Intranet eingesetzt (privater IP-Adressbereich, zu dem das lokale VPN-Gateway selbst gehört). Als Zielnetze dienen für die automatisch erstellten VPN-Regeln die Netzbereiche aus der IP-Routing-Tabelle, für die als Router ein entferntes VPN-Gateway eingetragen ist.

Werden zwei einfache lokale Netzwerke gekoppelt, ist es der VPN-Automatik möglich, aus dem IP-Adressbereich des eigenen LANs und dem Eintrag des entfernten LAN in der IP-Routing-Tabelle die erforderliche Netzbeziehung ableiten.

Manuell

Die Regelerstellung für die Netzbeziehungen erfolgt wie die manuelle Regel-Definition für IPv4 oder IPv6.

IPv4-Regeln

Gibt an, welche IPv4-Regeln für diese VPN-Verbindung gelten sollen.

Die IPv4-Regeln stehen in der Tabelle **VPN** > **Allgemein** > **Netzwerk-Regeln**.

IPv6-Regeln

Gibt an, welche IPv6-Regeln für diese VPN-Verbindung gelten sollen.

Die IPv6-Regeln stehen in der Tabelle **VPN** > **Allgemein** > **Netzwerk-Regeln**.

IKE-Config-Mode

IKE-CFG

Bestimmt den IKEv2-Config-Modus dieser Verbindung für RAS-Einwahlen.

Mögliche Werte sind:

- Aus: IKEv2-Config-Modus deaktiviert
- Server: Der Router verteilt Konfigurationsparameter (z. B. Adressen oder DNS-Server) an VPN-Clients Die zu vergebenden Parameter werden im IPv4- bzw. IPv6-Adresspool konfiguriert.
- Client: Der Router fragt beim Server Konfigurationsparameter (z. B. Adressen oder DNS-Server) an.

IPv4-Adress-Pool

IPv4-Adressen und DNS-Server für Einwahlzugänge im IKE-CFG-Modus Server.

IPv6-Adress-Pool

IPv6-Adressen und DNS-Server für Einwahlzugänge im IKE-CFG-Modus Server.

Split-DNS-Profil

Name des Split-DNS-Profils. Das Split-DNS-Profil ist nur aktiv, falls **IKE-CFG** den Wert **Server** hat.

Routing

Gibt die Routen an, die der Gegenseite dynamisch per IKE-CFG Mode übermittelt werden sollen. Diese Funktion ist nur im IKEv2-CFG Mode für Client und Server möglich.

Die Routen für IPv4- und IPv6-Verbindungen stehen in den Tabellen **VPN** > **IKEv2/IPSec** > **Erweiterte Einstellungen** > **IPv4-Routing / IPv6-Routing**.

CFG-Client-Profil

Wählen Sie ein CFG-Client-Profil aus, welches Sie unter *CFG-Client-Profil* auf Seite 891 angelegt haben. Dieses Profil bestimmt, ob das Gerät in der Rolle CFG-Mode Client eine Adresse beim CFG-Mode-Server anfragen soll.

HSVPN

High Scalability VPN (HSVPN)

In SD-WAN-Szenarien, bei denen Filialen Verbindungen zu einer oder mehreren Zentralen aufbauen, sind in der Regel mehrere logische Netze vorhanden, die sicher über VLAN und ARF voneinander getrennt werden müssen, z. B. Zahlungsverkehr, Warenwirtschaft oder Hotspot. Diese lokalen Netze wurden bisher entweder als „gestapelte" Tunnel, d. h. PPTP oder L2TP innerhalb eines VPN-Tunnels oder als einzelne IPSec-VPN-Tunnel mit der Zentrale verbunden. Diese Architekturen skalieren aber bei einer großen Anzahl von Filialen und vielen ARF-Netzen nicht besonders gut. Beispielsweise ergibt sich bei 1.000 Filialen und 8 ARF-Netzen eine Anzahl

von 8.000 Tunneln bei einer Architektur mit einem Tunnel pro ARF-Netz. Gestapelte Tunnel haben aufgrund des Protokoll-Overheads Performance- und MTU-Einschränkungen.

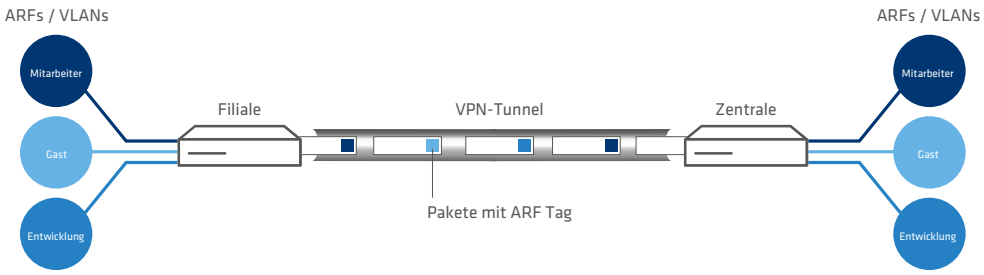


Abbildung 6: LANCOM HSVPN-Szenario für SD-WAN

Die neue Architektur LANCOM HSVPN („LANCOM High Scalability VPN“) löst diese Herausforderungen. Bei HSVPN werden Pakete aus ARF-Netzen innerhalb eines IPSec-Tunnels mit einem ARF-Tag markiert und ohne Overhead im VPN-Tunnel transportiert. Diese Tagging-Methode auf Layer 2 entspricht dem VLAN-Ansatz für Layer 3 und bietet somit das gleiche Sicherheitsniveau wie VLAN. Dadurch, das insgesamt weniger Tunnel benötigt werden, verbessern sich die Tunnelaufbauzeiten insbesondere im Fail-over-Fall. Auch bzgl. MTU gibt es keine großen Einschränkungen.

Die folgenden groben Konfigurationsschritte sind dafür notwendig:

1. Anlegen der einzelnen ARF-Netze
2. Anlegen eines IKEv2-Tunnels
3. Im HSVPN-Konfigurationsprofil des IKEv2-Tunnels (*HSVPN-Profile* auf Seite 887) werden die erlaubten ARF-Netze als Tag-Liste konfiguriert
4. Für die gewünschten ARF-Netze müssen entsprechende Routen auf den HSVPN-Tunnel angelegt werden

Grundsätzlich unterstützt LANCOM HSVPN zwei Betriebsarten:

- Betrieb als klassisches Site-to-Site VPN
- Betrieb im CFG-Mode mit IKEv2-Routing, wobei neben den Routen auch die zugehörigen Routing-Tags übertragen werden

Aktuelle Einschränkungen:

- Multicast Routing über HSVPN wird derzeit nicht unterstützt. Hierzu ist ein separater VPN-Tunnel für Multicast erforderlich.
- OSPF über HSVPN wird nicht unterstützt

Definieren Sie hier den Namen des HSVPN-Profils aus der Tabelle *HSVPN-Profile* auf Seite 887.

Auto-IP

Mittels des Auto-IP-Parameters kann eine VPN-Zentrale einer VPN-Filiale die IP-Adresse für das Messziel der *Dynamic Path Selection* übermitteln. Dazu wird auf der Zentrale der Parameter Auto-IP konfiguriert. Auf der Filiale muss dann als (IPv4-)Messziel 0.0.0.0 bzw. als IPv6-Messziel :: eingetragen werden, damit die Filiale das Messziel automatisch von der Zentrale übernimmt.

Verweist auf das entsprechende Auto-IP-Profil, welches Sie unter *IKEv2-Auto-IP-Profil* auf Seite 893 einrichten.

RADIUS-Auth.-Server

Bestimmt den RADIUS-Server für die Autorisierung des VPN-Peers. Den RADIUS-Server für IKEv2 konfigurieren Sie unter **VPN** > **IKEv2/IPSec** unter **Erweiterte Einstellungen**.

RADIUS-Acc.-Server

Bestimmt den RADIUS-Server für das Accounting des VPN-Peers. Den RADIUS-Server für IKEv2 konfigurieren Sie unter **VPN** > **IKEv2/IPSec** unter **Erweiterte Einstellungen**.

IPv6-Profil

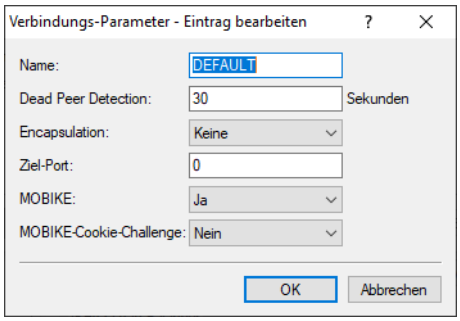
Dieser Eintrag gibt den Namen des IPv6-WAN-Profils an. Ein leerer Eintrag schaltet IPv6 für dieses Interface ab. Die IPv6-Gegenstellen konfigurieren Sie unter **IPv6** > **Allgemein** > **IPv6-Schnittstellen** > **WAN-Profile**.

Kommentar

Vergeben Sie diesem Eintrag einen aussagekräftigen Kommentar.

11.19.1.2 Verbindungs-Parameter

In dieser Tabelle definieren Sie die Parameter von IKEv2-VPN-Verbindungen, die nicht Bestandteil der SA-Verhandlung sind. Es existiert ein Standardeintrag „DEFAULT" mit gängigen Einstellungen.



Name

Enthält den eindeutigen Namen dieses Eintrages. Diesen Namen ordnen Sie den Verbindungen in der **Verbindungs-Liste** im Feld „Verbindungs-Parameter" zu.

Dead Peer Detection

Enthält die Zeit in Sekunden, nach der das Gerät die Verbindung beendet, wenn es in der Zwischenzeit den entfernten Peer nicht mehr erreicht.

Encapsulation

In manchen Szenarien kann der normale VPN-Port 500 nicht sinnvoll verwendet werden, z. B., wenn Firewalls im Weg sind. Hier können sie SSL bzw. UDP einstellen. In Verbindung mit **Ziel-Port** kann ein beliebiger Ziel-Port konfiguriert werden. Der Aufbau des IKEv2-Tunnels wird bei UDP mit Port 4500 bzw. mit dem in **Ziel-Port** eingestellten Port durchgeführt. Sollte dort 500 eingestellt sein, dann wird dies ignoriert und stattdessen der Port 4500 verwendet. Bei SSL wir der Aufbau des Tunnels mit Port 443 durchgeführt bzw. mit dem in Destination-Port eingestellten Port. Sollte dort 500 oder 4500 eingestellt sein, dann wird dies ignoriert und stattdessen der Port 443 verwendet. In der Einstellung „Keine" wird der Port 500 genommen und die Einstellung in **Ziel-Port** ignoriert.

Den konfigurierbaren Port kann man für Szenarien verwenden, wo ein LANCOM Router selbst schon auf den Standard-Ports VPN-Tunnel annimmt. Durch eine Portforwarding-Regel könnten somit diese Ports auf beliebige Ziele weitergeleitet werden.

Ziel-Port

Hier können Sie den Ziel-Port definieren, der abhängig von der Einstellung in **Encapsulation** genommen wird. Bei einer von 500 abweichenden Einstellung wird automatisch eine UDP-Encapsulation durchgeführt.

MOBIKE

Definiert, ob MOBIKE nach *RFC 4555* unterstützt werden soll.

MOBIKE nach RFC 4555 für IKEv2 bietet mobilen Clients die Möglichkeit, zwischen verschiedenen Netzen zu roamen und dabei den VPN-Tunnel nicht abbauen zu müssen. Ein VPN-Client kann beispielsweise nahtlos vom Mobilfunk ins WLAN roamen und dabei wird seine externe IP-Adresse auf dem VPN-Gateway durch eine IKEv2-Update-Nachricht aktualisiert. Der Vorteil ist, dass der VPN-Tunnel bzw. die Security Associations (SAs) nicht abgebaut und wieder neu aufgebaut werden muss.

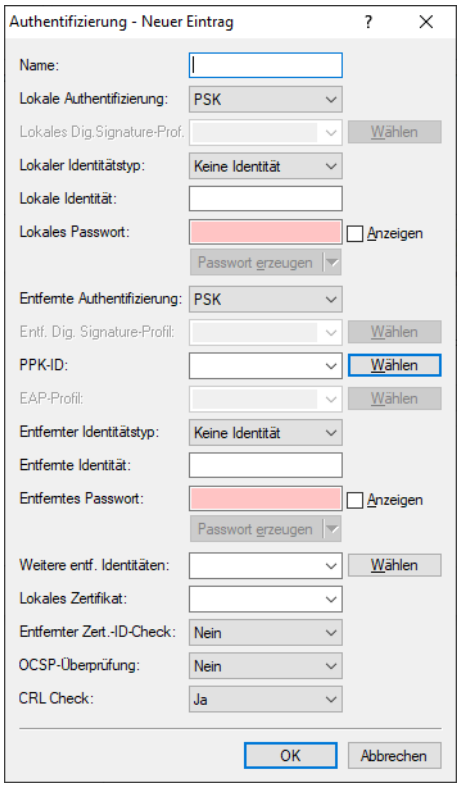
MOBIKE wird nur als Responder-Rolle unterstützt, d. h. wenn VPN-Clients Verbindungen zum LANCOM VPN-Router aufbauen. Der Aufbau von VPN-Tunneln mit MOBIKE-Erweiterung wird nicht unterstützt.

MOBIKE-Cookie-Challenge

Definiert, ob das Gerät eine Cookie-Challenge senden soll um festzustellen, ob der VPN-Client auch unter der neuen Adresse tatsächlich Pakete empfangen kann („Return Routability Check“).

11.19.1.3 Authentifizierung

In dieser Tabelle konfigurieren Sie die Parameter für die IKEv2-Authentifizierung der lokalen und mindestens einer entfernten Identität.



Name

Enthält den eindeutigen Namen dieses Eintrages. Diesen Namen ordnen Sie den Verbindungen in der **Verbindungs-Liste** im Feld „Authentifizierung“ zu.

Lokale Authentifizierung

Legt die Authentifizierungsmethode für die lokale Identität fest. Mögliche Werte sind:

- PSK: Pre-Shared Key
- RSA-Signature: Verwendung von digitalen Zertifikaten mit privatem RSA-Schlüssel und RSA-Signaturschema

- Digitale-Signatur: Verwendung von konfigurierbaren Authentifizierungsmethoden mit digitalen Zertifikaten nach RFC 7427. Dieses Verfahren ist ein erweiterbares und flexibles Authentifizierungsverfahren, bei dem z. B. Padding- und Hash-Verfahren frei konfiguriert werden können.
- ECDSA-256, ECDSA-384, ECDSA-521: Verwendung von Elliptic Curve Digital Signature Algorithm (ECDSA) nach RFC 4754 zur Authentifizierung.

  ECDSA-Signaturen sind grundsätzlich kleiner als RSA-Signaturen bei vergleichbarer kryptografischer Stärke. ECDSA-Schlüssel und Zertifikate sind in Bezug auf Dateigröße ebenso deutlich kleiner als RSA-basierte Schlüssel und Zertifikate. Des Weiteren sind ECDSA-Operationen auf vielen Geräten grundsätzlich schneller in der Berechnung. Die folgenden Verfahren werden bei IKEv2 unterstützt.

  - ECDSA with SHA-256 on the P-256 curve
  - ECDSA with SHA-384 on the P-384 curve
  - ECDSA with SHA-512 on the P-521 curve

  Bei Verwendung von OpenSSL müssen die folgenden vordefinierten Kurven als Parameter für ECDSA bei IKEv2 verwendet werden:

  - prime256v1 bei ECDSA-256
  - secp384r1bei ECDSA-384
  - secp521r1 bei ECDSA-512

  Folgende Einschränkungen gelten bei der Verwendung von ECDSA:

  - ECDSA-basierte Zertifikate können derzeit nicht von der LCOS-eigenen CA erzeugt werden. Ebenso ist der automatische Zertifikatsbezug per SCEP nicht möglich. ECDSA-Zertifikate müssen mit einer externen Anwendung, wie z. B. OpenSSL oder mit Hilfe von XCA erzeugt werden und anschließend ins Gerät geladen werden.

Das Gerät verwendet die konfigurierte Authentifizierungsmethode beim Verbindungsaufbau mit der Gegenstelle. Die Methode muss mit der entsprechenden Konfiguration auf der Gegenseite übereinstimmen.

Dabei es möglich, unterschiedliche Authentifizierungsverfahren für die lokale und entfernte Authentifizierung zu verwenden. Beispielsweise kann sich die Zentrale per RSA-Signature ausweisen, während Filialen oder Clients PSK zur Authentifizierung verwenden.

Lokales Digitales Signatur-Profil

Profilname des verwendeten lokalen Digital-Signatur-Profils.

Lokaler Identitätstyp

Definiert den ID-Typ der lokalen Identität an. Entsprechend interpretiert das Gerät die Eingabe unter „Lokale Identität“. Mögliche Angaben sind:

- Keine Identität: Es wird keine Identität übertragen.
- IPv4-Adresse: Das Gerät verwendet eine IPv4-Adresse als lokale ID.
- IPv6-Adresse: Das Gerät verwendet eine IPv6-Adresse als lokale ID.
- Domänen-Name (FQDN): Das Gerät verwendet einen Domänen-Namen als lokale ID.
- E-Mail-Adresse (FQUN): Das Gerät verwendet eine E-Mail-Adresse als lokale ID.
- ASN.1-Distinguished-Name: Das Gerät verwendet einen Distinguished Name als lokale ID (z. B. „CN=client01.example.com,O=test,C=DE“
- Key-ID (Gruppenname): Das Gerät verwendet den Gruppennamen als lokale ID. Den Gruppennamen können sie beliebig definieren.

Lokale Identität

Enthält die lokale Identität. Die Bedeutung dieser Eingabe ist abhängig von der Einstellung unter „Lokaler Identitätstyp“.

Lokales Passwort

Enthält das Passwort der lokalen Identität. Mit diesem Passwort authentifiziert sich das Gerät bei der Gegenseite. Das lokale und entfernte Passwort kann identisch oder unterschiedlich sein.

Entfernte Authentifizierung

Legt die Authentifizierungsmethode für die entfernte Identität fest. Mögliche Werte sind:

- PSK: Pre-Shared Key
- RSA-Signature: Verwendung von digitalen Zertifikaten mit privatem RSA-Schlüssel und RSA-Signaturschema
- Digitale-Signatur: Verwendung von konfigurierbaren Authentifizierungsmethoden mit digitalen Zertifikaten nach RFC 7427. Dieses Verfahren ist ein erweiterbares und flexibles Authentifizierungsverfahren, bei dem z. B. Padding- und Hash-Verfahren frei konfiguriert werden können.
- ECDSA-256, ECDSA-384, ECDSA-521: Verwendung von Elliptic Curve Digital Signature Algorithm (ECDSA) nach RFC 4754 zur Authentifizierung.

  ECDSA-Signaturen sind grundsätzlich kleiner als RSA-Signaturen bei vergleichbarer kryptografischer Stärke. ECDSA-Schlüssel und Zertifikate sind in Bezug auf Dateigröße ebenso deutlich kleiner als RSA-basierte Schlüssel und Zertifikate. Des Weiteren sind ECDSA-Operationen auf vielen Geräten grundsätzlich schneller in der Berechnung. Die folgenden Verfahren werden bei IKEv2 unterstützt.

  - ECDSA with SHA-256 on the P-256 curve
  - ECDSA with SHA-384 on the P-384 curve
  - ECDSA with SHA-512 on the P-521 curve

  Bei Verwendung von OpenSSL müssen die folgenden vordefinierten Kurven als Parameter für ECDSA bei IKEv2 verwendet werden:

  - prime256v1 bei ECDSA-256
  - secp384r1bei ECDSA-384
  - secp521r1 bei ECDSA-512

  Folgende Einschränkungen gelten bei der Verwendung von ECDSA:

  - ECDSA-basierte Zertifikate können derzeit nicht von der LCOS-eigenen CA erzeugt werden. Ebenso ist der automatische Zertifikatsbezug per SCEP nicht möglich. ECDSA-Zertifikate müssen mit einer externen Anwendung, wie z. B. OpenSSL oder mit Hilfe von XCA erzeugt werden und anschließend ins Gerät geladen werden.

- EAP: Extensible Authentication Protocol

  EAP ist kein festes Authentifizierungsverfahren, sondern es bietet einen Rahmen für beliebige Authentifizierungsverfahren, wie beispielsweise TLS (Authentifizierung per Zertifikat) oder MSCHAP (Authentifizierung per Benutzername / Passwort).

  Die EAP-Authentifizierung übernimmt dabei ein externer RADIUS-Server wie z. B. der LANCOM RADIUS Server, FreeRADIUS oder Microsoft Network Policy Server (NPS). Das VPN-Gateway übernimmt dabei nur die Vermittlerrolle zwischen Client und RADIUS-Server. Das VPN-Gateway muss sich gegenüber dem Client mit einem gültigen Zertifikat per RSA-Signature-Verfahren authentifizieren. Der RADIUS-Server muss ebenso ein gültiges Zertifikat vorweisen. Die notwendigen Zertifikate können beispielsweise mit der LANCOM SCEP CA im Router erstellt werden. Nach der Erstellung müssen die jeweiligen Zertifikatsconatiner in das VPN-Gateway sowie in den RADIUS-Server importiert werden.

  Die Nutzung des Features IKEv2 EAP-Authentifizierung benötigt auf LANCOM Routern die VPN-25 Option oder einen Router mit 25 oder mehr VPN-Tunneln. Ob der Router IKEv2 EAP unterstützt, kann im LCOS Status-Menü unter **Status** > **Software-Info** > **IKEv2-EAP-License** überprüft werden.

  Siehe auch *EAP und IEEE 802.1X* auf Seite 962.

Das Gerät verwendet die konfigurierte Authentifizierungsmethode beim Verbindungsaufbau mit der Gegenstelle. Die Methode muss mit der entsprechenden Konfiguration auf der Gegenseite übereinstimmen.

Dabei es möglich, unterschiedliche Authentifizierungsverfahren für die lokale und entfernte Authentifizierung zu verwenden. Beispielsweise kann sich die Zentrale per RSA-Signature ausweisen, während Filialen oder Clients PSK zur Authentifizierung verwenden.

Entferntes Digitales Signatur-Profil

Profilname des entfernten Digital-Signatur-Profils.

PPK-ID

Geben Sie hier den Namen der PPK-ID (Post-quantum Preshared Keys nach *RFC 8784*) aus der Tabelle der *PPKs (Post-quantum Preshared Keys)* auf Seite 883 ein.

EAP-Profil

Geben Sie ein EAP-Profil an, wenn als Methode für die **Entfernte Authentifizierung** EAP ausgewählt wurde. Die EAP-Profile werden unter *EAP-Profile* auf Seite 884 definiert.

Entfernter Identitätstyp

Zeigt den ID-Typ an, den das Gerät von der entfernten Identität erwartet. Entsprechend interpretiert das Gerät die Eingabe unter „Entfernte Identität". Mögliche Angaben sind:

- Keine Identität: Das Gerät akzeptiert jede ID des entfernten Gerätes. Eine Angabe im Feld „Entfernte Identität" ignoriert das Gerät.
- IPv4-Adresse: Das Gerät erwartet eine IPv4-Adresse als entfernte ID.
- IPv6-Adresse: Das Gerät erwartet eine IPv6-Adresse als entfernte ID.
- Domänen-Name (FQDN): Das Gerät erwartet einen Domänen-Namen als entfernte ID.
- E-Mail-Adresse (FQUN): Das Gerät erwartet eine E-Mail-Adresse als entfernte ID.
- ASN.1-Distinguished-Name: Das Gerät erwartet einen Distinguished Name als entfernte ID (z. B. „CN=client01.example.com,O=test,C=DE").
- Key-ID (Gruppenname): Das Gerät erwartet den Gruppennamen als entfernte ID.

Entfernte Identität

Enthält die entfernte Identität. Die Bedeutung dieser Eingabe ist abhängig von der Einstellung unter „Entfernter Identitätstyp".

Entferntes Passwort

Enthält das Passwort der entfernten Identität.

Weitere entf. Identitäten

Für redundante VPN-Szenarien ist die Angabe von alternativen entfernten Identitäten möglich.

Konfigurieren Sie hier weitere entfernte Identitäten aus der Tabelle **Erweiterte Einstellungen** > **Identitäten-Liste**.

Lokales Zertifikat

Geben Sie das lokale VPN-Zertifikat an, das das Gerät bei ausgehenden Verbindungen verwendet.

Die entsprechenden VPN-Zertifikate „VPN1" bis „VPN9" konfigurieren Sie unter **Zertifikate** > **SCEP-Client** in der **Zertifikat-Tabelle**.

Entfernte Zertifikatsprüfung

Diese Option bestimmt, ob das Gerät prüft, ob die angegebene entfernte Identität im empfangenen Zertifikat enthalten ist.

OCSP-Überprüfung

Mit dieser Einstellung aktivieren Sie die Echtzeitüberprüfung eines X.509-Zertifikats via OCSP, welche den Gültigkeitsstatus des Zertifikates der Gegenstelle abfragt. Um die OCSP-Prüfung für einzelne VPN-Verbindungen

zu verwenden, müssen Sie zunächst den globalen OCSP-Client für VPN-Verbindungen aktivieren und anschließend Profillisten gültiger Zertifizierungsstellen anlegen, bei denen das Gerät die Echtzeitprüfung durchführt.

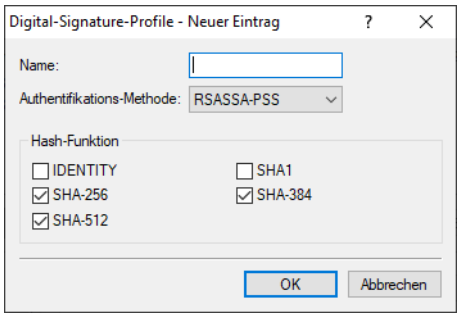
CRL Check

Mit dieser Einstellung aktivieren Sie die Überprüfung eines X.509-Zertifikats via Zertifikatssperrlisten (Certificate Revocation List, CRL), welche den Gültigkeitsstatus des Zertifikats der Gegenstelle abfragt.

Schalten Sie diese Überprüfung nur ab, wenn Sie die Überprüfung auf einem anderen Weg durchführen, z. B. über OCSP.

11.19.1.4 Digitale Signatur-Profile

In dieser Tabelle konfigurieren Sie die Parameter für die IKEv2-Authentifizierung.



Name

Enthält den eindeutigen Namen dieses Eintrages. Diesen Namen können Sie an drei Stellen zuweisen. Im Bereich **Authentifizierung** in den Feldern **Lokales Dig.Signature-Prof.** und **Entf. Dig. Signature-Profil** sowie unter **Erweiterte Einstellungen** > **Authentifizierung** > **Identitäten** > **Entf. Dig. Signature-Profil**.

Authentifizierungs-Methode

Legt die Authentifizierungsmethode für die digitale Signatur fest. Mögliche Werte sind:

- RSASSA-PSS: RSA mit verbessertem probabilistischem Signatur-Schema nach Version 2.1 von PKCS #1 (probabilistic signature scheme with appendix)
- RSASSA-PKCS1-v1_5: RSA nach der älteren Version des Signature-Schemas nach Version 1.5 von PKCS #1 (signature scheme with appendix)
- ECDSA: Elliptic Curve Digital Signature Algorithm (ECDSA)
- EdDSA25519: Edwards Curve 2551 (EdDSA25519) nach *RFC 8420*
- EdDSA448: Edwards Curve 448 (EdDSA448) nach *RFC 8420*

Bei Auswahl von RSASSA-PKCS1-v1_5 wird geprüft, ob die Gegenstelle auch das bessere Verfahren RSASSA-PSS unterstützt und ggfs. auf dieses gewechselt. Falls RSASSA-PSS ausgewählt ist, dann ist ein Rückfall auf das ältere RSASSA-PKCS1-v1_5 nicht vorgesehen.

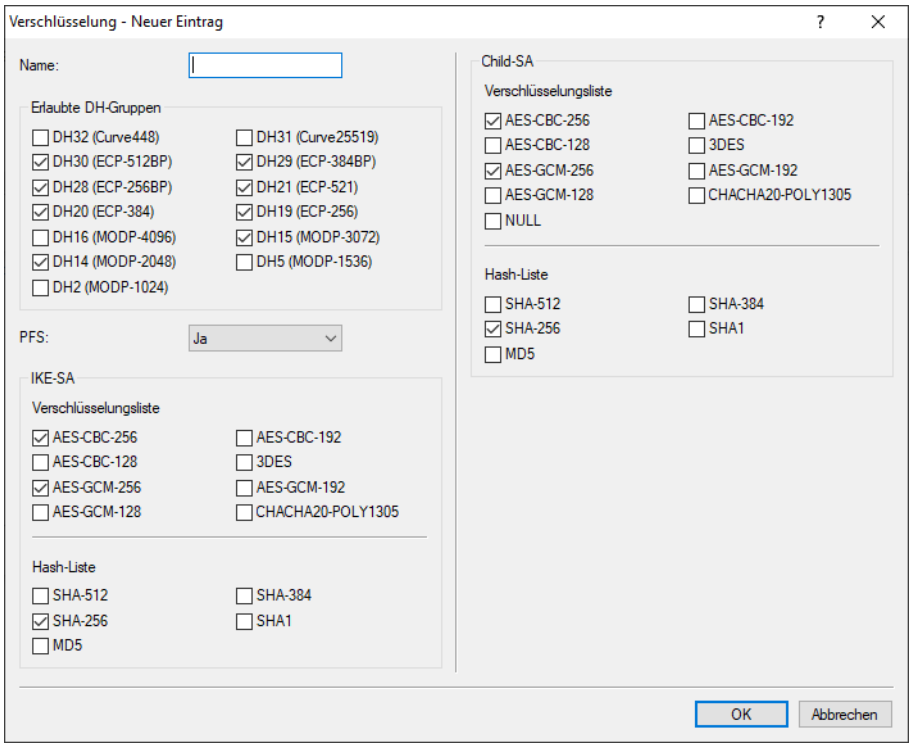
Legen Sie zudem die zu verwendenden Secure Hash Algorithmen (SHA) fest.

11.19.1.5 Verschlüsselung

In dieser Tabelle konfigurieren Sie die Verschlüsselungsparameter. Es existiert ein Standardeintrag „DEFAULT“ mit gängigen Einstellungen.

Eine Mehrfachauswahl der Parameter ist möglich. Diese Parameterlisten propagiert das Gerät im IKE-Protokoll und in CHILD-SAs. Beide VPN-Partner verständigen sich anschließend auf einen Algorithmus der propagierten Listen. Beim Aufbau der ersten IKE-SA einigen sich die VPN-Partner auf die höchste der gegenseitig propagierten DH-Gruppen. Diese DH-Gruppe nutzen die VPN-Partner, wenn sie die IKE-SAs erneuern oder wenn sie CHILD-SAs erzeugen oder erneuern (bei aktiviertem PFS).

Die Verbindung zwischen den VPN-Partnern kommt zustande, wenn es in der Menge der konfigurierten Verschlüsselungsparameter Gemeinsamkeiten gibt. Stimmen die Parameter in keinem Fall überein, findet keine Verbindung statt.



Name

Enthält den eindeutigen Namen dieses Eintrages. Diesen Namen ordnen Sie den Verbindungen in der **Verbindungs-Liste** im Feld „Verschlüsselung“ zu.

Erlaubte DH-Gruppen

Enthält die Auswahl der Diffie-Hellman-Gruppen, auf deren Basis die VPN-Partner einen Schlüssel für den Datenaustausch erstellen. Je höher die gewählte DH-Gruppe, desto komplexer ist der erzeugte Schlüssel. Aktuell werden folgende Gruppen unterstützt:

- DH-2 (1024-Bit Modulus)
- DH-5 (1536-Bit Modulus)
- DH-14 (2048-Bit Modulus)
- DH-15 (3072-Bit Modulus)
- DH-16 (4096-Bit Modulus)
- DH-19 (256-bit random ECP group)
- DH-20 (384-bit random ECP group)
- DH-21 (521-bit random ECP group)
- DH-28 (brainpoolP256r1)
- DH-29 (brainpoolP384r1)
- DH-30 (brainpoolP512r1)

- DH-31 (Curve25519)
- DH-32 (Curve448)

PFS

Gibt an, ob Perfect Forward Secrecy (PFS) aktiviert ist.

Verschlüsselungsliste

Gibt an, welche Verschlüsselungsalgorithmen aktiviert sind. Folgende Verschlüsselungsalgorithmen stehen zur Auswahl:

- AES-CBC-128
- AES-CBC-192
- AES-CBC-256
- 3DES
- AES-GCM-128
- AES-GCM-192
- AES-GCM-256
- Chacha20-Poly1305

  ChaCha20 Datenstromverschlüsselung zusammen mit dem Poly1305 Authentifikator, siehe *RFC 7634*.

  Bitte beachten Sie, dass ChaCha20-Poly1305 derzeit nicht durch Hardware beschleunigt wird und daher nicht für VPN-Szenarien empfohlen wird, in denen eine hohe Verschlüsselungsleistung benötigt wird.
- NULL

  Hier erfolgt keine Verschlüsselung der Datenpakete mehr. Diese Funktion wird nur in speziellen Szenarien benötigt und generell nicht empfohlen.

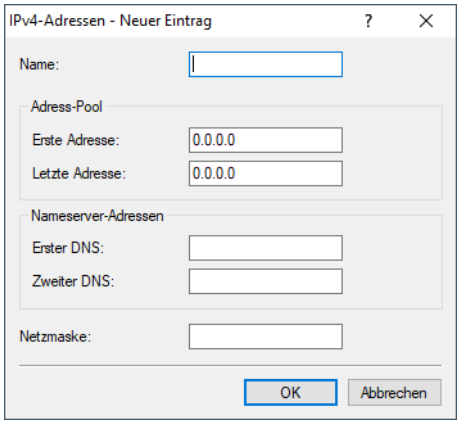
Hash-Liste

Gibt an, welche Hash-Algorithmen aktiviert sind. Folgende Hash-Algorithmen stehen zur Auswahl:

- SHA1
- SHA-256
- SHA-384
- SHA-512
- MD5

11.19.1.6 IPv4-Adressen

In dieser Tabelle konfigurieren Sie die IPv4-Parameter, die das Gerät den einwählenden VPN-Clients per CFG-Mode zuweist.



Name

Enthält den Namen des IPv4-Adresspools.

Adress-Pool

Erste Adresse

Geben Sie hier die erste IPv4-Adresse des Adressbereiches ein, den Sie den VPN-Clients zur Verfügung stellen wollen.

Letzte Adresse

Geben Sie hier die letzte IPv4-Adresse des Adressbereiches ein, den Sie den VPN-Clients zur Verfügung stellen wollen.

Der hier definierte Adress-Pool sollte außerhalb der definierten Netze liegen. Andernfalls müssen Sie Proxy-ARP aktivieren.

Nameserver-Adressen

Erster DNS

Enthält die erste DNS-Adresse.

Zweiter DNS

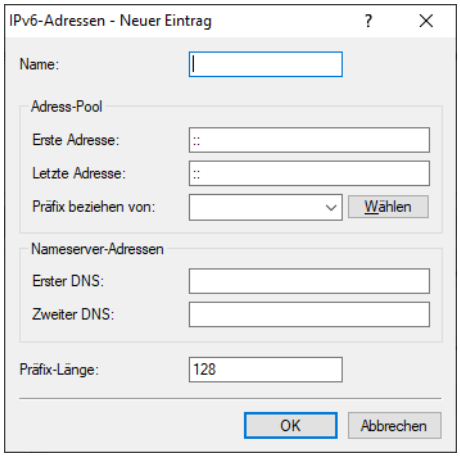
Enthält die zweite DNS-Adresse.

Netzmaske

Optionale Netzmaske, die für die verhandelte IP-Adresse mitgeschickt wird.

11.19.1.7 IPv6-Adressen

In dieser Tabelle konfigurieren Sie die IPv6-Parameter, die das Gerät den einwählenden VPN-Clients per CFG-Mode zuweist.



Name

Enthält den Namen des IPv6-Adresspools.

Adress-Pool

Erste Adresse

Geben Sie hier die erste IPv6-Adresse des Adressbereiches ein, den Sie den VPN-Clients zur Verfügung stellen wollen.

Letzte Adresse

Geben Sie hier die letzte IPv6-Adresse des Adressbereiches ein, den Sie den VPN-Clients zur Verfügung stellen wollen.

Präfix beziehen von

Mit diesem Parameter können Sie den VPN-Clients Adressen aus dem Präfix zuteilen, das der Router vom WAN-Interface per DHCPv6-Präfix-Delegation vom Provider bezogen hat. Wählen Sie hier das entsprechende WAN-Interface aus. Hat der Provider beispielsweise das Präfix „2001:db8::/64“ zugewiesen, dann können Sie beim Parameter **Erste Adresse** den Wert „::1“ und bei **Letzte Adresse** den Wert „::9“ eingeben. Zusammen mit dem vom Provider delegierten Präfix „2001:db8::/64“ erhalten Clients dann Adressen aus dem Pool von „2001:db8::1“ bis „2001:db8::9“. Ist das Provider-Präfix größer als „/64“, z. B. „/48“ oder „/56“, so müssen Sie das Subnetting für das logische Netzwerk in den Adressen berücksichtigen.

Beispiel:

- Zugewiesenes Provider-Präfix: 2001:db8:abcd:aa::/56
- /64 als Präfix des logischen Netzwerks (Subnetzt-ID 1): 2001:db8:abcd:aa01::/64
- Erste Adresse: 0:0:0:0001::1
- Letzte Adresse: 0:0:0:0001::9

Derzeit wird kein Neighbor Discovery Proxy für IPv6 unterstützt. Deshalb darf der Adressbereich des Pools nicht mit Adressbereichen bzw. Präfixen überlappen, die bereits für andere Netze auf dem Router verwendet werden.

Nameserver-Adressen

Erster DNS

Enthält die erste DNS-Adresse.

Zweiter DNS

Enthält die zweite DNS-Adresse.

Präfix-Länge

Optionale Präfix-Länge, die für die verhandelte IP-Adresse mitgeschickt wird.

11.19.1.8 Split-DNS

Beim VPN Split Tunneling werden nur Anwendungen durch den VPN-Tunnel gesendet, welche bestimmte Endpunkte hinter dem VPN-Tunnel erreichen sollen. Der gesamte andere Datenverkehr wird am VPN-Tunnel vorbei direkt ins Internet gesendet. Die Definition, welche IP-Netze durch den Tunnel erreichbar sein sollen, lassen sich durch VPN-Regeln definieren.

Split-DNS ermöglicht die DNS-Auflösung bestimmter interner Domänen, z. B. „*.firma.de“ über den VPN-Tunnel, während für alle anderen DNS-Anfragen ein öffentlicher DNS-Server verwendet wird. Hierbei weist der IKE-Config-Mode-Server dem Client eine oder mehrere Split-DNS-Domänen dynamisch über das Attribut INTERNAL_DNS_DOMAIN beim Verbindungsaufbau zu. Die empfangene Domain-Liste trägt der Client in seine lokale DNS-Weiterleitungsliste ein. Der Client muss dieses Attribut unterstützen.

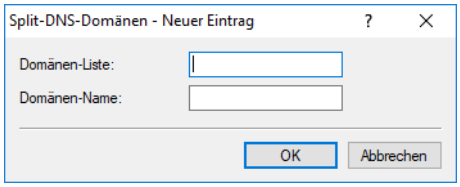
Split-DNS für IKEv2 wird von LANCOM VPN-Routern in der Rolle IKE-Config-Mode Client und Server unterstützt. Bei Site-to-Site-VPN-Verbindungen wird die dynamische Split-DNS-Zuweisung im IKE-Protokoll nicht unterstützt und muss über statische DNS-Weiterleitungen auf den entsprechenden VPN-Endpunkten konfiguriert werden.

Die Split-DNS-Konfiguration wird in der IKEv2-Verbindungsliste als Split-DNS-Profil in der CFG-Mode-Betriebsart „Server“ zugewiesen.

In LANconfig definieren Sie zuerst die gewünschten Domänen unter **VPN** > **IKEv2 / IPSec** > **Split-DNS-Domänen**, dann weisen Sie diese unter **VPN** > **IKEv2 / IPSec** > **Split-DNS-Profile** einem Profil zu, welches Sie in der **Verbindungsliste** im IKE Config-Mode verwenden können, falls dort **IKE-CFG** auf **Server** eingestellt wird.

Split-DNS-Domänen

In LANconfig erfolgt die Konfiguration der Split-DNS-Domänen unter **VPN** > **IKEv2 / IPSec** > **Split-DNS-Domänen**.



Domänen-Liste

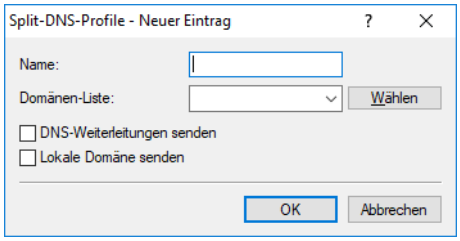
Vergeben Sie einen Namen für die Domänen-Liste.

Domänen-Name

Split-DNS-Domänen-Name, den das VPN-Gateway an VPN-Clients senden soll, z. B. „firma.intern“. Mehrere Domänen-Namen können durch mehrere Einträge mit dem gleichen Bezeichner der Domänen-Liste konfiguriert werden.

Split-DNS-Profile

In LANconfig erfolgt die Konfiguration der Split-DNS-Profile unter **VPN** > **IKEv2 / IPSec** > **Split-DNS-Profile**.



Name

Vergeben Sie einen Namen für dieses Profil.

Domänen-List

Name der Liste mit Split-DNS-Domänen, die das VPN-Gateway an VPN-Clients senden soll.

DNS-Weiterleitungen senden

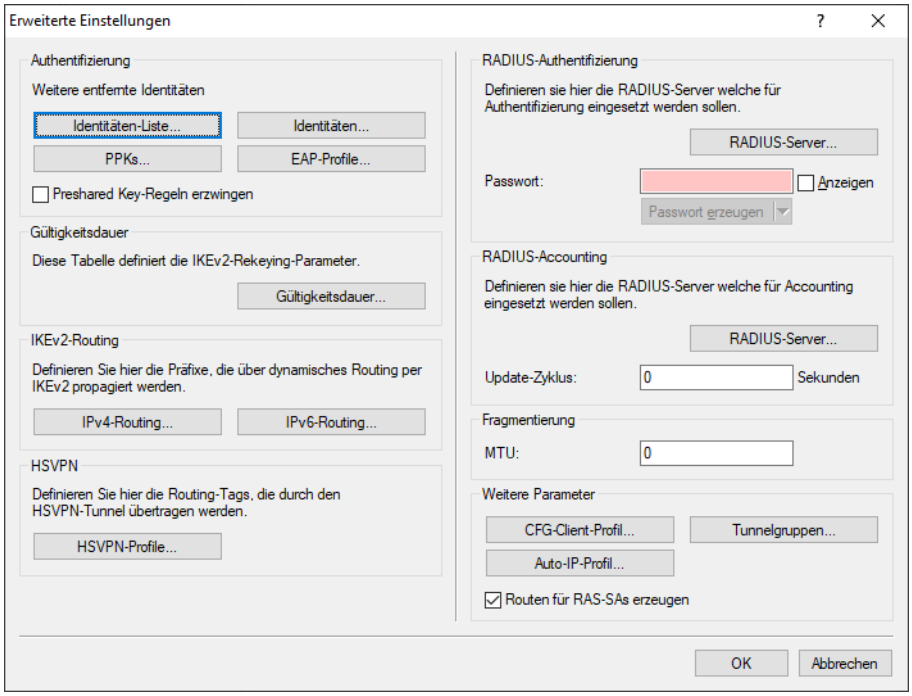
Stellen Sie ein, ob das VPN-Gateway seine lokal konfigurierten DNS-Weiterleitungen an VPN-Clients senden soll.

Lokale Domäne senden

Stellen Sie ein, ob das VPN-Gateway seine eigene lokal konfigurierte Domäne an VPN-Clients senden soll.

11.19.1.9 Erweiterte Einstellungen

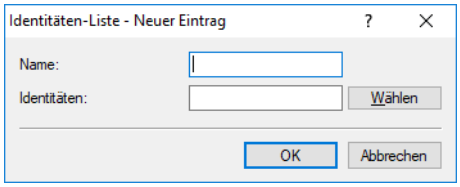
In diesem Dialog konfigurieren Sie die Einstellungen zur Authentifizierung weiterer entfernter Identitäten, die IKEv2-Rekeying-Parameter, die Präfixe für das IKEv2-Routing, die Routing-Tags für High Scalability VPN (HSVPN), die durch den HSVPN-Tunnel übertragen werden, die RADIUS-Server für IKEv2, die IKEv2-Fragmentierung, die Client-Profile, die in der Rolle CFG-Mode Client verwendet werden können, um zu steuern, ob eine Anfrage beim CFG-Mode Server durchgeführt werden soll, sowie die IKEv2-Tunnelgruppen.



Authentifizierung

Identitäten-Liste

In dieser Tabelle fassen Sie weitere entfernte Identitäten in einer Gruppe zusammen.



Name

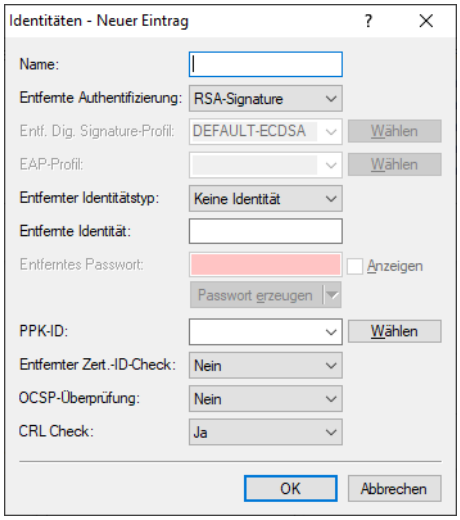
Enthält den eindeutigen Namen dieses Eintrages.

Identität

Listet die weiteren entfernten Identitäten auf, die in dieser Gruppe zusammengefasst sind. Diese Identitäten konfigurieren Sie unter **Identitäten**.

Identitäten

In dieser Tabelle konfigurieren Sie weitere entfernte Identitäten. Diesen Namen wählen Sie bei der Gruppierung von entfernten Identitäten unter **Identitäten-Liste** aus.



Name

Enthält den eindeutigen Namen dieses Eintrages.

Entfernte Authentifizierung

Legt die Authentifizierungsmethode für die entfernte Identität fest.

Entf. Dig. Signature-Profil

Falls als **Entfernte Authentifizierung** „Digital-Signature“ ausgewählt wird, dann geben Sie hier den Profilnamen des entfernten Digital-Signatur-Profils an.

Entfernter Identitätstyp

Zeigt den ID-Typ an, den das Gerät von der entfernten Identität erwartet. Entsprechend interpretiert das Gerät die Eingabe unter „Entfernte Identität“. Mögliche Angaben sind:

- Keine Identität: Das Gerät akzeptiert jede ID des entfernten Gerätes. Eine Angabe im Feld „Entfernte Identität“ ignoriert das Gerät.
- IPv4-Adresse: Das Gerät erwartet eine IPv4-Adresse als entfernte ID.
- IPv6-Adresse: Das Gerät erwartet eine IPv6-Adresse als entfernte ID.
- Domänen-Name (FQDN): Das Gerät erwartet einen Domänen-Namen als entfernte ID.
- E-Mail-Adresse (FQUN): Das Gerät erwartet eine E-Mail-Adresse als entfernte ID.
- ASN.1-Distinguished-Name: Das Gerät erwartet einen Distinguished Name als entfernte ID.
- Key-ID (Gruppenname): Das Gerät erwartet den Gruppennamen als entfernte ID.

Entfernte Identität

Enthält die entfernte Identität. Die Bedeutung dieser Eingabe ist abhängig von der Einstellung unter „Entfernter Identitätstyp“.

Entferntes Passwort

Enthält das Passwort der entfernten Identität.

PPK-ID

Geben Sie hier den Namen der PPK-ID (Post-quantum Preshared Keys nach *RFC 8784*) ein aus der Tabelle der *PPKs (Post-quantum Preshared Keys)* auf Seite 883.

Entfernter Zertifikats-ID-Check

Diese Option bestimmt, ob das Gerät prüft, ob die angegebene entfernte Identität im empfangenen Zertifikat enthalten ist.

OCSP-Überprüfung

Mit dieser Einstellung aktivieren Sie die Echtzeitüberprüfung eines Zertifikates via Online Certificate Status Protocol (OCSP), welche den Gültigkeitsstatus des Zertifikats der Gegenstelle abfragt. Um die OCSP-Prüfung für einzelne VPN-Verbindungen zu verwenden, müssen Sie zunächst den globalen OCSP-Client für VPN-Verbindungen aktivieren und anschließend Profillisten gültiger Zertifizierungsstellen anlegen, bei denen das Gerät die Echtzeitprüfung durchführt.

Beachten Sie, dass die Prüfung via OCSP allein den Sperrstatus eines Zertifikates abfragt, jedoch nicht die mathematische Korrektheit seiner Signatur, seine Gültigkeitsdauer oder sonstige Nutzungsbeschränkungen prüft.

CRL Check

Mit dieser Einstellung aktivieren Sie die Überprüfung eines X.509-Zertifikats via Zertifikatssperrlisten (Certificate Revocation List, CRL), welche den Gültigkeitsstatus des Zertifikats der Gegenstelle abfragt.

Schalten Sie diese Überprüfung nur ab, wenn Sie die Überprüfung auf einem anderen Weg durchführen, z. B. über OCSP.

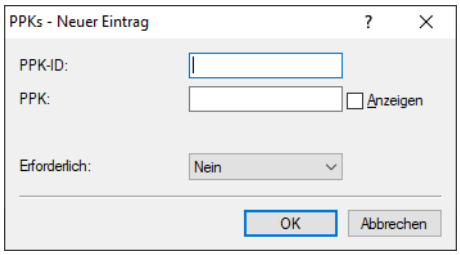
PPKs (Post-quantum Preshared Keys)

Quantencomputer stellen eine mögliche Herausforderung für aktuelle kryptografische Algorithmen dar, wie sie beispielsweise im IKEv2 VPN verwendet werden. Aktuelle Algorithmen gelten nach heutigem Stand als sehr robust, aber es besteht die Herausforderung, dass ein Angreifer heute verschlüsselte Daten aufzeichnen kann und diese mit Quantencomputern in der Zukunft entschlüsseln könnte.

Das *RFC 8784* „Mixing Preshared Keys in the Internet Key Exchange Protocol Version 2 (IKEv2) for Post-quantum Security“ bietet eine Möglichkeit, resistent gegen Quantencomputer zu sein, wenn Passwörter (PSKs) verwendet werden. Die Erweiterung besteht darin, dass in das standardmäßig verwendete IKEv2 Passwort-Verfahren (PSK) ein weiterer Schlüssel in Form eines Post-quantum Preshared Key (PPK) „gemixt“ wird, um die Resistenz zu erhöhen.

Bestehende IKEv2-PSK-Tunnel können einfach um PPKs ergänzt werden. Der PPK ist unabhängig vom bereits vorhandenen PSK.

LCOS unterstützt die manuelle Konfiguration von PPKs. Automatische Verfahren zur Änderung bzw. Wechsel von PPKs werden nicht unterstützt.



PPK-ID

Vergeben Sie einen eindeutigen Namen für diesen Eintrag. Eingabeformat ist möglich als Zeichenkette oder Hexadezimalzahl (identifiziert durch ein führendes 0x).

PPK

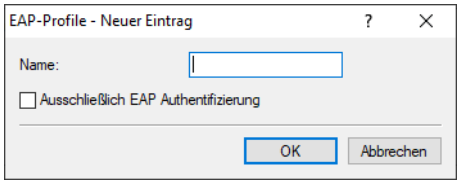
Vergeben Sie hier den Post-quantum Preshared Key als Zeichenkette oder Hexadezimalzahl (identifiziert durch ein führendes 0x).

Erforderlich

Wird die Verwendung von PPKs als erforderlich konfiguriert, so wird die entsprechende VPN-Verbindung abgelehnt, falls die Gegenseite kein PPK unterstützt oder konfiguriert hat. Wird die Verwendung von PPKs als optional konfiguriert, so werden sowohl Verbindungen mit PPK als auch ohne PPK akzeptiert.

EAP-Profile

In dieser Tabelle konfigurieren Sie EAP-Profile. Diese wählen Sie bei der **Authentifizierung** aus, wenn Sie als Methode für die **entfernte Authentifizierung** EAP auswählen.



Name

Geben Sie diesem EAP-Profil einen Namen, über den es referenziert werden kann.

Ausschließlich EAP-Authentifzierung

Erlaubt optional die gegenseitige Authentifizierung der Gegenstellen innerhalb des EAP. Die Authentifizierung außerhalb des EAP entfällt dann. Siehe auch *RFC 5998*.

Passwort-Regeln

Preshared Key-Regeln erzwingen

Mit dieser Option haben Sie die Möglichkeit, das Erzwingen von Passwort-Regeln zu aktivieren oder zu deaktivieren. Es gelten dann die folgenden Regeln für die Pre-Shared Keys (PSK) bei IKEv2:

› Die Länge des Passworts muss mindestens 32 Zeichen betragen.

› Das Passwort muss mindestens 3 der 4 Zeichenklassen Kleinbuchstaben, Großbuchstaben, Zahlen und Sonderzeichen enthalten.

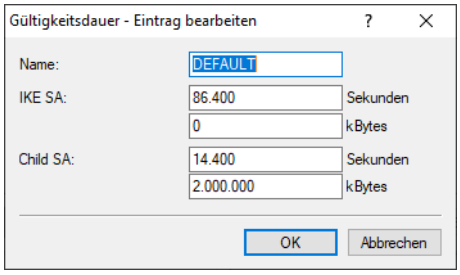
Diese Regeln gelten nicht für PSK, die von einem RADIUS-Server verwaltet und bezogen werden.

Gültigkeitsdauer

In dieser Tabelle definieren Sie die IKEv2-Rekeying-Parameter. Es existiert ein Standardeintrag „DEFAULT" mit gängigen Einstellungen.

Je Phase unterscheidet das Gerät nach Zeit oder zu übertragender Datenmenge. Der Parameter, der als erstes seinen festgelegten Grenzwert erreicht, startet die Erneuerung des entsprechenden IKEv2-Schlüssels.

Der Wert „0" bedeutet, dass das Gerät keinen Grenzwert für den entsprechenden Schlüssel festlegt.



Name

Enthält den eindeutigen Namen dieses Eintrages.

IKE SA

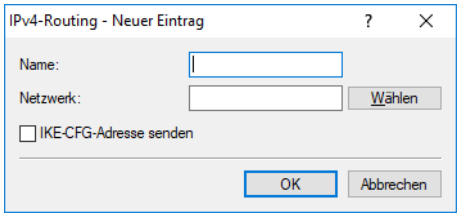
Enthält die Zeit in Sekunden und / oder die Datenmenge in Kilobyte bis zur Erneuerung des IKE-SA-Schlüssels.

Child SA

Enthält die Zeit in Sekunden und / oder die Datenmenge in Kilobyte bis zur Erneuerung des CHILD-SA-Schlüssels.

IPv4-Routing

In dieser Tabelle konfigurieren Sie die IPv4-Netze, die das Gerät über dynamisches Routing per IKEv2 propagiert.



Name

Enthält den eindeutigen Namen dieses Eintrages.

Netzwerk

Enthält die kommaseparierte Liste von IP-Subnetzen.

Die Angabe der Netze ist in den folgenden Formaten möglich:

- IP-Adresse
- IP-Adresse/Netzmaske
- IP-Adresse/Netzmaske@Tag
- IP-Adresse/Präfixlänge
- IP-Adresse/Präfixlänge@Tag
- IP-Schnittstellen-Name
- IP-Schnittstellen-Name@Tag
-

Die Angabe mit Routing Tag wird bei HSVPN verwendet. Siehe hierzu auch HSVPN im Abschnitt *Verbindungs-Liste* auf Seite 866.

Die Konfiguration der IP-Subnetze erfolgt unter **IPv4** > **Allgemein** im Abschnitt **Eigene Adressen**.

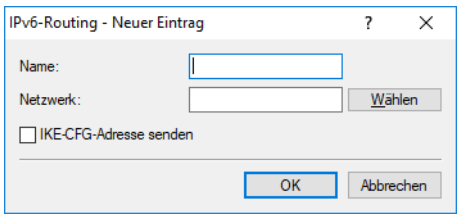
IKE-CFG-Adresse senden

Als Client sendet das Gerät die erhaltene CFG-Mode-Adresse an den VPN-Peer (Server).

Diese Option ist nur dann erforderlich, falls die Gegenseite keinen automatischen Routing-Eintrag für zugewiesene IP-Adressen erzeugt. LANCOM Router erzeugen die notwendigen Routen automatisch.

IPv6-Routing

In dieser Tabelle konfigurieren Sie die IPv6-Netze, die das Gerät über dynamisches Routing per IKEv2 propagiert.



Name

Enthält den eindeutigen Namen dieses Eintrages.

Netzwerk

Enthält die kommaseparierte Liste von IPv6-Subnetzen.

Die Angabe der Netze ist in den folgenden Formaten möglich:

- IPv6-Adresse
- IPv6-Adresse/Präfixlänge
- IPv6-Adresse/Präfixlänge@Tag
- IPv6-Schnittstellen-Name
- IPv6-Schnittstellen-Name@Tag

Die Angabe mit Routing Tag wird bei HSVPN verwendet. Siehe hierzu auch HSVPN im Abschnitt *Verbindungs-Liste* auf Seite 866.

Die Konfiguration der IP-Subnetze erfolgt unter **IPv6** > **Allgemein** im Abschnitt **IPv6-Netzwerke**.

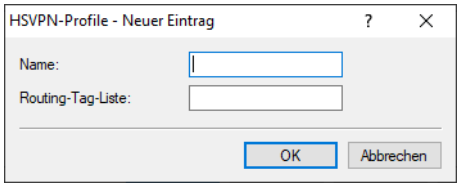
IKE-CFG-Adresse senden

Als Client sendet das Gerät die erhaltene CFG-Mode-Adresse an den VPN-Peer (Server).

Diese Option ist nur dann erforderlich, falls die Gegenseite keinen automatischen Routing-Eintrag für zugewiesene IP-Adressen erzeugt. LANCOM Router erzeugen die notwendigen Routen automatisch.

HSVPN-Profile

In dieser Tabelle werden die HSVPN-Profile konfiguriert. Wechseln Sie zur Konfiguration in LANconfig in die Ansicht **VPN** > **IKEv2/IPSec** > **Erweiterte Einstellungen** und konfigurieren Sie im Abschnitt **HSVPN** die **HSVPN-Profile**.



Name

Vergeben Sie einen Namen für das HSVPN-Profil.

Routing-Tag-Liste

Definieren Sie hier die Routing-Tags als kommaseparierte Liste (z. B. 1,2,3), die über HSVPN übertragen werden sollen. Die Rtg-Tag-Liste muss zwischen beiden VPN-Partnern identisch sein, damit alle gewünschten ARF-Netze transportiert werden.

RADIUS-Authentifizierung

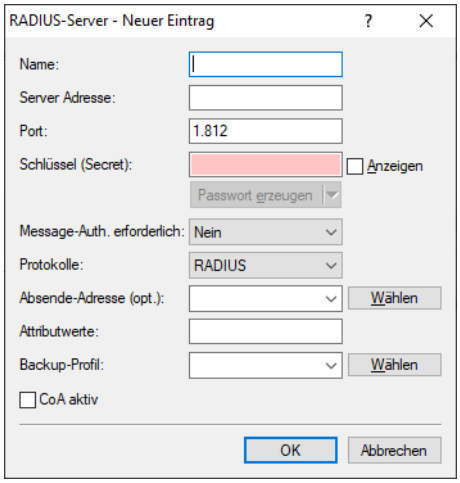
Im Abschnitt **RADIUS-Authentifizierung** konfigurieren Sie die Einstellungen der RADIUS-Server zur Autorisierung von VPN-Clients.

Bestimmen Sie im Feld **Passwort** das Passwort, das der RADIUS-Server im Access-Request-Attribut als Benutzer-Passwort erhält.

Der RADIUS-Server ordnet dieses Passwort normalerweise direkt einem VPN-Peer zu, um diesen für den Netzwerkzugang zu autorisieren. Bei IKEv2 autorisiert jedoch nicht der RADIUS-Server den anfragenden VPN-Peer, sondern das LANCOM Gateway, nachdem es die entsprechende Autorisierung in der `Access-Accept`-Nachricht des RADIUS-Servers erhalten hat.

Entsprechend geben Sie an dieser Stelle ein Dummy-Passwort ein.

Mit einem Klick auf **RADIUS-Server** öffnet sich der Dialog zur Konfiguration des RADIUS-Servers.



Name

Geben Sie eine Bezeichnung für diesen Eintrag ein.

Server-Adresse

Geben Sie den Hostnamen für den RADIUS-Server an (IPv4-, IPv6- oder DNS-Adresse).

Port

Geben Sie den UDP-Port des RADIUS-Servers an. Der Wert „1812“ ist als Standardwert voreingestellt.

Schlüssel (Secret)

Dieser Eintrag enthält den Schlüssel (Shared Secret) zur Autorisierung des LANCOM-Gateways am RADIUS-Server.

Bestätigen Sie den angegebenen Schlüssel durch eine erneute Eingabe im darauf folgenden Feld.

Message-Authenticator erforderlich

Definiert, ob das Vorhandensein des Message-Authenticator-Attributs in RADIUS-Nachrichten auf Client-Seite erforderlich ist. Die Client-Seite ist die Seite, die den RADIUS-Accept/Fail empfängt.

Protokolle

Wählen Sie aus dem Drop-Down-Menü zwischen dem normalen RADIUS-Protokoll und dem sicheren RADSEC-Protokoll für die RADIUS-Anfrage.

Absende-Adresse (opt.)

Geben Sie hier ggf. die Loopback-Adresse des Gerätes an.

Attributwerte

LCOS ermöglicht es, die RADIUS-Attribute für die Kommunikation mit einem RADIUS-Server (sowohl Authentication als auch Accounting) zu konfigurieren.

Die Angabe der Attribute erfolgt als semikolon-separierte Liste von Attribut-Nummern oder -Namen und einem entsprechenden Wert in der folgenden Form:

`<Attribut_1>=<Wert_1>;<Attribut_2>=<Wert_2>`

Da die Anzahl der Zeichen begrenzt ist, lässt sich der Name abkürzen. Das Kürzel muss dabei eindeutig sein. Beispiele:

- `NAS-Port=1234` ist nicht erlaubt, da das Attribut nicht eindeutig ist (`NAS-Port`, `NAS-Port-Id` oder `NAS-Port-Type`).
- `NAS-Id=ABCD` ist erlaubt, da das Attribut eindeutig ist (`NAS-Identifier`).

Als Attribut-Wert ist die Angabe von Namen oder RFC-konformen Nummern möglich. Für das Gerät sind die Angaben `Service-Type=Framed` und `Service-Type=2` identisch.

Die Angabe eines Wertes in Anführungszeichen (`"<Wert>"`) ist möglich, um Sonderzeichen wie Leerzeichen, Semikolon oder Gleichheitszeichen mit angeben zu können. Das Anführungszeichen erhält einen umgekehrten Schrägstrich vorangestellt (`\"`), der umgekehrte Schrägstrich ebenfalls (`\\`).

Als Werte sind auch die folgenden Variablen erlaubt:

`%n`

Gerätename

`%e`

Seriennummer des Gerätes

`%%`

Prozentzeichen

`%{name}`

Original-Name des Attributes, wie ihn die RADIUS-Anwendung überträgt. Damit lassen sich z. B. Attribute mit originalen RADIUS-Attributen belegen: `Called-Station-Id=%{NAS-Identifier}` setzt das Attribut `Called-Station-Id` auf den Wert, den das Attribut `NAS-Identifier` besitzt.

Backup-Profil

Wählen Sie aus der Liste der RADIUS-Server-Profile ein Profil als Backup-Server.

CoA aktiv

Hier aktivieren bzw. deaktivieren Sie **CoA**.

Als CoA-Nachricht wird die Disconnect-Nachricht unterstützt, um einen verbundenen VPN-Benutzer bzw. eine VPN-Gegenstelle zu trennen. Die CoA-Disconnect-Nachricht muss den Benutzernamen als RADIUS Attribut „User-Name" sowie das Attribut „NAS-IP-Adresse" enthalten. Um die Funktion zu aktivieren muss zusätzlich *Dynamische Autorisierung* global aktiviert werden und ein CoA-Client-Zugriff konfiguriert werden.

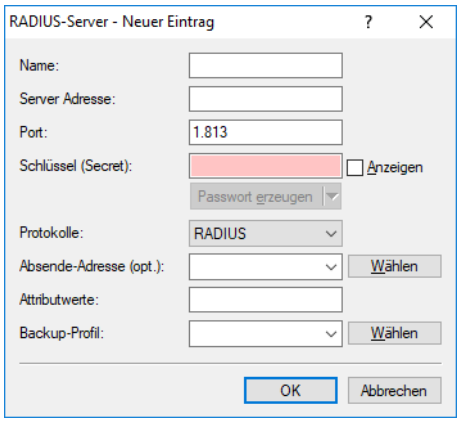
Die Auswahl der hier konfigurierten RADIUS-Server erfolgt in der Verbindungsliste unter **VPN** > **IKEv2/IPSec** > **Verbindungs-Liste** im Feld **RADIUS-Auth.-Server**.

RADIUS-Accounting

Im Abschnitt **RADIUS-Accounting** konfigurieren Sie die Einstellungen der RADIUS-Server zum Accounting von VPN-Clients.

Bestimmen Sie im Feld **Update-Zyklus** die Zeit in Sekunden zwischen zwei aufeinanderfolgenden Interim-Update-Nachrichten. Das Gerät fügt zufällig eine Toleranz von ±10% ein, um die Update-Nachrichten paralleler Accounting Sessions zeitlich voneinander abzutrennen.

Mit einem Klick auf **RADIUS-Server** öffnet sich der Dialog zur Konfiguration des RADIUS-Servers.



Name

Geben Sie eine Bezeichnung für diesen Eintrag ein.

Server-Adresse

Geben Sie den Hostnamen für den RADIUS-Server an (IPv4-, IPv6- oder DNS-Adresse).

Port

Geben Sie den UDP-Port des RADIUS-Servers an. Der Wert „1813“ ist als Standardwert voreingestellt.

Schlüssel (Secret)

Dieser Eintrag enthält den Schlüssel (Shared Secret) zur Autorisierung des LANCOM-Gateways am RADIUS-Server.

Bestätigen Sie den angegebenen Schlüssel durch eine erneute Eingabe im darauf folgenden Feld.

Protokolle

Wählen Sie aus dem Drop-Down-Menü zwischen dem normalen RADIUS-Protokoll und dem sicheren RADSEC-Protokoll für die RADIUS-Anfrage.

Absende-Adresse (opt.)

Geben Sie hier ggf. die Loopback-Adresse des Gerätes an.

Attributwerte

LCOS ermöglicht es, die RADIUS-Attribute für die Kommunikation mit einem RADIUS-Server (sowohl Authentication als auch Accounting) zu konfigurieren.

Die Angabe der Attribute erfolgt als semikolon-separierte Liste von Attribut-Nummern oder -Namen und einem entsprechenden Wert in der folgenden Form:

`<Attribut_1>=<Wert_1>;<Attribut_2>=<Wert_2>`

Da die Anzahl der Zeichen begrenzt ist, lässt sich der Name abkürzen. Das Kürzel muss dabei eindeutig sein. Beispiele:

- `NAS-Port=1234` ist nicht erlaubt, da das Attribut nicht eindeutig ist (`NAS-Port`, `NAS-Port-Id` oder `NAS-Port-Type`).
- `NAS-Id=ABCD` ist erlaubt, da das Attribut eindeutig ist (`NAS-Identifier`).

Als Attribut-Wert ist die Angabe von Namen oder RFC-konformen Nummern möglich. Für das Gerät sind die Angaben `Service-Type=Framed` und `Service-Type=2` identisch.

Die Angabe eines Wertes in Anführungszeichen (`"<Wert>"`) ist möglich, um Sonderzeichen wie Leerzeichen, Semikolon oder Gleichheitszeichen mit angeben zu können. Das Anführungszeichen erhält einen umgekehrten Schrägstrich vorangestellt (`\"`), der umgekehrte Schrägstrich ebenfalls (`\\`).

Als Werte sind auch die folgenden Variablen erlaubt:

`%n`

Gerätename

`%e`

Seriennummer des Gerätes

`%%`

Prozentzeichen

`%{name}`

Original-Name des Attributes, wie ihn die RADIUS-Anwendung überträgt. Damit lassen sich z. B. Attribute mit originalen RADIUS-Attributen belegen: `Called-Station-Id=%{NAS-Identifier}` setzt das Attribut `Called-Station-Id` auf den Wert, den das Attribut `NAS-Identifier` besitzt.

Backup-Profil

Wählen Sie aus der Liste der RADIUS-Server-Profile ein Profil als Backup-Server.

Die Auswahl der hier konfigurierten RADIUS-Server erfolgt in der Verbindungsliste unter **VPN** > **IKEv2/IPSec** > **Verbindungs-Liste** im Feld **RADIUS-Acc.-Server**.

IKEv2-Fragmentierung

Die Fragmentierung von Datenpaketen richtet sich nach der Maximum Transmission Unit (MTU). Die MTU bezeichnet die maximale Größe, die ein Paket haben darf, um als Payload über einen Kanal versendet werden zu können. Diese wird zu Beginn einer Übertragung von beiden Kommunikationspartnern ausgehandelt, um die optimale Datenübertragung ohne eine zusätzliche Fragmentierung von Datenpaketen gewährleisten zu können.

In LCOS ist die IKEv2-Fragmentierung automatisch aktiviert. Sie können davon abweichend manuell eine maximale MTU definieren.

Wechseln Sie dazu in LANconfig in die Ansicht **VPN** > **IKEv2/IPSec** > **Erweiterte Einstellungen**.



Geben Sie im Abschnitt **Fragmentierung** im Feld **MTU** die maximale IP-Paketlänge / -größe in Byte an. Je kleiner Sie den Wert wählen, desto stärker ist die Fragmentierung der Nutzdaten.

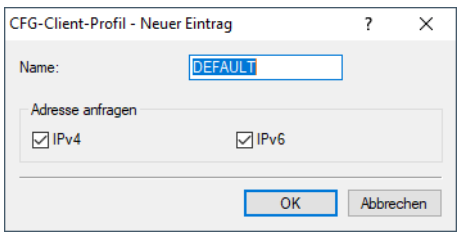
Die IKEv2-Fragmentierung nach RFC 7383 ermöglicht die effiziente Fragmentierung von IKEv2-Nachrichten vom VPN-Router selbst, sodass IKE-Pakete vom Transportnetz nicht mehr fragmentiert werden müssen. Grundsätzlich werden zwei Verfahren der IKEv2-Fragmentierung unterstützt:

- Herstellerspezifische Fragmentierung, kompatibel zu Drittherstellern
- Fragmentierung nach RFC 7383

Das Gerät wählt automatisch das beste Verfahren. Unterstützt eine VPN-Gegenseite beide Verfahren, so wird die Fragmentierung nach RFC 7383 bevorzugt.

CFG-Client-Profil

Wechseln Sie zur Konfiguration in LANconfig in die Ansicht **VPN** > **IKEv2/IPSec** > **Erweiterte Einstellungen** und konfigurieren Sie im Abschnitt **Weitere Parameter** die **CFG-Client-Profile**. Dieses Profil können Sie dann unter *Verbindungs-Liste* auf Seite 866 auswählen, um zu bestimmen, ob das Gerät in der Rolle CFG-Mode Client eine Adresse beim CFG-Mode-Server anfragen soll.



Name

Eindeutiger Name für das CFG-Client-Profil.

Adresse anfragen

Bestimmen Sie, ob für dieses Profil Adressen für IPv4 und / oder IPv6 angefragt werden sollen.

IKEv2-Tunnelgruppen

In bestimmten VPN-Szenarien ist es erforderlich, dass eine bestimmte Gruppe von VPN-Tunneln eines Geräts immer auf einem gemeinsamen VPN-Gateway terminiert wird bzw. zu diesem aufbaut. Dies ist beispielsweise dann erforderlich, wenn VPN-Tunnel in einem Load-Balancer-Verbund konfiguriert sind und VPN-Tunnel die alternative Gateway-Liste verwenden und ggf. unterschiedliche Wege bzw. ausgehende Internetverbindungen (DSL, LTE, Ethernet) zum Ziel nutzen.

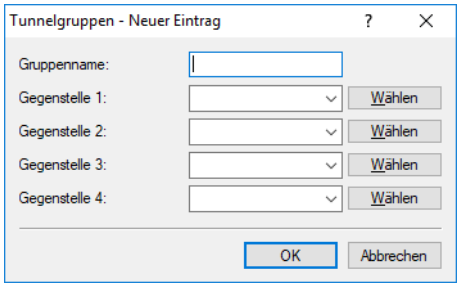
Voraussetzung für einen VPN-Load-Balancer ist, dass alle VPN-Tunnel immer auf einem gemeinsamen VPN-Gateway terminieren.

Die Funktion IKEv2-Tunnelgruppen stellt sicher, dass alle VPN-Tunnel einer Gruppe immer auf einem gemeinsamen VPN-Gateway terminieren. Der erste funktionierend aufgebaute VPN-Tunnel einer Gruppe gibt das gemeinsame VPN-Gateway vor und es werden VPN-Remote-Gateways aller anderen Tunnelgruppenmitglieder auf dieses Ziel umgeschrieben. In der Regel ist das der VPN-Tunnel, der am schnellsten zu Stande kommt. Eine neue Auswahl eines Gateways findet nur statt, wenn alle Tunnelgruppen-Mitglieder das Gateway nicht erreichen können.

Die Funktion der IKEv2-Tunnelgruppen kann grundsätzlich unabhängig von einem Load-Balancer genutzt werden.

Tunnelgruppen werden nicht in Zusammenhang mit IKEv2-Redirect und dem IKEv2 Redirect Load-Balancer unterstützt.

Wechseln Sie zur Konfiguration in LANconfig in die Ansicht **VPN** > **IKEv2/IPSec** > **Erweiterte Einstellungen** und konfigurieren Sie im Abschnitt **Weitere Parameter** die **Tunnelgruppen**.



Gruppenname

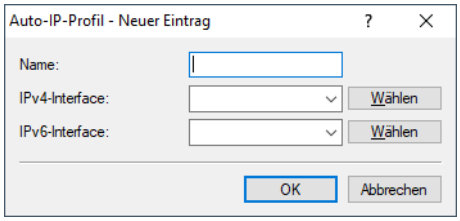
Eindeutiger Name für die Tunnelgruppe.

Gegenstelle 1-4

Jeweiliger Gegenstellenname des IKEv2 VPN-Tunnels, der in der Tunnelgruppe terminiert.

IKEv2-Auto-IP-Profil

Wechseln Sie zur Konfiguration in LANconfig in die Ansicht **VPN** > **IKEv2/IPSec** > **Erweiterte Einstellungen** und konfigurieren Sie im Abschnitt **Weitere Parameter** das **Auto-IP-Profil**.



Name

Eindeutiger Name des Auto-IP-Profils. Dieser wird unter *Auto-IP* auf Seite 869 referenziert.

IPv4-Interface

IPv4-Netzwerkname von dem die IPv4-Adresse an die VPN-Gegenseite für das Dynamic-Path-Selection-Messziel übermittelt werden soll.

Mögliche Werte: IPv4-Netzwerke

IPv6-Interface

IPv6-Interfacename, von dem die IPv6-Adresse an die VPN-Gegenseite für das Dynamic-Path-Selection-Messziel übermittelt werden soll.

Mögliche Werte: IPv6-LAN-Interfaces

11.19.1.10 LANCOM Advanced Mesh VPN (AMVPN)

Klassische VPN-Szenarien in der Standortvernetzung sind in der Regel sternförmig (Hub & Spoke) aufgebaut. Dabei bauen die angebundenen Filialen (Spokes) VPN-Tunnel zu einer oder mehreren Zentralen (Hubs) auf. In solchen traditionellen Szenarien ist ein Hub & Spoke-Netzwerk-Design eine logische Topologieentscheidung, denn es fließen Daten hauptsächlich

zwischen Filiale und Zentrale, da dort zentrale Server stehen, z. B. das Warenwirtschaftssystem, Datenbanken oder Webserver.

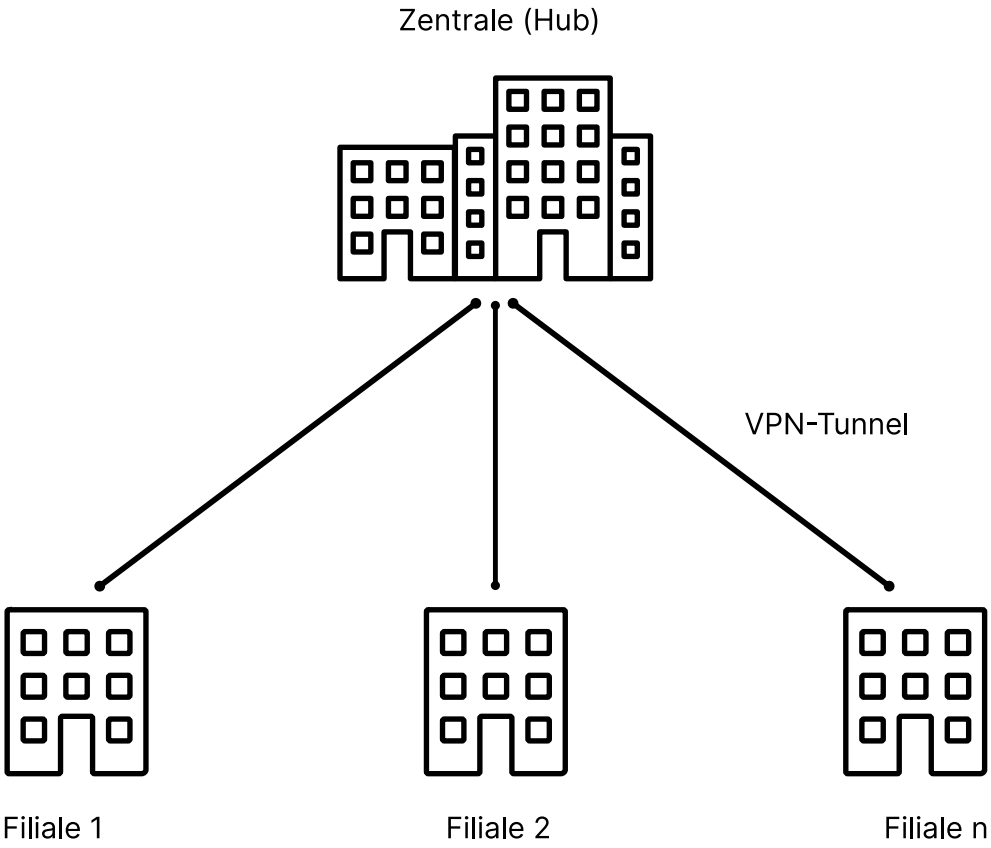


Abbildung 7: Klassische Standortvernetzung (Hub & Spoke)

Die Vorteile dieses sternförmigen Netzwerkdesigns sind der einfache Aufbau und die zentrale Steuerung in der Zentrale. Der Nachteil ist jedoch, dass sämtlicher Datenverkehr - auch der zwischen einzelnen Filialen wie z. B. Telefonie oder Dateiaustausch über einen File-Server - immer über den indirekten Weg über die Zentrale erfolgt. Dadurch wird die

Internetanbindung der Zentrale mit dem Datenverkehr zwischen den Filialen belastet und somit zum Flaschenhals der gesamten Kommunikation.

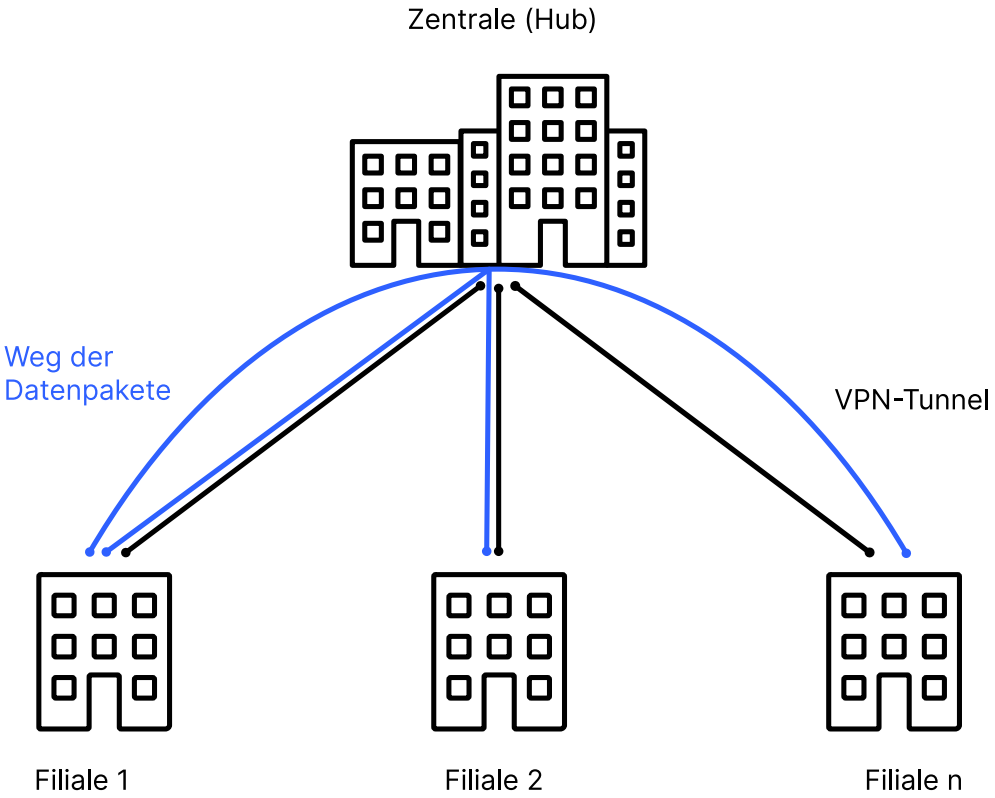


Abbildung 8: Datenaustausch zwischen Filialen bei klassischer Standortvernetzung (Hub & Spoke)

Wenn der Datenverkehr zwischen den Filialen der größte Anteil der Verkehrsbeziehung darstellt, ist es ein praktischer Lösungsansatz, direkte VPN-Tunnel zwischen den Filialen manuell zu konfigurieren. In diesem Fall spricht man von einem VPN-Mesh-Szenario. In einfachen Szenarien funktioniert dieser manuelle Ansatz noch gut. Wenn es allerdings viele Filialen gibt und viele mögliche VPN-Tunnel, so skaliert dieser starre, einzeln und fest konfigurierte Ansatz nicht mehr.

LANCOM bietet für dieses Szenario die Lösung „Advanced Mesh VPN“. Hierbei besteht zunächst eine klassische sternförmige VPN-Struktur, in der alle Filialen zu Beginn einen VPN-Tunnel zur Zentrale aufbauen. Gibt es nun Datenverkehr zwischen den Filialen, so wird dynamisch ein VPN-Tunnel als Abkürzung zwischen den beiden beteiligten Filialen aufgebaut. Die Daten fließen nun direkt in einem VPN-Tunnel zwischen den Filialen, ohne dass die Daten den Weg über die Zentrale gehen.

Dabei fließen nur die ersten Datenpakete immer den langen Weg von der Filiale A über die Zentrale zur zweiten Filiale B. Erst beim Empfang der ersten Datenpakete in der Zielfiliale initiiert die Zielfiliale einen dynamischen VPN-Tunnel zur Filiale mit dem Ursprung des Datenpakets. Fließen nach einiger Zeit keinen Daten mehr, so wird der Tunnel dynamisch wieder abgebaut.

Der Vorteil: Deutlich weniger Traffic in der Zentrale und einhergehend höhere Performance im gesamten Unternehmensnetzwerk.

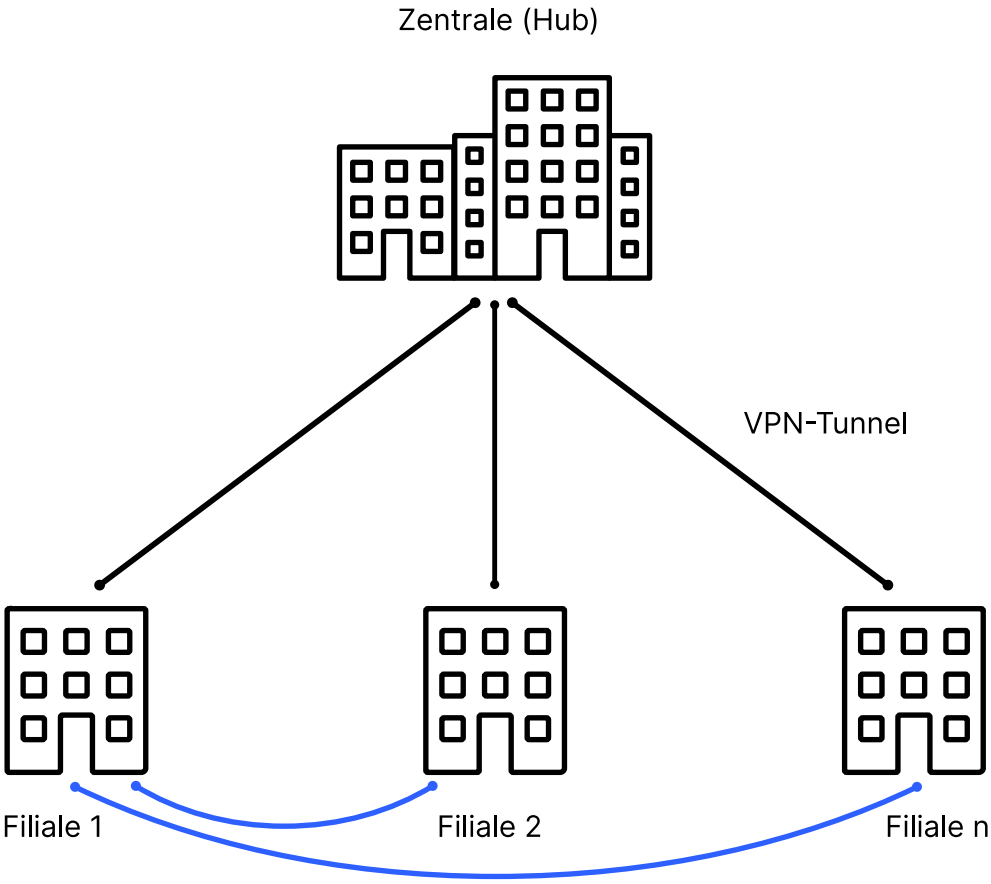


Abbildung 9: Standortvernetzung über Advanced Mesh VPN

Folgende grundsätzlichen Schritte sind zur Konfiguration von Advanced Mesh VPN notwendig:

1. Konfiguration der statischen VPN-Tunnel zwischen Filiale und Zentrale.
2. Anlegen einer Mesh-VPN-Tunnel-Vorlage (Template) in der IKEv2-Gegenstellen-Tabelle, die die gemeinsamen VPN-Eigenschaften wie Verschlüsselung, PSK oder Zertifikat für die dynamischen Mesh-VPN-Tunnel enthält.
3. Aktivierung der Mesh-VPN-Funktionalität und Konfiguration der globalen Mesh-Parameter auf allen beteiligten VPN-Routern.

Wie erfolgt der dynamische Aufbau eines Mesh-VPNs?

1. Filiale A sendet Datenpakete in den VPN-Tunnel über den bestehenden statischen VPN-Tunnel zur Zentrale an Filiale B.
2. Der Router in Filiale B erkennt eine neue Session, da Datenpakete von einem unbekannten Subnetz in dem VPN-Tunnel von der Zentrale ankommen.
3. Filiale B sendet eine verschlüsselte herstellerspezifischen IKEv2-Nachricht an die Zentrale. Die Nachricht enthält die privaten Subnetze bzw. IP-Adressen der gewünschten Kommunikationsbeziehung und die öffentliche IP-Adresse der Filiale B.
4. Die Zentrale empfängt die herstellerspezifische IKEv2-Nachricht im VPN-Tunnel von Filiale B und leitet sie über den VPN-Tunnel, der zur Filiale A führt, an Filiale A.
5. Filiale A empfängt die herstellerspezifische IKEv2-Nachricht der Zentrale.

6. Filiale A erzeugt einen dynamischen Mesh-VPN-Tunnel und baut diesen direkt zur IP-Adresse der Filiale B auf. Die notwendigen Informationen zum Aufbau des Tunnels entnimmt der Router aus der herstellerspezifische IKEv2-Nachricht (Gateway IP-Adresse, Subnetz etc.).
7. Filiale B nimmt den Tunnelaufbau von Filiale A an und aktualisiert ihre lokale Routing-Tabelle auf das Subnetz von Filiale A mit Ziel-Gateway der öffentlichen IP-Adresse von Filiale A. Das private Subnetz der Filiale A wird per IKEv2-Routing als IKEv2-Nachricht während des VPN-Tunnelaufbaus verwendet und ist spezifischer als die Route in die Zentrale.
8. Es fließen nun Daten direkt zwischen Filiale A und B, da die Routen auf beiden Seiten auf den dynamischen VPN-Tunnel zeigen.
9. Werden nach einem Timeout keine Daten mehr übertragen, so wird der Mesh-VPN-Tunnel abgebaut.

- Die ersten Datenpakete fließen immer zuerst über den Tunnel zur Zentrale und lösen dann den Aufbau eines dynamischen Tunnels aus.
- Ein Ping auf die LAN-IP-Adresse des Routers der Gegenseite löst keinen Mesh-VPN-Tunnelaufbau aus. Nur Datenpakete an Endpunkte im LAN lösen einen Tunnelaufbau aus, da nur diese von der Router-Firewall korrekt erkannt werden können. Ein Ping an eine (ggf. nichtexistierende) IP-Adresse im LAN löst aber den Aufbau eines VPN-Mesh-Tunnels aus.
- Bestehende Firewall-Sessions der ersten Datenpakete über die Zentrale werden nach erfolgreichem VPN-Mesh-Tunnelaufbau auf den neu aufgebauten Mesh-Tunnel umgezogen (Session Switchover).
- Die Filiale, die einen dynamischen VPN-Mesh-Tunnel annehmen soll, muss über eine öffentliche IP-Adresse (IPv4 oder IPv6) verfügen und von außen erreichbar sein. Router mit einer Mobilfunkverbindung verfügen in der Regel nicht über eine öffentliche IP-Adresse.
- LANCOM Advanced Mesh VPN ist eine herstellerspezifische Implementierung basierend auf IKEv2 und funktioniert nur zwischen LCOS-basierten LANCOM VPN-Routern. Der LANCOM Advanced VPN Client unterstützt dies nicht.
- Die Sicherheit basiert vollständig auf IKEv2 / IPSec und kann alle Einstellungen wie PSK, Zertifikate, Verschlüsselungsalgorithmen oder LANCOM HSVPN von IKEv2 verwenden.
- Alle beteiligten Router (Filiale, Zentrale) benötigen LCOS 10.70 oder höher.

Für Traces des LANCOM Advanced Mesh VPN wurde der Parameter `VPN-Mesh` hinzugefügt. Siehe auch *Trace-Ausgaben* auf Seite 308.

Lizenzierung

Mesh-VPN-Tunnel werden separat und zusätzlich zu den normalen VPN-Tunneln gezählt. Sind die Lizenzen für Mesh-VPN-Tunnel erschöpft, so wird kein Mesh-Tunnel aufgebaut und die Daten laufen weiterhin den längeren Weg über die Zentrale. Zentralseitige Geräte sind auf 200 Mesh-Tunnel in allen Ausbaustufen begrenzt.

Die folgenden Mesh-VPN-Lizenzen gelten (in Abhängigkeit der Anzahl der normalen VPN-Tunnel):

Tabelle 28: Mesh-VPN-Tunnel-Lizenzen

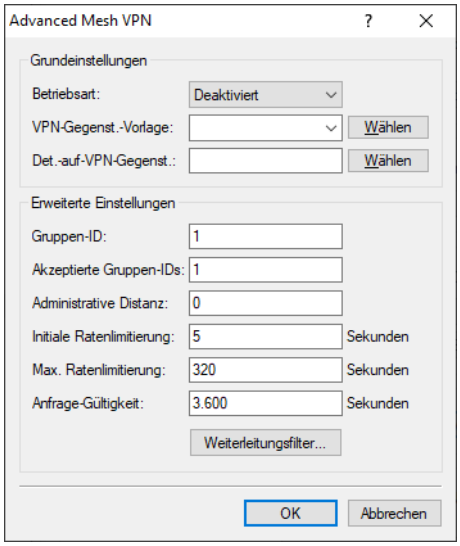
Kategorie	Geräte	Anzahl Lizenzen	
		VPN-Tunnel	Mesh-VPN-Tunnel
CPE	R88x, 88x VoIP, 1640E	3	6
CPE	179x, 18xx	5	10
CPE	179x, 18xx mit VPN 25	25	50
CPE	19xx	25	50
CPE	19xx mit VPN 50	50	100
CPE	19xx mit VPN 100	100	200

Kategorie	Geräte	Anzahl Lizenzen	
		VPN-Tunnel	Mesh-VPN-Tunnel
Zentrale	ISG-1000	100	200
Zentrale	ISG-4000	200	200
Zentrale	ISG-5000	100	200
Zentrale	ISG-8000	250	200

Advanced Mesh VPN konfigurieren

Konfigurieren Sie Advanced Mesh VPN in LANconfig unter **VPN** > **IKEv2 / IPSec** > **Erweiterte Einstellungen** > **Advanced Mesh VPN**.





Betriebsart

Dieser Schalter beeinflusst die Arbeitsweise des Mesh-VPNs und aktiviert das Verhalten als Spoke oder Hub oder beide Rollen gleichzeitig. Mögliche Werte:

Deaktiviert

Die Mesh-VPN-Funktion ist deaktiviert, die Mesh-Nachrichten werden nicht gesendet, weitergeleitet oder verarbeitet. Mesh-VPN-Tunnel können weder aufgebaut noch angenommen werden.

Hub

Das Gerät übernimmt die Rolle des zentralseitigen VPN-Gateways. Die Mesh-Nachrichten werden zwischen den Tunneln weitergeleitet. Das Gerät baut selber keine Mesh-VPN-Tunnel auf oder nimmt sie an.

Spoke

Das Gerät übernimmt die Funktion einer Filiale und baut Mesh-VPN-Tunnel auf und nimmt diese an.

Hub&Spoke

Das Gerät übernimmt die Rolle des zentralseitigen VPN-Gateways und baut außerdem noch Mesh-VPN-Tunnel zu anderen Spokes auf und nimmt Mesh-VPN-Tunnel an.

VPN-Gegenstellen-Vorlage

Dieser Parameter verweist auf einen Eintrag in der IKEv2-Gegenstellen-Tabelle. Dieser Eintrag wird als Konfigurationsvorlage für die Mesh-VPN-Tunnel verwendet.

Detektiere auf VPN-Gegenstelle

Eine kommaseparierte Liste von VPN-Gegenstellen, auf die der (Firewall-)Detektor reagieren soll. Dieser Eintrag wird auf Filialen benötigt, um eingehende Sessions zu detektieren. Kann leer gelassen werden bspw. auf Filialen, die hinter einem NAT (ohne Portforwarding) stehen und daher nicht als Responder eines Mesh-Tunnels fungieren können.

Gruppen-ID

Jedes Gerät kann einer Gruppe zugeordnet werden, mit der die eigenen Requests versendet werden. Damit wird es möglich das Mesh in kleinere Gruppen zu unterteilen, z. B. regionale Mesh-Strukturen.

Akzeptierte Gruppen-IDs

Eine kommaseparierte Liste, die angibt, welche Mesh-Gruppen-IDs akzeptiert werden. Eine Anfrage von einer Gruppen-ID, die nicht unter diesem Punkt aufgeführt ist, wird verworfen.

Administrative Distanz

Die Distanz, mit der die über den Mesh-Tunnel erhaltenen Routen beim IP-Router eingetragen werden. Der Sonderwert „0“ ist gleichbedeutend mit dem internen Default von „15“.

Initiale Ratenlimitierung

Um das Netzwerk zu schonen, werden angeforderte Netze (Adressen) mit einer zeitlichen Sperre versehen. Hier wird die initiale Sperrzeit in Sekunden angegeben.

Max. Ratenlimitierung

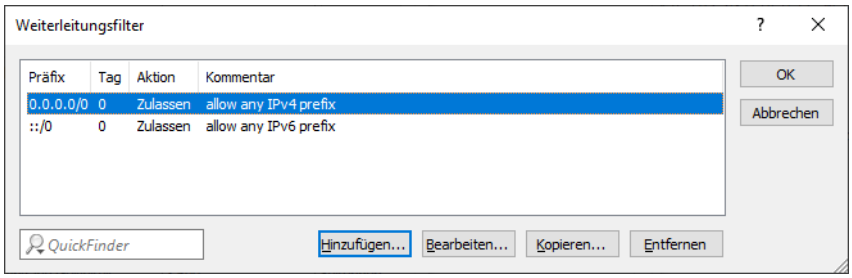
Die Sperrzeit aus der **Initialen Ratenlimitierung** wird jeweils verdoppelt, bis die **Maximale Ratenlimitierung** erreicht wird.

Anfrage Gültigkeit

Nach Ablauf der Sperrzeit werden bereits angefragte Netze (Adressen) weiter vorgehalten. Diese Gültigkeit beginnt immer mit Ablauf der Sperre und bricht ab, wenn das Gerät einen Request für dieses Netzwerk (diese Adresse) sendet oder empfängt.

Weiterleitungsfilter

Mithilfe dieser Filterliste können Anfragen an bestimmte Netzwerke auf dem Hub gefiltert werden. Wenn das angefragte Netzwerk aus einer Mesh-Nachricht mit keiner Tabellenzeile übereinstimmt, wird die Anfrage durchgelassen (Allow-All).



Präfix

Definiert das Präfix, für das eine Regel gelten soll, z. B. 10.0.0.0/24 oder 2001:db8::/32.

Tag

Definiert das zugehörige Routing Tag bzw. den Routing-Kontext zu dem die Filterregel gehört.

Aktion

Definiert die Aktion für diesen Filtereintrag. Mögliche Werte: Zulassen, Ablehnen.

Kommentar

Vergeben Sie diesem Eintrag einen aussagekräftigen Kommentar.

Tutorial: Einrichtung von Advanced Mesh VPN

Ausgangsszenario: Das Szenario besteht aus zwei Filialen (A und B) mit öffentlichen IPv4-Adressen sowie einer Zentrale, ebenfalls mit einer öffentlichen IPv4-Adresse. Die beiden Filialen haben bereits einen statischen IKEv2-VPN-Tunnel zur Zentrale eingerichtet, der aufgebaut ist. Die VPN-Gegenstelle auf den Filialen heißt jeweils „ZENTRALE". Filiale A hat das Subnetz 192.168.1.0/24 und Filiale B das Subnetz 192.168.2.0/24 mit dem Namen „INTRANET".

Konfiguration der Filiale A

1. Legen Sie einen neuen Eintrag, z. B. „MESH-TEMPLATE", in der IKEv2-Verbindungsliste unter **VPN** > **IKEv2 / IPSec** > **Verbindungs-Liste** an.

   Dieser Eintrag dient als Vorlage, aus der die dynamischen Mesh-Tunnel ihre Parameter übernehmen.

2. Als **Haltezeit** wird die Zeit konfiguriert, nach der die Mesh-VPN-Tunnel ohne Datenverkehr getrennt werden sollen, z. B. 300 Sekunden.

   Eine Deaktvierung der Haltezeit über den Wert 0 wird nicht empfohlen, da dynamische Mesh-VPN-Tunnel niemals bei Inaktivität abgebaut werden und Lizenzen verbrauchen.

3. Das **entfernte Gateway** muss leer gelassen werden, da es dynamisch bestimmt wird.

4. Über den Parameter **Routing** wird das lokale Netz an die gegenüberliegende Filiale übertragen, in diesem Fall das Netz „INTRANET". Legen Sie dazu in der Tabelle **IPv4-Routing** unter **VPN** > **IKEv2 / IPSec** > **Erweiterte Einstellungen** einen neuen Eintrag an. Wählen Sie z. B. als Name „INTRANET-ROUTING" und wählen Sie im Feld **Netzwerk** das lokale Netzwerk aus, das für Mesh VPN verwendet werden soll, z. B. „INTRANET".

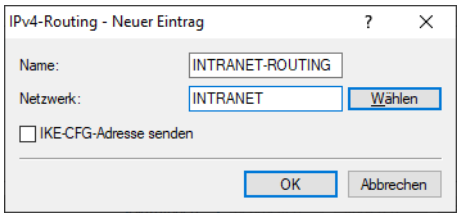


Abbildung 10: Beispiel für den IPv4-Routing-Eintrag

5. Wählen Sie unter **Authentifizierung** die Option **Quelle verwalten** aus. Erzeugen Sie einen neuen Eintrag, z. B. „MESH". Geben Sie die **lokale Identität** der Filiale an, sowie den **PSK**, der für alle dynamischen Mesh-Tunnel verwendet wird. Der PSK muss auf allen beteiligten Filialen für den Mesh-VPN-Tunnel identisch sein. Dieser wird dann im Feld **Entferntes Passwort** eingetragen. Lassen Sie das Feld **entfernte Identität** leer und wählen Sie die

Option „Keine Identität“ für **entfernter Identitätstyp**, so dass alle ankommenden Identitäten mit dem korrekten PSK als Mesh-Tunnel akzeptiert werden.

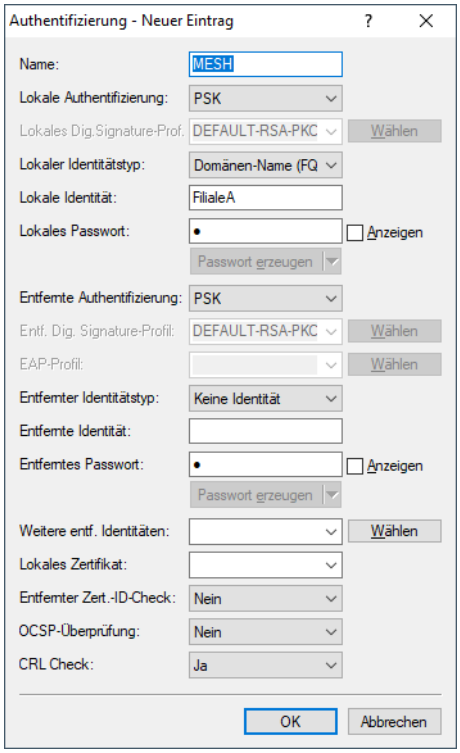


Abbildung 11: Beispiel für die Authentifizierungs-Einstellungen

6. Setzen Sie die **VPN-Regel** auf „ANY“ bzw. wählen Sie für **IPv4-Regeln** den Eintrag „RAS-WITH-NETWORK-SELECTION“. Somit wird 0.0.0.0/0 <=> 0.0.0.0/0 verwendet.
7. Setzen Sie die **Regelerzeugung** auf „Manuell“.

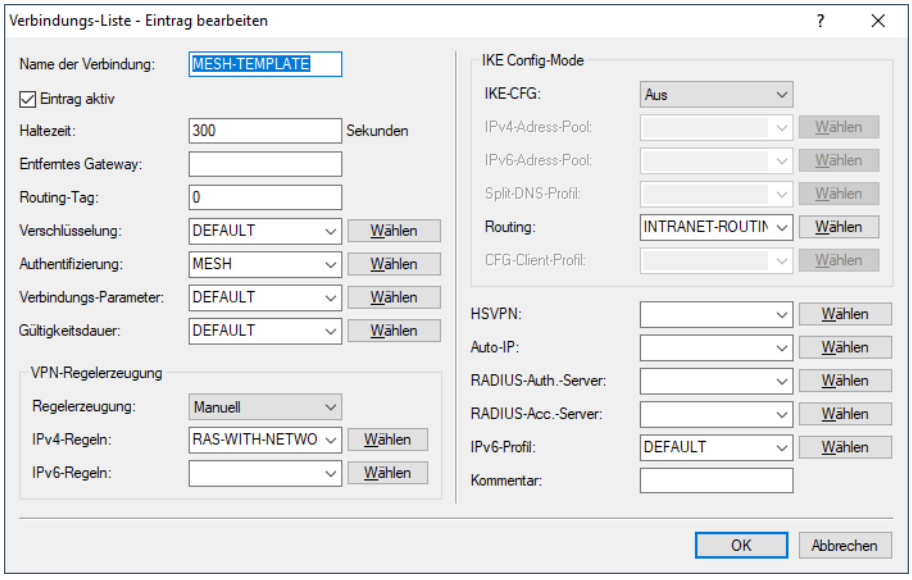


Abbildung 12: Beispiel für das Mesh-VPN-Template in der Verbindungs-Liste

8. Konfigurieren Sie nun die Mesh-VPN-Parameter unter **VPN** > **IKEv2 / IPSec** > **Erweiterte Einstellungen** > **Advanced Mesh VPN**.

9. Setzen Sie die **Betriebsart** auf „Spoke“.
10. Wählen Sie unter **VPN-Gegenstellen-Vorlage** die zuvor angelegte IKEv2-Gegenstelle als Vorlage für die Mesh-VPN-Tunnel aus.
11. Wählen Sie unter **Detektiere auf VPN-Gegenstelle** den Namen der VPN-Gegenstelle aus, der dem Namen des Tunnels zur Zentrale entspricht.

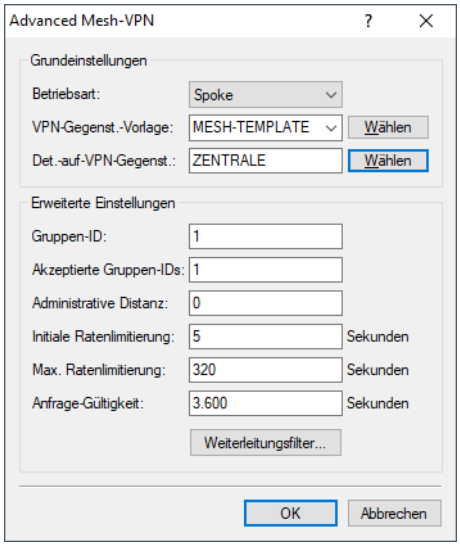


Abbildung 13: Beispiel für die Advanced Mesh VPN-Einstellungen in der Filiale

Konfiguration der Filiale B

12. Die Konfiguration erfolgt analog zur Filiale A. Ändern Sie die **lokale Identität** bei der **Authentifizierung**entsprechend auf den Namen der Filiale B.

Konfiguration der Zentrale

13. Da die Zentrale selbst keine dynamischen Mesh-Tunnel aufbaut, wird auch keine Gegenstellen-Vorlage angelegt. Setzen Sie die **Betriebsart** bei Advanced Mesh VPN auf „Hub“.

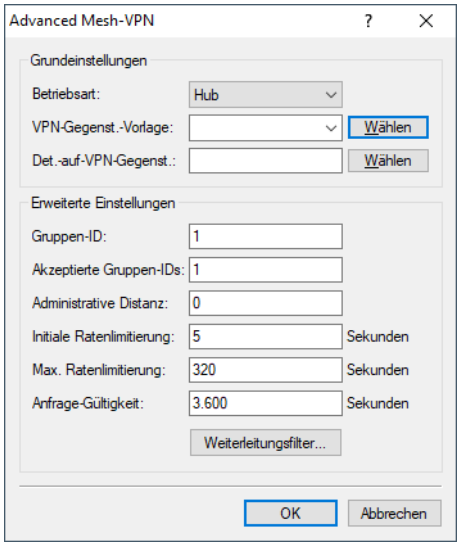


Abbildung 14: Beispiel für die Advanced Mesh VPN-Einstellungen in der Zentrale

Wenn Sie nun Daten von der Filiale A an Filiale B übertragen, so gehen die ersten Pakete über den Umweg der Zentrale. Daraufhin wird der dynamische Mesh-Tunnel zwischen den Filialen aufgebaut.

Ein Ping auf die IP-Adresse des Routers der gegenüberliegenden Seite wird keinen Mesh-Tunnel aufbauen. Es muss eine (ggf. nichtexistierende) Station im LAN der anderen Seite als Ziel verwendet werden.

11.19.1.11 IKEv2 Load-Balancer

Der IKEv2 Load-Balancer ermöglicht es, eingehende IKEv2-Verbindungen abhängig von momentaner Auslastung / Anzahl VPN-Tunnel etc. sinnvoll auf andere Gateways zu verteilen. Um dies zu erreichen wird der IKEv2 Redirect Mechanismus verwendet.

In größeren VPN-Szenarien werden in der Regel redundante VPN-Gateways verwendet. Oft werden davon allerdings nicht alle Gateways gleichmäßig genutzt bzw. manche Gateways werden als Reserve für den Backup-Fall vorgehalten. Dies führt zu einer ungleichmäßigen Ressourcen-Auslastung der Gesamtinstallation.

Werden mehrere VPN-Gateways genutzt, so müssen diese Gateways auf allen Clients konfiguriert werden. Soll insbesondere ein neues VPN-Gateway installiert werden, so muss dieses Gateway auf allen Clients nachträglich konfiguriert werden. IKEv2 bietet mit dem Redirect-Mechanismus (RFC 5685) eine Erweiterung bei der ein VPN-Gateway einen Client auf ein anderes Gateway umleiten bzw. weiterleiten kann.

Auf Basis des IKEv2- Redirect-Mechanismus kann im Zusammenspiel mit VRRP ein hochverfügbarer IKEv2 Load-Balancer für Enterprise-Szenarien erreicht werden.

Im ersten Schritt wird ein VRRP-Verbund auf allen beteiligen VPN-Gateways aktiviert. Die virtuelle VRRP-IP-Adresse ist gleichzeitig die Master-IP-Adresse des IKEv2-Load-Balancer-Verbundes. Die VPN-Gateways tauschen nun durch regelmäßige Status-Nachrichten per Multicast Informationen über ihre Last bzw. ihre Verfügbarkeit aus. Sollte der Master ausfallen, so wird automatisch ein anderes VPN-Gateway zum Master gewählt.

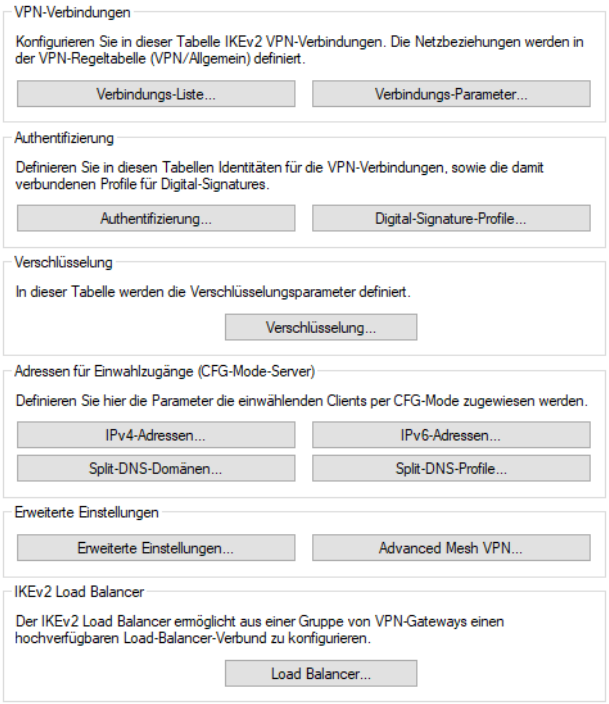
Auf den Clients wird nur noch die Master-IP-Adresse konfiguriert. Baut nun ein Client eine VPN-Verbindung zu dieser IP-Adresse auf, so prüft das Master Gateway die Last der VPN-Gateways und leitet den Client auf das Gateway mit der geringsten Last um. Dabei schickt das Master Gateway entweder ein Redirect in der IKE_SA_INIT-Antwort oder in der IKE-Auth-Phase. Die Umleitungsentscheidung wird anhand der freien VPN-Tunnel der beteiligen Gateways getroffen. Dabei wird der VPN-Client auf das VPN-Gateway mit der niedrigsten Anzahl an aktiven Tunneln umgeleitet.

Die virtuelle Gateway-Adresse dient somit nur für den ersten Kontakt mit anschließendem Redirect. Der Client baut dann den eigentlichen VPN-Tunnel zu einer anderen Gateway-Adresse auf.

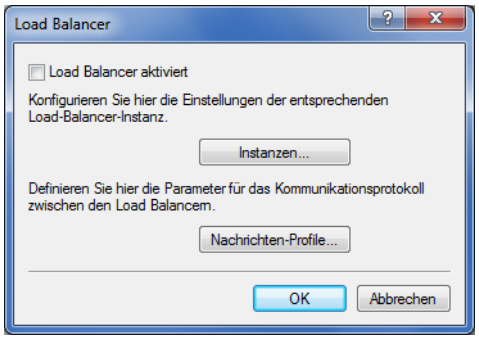
Folgende Randbedingungen sind zu beachten:

- VRRP wird für die automatische Wahl des Master-Gateways benötigt.
- Die beteiligten VPN-Gateways müssen eine gemeinsame Layer-2 Verbindung für VRRP und dem Austausch von Status-Nachrichten per Multicast haben.
- VRRP wird aktuell nur auf LAN-Schnittstellen unterstützt.
- Es wird ein vorgeschalteter Router (ggf. ebenfalls redundant ausgelegt) für den WAN-Zugang benötigt.
- Der Client muss IKEv2-Gateway Redirect nach RFC 5685 unterstützen (gilt aktuell für LANCOM Router und den LANCOM Advanced VPN-Client unter Windows).

In **LANconfig** konfigurieren Sie den IKEv2 Load-Balancer unter **VPN** > **IKEv2/IPSec** > **IKEv2 Load Balancer**



im Menü **Load Balancer**.

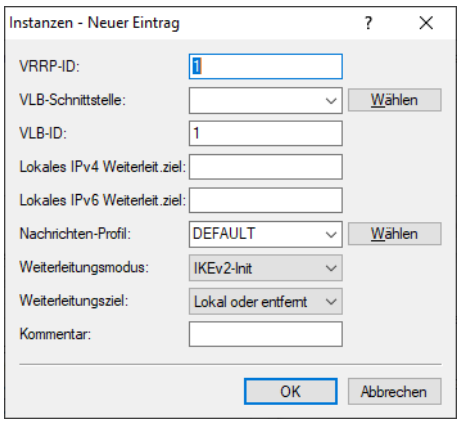


Load Balancer aktiviert

Aktiviert den IKEv2 Load-Balancer.

Instanzen

IKEv2 Load-Balancer-Instanzen konfigurieren Sie in der Tabelle **Instanzen**.



VRRP-ID

VRRP-ID (Router-ID), die für diese IKEv2 Load-Balancer-Instanz verwendet werden soll. VRRP muss dazu auf diesem Gerät aktiviert und für diese VRRP-ID konfiguriert sein.

Mögliche Werte:

0 bis 255

Default: 1

VLB-Schnittstelle

Definiert die Schnittstelle bzw. das logische Netzwerk auf dem der IKEv2-Loadbalancer VPN-Tunnel annehmen soll. Auf dieser Schnittstelle muss ebenfalls VRRP konfiguriert bzw. aktiv sein.

VLB-ID

Definiert die eindeutige Kennung der Load-Balancer-Instanz. Default: 1

Lokales IPv4 Weiterleitungsziel

IPv4-Adresse oder FQDN, auf dem das Gerät VPN-Tunnel annehmen soll. Auf diese Adresse wird ein VPN-Client durch den Master im Load-Balancer-Verbund weitergeleitet.

Hierbei handelt es sich nicht um die virtuelle VRRP-IP-Adresse.

Lokales IPv6 Weiterleitungsziel

Globale IPv6-Adresse oder FQDN, auf dem das Gerät VPN-Tunnel annehmen soll. Auf diese Adresse wird ein VPN-Client durch den Master im Load-Balancer-Verbund weitergeleitet. Link-Lokale Adressen werden nicht unterstützt.

Hierbei handelt es sich nicht um die virtuelle VRRP-IP-Adresse.

Nachrichten-Profil

Nachrichten-Profil, das für diese Instanz verwendet werden soll. Das Nachrichten-Profil enthält die Parameter für das Status-Protokoll, mit dem das Gerät seine Status-Informationen an den Load-Balancer-Verbund kommuniziert.

Default: DEFAULT.

Falls hier eine IPv6-Adresse konfiguriert wird, dann muss ebenfalls die IPv6-Firewall-Regel ALLOW_VLB aktiviert werden.

Weiterleitungsmodus

Definiert, in welcher Phase der IKEv2-Verhandlung das VPN-Gateway Clients auf ein anderes Gateway weiterleitet.

Dieser Parameter ist nur wirksam, falls das Gerät VRRP-Master ist.

Mögliche Werte:

IKEv2-Init (Default)

Die Redirect-Nachricht wird innerhalb der IKE_SA_INIT Antwort des VPN-Gateways gesendet.

IKEv2-Auth

Die Redirect-Nachricht wird innerhalb der IKE_AUTH-Phase gesendet, nachdem der Client sich beim VPN-Gateway identifiziert hat.

Weiterleitungsziel

Definiert das Weiterleitungsziel an das VPN-Clients weitergeleitet werden.

Der Parameter ist nur wirksam, falls das Gerät VRRP-Master ist.

Mögliche Werte:

Lokal oder entfernt

Clients werden sowohl auf die eigene IP-Adresse des Geräts als auch auf andere entfernte Gateways des Verbunds umgeleitet.

Nur entfernt

Clients werden nur auf andere VPN-Gateways weitergeleitet. Dies führt dazu, dass VPN-Clients gleichmäßig auf alle anderen Gateways mit Ausnahme des Master Gateways umgeleitet werden.

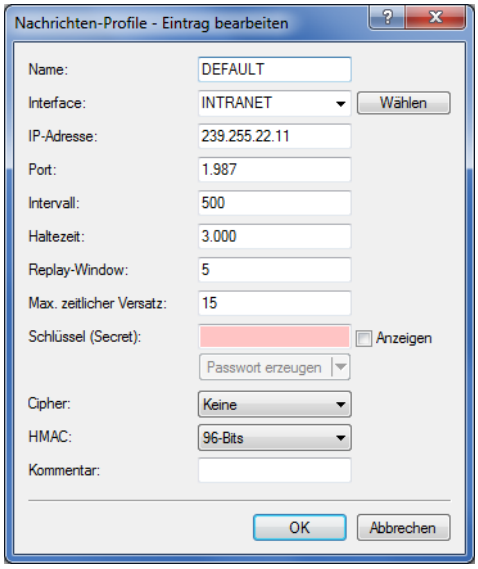
Hiermit lassen sich Szenarien konfigurieren, in denen der Load-Balancer-Master nur Clients verteilt, aber selbst keine VPN-Tunnel terminiert.

Kommentar

Geben Sie eine aussagekräftige Beschreibung für diesen Eintrag an.

Nachrichten-Profile

Die Tabelle **Nachrichten-Profile** enthält die Parameter für das Status-Protokoll, mit dem VPN-Gateways ihre Status-Informationen an den Load-Balancer-Verbund kommunizieren.



Name

Eindeutiger Name für dieses Profil

Interface

Interface, auf dem der IKEv2 Load-Balancer Statusnachrichten mit anderen VPN-Gateways des Verbunds austauscht.

Mögliche Werte sind alle Einträge aus der Tabelle IPv4-Netzwerke

IP-Adresse

Definiert die Multicast IP-Adresse zur Kommunikation der IKEv2 Load-Balancer im lokalen Netzwerk.

Default: 239.255.22.11

Port

Definiert den Port zur Kommunikation der IKEv2 Load-Balancer im lokalen Netzwerk.

Default: 1987

Intervall

Intervall (in Millisekunden), in dem Status-Nachrichten zwischen den IKEv2 Load-Balancern ausgetauscht werden.

Mögliche Werte:

0 bis 65535

Default: 500

Haltezeit

Definiert die Zeit in Millisekunden, nach der das Gerät von anderen IKEv2 Load-Balancern bei ausbleibenden Status-Nachrichten als deaktiviert vermerkt wird.

Die Haltezeit muss größer als das Intervall sein. Empfohlen wird der mindestens dreifache Wert des Parameters **Intervall**.

Mögliche Werte:

0 bis 65535

Default: 3000

Replay Window

Größe des Replay Windows (Anzahl Nachrichten) für Status-Nachrichten der IKEv2 Load-Balancer. Nachrichten, die nicht mehr in das Replay Windows passen, werden bei Empfang verworfen.

Mögliche Werte:

1 bis 9

Default: 5

0

Deaktiviert die Replay Detection.

Max. zeitlicher Versatz

Maximal erlaubte zeitliche Abweichung (in Sekunden) der Zeitstempel in Status-Nachrichten der IKEv2 Load-Balancer. Nachrichten mit einer höheren Abweichung werden bei Empfang verworfen.

Mögliche Werte:

0 bis 255

Default: 15

Schlüssel

Gemeinsames Passwort für das Kommunikationsprotokoll der Load-Balancer.

Das Passwort muss auf allen VPN-Gateways eines Verbundes identisch sein.

Mögliche Werte:

Bis zu 32 beliebige Zeichen

Cipher

Definiert den verwendeten Verschlüsselungsalgorithmus für Status-Nachrichten der IKEv2 Load-Balancer.

Mögliche Werte:

Keine (Default)

AES-128-GCM

AES-192-GCM

AES-256-GCM

HMAC

Definiert den verwendeten Signierungsalgorithmus für Status-Nachrichten der IKEv2 Load-Balancer.

Mögliche Werte:

Keine

96 Bits (Default)

128 Bits

Kommentar

Geben Sie eine aussagekräftige Beschreibung für diesen Eintrag an.

11.19.2 Zwei-Faktor-Authentifizierung im VPN

Ab LCOS 10.70 unterstützt LCOS die VPN-Zwei-Faktor-Authentifizierung (EAP-OTP) mit dem LANCOM Advanced VPN Client. Dazu kann der interne RADIUS-Server OTP-Benutzer verwalten.

Der VPN-Benutzer hat neben seinem normalen VPN-Benutzernamen und Passwort (EAP-MSCHAPv2) eine Authenticator-App z. B. auf seinem Smartphone, auf der ein zweiter Faktor generiert wird und zusätzlich zum Benutzernamen / Passwort verwendet wird. Zwei-Faktor-Authentifizierung ist bei IKEv2 laut RFC nur mit EAP möglich, so dass einfache PSK oder RSA-Signature-Verfahren nicht verwendet werden können. LCOS unterstützt eine herstellerspezifische Implementierung zusammen mit dem LANCOM Advanced VPN Client.

Als Authenticator können beliebige Apps verwendet werden, z. B. von Google, Microsoft oder NCP. Diese Apps finden Sie im Appstore Ihres mobilen Geräts.

Die Vorgehensweise zur Einrichtung ist wie folgt: Zunächst muss EAP-VPN mit IKEv2 im LANCOM Gerät konfiguriert werden. Dazu wird der interne RADIUS-Server mit seinen Benutzerkonten verwendet. Zusätzlich zu einem RADIUS-Benutzerkonto muss ein OTP-Benutzer anlegt werden. Im Anschluss kann in der WEBconfig unter **Extras** > **EAP-OTP-Benutzer** ein QR-Code abgerufen werden, der von der Authenticator-App eingescannt werden muss. Dieser QR-Code gilt pro Benutzer und muss jedes Mal verwendet werden, wenn eine Authenticator-App eingerichtet werden soll. Die WEBconfig generiert aus den Parametern der Tabelle **OTP-Benutzerkonten** einen QR-Code pro Benutzer der

von Authenticator-Apps eingescannt werden kann. Alternativ kann in den meisten Apps der Schlüssel manuell hinzugefügt werden.

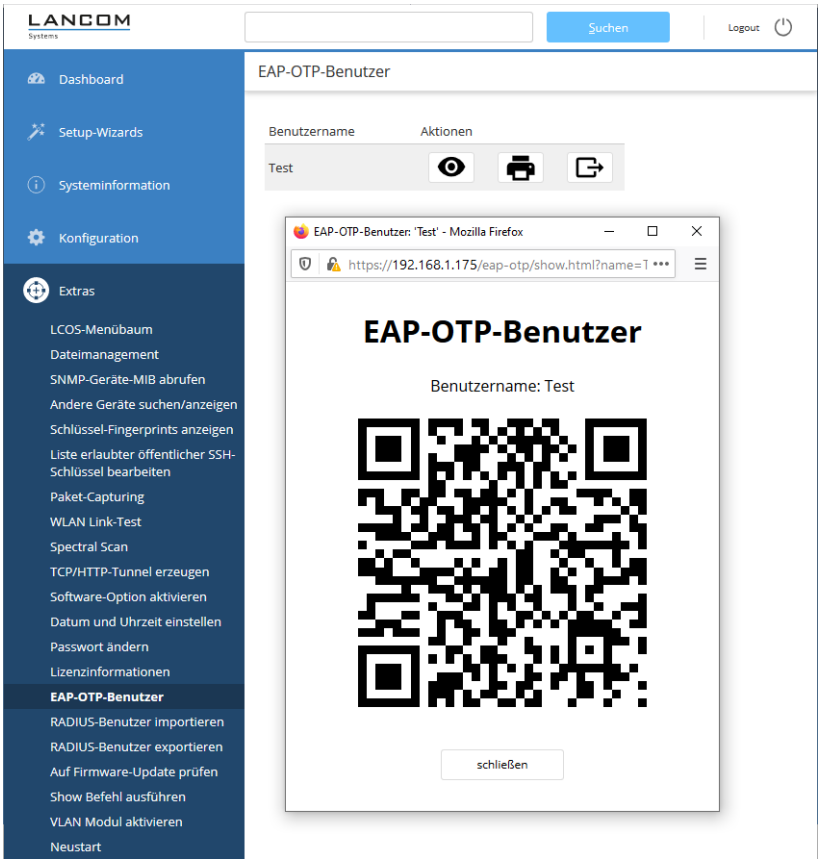


Abbildung 15: WEBconfig: Extras > EAP-OTP-Benutzer

Eine Anleitung zur Einrichtung des gesamten Szenarios finden Sie in der *LANCOM Support Knowledge Base*.

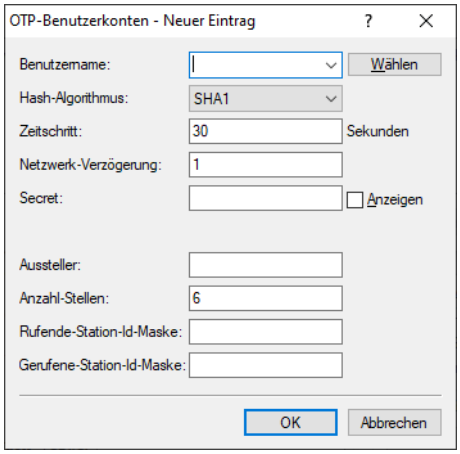
Bitte beachten Sie, dass für eine korrekte zeitliche Synchronisierung mit dem Authenticator der Router über die aktuelle Uhrzeit verfügen muss. Aktivieren Sie dazu den NTP-Client im Router unter **Datum/Zeit** > **Synchronisierung** > **NTP-Client-Einstellungen**.

11.19.2.1 Konfiguration mit LANconfig

OTP-Benutzerkonten

In der Tabelle OTP-Benutzerkonten werden die OTP-Benutzer definiert. Für EAP-OTP muss der Benutzer mit seinem normalen Passwort in der Tabelle der *RADIUS-Benutzerkonten* angelegt werden, sowie zusätzlich in dieser Tabelle mit dem OTP-Secret angelegt werden.

Die Konfiguration der OTP-Benutzerkonten erfolgt über **RADIUS** > **Server** > **Benutzer-Datenbank** > **OTP-Benutzerkonten**.



Benutzername

Geben Sie hier den Namen des OTP-Benutzers ein. Dieser muss in der Tabelle RADIUS-Benutzerkonten bereits mit gleichem Namen enthalten sein.

Hash-Algorithmus

Definiert den verwendeten Hash-Algorithmus.

Beachten Sie, dass die Authenticator-App den maximal möglichen Hash-Algorithmus unterstützt. Der Google Authenticator unterstützt aktuell z. B. auf bestimmten Android-Plattformen nur SHA1.

Zeitschritt

Definiert das Intervall in Sekunden, nach dem ein neues OTP berechnet wird. Default: 30 Sekunden

Netzwerk-Verzögerung

Definiert, um wie viele Zeitschritte die Uhr des Clients maximal abweichen darf. Der RADIUS-Server prüft das um diesen Wert ältere bzw. neuere OTP.

Secret

Definiert das eigentliche Shared Secret, das mit der Authenticator-App geteilt werden muss. Das Secret muss für jeden Benutzer unterschiedlich sein. Es gibt aktuell in der Tabelle drei Eingabemöglichkeiten:

Base32 (Default)

Präfix „base32:“ und danach das Base32-kodierte Secret. Der Präfix „base32:“ darf auch weggelassen werden.

Hexadezimal

Präfix „hex:“ und danach eine gerade Anzahl von Hex-Digits.

Plain text passphrase

Präfix „ascii:“ und danach die Zeichen.

Für den Google Authenticator muss das Secret 16 Zeichen (80 Bit, Base32 codiert) lang sein, z. B. E3U5IDWEE3KFCJ7G

Aussteller

Frei definierbarer Text, der im Authenticator dazu dient, mehrere Schlüssel auseinanderzuhalten, wenn der gleiche Benutzername verwendet wird. Darf keinen Doppelpunkt enthalten.

Anzahl Stellen

Länge der OTPs. Default: 6.

Für den Google-Authenticator sollte der Wert 6 verwendet werden.

Rufende Station

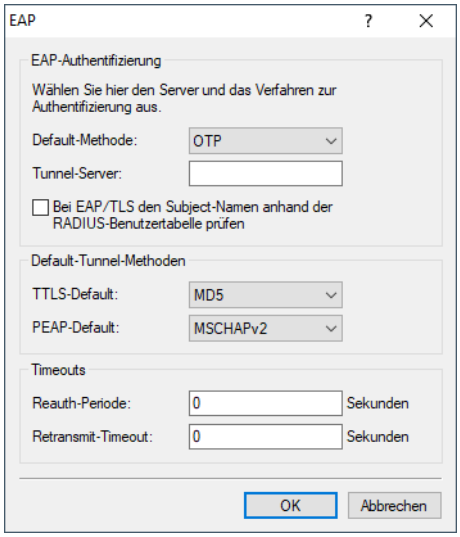
Diese Maske schränkt die Gültigkeit des Eintrags auf bestimmte IDs ein, die die rufende Station übermittelt.

Gerufene Station

Diese Maske schränkt die Gültigkeit des Eintrags auf bestimmte IDs ein, die die gerufene Station übermittelt.

EAP-OTP

RADIUS > **Server** > **Erweiterte Einstellungen** > **EAP**



Die **Default-Methode** wurde um den Wert OTP erweitert.

OTP

One Time Password. Dieser Wert muss bei EAP-OTP für die *Zwei-Faktor-Authentifizierung im VPN* verwendet werden, da beim LANCOM Advanced VPN-Client die EAP-Methode vom EAP-Server vorgegeben wird.

11.19.3 RADIUS-Unterstützung für IKEv2

LCOS ermöglicht es, die IKEv2-Konfiguration für Autorisierung und Accounting von VPN-Peers durch einen externen RADIUS-Server durchführen zu lassen. Außerdem ist die Verwaltung der VPN-Clients für das dynamische IKEv2-Load-Balancing über RADIUS realisiert.

In mittleren bis großen VPN-Szenarien sind die Tabellen für VPN-Konfigurationen in der Regel sehr umfangreich und komplex. Wenn mehrere VPN-Gateways aus Redundanzgründen zum Einsatz kommen, muss sichergestellt werden, dass die Konfiguration auf allen VPN-Gateways identisch ist.

Der Einsatz eines zentralen RADIUS-Servers ermöglicht die fast vollständige Auslagerung der Konfiguration der VPN-Parameter vom VPN-Gateway auf einen oder mehrere RADIUS-Server. Sobald eine VPN-Gegenstelle eine VPN-Verbindung zum Gerät aufbauen will, versucht das Gerät, die ankommende Verbindung per RADIUS zu authentifizieren und weitere notwendige Verbindungsparameter wie z. B. VPN-Netzbeziehungen, CFG-Mode-Adresse oder DNS-Server vom RADIUS-Server abzurufen. Dabei wird der Benutzer nicht vom RADIUS-Server anhand des Benutzernamens/Passworts freigeschaltet, sondern dieser liefert dem VPN-Gateway das richtige Passwort für den angefragten Benutzer und dieser

wird dann durch den VPN-Gateway selbst freigeschaltet. Der VPN-Gateway baut dann den Tunnel komplett auf, wobei der RADIUS-Server hier dem VPN-Tunnel weitere Attribute übergeben kann.

Dabei kann die VPN-Konfiguration entweder vollständig oder nur teilweise vom RADIUS-Server abgerufen mit lokal vorhandenen Parametern kombiniert werden. Dieser Mechanismus funktioniert nur für ankommende Verbindungen.

Durch das optionale RADIUS-Accounting können Informationen über VPN-Verbindungen zentral auf einem RADIUS-Server gesammelt werden. Diese Informationen können z. B. aus Verbindungsdauer des Clients, Aufbauzeitpunkt oder das übertragene Datenvolumen bestehen.

Die Konfiguration der RADIUS-Server erfolgt in LANconfig unter **VPN** > **IKEv2/IPSec** > **Erweiterte Einstellungen**.

RADIUS-Autorisierung

Das LANCOM-Gateway überträgt bei der Anmeldung eines VPN-Peers die folgenden RADIUS-Attribute im `Access-Request` an den RADIUS-Server:

ID	Bezeichnung	Bedeutung
1	User-Name	Die Remote-ID des VPN-Peers, wie er sie in der `AUTH`-Verhandlung mit dem LANCOM-Gateway überträgt.
2	User-Passwort	Das Dummy-Passwort, wie es in LANconfig unter **VPN** > **IKEv2/IPSec** > **Erweiterte Einstellungen** > **Passwort** konfiguriert ist.
4	NAS-IP-Address	Gibt die IPv4-Adresse des Gateways an, das den Zugang für einen Anwender anfragt. Erfolgt die Verbindung über eine IPv6-Verbindung, überträgt das Gateway stattdessen das Attribut „95“ (siehe unten).
6	Servcie-Type	Der Service-Type ist immer „Outbound (5)“ bzw. „Dialout-Framed-User“.
31	Calling-Station-Id	Gibt die ID (als IPv4- oder IPv6-Adresse) der rufenden Station an (z. B. des VPN-Clients).
95	NAS-IPv6-Address	Gibt die IPv6-Adresse des Gateways an, das den Zugang für einen Anwender anfragt. Erfolgt die Verbindung über eine IPv4-Verbindung, überträgt das Gateway stattdessen das Attribut „4“ (siehe oben).

Von den in der `Access-Accept`-Antwort des RADIUS-Servers enthaltenen Attributen wertet das LANCOM-Gateway daraufhin die folgenden, teils vendor-spezifischen Attribute aus:

ID	Bezeichnung	Bedeutung
8	Framed-IP-Address	IPv4-Adresse für den Client (im IKE-CFG-Mode „Server“).
9	Framed-IP-Netmask	Gibt die IP-Netzmaske an, die für den Client zu konfigurieren ist (im IKE-CFG-Mode „Server“). Dieser Attributwert führt dazu, dass eine statische Route für die Framed-IP-Adresse mit der angegebenen Maske hinzugefügt wird.
22	Framed-Route	IPv4-Routen, die in Richtung des Clients (Next-Hop-Client) auf dem VPN-Gateway in der Routing-Tabelle eingetragen werden sollen. Format (String): <Präfix> [ifc=<Zielinterface>] [rtg_tag=<Routing-Tag>] [admin_distance=<Distanz>] **<Präfix>** IPv4-Adresse + '/' + Präfixlänge oder Netzmaske

ID	Bezeichnung	Bedeutung
		ifc=<Zielinterface> Name des IP-Interfaces oder eines Load-Balancers, auf den die Route zeigen soll, oder „#Ifc". Wenn kein Zielinterface angegeben ist oder es „#Ifc" lautet, dann zeigt die Route auf das VPN-Interface für den betreffenden Einwahlclient. Der Interfacename kann bis zu 16 Zeichen enthalten. **rtg_tag=<Routing-Tag>** Routing-Tag für die Route. Wenn es nicht angegeben wird, bekommt die Route das Tag des Einwahlinterfaces. **admin_distance=<Distanz>** Administrative Distanz der Route als Zahl von 0 bis 255. Wenn sie nicht angegeben wird, bekommt die Route die standardmäßige Distanz für VPN-Routen.
69	Tunnel-Password	Setzt bei Verwendung von synchronen PSKs die Passwörter der lokalen und der entfernten Identität auf den selben Wert.
88	Framed-Pool	Name des IPv4-Adressen-Pools, aus dem der Client die IP-Adresse und den DNS-Server bezieht. Die Werte in „Framed-IP-Address" und „LCS-DNS-Server-IPv4-Address" haben gegenüber diesem Attribut Vorrang.
99	Framed-IPv6-Route	IPv6-Routen, die in Richtung des Clients (Next-Hop-Client) auf dem VPN-Gateway in der Routing-Tabelle eingetragen werden sollen. Format (String): <Präfix> [ifc=<Zielinterface>] [rtg_tag=<Routing-Tag>] [admin_distance=<Distanz>] **<Präfix>** IPv6-Adresse + '/' + Präfixlänge **ifc=<Zielinterface>** Name des IP-Interfaces oder eines Load-Balancers, auf den die Route zeigen soll, oder „#Ifc". Wenn kein Zielinterface angegeben ist oder es „#Ifc" lautet, dann zeigt die Route auf das VPN-Interface für den betreffenden Einwahlclient. Der Interfacename kann bis zu 16 Zeichen enthalten. **rtg_tag=<Routing-Tag>** Routing-Tag für die Route. Wenn es nicht angegeben wird, bekommt die Route das Tag des Einwahlinterfaces.

ID	Bezeichnung	Bedeutung
		admin_distance=<Distanz> Administrative Distanz der Route als Zahl von 0 bis 255. Wenn sie nicht angegeben wird, bekommt die Route die standardmäßige Distanz für VPN-Routen.
168	Framed-IPv6-Address	IPv6-Adresse für den Client (im IKE-CFG-Mode „Server“).
169	DNS-Server-IPv6-Address	IPv6-DNS-Server für den Client (im IKE-CFG-Mode „Server“).
172	Stateful-IPv6-Address-Pool	Name des IPv6-Adressen-Pools (im IKE-CFG-Mode „Server“).
LANCOM 19	LCS-IKEv2-Local-Password	Lokaler IKEv2-PSK
LANCOM 20	LCS-IKEv2-Remote-Password	Entfernter IKEv2-PSK
LANCOM 21	LCS-DNS-Server-IPv4-Address	IPv4-DNS-Server für den Client (im IKE-CFG-Mode „Server“)
LANCOM 22	LCS-VPN-IPv4-Rule	Beinhaltet die IPv4-Netzwerkregeln (Beispiele: siehe unten)
LANCOM 23	LCS-VPN-IPv6-Rule	Beinhaltet die IPv6-Netzwerkregeln (Beispiele: siehe unten)
LANCOM 24	LCS-Routing-Tag	Routing-Tag, das für den Client konfiguriert werden soll (IPv4/IPv6).
LANCOM 25	LCS-IKEv2-IPv4-Route	Routen in Präfix-Schreibweise (z. B. „192.168.1.0/24“), die das LANCOM-Gateway per `INTERNAL_IP4_SUBNET` an den Client übertragen soll. Die Auswertung von mehreren Attributen ist möglich.
LANCOM 26	LCS-IKEv2-IPv6-Route	Routen in Präfix-Schreibweise (z. B. „2001:db8::/64“), die das LANCOM-Gateway per `INTERNAL_IP6_SUBNET` an den Client übertragen soll. Die Auswertung von mehreren Attributen ist möglich.
LANCOM 27	LCS-IKEv2-DNS-Domain	Split-DNS-Domains (Liste), die das Gateway per Attribut `INTERNAL_DNS_DOMAIN` im IKE-CFG-Mode „Server“ an den Client übertragen soll, z. B. `mydomain.intern, example.com`.
LANCOM 28	LCS-Load-Balancer	Format (String): <Load-Balancer-Name> [client_binding={no|yes}] Der <Load-Balancer-Name> kann bis zu 16 Zeichen lang sein und gibt eine entsprechende Load-Balancing-Gegenstelle auf den LANCOM Routern an. Diese Gegenstelle wird für das dynamische IKEv2-VPN-Load-Balancing verwendet und darf daher nicht unter **IP-Router** > **Load Balancing** bereits für statisches Load-Balancing verwendet werden. Die Option „client_binding“ schaltet das Client Binding (siehe *Client-Binding* auf Seite 430) ein oder aus. Ohne diese Angabe ist Client Binding aus. Der erste sich verbindende IKEv2-VPN-Client gibt diese Einstellung vor. Danach erfolgende andere Einstellungen für das Client Binding in Verbindung mit dieser Load-Balancing-Gegenstelle werden ignoriert.
LANCOM 29	LCS-IKEv2-Routing-Tag-List	Format (String): #, z. B. `0,3,7` Beinhaltet die Routing-Tags, die über HSVPN übertragen werden sollen.
LANCOM 30	LCS-IKEv2-IPv4-Tagged-Route	Format (String): <Präfix> rtg_tag=<Routing-Tag>

ID	Bezeichnung	Bedeutung
		<Präfix> HSVPN IPv4-Route die der CFG-Mode-Server im Rahmen des IKEv2-Routings an den Client übermittelt. **rtg_tag=<Routing-Tag>** Das hierbei verwendete Routing-Tag. Z. B. `192.168.1.0/24 rtg_tag=1` Ein Präfix mit Routing-Tag kann mehrfach im Attribut vorkommen und wird durch ein Komma getrennt.
LANCOM 31	LCS-IKEv2-IPv6-Tagged-Route	Format (String), <Präfix> rtg_tag=<Routing-Tag> **<Präfix>** HSVPN IPv6-Route die der CFG-Mode-Server im Rahmen des IKEv2-Routings an den Client übermittelt. **rtg_tag=<Routing-Tag>** Das hierbei verwendete Routing-Tag. Z. B. `2001:db8::/64 rtg_tag=1` Ein Präfix mit Routing-Tag kann mehrfach im Attribut vorkommen und wird durch ein Komma getrennt.
LANCOM 32	LCS-IPv6-Prefix-Length	Gibt die IPv6-Präfix-Länge an, die für den Client zu konfigurieren ist (im IKE-CFG-Mode „Server").
LANCOM 33	LCS-IKEv2-PPK	Gibt den Post-quantum Preshared Key als Zeichenkette oder Hexadezimalzahl (identifiziert durch ein führendes 0x) an.
LANCOM 34	LCS-IKEv2-PPK-MANDATORY	Gibt an, ob die Verwendung des übergebenen Post-quantum Preshared Key (PPK) gefordert wird. Falls ja, dann wird die entsprechende VPN-Verbindung abgelehnt, falls die Gegenseite kein PPK unterstützt oder konfiguriert hat. Wird die Verwendung von PPKs als optional konfiguriert, so werden sowohl Verbindungen mit PPK als auch ohne PPK akzeptiert.

Beispiel: RADIUS-Attribute für einen einfachen Loadbalancer aus IKEv2-VPN-Tunneln auf der Zentrale

```
LCS-Load-Balancer=LB1
Framed-Route=192.168.45.0/24 ifc=LB1;
```

Beipiele für Netzwerkregeln

Das Format für eine Netzwerkregel im Radius-Server gestaltet sich in der Form `<lokale Netze> * <entfernte Netze>`.

Die Einträge für `<Lokale Netze>` und `<entfernte Netze>` setzen sich dabei aus komma-separierten Listen zusammen.

Beispiel 1: `10.1.1.0/24,10.2.0.0/16 * 172.32.0.0/12`

Daraus ergeben sich die folgenden Netzwerkregeln:

- `10.2.0.0/255.255.0.0` <-> `172.16.200.0/255.255.255.255`
- `10.1.1.0/255.255.255.0` <-> `172.16.200.0/255.255.255.255`

Beispiel 2: `10.1.1.0/24 * 0.0.0.0/0`

Daraus ergibt sich die folgende Netzwerkregel:

- `10.1.1.0/255.255.255.0` <-> `0.0.0.0/0.0.0.0`

Dabei bedeutet `0.0.0.0/0` „ANY“, d. h. ein beliebiges Netz. `0.0.0.0/32` kann dazu verwendet werden, einen CFG-Mode-Client genau auf seine (noch unbekannte) Config-Mode-Adresse einzuschränken. Diese Adresse kommt z. B. aus einem Adress-Pool auf dem Gerät oder ebenfalls aus dem RADIUS-Server.

Beispiel 3: `2001:db8:1::/48 * 2001:db8:6::/48`

RADIUS-Accounting

Das LANCOM-Gateway zählt die übertragenen Datenpakete und -Oktette und sendet diese Daten regelmäßig als `Accounting-Request`-Nachrichtenan an den Accounting-RADIUS-Server. Der RADIUS-Server beantwortet diese Meldung daraufhin jeweils mit einer `Accounting-Response`-Nachricht.

Die `Accounting-Request`-Nachrichten besitzen die folgenden Status-Typen:

Start

Sobald sich ein VPN-Peer am LANCOM-Gateway anmeldet, startet das Gateway über IKEv2 eine Accounting-Session und sendet eine `Start`-Statusmeldung mit entsprechenden RADIUS-Attributen an den Accounting-RADIUS-Server.

Interim-Update

Während einer laufenden Accounting-Session sendet das Gateway in definierten Zeitabständen `Interim-Update`-Statusmeldungen an den Accounting-RADIUS-Server, der auch die `Start`-Statusmeldung als gültig beantwortet hat. Eventuell konfigurierte Backup-Server ignoriert das Gateway.

Stop

Nach dem Ende einer Sitzung sendet das LANCOM-Gateway eine `Stop`-Statusmeldung an den Accounting-RADIUS-Server. Auch diese Meldung sendet es nur an den Accounting-RADIUS-Server, der auch die `Start`-Statusmeldung als gültig beantwortet hat. Eventuell konfigurierte Backup-Server ignoriert das Gateway.

In der `Access-Request`-Meldung überträgt das Gateway die folgenden RADIUS-Attribute an den RADIUS-Server:

ID	Bezeichnung	Bedeutung	Status-Typ
1	User-Name	Die Remote-ID des VPN-Peers, wie er sie in der `AUTH`-Verhandlung mit dem LANCOM-Gateway überträgt.	› Start › Interim-Update › Stop

ID	Bezeichnung	Bedeutung	Status-Typ
4	NAS-IP-Address	Gibt die IPv4-Adresse des Gateways an, das den Zugang für einen Anwender anfragt. Erfolgt die Verbindung über eine IPv6-Verbindung, überträgt das Gateway stattdessen das Attribut „95“ (siehe unten).	› Start › Interim-Update › Stop
8	Framed-IP-Address	IPv4-Adresse des VPN-Clients.	› Start › Interim-Update › Stop
31	Calling-Station-Id	Gibt die ID (als IPv4- oder IPv6-Adresse) der rufenden Station an (z. B. des VPN-Clients).	› Start › Interim-Update › Stop
32	NAS-Identifier	Der Gerätename des Gateways.	› Start › Interim-Update › Stop
40	Acct-Status-Type	Beinhaltet den Status-Typ „Start“ (1).	› Start
40	Acct-Status-Type	Beinhaltet den Status-Typ „Interim-Update“ (3).	› Interim-Update
40	Acct-Status-Type	Beinhaltet den Status-Typ „Stop“ (2).	› Stop
42	Acct-Input-Octets	Enthält die Anzahl der aus Richtung VPN-Peer empfangenen Oktette. Der Wert bezieht sich auf die entschlüsselten Daten, beginnend mit dem IP-Header.	› Interim-Update › Stop
43	Acct-Output-Octets	Enthält die Anzahl der zum VPN-Peer gesendeten Oktette. Der Wert bezieht sich auf die entschlüsselten Daten, beginnend mit dem IP-Header.	› Interim-Update › Stop
44	Acct-Session-Id	Der Name des VPN-Peers und der Zeitstempel zum Session-Start bilden die eindeutige Session-ID.	› Start › Interim-Update › Stop
46	Acct-Session-Time	Enthält die verstrichene Zeit in Sekunden seit Beginn der Session.	› Interim-Update › Stop
47	Acct-Input-Packets	Enthält die Anzahl der aktuell aus Richtung VPN-Peer empfangenen Datenpakete.	› Interim-Update › Stop
48	Acct-Output-Packets	Enthält die Anzahl der aktuell zum VPN-Peer gesendeten Datenpakete.	› Interim-Update › Stop
49	Acct-Terminate-Cause	Enthält die Ursache für die Beendigung der Session.	› Stop
52	Acct-Input-Gigawords	Enthält die Anzahl der aus Richtung VPN-Peer empfangenen Gigawords. Der Wert bezieht sich auf die entschlüsselten Daten, beginnend mit dem IP-Header.	› Interim-Update › Stop
53	Acct-Input-Gigawords	Enthält die Anzahl der zum VPN-Peer gesendeten Gigawords. Der Wert bezieht sich auf die entschlüsselten Daten, beginnend mit dem IP-Header.	› Interim-Update › Stop
95	NAS-IPv6-Address	Gibt die IPv6-Adresse des Gateways an, das den Zugang für einen Anwender anfragt. Erfolgt die Verbindung über eine IPv6-Verbindung, überträgt das Gateway stattdessen das Attribut „4“ (siehe oben).	› Start › Interim-Update › Stop
168	Framed-IPv6-Address	IPv6-Adresse des VPN-Clients.	› Start

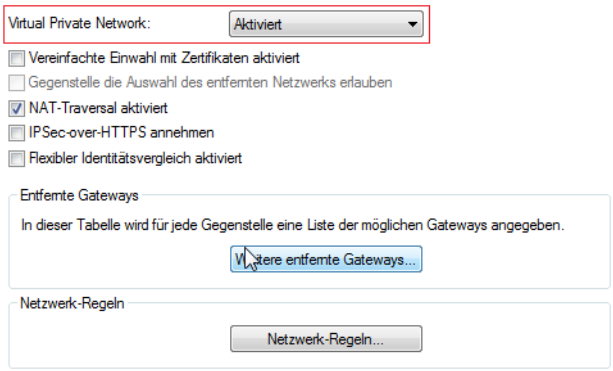
ID	Bezeichnung	Bedeutung	Status-Typ
			› Interim-Update › Stop

11.19.4 Tutorial: Einrichtung von IKEv2 unter LANconfig

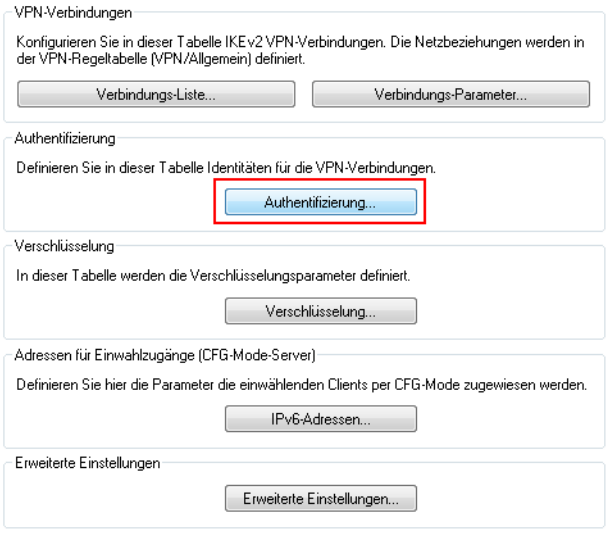
Ausgangsszenario: Zwei LANCOM-Router sind über eine WAN-Verbindung miteinander verbunden und sollen mit Hilfe von IKEv2/IPSec-VPN eine sichere VPN-Verbindung untereinander aufbauen. Bei den Routern handelt es sich um einen LANCOM 1800VAW in der Zentrale und einen LANCOM 1800VA-4G in der Filiale.

Eine bestehende WAN-Verbindung zwischen beiden Geräten wird vorausgesetzt.

1. **Aktivieren von VPN**: Öffnen Sie den Menüpunkt **VPN** > **Allgemein** in der Konfiguration der beiden Router und wählen Sie unter **Virtual Private Network** die Option **Aktiviert**. Hiermit haben Sie VPN auf dem jeweiligen Gerät aktiviert.

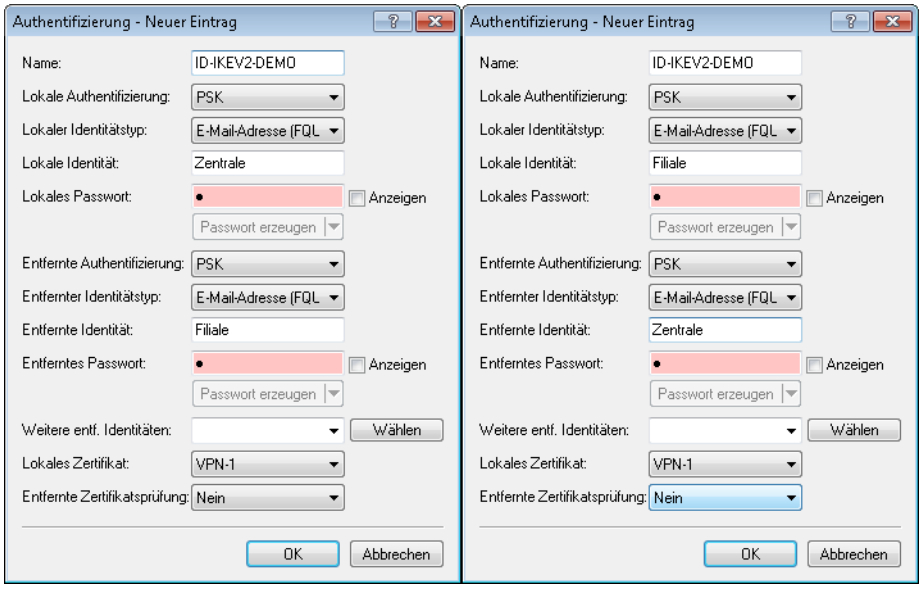


2. **Konfiguration der Authentifizierung**: Definieren Sie für die VPN-Verbindung die Art der Authentifizierung. Öffnen Sie dazu den Menüpunkt **VPN** > **IKEv2/IPSec** und klicken Sie auf die Schaltfläche **Authentifizierung**.



3. Klicken Sie auf die Schaltfläche **Hinzufügen**, um eine neue Authentifizierung zu konfigurieren. Tragen Sie in dem Konfigurationsfenster die Informationen zur Authentifizierung für die VPN-Verbindung ein.

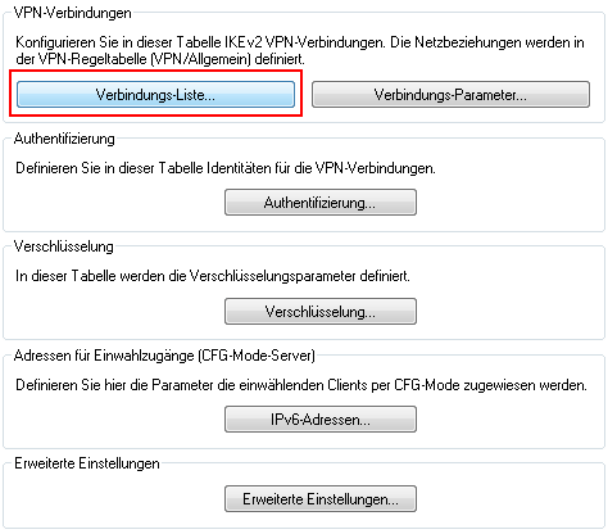
Im folgenden Screenshot sind die Konfigurationen für beide Geräte zum direkten Vergleich nebeneinander aufgeführt. Hierbei wird nur auf die Konfigurationsparameter eingegangen, die von den Default-Werten abweichen.



In der linken Bildhälfte ist der LANCOM 1800VAW abgebildet, rechts sehen Sie die Parameter des LANCOM 1800VA-4G.

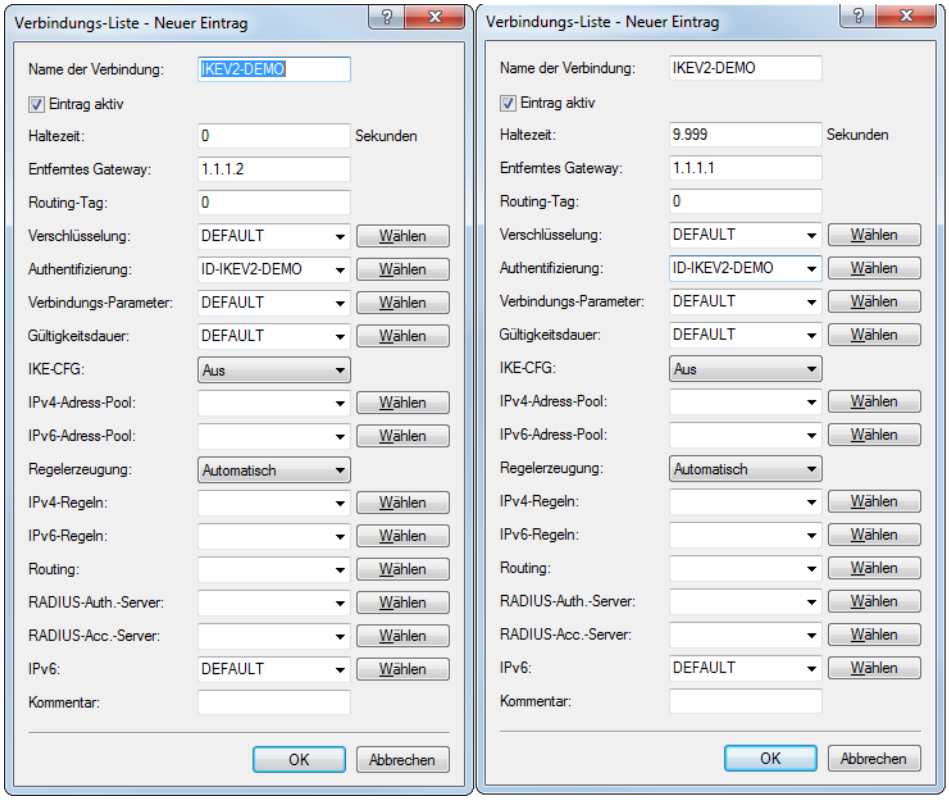
Parameter	Beschreibung
Name	Geben Sie den Namen für die Authentifizierung ein. In diesem Beispiel wurde **ID-IKEV2-DEMO** auf beiden Geräten gewählt. Dieser Eintrag wird später in der VPN-Verbindungs-Liste genutzt.
Lokale Authentifizierung	Wählen Sie den Typ der Authentifizierung an diesem Router aus. In diesem Beispiel wird die Authentifizierung über einen Pre-shared Key (PSK) vorgenommen.
Lokaler Identitätstyp	Wählen Sie den Typ der Identität bei diesem Router aus. In diesem Beispiel wurde der Identitätstyp **E-Mail-Adresse (FQUN)** gewählt.
Lokale Identität	Bestimmen Sie die lokale Identität. In diesem Beispiel wurde für den 1800VAW die lokale Identität **Zentrale** und für den 1800VA-4G die lokale Identität **Filiale** gewählt.
Lokales Passwort	Der Pre-shared Key, der verwendet wird, um sich an diesem Router erfolgreich zu authentifizieren.
Entfernte Authentifizierung	Wählen Sie den Authentifizierungstypen des Routers der Gegenseite aus. Bei dem 1800VAW entspricht dieser Eintrag dem Eintrag „Lokale Authentifizierung“ am 1800VA-4G.
Entfernter Identitätstyp	Wählen Sie den Typ der entfernten Identität (des Routers der Gegenseite) aus. Bei dem 1800VAW entspricht dieser Eintrag dem lokalen Identitätstyp des 1800VA-4G.
Entfernte Identität	Geben Sie die Identität der Gegenseite an. Bei dem 1800VAW entspricht dieser Eintrag dem Eintrag „Lokale Identität“ am 1800VA-4G.
Entferntes Passwort	Der Pre-shared Key, der verwendet wird, um sich an der Gegenseite zu authentifizieren. Bei dem 1800VAW entspricht dieser Eintrag dem lokalen Passwort des 1800VA-4G.

4. **Konfiguration der Verbindungs-Liste**: Konfigurieren Sie die Verbindungs-Listen der einzelnen Router. Zur Konfiguration öffnen Sie den Menüpunkt **VPN** > **IKEv2/IPSec** und klicken Sie auf die Schaltfläche **Verbindungs-Liste**.



5. Um eine neue VPN-Verbindung zu erstellen, klicken Sie auf die Schaltfläche **Hinzufügen**.

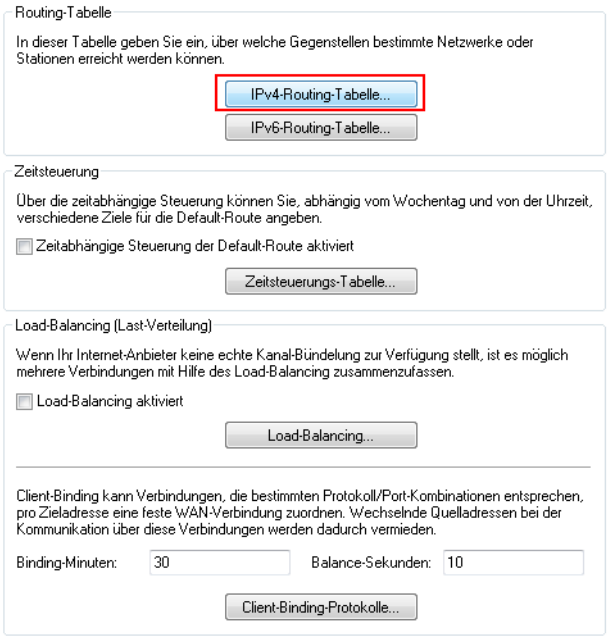
Im folgenden Screenshot sind die Konfigurationen für beide Geräte zum direkten Vergleich nebeneinander aufgeführt. Hierbei wird nur auf die Konfigurationsparameter eingegangen, die von den Default-Werten abweichen.



In der linken Bildhälfte ist der LANCOM 1800VAW abgebildet, rechts sehen Sie die Parameter des LANCOM 1800VA-4G.

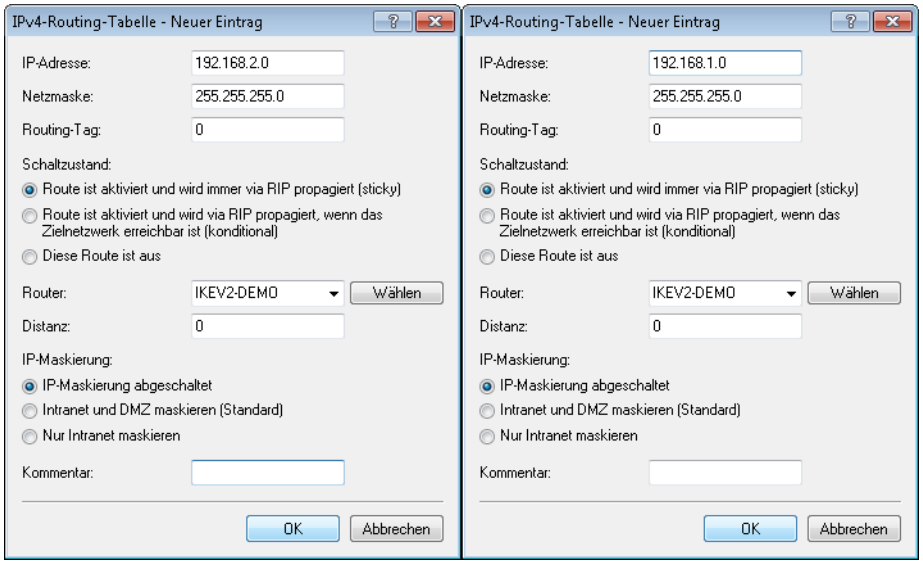
Parameter	Beschreibung
Eintrag aktiv	Setzen Sie den Haken in der Checkbox, um die Verbindung zu aktivieren.
Name der Verbindung	Geben Sie die Bezeichnung für die VPN-Verbindung an. Dieser Eintrag wird später in der Routing-Tabelle genutzt.
Haltezeit	Geben Sie die Haltezeit in Sekunden für die VPN-Verbindung an. In diesem Beispiel wird bei dem 1800VAW eine **0** eingetragen. Dies bedeutet, dass dieser Router die VPN-Verbindung nicht aktiv aufbaut. Bei dem 1800VA-4G wird der Wert **9999** eingetragen. Dieser Wert besagt, dass der Router die Verbindung nicht aktiv trennt und nach einer Trennung versucht, diese direkt wieder aufzubauen.
Entferntes Gateway	Geben Sie die IP-Adresse an, unter der die Gegenseite erreichbar ist. In diesem Beispiel ist die IP-Adresse der WAN-Schnittstelle des 1800VAW `1.1.1.1` und die des 1800VA-4G `1.1.1.2`. Falls der 1800VA-4G über eine dynamische IP-Adresse verfügen sollte, dann muss der Wert für das **Entfernte Gateway** auf dem 1800VAW auf `0.0.0.0` statt `1.1.1.2` gesetzt werden.
Authentifizierung	Wählen Sie die Authentifizierung aus. Der Eintrag entspricht hierbei dem Namen der Authentifizierung, die Sie in **Schritt 3** festgelegt haben.

6. **Konfiguration der Routing-Tabelle**: Konfigurieren Sie die Routen, damit die Pakete vom Router durch den VPN-Tunnel an die VPN-Gegenstelle geschickt werden können. Hierzu öffnen Sie den Menüpunkt **IP-Router** > **Routing** und klicken auf die Schaltfläche **IPv4-Routing-Tabelle**.



7. Um eine weitere Route zu erzeugen, klicken Sie auf die Schaltfläche **Hinzufügen**. In dem Konfigurationsfenster werden die Informationen zu der zu konfigurierenden Route der einzelnen Router eingetragen.

Im folgenden Screenshot sind die Konfigurationen für beide Geräte zum direkten Vergleich nebeneinander aufgeführt. Hierbei wird nur auf die Konfigurationsparameter eingegangen, die von den Default-Werten abweichen.



In der linken Bildhälfte ist der LANCOM 1800VAW abgebildet, rechts sehen Sie die Parameter des LANCOM 1800VA-4G.

Parameter	Beschreibung
IP-Adresse	Tragen Sie das IP-Netzwerk ein, welches durch den VPN-Tunnel erreicht werden soll. In diesem Beispiel soll das IP-Netzwerk `192.168.2.0` vom 1800VAW und das IP-Netzwerk `192.168.1.0` vom 1800VA-4G erreicht werden.
Netzmaske	Geben Sie die Netzmaske des oben angegebenen IP-Netzwerkes an.
Schaltzustand	Wählen Sie den Schaltzustand **Route ist aktiviert und wird immer per RIP propagiert** aus. Dies aktiviert den Eintrag, so dass er benutzt werden kann.
Router	Als Router tragen Sie den Namen der VPN-Verbindung ein, den Sie in **Schritt 4** eingetragen haben.
IP-Maskierung	Wählen Sie **IP-Maskierung abgeschaltet** aus, damit der Router das andere Netzwerk nicht hinter seiner IP-Adresse maskiert.

8. Schreiben Sie die Konfiguration in beide Geräte zurück.
9. Überprüfen Sie die VPN-Verbindung einfach über LANmonitor. LANmonitor zeigt Ihnen den Status der VPN-Verbindung an.

11.19.5 Tutorial: Einrichtung einer zertifikatsbasierten IKEv2-VPN-Verbindung (RSA)

Ausgangsszenario: Zwei LANCOM Router sind über eine WAN-Verbindung miteinander verbunden und sollen mit Hilfe einer zertifikatsbasierten IKEv2-VPN-Verbindung sicher miteinander kommunizeiren. Als Router kommen LANCOM Central Site Gateways, WLAN Controller oder LANCOM Router mit aktivierter VPN 25-Option (bei Verwendung der Smart Certificate Funktion) in Frage.

Eine bestehende WAN-Verbindung zwischen beiden Geräten wird vorausgesetzt.

Die Zertifikate für die beteiligten LANCOM Router wurden bereits erstellt.

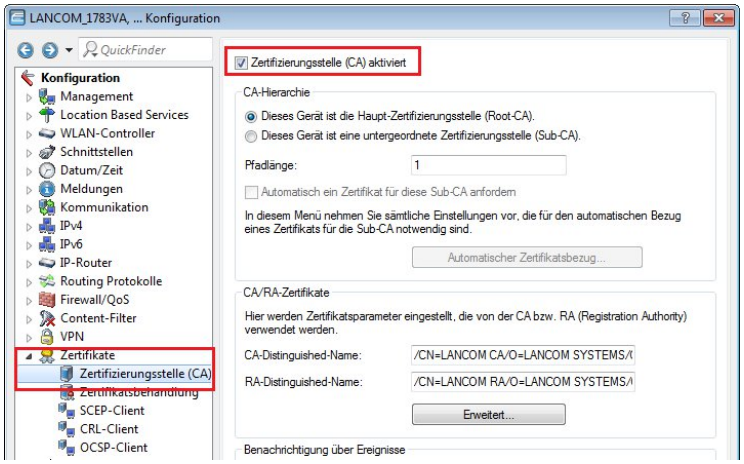
1. Aktivieren der Zertifizierungsstellen-Funktion im LANCOM Router der Zentrale

   In diesem Konfigurationsbeispiel soll der LANCOM Router in der Zentrale als CA für die Erstellung der Zertifikate verwendet werden (Smart Certificate Funktion). Wenn Sie Zertifikate einer anderen CA verwenden möchten, müssen Sie die CA des LANCOM Routers nicht verwenden und können diesen Konfigurationsschritt überspringen.

   a) Öffnen Sie die Konfiguration des LANCOM Routers der Zentrale in LANconfig und wechseln Sie in das Menü **Zertifikate** > **Zertifizierungsstelle (CA)**.

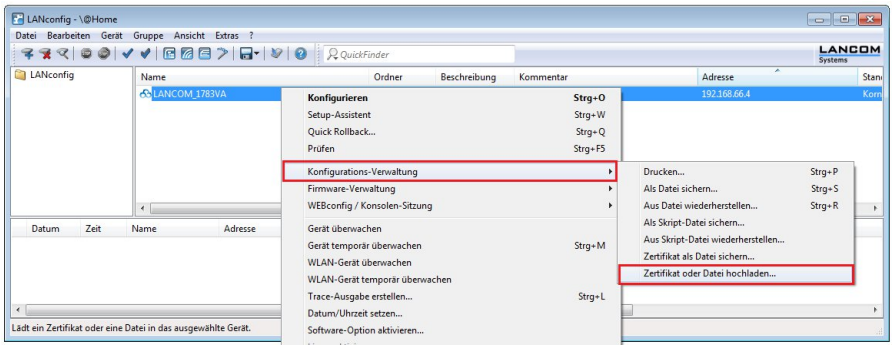
   b) Haken Sie die Option **Zertifizierungsstelle (CA) aktiviert** an. Der LANCOM Router soll als Haupt-Zertifizierungsstelle (Root-CA) arbeiten.

      Alle anderen Parameter belassen wir in diesem Konfigurationsbeispiel bei den voreingestellten Werten.



2. Hochladen der Zertifikate in die LANCOM Router

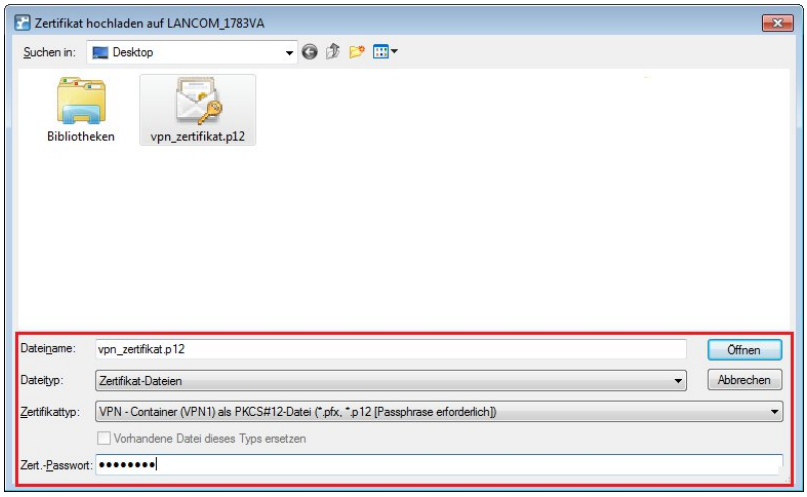
   a) Führen Sie jeweils einen rechten Mausklick auf den LANCOM Router in LANconfig aus und wählen Sie die Option **Konfigurations-Verwaltung** > **Zertifikat oder Datei hochladen**.



   b) Wählen Sie im folgenden Dialog die jeweilige Zertifikatsdatei für den LANCOM Router aus.

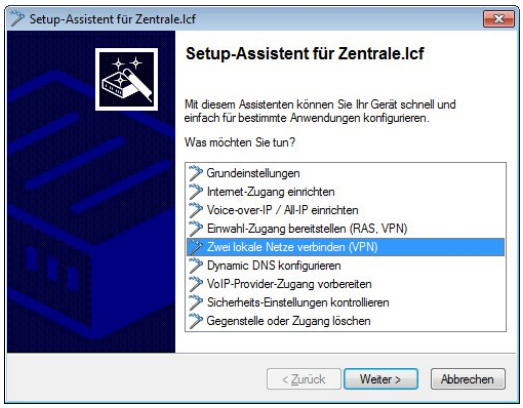
   c) Im Feld **Zertifikattyp** müssen Sie einen VPN-Container auswählen.

d) Im Feld **Zert.-Passwort** müssen Sie das Passwort der Zertifikatsdatei eintragen. Klicken Sie dann auf **Öffnen** um den Hochladevorgang zu starten.

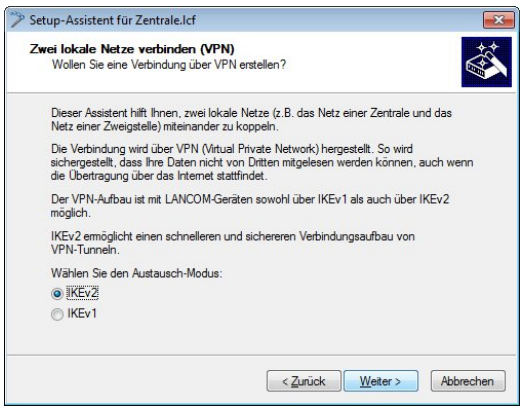


3. Konfigurieren der zertifikatsbasierten VPN-Verbindung im LANCOM Router der Zentrale

a) Starten Sie den Setup-Assistent in LANconfig und wählen Sie die Option **Zwei lokale Netze verbinden (VPN)**.



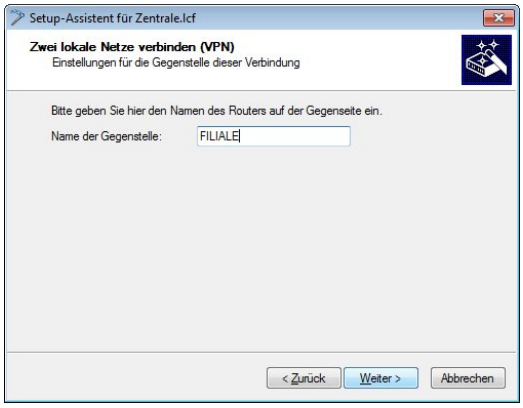
b) Es soll eine **IKEv2**-VPN-Verbindung erstellt werden.



c) **IPSec-over-HTTPS** wird in diesem Konfigurationsbeispiel nicht verwendet.

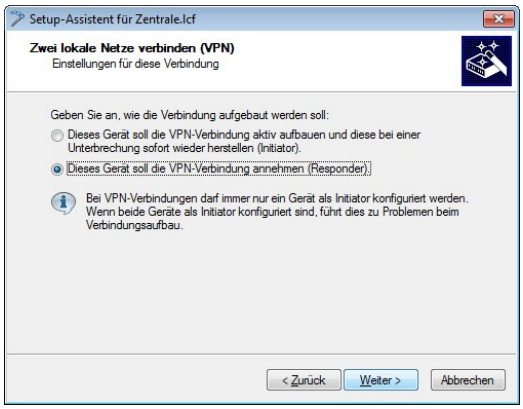


d) Geben Sie eine **Namensbezeichnung für den LANCOM Router auf der Gegenseite** an.

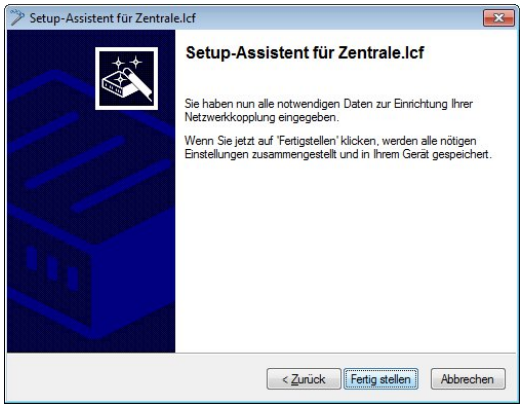


e) In den folgenden zwei Dialogen können Sie beliebige Werte eintragen, da diese später in der Konfiguration des LANCOM Routers manuell durch Zertifikats-Authentifizierungs-Parameter ersetzt werden.

f) Da der LANCOM Router in der Zentrale die VPN-Verbindung annimmt, muss keine Gateway-Adresse eingetragen werden. Geben Sie das lokale Netzwerk an, welches auf der Gegenseite erreicht werden soll.



g) Klicken Sie auf **Fertig stellen** um den Setup-Assistent zu beenden und die Konfiguration in den LANCOM Router zurück zu schreiben.



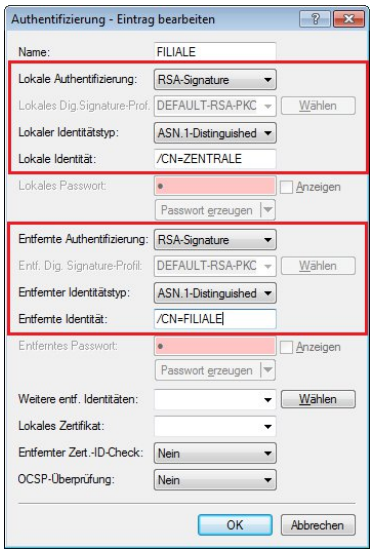
h) Öffnen Sie die Konfiguration des LANCOM Routers in LANconfig und wechseln Sie in das Menü **VPN** > **IKEv2/IPSec** > **Authentifizierung**.

i) Wählen Sie den bestehenden Eintrag für die zertifikatsbasierte VPN-Client-Verbindung aus (hier: FILIALE).

j) Passen Sie die Parameter für die **lokale und entfernte Authentifizierung** jeweils auf die Werte **RSA-Signature** und **ASN.1 Distinguished Name** an.

k) Tragen Sie als **lokale Identität** den Namen des Zertifikats vom LANCOM Router der Zentrale ein.

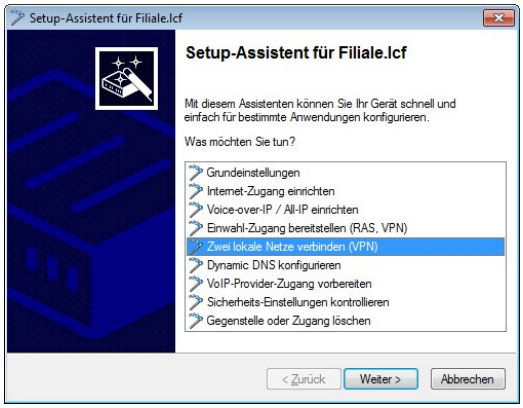
l) Tragen Sie als **entfernte Identität** den Namen des Zertifikats vom LANCOM Router der Filiale ein.



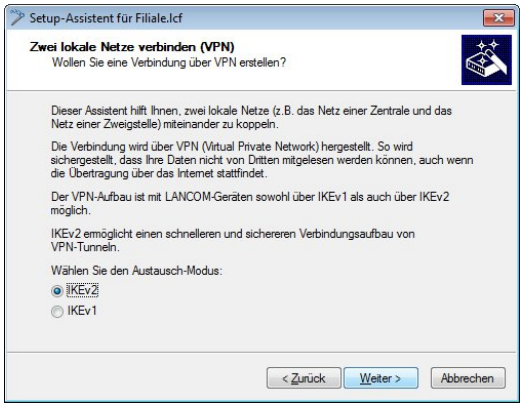
m) Schreiben Sie die Konfiguration in den LANCOM Router der Zentrale zurück.

4. Konfigurieren der zertifikatsbasierten VPN-Verbindung im LANCOM Router der Filiale

a) Starten Sie den Setup-Assistenten in LANconfig und wählen Sie die Option **Zwei lokale Netze verbinden (VPN)**.



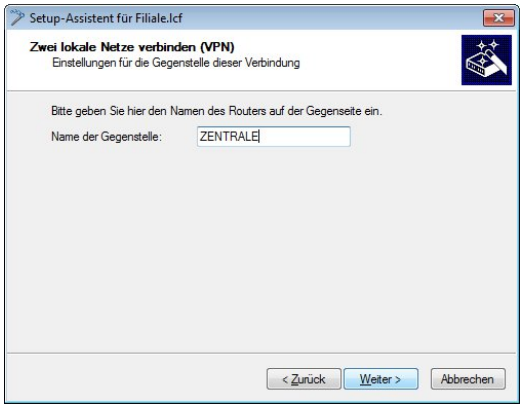
b) Es soll eine **IKEv2**-VPN-Verbindung erstellt werden.



c) **IPSec-over-HTTPS** wird in diesem Konfigurationsbeispiel nicht verwendet.

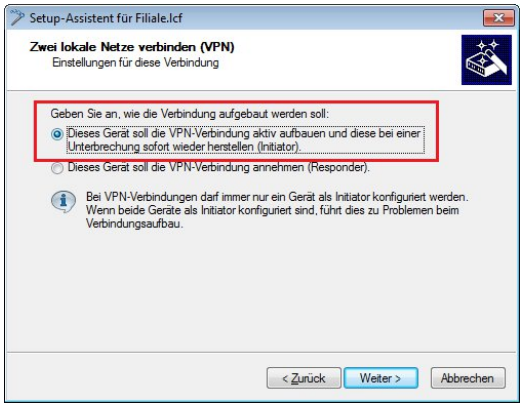


d) Geben Sie eine **Namensbezeichnung für den LANCOM Router auf der Gegenseite** an.



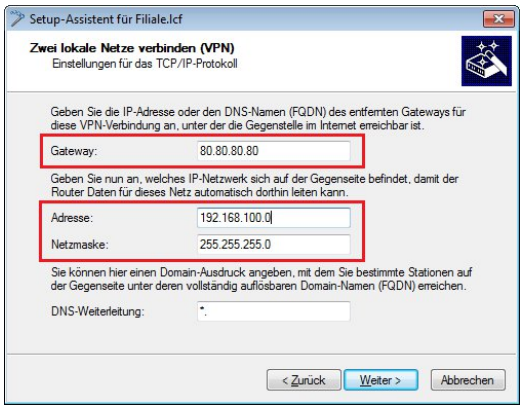
e) In den folgenden zwei Dialogen können Sie beliebige Werte eintragen, da diese später in der Konfiguration des LANCOM Routers manuell durch Zertifikats-Authentifizierungs-Parameter ersetzt werden.

f) Der LANCOM Router in der Filiale soll die VPN-Verbindung zur Zentrale aufbauen.

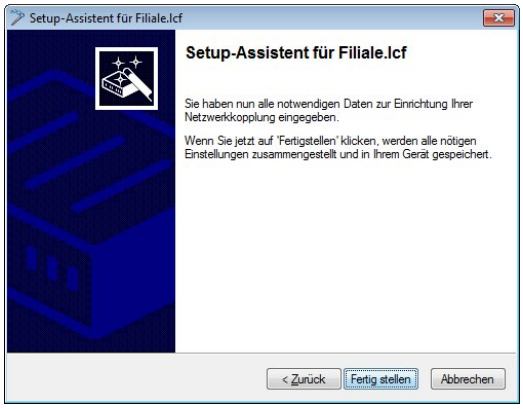


g) Da der LANCOM Router in der Filiale die VPN-Verbindung zur Zentrale aufbaut, muss die Gateway-Adresse der Zentrale eingetragen werden.

h) Geben Sie das lokale Netzwerk an, welches auf der Gegenseite erreicht werden soll.



i) Klicken Sie auf **Fertig stellen** um den Setup-Assistenten zu beenden und die Konfiguration in den LANCOM Router zurück zu schreiben.



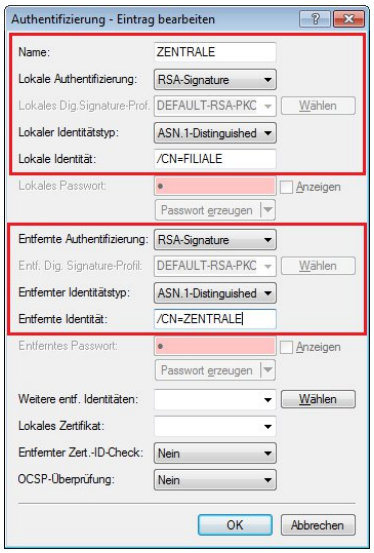
j) Öffnen Sie die Konfiguration des LANCOM Routers in LANconfig und wechseln Sie in das Menü **VPN** > **IKEv2/IPSec** > **Authentifizierung**.

k) Wählen Sie den bestehenden Eintrag für die zertifikatsbasierte VPN-Verbindung aus (hier: ZENTRALE).

l) Passen Sie die Parameter für die **lokale und entfernte Authentifizierung** jeweils auf die Werte **RSA-Signature** und **ASN.1 Distinguished Name** an.

m) Tragen Sie als **lokale Identität** den Namen des Zertifikats vom LANCOM Router der Filiale ein.

n) Tragen Sie als **entfernte Identität** den Namen des Zertifikats vom LANCOM Router der Zentrale ein.



o) Schreiben Sie die Konfiguration in den LANCOM Router der Filiale zurück.

Die zertifikatsbasierte IKEv2-VPN-Verbindung zur Zentrale wird nach kurzer Zeit aufgebaut.

11.19.6 Tutorial: Einrichtung einer zertifikatsbasierten IKEv2-VPN-Verbindung (Digital Signature)

Ausgangsszenario: Zwei LANCOM Router sind über eine WAN-Verbindung miteinander verbunden und sollen mit Hilfe einer zertifikatsbasierten IKEv2-VPN-Verbindung sicher miteinander kommunizeiren. Als Router kommen LANCOM Central Site Gateways, WLAN Controller oder LANCOM Router mit aktivierter VPN 25-Option (bei Verwendung der Smart Certificate Funktion) in Frage.

Eine bestehende WAN-Verbindung zwischen beiden Geräten wird vorausgesetzt.

Die Zertifikate für die beteiligten LANCOM Router wurden bereits erstellt.

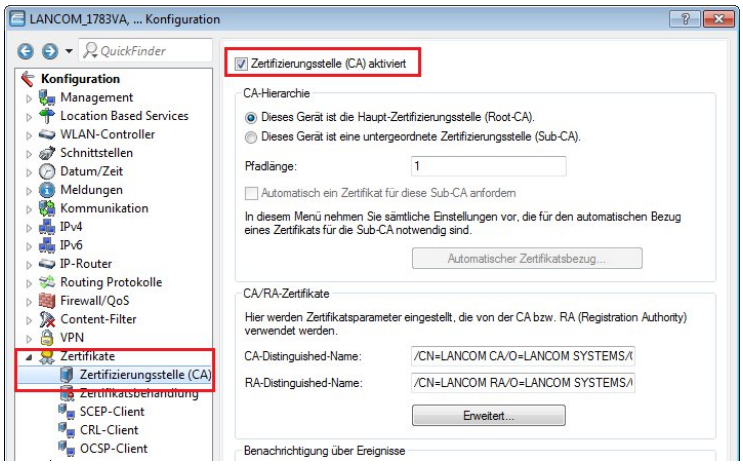
1. Aktivieren der Zertifizierungsstellen-Funktion im LANCOM Router der Zentrale

In diesem Konfigurationsbeispiel soll der LANCOM Router in der Zentrale als CA für die Erstellung der Zertifikate verwendet werden (Smart Certificate Funktion). Wenn Sie Zertifikate einer anderen CA verwenden möchten, müssen Sie die CA des LANCOM Routers nicht verwenden und können diesen Konfigurationsschritt überspringen.

a) Öffnen Sie die Konfiguration des LANCOM Routers der Zentrale in LANconfig und wechseln Sie in das Menü **Zertifikate** > **Zertifizierungsstelle (CA)**.

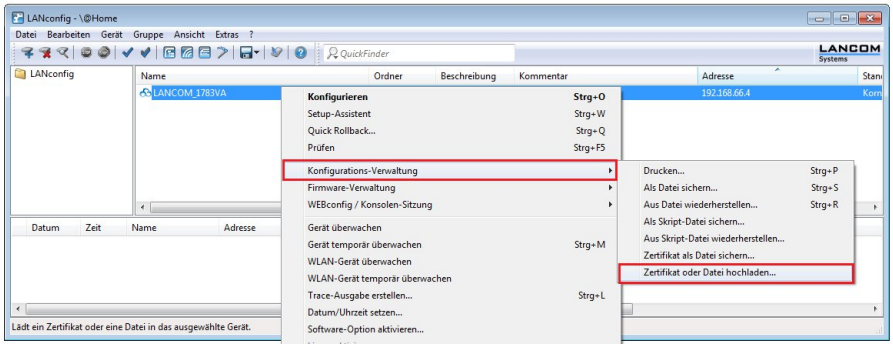
b) Haken Sie die Option **Zertifizierungsstelle (CA) aktiviert** an. Der LANCOM Router soll als Haupt-Zertifizierungsstelle (Root-CA) arbeiten.

Alle anderen Parameter belassen wir in diesem Konfigurationsbeispiel bei den voreingestellten Werten.



2. Hochladen der Zertifikate in die LANCOM Router

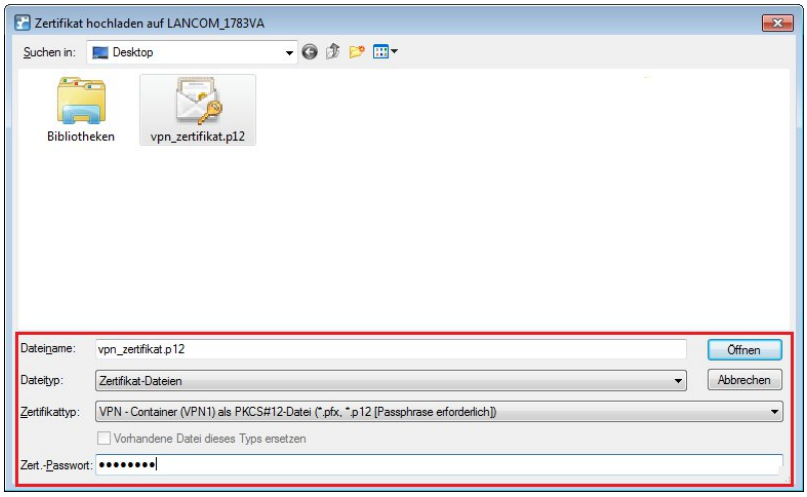
a) Führen Sie jeweils einen rechten Mausklick auf den LANCOM Router in LANconfig aus und wählen Sie die Option **Konfigurations-Verwaltung** > **Zertifikat oder Datei hochladen**.



b) Wählen Sie im folgenden Dialog die jeweilige Zertifikatsdatei für den LANCOM Router aus.

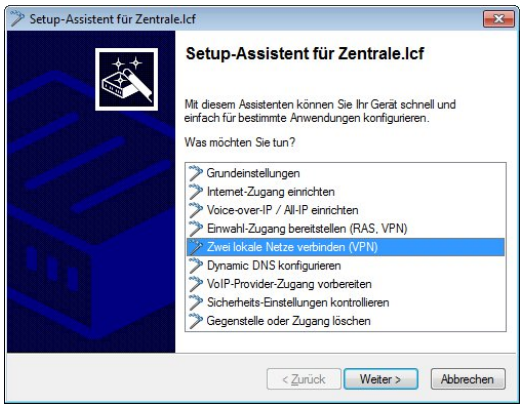
c) Im Feld **Zertifikattyp** müssen Sie einen VPN-Container auswählen.

d) Im Feld **Zert.-Passwort** müssen Sie das Passwort der Zertifikatsdatei eintragen. Klicken Sie dann auf **Öffnen** um den Hochladevorgang zu starten.

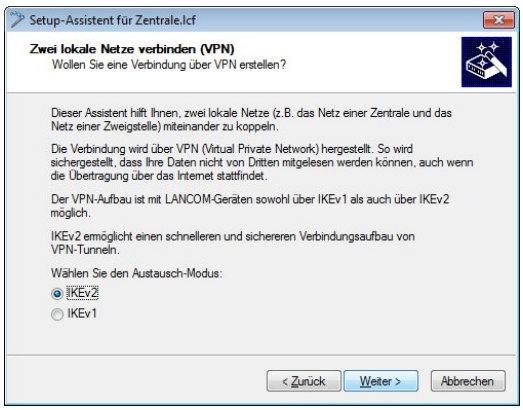


3. Konfigurieren der zertifikatsbasierten VPN-Verbindung im LANCOM Router der Zentrale

a) Starten Sie den Setup-Assistent in LANconfig und wählen Sie die Option **Zwei lokale Netze verbinden (VPN)**.



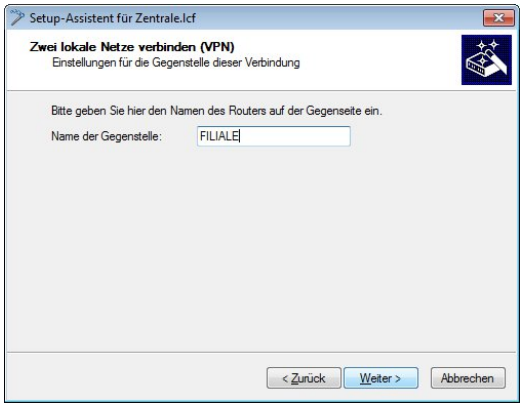
b) Es soll eine **IKEv2**-VPN-Verbindung erstellt werden.



c) **IPSec-over-HTTPS** wird in diesem Konfigurationsbeispiel nicht verwendet.

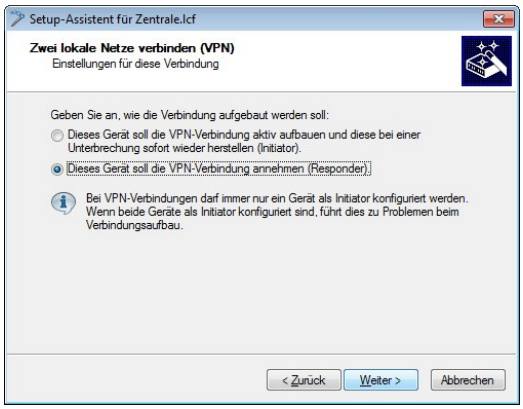


d) Geben Sie eine **Namensbezeichnung für den LANCOM Router auf der Gegenseite** an.

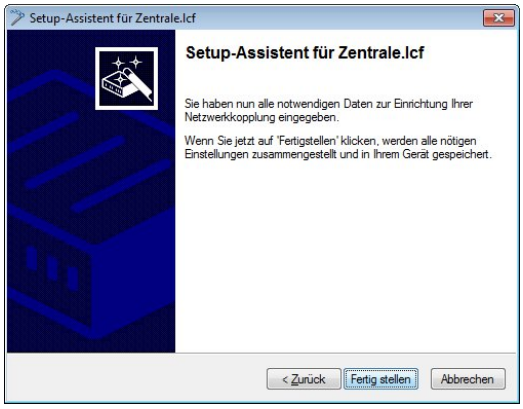


e) In den folgenden zwei Dialogen können Sie beliebige Werte eintragen, da diese später in der Konfiguration des LANCOM Routers manuell durch Zertifikats-Authentifizierungs-Parameter ersetzt werden.

f) Da der LANCOM Router in der Zentrale die VPN-Verbindung annimmt, muss keine Gateway-Adresse eingetragen werden. Geben Sie das lokale Netzwerk an, welches auf der Gegenseite erreicht werden soll.



g) Klicken Sie auf **Fertig stellen** um den Setup-Assistent zu beenden und die Konfiguration in den LANCOM Router zurück zu schreiben.



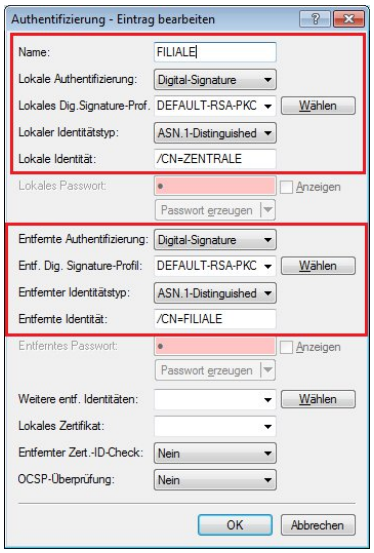
h) Öffnen Sie die Konfiguration des LANCOM Routers in LANconfig und wechseln Sie in das Menü **VPN** > **IKEv2/IPSec** > **Authentifizierung**.

i) Wählen Sie den bestehenden Eintrag für die zertifikatsbasierte VPN-Client-Verbindung aus (hier: FILIALE).

j) Passen Sie die Parameter für die **lokale und entfernte Authentifizierung** jeweils auf die Werte **Digital-Signature** und **ASN.1 Distinguished Name** an.

k) Tragen Sie als **lokale Identität** den Namen des Zertifikats vom LANCOM Router der Zentrale ein.

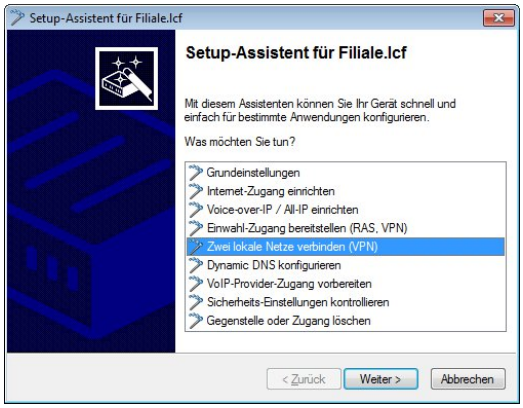
l) Tragen Sie als **entfernte Identität** den Namen des Zertifikats vom LANCOM Router der Filiale ein.



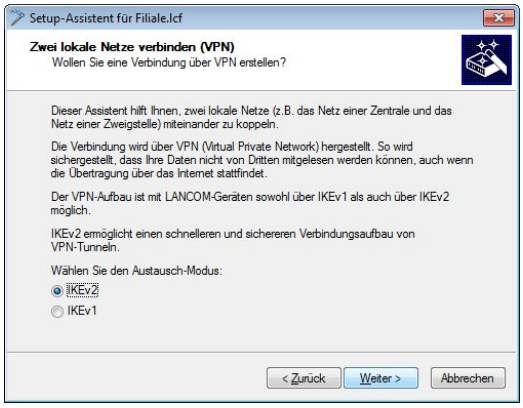
m) Schreiben Sie die Konfiguration in den LANCOM Router der Zentrale zurück.

4. Konfigurieren der zertifikatsbasierten VPN-Verbindung im LANCOM Router der Filiale

a) Starten Sie den Setup-Assistenten in LANconfig und wählen Sie die Option **Zwei lokale Netze verbinden (VPN)**.



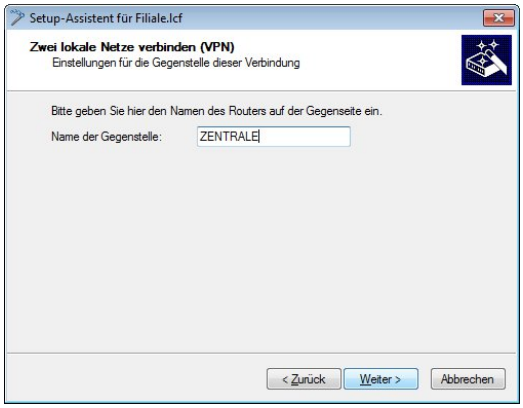
b) Es soll eine **IKEv2**-VPN-Verbindung erstellt werden.



c) **IPSec-over-HTTPS** wird in diesem Konfigurationsbeispiel nicht verwendet.

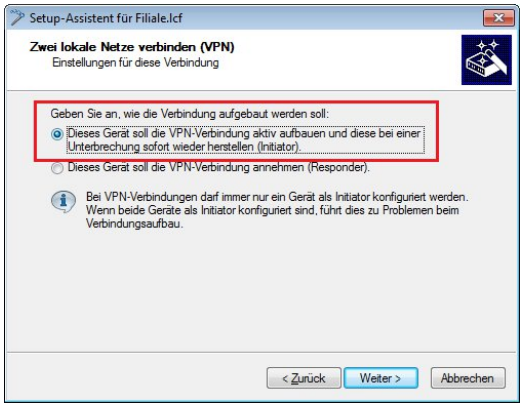


d) Geben Sie eine **Namensbezeichnung für den LANCOM Router auf der Gegenseite** an.



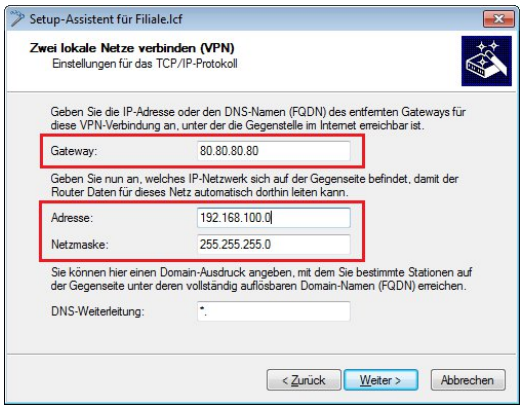
e) In den folgenden zwei Dialogen können Sie beliebige Werte eintragen, da diese später in der Konfiguration des LANCOM Routers manuell durch Zertifikats-Authentifizierungs-Parameter ersetzt werden.

f) Der LANCOM Router in der Filiale soll die VPN-Verbindung zur Zentrale aufbauen.

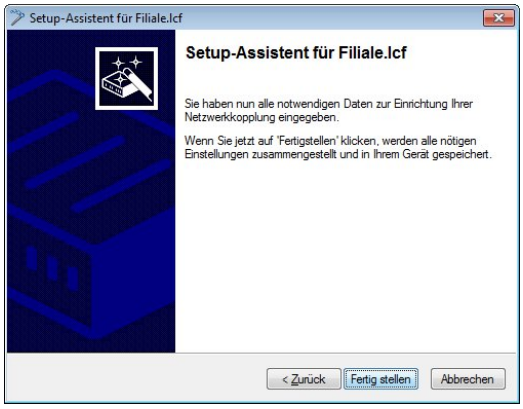


g) Da der LANCOM Router in der Filiale die VPN-Verbindung zur Zentrale aufbaut, muss die Gateway-Adresse der Zentrale eingetragen werden.

h) Geben Sie das lokale Netzwerk an, welches auf der Gegenseite erreicht werden soll.



i) Klicken Sie auf **Fertig stellen** um den Setup-Assistenten zu beenden und die Konfiguration in den LANCOM Router zurück zu schreiben.



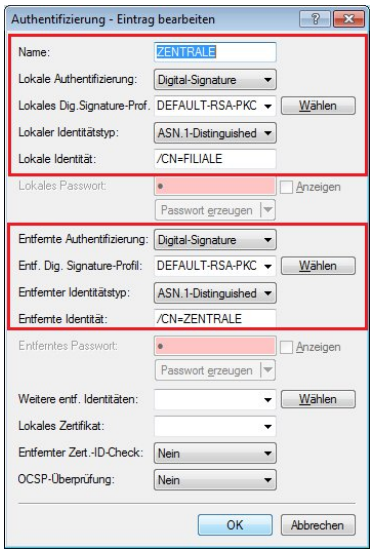
j) Öffnen Sie die Konfiguration des LANCOM Routers in LANconfig und wechseln Sie in das Menü **VPN** > **IKEv2/IPSec** > **Authentifizierung**.

k) Wählen Sie den bestehenden Eintrag für die zertifikatsbasierte VPN-Verbindung aus (hier: ZENTRALE).

l) Passen Sie die Parameter für die **lokale und entfernte Authentifizierung** jeweils auf die Werte **RSA-Signature** und **ASN.1 Distinguished Name** an.

m) Tragen Sie als **lokale Identität** den Namen des Zertifikats vom LANCOM Router der Filiale ein.

n) Tragen Sie als **entfernte Identität** den Namen des Zertifikats vom LANCOM Router der Zentrale ein.



o) Schreiben Sie die Konfiguration in den LANCOM Router der Filiale zurück.

Die zertifikatsbasierte IKEv2-VPN-Verbindung zur Zentrale wird nach kurzer Zeit aufgebaut.

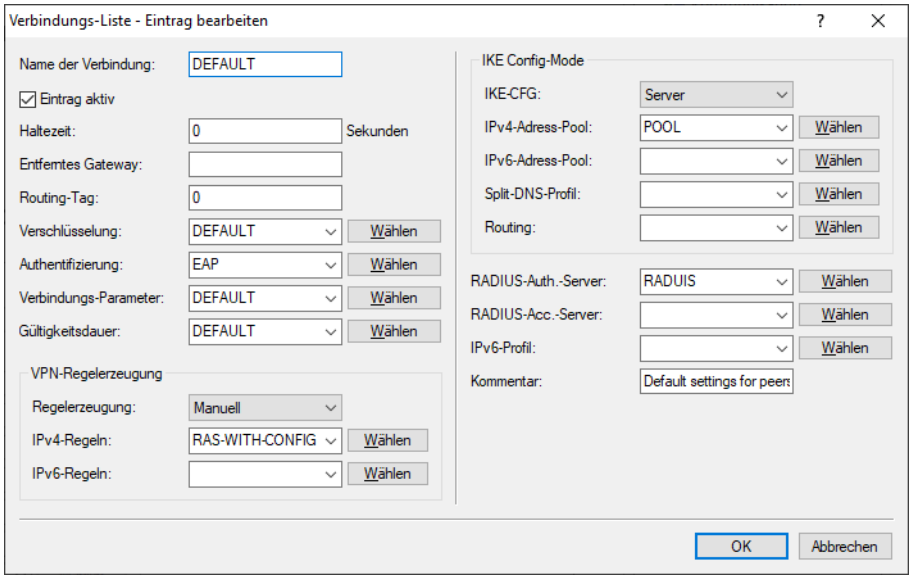
11.19.7 Tutorial – EAP-Client gegen einen EAP-Server

Im folgenden Tutorial soll ein EAP-Client gegen einen EAP-Server konfiguriert werden.

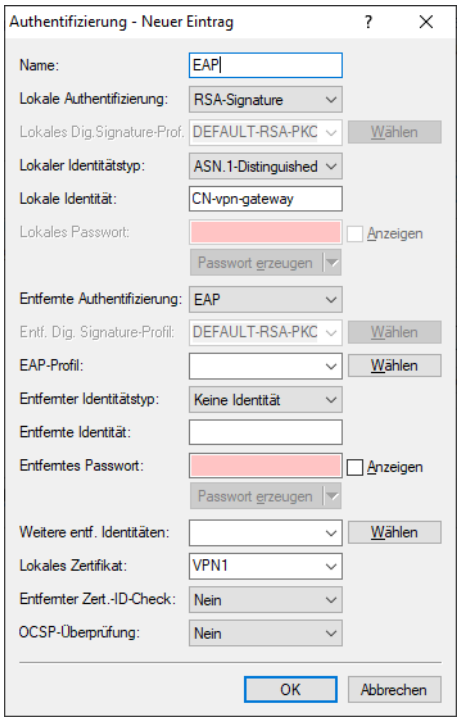
1. Erstellen Sie zwei Zertifikate bzw. Zertifikatscontainer, z. B. mit der LANCOM SCEP CA oder OpenSSL.
2. Importieren Sie sowohl ein Zertifikat in das VPN-Gateway als auch ein Zertifikat in den RADIUS-Server.

   Achten Sie darauf, dass der Subject Alternative Name (SAN) dem gültigen DNS-Namen des VPN-Gateways entspricht und der VPN-Client das Gateway unter diesem DNS-Namen kontaktiert.
3. Zur Herstellung der Vertrauensbeziehung importieren Sie zusätzlich das gültige CA-Zertifikat in den IKEv2-EAP-Client.

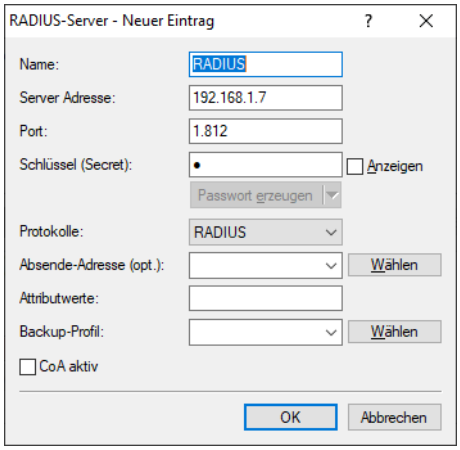
4. Editieren Sie den DEFAULT-Eintrag der IKEv2-Gegenstellen-Tabelle unter **VPN** > **IKEv2/IPSec** > **VPN-Verbindungen** > **Verbindungs-Liste** wie folgt:



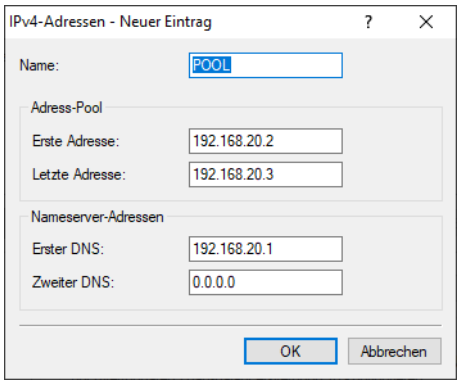
5. Legen Sie eine neue Zeile in der Tabelle IKEv2-Authentifizierung unter **VPN** > **IKEv2/IPSec** > **Authentifizierung** an. Die Lokale Authentifizierung des VPN-Gateways erfolgt über Zertifikat (RSA-Signature), die Entfernte Authentifizierung der Clients erfolgt per EAP.



6. Konfigurieren Sie den RADIUS-Server unter **VPN** > **IKEv2/IPSec** > **Erweiterte Einstellungen** > **RADIUS-Authentifizierung** > **RADIUS-Server**.



7. Konfigurieren Sie einen Adress-Pool unter **VPN** > **IKEv2/IPSec** > **IPv4-Adressen**.



11.20 Anwendungskonzepte für LANconfig

In diesem Abschnitt finden Sie verschiedene Anwendungskonzepte für LANconfig.

11.20.1 1-Click-VPN für Netzwerke (Site-to-Site)

Die Einstellungen für die Kopplung von Netzwerken können sehr komfortabel über den 1-Click-VPN-Assistenten vorgenommen werden. Dabei können sogar mehrere Router gleichzeitig an ein zentrales Netzwerk gekoppelt werden.

1. Markieren Sie in LANconfig die Router, für die Sie eine VPN-Kopplung zu einem zentralen Router einrichten möchten.
2. Ziehen Sie die Geräte mit der Maus auf den Eintrag für den zentralen Router.
3. Der 1-Click-VPN Site-to-Site-Assistent startet. Geben Sie den Namen für diesen Zugang ein und wählen Sie aus, über welche Adresse der Router aus dem Internet erreichbar ist.
4. Wählen Sie aus, ob der Verbindungsaufbau über den Namen bzw. die IP-Adresse des zentralen Routers erfolgen soll. Geben Sie dazu die Adresse bzw. den Namens des zentralen Routers an.
5. Im letzten Schritt legen Sie fest, wie die verbundenen Netzwerke untereinander kommunizieren können:
   - Nur das INTRANET der Zentrale wird für die Außenstellen verfügbar gemacht.
   - Alle privaten Netze der Außenstellen können ebenfalls über die Zentrale untereinander verbunden werden.

Alle Eingaben werden nur einmal für das Zentralgerät vorgenommen und dann in den Geräteeigenschaften hinterlegt.

11.20.2 1-Click-VPN für Advanced VPN Client

VPN-Zugänge für Mitarbeiter, die sich mit Hilfe des LANCOM Advanced VPN Clients in ein Netzwerk einwählen, lassen sich sehr einfach mit dem Setup-Assistenten erstellen und in eine Datei exportieren, die vom LANCOM Advanced VPN Client als Profil eingelesen werden kann. Dabei werden die erforderlichen Informationen der aktuellen Konfiguration des VPN-Routers entnommen und mit zufällig ermittelten Werten ergänzt (z. B. für den Preshared Key).

1. Starten Sie im LANconfig über **Gerät** > **Setup Assistent** den Setup-Assistenten **Einwahl-Zugang bereitstellen (RAS, VPN)**.
2. Wählen Sie im Folgefenster **VPN-Verbindung-über das Internet** und klicken Sie **Weiter**.
3. Wählen Sie aus der Liste den Eintrag **LANCOM Advanced VPN Client [...]** und aktivieren Sie die Option **Beschleunigen Sie das Konfigurieren mit 1-Click-VPN**.
4. Geben Sie im nächsten Schritt den Namen für diesen Zugang ein und wählen Sie aus, über welche Adresse der Router aus dem Internet erreichbar ist.
5. Im letzten Schritt können Sie wählen, wie die neuen Zugangsdaten ausgegeben werden sollen:
   - Profil als Importdatei für den LANCOM Advanced VPN Client speichern
   - Profil per E-Mail versenden
   - Profil ausdrucken

Das Versenden der Profildatei per E-Mail stellt ein Sicherheitsrisiko dar, weil die E-Mail unterwegs ggf. abgehört werden könnte. Zum Versenden der Profildatei per E-Mail muss in der Konfiguration des Geräts ein SMTP-Konto mit den erforderlichen Zugangsdaten eingerichtet sein. Außerdem muss auf dem Konfigurationsrechner ein E-Mail-Programm als Standard-Mail-Anwendung eingerichtet sein, über die auch andere Anwendungen E-Mails versenden dürfen.

Beim Erstellen des VPN-Zugangs werden Einstellungen verwendet, die optimal auf die Verwendung im LANCOM Advanced VPN Client abgestimmt sind, darunter z. B.:

- Gateway: Sofern im VPN-Router definiert, wird hier ein DynDNS-Name verwendet, ansonsten die IP-Adresse
- FQDN: Kombination aus dem Namen der Verbindung, einer fortlaufenden Nummer und der internen Domäne im VPN-Router
- Domäne: Sofern im VPN-Router definiert, wird hier die interne Domäne verwendet, ansonsten ein DynDNS-Name oder die IP-Adresse
- VPN IP-Netze: Alle im Gerät definierten IP-Netzwerke vom Typ 'Intranet'.
- Preshared Key: Zufällig generierter Schlüssel mit einer Länge von 16 ASCII-Zeichen.
- Verbindungsmedium: Für den Verbindungsaufbau wird das LAN genutzt.
- VoIP-Priorisierung: Die VoIP-Priorisierung ist standardmäßig aktiviert.
- Exchange Mode: Als Exchange-Mode wird der 'Aggressive Mode' verwendet.
- IKE-Config-Mode: Der IKE-Config-Mode ist aktiviert, die IP-Adress-Informationen für den LANCOM Advanced VPN Client werden automatisch vom VPN-Router zugewiesen.

12 Virtuelle LANs (VLANs)

12.1 Was ist ein Virtuelles LAN?

Die steigende Verfügbarkeit von preiswerten Layer-2-Switches erlaubt den Aufbau sehr viel größerer LANs als in der Vergangenheit. Bisher wurden oft kleinere Abschnitte eines Netzwerks mit Hubs zusammengeschlossen. Diese einzelnen Segmente (Collision Domains) wurden dann über Router zu größeren Einheiten zusammengeschlossen. Da ein Router jedoch immer die Grenze zwischen zwei LANs bildet, entstehen in dieser Struktur mehrere LANs mit eigenen IP-Adresskreisen.

Mit dem Einsatz von Switches können dagegen sehr viel mehr Stationen zu einem großen LAN zusammen geschlossen werden. Durch die gezielte Steuerung des Datenflusses auf die einzelnen Ports wird die verfügbare Bandbreite besser genutzt als beim Einsatz von Hubs, die Konfiguration und Wartung von Routern im Netzverbund entfällt.

Aber auch eine auf Switches basierende Netzwerkstruktur hat ihrer Nachteile:

- Broadcasts werden wie auch bei den Hubs über das gesamte LAN gesendet, selbst wenn die entsprechenden Datenpakete nur für ein bestimmtes Segment des LANs von Bedeutung sind. Bei einer ausreichenden Anzahl von Stationen im Netz kann das schon zu einer deutlichen Einschränkung der verfügbaren Bandbreite im LAN führen.
- Der gesamte Datenverkehr auf dem physikalischen LAN ist „öffentlich". Selbst wenn einzelne Segmente unterschiedliche IP-Adresskreise nutzen, kann jede Station im LAN theoretisch den Datenverkehr aus allen logischen Netzen auf dem Ethernetstrang abhören. Der Schutz einzelner LAN-Segmente mit Firewalls oder Router erhöht wieder die Anforderungen an die Administration des Netzwerks.

Eine Möglichkeit, diese Probleme zu überwinden, stellen die virtuellen LANs (VLAN) dar, wie sie in IEEE 802.1p/q beschrieben sind. Bei diesem Konzept werden auf einem physikalischen LAN mehrere virtuelle LANs definiert, die sich gegenseitig nicht behindern und die auch den Datenverkehr der jeweils anderen VLANs auf dem physikalischen Ethernetstrang nicht empfangen oder abhören können.

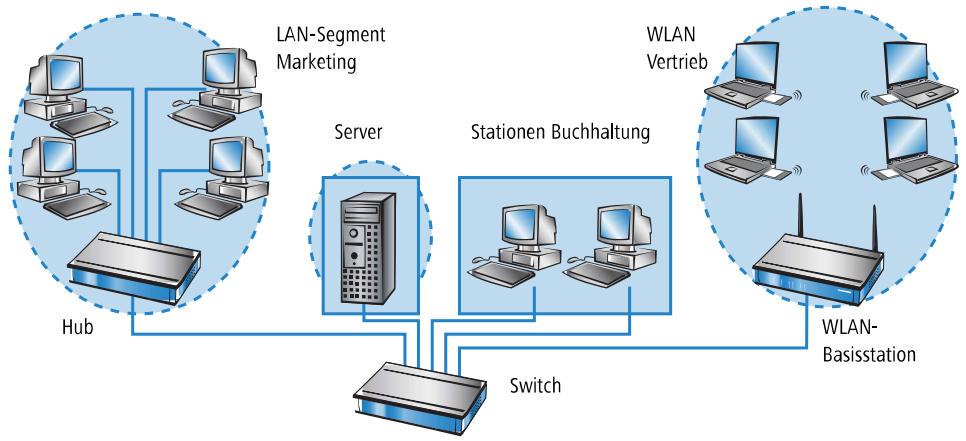
12.2 So funktioniert ein VLAN

Mit der Definition von VLANs auf einem LAN sollen folgende Ziele erreicht werden:

- Der Datenverkehr von bestimmten logischen Einheiten soll gegenüber anderen Netzteilnehmern abgeschirmt werden.
- Der Broadcast-Datenverkehr soll ebenfalls auf die logischen Einheiten reduziert werden und nicht das gesamte LAN belasten.
- Der Datenverkehr von bestimmten logischen Einheiten soll gegenüber anderen Netzteilnehmern mit einer besonderen Priorität übertragen werden.

Zur Verdeutlichung ein Beispiel: In einem LAN ist an einem Switch ein Hub angeschlossen, der vier Stationen aus dem Marketing an das Netz anbindet. Ein Server und zwei Stationen der Buchhaltung sind direkt an den Switch angeschlossen.

Den letzten Abschnitt bildet die Basisstation eines Funknetzwerks, in dem sich vier WLAN-Clients aus dem Vertrieb befinden.



Die Stationen aus Marketing und Vertrieb sollen miteinander kommunizieren und auf den Server zugreifen können.Die Buchhaltung benötigt ebenfalls Zugriff auf den Server, soll aber ansonsten von den anderen Stationen abgeschirmt werden.

12.2.1 Frame-Tagging

Um den Datenverkehr eines virtuellen LANs gegen die anderen Netzteilnehmer abschirmen und ggf. priorisieren zu können, müssen die Datenpakete eine entsprechende Kennzeichnung aufweisen. Dazu werden die MAC-Frames um ein zusätzliches Merkmal (ein "Tag") erweitert. Das entsprechende Verfahren wird daher auch als „Frame-Tagging" bezeichnet.

Das Frame-Tagging muss dabei so realisiert sein, dass folgende Anforderungen erfüllt werden:

- Datenpakete mit und ohne Frame-Tagging müssen auf einem physikalischen LAN parallel nebeneinander her existieren können.
- Stationen und Switches im LAN, welche die VLAN-Technik nicht unterstützen, müssen die Datenpakete mit Frame-Tagging ignorieren bzw. wie „normale" Datenpakete behandeln.

Das Tagging wird durch ein zusätzliches Feld im MAC-Frame realisiert. In diesem Feld sind zwei für das virtuelle LAN wesentliche Informationen enthalten:

- **VLAN-ID**: Mit einer eindeutigen Nummer wird das virtuelle LAN gekennzeichnet. Diese ID bestimmt die Zugehörigkeit eines Datenpakets zu einem logischen (virtuellen) LAN. Mit diesem 12-Bit-Wert können bis zu 4094 unterschiedliche VLANs definiert werden (die VLAN-IDs 0 und 4095 sind reserviert bzw. nicht zulässig).

  Die VLAN-ID 1 wird von vielen Geräten als Default-VLAN-ID verwendet. Bei einem unkonfigurierten Gerät gehören alle Ports zu diesem Default-VLAN. Diese Zuweisung kann bei der Konfiguration allerdings auch wieder verändert werden.

- **Priorität**: Die Priorität eines VLAN-gekennzeichneten Datenpakets wird mit einem 3-Bit-Wert markiert. Dabei steht die 0 für die geringste, die 7 für die höchste Priorität. Datenpakete ohne VLAN-Tag werden mit der Priorität 0 behandelt.

Durch dieses zusätzliche Feld werden die MAC-Frames länger als eigentlich erlaubt. Diese überlangen Pakete können nur von VLAN-fähigen Stationen und Switches richtig erkannt und ausgewertet werden. Bei Netzteilnehmern ohne VLAN-Unterstützung führt das Frame-Tagging quasi nebenbei zum gewünschten Verhalten:

- Switches ohne VLAN-Unterstützung leiten diese Datenpakete einfach weiter und ignorieren die zusätzlichen Felder im MAC-Frame.
- Stationen ohne VLAN-Unterstützung können in den Paketen aufgrund des eingefügten VLAN-Tags den Protokolltyp nicht erkennen und verwerfen sie stillschweigend.

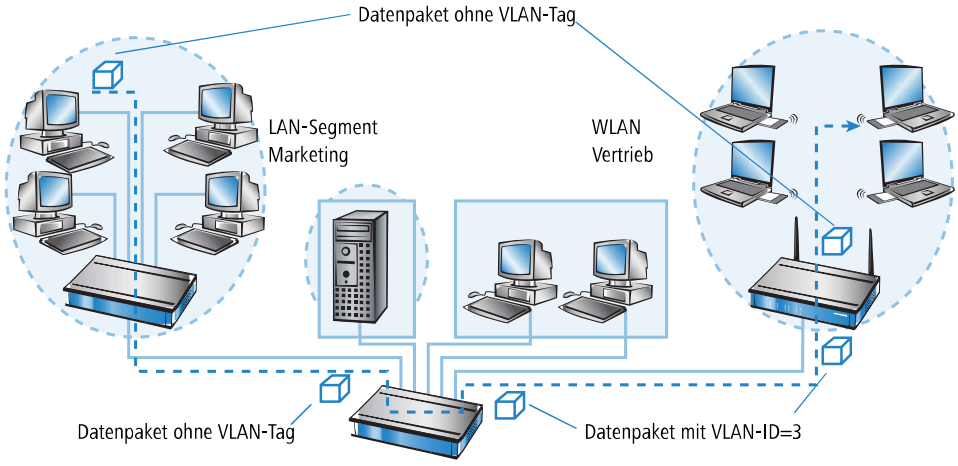
Ältere Switches im LAN können überlange Frames möglicherweise nicht richtig zwischen den einzelnen Ports weiterleiten und verwerfen die getaggten Pakete.

12.2.2 Umsetzung in den Schnittstellen des LANs

Mit den virtuellen LANs sollen bestimmte Stationen zu logischen Einheiten zusammengefasst werden. Die Stationen selbst können aber die notwendigen VLAN-Tags in der Regel weder erzeugen noch verarbeiten.

Der Datenverkehr zwischen den Netzteilnehmern läuft immer über die verschiedenen Schnittstellen (Interfaces) der Verteiler im LAN. Diesen Verteilern (Switches, Basisstationen) fällt damit also die Aufgabe zu, die VLAN-Tags der gewünschten Anwendung entsprechend in die Datenpakete einzubauen, sie auszuwerten und ggf. wieder zu entfernen. Da die logischen Einheiten jeweils mit den verschiedenen Interfaces der Verteiler verbunden sind, werden die Regeln über die Generierung und Verarbeitung der VLAN-Tags den einzelnen Schnittstellen zugewiesen.

Greifen wir dazu das erste Beispiel wieder auf:



Ein Rechner aus dem Marketing schickt ein Datenpaket an einen Rechner im Vertrieb. Der Hub im Marketing leitet das Paket einfach weiter an den Switch. Der Switch empfängt das Paket auf seinem Port Nr. 1 und weiß, dass dieser Port zum VLAN mit der VLAN-ID 3 gehört. Er setzt in den MAC-Frame das zusätzliche Feld mit dem richtigen VLAN-Tag ein und gibt das Paket auch nur auf den Ports (2 und 5) wieder aus, die ebenfalls zum VLAN 3 gehören. Die Basisstation im Vertrieb empfängt das Paket auf dem LAN-Interface. Anhand der Einstellungen kann die Basisstation erkennen, dass die WLAN-Schnittstelle ebenfalls zum VLAN 3 gehört. Sie entfernt das VLAN-Tag aus dem MAC-Frame und gibt das Paket auf der drahtlosen Schnittstelle wieder aus. Der Client im WLAN kann das Paket, das nun wieder die normale Länge hat, wie jedes andere Datenpaket ohne VLAN-Tagging verarbeiten.

12.2.3 Anwendungsbeispiele

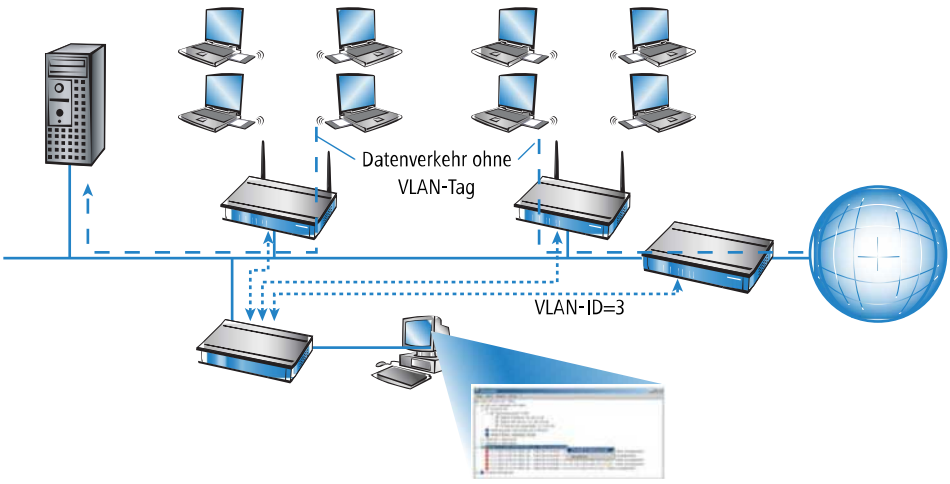
Die Hauptanwendung von virtuellen LANs ist die Aufgabe, auf einem physikalischen Ethernetstrang unterschiedliche logische Netzwerke einzurichten, deren Datenverkehr vor den anderen logischen Netzen geschützt ist.

Die folgenden Abschnitte zeigen Beispiele für den Einsatz von virtuellen LANs vor diesem Hintergrund.

12.2.3.1 Management- und User-Traffic auf einem LAN

Auf dem Campus einer Universität werden mehrere Hotspots aufgestellt. Damit ist den Studenten über Notebooks mit WLAN der Zugang zum Server der Bibliothek und zum Internet möglich. Die Hotspots sind an das LAN der Universität

angeschlossen. Über dieses LAN greifen die Administratoren auch auf die Basisstationen zu, um über SNMP verschiedene Management-Aufgaben zu erledigen.

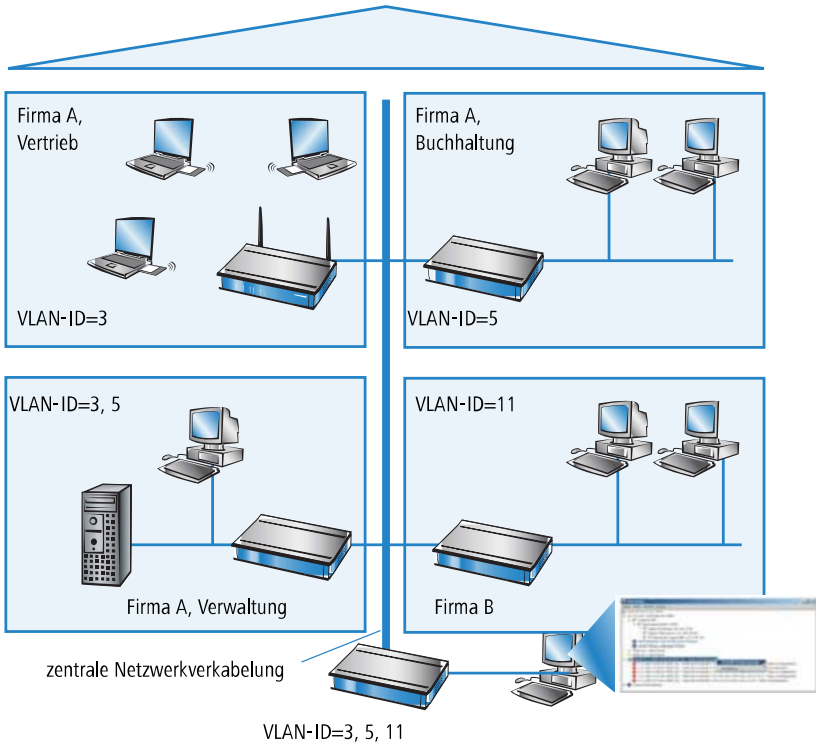


Mit dem Einrichten eines virtuellen LANs zwischen den Basisstationen und dem Switch der Administratoren wird der Management-Datenverkehr von dem „öffentlichen" Verkehr auf dem LAN abgeschirmt.

12.2.3.2 Verschiedene Organisationen auf einem LAN

Die Flexibilität der modernen Arbeitswelt bringt für die Administratoren neue Herausforderungen an die Planung und Wartung der Netzwerkstrukturen. In öffentlichen Bürogebäuden ändert sich permanent die Belegung der Räume durch die Mieter, und auch innerhalb einer Firma werden die Teams häufig neu zusammengestellt. In beiden Fällen müssen die einzelnen Einheiten jedoch über ein unabhängiges, abgeschirmtes LAN verfügen. Diese Aufgabe lässt sich mit

Änderungen an der Hardware nur sehr aufwändig oder gar nicht realisieren, weil z. B. in einem Bürogebäude nur eine zentrale Verkabelung vorhanden ist.



Mit virtuellen LANs lässt sich diese Aufgabe sehr elegant lösen. Auch bei einem späteren Wechsel von Abteilungen oder Firmen im Gebäude kann die Netzstruktur sehr einfach angepasst werden.

Alle Netzteilnehmer nutzen in diesem Beispiel das zentrale Ethernet, das mit den angeschlossenen Geräten von einem Dienstleister überwacht wird. Die Firma A hat drei Abteilungen in zwei Etagen. Der Vertrieb kann über die VLAN-ID 3 mit der Verwaltung kommunizieren, die Buchhaltung mit der Verwaltung über die VLAN-ID 5. Untereinander sehen sich die Netze von Buchhaltung und Vertrieb nicht. Die Firma B ist über die VLAN-ID 11 ebenfalls von den anderen Netzen abgeschirmt, nur der Dienstleister kann zu Wartungszwecken auf alle Geräte zugreifen.

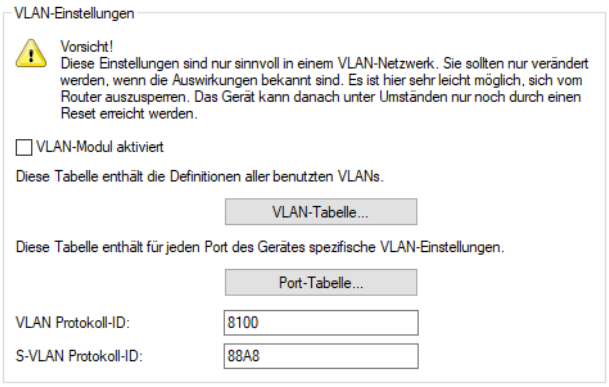
12.3 Konfiguration von VLANs

Die Konfiguration im VLAN-Bereich der Geräte hat zwei wichtige Aufgaben:

- Virtuelle LANs definieren und ihnen dabei einen Namen, eine VLAN-ID und die zugehörigen Interfaces zuordnen
- Für die Interfaces definieren, wie mit Datenpaketen mit bzw. ohne VLAN-Tags verfahren werden soll

12.3.1 Allgemeine Einstellungen

In diesem Dialog finden Sie die allgemeinen Einstellungen für das VLAN.



LANconfig: **Schnittstellen** > **VLAN**

Konsole: **Setup** > **VLAN**

12.3.1.1 VLAN-Modul aktivieren

Schalten Sie das VLAN-Modul nur ein, wenn Sie mit den Auswirkungen der VLAN-Nutzung vertraut sind.

Mit fehlerhaften VLAN-Einstellungen können Sie den Konfigurationszugang zum Gerät verhindern.

Um eine funktionierende initiale VLAN-Konfiguration zu erhalten, ist es neben dem Einschalten des VLAN-Moduls ebenfalls erforderlich, die VLAN-ID des Management-IP-Netzes (normalerweise „Intranet“) anzupassen – in der Regel auf die VLAN-ID 1, die im VLAN-Modul bei Standardeinstellungen die Port-VLAN-ID ist. Diese Schritte müssen zusammen ausgeführt werden, z. B. via LANconfig oder mittels der WEBconfig-Aktion unter **Extras** > **VLAN Modul aktivieren**. Ein Klick auf **Ausführen** aktiviert das VLAN-Modul und führt gleichzeitig eine Anpassung aller IPv4- und IPv6-Netzwerke, welche die VLAN-ID 0 haben, auf die VLAN-ID 1 durch.

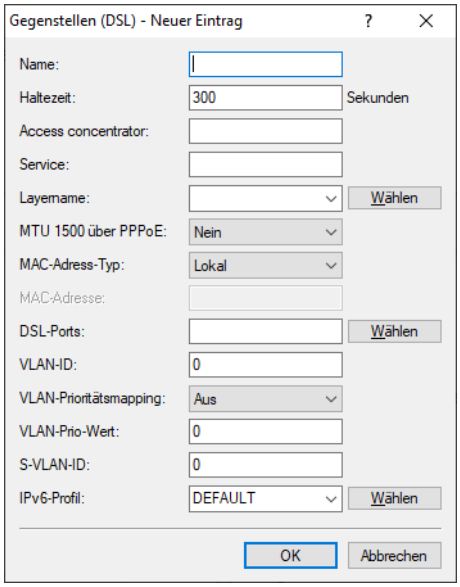
12.3.1.2 VLAN-Tagging-Modus

Beim Übertragen von VLAN-getaggten Netzen über Netze der Provider, die ihrerseits VLAN verwenden, setzen die Provider teilweise spezielle VLAN-Tagging-IDs ein. Um die VLAN-Übertragung darauf einzustellen, kann der Ethernet2-Typ des VLAN-Tags als Tag-Value als 16-Bit-Hexadezimalwert eingestellt werden. Default ist 8100 (VLAN-Tagging nach 802.1p/q), andere gängige Werte für VLAN-Tagging wären z. B. 9100 oder 9901.

12.3.1.3 Q-in-Q-VLAN

Der Router unterstützt doppeltes VLAN-Tagging („stacked VLAN“) bzw. Q-in-Q-VLAN nach IEEE 802.1ad auf WAN-Verbindungen. Mit Q-in-Q-VLAN können Service Provider Layer-2-Ethernetverbindungen zwischen Kundenstandorten

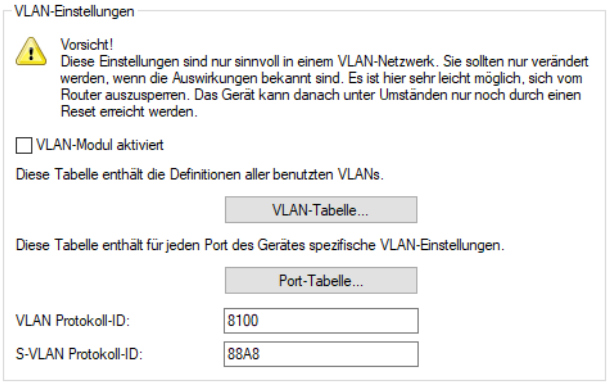
ermöglichen und das kundeneigene VLAN unverändert übertragen. Das innere VLAN (C-VLAN) wird dabei vom Kunden verwendet, das äußere VLAN (S-VLAN) vom Service Provider.



LANconfig: **Kommunikation** > **Gegenstellen** > **Gegenstellen (DSL)**

S-VLAN-ID

Konfigurieren Sie hier das S-VLAN bei doppeltem VLAN-Tagging (Q-in-Q-VLAN-Verbindungen nach IEEE 802.1ad). Das VLAN wird auch als äußeres VLAN bezeichnet. Die verwendete S-VLAN-Protokoll-ID kann unter **Schnittstellen** > **VLAN** konfiguriert werden.



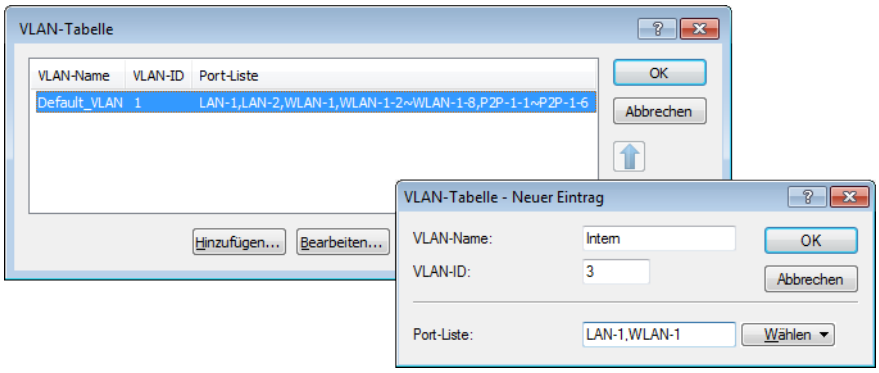
LANconfig: **Schnittstellen** > **VLAN**

S-VLAN Protokoll-ID

Definiert die VLAN-Tagging-ID für Q-in-Q-VLAN-Tagging. Der Ethernet2-Typ des VLAN-Tags wird als „Tag-Value“ als 16 Bit-Hexadezimalwert konfiguriert. Default nach IEEE 802.1ad ist „88a8“, ein anderer gängiger Wert für VLAN-Tagging wäre z. B. „8100“.

12.3.2 Die Netzwerktabelle

In der Netzwerktabelle werden die virtuellen LANs definiert, an denen das Gerät teilnehmen soll.



LANconfig: **Schnittstellen** > **VLAN** > **VLAN-Tabelle**

Konsole: **Setup** > **VLAN** > **Netzwerke**

VLAN-Name

Der Name des VLANs dient nur der Beschreibung bei der Konfiguration. Dieser Name wird an keiner anderen Stelle verwendet.

VLAN-ID

Diese Nummer kennzeichnet das VLAN eindeutig.

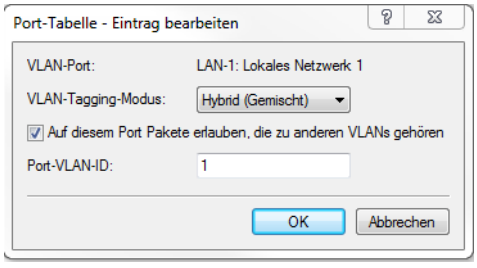
Portliste

In dieser Liste werden die Interfaces des Geräts eingetragen, die zu dem VLAN gehören.

Für ein Gerät mit einem LAN-Interface und einem WLAN-Port können z. B. die Ports “LAN-1” und “WLAN-1” eingetragen werden. Bei Portbereichen werden die einzelnen Ports durch eine Tilde getrennt: “P2P-1~P2P-4”.

12.3.3 Die Porttabelle

In der Porttabelle werden die einzelnen Ports des Gerätes für die Verwendung im VLAN konfiguriert. Die Tabelle hat einen Eintrag für jeden Port des Gerätes mit folgenden Werten:



LANconfig: **Schnittstellen** > **VLAN** > **Port-Tabelle**

Konsole: **Setup** > **VLAN** > **Port-Tabelle**

Port

Der Name des Ports, nicht editierbar

Tagging-Modus

Steuert die Verarbeitung und Zuweisung von VLAN-Tags auf diesem Port.

Access (Niemals)

Ausgehende Pakete erhalten auf diesem Port kein VLAN-Tag. Eingehende Pakete werden so behandelt, als hätten sie kein VLAN-Tag. Haben die eingehenden Pakete ein VLAN-Tag, so wird es ignoriert und so behandelt, als ob es zur Payload des Paketes gehört. Eingehende Pakete werden immer dem für diesen Port definierten VLAN zugewiesen.

Trunk (Immer)

Ausgehende Pakete erhalten auf diesem Port immer ein VLAN-Tag, egal ob sie dem für diesen Port definierten VLAN angehören oder nicht. Eingehende Pakete müssen über ein VLAN-Tag verfügen, anderenfalls werden sie verworfen.

Hybrid (Gemischt)

Erlaubt einen gemischten Betrieb von Paketen mit und ohne VLAN-Tags auf dem Port. Pakete ohne VLAN-Tag werden dem für diesen Port definierten VLAN zugeordnet. Ausgehende Pakete erhalten ein VLAN-Tag, außer sie gehören dem für diesen Port definierten VLAN an.

Auf diesem Port Pakete erlauben, die zu anderen VLANs gehören

Diese Option gibt an, ob getaggte Datenpakete mit beliebigen VLAN-IDs akzeptiert werden sollen, auch wenn der Port nicht Mitglied dieses VLANs ist.

Port-VLAN-ID

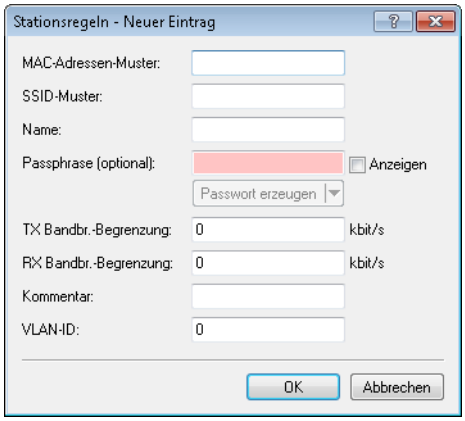
Diese Port-ID hat zwei Funktionen:

- Ungetaggte Pakete, die auf diesem Port im Modus **Hybrid (gemischt)** empfangen werden, werden diesem VLAN zugeordnet, ebenso sämtliche ankommenden Pakete im Modus **Access (Niemals)**.
- Im Modus **Hybrid (gemischt)** entscheidet dieser Wert darüber, ob ausgehende Pakete ein VLAN-Tag erhalten oder nicht: Pakete, die dem für diesen Port definierten VLAN zugeordnet wurden, erhalten **kein** VLAN-Tag, alle anderen erhalten ein VLAN-Tag.

12.4 Konfigurierbare VLAN-IDs

12.4.1 VLAN-IDs für WLAN-Clients

VLANs werden im Gerät üblicherweise fest mit einem LAN-Interface verbunden. Alle Pakete, die über dieses Interface geleitet werden, bekommen daher bei Aktivierung des VLAN-Moduls die gleiche VLAN-ID. In manchen Fällen ist es jedoch erwünscht, die verschiedenen Benutzer eines WLANs auch unterschiedlichen VLANs zuzuordnen.



LANconfig: **Wireless-LAN** > **Stationen/LEPS** > **Stationsregeln**

Konsole: **Setup** > **WLAN** > **Access-List**

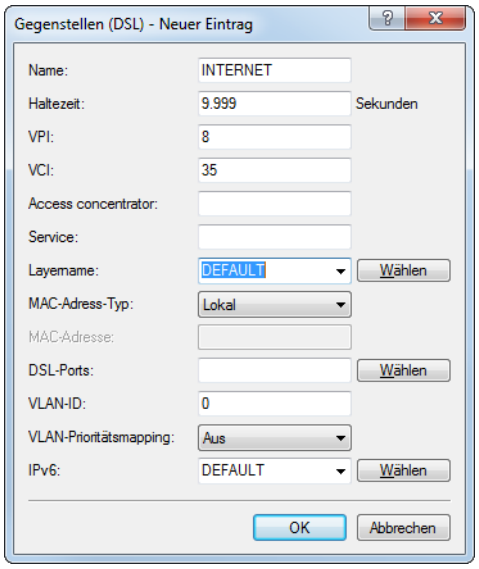
Die client-spezifische VLAN-ID kann Werte von 0 bis 4094 annehmen. Der Defaultwert von 0 steht für eine nicht spezifizierte VLAN-ID. In diesem Fall wird der Client dem VLAN-Port des logischen WLAN-Netzwerks zugeordnet.

Folgende Voraussetzungen müssen erfüllt sein, damit die client-spezifische VLAN-Zuweisung gelingt:

- Der VLAN-Betrieb muss aktiviert sein.
- Die VLAN-IDs, die einzelnen Clients zugewiesen werden sollen, müssen in der VLAN-Netzwerk-Tabelle enthalten sein.
- Die LAN-Interfaces und alle WLAN-Interfaces, die von den Clients genutzt werden, müssen dem entsprechenden VLAN zugeordnet sein.

12.4.2 VLAN-IDs für DSL-Interfaces

In manchen DSL-Netzen werden VLAN-Tags verwendet, so wie sie auch in lokalen Netzen zur Unterscheidung von logischen Netzwerken auf gemeinsam genutzten Übertragungsmedien eingesetzt werden. Um diese VLAN-Tags im Router richtig verarbeiten zu können, kann zu jeder DSL-Gegenstelle eine entsprechende VLAN-ID definiert werden.



LANconfig: **Kommunikation** > **Gegenstellen** > **Gegenstellen (DSL)**

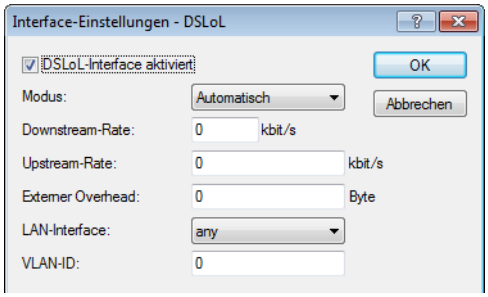
Konsole: **Setup** > **WAN** > **DSL-Breitband-Gegenstellen**

VLAN-ID

ID, mit der das VLAN auf der DSL-Verbindung eindeutig identifiziert werden kann.

12.4.3 VLAN-IDs für DSLoL-Interfaces

Um den Datenverkehr über ein DSLoL-Interface besser vom restlichem Traffic separieren zu können, kann für das DSLoL-Interface auf der Konsole unter **Setup** > **Interfaces** > **DSLoL** oder im LANconfig unter **Schnittstellen** > **WAN** > **Interface-Einstellungen** bei den Einstellungen für das DSLoL-Interface im Feld **VLAN-ID** diese ID eingestellt werden.



12.5 VLAN-Tags auf Layer 2/3 im Ethernet

12.5.1 Einleitung

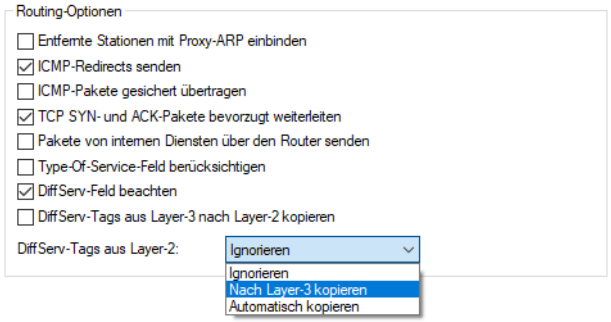
VLAN-Tags bieten auch bei solchen Switches, die keine IP-Header auswerten können, die Möglichkeit einer einfachen QoS-Steuerung. Der Standard IEEE 802.1p definiert ein Prioritäts-Tag im VLAN-Header mit einer Länge von drei Bit, das den ersten drei Bit des DSCP-Felder (Differentiated Services Code Point – DiffServ) bzw. der Precedence im ToS-Feld (Type of Service) entspricht. Bei der Verarbeitung der VLAN-getaggten Pakete müssen Empfangs- und Senderichtung getrennt betrachtet werden:

- Wird ein getaggtes Ethernet-Paket empfangen, so gibt es drei Möglichkeiten das Tag zu verarbeiten:
  - Das VLAN-Tag wird ignoriert.
  - Das VLAN-Tag wird immer in das DiffServ- bzw. TOS-Feld kopiert.
  - Das VLAN-Tag wird nur dann in das DiffServ- bzw. TOS-Feld kopiert, wenn dort noch keine Kennzeichnung vorhanden ist, die Precedence also '000' ist.
- Beim Senden eines Paketes auf das Ethernet kann das VLAN-Tag in Abhängigkeit von der Precedence gesetzt werden. Dies darf aber nur dann geschehen, wenn der Empfänger diese Tags auch versteht, d. h. getaggte Pakete empfangen kann. Daher werden die Tags nur für solche Stationen gesetzt, wenn LCOS von der jeweiligen Adresse getaggte Pakete empfangen hat.

Beim Empfang eines getaggten Pakets wird das Tag im zugehörigen Eintrag der Verbindungsliste gespeichert. Wenn ein Paket mit gesetzter Precedence gesendet werden soll, dann wird die zuvor hinterlegte VLAN-ID mit der Precedence in das Paket als VLAN-Tag eingetragen. Wenn von einer Verbindung weitere Verbindungen geöffnet werden, wie z. B. bei FTP, dann wird das Tag an die neuen Einträge vererbt.

12.5.2 Konfiguration des VLAN-Taggings auf Layer 2 / 3

Bei der Konfiguration des VLAN-Taggings auf Layer 2 / 3 wird neben den allgemeinen Routing-Einstellungen das Verhalten beim Empfangen und beim Senden getaggten Pakete definiert.



LANconfig: **IP-Router** > **Allgemein**

Konsole: **Setup** > **IP-Router** > **Routing-Methode**

Type-Of-Service-Feld berücksichtigen

Das TOS / DiffServ-Feld wird als TOS-Feld betrachtet, es werden die Bits 'Low-Delay' und 'High-Reliability' ausgewertet.

DiffServ-Feld beachten

Das TOS / DiffServ-Feld wird als DiffServ-Feld betrachtet. Nach Auswertung der Precedence werden Pakete mit den Code Points AFxx gesichert und Pakete mit den Code Points EF bevorzugt übertragen. Alle anderen Pakete werden normal übertragen.

DiffServ-Tags aus Layer-2

Die Einstellung für das Layer2-Layer3-Tagging regelt das Verhalten beim Empfangen eines Datenpakets:

Ignorieren

VLAN-Tags werden ignoriert.

Nach Layer-3 kopieren

Prioritäts-Bits im VLAN-Tag werden immer in die Precedence des DSCP kopiert.

Automatisch kopieren

Prioritäts-Bits im VLAN-Tag werden nur dann in die Precedence des DSCP kopiert, wenn diese '000' ist.

DiffServ-Tags aus Layer-3 nach Layer-2 kopieren

Die Einstellung für das Layer3-Layer2-Tagging regelt das Verhalten beim Senden eines Datenpakets. Wenn diese Option aktiviert ist, werden VLAN-Tags mit Prioritäts-Bits erzeugt, die aus der Precedence des DSCP stammen, wenn der Empfänger mindestens ein getaggtes Paket verschickt hat.

13 Wireless LAN – WLAN

13.1 Einleitung

Die folgenden Abschnitte beschreiben allgemein die Funktionalität des LCOS-Betriebssystems im Zusammenhang mit Funknetzwerken. Welche Funktionen von Ihrem Gerät unterstützt werden, entnehmen Sie bitte dem Handbuch zum jeweiligen Gerät.

In diesem Kapitel stellen wir Ihnen kurz die Technologie von Funk-Netzwerken vor. Außerdem geben wir Ihnen einen Überblick über die vielfältigen Einsatzmöglichkeiten, Funktionen und Fähigkeiten Ihrer LANCOM WLAN-Geräte.

Ein Funk-LAN verbindet einzelne Endgeräte (PCs und mobile Rechner) zu einem lokalen Netzwerk (auch LAN – **L**ocal **A**rea **N**etwork). Im Unterschied zu einem herkömmlichen LAN findet die Kommunikation nicht über Netzwerkkabel, sondern über Funkverbindungen statt. Aus diesem Grund nennt man ein Funk-LAN auch **W**ireless **L**ocal **A**rea **N**etwork (WLAN).

In einem Funk-LAN stehen alle Funktionen eines kabelgebundenen Netzwerks zur Verfügung: Zugriff auf Dateien, Server, Drucker etc. ist ebenso möglich wie die Einbindung der einzelnen Stationen in ein firmeninternes Mailsystem oder der Zugang zum Internet.

Die Vorteile von Funk-LANs liegen auf der Hand: Notebooks und PCs können dort aufgestellt werden, wo es sinnvoll ist – Probleme mit fehlenden Anschlüssen oder baulichen Veränderungen gehören bei der drahtlosen Vernetzung der Vergangenheit an. Funk-LANs sind außerdem einsetzbar für Verbindungen über größere Distanzen. Teure Mietleitungen und die damit verbundenen baulichen Maßnahmen können gespart werden.

LANCOM Systems unterscheidet zwei Typen von WLAN-Geräten, die für verschiedene Einsatzbereich vorgesehen sind und dementsprechend spezielle Funktionen und Konfigurationsmöglichkeiten bieten:

- LANCOM Access Points (APs) werden üblicherweise verwendet, um ein oder mehrere WLANs mit kabelgebundenen LAN zu verbinden. Sie übertragen dabei die Daten der Clients nur in der Funktion einer „Bridge“, das Routing ins Internet oder zu anderen Gegenstellen wird von anderen Netzwerkkomponenten übernommen. Die APs verfügen daher in der Regel nur über eine oder mehrere Ethernetschnittstellen.
- LANCOM Wireless Router verfügen neben einer oder mehreren Ethernetschnittstellen zusätzlich über WAN-Schnittstellen für VDSL, ADSL und / oder DSL. Diese Geräte verbinden die WLAN-Funktionen mit der Aufgabe des Routings in das Internet oder zu anderen Gegenstellen in einer zentralen Netzwerkkomponente.

In den folgenden Abschnitten wird meistens der Begriff “Access Point” als Synonym für beide Gerätetypen verwendet, sofern nicht explizit zwischen LANCOM Wireless Router und LANCOM Access Point unterschieden wird.

Die Geräte können entweder als autarke APs mit eigener Konfiguration betrieben werden (WLAN-Module in der Betriebsart „Access Point-Modus“) oder als Teilnehmer in einer WLAN-Infrastruktur, die von einem zentralen WLAN-Controller (WLC) gesteuert wird (Betriebsart „Managed-Modus“).

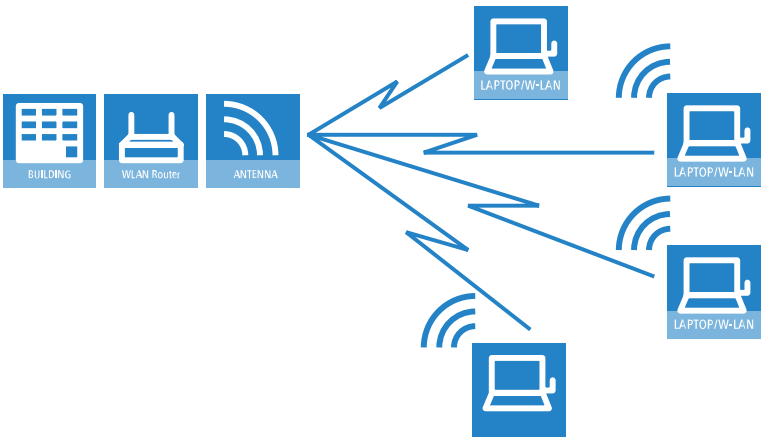
13.2 Anwendungsszenarien

WLAN-Systeme eignen sich in vielen Bereichen als Ersatz für oder Ergänzung zu verkabelten Netzwerken. In manchen Fällen bieten WLANs sogar völlig neue Anwendungsmöglichkeiten, die einen enormen Fortschritt in der Organisation der Arbeit oder deutliche Einsparpotenziale bedeuten.

- Größere Funk-LANs, evtl. Anschluss an LAN und Internet mit einem oder mehreren APs (Infrastruktur-Modus)
- Hotspot oder Gastzugang
- Verbinden zweier LANs über eine Funkstrecke (Point-to-Point-Modus)
- Relaisfunktion zur Verbindung von Netzwerken über mehrere APs
- Anbindung von Geräten mit Ethernet-Schnittstelle über einen AP (Client-Modus)
- Zentrale Verwaltung durch einen WLC (Managed-Modus)
- WDS (Wireless Distribution System)
- Datenübertragung zu bewegten Objekten im Industriebereich
- Durchleiten von VPN-verschlüsselten Verbindungen mit VPN Pass-Through
- Einfache, direkte Verbindung zwischen Endgeräten ohne AP (Ad-hoc-Modus)

13.2.1 Infrastruktur-Modus

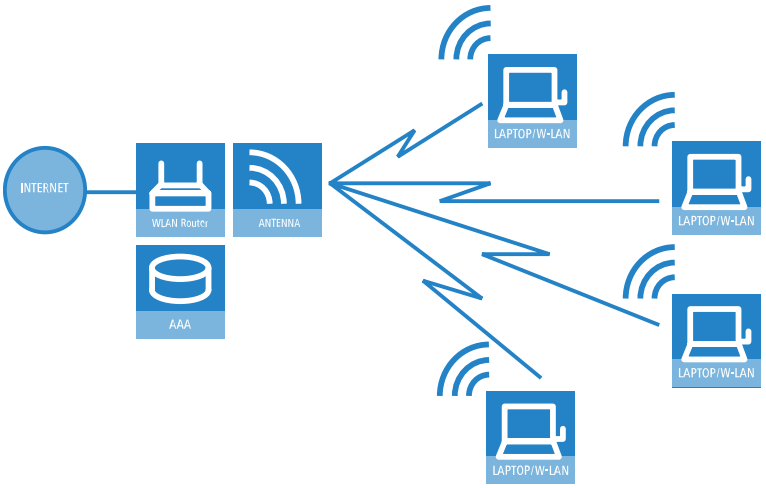
Im Infrastruktur-Modus verbinden sich die WLAN-Clients mit einem zentralen Vermittlungspunkt, dem AP. Der AP spannt eine oder mehrere Funkzellen (WLAN-Netzwerke) auf, regelt die Zugangsrechte der WLAN-Clients zu diesen Funkzellen, die Kommunikation der Clients untereinander und den Zugang zu anderen Netzwerken. In größeren WLAN-Anwendungen (z. B. in Unternehmen, deren Geschäftsräume sich über mehrere Gebäude oder Etagen verteilen) können auch mehrere verbundene APs einen gemeinsamen Zugang für WLAN-Clients anbieten. Je nach Bedarf können die Clients zwischen den verschiedenen APs wechseln (Roaming). Da diese Lösung in vielen Hochschulen und Universitäten eingesetzt wird, um den Studenten und wissenschaftlichen Mitarbeitern überall einen Netzwerkzugang zu ermöglichen, spricht man hier auch von „Campus-Ausleuchtung".



13.2.2 Hotspot oder Gastzugang

Bei einem Hotspot handelt es sich um eine spezielle Variante des zuvor beschriebenen Infrastruktur-Modus. Während der normale Infrastruktur-Modus nur den Mitgliedern einer geschlossenen Benutzergruppe einen Zugang zum Netzwerk mit allen erforderlichen Diensten erlaubt, bietet ein Hotspot gegen Zahlung einer entsprechenden Gebühr allen WLAN-Clients in Reichweite den Netzwerkzugang an (in der Regel beschränkt auf Internetnutzung). Neben den Unterschieden in der Konfiguration der APs werden für den Aufbau eines Hotspots Authentisierungs-, Authorisierungs- und Accountingfunktionen (AAA) benötigt, wie sie beispielsweise die Public Spot Optionen bereitstellen. Hotspots werden üblicherweise an öffentlichen Orten eingesetzt, an denen sich viele Personen mit Bedarf für einen vorübergehenden Internetzugang aufhalten, z. B. auf Flughäfen, in Cafés oder Hotels.

Ein Hotspot bietet einem WLAN-Client ohne Konfigurationsaufwand im AP und nur für eine bestimmte Zeit einen Zugang zum Netzwerk – daher wird diese Variante auch häufig in Unternehmen eingesetzt, um Gästen z. B. einen vorübergehenden Internetzugang zu ermöglichen.

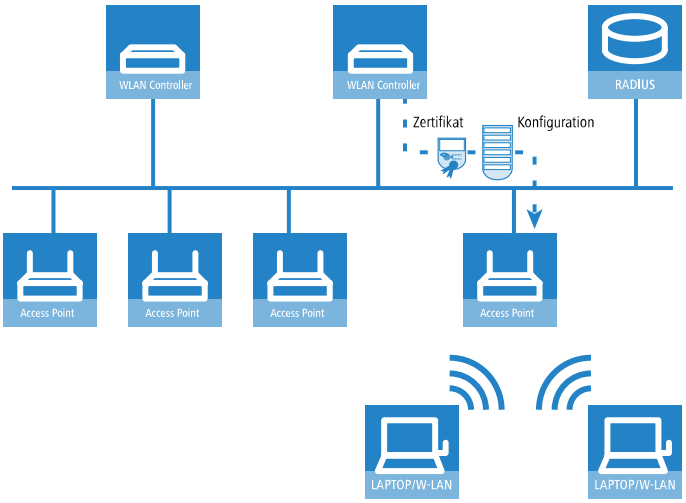


13.2.3 Managed-Modus

Der weit verbreitete Einsatz von Wireless-Geräten hat zu einem deutlich komfortableren und flexibleren Zugang zu Netzwerken in Firmen, Universitäten und anderen Organisationen geführt. Mit einem zentralen WLAN-Management wird die Konfiguration der APs im Managed-Modus nicht mehr in den Geräten selbst vorgenommen, sondern in einer zentralen Instanz, dem WLAN-Controller (WLC).

Der WLC authentifiziert die APs und überträgt den zugelassenen Geräten ein Zertifikat und eine passende Konfiguration. Dadurch kann die Konfiguration des WLANs komfortabel von einer zentralen Stelle übernommen werden und die Konfigurationsänderungen wirken sich zeitgleich auf alle APs aus.

Mit Hilfe des Split-Managements kann die WLAN-Konfiguration von der restlichen Router-Konfiguration getrennt werden. Auf diese Weise können z. B. in Filialen oder Home-Offices die Router- und VPN-Einstellungen lokal erfolgen, die WLAN-Konfiguration kann über einen LANCOM WLAN Controller in der Zentrale erfolgen.



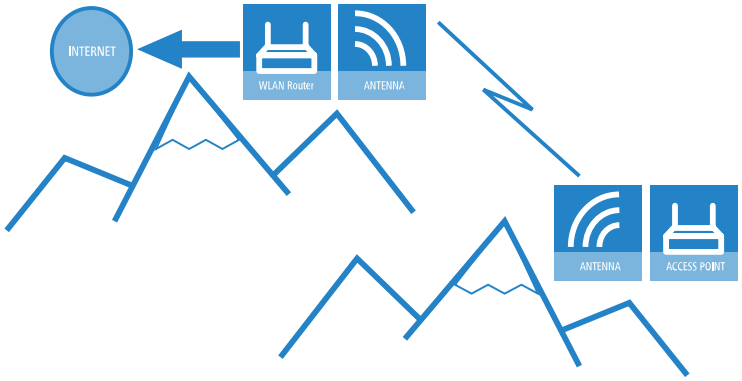
13.2.4 WLAN-Bridge (Point-to-Point)

Während es sich bei den bisher vorgestellten Anwendungsszenarien immer um die Anbindung von mehreren WLAN-Clients an einen AP handelt (Point-to-Multipoint), spielen die WLAN-Systeme gerade im Outdoor-Bereich ihre Stärken auch und vor allem bei der Verbindung von zwei APs aus (Point-to-Point). Mit der Einrichtung einer Funkstrecke zwischen zwei

APs kann z. B. ein Produktionsgebäude auf einem weitläufigen Unternehmensgelände sehr einfach in das Netzwerk eingebunden werden.



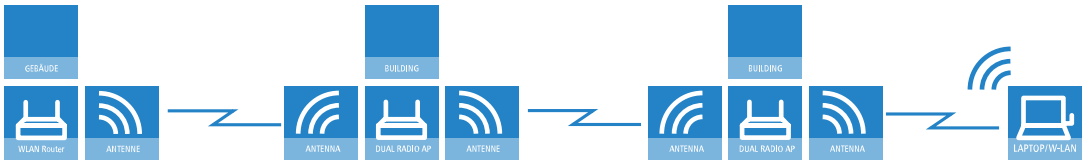
Mit einer Punkt-zu-Punkt-Verbindung kann aber z. B. auch in schwierigem Gelände (z. B. in den Bergen oder auf einer Insel) ein Internetzugang an Orten bereitgestellt werden, an denen eine Verkabelung zu aufwendig wäre. Bei direkter Sichtbeziehungen zwischen den beiden APs können mit diesen Funkstrecken Distanzen von mehreren Kilometern überbrückt werden.



13.2.5 WLAN-Bridge im Relais-Betrieb

In manchen Fällen müssen größere Distanzen zwischen zwei Standorten überbrückt werden als mit einer einfachen Funkstrecke realisiert werden kann. Das ist z. B. dann der Fall, wenn die Distanz zwischen den APs über die tatsächliche Reichweite hinausgeht oder wenn Hindernisse zwischen den APs die direkte Funkübertragung stören oder verhindern.

In solchen Fällen kann durch eine Verkettung von mehreren APs mit jeweils zwei WLAN-Modulen eine Verbindung zwischen den beiden Endpunkten hergestellt werden. Da die APs an den Zwischenstationen in der Regel nur als Schaltstelle dienen, nennt man diese Betriebsart der APs auch „Relais-Modus".

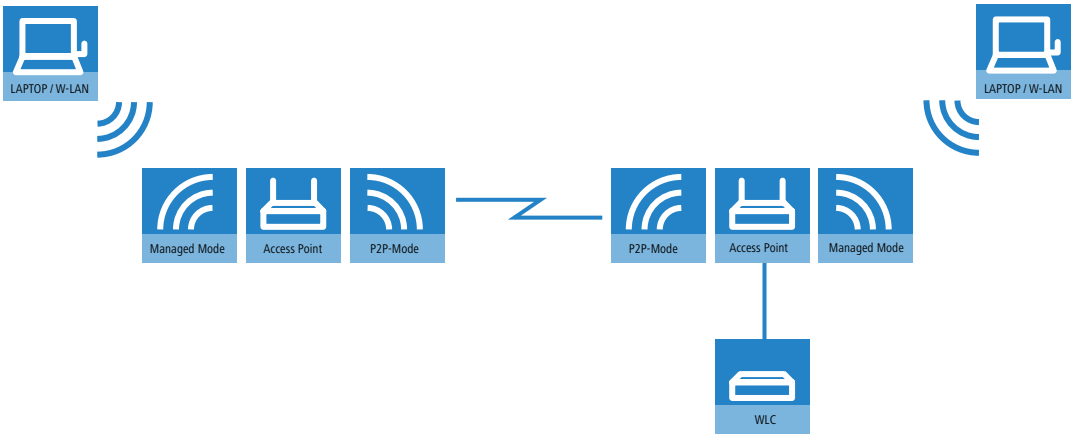


Obwohl LANCOM APs auch pro Radio-Modul neben WLAN-Clients auch noch mehrere P2P-Strecken gleichzeitig bedienen können, empfiehlt sich aus Performance-Gründen die Verwendung von LANCOM Access Points mit zwei Funkmodulen für die Relais-Stationen.

13.2.6 WLAN-Bridge zum AP – managed und unmanaged gemischt

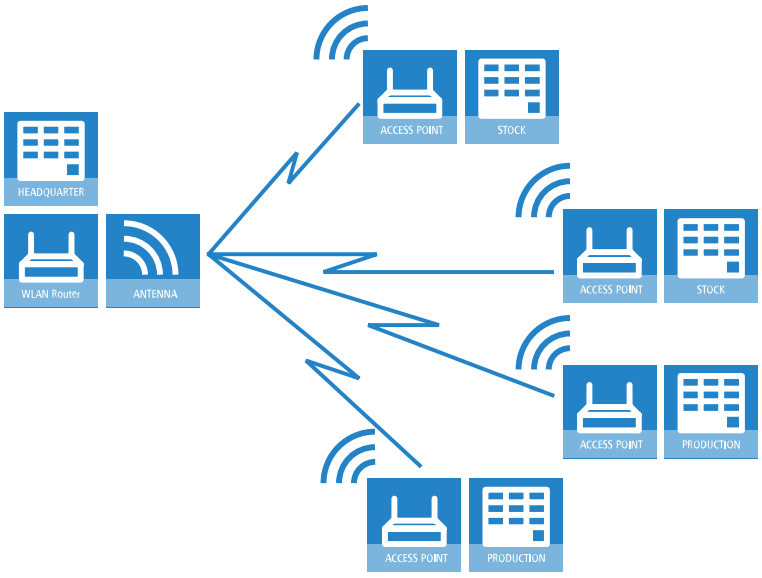
Die von einem zentralen WLC verwalteten APs werden in der Regel direkt mit dem kabelgebundenen Ethernet verbunden. Wenn das nicht möglich ist, können die managed APs auch über eine WLAN-Bridge in das LAN eingebunden werden,

sofern sie über zwei WLAN-Module verfügen. Ein WLAN-Modul wird in diesem Anwendungsfall als managed AP betrieben, dieses WLAN-Modul bezieht seine Konfiguration immer zentral vom WLC. Das andere WLAN-Modul wird dabei fest als WLAN-Bridge konfiguriert.



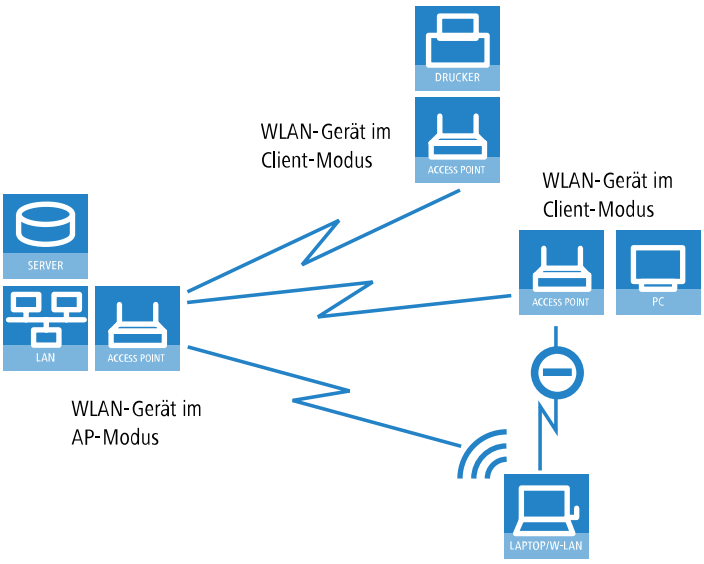
13.2.7 Wireless Distribution System (Point-to-Multipoint)

Eine besondere Variante der Funkstrecken ist die Anbindung von mehreren verteilten APs an eine zentrale Station – das Point-to-Multipoint-WLAN (P2MP) wird auch als Wireless Distribution System bezeichnet (WDS). In dieser Betriebsart werden z. B. mehrere Gebäude auf einem Betriebsgelände mit dem Verwaltungsgebäude verbunden. Der zentrale AP oder Wireless Router wird dabei als „Master" konfiguriert, die WDS-Gegenstellen als „Slave".



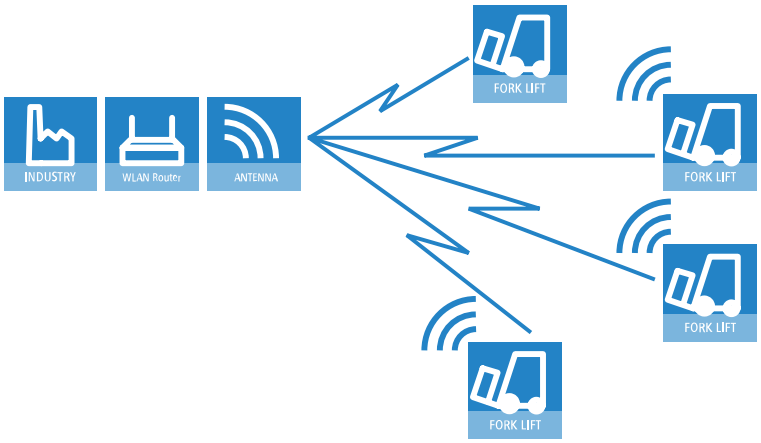
13.2.8 Client-Modus

Zur Anbindung von einzelnen Geräten mit einer Ethernet-Schnittstelle in ein WLAN können APs in den sogenannten Client-Modus versetzt werden, in dem sie sich wie ein herkömmlicher WLAN-Adapter verhalten und nicht wie ein AP. Über den Client-Modus ist es also möglich, auch Geräte wie PCs oder Drucker, die ausschließlich über eine Ethernet-Schnittstelle verfügen, in ein WLAN einzubinden.



13.2.9 Client-Modus bei bewegten Objekten im Industriebereich

Völlig neue Anwendungen ermöglichen WLAN-Systeme im industriellen Bereich durch die Datenübertragung zu bewegten Objekten. So ist z. B. in der Logistik eine kontinuierliche Anbindung von Gabelstaplern über WLAN an das Firmennetzwerk möglich. Mit mobilen Barcode-Scannern ausgestattet können so alle Warenbewegungen in einem Lager in Echtzeit an das Warenwirtschaftssystem weitergegeben werden, sodass alle Mitarbeiter jederzeit auf einen aktuellen Lagerbestand zugreifen können.



13.3 WLAN-Standards

LANCOM WLAN-Geräte arbeiten nach dem Standard IEEE 802.11. Diese Standard-Familie stellt eine Erweiterung der bereits vorhandenen IEEE-Normen für LANs dar, von denen IEEE 802.3 für Ethernet die bekannteste ist. Innerhalb der IEEE 802.11 Familie gibt es verschiedene Standards für die Funkübertragung in unterschiedlichen Frequenzbereichen und mit unterschiedlichen Geschwindigkeiten.

Durch die Einhaltung der IEEE-Standards arbeiten die LANCOM WLAN-Geräte problemlos und zuverlässig auch mit Geräten anderer Hersteller zusammen.

Der Betrieb des integrierten WLAN-Moduls der Access Points ist jeweils nur in einem Frequenzband, also entweder 2,4 GHz oder 5 GHz möglich. Der gleichzeitige Betrieb verschiedener Frequenzbänder in einem WLAN-Modul ist nicht möglich – Access Points mit zwei WLAN-Modulen (Dual-Radio) können hingegen für jedes WLAN-Modul Hardware-abhängig ein anderes Frequenzband nutzen. Da die Standards abwärtskompatibel zueinander sind, ist der gleichzeitige Betrieb dieser Standards auf einem WLAN-Modul mit Geschwindigkeitseinbußen möglich.

13.4 WLAN-Sicherheit

13.4.1 Grundbegriffe

Auch wenn immer wieder in Zusammenhang mit Computernetzen pauschal von „Sicherheit" gesprochen wird, so ist es doch für die folgenden Ausführungen wichtig, die dabei gestellten Forderungen etwas näher zu differenzieren.

13.4.1.1 Authentifizierung

Als ersten Punkt der Sicherheit betrachten wir den Zugangsschutz:

- Dabei handelt es sich zum einen um einen Schutzmechanismus, der nur autorisierten Nutzern den Zugang zum Netzwerk gewährt.
- Zum anderen soll aber auch sichergestellt werden, dass der Client sich mit genau dem gewünschten AP verbindet, und nicht mit einem von unbefugten Dritten eingeschmuggelten AP mit dem gleichen Netzwerk-Namen. So eine Authentifizierung kann z. B. durch Zertifikate oder Passwörter gewährleistet werden.

13.4.1.2 Authentizität

Authentizität: Nachweis der Urheberschaft von Daten und der Echtheit des Datenmaterials; die Durchführung eines solchen Nachweises bezeichnet man als Authentifizierung.

13.4.1.3 Integrität

Ist der Zugang einmal gewährt, so möchte man sicherstellen, dass Datenpakete den Empfänger unverfälscht erreichen, d. h. dass niemand die Pakete verändert oder andere Daten in den Kommunikationsweg einschleusen kann. Die Manipulation der Datenpakete selbst kann man nicht verhindern; aber man kann durch geeignete Prüfsummenverfahren veränderte Pakete identifizieren und verwerfen.

13.4.1.4 Vertraulichkeit

Vom Zugangsschutz getrennt zu sehen ist die Vertraulichkeit, d. h. unbefugte Dritte dürfen nicht in der Lage sein, den Datenverkehr mitzulesen. Dazu werden die Daten verschlüsselt. Solche Verschlüsselungsverfahren sind z. B. AES oder RC4. Zur Verschlüsselung gehört natürlich auf der Empfängerseite eine entsprechende Entschlüsselung, üblicherweise mit dem gleichen Schlüssel (so genannte symmetrische Verschlüsselungsverfahren). Dabei ergibt sich natürlich das Problem, wie der Sender dem Empfänger den verwendeten Schlüssel erstmalig mitteilt – eine einfache Übertragung könnte von einem Dritten sehr einfach mitgelesen werden, der damit den Datenverkehr leicht entschlüsseln könnte.

Im einfachsten Fall überlässt man dieses Problem dem Anwender, d. h. man setzt die Möglichkeit voraus, dass er die Schlüssel auf beiden Seiten der Verbindung bekannt machen kann. In diesem Fall spricht man von Pre-Shared-Keys oder kurz PSK.

Ausgefeiltere Verfahren kommen dann zum Einsatz, wenn der Einsatz von PSK nicht praktikabel ist, z. B. in einer über SSL aufgebauten HTTP-Verbindung – hierbei kann der Anwender nicht so einfach an den Schlüssel von einem entfernten Web-Server gelangen. In diesem Falle werden so genannte asymmetrische Verschlüsselungsverfahren wie z. B. RSA eingesetzt, d. h. zum **Ent**schlüsseln der Daten wird ein anderer Schlüssel als zum **Ver**schlüsseln benutzt, es kommen also

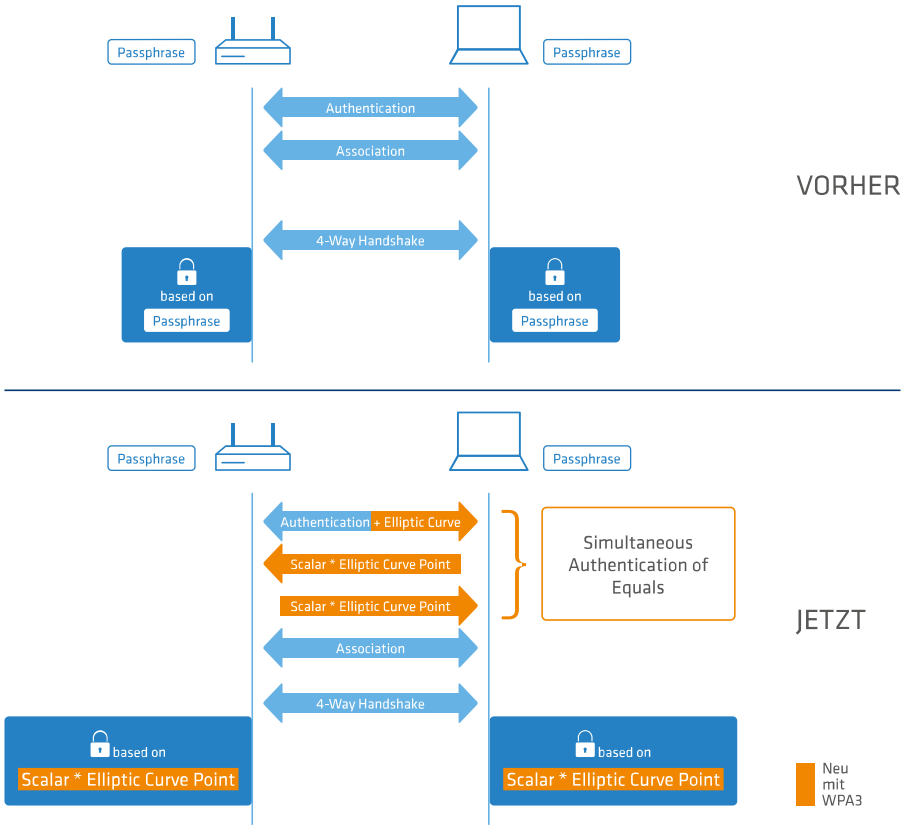
Schlüsselpaare zum Einsatz. Solche Verfahren sind jedoch viel langsamer als symmetrische Verschlüsselungsverfahren, was zu einer zweistufigen Lösung führt:

- Der Sender verfügt über ein asymmetrisches Schlüsselpaar. Den öffentlichen Teil dieses Schlüsselpaares, also den Schlüssel zum **Ver**schlüsseln, überträgt er an den Empfänger, z. B. in Form eines Zertifikats. Da dieser Teil des Schlüsselpaares nicht zum **Ent**schlüsseln genutzt werden kann, gibt es hier keine Bedenken bzgl. der Sicherheit.
- Der Empfänger wählt einen beliebigen symmetrischen Schlüssel aus. Dieser symmetrische Schlüssel, der sowohl zum **Ver**- als auch zum **Ent**schlüsseln dient, muss nun gesichert zum Sender übertragen werden. Dazu wird er mit dem öffentlichen Schlüssel des Senders verschlüsselt und an den Sender zurückgeschickt. Der symmetrische Schlüssel kann nun ausschließlich mit dem privaten Schlüssel des Senders wieder entschlüsselt werden. Ein potenzieller Mithörer des Schlüsselaustauschs kann diese Information aber nicht entschlüsseln, die Übertragung des symmetrischen Schlüssels ist also gesichert.

13.4.2 WPA3 (Wi-Fi Protected Access 3)

Der 2018 eingeführte WPA3-Standard der Wi-Fi-Alliance bietet gegenüber dem bereits 2004 eingeführten Vorgängerstandard WPA2 eine verbesserte Sicherheit durch eine Kombination verschiedener aktueller Sicherheitsverfahren. Wie WPA2 existiert auch WPA3 in den Ausprägungen WPA3-Personal und WPA3-Enterprise.

WPA3-Personal bietet durch die Verwendung des Authentisierungsverfahrens Simultaneous Authentication of Equals (SAE) eine Methode, die lediglich ein Passwort für die Authentifizierung voraussetzt und dennoch Brute-Force- und Wörterbuch-Attacken ins Leere laufen lässt. Zudem bietet dieses Verfahren erstmalig Forward Secrecy – dies bedeutet, dass in der Vergangenheit mitgeschnittener, WPA3-gesicherter Datenverkehr auch später nicht mehr entschlüsselt werden kann, wenn der Angreifer Kenntnis des Pre-Shared Keys erlangt.



Zusätzlich kann bei WPA3-Enterprise die Unterstützung für CNSA Suite B-Kryptographie eingeschaltet werden, welche ein optionaler Teil von WPA3-Enterprise für Hochsicherheitsumgebungen ist. Suite B stellt sicher, dass alle Glieder in der Verschlüsselungskette aufeinander abgestimmt sind. Suite B bildet Klassen von Bitlängen für Hash-, symmetrische und asymmetrische Verschlüsselungsverfahren, die passende Schutzniveaus bieten. So passt zum Beispiel zu AES mit 128 Bit

ein SHA-2-Hash mit 256 Bit. Wenn Suite B zum Einsatz kommt, ist die Unterstützung aller anderen Kombinationen ausdrücklich ausgeschlossen. In der Verschlüsselungskette gibt es folglich nur noch gleich starke Glieder.

In beiden Varianten ist nun die Verwendung von Protected Management Frames (PMF) nach IEEE 802.11w verpflichtend. PMF verhindern, dass Angreifer durch Deassoziieren mittels gefälschter Management Frames und Belauschen der Wiederanmeldung Material bekommen, um das WLAN-Passwort zu errechnen.

13.4.2.1 WPA3-Personal

In den WLAN-Verschlüsselungseinstellungen unter **Wireless-LAN** > **Allgemein** > **Interfaces** > **Logische WLAN-Einstellungen** können nun die neuen WPA-Versionen **WPA3** und **WPA2/3** ausgewählt werden.

Bei Auswahl von **WPA3** können sich nur noch WLAN-Clients anmelden, die WPA3-Personal unterstützen; die Authentisierung wird mit dieser Konfiguration nur noch über Simultaneous Authentication of Equals (SAE) zugelassen. Ebenfalls wird für diese SSID nun die Verwendung von PMF (Protected Management Frames nach 802.11w; verpflichtender Bestandteil von WPA3) erzwungen.

Bei Auswahl von **WPA2/3** werden diese beiden WPA-Versionen parallel angeboten. Diese Auswahl ermöglicht den Mischbetrieb von WLAN-Clients, die nur WPA2 unterstützen mit WLAN-Clients, die bereits WPA3 unterstützen. Für WPA3-kompatible WLAN-Clients wird in dieser Konfiguration die Verwendung von PMF erzwungen; für WPA2-kompatible WLAN-Clients wird PMF aus Gründen der Abwärtskompatibilität optional angeboten.

13.4.2.2 WPA3-Enterprise

WPA3-Enterprise ändert oder ersetzt die in WPA2-Enterprise definierten Protokolle nicht grundlegend. Stattdessen definiert es Richtlinien, um eine größere Konsistenz bei der Anwendung dieser Protokolle zu gewährleisten und die gewünschte Sicherheit zu gewährleisten.

In den WLAN-Verschlüsselungseinstellungen unter **Wireless-LAN** > **Allgemein** > **Interfaces** > **Logische WLAN-Einstellungen** können nun die neuen WPA-Versionen **WPA3** und **WPA2/3** ausgewählt werden.

Bei Auswahl von **WPA3** können sich nur noch WLAN-Clients anmelden, die WPA3-Enterprise unterstützen. Für diese SSID wird die Verwendung von PMF (Protected Management Frames nach 802.11w; verpflichtender Bestandteil von WPA3) erzwungen.

Bei Auswahl von **WPA2/3** werden diese beiden WPA-Versionen parallel angeboten. Diese Auswahl ermöglicht den Mischbetrieb von WLAN-Clients, die nur WPA2 unterstützen mit WLAN-Clients, die bereits WPA3 unterstützen. Für WPA3-kompatible WLAN-Clients wird in dieser Konfiguration die Verwendung von PMF erzwungen; für WPA2-kompatible WLAN-Clients wird PMF aus Gründen der Abwärtskompatibilität optional angeboten.

Suite B-Kryptographie

Zusätzlich kann die Unterstützung für Commercial National Security Algorithm (CNSA) Suite B-Kryptographie eingeschaltet werden, welche ein optionaler Teil von WPA3-Enterprise für Hochsicherheitsumgebungen ist. Suite B stellt sicher, dass alle Glieder in der Verschlüsselungskette aufeinander abgestimmt sind. Suite B bildet Klassen von Bitlängen für Hash-, symmetrische und asymmetrische Verschlüsselungsverfahren, die passende Schutzniveaus bieten. So passt zum Beispiel zu AES mit 128 Bit ein SHA-2-Hash mit 256 Bit. Wenn Suite B zum Einsatz kommt, ist die Unterstützung aller anderen Kombinationen ausdrücklich ausgeschlossen. In der Verschlüsselungskette gibt es folglich nur noch gleich starke Glieder.

Weitere Informationen zu CNSA Suite B finden Sie unter folgendem Link: *CNSA Algorithm Suite Factsheet*

Mit dem Schalter **WPA 802.1X Sicherheitsstufe** unter **Wireless-LAN** > **Allgemein** > **Interfaces** > **Logische WLAN-Einstellungen** kann die Suite B-Kryptographie optional eingeschaltet werden. Wird die Unterstützung für „Suite B 192 Bits“ eingeschaltet, werden die folgenden EAP Cipher-Suiten erzwungen:

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

Andere Cipher-Suiten können nicht verwendet werden. Ebenfalls wird eine Mindest-Schlüssellänge von 3072 Bit für die RSA- und Diffie-Hellman-Schlüsselaustauschverfahren, sowie 384 Bit für die ECDSA- und ECDHE-Schlüsselaustauschverfahren erzwungen. Zusätzlich wird der Sitzungschlüssel-Typ AES-GCMP-256 erzwungen.

Werden diese Cipher-Suiten von den verwendeten WLAN-Clients oder der restlichen Infrastruktur (z. B. RADIUS-Server) nicht unterstützt, dann ist keine Verbindung möglich!

Wird die Unterstützung für „Suite B 128 Bits" eingeschaltet, werden die folgenden EAP Cipher-Suiten erzwungen:

- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

Andere Cipher-Suiten können nicht verwendet werden. Ebenfalls wird eine Mindest-Schlüssellänge von 3072 Bit für die RSA- und Diffie-Hellman-Schlüsselaustauschverfahren, sowie 384 Bit für die ECDSA- und ECDHE-Schlüsselaustauschverfahren erzwungen. Zusätzlich wird der Sitzungschlüssel-Typ AES-GCMP-128 erzwungen.

Da die Sitzunggschlüssel-Typen AES-GCMP-128 und AES-GCMP-256 nicht von allen WLAN-Modulen unterstützt werden, kann die Verwendung der Suite B-Kryptographie je nach Gerätetyp eingeschränkt oder nicht möglich sein.

Werden diese Cipher-Suiten von den verwendeten WLAN-Clients oder der restlichen Infrastruktur (z. B. RADIUS-Server) nicht unterstützt, dann ist keine Verbindung möglich!

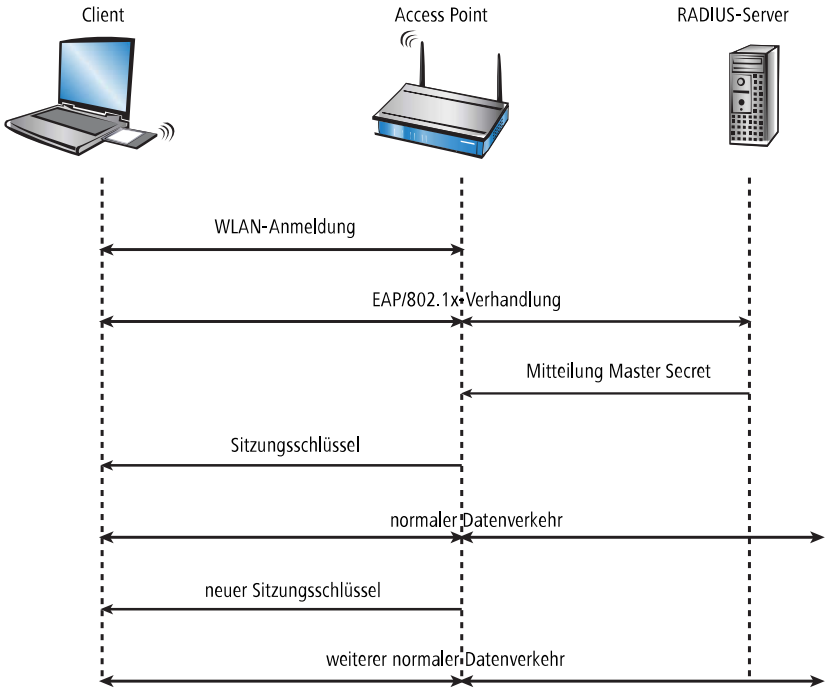
13.4.3 IEEE 802.11i / WPA2

Mitte 2004 wurde der Standard 802.11i vom IEEE verabschiedet, der auch als Wi-Fi Protected Access 2 (WPA2) bekannt ist. WPA2 erlaubt zum einen die Authentifizierung und Autorisierung der Benutzer über IEEE 802.1X und bietet zum anderen eine Unterstützung des Verschlüsselungsverfahrens AES, das eine weitaus höhere Sicherheit bietet als die in WEP oder WPA verwendeten Verfahren. Die folgenden Abschnitte stellen einige der relevanten technischen Aspekte vor.

13.4.3.1 EAP und IEEE 802.1X

Eine deutliche Steigerung in der Absicherung von WLANs kann erzielt werden, wenn für eine Verbindung keine festen Schlüssel definiert werden sondern diese Schlüssel dynamisch ausgehandelt werden. Als dabei anzuwendendes Verfahren hat sich dabei das Extensible Authentication Protocol (EAP) durchgesetzt. Wie der Name schon nahelegt, ist der ursprüngliche Zweck von EAP die Authentifizierung, d. h. der geregelte Zugang zu einem WLAN – die Möglichkeit, einen für die folgende Sitzung gültigen Schlüssel zu installieren, fällt dabei sozusagen als Zusatznutzen ab. Die folgende Abbildung zeigt den grundsätzlichen Ablauf einer mittels EAP geschützten Sitzung.

Der Einsatz von EAP / 802.1X ist grundsätzlich auch bei WEP möglich. In der Regel wird dieses Verfahren jedoch bei WLANs nach WPA2 eingesetzt.



In der ersten Phase meldet sich der Client wie gewohnt beim AP an und erreicht einen Zustand, in dem er bei dem früher verwendeten WEP jetzt über den AP Daten senden und empfangen könnte – nicht so jedoch bei EAP, denn in diesem Zustand verfügt der Client ja noch über keinerlei Schlüssel, mit denen man den Datenverkehr vor Abhören schützen könnte. Stattdessen steht der Client aus Sicht des APs in einem 'Zwischenzustand', in dem er nur bestimmte Pakete vom Client weiter leitet, und diese auch nur gerichtet an einen Authentifizierungs-Server. Bei diesen Paketen handelt es sich um das bereits erwähnte EAP/802.1X. Der AP packt diese Pakete in RADIUS-Anfragen um und reicht sie an den Authentifizierungs-Server weiter. Umgekehrt wandelt der AP darauf vom RADIUS-Server kommende Antworten wieder in EAP-Pakete um und reicht sie an den Client weiter.

Der AP dient dabei sozusagen als 'Mittelsmann' zwischen Client und Server: er muss den Inhalt dieser Pakete nicht prüfen, er stellt lediglich sicher, dass kein anderer Datenverkehr von oder zu dem Client erfolgen kann. Über den so gebildeten „Tunnel“ durch den AP versichern sich Client und Server nun ihrer gegenseitigen Authentizität, d. h. der Server überprüft die Zugangsberechtigung des Clients zum Netz, und der Client überprüft, ob er wirklich mit dem richtigen Netz verbunden ist. Von Hackern aufgestellte „wilde“ APs lassen sich so erkennen.

Es gibt eine ganze Reihe von Authentifizierungsverfahren, die in diesem Tunnel angewendet werden können. Ein gängiges Verfahren ist z. B. TLS, bei dem Server und Client Zertifikate austauschen, ein anderes ist TTLS, bei dem nur der Server ein Zertifikat liefert – der Client authentifiziert sich über einen Benutzernamen und ein Passwort.

Nachdem die Authentifizierungsphase abgeschlossen ist, ist gleichzeitig auch ein ohne Verschlüsselung gesicherter Tunnel entstanden, in den im nächsten Schritt der AP eingebunden wird. Dazu schickt der RADIUS-Server das sogenannte 'Master Secret', einen während der Verhandlung berechneten Sitzungsschlüssel, zum AP. Das LAN hinter dem AP wird in diesem Szenario als sicher betrachtet, von daher kann diese Übertragung im Klartext erfolgen.

Mit diesem Sitzungsschlüssel übernimmt der AP jetzt den gebildeten Tunnel und kann ihn nutzen, um dem Client die eigentlichen Schlüssel mitzuteilen. Je nach Fähigkeiten der Access-Point-Hardware kann das ein echter Sitzungsschlüssel sein, d. h. ein Schlüssel, der nur für Datenpakete zwischen dem AP und genau diesem Client benutzt wird. Ältere WEP-Hardware verwendet meistens nur Gruppenschlüssel, den der AP für die Kommunikation mit mehreren Clients benutzt.

Der besondere Vorteil dieses Verfahrens ist, dass der AP über den EAP-Tunnel die Schlüssel regelmäßig wechseln kann, d. h. ein sogenanntes Rekeying durchführen kann. Auf diese Weise lassen sich Schlüssel gegen andere ersetzen, lange

bevor sie durch IV-Kollisionen Gefahr laufen, geknackt zu werden. Eine gängige 'Nutzungszeit' für so einen Schlüssel sind z. B. 5 Minuten.

Status-Zähler für IEEE 802.1X-Anmeldevorgänge

Eine Übersichtstabelle mit der Anzahl akzeptierter und zurückgewiesener Verbindungsanfragen je logischer Schnittstelle finden Sie auf der Konsole unter **Status** > **IEEE802.1X** > **Ports**.

Zusätzlich zeigt Ihnen die Übersicht an, wie oft bei einer Schnittstelle das Authorisierungslimit erreicht wurde.

Ports

Port	Anzahl-Accept	Anzahl-Reject	Anzahl-ReauthMax-erreicht
LAN-1	0	0	0
LAN-2	0	0	0
LAN-3	0	0	0
LAN-4	0	0	0
WLAN-1	0	0	0
P2P-1-1	0	0	0
P2P-1-2	0	0	0
P2P-1-3	0	0	0
P2P-1-4	0	0	0
P2P-1-5	0	0	0
P2P-1-6	0	0	0
P2P-1-7	0	0	0
P2P-1-8	0	0	0
P2P-1-9	0	0	0
P2P-1-10	0	0	0
P2P-1-11	0	0	0
P2P-1-12	0	0	0
P2P-1-13	0	0	0
P2P-1-14	0	0	0

13.4.3.2 WPA mit Passphrase

Der bei EAP / 802.1X beschriebene Handshake läuft bei WPA grundsätzlich ab, d. h. der Anwender wird niemals selber irgendwelche Schlüssel definieren müssen. In Umgebungen, in denen kein RADIUS-Server zur Erteilung des Master-Secrets vorhanden ist (z. B. bei kleineren Firmen) sieht WPA deshalb neben der Authentifizierung über einen RADIUS-Server noch das PSK-Verfahren vor; dabei muss der Anwender sowohl auf dem Access Point als auch auf allen Stationen eine zwischen 8 und 63 Zeichen lange Passphrase eingeben, aus der zusammen mit der verwendeten SSID das Master-Secret über ein Hash-Verfahren berechnet wird. Das Master Secret ist in so einem PSK-Netz also konstant, trotzdem ergeben sich immer unterschiedliche Sitzungs-Schlüssel.

In einem PSK-Netz hängen sowohl Zugangsschutz als auch Vertraulichkeit davon ab, dass die Passphrase nicht in unbefugte Hände gerät. Solange dies aber gegeben ist, bietet WPA-PSK eine deutlich höhere Sicherheit gegen Einbrüche und Abhören als jede WEP-Variante. Für größere Installationen, in denen eine solche Passphrase einem zu großen Nutzerkreis bekannt gemacht werden müsste, als dass sie geheimzuhalten wäre, wird EAP / 802.1X in Zusammenhang mit dem hier beschriebenen Key-Handshake genutzt.

Unkonfigurierte Access Points und Wireless Router können im Auslieferungszustand nicht über die WLAN-Schnittstelle in Betrieb genommen werden. Die WLAN-Module sind ausgeschaltet. Die Access Points suchen selbstständig im LAN einen WLC, von dem sie automatisch eine Konfiguration beziehen können.

Status-Zähler für WPA-PSK-Anmeldevorgänge

Eine Übersicht über die Anzahl fehlgeschlagener WPA-PSK Anmeldevorgänge finden Sie im LCOS-Menübaum unter **Status** > **WLAN** > **Verschlüsselung**.

Zusätzlich erhalten Sie eine Übersicht über erfolgreiche Anmeldeversuche sowie die Anzahl zurückgewiesener Anmeldungen aufgrund falscher Passphrasen.

Verschluesselung

Interface	Verschluesselung	Methode	WPA-Version	WPA1-Sitzungsschluessel	WPA2-Sitzungsschluessel	PMK-Caching	Prae-Authentisierung	OKC	Gesch.-Mgmt-Frames	WPA2-Schluessel-Management	WPA-PSK-Anzahl-erfolgreich	WPA-PSK-Anzahl-Fehler	WPA-PSK-Anzahl-falsche-Passphrase
WLAN-1	ja	802.11i-WPA-PSK	WPA1/2	TKIP/AES	TKIP/AES	ja	ja	nein	nein	Standard	0	0	0
WLAN-1-2	ja	802.11i-WPA-PSK	WPA1/2	TKIP	AES	ja	ja	nein	nein	Standard	0	0	0
WLAN-1-3	ja	802.11i-WPA-PSK	WPA1/2	TKIP	AES	ja	ja	nein	nein	Standard	0	0	0
WLAN-1-4	ja	802.11i-WPA-PSK	WPA1/2	TKIP	AES	ja	ja	nein	nein	Standard	0	0	0
WLAN-1-5	ja	802.11i-WPA-PSK	WPA1/2	TKIP	AES	ja	ja	nein	nein	Standard	0	0	0
WLAN-1-6	ja	802.11i-WPA-PSK	WPA1/2	TKIP	AES	ja	ja	nein	nein	Standard	0	0	0

Wählen Sie in der Tabelle eine Schnittstelle aus (z. B. WLAN-1), um sich Informationen für die gewählte Schnittstelle anzeigen zu lassen.

Verschluesselung

Interface	WLAN-1
Verschluesselung	ja
Methode	802.11i-WPA-PSK
WPA-Version	WPA1/2
WPA1-Sitzungsschluessel	TKIP/AES
WPA2-Sitzungsschluessel	TKIP/AES
PMK-Caching	ja
Prae-Authentisierung	ja
OKC	nein
Gesch.-Mgmt-Frames	nein
WPA2-Schluessel-Management	Standard
WPA-PSK-Anzahl-erfolgreich	0
WPA-PSK-Anzahl-Fehler	0
WPA-PSK-Anzahl-falsche-Passphrase	0

13.4.3.3 TKIP

Beim Temporal Key Integrity Protocol (TKIP) handelt es sich um eine Zwischenlösung, die nur übergangsweise bis zur Einführung eines wirklich starken Verschlüsselungsverfahrens genutzt werden soll, aber trotzdem einige Probleme des bis dahin verwendeten WEP löst. Der Einsatz von TKIP wird nur beim Betrieb von älteren WLAN-Clients empfohlen, die keine Unterstützungg für AES bieten.

Wenn eine SSID ausschließlich WEP oder WPA mit TKIP als Verschlüsselungsverfahren verwendet, erreichen die angebundenen WLAN-Clients eine maximale Brutto-Datenrate von 54 MBit/s.

13.4.3.4 AES

Die augenfälligste Erweiterung betrifft die Einführung eines neuen Verschlüsselungsverfahrens, nämlich AES-CCM. Wie der Name schon andeutet, basiert dieses Verschlüsselungsverfahren auf dem DES-Nachfolger AES, im Gegensatz zu WEP und TKIP, die beide auf RC4 basieren. Da ältere WLAN-Clients zum Teil nur TKIP unterstützen, definiert 802.11i auch weiterhin TKIP, allerdings mit umgekehrtem Vorzeichen: eine 802.11i-standardkonforme Hardware muss AES unterstützen, während TKIP optional ist – bei WPA war es genau umgekehrt, hier ist die Verwendung von AES optional. Ab WPA3 müssen zum Zeitpunkt der Verabschiedung als sicher betrachtete Verfahren eingesetzt werden. Verfahren wie TKIP, bei denen Sicherheitslücken bekannt sind, dürfen dann nicht mehr eingesetzt werden.

Der Zusatz CCM bezieht sich auf die Art und Weise, wie AES auf WLAN-Pakete angewendet wird. Das Verfahren ist insgesamt recht kompliziert, weshalb CCM sinnvoll eigentlich nur in Hardware implementiert werden wird – software-basierte Implementationen sind zwar möglich, führen aber auf den üblicherweise in Access Points eingesetzten Prozessoren zu erheblichen Geschwindigkeitseinbußen.

Im Gegensatz zu TKIP benötigt AES nur noch einen 128 Bit langen Schlüssel, mit dem sowohl die Verschlüsselung als auch der Schutz gegen unerkanntes Verändern von Paketen erreicht wird. Des weiteren ist CCM voll symmetrisch, d. h. es wird der gleiche Schlüssel in beide Kommunikationsrichtungen angewendet – eine standardkonforme

TKIP-Implementierung hingegen verlangt die Verwendung unterschiedlicher Michael-Schlüssel in Sende- und Empfangsrichtung, so dass CCM in seiner Anwendung deutlich unkomplizierter ist als TKIP.

Ähnlich wie TKIP verwendet CCM einen 48 Bit langen Initial Vector in jedem Paket – eine IV-Wiederholung ist damit in der Praxis ausgeschlossen. Wie bei TKIP merkt der Empfänger sich den zuletzt benutzten IV und verwirft Pakete mit einem IV, der gleich oder niedriger als der Vergleichswert ist.

13.4.3.5 Prä-Authentifizierung und PMK-Caching

802.11i soll den Einsatz von WLAN auch für Sprachverbindungen (VoIP) in Unternehmensnetzen erlauben. Vor allem in Zusammenhang mit WLAN-basierten schnurlosen Telefonen kommt einem schnellen Roaming, d. h. dem Wechsel zwischen APs ohne längere Unterbrechungen, eine besondere Bedeutung zu. Bei Telefongesprächen sind bereits Unterbrechungen von wenigen 100 Millisekunden störend, allerdings kann eine vollständige Authentifizierung über 802.1X inklusive der folgenden Schlüsselverhandlung mit dem AP deutlich länger dauern.

Als erste Maßnahme wurde deshalb das sogenannte PMK-Caching eingeführt. Das PMK dient nach einer 802.1X-Authentifizierung zwischen Client und AP als Basis für die Schlüsselverhandlung. In VoIP-Umgebungen ist es denkbar, dass ein Anwender sich zwischen einer relativ kleinen Zahl von APs hin- und herbewegt. Dabei wird es vorkommen, dass ein Client wieder zu einem AP wechselt, an dem er bereits früher einmal angemeldet war. In so einem Fall wäre es unsinnig, die ganze 802.1X-Authentifizierung noch einmal zu wiederholen. Aus diesem Grund kann der AP das PMK mit einer Kennung, der sogenannten PMKID, versehen, die er an den Client übermittelt. Bei einer Wiederanmeldung fragt der Client mittels der PMKID, ob er dieses PMK noch vorrätig hat. Falls ja, kann die 802.1X-Phase übersprungen werden und die Verbindung ist schnell wieder verfügbar. Diese Optimierung greift naturgemäß nicht, wenn das PMK in einem WLAN aufgrund einer Passphrase berechnet wird, denn dann ist es ja ohnehin überall gleich und bekannt.

Eine weitere Maßnahme erlaubt auch für den Fall der erstmaligen Anmeldung eine Beschleunigung, sie erfordert aber etwas Vorausschau vom Client: dieser muss bereits im Betrieb eine schlechter werdende Verbindung zum AP erkennen und einen neuen AP selektieren, während er noch Verbindung zum alten AP hat. In diesem Fall hat er die Möglichkeit, die 802.1X-Verhandlung über den alten AP mit dem neuen AP zu führen, was wiederum die 'Totzeit' um die Zeit der 802.1X-Verhandlung verkürzt.

13.4.4 TKIP und WPA

Wie in den letzten Abschnitten klar geworden ist, ist der WEP-Algorithmus prinzipiell fehlerhaft und unsicher; die bisherigen Maßnahmen waren im wesentlichen entweder 'Schnellschüsse' mit nur geringen Verbesserungen oder so kompliziert, dass sie für den Heimbenutzer oder kleine Installationen schlicht unpraktikabel sind.

Die IEEE hatte nach Bekanntwerden der Probleme mit WEP mit der Entwicklung des Standards IEEE 802.11i begonnen. Als Zwischenlösung wurde von der Wi-Fi-Alliance der 'Standard' Wi-Fi Protected Access (WPA) definiert. WPA setzt auf die folgenden Änderungen:

- TKIP und Michael als Ersatz für WEP
- Ein standardisiertes Handshake-Verfahren zwischen Client und AP zur Ermittlung / Übertragung der Sitzungsschlüssel.
- Ein vereinfachtes Verfahren zur Ermittlung des im letzten Abschnitt erwähnten Master Secret, das ohne einen RADIUS-Server auskommt.
- Aushandlung des Verschlüsselungsverfahrens zwischen AP und Client.

Bei der Verschlüsselung werden bekannte Bestandteile des WEP-Verfahrens weiter verwendet, aber an den entscheidenden Stellen um den „Michael-Hash" zur besseren Verschlüsselung und das TKIP-Verfahren zur Berechnung der RC4-Schlüssel erweitert. Desweiteren ist der intern hochgezählte und im Paket im Klartext übertragene IV statt 24 jetzt 48 Bit lang – damit ist das Problem der sich wiederholenden IV-Werte praktisch ausgeschlossen.

Als weiteres Detail mischt TKIP in Berechnung der Schlüssel auch noch die MAC-Adresse des Senders ein. Auf diese Weise ist sichergestellt, dass eine Verwendung gleicher IVs von verschiedenen Sendern nicht zu identischen RC4-Schlüsseln und damit wieder zu Angriffsmöglichkeiten führt.

Der Michael-Hash stell jedoch keine besonders hohe kryptographische Hürde dar: kann der Angreifer den TKIP-Schlüssel brechen oder verschlüsselte Pakete durch Modifikationen ähnlich wie bei WEP an der CRC-Prüfung vorbeischleusen, bleiben nicht mehr allzu viele Hürden zu überwinden. WPA definiert aus diesem Grund Gegenmaßnahmen, wenn ein

WLAN-Modul mehr als zwei Michael-Fehler pro Minute erkennt: sowohl Client als auch AP brechen dann für eine Minute den Datentransfer ab und handeln danach TKIP- und Michael-Schlüssel neu aus.

Mit der Zeit werden Möglichkeiten gefunden, die Verschlüsselungsprotokolle zu kompromittieren. Die Wi-Fi-Alliance hat dem mit den Zertifizierungsstandards WPA2 und später WPA3 entgegengewirkt, indem dort jeweils modernere Verschlüsselungsverfahren zum Einsatz kommen, während bekannt unsichere Verfahren nicht mehr verwendet werden dürfen.

13.4.4.1 Verhandlung des Verschlüsselungsverfahrens

Da die ursprüngliche WEP-Definition eine feste Schlüssellänge von 40 Bit vorschrieb, musste bei der Anmeldung eines Clients an einem AP lediglich angezeigt werden, ob eine Verschlüsselung genutzt wird oder nicht. Bereits bei Schlüssellängen von mehr als 40 Bit muss aber auch die Länge des verwendeten Schlüssels bekannt gegeben werden. WPA stellt einen Mechanismus bereit, mit dem sich Client und AP über das zu verwendende Verschlüsselungs- und Authentifizierungsverfahren verständigen können. Dabei werden folgenden Informationen bereitgestellt:

- Eine Liste von Verschlüsselungsverfahren, die der AP für den Pairwise Key anbietet – hier ist WEP explizit nicht mehr erlaubt.
- Eine Liste von Authentifizierungsverfahren, über die sich ein Client gegenüber dem WLAN als zugangsberechtigt zeigen kann – mögliche Verfahren sind z. B. EAP / 802.1X oder PSK.

Wie erwähnt, sieht der ursprüngliche WPA-Standard einzig TKIP / Michael als verbessertes Verschlüsselungsverfahren vor. Mit der Weiterentwicklung des 802.11i-Standards wurde das weiter unten beschriebene AES / CCM-Verfahren hinzugenommen. So ist es heutzutage in einem WPA-Netz möglich, dass einige Clients über TKIP mit dem AP kommunizieren, andere Clients jedoch über AES.

13.4.5 WEP

WEP ist eine Abkürzung für Wired Equivalent Privacy. Die primäre Zielsetzung von WEP ist die Vertraulichkeit von Daten. Im Gegensatz zu Signalen, die über Kabel übertragen werden, breiten sich Funkwellen beliebig in alle Richtungen aus – auch auf die Straße vor dem Haus und an andere Orte, wo sie gar nicht erwünscht sind. Das Problem des unerwünschten Mithörens tritt bei der drahtlosen Datenübertragung besonders augenscheinlich auf, auch wenn es prinzipiell auch bei größeren Installationen kabelgebundener Netze vorhanden ist – allerdings kann man den Zugang zu Kabeln durch entsprechende Organisation eher begrenzen als bei Funkwellen.

WEP bietet deutlich geringere Sicherheit als IEEE 802.1X / WPA2. Aus Gründen der Kompatibilität zu älteren WLAN-Clients unterstützen LANCOM APs weiterhin dieses Verschlüsselungsverfahren. LANCOM empfiehlt jedoch ausdrücklich, nach Möglichkeit eine bessere Absicherung der WLANs (z. B. nach IEEE 802.1X / WPA2 oder WPA3) zu verwenden.

13.4.6 LANCOM Enhanced Passphrase Security (LEPS)

Mit dem Verschlüsselungsverfahren WPA2 wird der Datenverkehr im WLAN gegen unerwünschte „Lauschangriffe" geschützt. Die Verwendung einer Passphrase als zentraler Schlüssel ist dabei sehr einfach zu handhaben, ein RADIUS-Server wie in 802.1X-Installationen wird nicht benötigt.

Dennoch birgt die Verwendung des abhörsicheren Verfahrens WPA2 einige Schwachstellen:

- Eine Passphrase gilt **global** für **alle** WLAN-Clients
- Die Passphrase kann durch Unachtsamkeit ggf. an Unbefugte weitergegeben werden
- Mit der „durchgesickerten" Passphrase kann jeder Angreifer in das Funknetzwerk eindringen

In der Praxis bedeutet das: Falls die Passphrase „verloren geht" oder ein Mitarbeiter mit Kenntnis der Passphrase das Unternehmen verlässt, müsste aus Sicherheitsaspekten die Passphrase im Access Point geändert werden – und damit auch in allen WLAN-Clients. Da das nicht immer sichergestellt werden kann, würde sich also ein Verfahren anbieten, bei dem nicht eine globale Passphrase für alle WLAN-Clients gemeinsam gilt, sondern für jeden Benutzer im WLAN eine eigene Passphrase konfiguriert werden kann. In diesem Fall muss z. B. beim Ausscheiden eines Mitarbeiters aus dem

Unternehmen nur seine „persönliche“ Passphrase gelöscht werden, alle anderen behalten ihre Gültigkeit und Vertraulichkeit.

Mit LEPS hat LANCOM Systems GmbH zwei effiziente Verfahren entwickelt, welche die einfache Konfigurierbarkeit von IEEE 802.11i mit Passphrase nutzen und dabei die möglichen Unsicherheiten bei der Nutzung einer globalen Passphrase vermeiden.

Mit LEPS-U (LANCOM Enhanced Passphrase Security User) vergeben Sie einzelnen Clients oder ganzen Gruppen ein individuelles WLAN-Passwort für eine SSID. Über LEPS-MAC (LANCOM Enhanced Passphrase Security MAC) authentifizieren Sie die Clients noch zusätzlich anhand ihrer MAC-Adresse – ideal für sichere Unternehmensnetzwerke!

13.4.6.1 LANCOM Enhanced Passphrase Security User (LEPS-U)

Mit LANCOM Enhanced Passphrase Security User (LEPS-U) kann eine Menge von Passphrasen konfiguriert werden, die dann den einzelnen Benutzern oder Gruppen zugeordnet werden können. Somit gibt es nicht eine globale Passphrase für eine SSID, sondern mehrere, die dann individuell verteilt werden können.

Dies kann für das Onboarding von Geräten in das Netzwerk genutzt werden. Wenn ein Netzwerk-Betreiber z. B. mehrere WLAN-Geräte in verschiedene Bereiche seines Netzwerks „onboarden“ will, aber die Geräte nicht selber konfigurieren will, da dies die Benutzer der Geräte selber erledigen sollen. In diesem Fall erhalten die Benutzer lediglich einen Preshared Key für das Firmen-WLAN ausgehändigt, welchen die Benutzer selber für ihre Geräte verwenden können. Je nach Preshared Key werden die Benutzer automatisch durch Zuordnung zu einem VLAN einem bestimmten Netzwerk zugewiesen. Da LEPS-U ausschließlich auf der Infrastrukturseite konfiguriert wird, ist jederzeit die volle Kompatibilität zu Fremdprodukten gegeben.

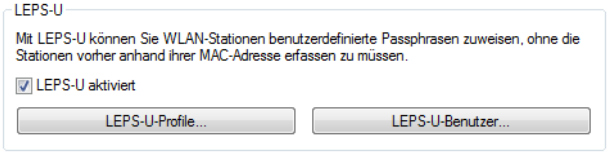
Die Unsicherheit von globalen Passphrasen wird durch LEPS-U grundsätzlich behoben. Jedem Benutzer wird hierbei seine eigene individuelle Passphrase zugewiesen. Falls eine einem Benutzer zugeordnete Passphrase „verloren geht“ oder ein Mitarbeiter mit Kenntnis seiner Passphrase das Unternehmen verlässt, dann muss nur die Passphrase dieses Benutzers geändert bzw. gelöscht werden. Alle anderen Passphrasen behalten ihre Gültigkeit und Vertraulichkeit.

Aus technischen Gründen ist LEPS-U nur mit der WPA-Version WPA2 kompatibel.

Aus technischen Gründen ist LEPS-U nicht mit Fast Roaming kompatibel.

Konfiguration

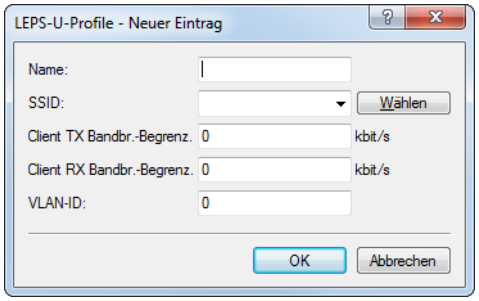
Die Konfiguration der **LEPS-U-Profile** und **LEPS-U-Benutzer** finden Sie in LANconfig unter **Wireless-LAN** > **Stationen/LEPS** > **LEPS-U**. Über den Schalter **LEPS-U aktiviert** wird LEPS-U eingeschaltet.



Bei der Konfiguration von LEPS-U wird jedem Benutzer, der sich mit Clients im WLAN anmelden können soll, eine individuelle Passphrase zugeordnet. Dazu werden LEPS-U-Profile angelegt, damit einige Einstellungen nicht bei jedem Benutzer erneut vorgenommen werden müssen. Anschließend legen Sie die LEPS-U-Benutzer mit der zugehörigen individuellen Passphrase an und verknüpfen diesen mit einem der vorher angelegten LEPS-U-Profile.

LEPS-U-Profile

Konfigurieren Sie hier LEPS-U-Profile und verbinden Sie sie mit einer SSID. Anschließend können die LEPS-U-Profile den LEPS-U-Benutzern zugeordnet werden.



Name

Vergeben Sie hier einen eindeutigen Namen für das LEPS-U-Profil.

SSID

Wählen Sie hier die SSID bzw. beim WLC das logische WLAN-Netzwerk aus, für die das LEPS-U-Profil gültig sein soll. Es können sich nur LEPS-U-Benutzer an der SSID bzw. beim WLC an dem logischen WLAN-Netzwerk anmelden, mit der sie über das LEPS-U-Profil verbunden sind.

Client TX Bandbr.-Begrenz.

Hier können Sie eine Sende-Bandbreiten-Begrenzung in kbit/s für die sich einbuchenden WLAN-Clients einstellen.

Client RX Bandbr.-Begrenz.

Hier können Sie eine Empfangs-Bandbreiten-Begrenzung in kbit/s für die sich einbuchenden WLAN-Clients einstellen.

VLAN-ID

Hier können Sie festlegen, welcher VLAN-ID ein LEPS-U-Benutzer, der mit diesem Profil verbunden ist, zugewiesen wird.

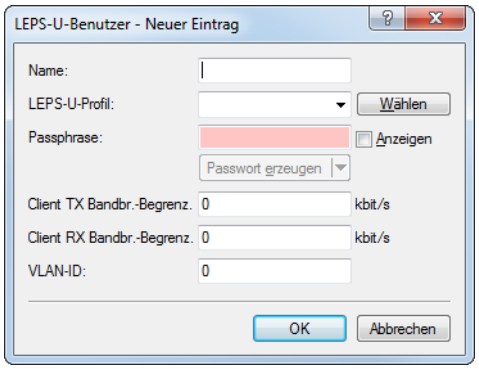
LEPS-U-Benutzer

Legen Sie hier einzelne LEPS-U-Benutzer an. Jeder LEPS-U-Benutzer muss mit einem zuvor angelegten Profil verbunden werden und eine individuelle WPA-Passphrase zugewiesen bekommen. Mit dieser Passphrase kann sich dann ein beliebiger Client an der SSID anmelden, für die der Benutzereintrag durch die Verknüpfung des Profils gültig ist. Der Benutzer wird anhand der verwendeten Passphrase identifiziert und dem in dieser Tabelle konfigurierten VLAN zugewiesen. Wird hier kein VLAN zugewiesen, wird er dem am Profil konfigurierten VLAN zugewiesen. Einstellungen am einzelnen Benutzer haben somit Priorität gegenüber Einstellungen am Profil.

Es gibt plattformspezifische Beschränkungen bei der Anzahl der gleichzeitig angelegten LEPS-U-Benutzer.

Gerät	Benutzer
L-15x, L-3xx, OAP-32x, OAP-8xx, IAP-32x, IAP-82x, LN-630acn	› pro SSID bis zu 300 Benutzer › Access Point gesamt: 2.000 Benutzer
L-45x, L(N)-8xx, L-13xx, LN-17xx	› pro SSID bis zu 1.000 Benutzer

Gerät	Benutzer
	Access Point gesamt: 6.000 Benutzer



Name

Vergeben Sie hier einen eindeutigen Namen für den LEPS-U-Benutzer.

LEPS-U-Profil

Wählen Sie hier das Profil aus, für das der LEPS-U-Benutzer gültig sein soll. Es können sich nur LEPS-U-Benutzer an der SSID anmelden, mit der sie über das LEPS-U-Profil verbunden sind.

Passphrase

Vergeben Sie hier die Passphrase, mit der der LEPS-U-Benutzer sich am WLAN anmelden soll.

Als Passphrase können Zeichenketten mit 8 bis 64 Zeichen verwendet werden. Wir empfehlen als Passphrasen zufällige Zeichenketten von mindestens 32 Zeichen Länge.

Client TX Bandbr.-Begrenz.

Hier können Sie eine Sende-Bandbreiten-Begrenzung in kbit/s für die sich einbuchenden WLAN-Clients einstellen. Wird hier keine Begrenzung konfiguriert, gilt eine eventuelle, im LEPS-U-Profil konfigurierte Begrenzung. Wird sowohl im LEPS-U-Profil als auch am LEPS-U-Benutzer eine Begrenzung konfiguriert, gilt die am LEPS-U-Benutzer konfigurierte Begrenzung.

Client RX Bandbr.-Begrenz.

Hier können Sie eine Empfangs-Bandbreiten-Begrenzung in kbit/s für die sich einbuchenden WLAN-Clients einstellen. Wird hier keine Begrenzung konfiguriert, gilt eine eventuelle, im LEPS-U-Profil konfigurierte Begrenzung. Wird sowohl im LEPS-U-Profil als auch am LEPS-U-Benutzer eine Begrenzung konfiguriert, gilt die am LEPS-U-Benutzer konfigurierte Begrenzung.

VLAN-ID

Hier können Sie festlegen, welcher VLAN-ID der LEPS-U-Benutzer zugewiesen wird. Wird hier keine VLAN-ID konfiguriert, gilt eine eventuelle, im LEPS-U-Profil konfigurierte VLAN-ID. Wird sowohl im LEPS-U-Profil als auch am LEPS-U-Benutzer eine VLAN-ID konfiguriert, gilt die am LEPS-U-Benutzer konfigurierte VLAN-ID.

13.4.6.2 LANCOM Enhanced Passphrase Security MAC (LEPS-MAC)

Bei LEPS-MAC wird jeder MAC-Adresse in einer zusätzlichen Spalte der ACL (Access Control List) eine **individuelle** Passphrase zugeordnet – eine beliebige Folge aus 8 bis 63 ASCII-Zeichen. Nur die Verbindung von Passphrase und MAC-Adresse erlaubt die Anmeldung am Access Point.

Da Passphrase und MAC-Adresse verknüpft sind, ist auch das Spoofing der MAC-Adressen wirkungslos – LEPS-MAC schließt damit auch einen möglichen Angriffspunkt gegen die ACL aus. Wenn als Verschlüsselungsart WPA2 verwendet wird, kann zwar die MAC-Adresse abgehört werden – die Passphrase wird bei diesem Verfahren jedoch nie über die

WLAN-Strecke übertragen. Angriffe auf das WLAN werden so deutlich erschwert, da durch die Verknüpfung von MAC-Adresse und Passphrase immer beide Teile bekannt sein müssen, um eine Verschlüsselung zu verhandeln.

LEPS-MAC kann sowohl lokal im Gerät genutzt werden als auch mit Hilfe eines RADIUS-Servers zentral verwaltet werden. LEPS-MAC funktioniert mit sämtlichen am Markt befindlichen WLAN-Client-Adaptern, ohne dass dort eine Änderung stattfinden muss. Da LEPS-MAC ausschließlich im Access Point konfiguriert wird, ist jederzeit die volle Kompatibilität zu Fremdprodukten gegeben.

Im Vergleich zu LEPS-U ist der Verwaltungsaufwand etwas höher, da für jedes Gerät die MAC-Adresse eingetragen werden muss.

Konfiguration

Bei der Konfiguration von LEPS-MAC wird jeder MAC-Adresse eines im WLAN zugelassenen Clients eine eigene Passphrase zugeordnet. Dies kann entweder als Eintrag in der Liste unter **Wireless-LAN** > **Stationen/LEPS** > **LEPS-MAC** > **Stationsregeln** (siehe *Stationen* auf Seite 1158) oder im RADIUS-Server geschehen. Pro MAC-Adresse wird ein Eintrag erzeugt – im Sinne des RADIUS-Servers ist die jeweilige MAC-Adresse also ein Benutzer. Zusätzlich muss unter **Wireless-LAN** > **Allgemein** > **Interfaces** > **Logische WLAN-Einstellungen** der MAC-Filter aktiviert sein, d. h., die Daten von den hier eingetragenen WLAN-Clients werden übertragen.

Als Passphrase können Zeichenketten mit 8 bis 64 Zeichen verwendet werden. Wir empfehlen als Passphrasen zufällige Zeichenketten von mindestens 32 Zeichen Länge.

Bei Speicherung der client-spezifischen Passphrasen in der Benutzertabelle eines RADIUS-Servers kann auch ein LAN-gebundenes Gerät als zentraler RADIUS-Server dienen und die Vorteile von LEPS-MAC nutzen.

13.4.7 Background WLAN Scanning

Zur Erkennung anderer APs in der eigenen Funkreichweite können LANCOM Wireless Geräte aktiv alle verfügbaren Kanäle prüfen, so wie das ein WLAN-Client machen würde, der nach verfügbaren APs sucht. Wenn dort ein anderer AP aktiv ist, werden die entsprechenden Informationen in der Scan-Tabelle gespeichert. Da diese Aufzeichnung im Hintergrund neben der „normalen" Funktätigkeit der APs abläuft, wird diese Funktion auch als „Background Scan" bezeichnet.

Das Background-Scanning wird vorwiegend für die folgenden Aufgaben eingesetzt:

- Rogue AP Detection
- Schnelles Roaming von WLAN-Clients

13.4.7.1 Rogue AP Detection

Als Rogue bezeichnet man solche WLAN-Geräte, die unerlaubt versuchen, als AP oder Client Teilnehmer in einem WLAN zu werden. Rogue APs sind solche APs, die z. B. von den Mitarbeitern einer Firma ohne Kenntnis und Erlaubnis der System-Administratoren an das Netzwerk angeschlossen werden und so über ungesicherte WLAN-Zugänge bewusst oder unbewusst Tür und Tor für potentielle Angreifer öffnen. Nicht ganz so gefährlich, aber zumindest störend sind z. B. APs in der Reichweite des eigenen WLAN, die zu fremden Netzwerken gehören. Verwenden solche Geräte dabei z. B. die gleiche SSID und den gleichen Kanal wie die eigenen APs (Default-Einstellungen), können die eigenen WLAN-Clients versuchen, sich bei dem fremden Netzwerk einzubuchen.

Da alle unbekannten APs in der Reichweite des eigenen Netzwerks oft eine mögliche Bedrohung und Sicherleitslücke, zumindest aber eine Störung darstellen, können mit dem Background-Scanning Rogue APs identifiziert werden, um ggf. weitere Maßnahmen zur Sicherung des eigenen Netzwerks einzuleiten.

13.4.7.2 Schnelles Roaming im Client-Modus

Das Verfahren des Background-Scanning kann aber auch mit anderen Zielen als der Rogue AP Detection verwendet werden. Ein AP im Client-Modus, der sich selbst bei einem anderen AP anmeldet, kann in einer mobilen Installation auch das Roaming-Verfahren nutzen. Dies ist z. B. dann der Fall, wenn der AP in einer Industrieanwendung auf einem Gabelstapler befestigt ist, der sich durch mehrere Hallen mit separaten APs bewegt. Normalerweise würde der WLAN-Client sich nur dann bei einem anderen AP einbuchen, wenn er die Verbindung zu dem bisherigen Access Point vollständig

verloren hat. Mit der Funktion des Background-Scanning kann der AP im Client-Modus schon vorher Informationen über andere verfügbare APs sammeln. Die Umschaltung auf einen anderen AP erfolgt dann nicht erst, wenn die bisherige Verbindung vollständig verloren wurde, sondern wenn ein anderer AP in Reichweite über ein stärkeres Signal verfügt.

13.4.7.3 Auswertung des Background-Scans

Die Informationen über die gefundenen APs können in der Statistik des APs eingesehen werden. Sehr komfortabel stellt der WLANmonitor die Scan-Ergebnisse dar und bietet darüber hinaus zusätzliche Funktionen wie das Gruppieren der APs oder die automatische Benachrichtigung per E-Mail beim Auftauchen neuer WLAN-Geräte.

13.4.8 Umgebungsscan zu einer konfigurierbaren Zeit starten

Die Umgebung Ihres WLAN kann regelmäßig nach Rogue APs abgesucht werden.

Daher können Sie Zeiten konfigurieren, zu denen täglich automatisiert ein Umgebungsscan nach Rogue APs durchgeführt wird.

Um den normalen Betrieb nicht unnötig zu stören, sollte ein solcher Umgebungsscan zu bestimmten Zeiten geschehen.

Daher bietet Ihnen dieses Feature die Option, täglich zu einer vordefinierten Zeit das konfigurierte Frequenzband scannen zu lassen.

Scannen bedeutet hier:

- aktives Scannen mittels Probe Requests.
- passives Scannen durch Empfang der fremden Beacons.



Unter gewissen Umständen ist nur passives Scannen möglich, z. B. wenn ein 5-GHz-Kanal momentan nicht als DFS-frei markiert ist. In diesem Fall darf nicht gesendet werden.

Zur Konfiguration über die Kommandozeile gibt es folgende Menüpunkte, hier beispielhaft mit Default-Werten:

```
root@LN-1700Esc:/Setup/Interfaces/WLAN/Environment-Scan
> ls -a

[1.3.6.1.4.1.2356.11][2.23.20.27]
Ifc      Operating  Hour    Minute  Channel-List
[1]      [2]          [3]    [4]     [5]
=========-------------------------------------------------------------------
WLAN-1    No           3      0
WLAN-2    No           3      0
```

Mittels „Hour“ und „Minute“ wird eingestellt, zu welchen Zeiten der Environment Scan täglich ausgeführt wird. In diesen Feldern ist auch die Cron-Syntax erlaubt. Mit der Channel-List können die zu scannenden Kanäle eingeschränkt werden (Angabe als kommaseparierte Liste). Erfolgt hier keine Angabe, werden alle Kanäle des Frequenzbandes, auf dem das Modul gerade arbeitet, gescannt.

Während des Scans verweilt das WLAN-Modul ca. drei Sekunden auf jedem Kanal. Anschließend wird der nächste Kanal gescannt. Wurden alle konfigurierten Kanäle gescannt, wechselt das Modul wieder in den regulären Betriebsmodus.



Während des Scans ist kein regulärer WLAN-Betrieb auf dem Modul möglich, anders als z. B. beim Background-Scan. Es ist aber sichergestellt, dass immer nur eines der beiden Module zur gleichen Zeit den Environment Scan durchführt, so dass auf dem jeweils anderen Modul noch der Regelbetrieb möglich ist.

Zusätzlich zur zeitgesteuerten Aktivierung des Environment Scan ist auch eine permanente Aktivierung möglich. Dazu kann das WLAN-Modul in den neu geschaffenen Betriebsmodus „Scanner“ versetzt werden (siehe Operation-Mode 7):

```
root@LN-1700Esc:/Setup/Interfaces/WLAN/Operational
> l

Ifc       Operating     Operation-Mode  Link-LED-Function     Broken-Link-Detection
==========================================================================================
WLAN-1    Yes           Scanner         Normal                No
WLAN-2    Yes           managed-AP      Normal                No

root@LN-1700Esc:/Setup/Interfaces/WLAN/Operational
> set ?
```

```
Possible input for columns in table 'Operational':
[  1] Ifc                   : WLAN-1 (1), WLAN-2 (2)
[  2] Operating             : Yes (0), No (1)
[  3] Operation-Mode        : Access-Point (1), managed-AP (4), Station (0),
                              Probe (5), Scanner (7)
[  4] Link-LED-Function     : Normal (0), Client-Mode-Strength (1), P2P-1-Strength (8))
[  5] Broken-Link-Detection : No (0), LAN-1 (1), LAN-2 (2)
```

Der Umgebungsscan wird hierdurch wie oben beschrieben durchgeführt; nach dem Scannen der konfigurierten Kanäle wird der Scan nicht beendet, sondern wieder von vorne begonnen.

Diese Betriebsart kann verwendet werden, um einen AP dediziert als "Scanner"-AP zu verwenden.

Das Ergebnis des Umgebungsscans kann in der Tabelle **Status** > **WLAN** > **Environment-Scan-Results** eingesehen werden.

Zur Konfiguration in LANconfig siehe *Umgebungs-Scan* auf Seite 1048.

13.4.9 Erkennung von Replay-Attacken

Bei mit AES oder TKIP verschlüsselten Paketen erhält jedes Paket eine eindeutige Sequenznummer, damit der Empfänger Replays erkennen und verwerfen kann. Sofern QoS aktiviert ist, muss der Empfänger sogar pro Prioritäts-Stufe einen solchen Replay-Zähler mithalten.

Damit ergibt sich eine Angriffsmöglichkeit, bei der ein Angreifer ein mitgesnifftes Paket auf einer anderen Prio-Stufe 'replayen' kann. Einige Ansätze für Angriffe auf TKIP beruhen auf diesem Umstand.

Seit LCOS-Version 7.70 gibt es im Empfänger neben der Replay-Prüfung pro Prio-Stufe eine weitere 'globale' Prüfung, die zuletzt von der Gegenstelle genutzte Sequenznummern mithält. Da Sequenznummern vom Sender nicht auf verschiedenen Prio-Stufen mehrfach genutzt werden dürfen, kann man so Replay-Attacken auf einer anderen Prio-Stufe in begrenztem Umfang erkennen.

Einige WLAN-Clients, z. B. aus dem Bereich der Mobiltelefone, nutzen eine fehlerhafte AES-Implementierung mit einem separaten Sequenzzähler im Sender pro Prio-Stufe, so dass die beschriebenen Mehrfachverwendungen bei diesen Geräten normal sind.

Um auch für diese Geräte einen Betrieb zu ermöglichen, kann die globale Prüfung der Krypto-Sequenz ausgelassen werden.

Konsole: **Setup** > **WLAN**

Globale-Krypto-Sequenz-Pruefung-auslassen

Stellen Sie hier die globale Prüfung der Krypto-Sequenz ein.

Mögliche Werte:

› Auto, Ja, Nein

Default:

› Auto

Besondere Werte:

› Auto: LCOS enthält eine Liste der für diese Verhalten bekannten Geräte und schaltet in der Einstellung 'Auto' die globale Sequenzprüfung ab. Für andere, noch nicht in der Liste enthaltenen Geräte muss die globale Sequenzprüfung manuell deaktiviert werden.

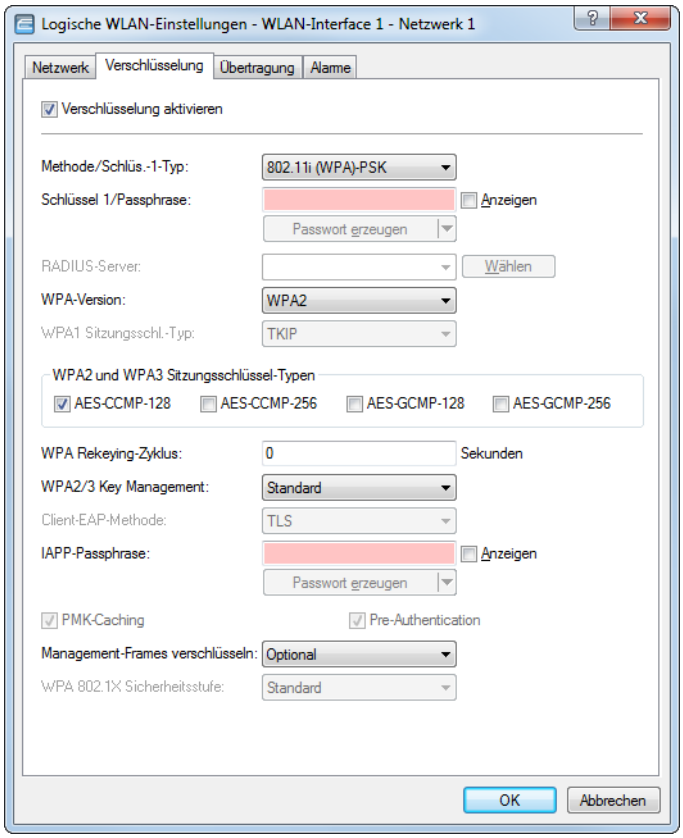
13.4.10 WLAN Protected Management Frames (PMF)

Die in einem WLAN übertragenen Management-Informationen zum Aufbau und Betrieb von Datenverbindungen sind standardmäßig unverschlüsselt. Jeder innerhalb einer WLAN-Zelle kann diese Informationen empfangen und auswerten, selbst wenn er nicht an einem AP angemeldet ist. Das birgt zwar keine Gefahren für eine verschlüsselte Datenverbindung,

kann aber die Kommunikation innerhalb einer WLAN-Zelle durch gefälschte Management-Informationen empfindlich stören.

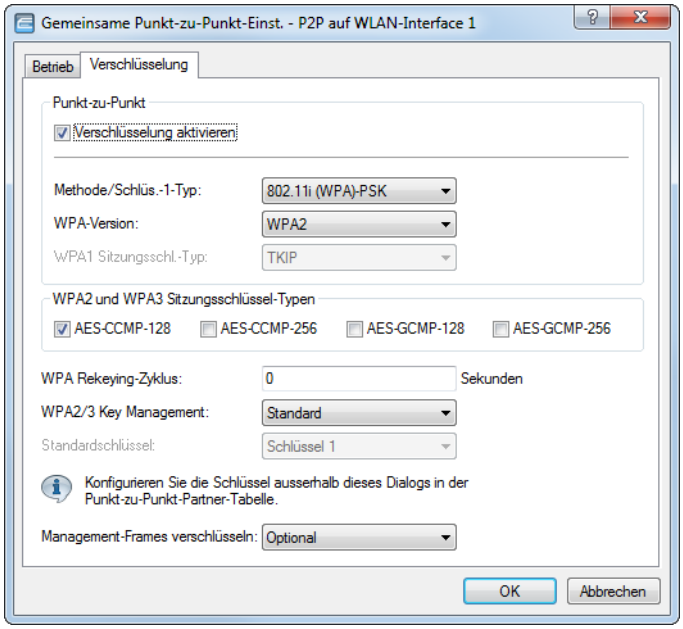
Der Standard IEEE 802.11w verschlüsselt die übertragenen Management-Informationen, so dass ein Angreifer, der nicht im Besitz des entsprechenden Schlüssels ist, die Kommunikation nicht mehr stören kann.

Um Protected Management Frames für ein logisches WLAN-Interface zu aktivieren, wechseln Sie in LANconfig in die Ansicht **Wireless-LAN** > **Allgemein** > **Logische WLAN-Einstellungen**, öffnen die Konfiguration der entsprechenden WLAN-Schnittstelle, wechseln auf den Reiter **Verschlüsselung** und wählen in der Auswahlliste **Management-Frames verschlüsseln** die entsprechende Option.

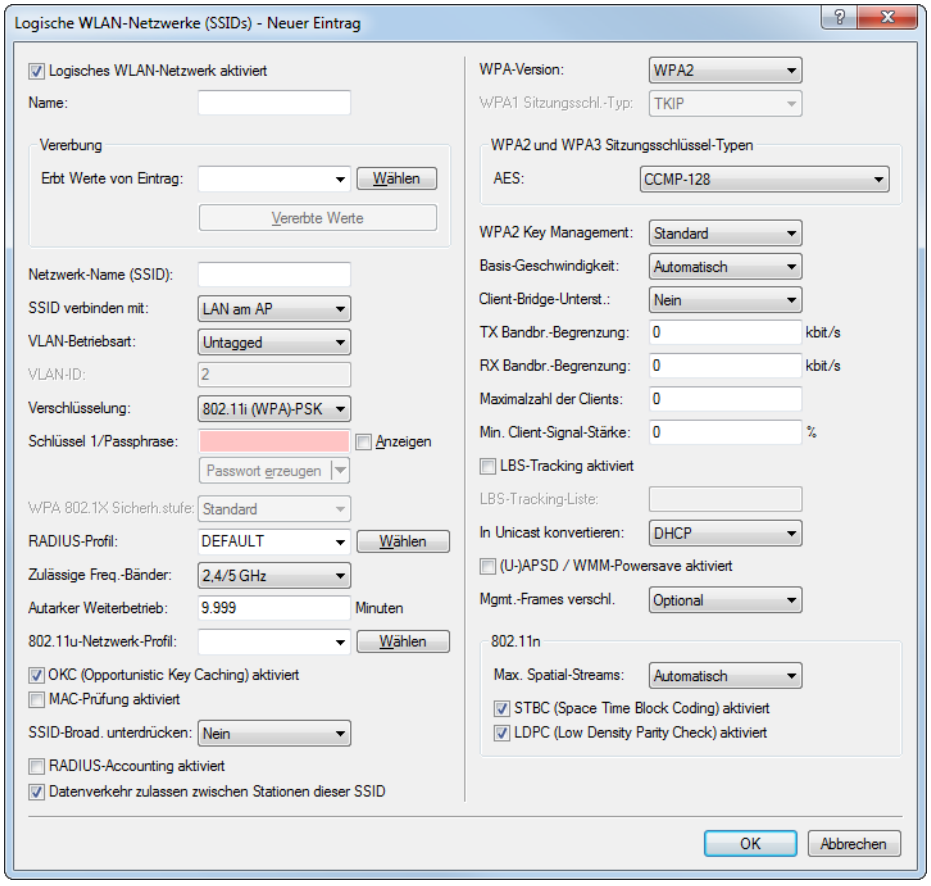


Um die Management-Frames bei P2P-Verbindung zwischen den Basisstationen zu verschlüsseln, wechseln Sie in LANconfig in die Ansicht **Wireless-LAN** > **Allgemein** > **Gemeinsame Punkt-zu-Punkt-Einst.**, öffnen die P2P-Konfiguration der

entsprechenden WLAN-Schnittstelle, wechseln auf den Reiter **Verschlüsselung** und wählen in der Auswahlliste **Management-Frames verschlüsseln** die entsprechende Option.



Um die Verschlüsselung von Management-Frames über einen WLAN-Controller zu verwalten, wechseln Sie in LANconfig in die Ansicht **WLAN-Controller** > **Profile**, klicken auf **Logische WLAN-Netzwerke (SSIDs)** und wählen in der Auswahlliste **Mgmt.-Frames verschlüsseln** die entsprechende Option.



Folgende Optionen stehen bei allen Konfigurationen zur Auswahl:

Nein

Das WLAN-Interface unterstützt kein PMF. Die WLAN-Management-Frames sind nicht verschlüsselt.

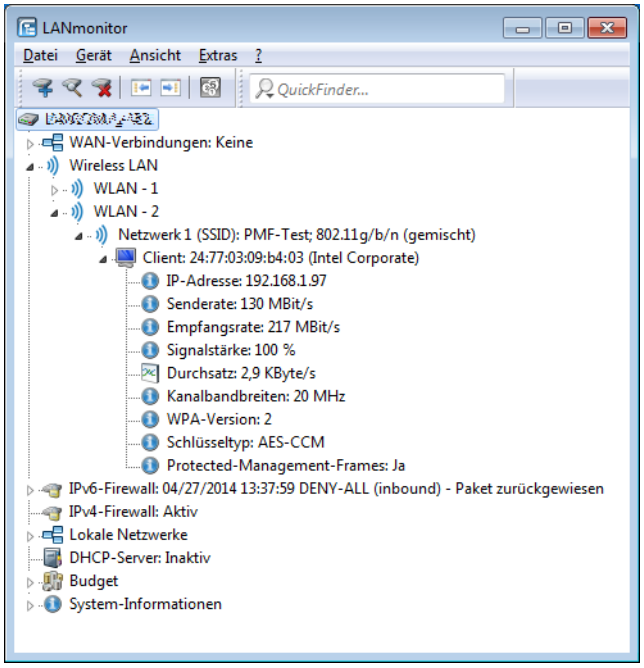
Erzwingen

Das WLAN-Interface unterstützt PMF. Die WLAN-Management-Frames sind immer verschlüsselt. Eine Verbindung zu WLAN-Clients, die PMF nicht unterstützen, ist nicht möglich.

Optional

Das WLAN-Interface unterstützt PMF. Die WLAN-Management-Frames sind je nach PMF-Unterstützung des WLAN-Clients verschlüsselt oder unverschlüsselt.

Der LANmonitor zeigt unterhalb des entsprechenden Clients an, ob dieser die WLAN-Management-Frames verschlüsselt.



13.5 LANCOM Active Radio Control (ARC)

Mit dem intelligenten WLAN-Optimierungskonzept **LANCOM Active Radio Control (ARC)** optimieren Sie nachhaltig Ihr Funkfeld und vermeiden proaktiv Störquellen im WLAN. Active Radio Control besteht aus mehreren, sich ideal ergänzenden Funktionen im LANCOM Betriebssystem LCOS, mithilfe dessen Sie die Leistungsfähigkeit Ihres WLANs deutlich verbessern. Alle Funktionen von Active Radio Control sind kostenlos enthalten im LANCOM Betriebssystem LCOS und lassen sich einfach über die entsprechenden Management-Tools bedienen.

RF Optimization (Funkfeldoptimierung)

Automatische Auswahl optimaler WLAN-Kanäle: WLAN-Clients profitieren von einem verbesserten Durchsatz dank reduzierter Kanalüberlappungen. In Controller basierten WLAN-Installationen erfolgt eine automatische Auswahl optimaler Kanäle für verwaltete Access Points.

Weitere Informationen dazu finden Sie in den Abschnitten *Adaptive RF Optimization* auf Seite 978 und *Funkfeldoptimierung* auf Seite 1227.

Airtime Fairness

Verbesserte Ausnutzung der WLAN-Bandbreite: Insbesondere in WLAN-Szenarien mit einer hohen Dichte an Endgeräten konkurrieren die Clients um die zur Verfügung stehende Bandbreite. Dabei wird aktiven Clients seitens des Access Points reihum eine Sendegelegenheit eingeräumt – ohne Berücksichtigung der notwendigen Übertragungszeit. So kommt es, dass langsamere (Legacy) Clients während der Übertragung von Datenpaketen schnellere Clients ausbremsen, obwohl diese in sehr kurzer Zeit ihre Datenübertragung abschließen könnten. Das Feature Airtime Fairness stellt sicher, dass die zur Verfügung stehende Bandbreite effizient ausgenutzt wird. Dazu werden die WLAN-Übertragungszeiten („Airtime") unter den aktiven Clients fair aufgeteilt. Die Folge: Dadurch dass alle Clients dieselbe Airtime zur Verfügung haben, können schnellere Clients entsprechend mehr Datendurchsatz in derselben Zeit erreichen.

Weitere Informationen dazu finden Sie im Abschnitt *Airtime Fairness* auf Seite 980.

Band Steering

Nutzen Sie die Bandbreite Ihres WLANs optimal aus: Der automatische, wahlweise vom AP oder WLC gesteuerte Wechsel von Clients in das 5-GHz-Frequenzband verdoppelt die WLAN-Performance, weil meist nur dort genügend Kanäle für eine Kanalbündelung zur Verfügung stehen.

Weitere Informationen dazu finden Sie im Abschnitt *WLAN Band Steering* auf Seite 982.

Client Steering

Mehr Leistung für WLAN Clients dank intelligenter Steuerung: Dank einer aktiven Steuerung von WLAN Clients auf den für sie sinnvollsten Access Point wird die Leistungsfähigkeit des WLANs in Controller-basierten Netzwerken deutlich gesteigert. Insbesondere in WLAN-Szenarien mit einer hohen Anzahl an Endgeräten ist Client Steering ideal für eine optimale Lastverteilung. Abhängig von vordefinierten Szenarien oder individuell festgelegten Parametern, wie Signalstärke, Frequenzband oder Anzahl der eingebuchten Clients, werden die Endgeräte auf dem für sie besten Access Point eingebucht und schöpfen so das volle Bandbreitenpotenzial aus. Und das Beste: alles passiert vollautomatisch, ohne dass Einstellungen an den Clients vorgenommen werden müssen.

Weitere Informationen dazu finden Sie im Abschnitt *Client Steering über den WLC* auf Seite 1230.

Client Management

Mit Client Management werden WLAN-Clients stets auf den für sie idealen Access Point sowie das beste Frequenzband gesteuert. Dieses Feature steigert somit die Qualität drahtloser Netzwerke jeder Größenordnung - egal ob im stand-alone-Betrieb oder orchestriert über die LANCOM Management Cloud. Die beliebten, aber bislang getrennten Funktionen Band Steering und Client Steering werden hiermit kombiniert und auch ohne den Betrieb mit einem WLAN-Controller bereitgestellt.

Im Vergleich zum bisherigen WLC-gestützten Client Steering funktioniert Client Management autark und ohne WLC. die Access Points kommunizieren dazu untereinander mittels des Protokolls IAPP.

Weitere Informationen dazu finden Sie im Abschnitt *Client Management* auf Seite 983.

Adaptive Noise Immunity

Besserer WLAN-Durchsatz durch Immunität vor Störsignalen: WLAN-Clients profitieren von deutlich mehr Datendurchsatz dank einer ungestörten Funkabdeckung. Durch aktivierte Adaptive Noise Immunity blendet ein Access Point Störquellen im Funkfeld aus und fokussiert sich ausschließlich auf WLAN-Clients mit ausreichender Signalstärke.

Weitere Informationen dazu finden Sie im Abschnitt *Adaptive Noise Immunity zur Abschwächung von Interferenzen im WLAN* auf Seite 987.

Spectral Scan

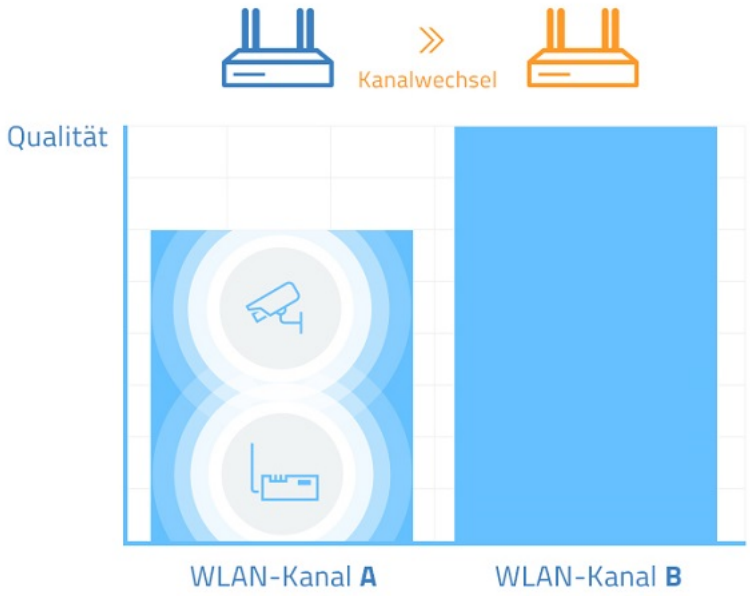
Überprüfen Sie Ihr WLAN-Funkspektrum auf Störquellen: Mit LANCOM Spectral Scan haben Sie ein professionelles Werkzeug für ein effizientes WLAN-Troubleshooting. Ein Scan des gesamten Funkspektrums identifiziert Störquellen außerhalb des WLANs und ermöglicht eine grafische Darstellung.

Weitere Informationen dazu finden Sie im Abschnitt *Spectral Scan* auf Seite 988.

13.5.1 Adaptive RF Optimization

Höherer WLAN-Durchsatz dank dynamischer Auswahl des qualitativ besten WLAN-Kanals durch den Access Point bei Kanalstörungen.

Mit der Auswahl des WLAN-Kanals wird der Teil des Frequenzbandes festgelegt, den ein AP für seine logischen WLANs verwendet. Um in der Funkreichweite eines anderen APs ein WLAN störungsfrei betreiben zu können, sollte jeder AP einen separaten Kanal nutzen – anderenfalls müssen sich die WLANs die Bandbreite des Kanals teilen (Shared Medium). Zu diesem Zweck nutzen LANCOM APs das Feature Adaptive RF Optimization. Dabei scannt der AP permanent das Funkfeld auf Störsignale. Wird ein bestimmter Schwellenwert (auf Basis der „Wireless Quality Indicators“) im aktuell verwendeten WLAN-Kanal überschritten, wechselt der AP automatisch auf einen qualitativ besseren Kanal. Diese intelligente Funktion ermöglicht es dem AP, sich an ein sich veränderndes Funkfeld dynamisch anzupassen, um somit die Robustheit des WLANs zu maximieren.

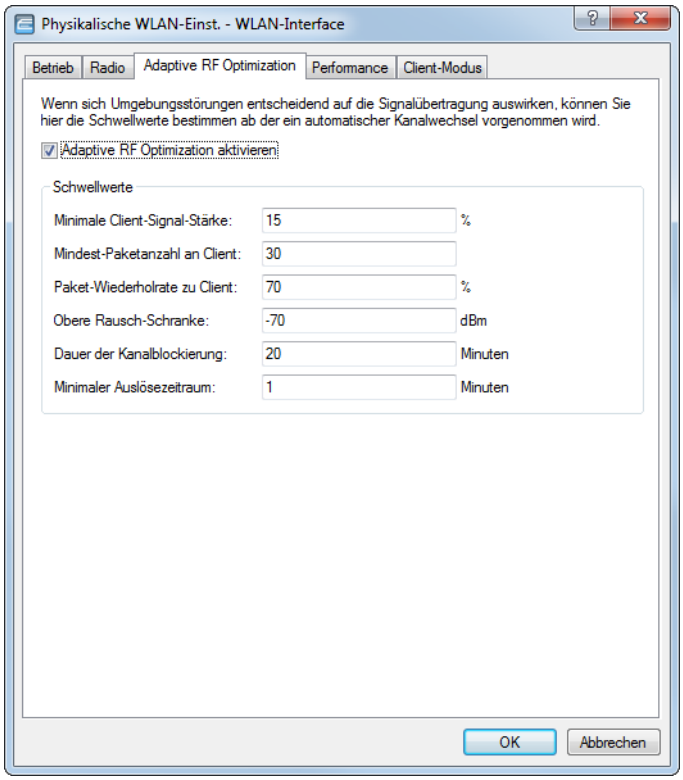


Sie haben in LANconfig die Möglichkeit, die Schwellenwerte, die zu einem automatischen Kanalwechsel führen, manuell festzulegen.

13.5.1.1 Adaptive RF Optimization mit LANconfig konfigurieren

Um die Funktion Adaptive RF Optimization über LANconfig konfigurieren zu können, ist es erforderlich, dass die zu konfigurierenden Geräte das Feature "Wireless Quality Indicators" anbieten.

Um die Adaptive RF Optimization mit LANconfig zu konfigurieren, wechseln Sie in die Ansicht **Wireless-LAN** > **Allgemein**. Klicken Sie anschließend im Abschnitt „Interfaces“ auf die Schaltfläche **Physikalische WLAN-Einst.**. Wählen Sie die gewünschte WLAN-Schnittstelle aus und wechseln Sie danach auf den Reiter **Adaptive RF Optimization**.



Adaptive RF Optimization aktivieren

Um die Überwachung der WLAN-Umgebung durch die Adaptive RF Optimization zu aktivieren, markieren Sie die Option **Adaptive RF Optimization aktivieren**.

Konfigurieren Sie anschließend die Schwellwerte, die einen automatischen Kanalwechsel auslösen sollen.

Minimale Client-Signal-Stärke

Definieren Sie die minimale Signalstärke, mit der ein Client gesehen werden muss. Wird dieser Wert unterschritten, wird der entsprechende Client nicht in der Auswertung berücksichtigt und kann somit auch kein Auslöser für einen Kanalwechsel sein. Die Angabe erfolgt in % (Defaultwert: 15).

Mindest-Paketanzahl an Client

Geben Sie an, wie viele Pakete mindestens an einen Client gesendet werden müssen (TX). Wird dieser Wert unterschritten, wird der entsprechende Client nicht in der Auswertung berücksichtigt und kann somit auch kein Auslöser für einen Kanalwechsel sein (Defaultwert: 30).

Paket-Wiederholrate zu Client

Hier definieren Sie die Obergrenze der Paket-Wiederholrate zu Clients. Hat ein Client mehr als die hier angegebene Prozentzahl an Paketen erhalten, berücksichtigt das Gerät diesen Client bei der Entscheidung für einen Kanalwechsel. Die Angabe erfolgt in % (Defaultwert: 70).

Obere Rausch-Schranke

Definieren Sie die Obergrenze des zulässigen Kanalrauschens. Die Angabe erfolgt in dBm (Defaultwert: -70).

Dauer der Kanalblockierung

Wird ein Kanal als unbrauchbar erkannt, wird er für diese Zeit markiert / blockiert. Dieser Wert steuert auch die Blockierungszeit des Kanalwechseltriggers, falls alle Kanäle gleichzeitig blockiert sind. Die Angabe erfolgt in Minuten (Defaultwert: 20).

Minimaler Auslösezeitraum

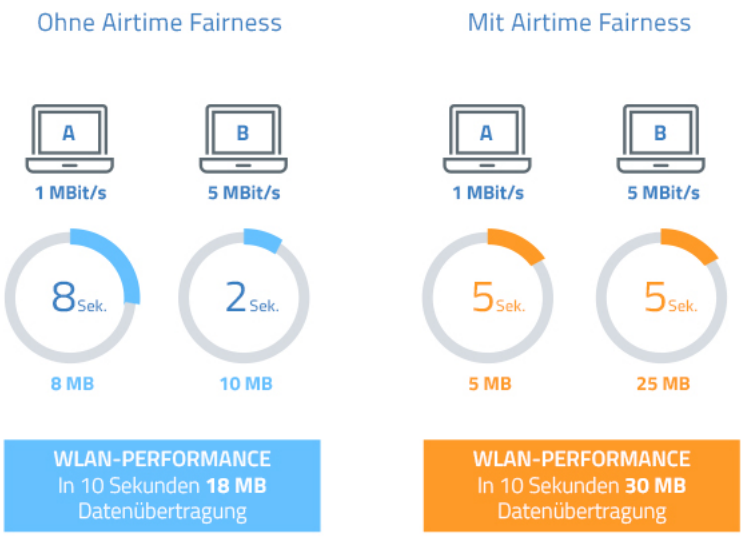
Geben Sie an, für wie lange ein Limit überschritten sein muss, bevor das Gerät eine Aktion auslöst. Erfolgt pro Periode (20 Sekunden) keine Limitüberschreitung, setzt das Gerät die abgelaufene Zeit zurück. Bei einer Limitüberschreitung über den gesamten angegebenen Zeitraum markiert / blockiert das Gerät den Kanal. Die Angabe erfolgt in Minuten (Defaultwert: 1).

Für diesen Wert empfehlen sich kleine einstellige Werte.

13.5.2 Airtime Fairness

Bessere WLAN-Performance durch effiziente Ausnutzung der zur Verfügung stehenden Bandbreite dank einer fairen Aufteilung der WLAN-Übertragungszeiten unter den aktiven Clients

Insbesondere in WLAN-Szenarien mit einer hohen Dichte an Endgeräten konkurrieren die Clients um die zur Verfügung stehende Bandbreite. Dabei sendet der AP reihum an die aktiven Clients – ohne Berücksichtigung der notwendigen Übertragungszeit. So kommt es, dass langsamere (Legacy) Clients während der Übertragung von Datenpaketen schnellere Clients ausbremsen, obwohl diese in sehr kurzer Zeit ihre Datenübertragung abschließen könnten. Das Feature „Airtime Fairness" stellt sicher, dass die zur Verfügung stehende Bandbreite effizient ausgenutzt wird. Dazu wird die WLAN-Übertragungszeit („Airtime") zwischen den aktiven Clients fair aufgeteilt. Die Folge: Dadurch, dass alle Clients dieselbe Airtime zur Verfügung haben, können schnellere Clients entsprechend mehr Datendurchsatz in derselben Zeit erreichen.

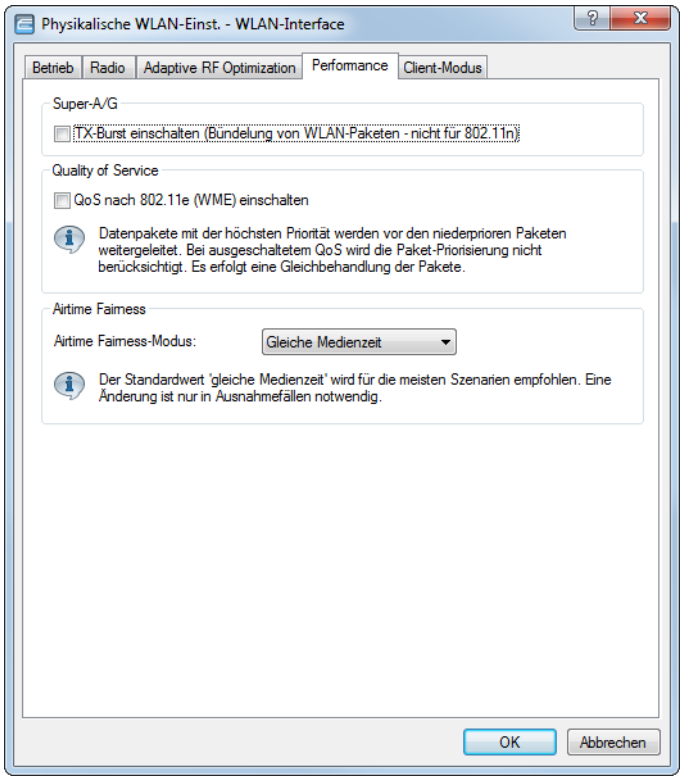


„Airtime" bedeutet WLAN-Übertragungszeit. Airtime Fairness stellt somit allen aktiven Clients eine WLAN-Übertragungszeit in Richtung der Clients entsprechend dem konfigurierten Airtime Fairness-Modus zur Verfügung. Dies verhindert z. B., dass ältere Clients moderne Clients ausbremsen.

Bei Geräten mit WLAN-Modulen, die den Standard IEEE 802.11ac unterstützen, ist die Funktion **Airtime Fairness** automatisch im WLAN-Modul aktiviert.

13.5.2.1 Airtime Fairness mit LANconfig konfigurieren

Wechseln Sie in die Ansicht **Wireless-LAN** > **Allgemein**. Klicken Sie anschließend im Abschnitt **Interfaces** auf die Schaltfläche **Physikalische WLAN-Einst.**. Wählen Sie bei Geräten mit mehreren WLAN-Schnittstellen die gewünschte WLAN-Schnittstelle aus und wechseln Sie danach auf den Reiter **Performance**.



Wählen Sie unter **Airtime Fairness-Modus** aus den verfügbaren Einstellmöglichkeiten die für Ihre WLAN-Umgebung passende Option aus:

Round-Robin-Verteilung

Das Gerät sendet nacheinander an die aktiven Clients im Netzwerk.

Gleiche Medienzeit

Alle Clients verfügen über die gleiche Airtime. Clients mit einer höheren Datenrate profitieren von dieser Einstellung, da sie in der gleichen Zeit mehr Daten empfangen können.

IEEE 802.11ac-fähige WLAN-Module verwenden bereits hardwareseitig einen Algorithmus, der dieser Einstellung entspricht.

802.11n bevorzugen

Diese Einstellung bevorzugt IEEE 802.11n-Clients gegenüber älteren Clients. Demnach erhalten Clients mit dem Standard 802.11a oder 802.11g im Verhältnis zum 802.11n lediglich 25% Airtime. Clients mit 802.11b-Standard erhalten nur 6,25% Airtime. Daher versendet das Gerät deutlich schneller Daten an Clients mit dem Standard IEEE 802.11n.

Gleiches Medienvolumen

Diese Einstellung bewirkt, dass das Gerät die Airtime so zuweist, dass alle Clients die gleiche Datenmenge aus Richtung des APs erhalten. Allerdings bremsen langsamere Clients die schnelleren Teilnehmer bei dieser Option aus.

Diese Einstellung ist nur sinnvoll, wenn ein gleicher Datendurchsatz bei allen Clients erforderlich ist.

13.5.3 WLAN Band Steering

Der Standard IEEE 802.11 enthält kaum Kriterien, nach denen ein WLAN-Client den AP für eine Verbindung auswählen sollte. Zwar gibt es allgemeine Richtlinien, wonach z. B. ein AP mit höherem RSSI-Wert (d. h. der empfangenen Signalstärke) zu bevorzugen ist. Doch in der Praxis beachten WLAN-Clients weder die oben angesprochenen Definitionen noch die allgemeinen Richtlinien konsequent. Wird eine SSID in sowohl 2,4 GHz als auch 5 GHz ausgestrahlt, besteht im Normalfall keine Möglichkeit auf die Entscheidung des Clients, welches Frequenzband er bevorzugt, Einfluss zu nehmen.

Die gezielte Zuweisung von WLAN-Clients, das sog. „Client Steering", basiert auf dem Prinzip, dass viele Clients die verfügbaren APs durch einen aktiven Scan-Vorgang ermitteln. Aktives Scannen bedeutet hier, dass ein Client Test-Anforderungspakete (Probe Requests) versendet, welche die Netzwerkkennung enthalten, zu der ein Client eine Verbindung aufbauen soll. APs mit der entsprechenden Kennung versenden daraufhin eine Test-Antwort und ermöglichen es dem Client auf diese Weise, eine Liste mit verfügbaren APs zu erstellen. Die Tatsache, dass die weitaus meisten WLAN-Clients sich nur mit solchen APs verbinden, von denen sie eine Test-Antwort (Probe Response) erhalten haben, kann zur Steuerung des Auswahlverhaltens (und somit zur gezielten Zuweisung) eingesetzt werden.

Für die gezielte Zuweisung gibt es mehrere, zum Teil sehr fortgeschrittene Kriterien. Eines dieser Kriterien betrifft die verwendeten Funkfrequenzbereiche, in denen Clients kommunizieren. So erwartet man von modernen Dual-Band-WLAN-Clients immer häufiger, dass diese den 5-GHz-Frequenzbereich gegenüber dem inzwischen überfüllten 2,4-GHz-Bereich bevorzugen. Weist man einem WLAN-Client ganz gezielt ein bestimmtes Frequenzband bzw. einen bestimmten Frequenzbereich zu, spricht man von Band Steering.

Die Liste mit den ermittelten (bzw. „gesehenen") Clients enthält alle Clients, von denen der AP ein Test-Anforderungspaket empfangen hat. Zusammen mit der Funkfrequenz, auf der der WLAN-Client die Test-Anforderung gesendet hat, bildet diese Liste eine der Entscheidungsgrundlagen für den AP, die betreffende Anforderung zu beantworten oder nicht.

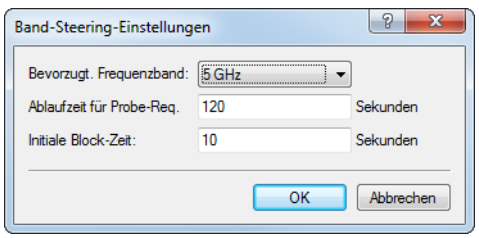
Weitere Kriterien für eine solche Entscheidungsfindung hängen mit den gemeldeten Kennungen der Clients und der Konfiguration der Geräte zusammen: So kann es z. B. vorkommen, dass auf dem bevorzugten Frequenzband weniger SSIDs gemeldet werden als auf dem weniger bevorzugten. Ebenso kann eine zu geringe Sendestärke beim Melden der SSIDs dazu führen, dass der Client auf dem bevorzugten Frequenzband keine Test-Antwort erhält. Für den letzteren Fall sollte man sicherstellen, dass der AP Test-Antworten auf dem weniger bevorzugten Frequenzband nicht durch den Steuerungsmechanismus unterdrückt. Die dafür verantwortliche, minimale Signalstärke können Sie über die folgenden Wege einstellen:

- LANconfig: **Wireless-LAN** > **Allgemein** > **Logische WLAN-Einstellungen** > **Netzwerk** > **Minimale Client-Signal-Stärke**
- Konsole: **Setup** > **Schnittstellen** > **WLAN** > **Netzwerk** > **Minimal-Stations-Staerke**

Sie können das Band-Steering des Access Points im LANconfig unter **Wireless-LAN** > **Client-Management** > **Client-Management** > **Management-Modus** durch die Einstellung **AP-basiertes Band-Steering** aktivieren und dann unter **Wireless-LAN** > **Client-Management** > **Experten-Einstellungen** > **Band-Steering-Einstellungen** verwalten.

13.5.3.1 Band Steering konfigurieren

Dieser Dialog bietet Ihnen die Möglichkeit, die Einstellungen für das Band Steering in LANconfig vorzunehmen.



Unter **Wireless-LAN** > **Client-Management** > **Experten-Einstellungen** > **Band-Steering-Einstellungen** stehen Ihnen folgende Funktionen zur Verfügung:

Bevorzugtes Frequenzband

Gibt das Frequenzband vor, auf welches das Gerät WLAN-Clients leitet. Mögliche Werte sind:

- **2,4 GHz**: Das Gerät leitet Clients auf das 2,4 GHz Frequenzband.
- **5 GHz**: Das Gerät leitet Clients auf das 5 GHz Frequenzband.

Ablaufzeit für Probe-Requests

Der Zeitraum, während dessen der Access Point den WLAN-Client auf das bevorzugte Frequenzband leitet. Der Standardwert lautet 120 Sekunden.

Initiale Block-Zeit

Geht ein Access Point mit einem 5-GHz-DFS-Funkmodul und aktiviertem Band Steering erstmalig oder nach einem Neustart in Betrieb, kann er während des DFS-Scans keine Dual-Band-fähigen WLAN-Clients erkennen. Als Folge kann der Access Point einen vorhandenen WLAN-Client nicht auf ein ggf. bevorzugtes 5-GHz-Band leiten. Stattdessen würde das 2,4-GHz-Funkmodul die Anfrage des Clients beantworten und ihn auf das 2,4-GHz-Band leiten.

Durch die Eingabe einer initialen Block-Zeit beantwortet das auf 2,4 GHz konfigurierte Funkmodul des Access Points Anfragen eines WLAN-Clients um die entsprechend angegebene Zeit später. Der Default-Wert ist 10 Sekunden.

Durch die verzögerte Antwort auf 2,4-GHz-Probe-Responses veranlasst der Access Point zusätzlich einen WLAN-Client, der ggf. den 5-GHz-Scan überspringt, weil er bereits einen Access Point auf 2,4 GHz erwartet, erneut auf 5 GHz zu scannen.

Das Einbuchen eines reinen 2,4-GHz-WLAN-Clients erfolgt ebenfalls erst nach der eingestellten Verzögerungszeit. Wenn keine 5-GHz-WLAN-Clients im Netzwerk vorhanden sind, sollte die Verzögerungszeit 0 Sekunden betragen.

13.5.4 Client Management

Mit Client Management werden WLAN-Clients stets auf den für sie idealen Access Point sowie das beste Frequenzband gesteuert. Dieses Feature steigert somit die Qualität drahtloser Netzwerke jeder Größenordnung - egal ob im stand-alone-Betrieb oder orchestriert über die LANCOM Management Cloud. Die beliebten, aber bislang getrennten Funktionen Band Steering und Client Steering werden hiermit kombiniert und auch ohne den Betrieb mit einem WLAN-Controller bereitgestellt.

Im Vergleich zum bisherigen WLC-gestützten Client Steering funktioniert Client Management autark und ohne WLC. die Access Points kommunizieren dazu untereinander mittels des Protokolls IAPP.

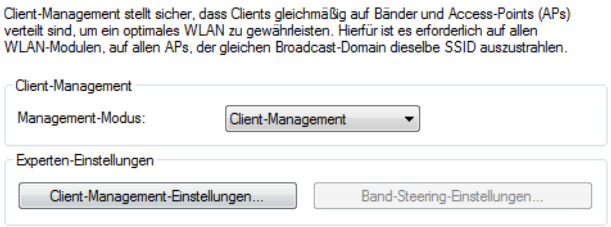
Damit die Kommunikation der Access Points untereinander funktioniert, ist es erforderlich, dass alle Access Points IAPP-Nachrichten austauschen können. IAPP-Nachrichten werden als Multicast übertragen. Gegebenenfalls sind auf Infrastrukturseite, insbesondere auf Switches, passende Ausnahmeregelungen im IGMP-Snooping oder anderen Filtermechanismen zu schaffen. IAPP verwendet die Multicast-Gruppe 224.0.1.76.

LANCOM Switches in der Defaulteinstellung sind bereits korrekt für das Client Management eingestellt.

Client Management stellt somit sicher, dass Clients gleichmäßig auf Frequenzbänder und Access Points verteilt sind, um ein optimales WLAN zu gewährleisten. Hierfür ist es erforderlich, dass sowohl auf allen WLAN-Modulen als auch auf allen Access Points der gleichen Broadcast-Domäne dieselbe SSID ausgestrahlt wird.

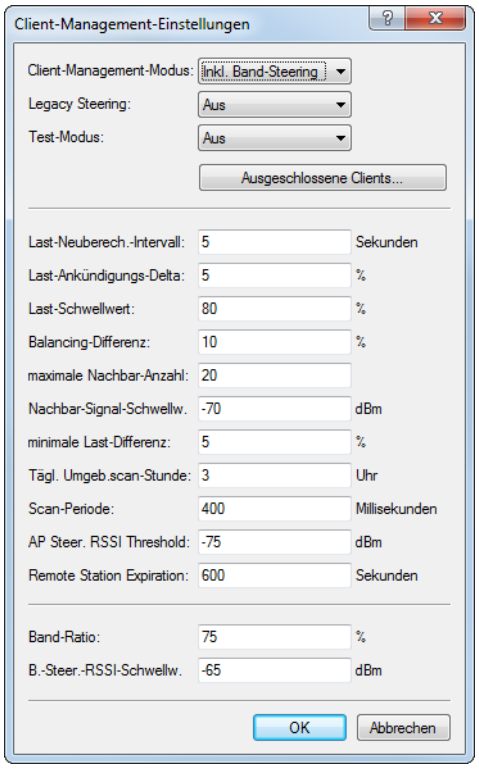
13.5.4.1 Konfiguration des Client Managements

Das Client Management können Sie unter **Wireless-LAN** > **Client-Management** > **Client-Management** > **Management-Modus** ein- bzw. ausschalten. Auf Neuinstallationen ist es per Voreinstellung eingeschaltet und benötigt normalerweise keine besonderen Einstellungen. Bei einem Access Point mit mehreren WLAN-Modulen kann alternativ auch das **AP-basierte Band-Steering** aktiviert werden. Siehe hierzu *WLAN Band Steering* auf Seite 982.



Experten-Einstellungen

Konfigurieren Sie unter **Wireless-LAN** > **Client-Management** > **Experten-Einstellungen** > **Client-Management** die Einstellungen des Client Managements. Mit den Voreinstellungen funktioniert das Client Management optimal in Büro- und Schulumgebungen.



Client-Management-Modus

Bei Access Point mit mehreren WLAN-Modulen kann das Client Management mit und ohne Band Steering durchgeführt werden.

Standardeinstellung: inkl. Band Steering

Legacy-Steering

Konfiguriert, ob auch Clients, die 802.11v nicht oder nicht korrekt unterstützen, vom Client Management auf andere Access Points geleitet werden sollen. Auch bei aktivem Legacy-Steering wird das Client Management weiterhin erst 802.11v-fähige Clients auf andere Access Points leiten; erst anschließend werden Clients, die

802.11v nicht unterstützen, geleitet. Legacy-Steering erzwingt das Umleiten dieser Clients durch eine erzwungene Trennung des Clients vom WLAN. Anschließend wird das erneute Einbuchen des Clients am aktuellen AP für eine gewisse Zeit blockiert, damit der Client seibsttätig einen anderen Access Point wählt. Dies kann im Gegensatz zum Leiten der Clients mittels 802.11v zu einer verschlechterten Benutzererfahrung führen. Dies ist vorrangig vom Verhalten der Legacy-Clients abhängig.

Standardeinstellung: Aus

Test-Modus

Betreibt Client-Management im Test-Modus: Umgebungs-Scans werden durchgeführt, Steering-Entscheidungen werden vom System getroffen und im Syslog verzeichnet, aber es findet kein tatsächliches Steering der Clients statt. Verwenden Sie den Test-Modus, um das Verhalten des Client Managements zu prüfen ohne tatsächliche Änderungen an Ihrem Netzwerk durchzuführen.

Standardeinstellung: Aus

Ausgeschlossene Clients

In vielen Umgebungen gibt es spezielle Clients, von denen bekannt ist, dass sie sich nicht gut verhalten. Stellen Sie sich ein Krankenhaus mit kundenspezifischen VoIP-Telefonen vor, die nicht in der Lage sind, Verbindungsabbrüche ordnungsgemäß zu behandeln, und die dazu neigen, sich an einen bestimmten Access Point zu halten. Um nun nicht das Client Management komplett abschalten zu müssen, kann man diese Clients von der Steuerung ausnehmen.

Konfigurieren Sie in der Tabelle die MAC-Adressen der Clients, die von einer Steuerung ausgenommen werden sollen. Als Wildcard-Zeichen kann der `*` verwendet werden, der für beliebige Zeichen steht. Dieses darf aber nicht als einziges Zeichen einer MAC-Adresse verwendet werden. Möglich sind also z. B. `01:23:45:12:34:56`, `01:*:56` oder `01:23:*`.

Last-Neuberechnungs-Intervall

Konfiguriert das Intervall, in dem die Last auf dem AP berechnet wird und Entscheidungen zum Steering der Clients getroffen werden. Erhöhen Sie den Wert, um die Last im Netzwerk zu reduzieren. Verringern Sie den Wert, um schneller eine Neuverteilung der Clients zu erreichen. Werte < 2 Sekunden werden aufgrund von negativen Effekten in der Netzwerk-Laufzeit nicht empfohlen. Werten von > 10 Sekunden werden nicht empfohlen, da das Steering der Clients sonst nicht rechtzeitig erfolgt. Es wird empfohlen, den standardmäßig eingestellten Wert nicht zu ändern.

Standardwert: 5 Sekunden

Last-Ankündigungs-Delta

Konfiguriert, bei welcher prozentualen Änderung der aktuellen Last ein Access Point diese auch außerhalb des regulären Ankündigungs-Intervalls an andere Access Points kommuniziert. Erhöhen Sie den Wert in Installationen mit vielen mobilen Clients. Verringern Sie den Wert in Installationen mit wenig beweglichen Clients. Die Standardeinstellung wurde in Hinblick auf Büro- und Schulumgebungen gewählt. Beachten Sie, dass dieser Wert unterhalb des für die Balancing-Differenz konfigurierten Wertes liegen sollte, um Fehlberechnungen zu vermeiden.

Standardwert: 5 %

Last-Schwellenwert

Konfiguriert den Last-Schwellenwert, ab dem der Access Point unabhängig vom Last-Schwellenwert der Nachbar-Access-Points mit dem Steering beginnt. Erhöhen Sie den Wert in low-quality/high-density-Szenarien wie Stadien. Verringern Sie den Wert in high-quality/high-throughput-Szenarien wie Büro/Schule.

Standardwert: 80 %

Balancing-Differenz

Konfiguriert die Last-Differenz zwischen Access Points, ab der Clients zum weniger belasteten Access Point geleitet werden. Hohe Werte führen zu weniger ausgeglichenen Installationen, niedrige Werte zu mehr Steering

der Clients. Erhöhen Sie den Wert, wenn zu viel Client Steering betrieben wird. Verringern Sie den Wert, wenn eine maximal ausgeglichene Installation erforderlich ist. Die Standardeinstellung wurde in Hinblick auf Büro- und Schulumgebungen gewählt.

Standardwert: 10 %

maximale Nachbar-Anzahl

Konfiguriert die Anzahl an Nachbar-Access Points, die vom Client Management auf dem aktuellen Access Point berücksichtigt werden. In High-Density-Szenarien kann eine niedrige Anzahl Vorteile bringen, da Clients so vorrangig auf in der Nähe befindliche Access Points geleitet werden und weniger Management-Kommunikation zwischen den einzelnen Access Points notwendig ist. Werte < 4 werden nicht empfohlen, da so keine ausreichende Anzahl an Access Points für eine sinnvolle Steering-Entscheidung zur Verfügung steht. Werte > 72 werden aufgrund von Limitierungen des 802.11-Protokolls nicht unterstützt.

Standardwert: 20 APs

Nachbar-Signal-Schwellenwert

Konfiguriert die Signalstärke, mit der ein AP gesehen werden muss, um als Nachbar-Access Point eingestuft zu werden. Erhöhen Sie den Wert für High-Density-Szenarien (z. B: -60, -50). Verringern Sie den Wert für Szenarien, in der eine große Abdeckung gefordert ist (z. B. -80,-90).

Standardwert: -70 dBm

minimale Last-Differenz

Konfiguriert die minimale Last-Differenz zwischen benachbarten Access Points, ab der zwischen diesen Access Points ein Steering durchgeführt wird. Das Steering wird nur durchgeführt, wenn der konfigurierte Last-Schwellenwert überschritten wurde. Zur Vermeidung von Fehlberechnung sollte die minimale Last-Differenz die konfigurierte Balancing-Differenz nicht überschreiten. Erhöhen Sie den Wert, um weniger Steering in der Installation zu betreiben. Verringern Sie den Wert, um mehr Steering in der Installation zu betreiben.

Standardwert: 5 %

Täglicher Umgebungsscan zu Stunde

Konfiguriert die Uhrzeit (00-23), zu der täglich der Umgebungs-Scan ausgeführt wird, welcher für das Client Management benötigt wird. Der genaue Zeitpunkt des Scans wird über ein Zeitfenster von 30 Minuten verteilt, um Konflikte zwischen gleichzeitig laufenden Umgebungs-Scans zu minimieren. Der Umgebungs-Scan dauert ca. 15 Sekunden an. Währenddessen können keine WLAN-Daten über das scannende WLAN-Modul übertragen werden.

Standardwert: 3 Uhr

Scan-Periode

Konfiguriert die Laufzeit des Umgebungs-Scans, der zur Identifikation von Nachbar-Access Points dient. Die Scan-Periode sollte das 2- bis 2,5-fache des konfigurierten Beacon-Intervalls betragen; der Standardwert wurde bereits für das Standard-Beacon-Intervall passend gewählt. Dieser Wert ist von 200 ms bis 1000 ms konfigurierbar.

Standardwert: 400 ms

AP Steer. RSSI Threshold

Die Signalstärke, die ein Client auf einem entferntem Access Point haben muss, damit er zu diesem gesteuert wird.

Eine höhere Signalschwelle bewirkt einen niedrigeren Wert potentiell steuerbarer Clients und limitiert somit die Möglichkeiten des Client Managements. Gleichzeitig wäre sie in Umgebungen mit hohen Qualtitätsanforderungen sinnvoll, z. B. bei starker Verwendung von VoIP. Dafür wird eine sehr gute Ausleuchtung und höhere Dichte der Access Points benötigt.

Eine niedrigere Signalschwelle bewirkt einen höheren Wert potentiell steuerbarer Clients, allerdings kann der Algorithmus hierbei auch Clients Access Points mit schlechter Signalqualität zuweisen. Es kann sogar passieren, dass sich Clients weigern, zu einem Access Point mit schlechterer Signalqualität gesteuert zu werden. Es würde in Umgebungen helfen, in denen ein großes Areal abgedeckt werden soll. Werte unterhalb von -80 dBm führen zu einem sehr schlechten Ergebnis, da die Wahrscheinlichkeit steigt, dass Clients sich nicht mit dem Access Point verbinden können, zu dem sie gesteuert werden sollen.

Der Standardwert passt für Büroumgebungen.

Standardwert: -75 dBm

Remote Station Expiration

Zeit, in der ein Access Point sich die Informationen über die Clients eines benachbarten Access Points merkt. Diese Informationen werden zur Beschleunigung der Lenkentscheidungen verwendet. Der Standardwert passt für Büroumgebungen mit einem relativ statischen Aufbau und wenigen sich bewegenden Clients. In Umgebungen mit vielen sich bewegenden oder nur kurzzeitig verbundenen Clients sollte man niedrigere Werte setzen. Zu hohe Werte führen zu Fehlsteuerungen, wenn die Informationen des Caches nicht mehr gültig sind.

Standardwert: 600 Sekunden

Band-Ratio

Konfiguriert die gewünschte Verteilung der Clients zwischen den Radio-Bändern. Das konfigurierte Verhältnis spezifiziert, welcher Anteil an Clients auf das 5-GHz-Band geleitet werden soll.

Standardwert: 75 %

Band-Steering-RSSI-Schwellenwert

Konfiguriert die Signalstärke (RSSI), mit der ein Client auf dem jeweils anderen Radio-Band „gesehen" werden muss, damit er auf dieses Band geleitet wird. Die Standardeinstellung wurde in Hinblick auf Büro-Umgebungen gewählt.

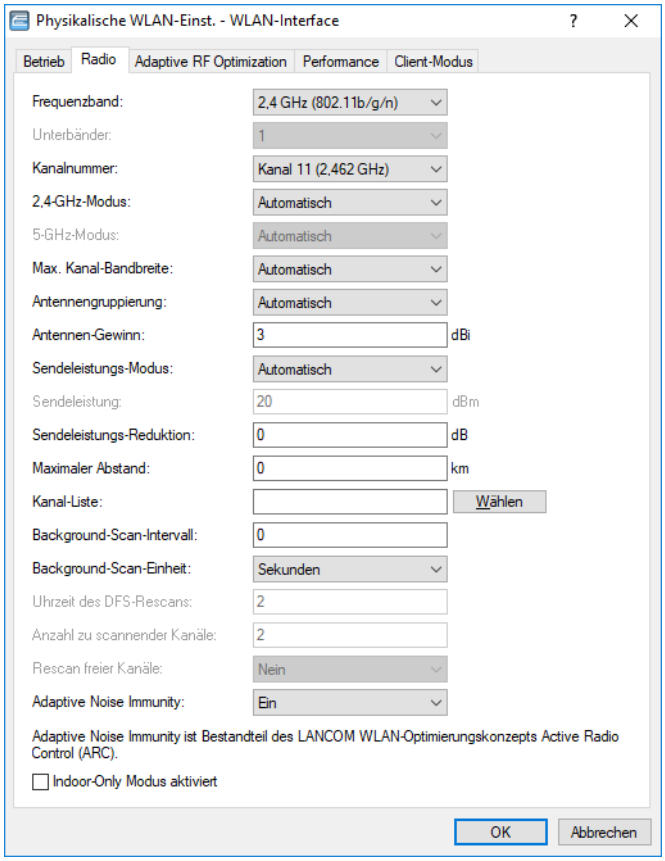
Standardwert: -65 dBm

13.5.5 Adaptive Noise Immunity zur Abschwächung von Interferenzen im WLAN

Innerhalb eines WLANs kann es aus unterschiedlichen Gründen zu Störungen durch Interferenzen kommen. Einerseits stören Geräte wie Mikrowellenherde oder Funktelefone die Datenübertragung, andererseits können die Netzgeräte selber durch Aussendung von Störfrequenzen die Kommunikation behindern. Die Art dieser Störungen ist jeweils charakteristisch. Bei der adaptiven Rausch-Immunität (Adaptive Noise Immunity, ANI) ermittelt der AP anhand verschiedener Fehlerzustände die für die aktuelle Situation beste Kompensation der Störungen. Durch die automatische Erhöhung der Rausch-Immunität wird die Funkzelle gezielt verkleinert, sodass sich die Auswirkungen der Interferenzen auf die Datenübertragung verringern.

Die aktuellen Werte sowie die Aufzeichnung der vergangenen Aktionen finden Sie auf der Konsole unter **Status** > **WLAN** > **Rausch-Immunität**.

Die adaptive Rausch-Immunität aktivieren Sie in LANconfig unter **Wireless-LAN** > **Allgemein** > **Interfaces** > **Physikalische WLAN-Einstellungen** > **Radio**.



Aktivieren Sie die Adaptive Noise Immunity, indem Sie im Auswahlfeld **Adaptive-Noise-Immunity** den Wert "Ein" auswählen.

13.5.6 Spectral Scan

Neben der Anbindung von Rechnern an das Internet nutzen professionelle Anwender das Wireless Local Area Network (WLAN) immer häufiger auch für geschäftsrelevante Prozesse. Als Beispiele seien hier der Zugriff auf Patientenakten, die Online-Überwachung einer Produktion oder die (idealerweise verzögerungsfreie) Übertragung von Video- und Audiodaten genannt. Die Zuverlässigkeit und die Leistungsfähigkeit eines WLAN-Systems nehmen daher kontinuierlich an Bedeutung zu.

Aufgrund der zunehmenden Nutzung und Bedeutung von WLAN für die Datenübertragung ergeben sich immer häufiger Situationen, in denen Geräte oder Systeme anderer Nutzer die WLAN-Frequenzbereiche zeitgleich nutzen. Dies können z. B. Mikrowellenherde, kabellose Telefone, Bluetooth-Geräte oder Video-Transmitter sein, wobei deren Signale sowohl kontinuierlich wie intermittierend auftreten können. Durch die zeitgleiche Nutzung eines Frequenzbandes bzw. Frequenzbereiches ergeben sich Interferenzen, die die Zuverlässigkeit und Leistungsfähigkeit eines WLANs stören oder beeinträchtigen können. Solche Störungen können zum Verlust von Datenpaketen oder zum Abbruch von Verbindungen führen. Ist die Überlagerung zu stark, kann es sogar zum vollständigen Ausfall des WLANs kommen.

Es ist daher zunehmend von Bedeutung, den aktuell verwendeten Frequenzbereich durch eine gezielte Analyse zu überprüfen. Dies dient einerseits dem Zweck, Interferenzen oder andere Störfaktoren zu erkennen und bei Bedarf Gegenmaßnahmen einzuleiten. Andererseits lässt sich so auch sicherstellen, dass das WLAN ordnungsgemäß und störungsfrei funktioniert.

Eine gezielte Analyse bietet die Möglichkeit, folgende Faktoren zu klären bzw. näher zu bestimmen:

- Ordnungsgemäßer und störungsfreier Betrieb des WLANs

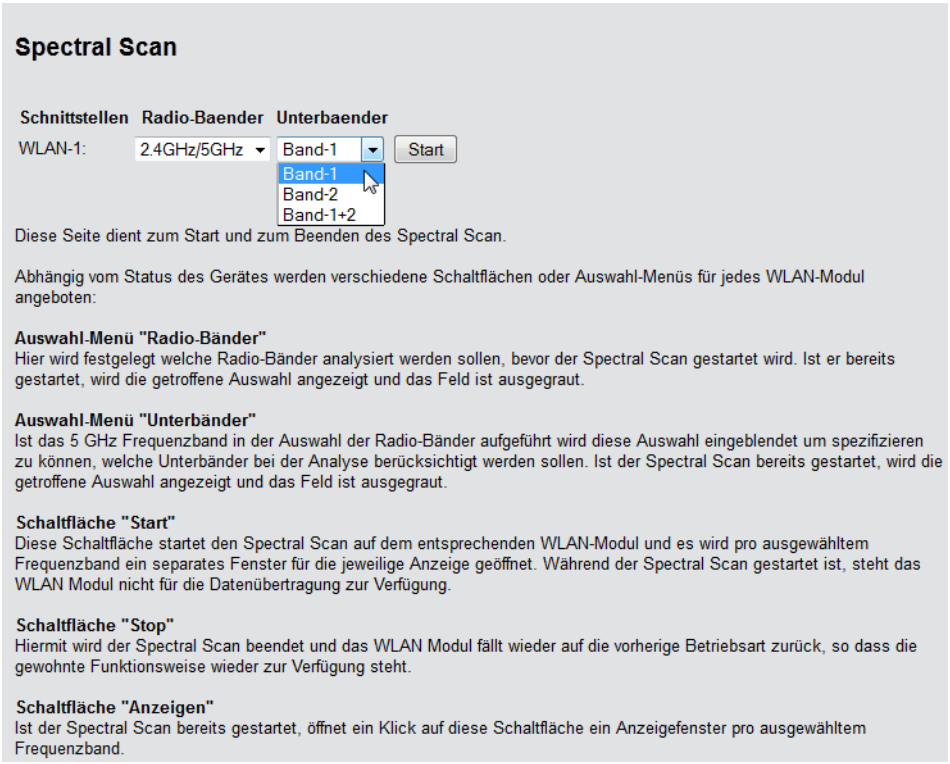
- Vorhandensein einer Interferenz bzw. eines Störsignals
- Anzeige oder Nennung der gestörten Bänder
- Stärke des Störsignals
- Regelmäßigkeit bzw. Häufigkeit des Störsignals
- Art und ggf. Herkunft des Störsignals

Die Untersuchung des für WLAN in Frage kommenden Frequenzbereiches findet auf der spektralen Ebene statt. Entsprechend hierzu werden die Ergebnisse grafisch wiedergeben, d. h. in Form von Echtzeit-Diagrammen oder Echtzeit-Übersichten, auf denen man Frequenzen und Störungen erkennen und ggf. ablesen kann. Hierbei ist zu bedenken, dass grafische Auswertungen eines spektralen Bereiches naturgemäß einen Interpretationsspielraum offen lassen und in manchen Fällen keine ganz eindeutigen Resultate ermöglichen. Ein Szenario wie das folgende wäre daher nicht ungewöhnlich: Sie stellen fest, dass Ihre aktuell verwendete Frequenz durch ein Signal gestört wird, das kontinuierlich auftritt und gleichbleibend stark ist. Sie können jedoch nicht eindeutig feststellen oder gar „ablesen", aus welchem Raum oder Gebäude das Signal kommt und welche Art von Gerät der Verursacher des Störsignals ist.

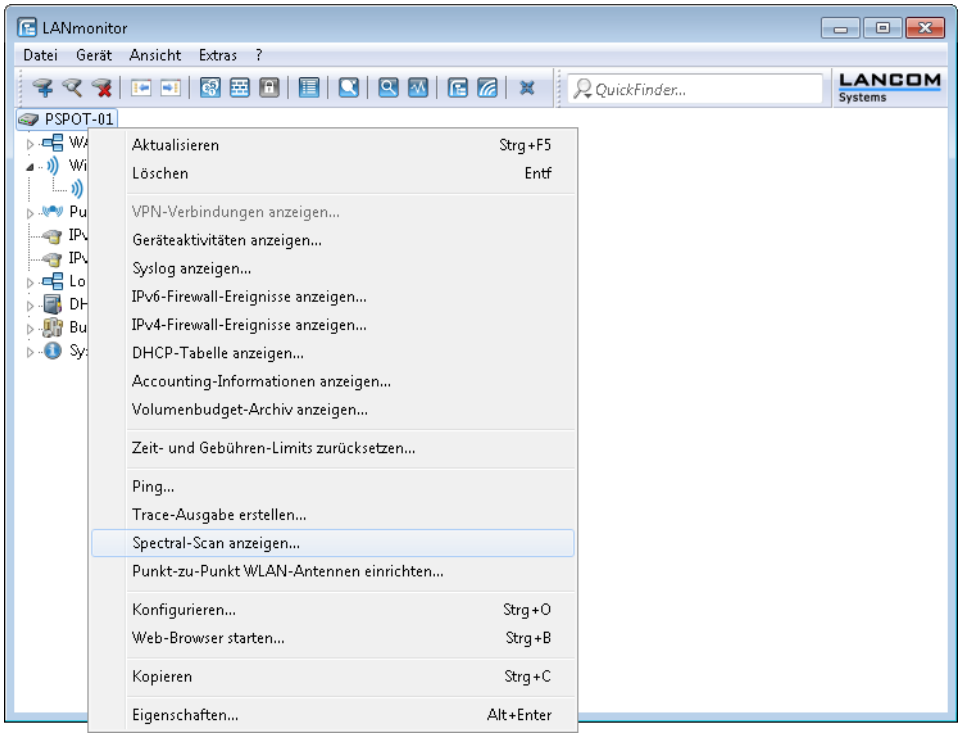
13.5.6.1 Funktionen des Software-Moduls

Das Software-Modul „Spectral Scan" bietet Ihnen die Möglichkeit, eine Spektralanalyse direkt am Access Point durchzuführen. Sie müssen sich also keine zusätzliche Soft- oder Hardware anschaffen, sondern können auf die integrierte Funktionalität zurückgreifen, um die in Frage kommenden Frequenzbereiche und -bänder zu untersuchen. Somit können Sie sich jederzeit einen grafischen Überblick über das Frequenzverhalten in Ihrem WLAN verschaffen, sei es nun zur Vorbeugung oder zur Aufdeckung von Störungen.

Ein Klick unter WEBconfig auf den Menüpunkt**Extras** > **Spectral Scan** öffnet den nachstehend abgebildeten Dialog:



Sie können den Spectral Scan auch aus dem LANmonitor heraus starten. Klicken Sie dazu das entsprechende Gerät in der Liste mit der rechten Maustaste an und wählen Sie im Kontextdialog den Punkt **Spectral Scan anzeigen**.



Wenn das WLAN-Modul deaktiviert ist (**Setup** > **Schnittstellen** > **WLAN** > **Betriebs-Einstellungen**), erscheint ein entsprechender Hinweis, und der Spectral Scan lässt sich nicht starten. Konfigurieren Sie den Access Point für die Betriebsart „Basisstation“ oder stellen Sie sicher, dass ein WLC den AP konfiguriert.

Hier stehen Ihnen folgende Einträge, Schaltflächen und Auswahl-Menüs zur Verfügung:

- **Schnittstellen**: Zeigt das ausgewählte, zu untersuchende WLAN-Modul an.
- **Radio-Baender**: Mit diesem Auswahl-Menü legen Sie fest, welches Frequenzband bzw. welche Frequenzbänder Sie untersuchen möchten. Wenn der Spectral Scan auf diesem Modul bereits gestartet ist, ist das betreffende Feld ausgegraut.
- **Unterbänder**: Dieses Auswahl-Menü ist nur aktiv, wenn Sie bei **Radio-Baender** entweder '5GHz' oder '2.4 GHz/5 Ghz' ausgewählt haben. Sie können dann festlegen, welche Unterbänder des 5GHz-Bandes bei der Analyse berücksichtigt werden sollen.
- **Start**: Ein Klick auf diese Schaltfläche startet die Analyse (den „Spectral Scan“) auf dem entsprechenden WLAN-Modul. Dabei öffnet sich ein separates Fenster pro ausgewähltem Frequenzband.
- **Stop**: Mit dieser Schaltfläche beenden Sie die Analyse. Das WLAN-Modul kehrt dann in die vorherige Betriebsart zurück und steht wieder mit der gewohnten Funktionalität zur Verfügung.

  Diese Schaltfläche erscheint erst nach dem Start des Moduls.

- **Anzeigen**: Sofern der Spectral Scan bereits gestartet ist, öffnen Sie mit einem Klick auf diese Schaltfläche ein Anzeigefenster pro ausgewähltem Frequenzband. Durch mehrfaches Betätigen der Schaltfläche können Sie mehrere Fenster öffnen.

Während des Analysevorgangs überträgt das untersuchte WLAN-Modul keine Daten und sendet keine SSID.

Weitere Informationen über die angezeigten Diagramme entnehmen Sie dem Abschnitt *Analyse-Fenster Spectral Scan*.

13.5.6.2 Analyse-Fenster Spectral Scan

Die Anzeige des Spectral Scans erfolgt in einer Browser-Anwendung. Damit sie ordnungsgemäß funktioniert, muss Ihr Browser Websockets in der aktuellen Version und das HTML5-Element `<canvas>` unterstützen. Der in LANmonitor integrierte Browser erfüllt alle Anforderungen.

Im separaten Analyse-Fenster des Spectral Scan haben Sie unterschiedliche Möglichkeiten, die jeweiligen Frequenzen bzw. Frequenzbereiche nebst möglichen Störungen darzustellen. Hierfür stehen Ihnen am oberen Rand des Fensters die folgenden Schaltflächen zur Verfügung:

- **Current**: Zeigt oder verbirgt die Kurve der aktuell gemessenen Werte.
- **Maximum**: Zeigt oder verbirgt die Maximalwerte des laufenden Spektrum-Scans, bezogen auf den aktuell eingestellten History-Bereich.
- **Average**: Zeigt oder verbirgt die Durchschnittswerte des laufenden Spektrum-Scan, bezogen auf den aktuell eingestellten History-Bereich.
- **History**: Zeigt oder verbirgt die zuletzt gemessenen Werte.
- **Number of history values**: Bestimmt die Anzahl der angezeigten, zuletzt gemessenen Ergebnisse. Sie können sich mindestens die letzten 5 und maximal die letzten 50 Messpunkte je Frequenz anzeigen lassen.
- **Last Channel**: Zeigt oder verbirgt den zuletzt benutzten Kanal.
- **Frequency**: Wechselt die Anzeige auf der x-Achse zwischen WLAN-Kanal und Frequenz.

Das Fenster enthält zwei grafische Darstellungen, die Ihnen die Messergebnisse unterschiedlich präsentieren. Das obere Diagramm zeigt auf der y-Achse die Signalstärke in dBm, auf der x-Achse entweder den jeweiligen WLAN-Kanal oder die entsprechende Frequenz. Das untere Diagramm enthält den zeitlichen Verlauf der Analyse in Form eines Wasserfall-Diagramms, wobei die y-Achse die Zeit darstellt, während die x-Achse wieder den jeweiligen WLAN-Kanal oder die entsprechende Frequenz zeigt. Diese Formen der Darstellung können sowohl andauernde als auch zeitlich variierende Störungen in den Frequenzen anschaulich machen, so dass Sie entsprechende Maßnahmen zur Verbesserung der Verbindung durchführen können (z. B. Wechsel des Kanals oder Identifizierung und Beseitigung der Störquelle). So weisen z. B. bestimmte Störquellen wie Mikrowellen-Geräte, DECT-Telefone (die im 2,4 GHz Frequenzbereich arbeiten) oder Audio-Video-Transmitter ganz typische Sendemuster auf, die in beiden Diagrammen deutlich hervortreten.

Am unteren Rand des Fensters sehen Sie einen mit **Time Slider** bezeichneten Schieberegler. Mit diesem können Sie für das Wasserfall-Diagramm den zu analysierenden Zeitraum der betreffenden Frequenz erweitern oder begrenzen. Alternativ können Sie über das Eingabefeld rechts neben dem Schieberegler auswählen, wie viele Messergebnisse Sie sich im Wasserfall-Diagramm anzeigen lassen möchten. Die Web-Applikation kann über den Time-Slider bis zu 300 Messwerte im Wasserfall-Diagramm zur Anzeige bringen, wobei sie insgesamt die Messwerte von maximal 24 Stunden zwischenspeichern kann.

Nachstehend sehen Sie einige exemplarische Analyse-Ergebnisse, die jeweils andere Einstellungen auf unterschiedliche Weise grafisch aufbereiten:

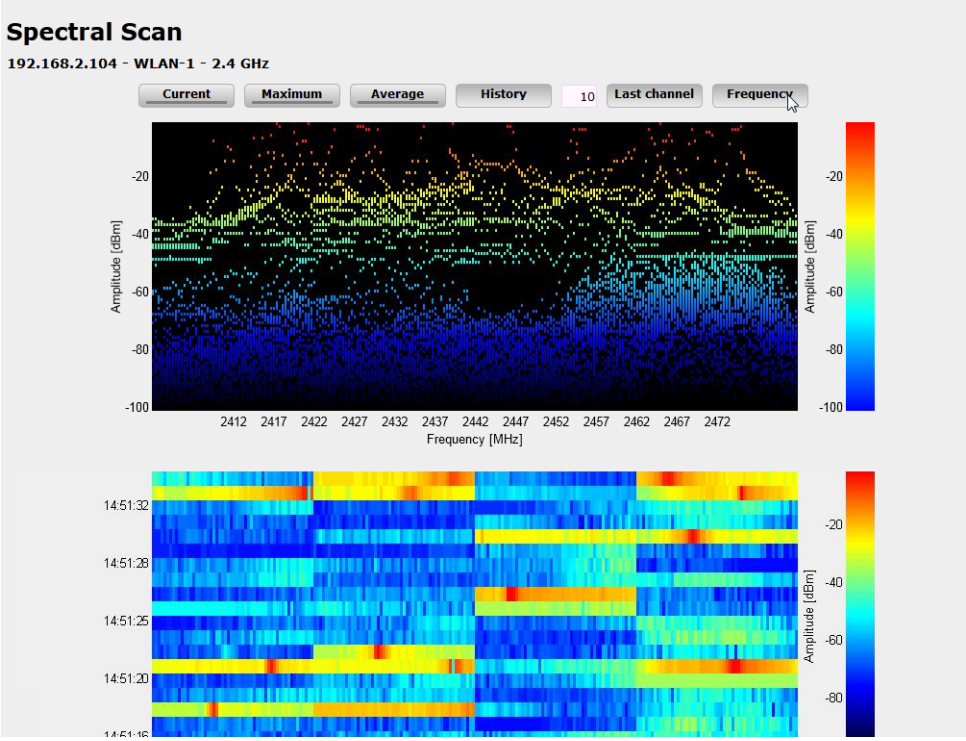


Abbildung 16: Spectral Scan, Frequenz-Anzeige der letzten 10 History-Werte

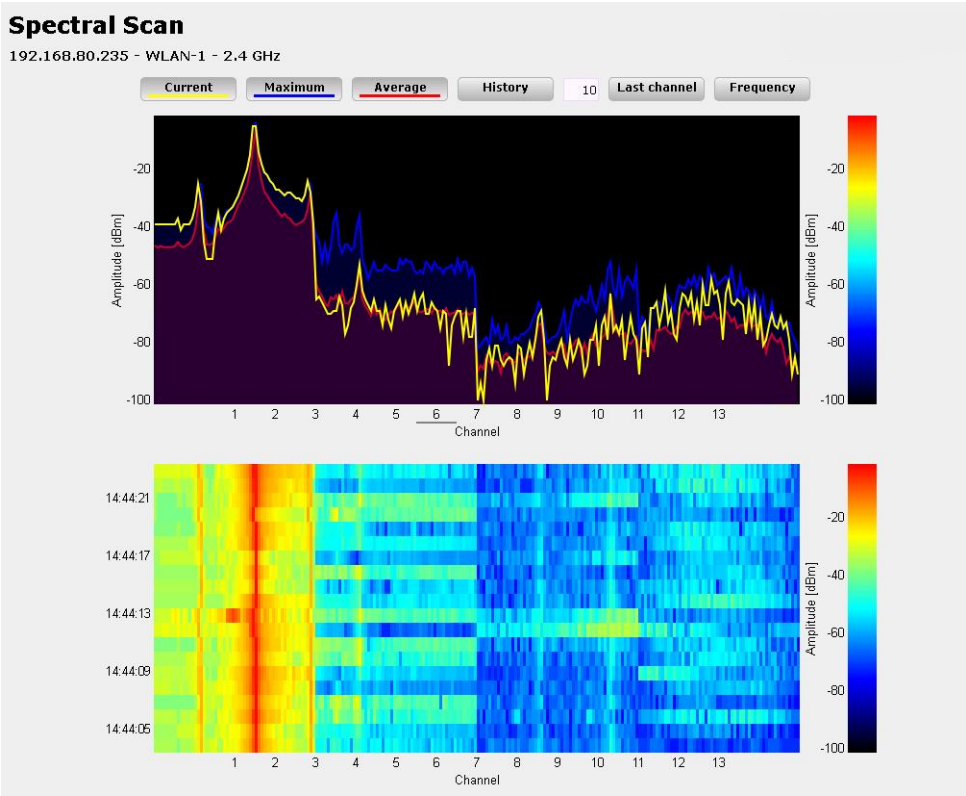


Abbildung 17: Spectral Scan, Kanal-Anzeige Current, Maximum, Average, Störung durch Funk-Kamera

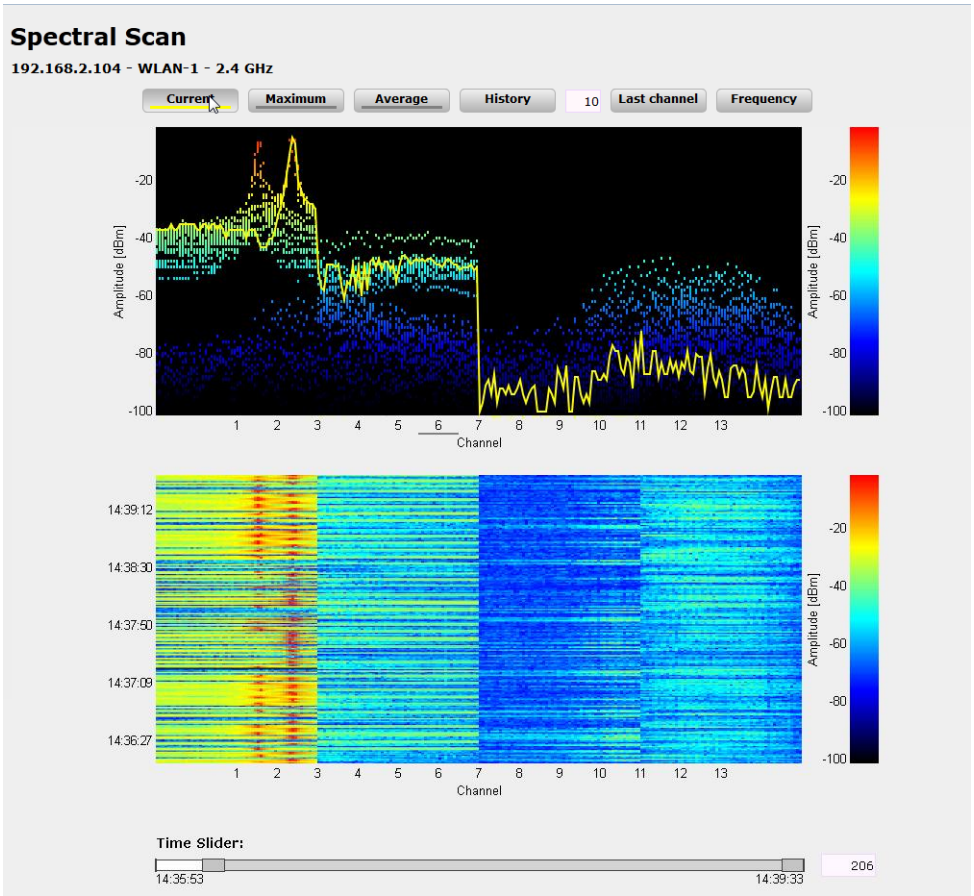


Abbildung 18: Spectral Scan, Kanal-Anzeige Current, letzte 10 History-Werte und „Time Slider", Störung durch Baby-Phone

13.6 Dynamic Frequency Selection (DFS)

Beim für 5-GHz-WLANs geforderten DFS-Verfahren (Dynamic Frequency Selection) wählt das Gerät automatisch eine freie Frequenz, um z. B. Radaranlagen nicht zu stören. Die Signale von Wetter-Radarstationen waren jedoch manchmal nicht sicher zu erkennen.

Die europäische Kommission forderte daher in Ergänzung zu den Standards ETSI EN 301 893 V1.3.1 und ETSI EN 301 893 V1.4.1, im Unterband 2 des 5-GHz-Bandes drei Kanäle (120, 124 und 128) auszusparen und solange nicht für die automatische Kanalwahl zu verwenden, bis Verfahren zur Erkennung der Wetter-Radar-Signaturen zur Verfügung stehen. Man bezeichnete die Version EN 301 893 V1.3 und EN 301 893 V1.4 kurz als „DFS-2".

Mitte 2010 trat die neue Version ETSI EN 301 893 V1.5.1 in Kraft, die einige Veränderungen für die Nutzung von WLAN-Frequenzen in den Bereichen 5,25 - 5,35 GHz und 5,47 - 5,725 GHz mit sich brachte. Die neue Version 1.5.1 regelte das DFS-Verfahren für diese Frequenzbereiche, um Radarstationen vor dem Einfluss durch WLAN-Systeme zu schützen. Bei der Erkennung von bestimmten Mustern in den empfangenen Funksignalen können seitdem WLAN-Systeme mit Hilfe von DFS die Radarstationen erkennen und einen automatischen Wechsel der verwendeten Kanäle durchführen. Im Unterschied zu den bisherigen Regelungen bezeichnete man die aktualisierte DFS-Version nach EN 301 893-V1.5 kurz als „DFS-3".

Generell bestimmen die Werte Pulsrate, Pulsbreite und Anzahl der Pulse ein Pulsmuster. Die bisherigen DFS-Verfahren gaben vor, nur feste Radarmuster zu prüfen, die durch definierte Kombinationen verschiedener Pulsraten und Pulsbreiten im WLAN-Gerät hinterlegt waren. Nach DFS-3 konnte das Gerät nun auch Muster aus wechselnden Pulsraten und

Pulsbreiten als Radarmuster erkennen. Außerdem konnten innerhalb eines Radarsignals zwei oder drei unterschiedliche Pulsraten verwendet werden.

Am 01.01.2013 endete die Gültigkeit der Version ETSI EN 301 893 V1.5.1 (DFS-3). Danach galt die neue Version ETSI EN 301 893 V1.6.1 (kurz „DFS-4"), die auch kürzere Radarimpulse erkennt.

Am 31.12.2014 endete die Gültigkeit der Version ETSI EN 301 893 V1.6.1 (DFS-4). Danach gilt die neue Version ETSI EN 301 893 V1.7.1 (kurz „DFS-5"), die einige Änderungen bzgl. der Signalstärke mit sich brachte. Seitdem gab es mehrere weitere Revisionen dieses Standards.

Für die Erkennung von Wetterradaren (Kanäle 120, 124 und 128 im Frequenzbereich 5,6 - 5,65 MHz) gelten besondere Nutzungsbedingungen. Die DFS-Implementierung im LCOS unterstützt die verschärften Erkennungsbedingungen nicht. Deshalb werden diese drei Kanäle von neueren LCOS-Versionen ausgespart.

Arbeitsweise

Nach dem Einschalten oder Booten wählt das Gerät aus den (z. B. aufgrund der Ländereinstellungen) verfügbaren Kanälen einen zufälligen Kanal aus und prüft, ob es auf diesem Kanal ein Radarsignal findet und ob auf diesem Kanal schon ein anderes WLAN arbeitet. Diesen Scan-Vorgang wiederholt es solange, bis es einen radarfreien Kanal mit möglichst wenig anderen Netzwerken findet. Anschließend wird der gewählte Kanal erneut für 60 Sekunden beobachtet, um evtl. auftretende Radarsignale sicher auszuschließen. Die Datenübertragung kann daher durch diesen Scan-Vorgang und die erneute Suche eines freien Kanals für 60 Sekunden unterbrochen werden.

Um diese Pausen in der Datenübertragung bei jedem Kanalwechsel zu verhindern, verlegt ein Gerät den Scanvorgang **vor** die Auswahl eines konkreten Kanals. Die Informationen über die gescannten Kanäle werden in einer internen Datenbank gespeichert:

- Wurde auf dem Kanal ein Radarsignal gefunden?
- Wieviele andere Netzwerke wurden auf dem Kanal gefunden?

Mit Hilfe dieser Datenbank wählt der AP einen Kanal aus einer Liste der radarfreien Kanäle mit der geringsten Anzahl an anderen Netzwerken aus (das ist der Betriebskanal). Nach der Auswahl eines Kanals kann die Datenübertragung dann sofort ohne weitere Wartezeit beginnen.

- Die „Blacklist" dieser Datenbank speichert die Kanäle, die aufgrund der gefundenen Radarsignale geblockt werden. Diese Einträge verschwinden nach jeweils 30 Minuten aus der Liste, um die Informationen ständig auf dem aktuellen Stand zu halten.
- Die „Whitelist" der Datenbank speichert die Kanäle, auf denen kein Radarsignal gefunden wurde. Diese Einträge bleiben für die nächsten 24 Stunden gültig, können aber zwischenzeitlich beim Auftreten eines Radarsignals durch einen Eintrag in der Blacklist überschrieben werden.

Standardmäßig nutzt der AP dauerhaft den Kanal, der beim ersten Scan als Betriebskanal gewählt wurde. Die Verbindungen können beliebig lange auf dem vom DFS-Algorithmus gewählten Kanal bestehen bleiben, bis entweder ein Radarsignal erkannt wird oder die Funkzelle neu gestartet wird (z. B. bedingt durch Umkonfigurieren des Geräts, Firmware-Upload oder einen Neustart).

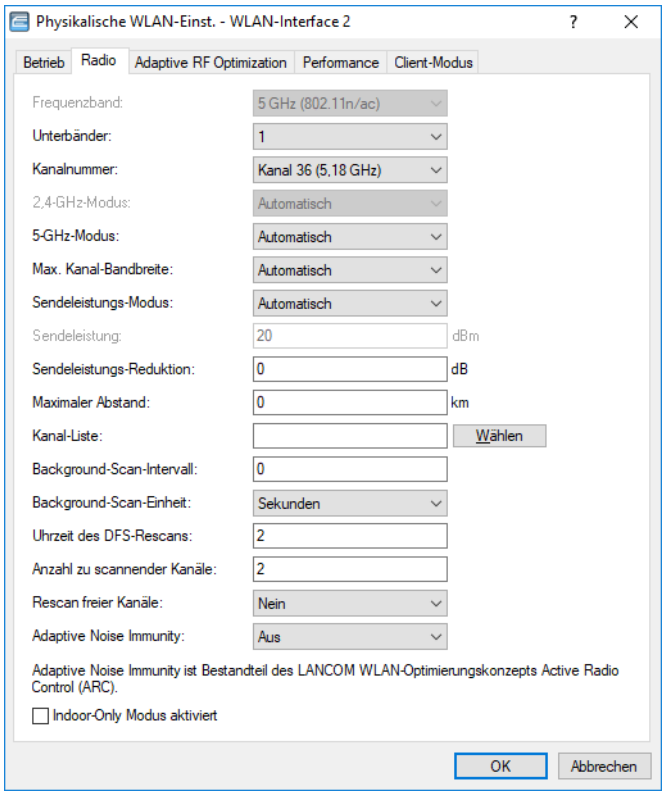
Ein erneuter 60-Sekunden-Scanvorgang ist unter den folgenden Voraussetzungen notwendig:

- Das Gerät wird eingeschaltet oder kalt gestartet. In diesem Fall ist die Datenbank leer, das Gerät kann nicht aus der Whitelist die bevorzugten Kanäle auswählen. Es ist ein Scanvorgang erforderlich.
- Innerhalb der ersten 24 Stunden nach dem Scanvorgang wird ein Kanalwechsel notwendig durch ein Radarsignal in der Reichweite des APs. In diesem Fall verfügt der AP über Alternativen in der Whitelist – er kann also den eingebuchten WLAN-Clients bzw. den P2P-Partnern den neuen Betriebskanal mitteilen und dann auf diesen Kanal wechseln. Die Dauer für diesen Vorgang liegt im Sekundenbereich, der Wechsel kann als unterbrechungsfrei angesehen werden.
- Das Gerät ist seit 24 Stunden in Betrieb, erst dann wird ein neuer Kanalscan notwendig. Die Einträge in der Whitelist sind aus der Datenbank „herausgealtert", der AP hat keinen alternativen Kanal, den er direkt als Betriebskanal nutzen könnte. In diesem Fall muss die Datenbank durch einen Scanvorgang neu gefüllt werden, es kommt zu einer einminütigen Unterbrechung des WLAN-Betriebs.

Grundsätzlich ist der Betreiber des WLANs zuständig für die Einhaltung der ETSI-Regelungen. LANCOM empfiehlt daher den zeitnahen Umstieg auf eine Firmware-Version mit aktueller DFS-Unterstützung.

13.6.1 DFS-Konfiguration

In LANconfig konfigurieren Sie die DFS-Einstellungen unter **Wireless-LAN** > **Allgemein** durch einen Klick auf **Physikalische WLAN-Einst.** und Auswahl des Reiters **Radio**.



Uhrzeit des DFS-Rescans

Dieser Eintrag bestimmt, um welche Uhrzeit (0-24 Uhr) das Gerät die DFS-Datenbank löscht und einen DFS-Rescan durchführt. Ohne Eintrag führt das Gerät erst dann einen DFS-Rescan durch, wenn kein freier Kanal mehr verfügbar ist. Das ist dann der Fall, wenn die beim initialen DFS-Scan ermittelte Kanalzahl die minimale Anzahl der freien Kanäle unterschreitet.

Für die Definition der Uhrzeit lassen sich Möglichkeiten der cron-Befehle nutzen: Der Eintrag '1,6,13' startet den Rescan immer um 1 Uhr, 6 Uhr und 13 Uhr. Der Eintrag '0-23/4' startet alle vier Stunden einen Rescan in der Zeit zwischen 0 und 23 Uhr.

Anzahl zu scannender Kanäle

Dieser Eintrag bestimmt die minimale Anzahl an freien Kanälen, die ein DFS-Scan erreichen muss. Der Standardwert '2' bedeutet, dass das Gerät solange einen DFS-Scan durchführt, bis es 2 freie Kanäle erkennt. Im Falle eines nötigen Kanalwechsels, z. B. auf Grund eines aktivierten Radarmusters, steht der zweite Kanal sofort für einen Wechsel zur Verfügung.

Der Wert '0' deaktiviert die Beschränkung. Die physikalische WLAN-Schnittstelle führt einen DFS-Scan auf sämtlichen zur Verfügung stehenden Kanälen aus.

Rescan freier Kanäle

Diese Auswahl bestimmt, ob die physikalische WLAN-Schnittstelle nach einem abgeschlossenen DFS-Rescan die als besetzt erkannten Kanäle löscht oder für weitere DFS-Rescans zwischenspeichert.

Ja

Die physikalische WLAN-Schnittstelle löscht nach einem abgeschlossenen DFS-Rescan die als besetzt erkannten Kanäle, damit diese bei einem erneuten DFS-Rescan wieder zur Verfügung stehen.

Nein

Das Gerät speichert nach einem abgeschlossenen DFS-Rescan die als besetzt erkannten Kanäle, so dass das Gerät diese Kanäle bei einem erneuten DFS-Rescan sofort überspringt (Default).

Sie können eine Bevorzugung bestimmter Kanäle vornehmen. LCOS versucht als erstes, ob ein in **Kanalnummer** eingestellter Kanal verwendet werden kann, danach probiert es die in der **Kanal-Liste** aufgeführten Kanäle durch. Sollten alle diese Kanäle durch Radarerkennung nicht verfügbar sein, dann werden die für das eingestellte Land möglichen Kanäle versucht.

Nach Ablauf der DFS-Sperrzeit wird versucht, wieder auf den eingestellten Kanal zurückzuwechseln. Ist dieser Kanal weiterhin nicht verfügbar, wird ein ggf. in der Kanalliste konfigurierter Kanal verwendet. Die DFS-Sperrzeit tritt in Kraft, sobald ein Kanal wegen Radarerkennung gesperrt wurde und sie beträgt in der Regel 30 Minuten.

Diese Bevorzugung hilft dabei, feste Kanalschemata in 5 GHz nutzen zu können, da nach DFS-Events schneller wieder die volle Kapazität des Netzwerkes genutzt werden kann.

Ist kein dedizierter Kanal für das WLAN-Modul konfiguriert (Kanalliste leer und Radio-Kanal „0" bzw. „Automatisch"), dann wird nach einem durch Radarerkennung ausgelösten Kanalwechsel der neue Kanal beibehalten und nicht auf den zuletzt verwendeten Kanal zurückgewechselt.

13.7 APSD – Automatic Power Save Delivery

13.7.1 Einleitung

Beim Automatic Power Save Delivery (APSD) handelt es sich um eine Erweiterung des Standards IEEE 802.11e. APSD wird in zwei Varianten angeboten:

- Unscheduled APSD (U-APSD)
- Scheduled APSD (S-APSD)

Die beiden Verfahren unterscheiden sich u. a. in der Nutzung der Übertragungskanäle. LANCOM APs und Wireless Router unterstützen U-APSD, auf dem auch das von der WiFi als WMM Power Save oder kurz WMMPS zertifizierte Verfahren basiert.

U-APSD ermöglicht für WLAN-Geräte eine deutliche Stromeinsparung. Ein besonders großer Bedarf für diese Funktion entsteht durch die immer stärkere Nutzung von WLAN-fähigen Telefonen (Voice over WLAN – VoWLAN).

Mit der Aktivierung des U-APSD für ein WLAN können die WLAN-Geräte im Gesprächsbetrieb in einen „Schlummer-Modus" wechseln, während sie auf das nächste Datenpaket warten. Die VoIP-Datenübertragung erfolgt in einem festen zeitlichen Raster – die WLAN-Geräte synchronisieren ihre aktiven Phasen mit diesem Zyklus, so dass sie rechtzeitig vor dem Empfang des nächsten Pakets wieder bereit sind. Der Stromverbrauch wird dadurch deutlich reduziert, die Gesprächszeit der Akkus wird merklich erhöht.

Das genaue Verhalten des Stromsparmodus wird zwischen AP und WLAN-Client ausgehandelt und wird dabei auf die spezifische Anwendung hin optimiert. APSD ist damit deutlich flexibler als das zuvor verwendete Stromsparverfahren, das in diesem Zusammenhang als „Legacy Power Save" bezeichnet wird.

13.7.2 Konfiguration

Konsole: **Setup** > **Schnittstellen** > **WLAN** > **Netzwerk**

APSD

Aktiviert den Stromsparmodus APSD für dieses logische WLAN-Netzwerk.

Mögliche Werte:

- Ein, Aus

Default:

- Aus



Bitte beachten Sie, dass zur Nutzung der Funktion APSD in einem logischen WLAN auf dem Gerät das QoS aktiviert sein muss. Die Mechanismen des QoS werden bei APSD verwendet, um den Strombedarf der Anwendungen zu optimieren.

13.7.3 Statistik

Konsole: **Status** > **WLAN** > **Netzwerke**

APSD

Zeigt an, ob APSD im jeweiligen WLAN (SSID) aktiv ist. APSD wird hier nur als aktiv angezeigt, wenn sowohl APSD in den Einstellungen des logischen WLANs als auch das globale QoS-Modul aktiviert sind.

Konsole: **Status** > **WLAN**

Stationstabelle

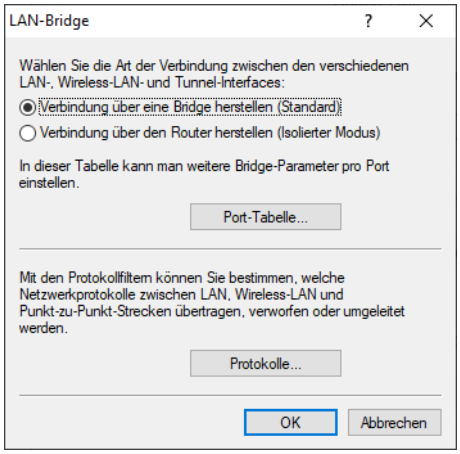
Zeigt in einer Bitmaske an, für welche Zugriffskategorien der eingebuchte WLAN-Client APSD nutzt:

- Voice (höchste Priorität)
- Video
- Best effort (einschließlich Datenverkehr von „Legacy Power Save"-Clients)
- Background (geringste Priorität).

13.8 WLAN-Routing (Isolierter Modus)

In der Standardeinstellung wird der Datenverkehr zwischen LAN und WLAN „gebrückt", also Layer-2-transparent übertragen. Dabei verläuft der Datenverkehr zwischen dem drahtgebundenen und den drahtlosen Netzwerken **nicht** über den IP-Router. Damit stehen auch die im IP-Router integrierten Funktionen Firewall und Quality-of-Service nicht für den Datenverkehr zwischen WLAN und LAN zur Verfügung. Um diese Möglichkeiten dennoch zu nutzen, werden die WLAN-Schnittstellen in den „isolierten Modus" versetzt, der Datenverkehr wird gezielt über den IP-Router geleitet.

Damit der IP-Router Daten zwischen LAN und WLAN richtig übertragen kann, müssen die beiden Bereiche über unterschiedliche IP-Adresskreise verfügen. Weitere Informationen finden Sie im Bereich Advanced Routing and Forwarding (ARF).



LANconfig: **Schnittstellen** > **LAN** > **LAN-Bridge**

Konsole: **Setup** > **LAN-Bridge** > **Isolierter-Modus**

13.9 Übernahme der User-Priorität von IEEE 802.11e in VLAN-Tags

IEEE 802.11e ist ein Standard zur Erweiterung der WLAN-Standards um Quality-of-Service-Funktionen (QoS). Wenn ein AP diesen Standard nutzt, kann das Gerät den angebundenen WLAN-Clients eine bestimmte Priorität zuweisen (User-Priorität). Mit der Priorisierung der WLAN-Datenpakete kann der AP u. a. die Daten von Voice-over-IP-Clients bevorzugt übertragen. Auf der LAN-Seite sind die APs in vielen Fällen mit einem Switch verbunden, verschiedene LAN-Segmente sind oft durch VLANs getrennt. Das kabelgebundene LAN nutzt andere Mechanismen zur Priorisierung der Datenpakete.

Das folgende Anwendungsbeispiel verdeutlicht die Situation:

- Ein WLAN-Client (z. B. VoIP-Telefon) ist an einen AP angebunden, QoS ist auf dem WLAN aktiviert, die Daten zwischen Telefon und AP sind nicht VLAN-getaggt.
- Der AP ist auf der Ethernet-Seite mit einem VLAN-fähigen Switch verbunden, die Daten zwischen AP und Switch sind VLAN-getaggt.

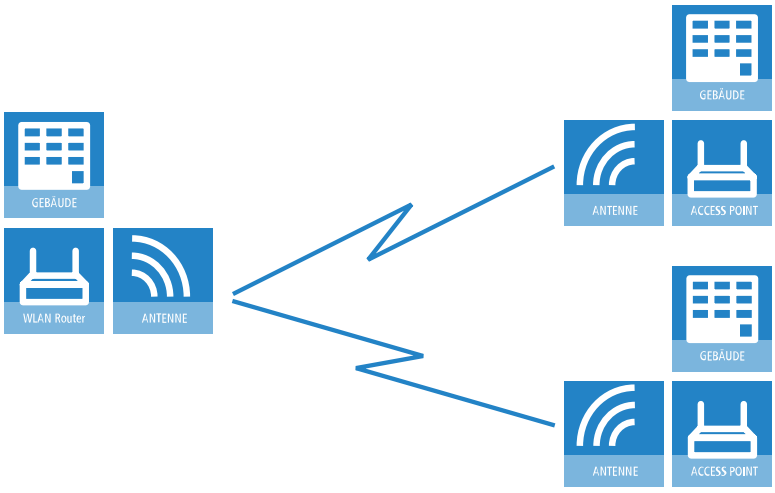
Der AP als Schnittstelle zwischen kabelgebundenem LAN und drahtlosem WLAN setzt die unterschiedlichen Priorisierungsinformationen entsprechend um:

- Bei der Übertragung von Daten vom AP zum WLAN-Client (Senderichtung aus Sicht des APs) ermittelt das Gerät die Priorität eines empfangenen Paketes entweder aus dem VLAN-Tag oder aus dem ToS/DSCP-Feld des IP-Headers. Mit dieser Priorität sendet der AP die Pakete an den Client.
- Bei der Übertragung von Daten vom WLAN-Client zum AP (Empfangsrichtung aus Sicht des APs) enthält das Datenpaket jedoch kein VLAN-Tag. In dieser Richtung untersucht der AP außerdem nicht den IP-Header. Stattdessen entnimmt der AP die User-Priorität aus dem WLAN-Paket und setzt diese entsprechend in das VLAN-Tag der ausgehenden Datenpakete in Richtung Switch ein.

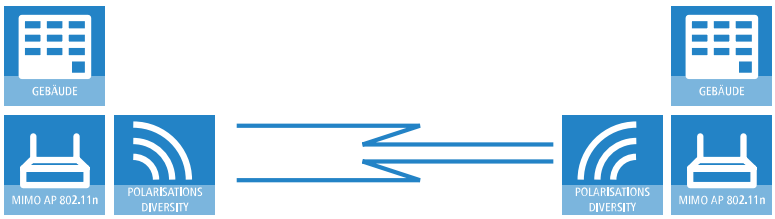
13.10 Aufbau von Punkt-zu-Punkt-Verbindungen

13.10.1 Konfiguration der Punkt-zu-Punkt-Verbindungen

LANCOM APs können nicht nur als zentrale Station in einem Funknetzwerk arbeiten, sie können im Punkt-zu-Punkt-Betrieb auch Funkstrecken über größere Distanzen bilden. So können z. B. zwei Netzwerke über mehrere Kilometer hinweg sicher verbunden werden – ohne direkte Verkabelungen oder teure Standleitungen.



Bei der Verwendung von APs und entsprechend polarisierten Antennen nach IEEE 802.11n können gleichzeitig zwei Funkbeziehungen zwischen den Endpunkten einer P2P-Verbindung aufgebaut werden. Damit können deutliche höhere Datenraten erzielt oder größere Entfernungen überwunden werden als beim Einsatz der anderen Standards.

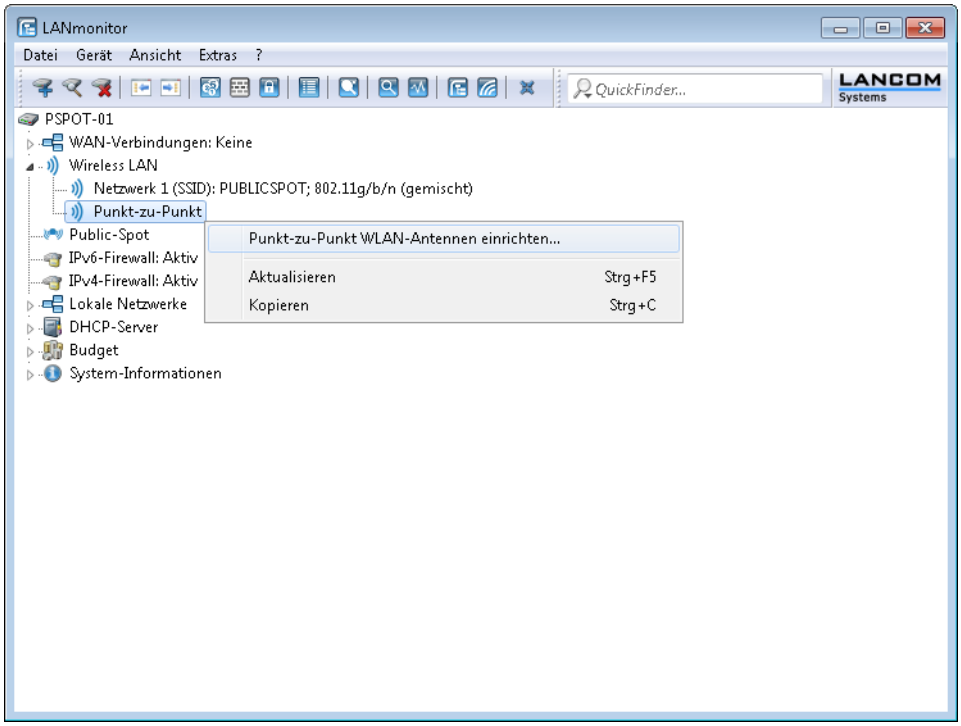


Dieser Abschnitt stellt die Grundlagen zur Auslegung von Point-to-Point-Strecken vor und gibt Hinweise zur Ausrichtung der Antennen.

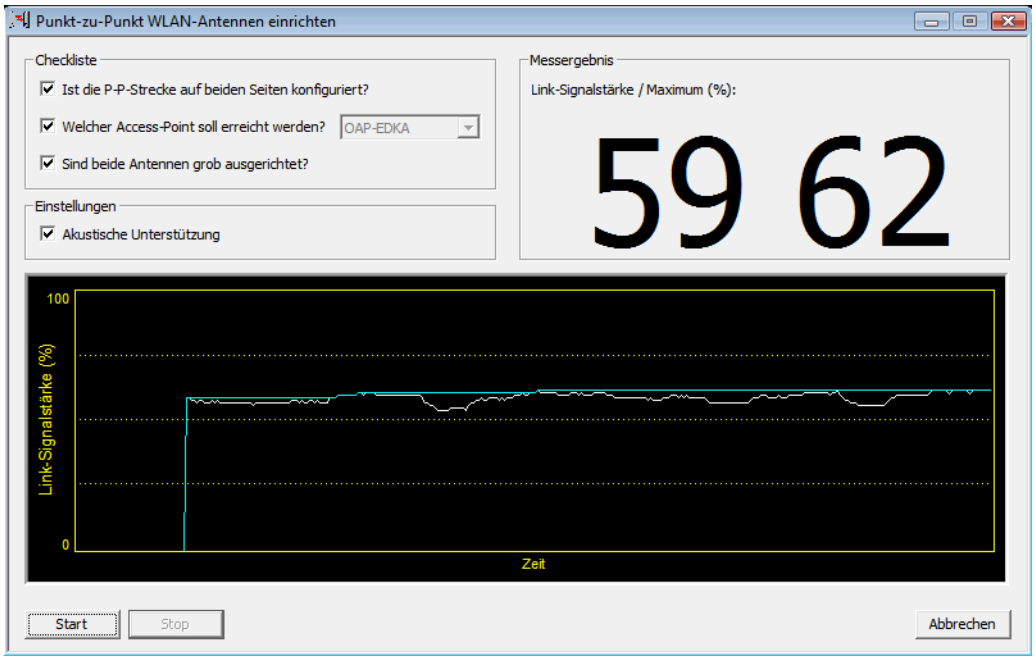
13.10.2 Einrichten von Punkt-zu-Punkt-Verbindungen mit dem LANmonitor

Um die Antennen für Punkt-zu-Punkt-Verbindungen möglichst gut ausrichten zu können, kann die aktuelle Signalqualität von P2P-Verbindungen über die LEDs des Gerätes oder im LANmonitor angezeigt werden. Der LANmonitor bietet dabei neben der optischen Anzeige der Link-Signalstärke auch eine akustische Unterstützung.

Im LANmonitor kann die Anzeige der Verbindungsqualität über das Kontext-Menü geöffnet werden. Ein Klick mit der rechten Maustaste auf den Eintrag 'Punkt-zu-Punkt' erlaubt den Aufruf **Punkt-zu-Punkt WLAN-Antennen einrichten**.



Der P2P-Dialog zeigt nach dem Start der Signalüberwachung jeweils die absoluten Werte für die aktuelle Signalstärke sowie den Maximalwert seit dem Start der Messung. Zusätzlich wird der zeitliche Verlauf mit dem Maximalwert in einem Diagramm angezeigt.



Bewegen Sie zunächst nur eine der beiden Antennen, bis sie den Maximalwert erreicht haben. Stellen Sie dann die erste Antenne fest und bewegen Sie auch die zweite Antenne in die Position, bei der Sie die höchste Signalqualität erzielen.

Zur genaueren Ausrichtung kann eine akustische Unterstützung aktiviert werden. Mit dieser Option wird abhängig von der aktuellen Link-Signalstärke ein Ton über den PC ausgegeben. Die maximale Link-Signalstärke wird mit einem Dauerton

signalisiert. Fällt die Link-Signalstärke unter das Maximum, wird der Abstand zum bisher erreichten Maximum durch Tonintervalle angezeigt. Je kürzer die Intervalle, um so näher liegt die Link-Signalstärke am Maximum.

13.10.3 Geometrische Auslegung von Outdoor-Funknetz-Strecken

Bei der Auslegung der Funkstrecken sind im Wesentlichen folgende Fragen zu beantworten:

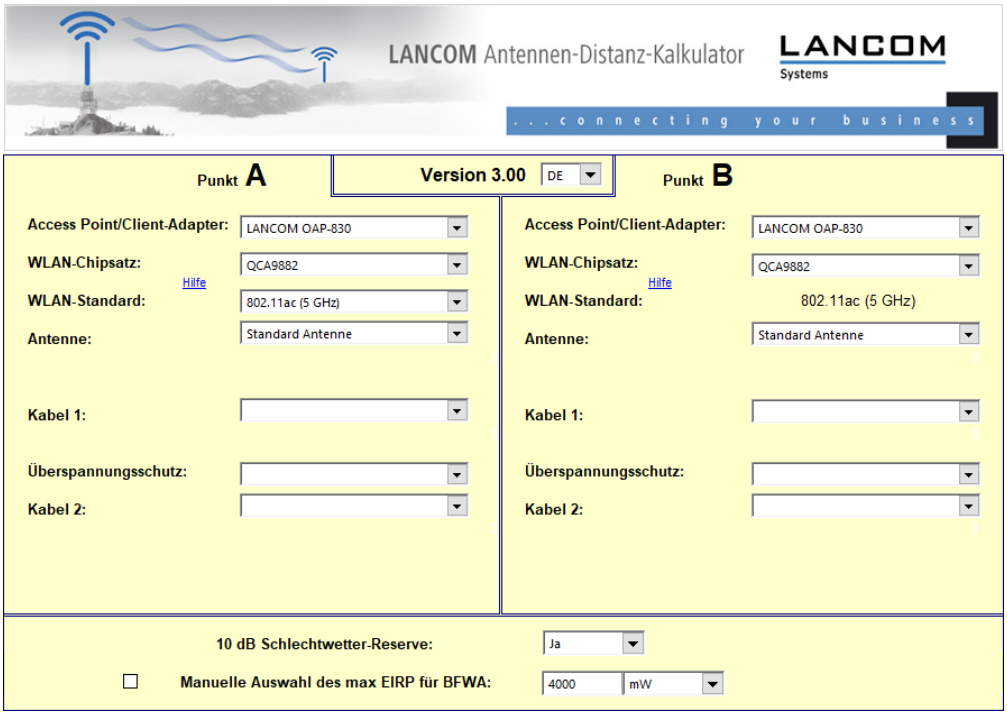
- Welche Antennen müssen für die gewünschte Anwendung eingesetzt werden?
- Wie müssen die Antennen positioniert werden, um eine einwandfreie Verbindung herzustellen?
- Welche Leistungen müssen die eingesetzten Antennen aufweisen, um einen ausreichenden Datendurchsatz innerhalb der gesetzlichen Grenzen zu gewährleisten?

13.10.3.1 Auswahl der Antennen mit dem LANCOM Antennen-Distanz-Kalkulator

Zur Berechnung der Ausgangsleistungen in den APs und für eine erste Abschätzung der erreichbaren Distanzen und Datenraten können Sie den *LANCOM Antennen-Distanz-Kalkulator* verwenden.

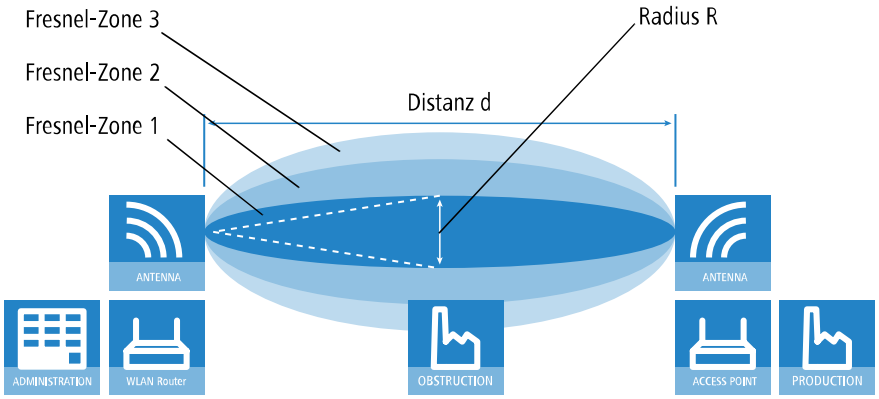
Nach Auswahl der verwendeten Komponenten (APs, Antennen, Blitzschutz und Kabel) berechnet der Kalkulator neben Datenraten und Distanzen auch den Antennen-Gewinn, der in den APs eingestellt werden muss.

Bitte beachten Sie, dass bei der Verwendung von 5 GHz-Antennen je nach Einsatzland zusätzliche Techniken wie die dynamische Frequenzwahl (Dynamic Frequency Selection – DFS) vorgeschrieben sein können. Der Betreiber der WLAN-Anlage ist für die Einhaltung der jeweils geltenden Vorschriften verantwortlich.



13.10.3.2 Positionierung der Antennen

Die Antennen strahlen ihre Leistung nicht linear, sondern in einem modellabhängigen Winkel ab. Durch die kugelförmige Ausbreitung der Wellen kommt es in bestimmten Abständen von der direkten Verbindung zwischen Sender und Empfänger zur Verstärkung oder zu Auslöschungen der effektiven Leistung. Die Bereiche, in denen sich die Wellen verstärken oder auslöschen, werden als Fresnel-Zonen bezeichnet.



Um die von der Antenne abgestrahlte Leistung möglichst vollständig auf die empfangende Antenne abzubilden, muss die Fresnel-Zone 1 frei bleiben. Jedes störende Element, das in diese Zone hineinragt, beeinträchtigt die effektiv übertragene Leistung deutlich. Dabei schirmt das Objekt nicht nur einen Teil der Fresnel-Zone ab, sondern führt durch Reflexionen zusätzlich zu einer deutlichen Reduzierung der empfangenen Strahlung.

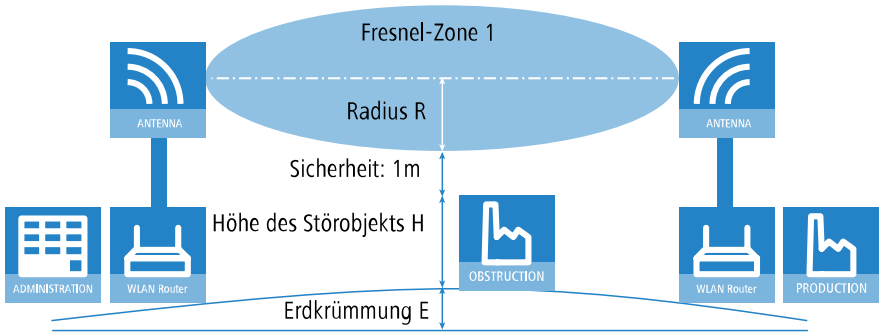
Der Radius (R) der Fresnel-Zone 1 berechnet sich bei gegebener Wellenlänge der Strahlung ( ) und der Distanz zwischen Sender und Empfänger (d) nach folgender Formel:

R = 0,5 * √ (* d)

Die Wellenlänge beträgt im 2,4-GHz-Band ca. 0,125 m, im 5-GHz-Band ca. 0,05 m.

Beispiel: Bei einer Distanz zwischen den beiden Antennen von 4 km ergibt sich im 2,4-GHz-Band der Radius der Fresnel-Zone 1 zu **11 m**, im 5-GHz-Band nur zu **7 m**.

Damit die Fresnel-Zone 1 frei und ungestört ist, müssen die Antennen das höchste Störobjekt um diesen Radius überragen. Die gesamte erforderliche Masthöhe (M) der Antennen ergibt sich nach folgendem Bild zu:



M = R + 1m + H + E (Erdkrümmung)

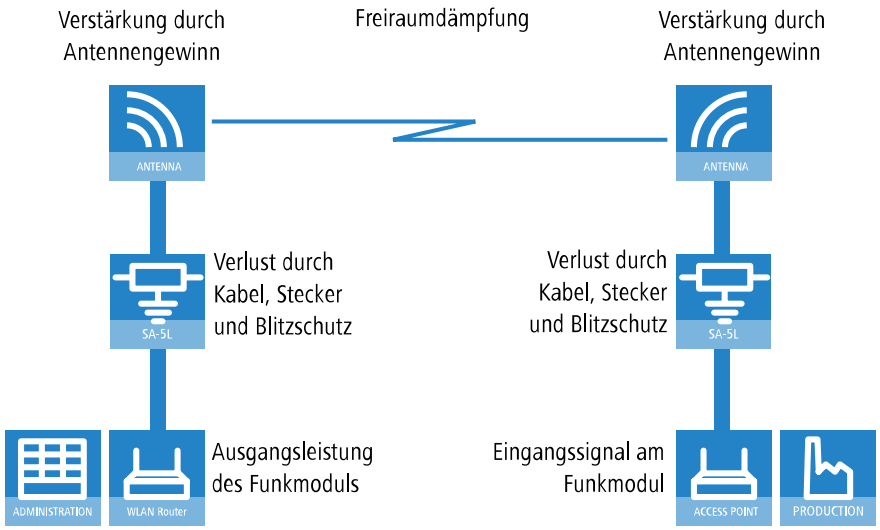
Die Höhe der Erdkrümmung (E) ergibt sich bei einer Distanz (d) zu E = d² * 0,0147 – bei einer Distanz von 8 km also immerhin schon fast 1 m!

Beispiel: Bei einer Distanz zwischen den beiden Antennen von 8 km ergibt sich im 2,4-GHz-Band die Masthöhe über dem höchsten Störobjekt von ca. **13 m**, im 5-GHz-Band zu **9 m**.

13.10.3.3 Antennen-Leistungen

Die Leistungen der eingesetzten Antennen müssen so ausgelegt sein, dass eine ausreichende Datenübertragungsrate erreicht wird. Auf der anderen Seite dürfen die länderspezifischen gesetzlichen Vorgaben für die maximal abgestrahlten Leistungen nicht überschritten werden.

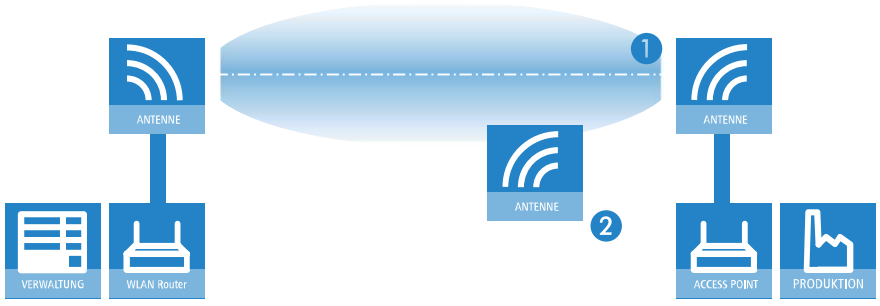
Die Berechnung der effektiven Leistungen führt dabei vom Funkmodul im sendenden AP bis zum Funkmodul im empfangenden AP. Dazwischen liegen dämpfende Elemente wie die Kabel, Steckverbindungen oder einfach die übertragende Luft und verstärkende Elemente wie die externen Antennen.



13.10.4 Ausrichten der Antennen für den P2P-Betrieb

Der Schutz der verwendeten Komponenten vor den Folgen von Blitzeinschlag oder anderen elektrostatischen Vorgängen ist einer der wichtigsten Aspekte bei der Auslegung und Installation von WLAN-Systemen im Outdoor-Einsatz. Bitte beachten Sie die entsprechenden Hinweise zum „Blitz- und Überspannungsschutz“, da LANCOM ansonsten keine Garantie für Schäden an den Komponenten übernehmen kann. Informationen zur Installation von WLAN-Systemen im Outdoor-Einsatz finden Sie im 'LANCOM Outdoor Wireless Guide'.

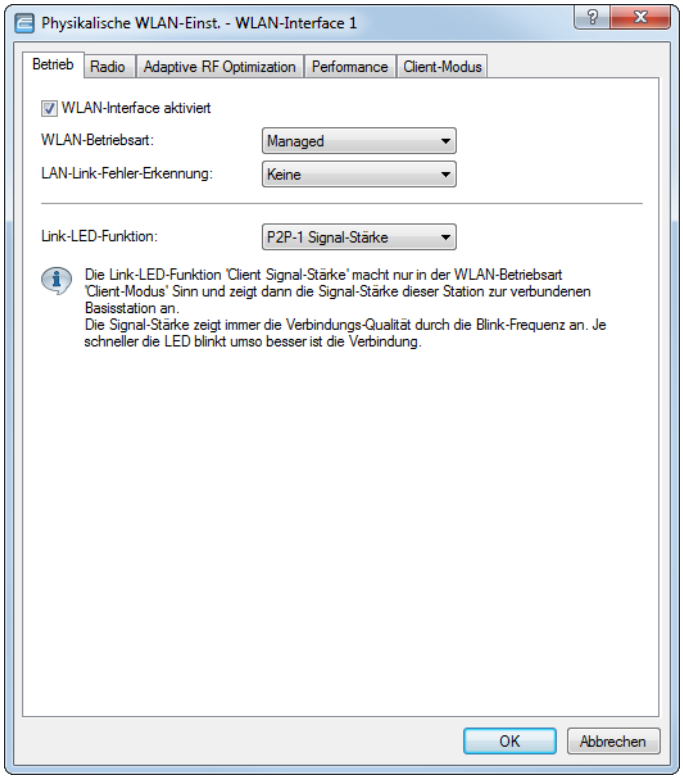
Beim Aufbau von P2P-Strecken kommt der genauen Ausrichtung der Antennen eine große Bedeutung zu. Je besser die empfangende Antenne in der „Ideallinie“ der sendenden Antenne liegt, desto besser ist die tatsächliche Leistung und damit die nutzbare Bandbreite **1**. Liegt die empfangende Antenne jedoch deutlich neben dem idealen Bereich, sind erhebliche Leistungsverluste zu erwarten **2**.



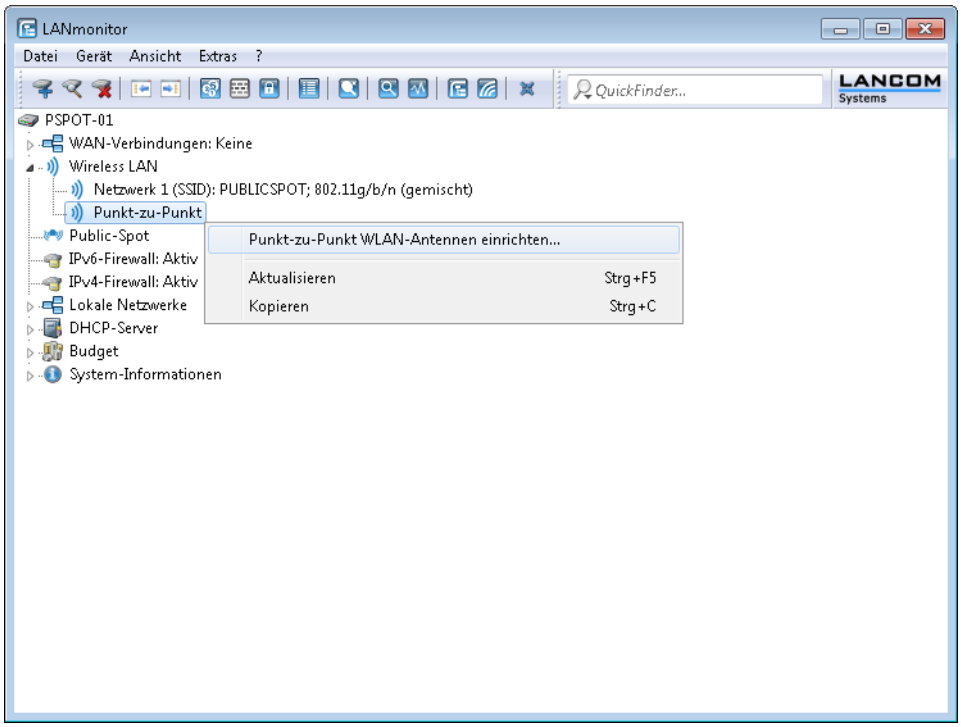
Um die Antennen möglichst gut ausrichten zu können, kann die aktuelle Signalqualität von P2P-Verbindungen über die LEDs des Gerätes oder im LANmonitor angezeigt werden.

Die Anzeige der Signalqualität über die LEDs muss für die physikalische WLAN-Schnittstelle aktiviert werden (LANconfig: **Wireless LAN** > **Allgemein** > **Physikalische WLAN-Einstellungen** > **Betrieb**). Je schneller die LED blinkt, umso besser

ist die Verbindung (eine Blinkfrequenz von 1 Hz steht für eine Signalqualität von 10 dB, eine Verdoppelung der Frequenz zeigt die jeweils doppelte Signalstärke).



Im LANmonitor kann die Anzeige der Verbindungsqualität über das Kontext-Menü geöffnet werden. Ein Klick mit der rechten Maustaste auf den Eintrag **Punkt-zu-Punkt** erlaubt den Aufruf **Punkt-zu-Punkt WLAN-Antennen einrichten**

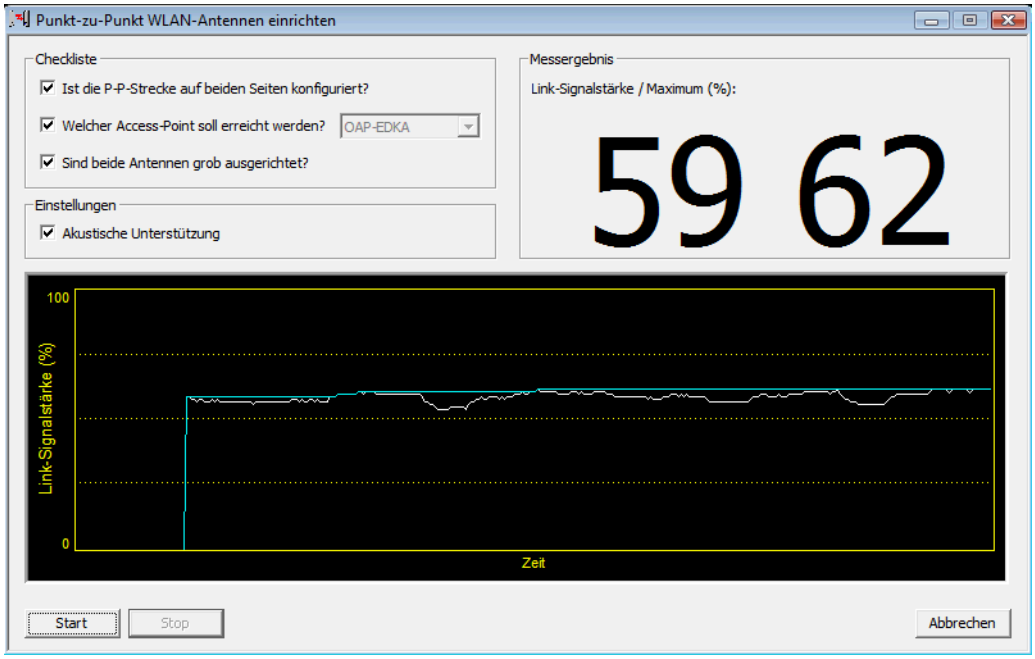


Der Eintrag **Punkt-zu-Punkt** ist im LANmonitor nur sichtbar, wenn in dem überwachten Gerät mindestens eine Basisstation als Gegenstelle für eine P2P-Verbindung eingerichtet ist (LANconfig: **Wireless LAN** > **Allgemein** > **Gemeinsame Punkt-zu-Punkt-Einst.** > **Betrieb**).

Im Dialog zur Einrichtung der Punkt-zu-Punkt-Verbindung fragt der LANmonitor die Voraussetzungen für den P2P-Verbindungsaufbau ab:

- Ist die P2P-Strecke auf beiden Seiten konfiguriert (gegenüberliegende Basisstation mit MAC-Adresse oder Stations-Namen definiert)?
- Ist die Punkt-zu-Punkt-Betriebsart aktiviert?
- Welcher AP soll überwacht werden? Hier können alle im jeweiligen Gerät als P2P-Gegenstelle eingetragenen Basis-Stationen ausgewählt werden.
- Sind beide Antennen grob ausgerichtet? Die Verbindung über die P2P-Strecke sollte schon grundsätzlich funktionieren, bevor die Einrichtung mit Hilfe des LANmonitors gestartet wird.

Der P2P-Dialog zeigt nach dem Start der Signalüberwachung jeweils die absoluten Werte für die aktuelle Signalstärke sowie den Maximalwert seit dem Start der Messung. Zusätzlich wird der zeitliche Verlauf mit dem Maximalwert in einem Diagramm angezeigt.



Bewegen Sie zunächst nur eine der beiden Antennen, bis Sie den Maximalwert erreicht haben. Stellen Sie dann die erste Antenne fest und bewegen Sie auch die zweite Antenne in die Position, bei der Sie die höchste Signalqualität erzielen.

13.10.5 Vermessung von Funkstrecken

Nach der Planung und Einrichtung kann die Funkstrecke vermessen werden, um den tatsächlichen Datendurchsatz zu bestimmen.

Weitere Informationen zu den verwendeten Tools und zum Mess-Aufbau finden Sie im *LANCOM Outdoor Wireless Guide* als Download unter *www.lancom-systems.de*.

13.10.6 Punkt-zu-Punkt-Betriebsart aktivieren

Das Verhalten eines APs beim Datenaustausch mit anderen APs wird in LANconfig unter **Wireless LAN** > **Allgemein** > **Gemeinsame Punkt-zu-Punkt-Einst.** > **Betrieb**in der **Punkt-zu-Punkt-Betriebsart** festgelegt:

Aus

Der AP kann nur mit mobilen Clients kommunizieren.

An

Der AP kann mit anderen Basis-Stationen und mit mobilen Clients kommunizieren.

Exklusiv

Der AP kann nur mit anderen Basis-Stationen kommunizieren.

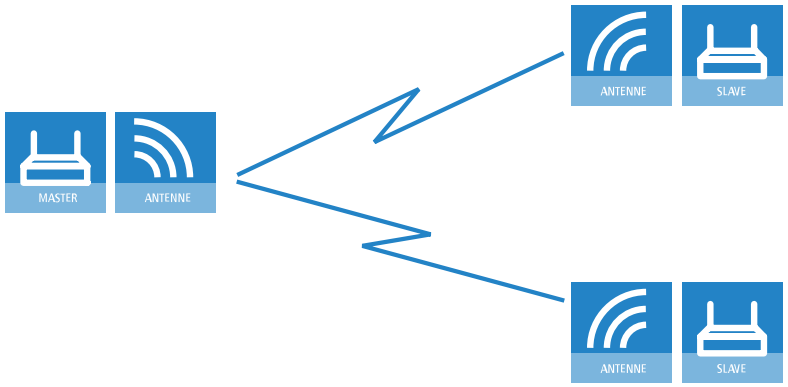
Bei der automatischen Suche nach einem freien WLAN-Kanal kann es im 5-GHz-Band zu gleichzeitigen Sendeversuchen mehrerer APs kommen, die sich in der Folge gegenseitig nicht finden. Diese Pattsituation kann mit dem geeigneten **Kanalwahlverfahren** verhindert werden:

Master

Dieser AP übernimmt die Führung bei der Auswahl eines freien WLAN-Kanals.

Slave

Alle anderen APs suchen solange nach dem freien Kanal, bis sie einen sendenden Master gefunden haben.



Es ist daher empfehlenswert, im 5-GHz-Band jeweils einen zentralen AP als 'Master' und alle anderen Punkt-zu-Punkt-Partner als 'Slave' zu konfigurieren. Auch im 2,4-GHz-Band bei aktivierter automatischer Kanalsuche erleichtert diese Einstellung den Aufbau von Punkt-zu-Punkt-Verbindungen.

Für die Verschlüsselung von Punkt-zu-Punkt-Verbindungen mit 802.11i / WPA ist die korrekte Konfiguration der Kanalwahlverfahren zwingend erforderlich (ein Master als Authentication Server und ein Slave als Client).

Die automatische Kanalwahl für P2P-Verbindungen im 5i GHz-Bereich ist nur aktiv, wenn das ausgewählte Länderprofil DFS unterstützt.

13.10.7 Konfiguration von P2P-Verbindungen

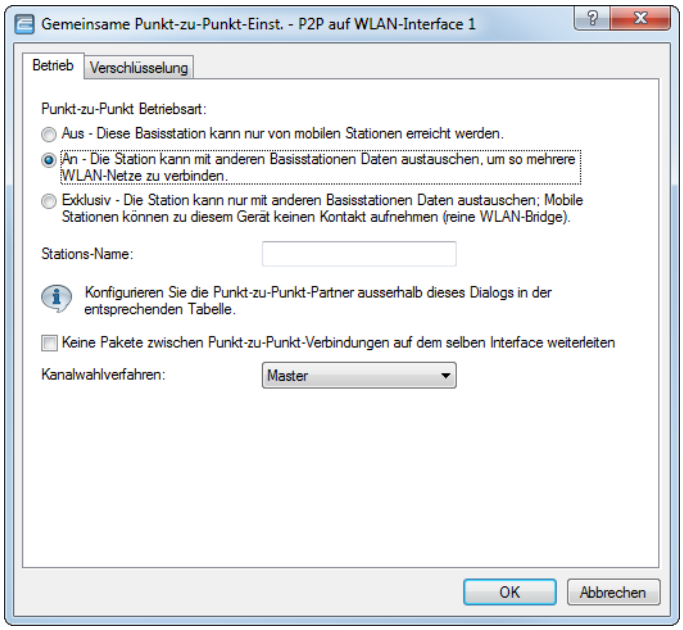
Bei der Konfiguration von Punkt-zu-Punkt-Verbindungen (P2P-Verbindungen) geben Sie neben der Punkt-zu-Punkt-Betriebsart und dem Kanalwahlverfahren wahlweise die MAC-Adressen oder die Stationsnamen der Gegenstellen an. Die Konfiguration kann in LANconfig entweder über den Setup-Assistenten **WLAN konfigurieren** oder manuell über den Konfigurationsdialog erfolgen.

Die nachfolgenden Schritte zeigen Ihnen, wie Sie manuell eine verschlüsselte oder unverschlüsselte P2P-Basis-Konfiguration erstellen.

Parallel zu einer P2P-Verbindung spannen die betreffenden APs automatisch je eine fixe SSID ***** P2P INFO ***** auf. Diese SSID dient als reines Verwaltungsnetz für den Verbindungaufbau und die Erreichbarkeitsprüfung

('Alive') eines Punkt-zu-Punkt-Partners. Den WLAN-Clients ist es nicht möglich, sich mit solch einem Netz zu verbinden.

1. Öffnen Sie den Konfigurationsdialog für das Gerät, das als P2P-Master bzw. P2P-Slave agieren soll, und wechseln Sie auf die Seite **Wireless LAN** > **Allgemein** > **Gemeinsame Punkt-zu-Punkt-Einst.**.
2. Wählen Sie das WLAN-Interface aus, welches Sie ausschließlich für die P2P-Verbindung benutzen wollen.

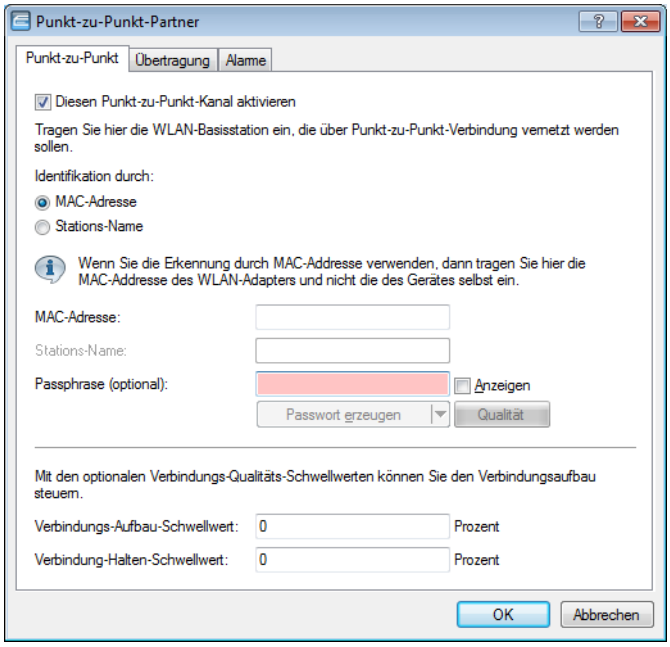


3. Aktivieren Sie die gewünschte **Punkt-zu-Punkt Betriebsart**, z. B. **An**.
4. Setzen Sie das **Kanalwahlverfahren** auf **Master** bzw. **Slave**.
5. Optional: Sofern die Gegenstelle die physikalische Schnittstelle nicht über die MAC-Adresse, sondern einen Alias-Namen identifizieren soll, geben Sie im Eingabefeld **Stations-Name** eine entsprechende Bezeichnung ein, z. B. `P2P_MASTER` bzw. `P2P_SLAVE`.
6. Optional: Passen Sie auf der Registerkarte **Verschlüsselung** bei Bedarf die Einstellungen für die IEEE 802.11i-Verschlüsselung der P2P-Verbindung an.

   Mit IEEE 802.11i lässt sich die Sicherheit von Punkt-zu-Punkt-Verbindungen im WLAN deutlich verbessern. Alle Vorteile von 802.11i wie die einfache Konfiguration und die starke Verschlüsselung mit AES stehen damit im P2P-Betrieb ebenso zur Verfügung wie die verbesserte Sicherheit der Passphrases durch LANCOM Enhanced Passphrase Security MAC (LEPS-MAC).

   Die Einstellungsmöglichkeiten sind weitgehend identisch mit denen der Verschlüsselung bei logischen WLAN-Interfaces, siehe *Einstellungen für die Verschlüsselung* auf Seite 1034. Standardmäßig ist die P2P-Verschlüsselung aktiviert und mit sinnvollen Werten vorbelegt.

7. Schließen Sie den Dialog mit **OK** und wählen Sie im Konfigurationdialog auf der gleichen Seite unter **Punkt-zu-Punkt-Partner** eine logische P2P-Verbindung aus, z. B. **P2P-1-1**.



8. Aktivieren Sie auf der Registerkarte **Punkt-zu-Punkt** den gewählten P2P-Kanal und geben Sie an, ob Ihr Gerät die Gegenstelle über eine **MAC-Adresse** oder einen **Stations-Namen** identifiziert. Je nach Auswahl tragen Sie anschließend im gleichnamigen Eingabefeld entweder die MAC-Adresse des physikalischen WLAN-Interfaces, das die Gegenstelle für die P2P-Verbindung benutzt, oder deren Stations-Namen ein.
   Sie finden die WLAN-MAC-Adresse auf einem Aufkleber, der unterhalb des jeweiligen Antennenanschlusses am Gehäuse des Gerätes angebracht ist. Verwenden Sie nur die als "WLAN-MAC" oder "MAC-ID" gekennzeichnete Zeichenkette. Bei den anderen ggf. angegebenen Adressen handelt es sich nicht um die WLAN-MAC-Adresse, sondern um die LAN-MAC-Adresse!

   Alternativ finden Sie die MAC-Adresse auch im Status-Menü unter **WLAN** > **Interfaces** > **MAC-Adresse**.

9. Geben Sie unter **Passphrase** ein gemeinsames Kennwort aus mindestens 8 Zeichen an (empfohlen: 32 Zeichen), mit dem Sie die P2P-Verbindung zusätzlich verschlüsseln. Die P2P-Verschlüsselung muss dafür aktiviert sein (siehe oben). In der Einstellung als P2P-Master wird die hier eingetragene Passphrase verwendet, um die Zugangsberechtigung der Slaves zu prüfen. In der Einstellung als P2P-Slave überträgt der AP diese Informationen an die Gegenseite, um sich dort anzumelden.
10. Optional: Wechsel Sie auf die Registerkarte **Übertragung**, um die Grenzwerte und Einstellung für die Paketübertragung vorzunehmen.

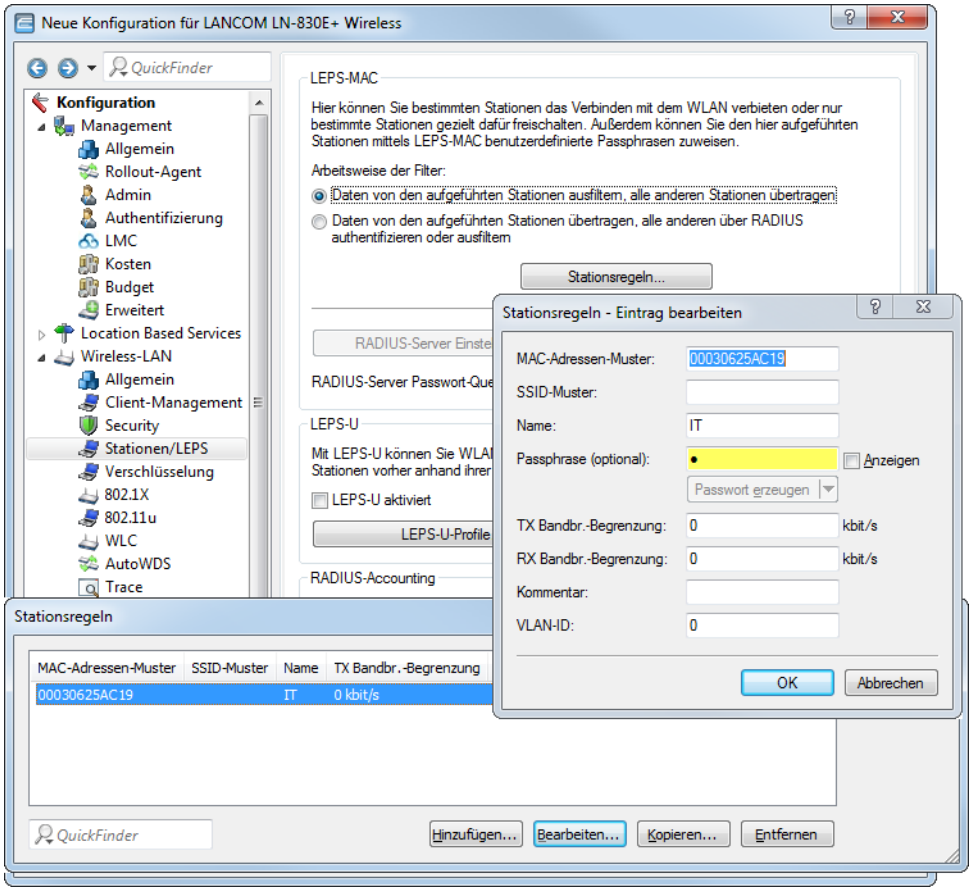
    Die Einstellungsmöglichkeiten sind weitgehend identisch mit denen der logischen WLAN-Netze, siehe *Einstellungen für die Alarme* auf Seite 1044. Standardmäßig sind sämtliche Parameter auf Optimierung und Automatik ausgerichtet.
11. Schließen Sie den Dialog mit **OK** und schreiben Sie die Konfiguration zurück auf das Gerät.
12. Nehmen Sie die äquivalenten Konfigurationsschritte für die Gegenstelle (Slave bzw. Master) vor.

13.10.8 LEPS-MAC für P2P-Verbindungen

Einen weiteren Sicherheitsgewinn erzielen Sie durch die zusätzliche Verwendung der LANCOM Enhanced Passphrase Security MAC (LEPS-MAC), also der Verknüpfung der MAC-Adresse mit der Passphrase.

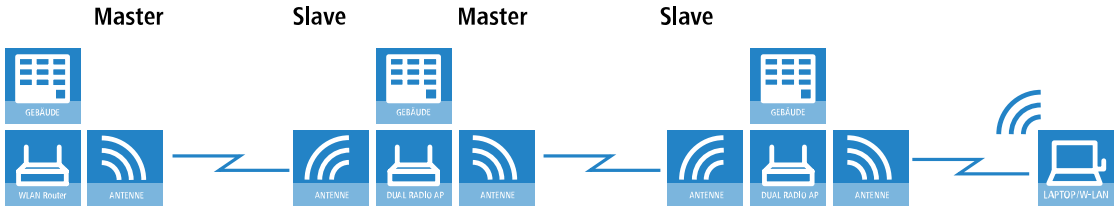
Mit LEPS-MAC können einzelne Punkt-zu-Punkt-Strecken (P2P) mit einer individuellen Passphrase abgesichert werden. Wenn bei einer P2P-Installation ein AP entwendet wird und dadurch Passphrase und MAC-Adresse bekannt werden, sind alle anderen per LEPS-MAC abgesicherten WLAN-Strecken weiterhin sicher.

Bei der Konfiguration mit LANconfig geben Sie die Passphrases der im WLAN zugelassenen Stationen (MAC-Adressen) im Konfigurationsbereich 'Wireless-LAN' auf der Registerkarte 'Stationen' unter der Schaltfläche **Stationen** ein.



13.10.9 Access Points im Relais-Betrieb

APs mit zwei Funkmodulen können Funkbrücken über mehrere Stationen hinweg aufbauen. Dabei wird jeweils ein WLAN-Modul als 'Master', das zweite als 'Slave' konfiguriert.



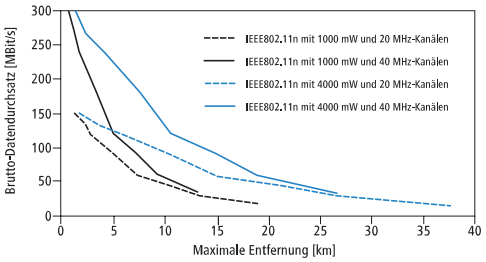
Mit dem Einsatz von Relais-Stationen mit jeweils zwei WLAN-Modulen wird gleichzeitig das Problem der „hidden station“ reduziert.

13.11 BFWA – mehr Sendeleistung für mehr Reichweite

BFWA steht für breitbandige, ortsfeste Funkstrecken, mit denen beispielsweise von einem Netzknoten ausgehend Verbindungen mit dem Internet für die angeschlossenen Teilnehmer zur Verfügung gestellt werden können. Die Frequenzen

wurden im Rahmen einer Allgemeinzuteilung von der Bundesnetzagentur bereitgestellt. BFWA funkt im 5,8 GHz-Bereich. Die maximal zulässige Sendeleistung beim Betrieb von BFWA-Funkstrecken liegt bei 4000 mW EIRP (Equivalent Isotropic Radiated Power).

In dieser hohen zulässigen Sendeleistung liegt der Vorteil von BFWA. Denn ohne BFWA ist die zulässige maximale Sendeleistung für Outdoor WLAN-Richtfunksysteme im 5-GHz-Band auf 1000 mW beschränkt. Durch die Vervierfachung der zulässigen Strahlungsleistung können mit denselben Richtfunksystemen deutlich größere Distanzen überbrückt werden.



LANCOM APs auf Basis von 802.11n sowie alle aktuellen LANCOM APs unterstützen BFWA. Bei älteren APs ist die Unterstützung abhängig vom Chipsatz (AR-5414 Chipsatz). Der LANCOM Support informiert Sie bei diesen Modellen über eine mögliche Unterstützung von BFWA.

Weitere Informationen entnehmen Sie bitte dem Techpaper "Broadband Fixed Wireless Access (BFWA)", erhältlich als Download von *www.lancom-systems.de*.

13.12 Adaptive Transmission Power

Die dynamische Sendeleistungsanpassung ist gerade für professionelle Backup-Szenarien in WLAN-Umgebungen unverzichtbar. Fällt ein AP aus, erhöhen die verbleibenden APs automatisch ihre Sendeleistung, sodass eine vollständige WLAN-Abdeckung zu jeder Zeit sichergestellt ist.

Geben Sie dazu an, wie viele APs sich innerhalb einer Broadcast-Domäne befinden. Solange alle Geräte erreichbar sind, gilt für alle innerhalb dieser Gruppe befindlichen APs eine konfigurierbare Sendeleistungsreduktion (z. B. -6 dB). Dabei überprüfen die APs über das IAPP (Inter Access Point Protocol) ständig die korrekte Anzahl der APs im Netzwerk.

Fällt nun ein AP aus, ergibt die Überprüfung, dass die Anzahl der tatsächlich vorhandenen APs nicht der Anzahl der erwarteten APs entspricht, und die übrigen APs aktivieren die konfigurierte Rückfall-Sendeleistungs-Reduktion (z. B. 0 dB). Sobald der ausgefallene AP wieder erreichbar ist entspricht bei der Überprüfung die tatsächliche Anzahl der APs der Anzahl der erwarteten Geräte. Die übrigen APs senken die Sendeleistung wieder auf den Standardwert.

Näheres zur Konfiguration unter *Rückfall-Sendeleistungsreduktion (Adaptive Transmission Power)* auf Seite 1051.

13.13 Opportunistic Key Caching (OKC)

Authentifizierung von WLAN-Clients über EAP und 802.1x ist mittlerweile Standard in Unternehmens-Netzwerken, und auch beim öffentlichen Internet-Zugang findet es im Rahmen der Hotspot 2.0-Spezifikation immer mehr Verbreitung. Der Nachteil der Authentifizierung über 802.1x ist, dass die Zeit von Anmeldung bis zur Verbindung durch den Austausch von bis zu zwölf Datenpaketen zwischen WLAN-Client und AP sich merklich verlängert. Für die meisten Anwendungen, bei denen es nur um den Austausch von Daten geht, mag das nicht ins Gewicht fallen. Zeitkritische Anwendungen wie z. B. Voice-over-IP sind jedoch davon abhängig, dass die Neuanmeldung in einer benachbarten WLAN-Funkzelle die Kommunikation nicht beeinträchtigt.

Um dem entgegenzuwirken, haben sich bestimmte Authentifizierungsstrategien wie PMK-Caching und Pre-Authentifizierung etabliert, wobei auch durch Pre-Authentifizierung nicht alle Probleme behoben sind. Einerseits ist nicht sichergestellt, wie der WLAN-Client erkennt, ob der AP Pre-Authentifizierung beherrscht. Andererseits führt Pre-Authentifizierung zu einer erheblichen Belastung des RADIUS-Servers, der die Authentifizierungen von allen Clients und allen APs im WLAN-Netzwerk verarbeiten muss.

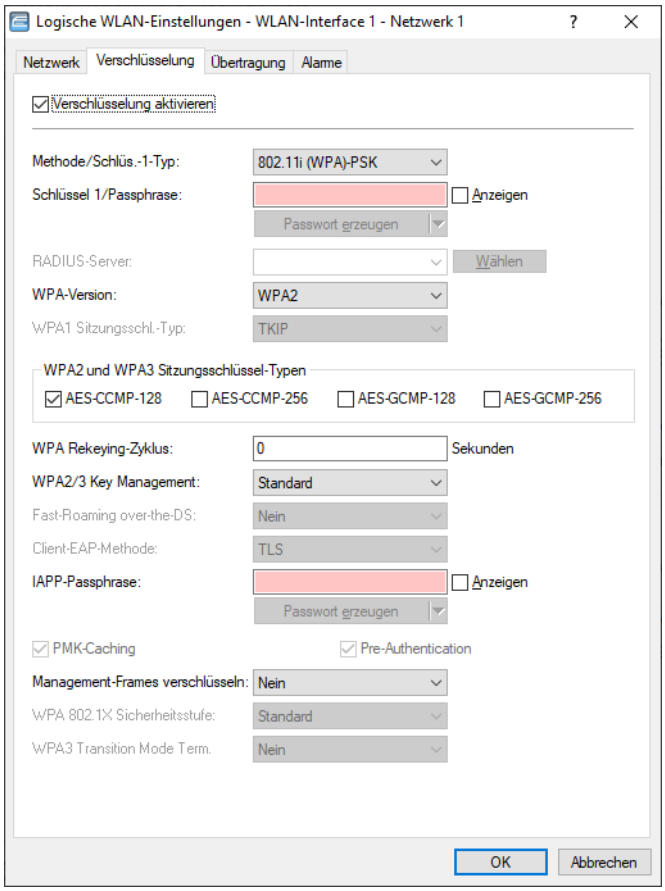
Das opportunistische Schlüssel-Caching verlagert die Schlüsselverwaltung auf einen WLC oder zentralen Switch, der alle APs im Netzwerk verwaltet. Meldet sich ein Client bei einem AP an, übernimmt der nachgeschaltete WLC als Authenticator die Schlüsselverwaltung und sendet dem AP den PMK, den schließlich der Client erhält. Wechselt der Client die Funkzelle, errechnet er aus diesem PMK und der MAC-Adresse des neuen APs eine PMKID und sendet die an den neuen AP in der Erwartung, dass der OKC aktiviert hat (deshalb "opportunistisch"). Kann der AP mit der PMKID nichts anfangen, handelt er mit dem Client eine normale 802.1x-Authentifizierung aus.

Ein LANCOM-AP kann auch OKC durchführen, falls der WLC vorübergehend nicht erreichbar ist. In diesem Fall speichert er den PMK und sendet ihn an den WLC, sobald er wieder verfügbar ist. Der schickt den PMK anschließend an alle APs im Netzwerk, so dass der Client sich beim Wechsel der Funkzelle dort über OKC anmelden kann.

13.13.1 Verschlüsseltes OKC über IAPP

Durch eine definierte IAPP-Passphrase (PMK-IAPP-Secret) auf einem AP ist es möglich, den PMK (Pairwise Master Key) verschlüsselt zu den anderen APs zu übertragen und dort zu speichern.

Die Eingabe der IAPP-Passphrase erfolgt im LANconfig unter **Wireless-LAN** > **Allgemein** > **Logische WLAN-Einstellungen** > **Verschlüsselung**.



13.14 Fast Roaming

Zusammen mit der Authentifizierung nach dem Standard IEEE 802.1X und dem Schlüsselmanagement nach dem Standard IEEE 802.11i bieten moderne WLAN-Installationen ein hohes Maß an Sicherheit und Vertraulichkeit der übertragenen Daten. Allerdings erfordern diese Standards die Übertragung zusätzlicher Datenpakete während der Verbindungsverhandlung sowie zusätzliche Rechenleistung auf Client- und Serverseite.

IEEE 802.11 benötigte ursprünglich zum Aufbau einer Datenverbindung zwischen WLAN-Client und Accesss Point lediglich bis zu sechs Datenpakete. Die Standard-Erweiterung IEEE 802.11i besserte Schwachstellen bei der WEP-Verschlüsselung aus, verlängerte dabei jedoch den Anmeldeprozess je nach Authentifizierungsmethode um ein Vielfaches.

Diese verlängerte Anmeldezeit des WLAN-Clients am Accesss Point ist für nicht zeitkritische Anwendungen ausreichend. Für ein reibungsloses, verlustfreies Roaming eines WLAN-Clients von einem Accesss Point zum nächsten, ist eine Verzögerung von mehr als 50 ms jedoch nicht akzeptabel. Als Beispiel seien hier Voice-over-IP (VoIP) oder die Anwendung in industriellen Echtzeit-Umgebungen genannt.

Methoden wie Pairwise Master Key Caching (PMK Caching), Pre-Authentication, Opportunistic Key Caching (OKC) sowie der Einsatz von zentralen WLAN-Controllern (WLC) zur Schlüsselverwaltung verbessern die Zeit für die Schlüsselaushandlung zwischen WLAN-Client und Accesss Point bei der Anmeldung. Allerdings reicht das immer noch nicht aus, die vergleichsweise lange Zeit für die Schlüsselverhandlung zwischen WLAN-Client und Accesss Point auf ein brauchbares Maß zu begrenzen.

Neben den verbesserten Verschlüsselungs-Protokollen ermöglicht es IEEE 802.11e dem WLAN-Client, eine zusätzliche Bandbreite beim Accesss Point zu reservieren. Auf diese Weise vermeidet der WLAN-Client Unterbrechungen z. B. bei VoIP-Verbindungen aufgrund von zu hoher Netzlast beim Accesss Point. Beim Roaming von einem Accesss Point zum nächsten muss der WLAN-Client diese zusätzliche Bandbreite erneut beim neuen Accesss Point reservieren. Die dafür notwendigen zusätzlichen Management-Frames erhöhen die Anmeldezeit jedoch wieder deutlich.

IEEE 802.11r sorgt dafür, dass sich bewegende WLAN-Clients beim Roaming ohne aufwändige Neuanmeldung und damit weitgehend störungsfrei von einem Accesss Point zum nächsten wechseln können. Das Ziel ist, die Anzahl der Datenpakete für die Anmeldung am AP wieder auf die vom IEEE 802.11 bekannten vier bis sechs Pakete zu verringern.

Wie beim Opportunistic Key Caching (OKC) existiert eine zentrale Schlüssel-Verwaltung, sinnvollerweise in Form eines WLCs, der die angeschlossenen Accesss Points mit den entsprechenden Anmeldedaten der WLAN-Clients versorgt. Im Gegensatz zum OKC kann der WLAN-Client beim Fast Roaming jedoch erkennen, ob der Accesss Point IEEE 802.11r beherrscht.

Die vom WLC verwalteten Accesss Points senden als Kennung das sogenannte „Mobility Domain Information Element (MDIE)“ aus, das den WLAN-Clients im Empfangsbereich u. a. mitteilt, welcher „Mobility Group“ der Accesss Point angehört. Anhand dieser Gruppenkennung erkennt der WLAN-Client, ob er derselben Domain angehört und sich somit ohne Verzögerung anmelden kann. Diese Mobility Domain hat der WLAN-Client während der ersten Anmeldung an einem Accesss Point mitgeteilt bekommen.

Die Domain-Kennung sowie spezielle, bei der Erstanmeldung generierte und an alle verwalteten Accesss Points übertragenen Schlüssel verringern die Verhandlungsschritte bei der Neuanmeldung bei einem Accesss Point auf die angestrebten vier bis sechs Schritte.

Um vergebliche und damit zeitraubende Anmeldeversuche mit abgelaufenen PMKs zu vermeiden, sieht IEEE 802.11r zusätzliche Informationen über die Gültigkeitsdauer von Schlüsseln vor. So kann der Client noch während einer bestehenden Verbindung mit dem aktuellen Accesss Point einen neuen PMK aushandeln. Dieser ist auch auf dem Accesss Point gültig, mit dem sich der WLAN-Client im Anschluss verbinden möchte.

Zusätzlich ermöglicht IEEE 802.11r in Form eines „Resource Requests“ die Reservierung von zusätzlicher Bandbreite auf dem neuen Accesss Point, ohne dass weitere Datenpakete wie bei IEEE 802.11e die Anmeldung unnötig verlängern.

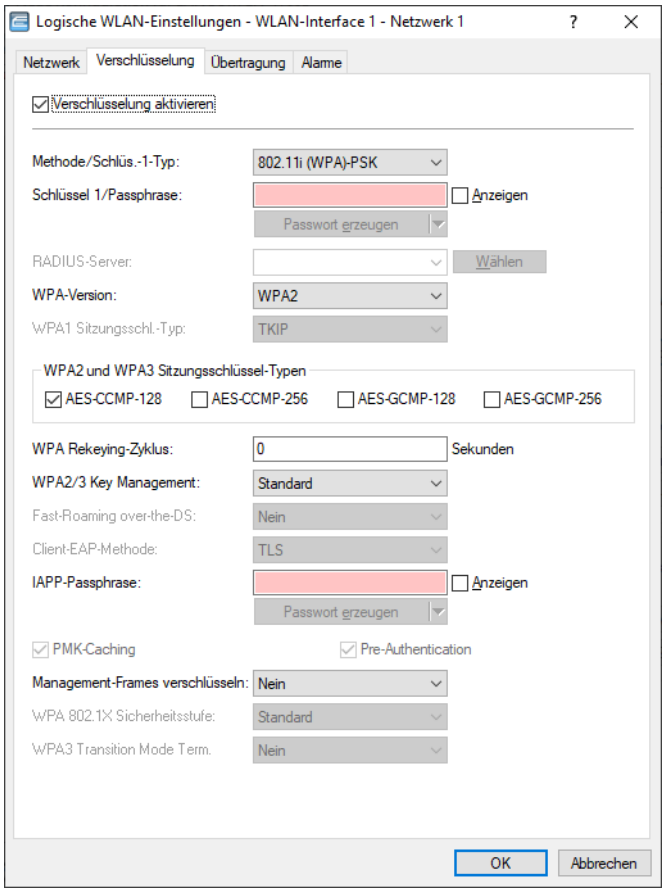
Ältere WLAN-Clients haben möglicherweise Probleme damit, eine Verbindung zu einer SSID mit aktiviertem 802.11r aufzubauen. Daher ist hier der Einsatz zweier SSIDs ratsam: eine SSID für ältere Clients ohne 802.11r-Unterstützung und eine weitere SSID mit aktiviertem 802.11r für Clients mit 802.11r-Unterstützung.

Das Fast-Roaming lässt sich in LANconfig einstellen unter **Wireless-LAN** > **Allgemein** > **Logische WLAN-Einstellungen** > **Verschlüsselung** > **WPA2/3 Key Management**.

13.14.1 Fast Roaming über IAPP

Um Fast Roaming über IAPP zu verwenden, ist es erforderlich, jeder Schnittstelle in den WLAN-Verbindungseinstellungen eine individuelle IAPP-Passphrase zuzuweisen. Diese wird verwendet, um die Pairwise Master Keys (PMKs) zu verschlüsseln. Somit können APs mit übereinstimmender IAPP-Passphrase (PMK-IAPP-Secret) PMKs untereinander austauschen und unterbrechungsfreie Verbindungen sicherstellen.

Die Eingabe der IAPP-Passphrase erfolgt im LANconfig unter **WLAN** > **Allgemein** > **Logische WLAN-Einstellungen** > **Verschlüsselung**.



Beachten Sie bitte, dass es für die Verwendung von IEEE 802.11r erforderlich ist, in den Verschlüsselungs-Einstellungen unter **WPA2/3 Key Management** die Option „Fast Roaming“ auszuwählen.

13.15 Bandbreitenbegrenzung im WLAN

Zur besseren Verteilung der Bandbreite bei mehreren Teilnehmern im WLAN können die verfügbaren Bandbreiten begrenzt werden. Diese Bandbreitenbegrenzung bietet sich z. B. an für Wireless ISPs, die Ihren Kunden nur eine definierte Bandbreite zur Verfügung stellen wollen.

Im Gegensatz zu Bandbreitenmanagement mit Hilfe von QoS (Quality of Service) wird mit diesem Verfahren keine Mindest-Bandbreite eingeräumt, sondern eine exakt definierte Maximal-Bandbreite. Auch wenn durch den

geringen Traffic anderer Netzteilnehmer eigentlich mehr Bandbreite verfügbar wäre, wird dem Benutzer hier immer nur die vorgegebene Bandbreite bereitgestellt.

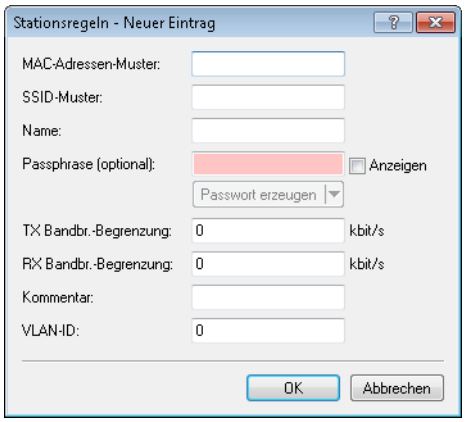
Die Einstellungen unterscheiden den Betrieb eines Gerätes als AP oder im Client-Modus.

13.15.1 Einstellung als Access Point

In der Betriebsart als AP können die maximal zulässigen Bandbreiten in Tx- und RX-Richtung für die WLAN-Clients festgelegt werden, die sich beim AP einbuchen. Dazu werden in der MAC-Zugangs-Liste die Werte für die maximale Tx- und Rx-Bandbreite in kBit/s eingetragen. Ein Wert von '0' signalisiert, dass in dieser Übertragungsrichtung keine Beschränkung der Bandbreite vorgesehen ist. Aus dem hier eingetragenen Wert und dem ggf. vom Client übermittelten Wert wird die tatsächlich bereitgestellte Bandbreite ermittelt.

Die Bedeutung der Werte Rx und Tx ist abhängig von der Betriebsart des Gerätes. In diesem Fall als AP steht Rx für „Daten senden“ und Tx für „Daten empfangen“.

Die maximalen Bandbreiten für die angeschlossenen Clients werden im LANconfig unter **Wireless-LAN** > **Stationen/LEPS** > **LEPS-MAC** > **Stationsregeln** eingetragen.



Kommentar

Kommentar zu diesem Eintrag.

VLAN-ID

VLAN-ID für den WLAN-Client.

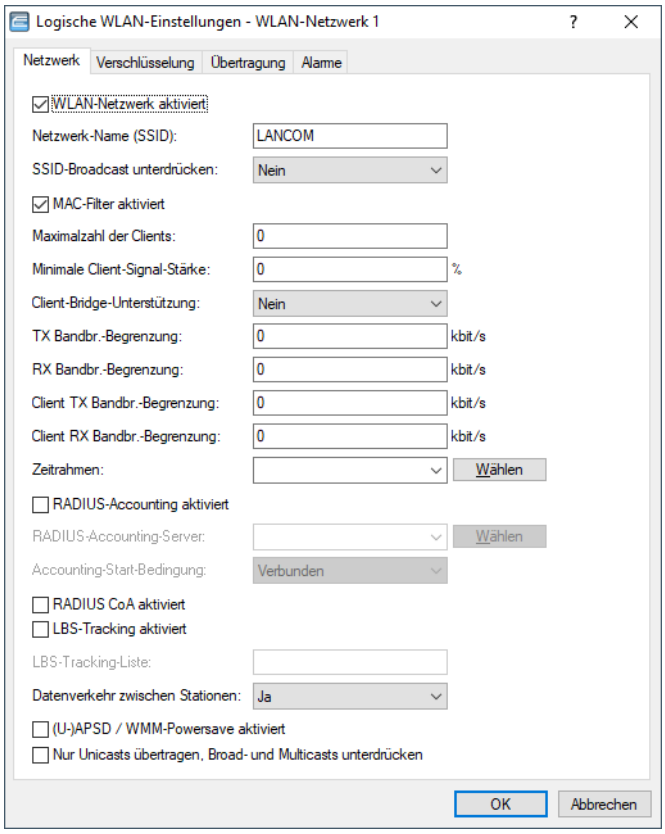
- Mögliche Werte: 0 bis 4094
- Besondere Werte: 0 schaltet die Verwendung von VLAN-Tagging aus.

13.15.2 Einstellung als Client

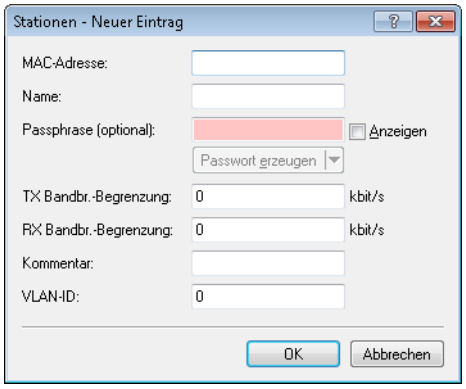
Wird das Gerät selbst als WLAN-Client betrieben, kann das Gerät beim Einbuchen beim AP seine maximalen Bandbreiten übermitteln. Der AP bildet dann mit ggf. eigenen Limits für diesen Client die tatsächlichen maximalen Bandbreiten.

Die Bedeutung der Werte Rx und Tx ist abhängig von der Betriebsart des Gerätes. In diesem Fall als Client steht Tx für „Daten senden“ und Rx für „Daten empfangen“.

Die maximalen Bandbreiten für ein Gerät im Client-Modus werden im LANconfig unter **Wireless-LAN** > **Allgemein** mit einem Klick auf **Logische WLAN-Einstellungen** und Auswahl der entsprechenden logischen WLAN-Schnittstelle auf der Registerkarte **Netzwerk** eingetragen.



Im WLC finden Sie die Bandbreitenbegrenzung der einzelnen Stationen unter **WLAN-Controller** > **Stationen/LEPS** > **LEPS-MAC** nach einem Klick auf **Stationsregeln**.



13.15.3 Bandbreitenbeschränkung der LAN-Schnittstellen

Bei einem Gerät mit integriertem WLAN-Modul können Sie ein Bandbreitenlimit für einzelne LAN-Schnittstellen definieren. Die Tabelle der LAN-Schnittstellen bietet zur Konfiguration der Bandbreitenbeschränkung die entsprechenden Parameter.

13.16 Automatische Anpassung der Übertragungsrate für Multicast- und Broadcast-Sendungen

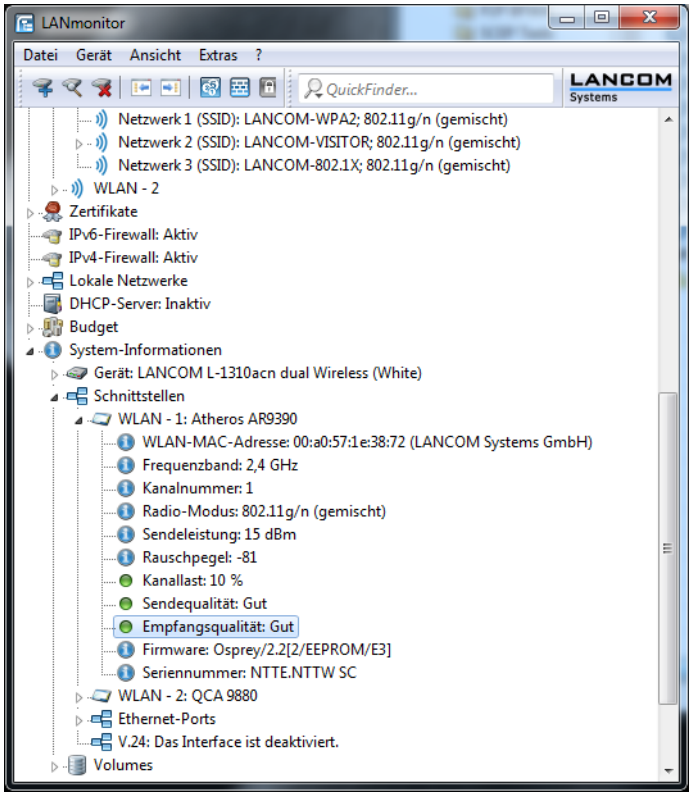
Während bei Unicast-Sendungen AP und Client die optimale Übertragungsgeschwindigkeit miteinander aushandeln können, findet systembedingt bei Multicast- und Broadcast-Sendungen die Kommunikation nur in eine Richtung statt: Vom AP zum Client. Die Clients können dem AP nicht zurückmelden, mit welcher maximalen Übertragungsgeschwindigkeit sie tatsächlich kommunizieren können.

Der AP hat zwei Möglichkeiten, die Übertragungsgeschwindigkeit für Multicast- und Broadcast-Sendungen festzulegen:

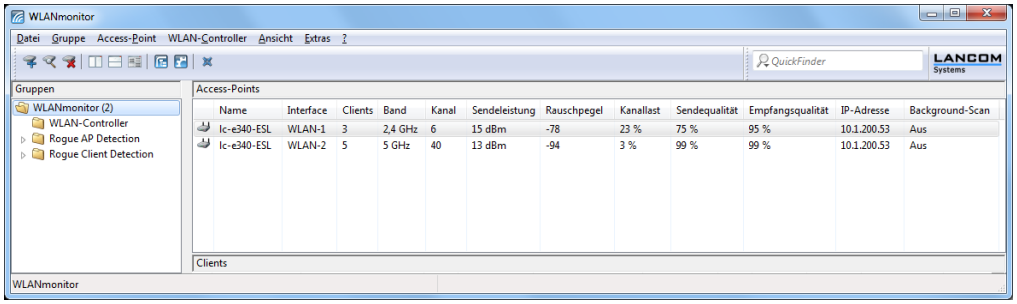
- **Feste Bitrate**: Die Übertragungsrate ist so bemessen, dass der langsamste Client im WLAN auch unter ungünstigen Bedingungen die Sendungen fehlerfrei und verständlich erhalten kann. Das kann dazu führen, dass der AP selbst dann mit einer geringeren Übertragungsrate sendet, wenn Umgebungsbedingungen und Clients eigentlich eine höhere Rate erlauben würden. Doch damit würde der AP das WLAN unnötig ausbremsen.
- **Automatische Bitrate**: Bei automatischer Festlegung der Übertragungsrate sammelt der AP die Informationen über die Übertragungsraten der einzelnen WLAN-Clients. Die Rate teilen die Clients dem AP automatisch bei jeder Unicast-Kommunikation mit. Aus der Liste der angemeldeten Clients wählt der AP nun ständig die jeweils niedrigste Übertragungsrate aus und überträgt damit die Multicast- und Broadcast-Sendungen.

13.17 LANCOM "Wireless Quality Indicators" (WQI)

LANmonitor bietet Ihnen die Möglichkeit, die Signalqualität der einzelnen Schnittstellen anhand von **Wireless Quality Indicators** anzuzeigen. Diese Darstellung von Empfangs- und Sendequalität (RX und TX) dient der schnellen Identifizierung der Signalqualität. Öffnen Sie zum Anzeigen dieser Informationen im LANmonitor den Bereich **System-Informationen** des Gerätes. Unter **Schnittstellen** werden Ihnen die Indikatoren angezeigt.



Der WLANmonitor zeigt Ihnen die **Wireless Quality Indicators** ebenfalls an. Klicken Sie hierfür auf den Gruppen-Hauptordner.

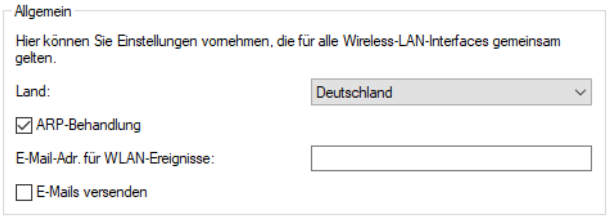


13.18 Konfiguration der WLAN-Parameter

Die Einstellungen für die Funknetzwerke erfolgen an verschiedenen Stellen in der Konfiguration:

- Manche Parameter betreffen die physikalische WLAN-Schnittstellen. Einige LANCOM Modelle verfügen über eine WLAN-Schnittstelle (Single Radio), andere Modelle haben ein zweites WLAN-Modul integriert (Dual Radio). Die Einstellungen für die physikalischen WLAN-Schnittstellen gelten für alle logischen Funknetzwerke, die mit diesem Modul aufgespannt werden. Zu diesen Parametern gehören z. B. die Sendeleistung der Antenne und die Betriebsart des WLAN-Moduls (AP oder Client).
- Andere Parameter beziehen sich nur auf die jeweiligen logischen Funknetze, die mit einem physikalischen Interface aufgespannt werden. Dazu gehört z. B. die SSID oder die Aktivierung der Verschlüsselung, z. B. 802.11i mit AES.
- Eine dritte Gruppe von Parametern hat zwar Auswirkungen auf den Betrieb des Funknetzwerks, ist aber nicht nur für WLANs von Bedeutung. Dazu gehören z. B. die Protokollfilter in der LAN-Bridge.

13.18.1 Allgemeine WLAN-Einstellungen



LANconfig: **Wireless-LAN** > **Allgemein**

Konsole: **Setup** > **WLAN**

Land

Der Betrieb von WLAN-Modulen ist international nicht einheitlich geregelt. Die Verwendung von bestimmten Funkkanälen ist z. B. in manchen Ländern nicht erlaubt. Um den Betrieb der APs auf die in dem jeweiligen Land zulässigen Parameter zu begrenzen, wird für alle physikalischen WLAN-Interfaces gemeinsam das Land eingestellt, in dem der AP betrieben wird.

ARP-Behandlung

Mobile Stationen im Funknetz, die sich im Stromsparmodus befinden, beantworten die ARP-Anfragen anderer Netzteilnehmer nicht oder nur unzuverlässig. Mit dem Aktivieren der 'ARP-Behandlung' übernimmt der AP diese Aufgabe und beantwortet die ARP Anfragen an Stelle der Stationen im Stromsparmodus.

E-Mail-Adr. für WLAN-Ereignisse

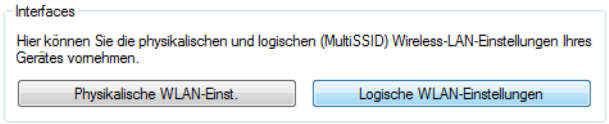
An diese E-Mail-Adresse werden Informationen über die Ereignisse im WLAN versendet, wenn dies über den nächsten Schalter aktiviert wird.

E-Mails versenden

Aktiviert das Versenden von Benachrichtigungsmails an die soeben angegebene E-Mail-Adresse.

13.18.2 Die physikalischen WLAN-Schnittstellen

Neben den allgemeinen WLAN-Parametern gelten eine Reihe von Einstellungen für jedes WLAN-Modul des APs speziell.

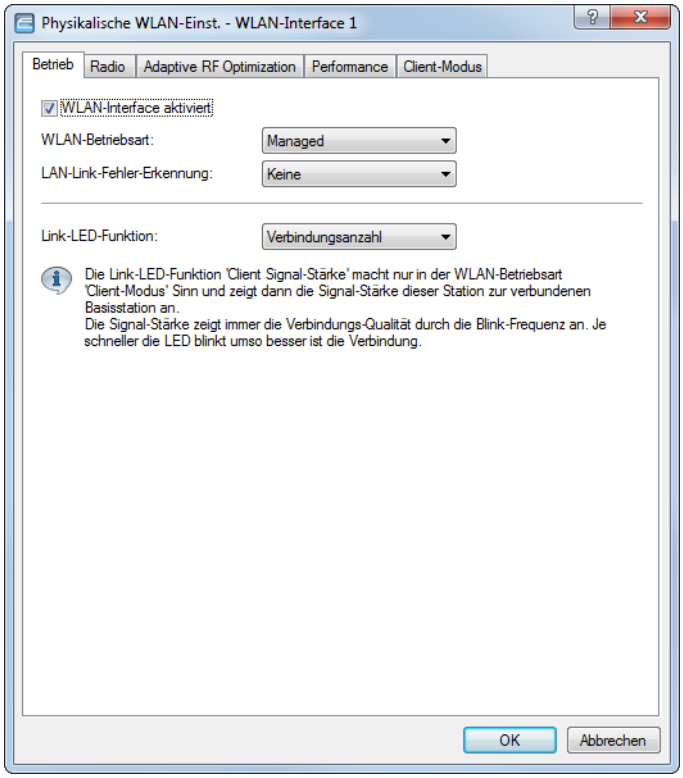


LANconfig: **Wireless-LAN** > **Allgemein** > **Interfaces** > **Physikalische WLAN-Einst.**

Falls der AP mehrere Funkmodule hat, dann muss zuerst dieses ausgewählt werden, danach gelangen Sie auf die Konfigurationsseiten des Moduls.

13.18.2.1 Betriebseinstellungen

Hier finden Sie die Betriebseinstellungen.



LANconfig: **Wireless LAN** > **Allgemein** > **Physikalische WLAN-Einstellungen** > **Betrieb**

Konsole: **Setup** > **Schnittstellen** > **WLAN** > **Betriebs-Einstellungen**

WLAN-Interface aktiviert

Wenn das WLAN-Interface nicht benötigt wird, kann es vollständig deaktiviert werden.

WLAN-Betriebsart

LANCOM APs können grundsätzlich in verschiedenen Betriebsarten arbeiten:

Basisstation

Als Basisstation (AP) stellt es für die WLAN-Clients die Verbindung zu einem kabelgebundenen LAN her.

Client

Als Client sucht das Gerät selbst die Verbindung zu einem anderen AP und versucht sich in einem Funknetzwerk anzumelden. In diesem Fall dient das Gerät also dazu, ein kabelgebundenes Gerät über eine Funkstrecke an eine Basisstation anzubinden.

Managed

Als Managed-AP sucht das Gerät einen zentralen WLC, von dem es eine Konfiguration beziehen kann.

Probe

In der Betriebsart **Probe** sammelt das Gerät nur WLAN-Informationen z. B. für einen integrierten Spektrum-Analyser.

LAN-Link-Fehler-Erkennung

Wenn ein AP keine Verbindung zum kabelgebundenen LAN hat, kann er in den meisten Fällen seine wesentliche Aufgabe – den eingebuchten WLAN-Clients einen Zugang zum LAN zu ermöglichen – nicht mehr erfüllen. Mit der Funktion der Broken-Link-Detection (Link-Fehler-Erkennung) können die WLAN-Module eines Gerätes deaktiviert werden, wenn die LAN-Verbindung verloren geht. So können die beim AP eingebuchten Clients einen anderen AP (mit ggf. schwächerem Signal) suchen und sich mit diesem verbinden

Mit dieser Funktion werden die WLAN-Module des Gerätes deaktiviert, wenn das zugeordnete LAN-Interface nicht über einen Link zum LAN verfügt.

Mögliche Werte:

Keine

Link-Fehler-Erkennung wird nicht genutzt.

LAN-1 bis LAN-n

Hängt von den verfügbaren LAN-Interfaces im Gerät ab. Alle WLAN-Module des Geräts werden deaktiviert, wenn das hier angegebene LAN-Interface keine Verbindung zum kabelgebundenen LAN hat.

Die Interface-Bezeichnungen LAN-1 bis LAN-n repräsentieren die logischen LAN-Schnittstellen. Die verfügbaren physikalischen Ethernet-Ports des Geräts müssen zur Nutzung dieser Funktion ggf. auf die entsprechenden Werte LAN-1 bis LAN-n eingestellt werden.

Die Link-Fehler-Erkennung kann auch für WLAN-Geräte in der Betriebsart als WLAN-Client genutzt werden. Bei eingeschalteter Link-Fehler-Erkennung werden die WLAN-Module eines WLAN-Clients nur dann aktiviert, wenn die entsprechenden LAN-Schnittstellen eine Verbindung zum kabelgebunden LAN haben.

Link-LED-Funktion

Bei der Einrichtung von Point-to-Point-Verbindungen oder in der Betriebsart als WLAN-Client ist es für eine möglichst gute Positionierung der Antennen wichtig, die Empfangsstärke in verschiedenen Positionen zu erkennen. Die WLAN-Link-LED kann z. B. für die Phase der Einrichtung zur Anzeige der Empfangsqualität genutzt werden. In der entsprechenden Betriebsart blinkt die WLAN-Link-LED umso schneller, je besser die Empfangsqualität in der jeweiligen Antennenposition ist.

Mögliche Werte:

Verbindungsanzahl

In dieser Betriebsart zeigt die LED mit einem „inversen Blitzen" die Anzahl der WLAN-Clients an, die bei dem AP als Client eingebucht sind. Nach der Anzahl der Blitzer für jeden Client erfolgt eine kurze Pause. Wählen Sie diese Betriebsart dann, wenn Sie das Gerät als Basisstation betreiben.

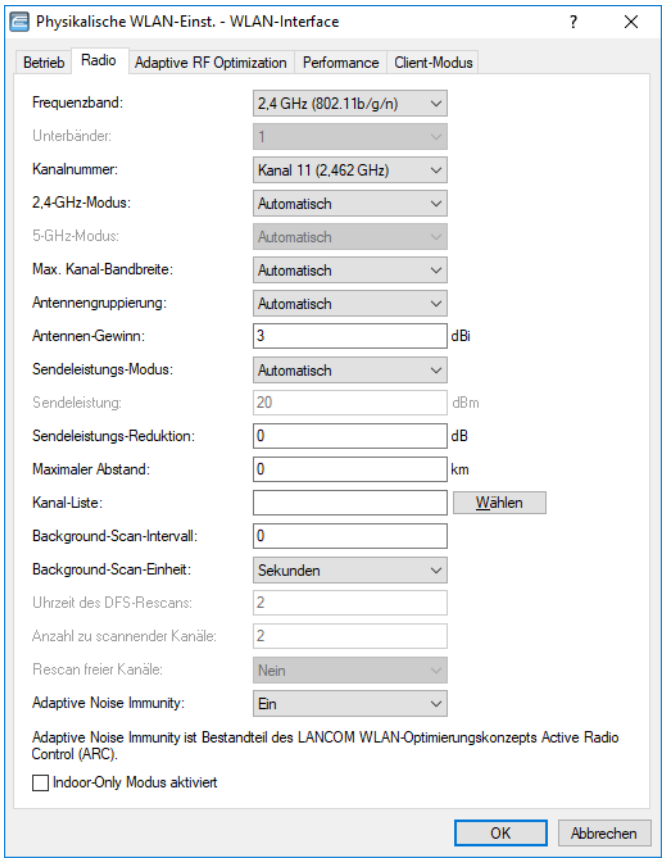
Client-Signalstärke

In dieser Betriebsart zeigt die LED die Signalstärke des APs an, bei dem ein AP selbst als Client eingebucht ist. Je schneller die LED blinkt, umso besser ist das Signal. Wählen Sie diese Betriebsart nur, wenn Sie den AP im Client-Modus betreiben.

P2P1- bis P2Px-Signalstärke

In dieser Betriebsart zeigt die LED die Signalstärke des jeweiligen P2P-Partners, mit dem ein AP eine P2P-Strecke bildet. Je schneller die LED blinkt, umso besser ist das Signal.

13.18.2.2 Radio-Einstellungen



LANconfig: **Wireless LAN** > **Allgemein** > **Physikalische WLAN-Einstellungen** > **Radio**

Frequenzband, Unterbänder

Mit der Auswahl des Frequenzbandes legen Sie fest, ob das WLAN-Modul im 2,4-GHz- oder im 5-GHz-Band arbeitet, und damit gleichzeitig die möglichen Funkkanäle.

Im 5-GHz-Band kann außerdem ein Unterband gewählt werden, an das wiederum bestimmte Funkkanäle und maximale Sendeleistungen geknüpft sind.

In einigen Ländern ist das DFS-Verfahren mit automatischer Kanalsuche vorgeschrieben. Mit der Wahl des Unterbands wird damit auch der Bereich der Funkkanäle festgelegt, die für die automatische Kanalauswahl verwendet werden kann.

Kanalnummer

Hier bestimmen Sie den Kanal für die Datenübertragung im Funktnetz.

Im 2,4-GHz-Band müssen zwei getrennte Funknetze mindestens drei Kanäle auseinander liegen, um Störungen zu vermeiden.

2,4-GHz-Modus / 5-GHz-Modus

Geben Sie an, welche(n) Funkstandard(s) die von Ihnen konfigurierte physikalische WLAN-Schnittstelle gegenüber einem WLAN-Client unterstützt.

Sowohl im 2,4-GHz- als auch im 5-GHz-Frequenzband existieren inzwischen unterschiedliche Funk-Standards, nach denen ein AP senden kann. Im 2,4-GHz-Frequenzband umfasst dies bislang die Standards IEEE 802.11b, IEEE 802.11g und IEEE 802.11n; im 5-GHz-Frequenzband die Standards IEEE 802.11a, IEEE 802.11n und IEEE 802.11ac. Je nach Gerätetyp und gewähltem Frequenzband haben Sie die Möglichkeit, einen AP exklusiv in einem bestimmten Modus zu betreiben oder einen der verschiedenen Kompatibilitätsmodi einzustellen.

Beachten Sie, dass WLAN-Clients, die lediglich einen langsameren Standard unterstützen, sich nicht mehr in Ihrem WLAN anmelden können, wenn Sie den Modus auf einen zu hohen Wert einstellen. Die Kompatibilität geht jedoch immer zu Lasten der Performance. Erlauben Sie daher ausschließlich jene Betriebsarten, die aufgrund der vorhandenen WLAN-Clients unbedingt erforderlich sind.

Sofern sich in Ihrem WLAN z. B. ausschließlich 802.11n-fähige WLAN-Clients befinden, empfiehlt sich die Wahl des Greenfield-Modus: Hierdurch unterbinden Sie die Anmeldung langsamerer Clients, welche das Netz andernfalls ausbremsen würden.

Um eine möglichst hohe Übertragungsgeschwindigkeit zu erreichen, gleichzeitig aber auch langsamere WLAN-Clients nicht auszuschließen, empfiehlt sich die Wahl eines Kompatibilitätsmodus (bei 2,4 GHz z. B. „802.11b/g/n (gemischt)“; bei 5 GHz „802.11a/n (gemischt)“). Im Kompatibilitätsmodus arbeitet eine physikalische WLAN-Schnittstelle grundsätzlich nach dem schnellsten Standard, fällt aber auf einen langsameren Standard zurück, wenn sich ein entsprechender WLAN-Client im Netz anmeldet. Im Rahmen von 802.11b können Sie dabei auswählen, ob die physikalische WLAN-Schnittstelle ausschließlich den 11-MBit-Modus oder auch den älteren 2-MBit-Modus unterstützten soll („(2Mbit-kompatibel)“).

Bei APs nach dem 802.11g-Standard haben Sie darüber hinaus die Möglichkeit, die Übertragungsgeschwindigkeit auf bis zu 108 MBit/s zu steigern. Im sogenannten Turbo-Modus nutzt ein AP gleichzeitig zwei benachbarte freie Kanäle für die Funkübertragung. Wenn Sie einen AP in den 108 Mbit/s-Turbo-Modus schalten, dann können ausschließlich noch diejenigen WLAN-Clients eine Verbindung zu dem AP aufbauen, welche ebenfalls im Turbo-Modus betrieben werden.

Der Turbo-Modus wird dem 802.11g-Standard zugeordnet, entspricht jedoch keinem offiziellen IEEE-Standard. Die Technik repräsentiert eigene Erweiterungen unterschiedlicher Chipsatz-Hersteller, die diese Technik auch unter der Bezeichnung „802.11g+“ oder „802.11g++“ vermarkten. Der Turbo-Modus ist daher ausschließlich auf APs mit reiner 802.11g-Hardware verfügbar.

Sofern Sie über die Einstellung „Automatisch“ die Wahl des 2,4- / 5-GHz-Modus dem Gerät überlassen, ist die Wahl des besten Modus vom verwendeten Frequenzband und den Fähigkeiten der Geräte-Hardware abhängig:

- Innerhalb des 2,4-GHz-Modus führt die Automatik entweder zu **802.11b/g/n (gemischt)** oder zu **802.11b/g (gemischt)**.
- Innerhalb des 5-GHz-Modus führt die Automatik entweder zu **802.11a/n/ac (gemischt)**, **802.11a/n (gemischt)** oder **54 Mbit/s-Modus**.

APs nach 802.11n sind im 2,4-GHz-Frequenzband prinzipiell abwärtskompatibel zu den vorhergehenden Standards IEEE 802.11b und IEEE 802.11g. Für im 802.11b- oder 802.11g-Modus betriebene 802.11n-Hardware sind lediglich die 802.11n-spezifischen Funktionen nicht verfügbar. Im 5-GHz-Frequenzband hingegen besteht diese Abwärtskompatibilität nicht: Die betreffenden 802.11n-Geräte müssen 802.11a explizit unterstützen.

Max. Kanal-Bandbreite

Legen Sie hier fest, wie und in welchem Umfang der AP die Kanal-Bandbreite für die physikalische(n) WLAN-Schnittstelle(n) festlegt. Mögliche Werte:

Automatisch

Der AP stellt die Kanal-Bandbreite automatisch optimal ein. Dabei lässt der AP die maximal verfügbare Bandbreite zu, sofern die momentanen Betriebsbedingungen dies erlauben. Andernfalls begrenzt der AP die Kanal-Bandbreite auf 20MHz.

20 MHz

Der AP benutzt auf 20 MHz gebündelte Kanäle.

40 MHz

Der AP benutzt auf 40 MHz gebündelte Kanäle.

80 MHz

Der AP benutzt auf 80 MHz gebündelte Kanäle.

Standardmäßig bestimmt die physikalische WLAN-Schnittstelle den Frequenzbereich, in dem die zu übertragenen Daten auf die Trägersignale aufmoduliert werden, automatisch. 802.11a/b/g nutzen 48 Trägersignale in einem 20 MHz-Kanal. Durch die Nutzung des doppelten Frequenzbereiches von 40 MHz können 96 Trägersignale eingesetzt werden, was zu einer Verdoppelung des Datendurchsatzes führt.

802.11n kann in einem 20 MHz-Kanal 52, in einem 40 MHz-Kanal sogar 108 Trägersignale zur Modulation nutzen. Für 802.11n bedeutet die Nutzung der 40 MHz-Option also einen Performance-Gewinn auf mehr als das Doppelte.

Antennengruppierung

Nur verfügbar für 802.11n.

LANCOM APs mit 802.11n-Unterstützung können bis zu drei Antennen zum Senden und Empfangen der Daten einsetzen. Der Einsatz mehrerer Antennen kann bei 802.11n unterschiedliche Ziele verfolgen:

- Verbesserung des Datendurchsatzes: Mit dem Einsatz von „Spatial Multiplexing“ können zwei parallele Datenströme realisiert werden, mit denen die doppelte Datenmenge übertragen werden kann.
- Verbesserung der Funk-Abdeckung: Mit dem Einsatz von „Cyclic Shift Diversity (CSD)“ kann ein Funksignal in unterschiedlichen Phasenlagen gesendet werden. Damit sinkt die Gefahr, dass es an bestimmten Stellen der Funkzelle zu Auslöschungen des Signals kommt.

Je nach Anwendung kann die Nutzung der Antennen eingestellt werden:

- Beim Einsatz des Geräts im AP-Modus zur Anbindung von WLAN-Clients ist in der Regel die parallele Nutzung aller drei Antennen zu empfehlen, um eine gute Netzabdeckung zu erzielen.
- Für die Nutzung von zwei parallelen Datenströmen z. B. bei Point-to-Point-Verbindungen mit einer entsprechenden Dual-Slant-Antenne werden die Antennen-Anschlüsse 1 + 2 **oder** 1 + 3 verwendet. Der nicht genutzte Antennen-Anschluss wird dabei jeweils deaktiviert.
- Bei Anwendungen mit nur einer Antenne (z. B. Outdoor-Anwendung mit einer Antenne) wird die Antenne an den Anschluss 1 angeschlossen, die Anschlüsse 2 und 3 werden deaktiviert.
- Mit der Einstellung „Automatisch“ werden alle verfügbaren Antennen genutzt.

Bitte beachten Sie für den Anschluss der Antennen: Der Antennen-Anschluss 1 muss immer verwendet werden. Je nach Montage und Verkabelung kann für die zweite Antenne entweder Anschluss 2 oder Anschluss 3 gewählt werden. Die softwareseitige Konfiguration des Gerätes muss dabei mit dem Anschluss der Antennenkabel übereinstimmen.

Antennen-Gewinn

Wenn Antennen mit einer höheren Sendeleistung eingesetzt werden, als in dem jeweiligen Land zulässig, ist eine Dämpfung der Leistung auf den zulässigen Wert erforderlich. Hier wird der Gewinn der Antenne abzüglich der tatsächlichen Kabeldämpfung eingetragen. Bei einer AirLancer Extender O-18a-Antenne mit einem Gewinn von 18 dBi wird bei einer Kabellänge von 4 m Länge mit einer Dämpfung 1 dB/m ein Antennen-Gewinn von 18 - 4 = 14 eingetragen. Aus diesem tatsächlichen Antennengewinn wird dann dynamisch unter Berücksichtigung der anderen eingestellten Parameter wie Land, Datenrate und Frequenzband die maximal mögliche Leistung berechnet und abgestrahlt.

Sendeleistungs-Modus

Im Modus **Automatisch** wird die maximal erlaubte und von der Hardware des Access Point realisierbare Sendeleistung verwendet. Zusätzlich kann die jeweils aktuelle WLAN-Sendeleistung um einen festen, im Feld **Sendeleistungs-Reduktion** konfigurierten Wert reduziert werden. Auf diese Weise kann die WLAN-Zellgröße an die Anforderungen eines Szenarios angepasst werden. Dieses Verfahren stößt an seine Grenzen, wenn durch eine professionelle WLAN-Ausleuchtung eine maximal zu erreichende Sendeleistung festgelegt wurde und gleichzeitig auch ein automatischer Wechsel zwischen Kanälen der verschiedenen 5-GHz-Unterbänder gewünscht ist. So ist z. B. im 5-GHz-Unterband 2 eine höhere Sendeleistung erlaubt als im Unterband 1. Die fest eingestellte Sendeleistungsreduktion würde nun einfach die höhere Sendeleistung im Unterband 2 um genau den selben Wert reduzieren, wie die geringere erlaubte Sendeleistung im Unterband 1. Man erhält als Resultat unterschiedliche Zellgrößen, abhängig vom gewählten Unterband. Im Modus **Manuell** kann die maximal zu erreichende **Sendeleistung** als absoluter Wert eingestellt werden, so dass unabhängig von der erlaubten maximalen Sendeleistung immer die gleiche Zellgröße erzielt wird.

In keinem Fall wird der Access Point die vom Gesetzgeber vorgegebenen Grenzen für die Sendeleistung überschreiten. Diese werden automatisch immer beachtet, unabhängig von der hier vorgenommenen Konfiguration.

Sendeleistung

Die gewünschte Sendeleistung in dBm.

Sendeleistungs-Reduktion

Statische Reduktion der Sendeleistung um den hier eingetragenen Wert, ohne Berücksichtigung anderer Parameter.

Durch die Sendeleistungs-Reduktion wird nur die abgestrahlte Leistung reduziert. Die Empfangsempfindlichkeit (der Empfangs-Antennengewinn) der Antennen bleibt davon unberührt. Mit dieser Variante können z. B. bei Funkbrücken große Entfernungen durch den Einsatz von kürzeren Kabeln überbrückt werden. Der Empfangs-Antennengewinn wird erhöht, ohne die gesetzlichen Grenzen der Sendeleistung zu übersteigen. Dadurch wird die maximal mögliche Distanz und insbesondere die erreichbare Datenübertragungsgeschwindigkeit verbessert.

Maximaler Abstand

Bei sehr großen Entfernungen zwischen Sender und Empfänger im Funknetz steigt die Laufzeit der Datenpakete. Ab einer bestimmten Grenze erreichen die Antworten auf die ausgesandten Pakete den Sender nicht mehr innerhalb der erlaubten Zeit. Mit der Angabe des maximalen Abstands kann die Wartezeit auf die Antworten erhöht werden. Diese Distanz wird umgerechnet in eine Laufzeit, die den Datenpaketen bei der drahtlosen Kommunikation zugestanden werden soll.

Kanal-Liste

Die Kanalauswahl erfolgt vom Access-Point grundsätzlich automatisch für das Frequenzband des eingestellten Landes, wenn hier kein Eintrag erfolgt.

Tragen Sie hier die Kanäle ein, auf die sich die automatische Auswahl beschränken soll. Wird hier nur ein Kanal angegeben, so wird nur dieser verwendet und es findet keine automatische Auswahl statt. Achten Sie deshalb darauf, dass die angegebenen Kanäle wirklich im Frequenzband des eingestellten Landes zur Verfügung stehen. Für das jeweilige Frequenzband ungültige Kanäle werden ignoriert.

Solange die Radarerkennung eingeschaltet ist, handelt es sich lediglich um eine Bevorzugung der hier eingetragenen Kanäle. Werden diese durch Radarimpulse beeinflusst, wird versucht auf weitere Kanäle auszuweichen die hier nicht aufgeführt sind. Erst wenn die Radarerkennung durch Einschalten des Indoor-Only-Modus abgeschaltet ist, findet die Auswahl der Kanäle exklusiv statt.

Die Angabe erfolgt als beliebige Komma-separierte Auflistung der gewünschten Kanäle, auf die sich die automatische Auswahl beschränken soll.

Zum Beispiel würde die Angabe "1,7-9,13" bei der automatischen Kanalsuche nur die Kanäle 1, 7 bis 9 und 13 berücksichtigen.

Background-Scan-Intervall / Background-Scan-Einheit

Wird hier ein Wert angegeben, so sucht der Wireless Router oder AP innerhalb dieses Intervalls zyklisch die aktuell ungenutzten Frequenzen des aktiven Bandes nach erreichbaren APs ab.

- Für Geräte im AP-Modus wird die Background-Scan-Funktion üblicherweise zur Rogue AP Detection eingesetzt. Das Scan-Intervall sollte hier der Zeitspanne angepasst werden, innerhalb derer unbefugte APs erkannt werden sollen, z. B. 1 Stunde.
- Für Geräte im Client-Modus wird die Background-Scan-Funktion hingegen meist für ein besseres Roaming von mobilen WLAN-Clients genutzt. Um ein schnelles Roaming zu erzielen, wird die Scan-Zeit hierbei auf z. B. 260 Sekunden beschränkt.
- Mit einer Hintergrund-Scan-Zeit von '0' wird die Funktion des Background-Scanning ausgeschaltet.

Mit der Zeiteinheit kann ausgewählt werden, ob der eingetragene Wert für Millisekunden, Sekunden, Minuten, Stunden oder Tage gilt, um einen möglichst anschaulichen Werte für das angestrebte Verhalten darzustellen.

Um Beeinträchtigungen der Datenübertragungsrate zu verhindern, beträgt das Intervall zwischen den einzelnen Kanal-Scans im AP-Modus mindestens 20 Sekunden. Kleinere Eingaben werden automatisch auf dieses Mindestintervall korrigiert. Zum Beispiel wird bei 13 zu scannenden Funkkanälen im 2.4-GHz-Band das gesamte Spektrum minimal innerhalb von 13 x 20 s = 260 Sekunden einmal gescannt.

Das Background-Scanning kann auf eine geringere Anzahl von Kanälen beschränkt werden, wenn der Indoor-Modus aktiviert wird. Auf diese Weise kann das Roaming für mobile Wireless Router oder APs im Client-Modus noch weiter verbessert werden.

DFS-Konfiguration

Konfigurieren Sie hier die DFS-Einstellungen.

Informationen zu Dynamic Frequency Selection finden Sie unter *Dynamic Frequency Selection (DFS)*.

Adaptive Noise Immunity

Aktivieren oder deaktivieren Sie hier die Adaptive Noise Immunity.

Informationen zu Adaptive Noise Immunity finden Sie unter *Adaptive Noise Immunity*.

Indoor-only Modus aktiviert

Mit der Auswahl des Frequenzbandes (2,4 oder 5 GHz) legen Sie u. a. die möglichen Kanäle fest, die für die Übertragung verwendet werden dürfen. Aus diesen möglichen Kanälen wählt ein AP bei automatischer Kanalwahl einen freien Kanal aus, um z. B. Störungen mit anderen Funksignalen zu vermeiden.

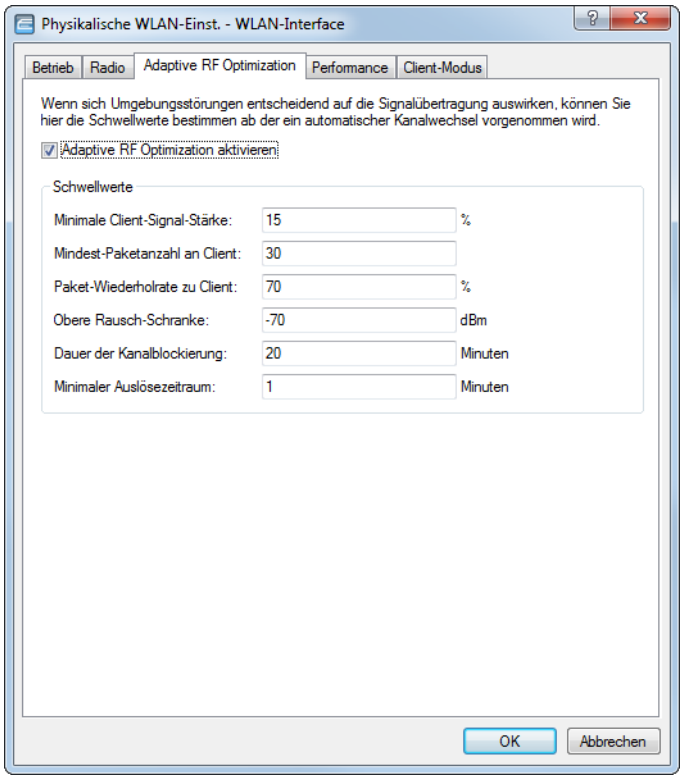
In einigen Ländern gelten spezielle Vorschriften, welche Frequenzbänder und Kanäle für die WLAN-Nutzung im Indoor- und Outdoor-Betrieb verwendet werden dürfen. So dürfen z. B. in Frankreich im 2,4-GHz-Band nicht alle verfügbaren Kanäle im Outdoor-Betrieb genutzt werden. In manchen Ländern ist das DFS-Verfahren für den Outdoor-Betrieb im 5-GHz-Band vorgeschrieben, um Störungen von Radaranlagen zu vermeiden.

Mit der Option 'Indoor-Only' kann ein AP auf den ausschließlichen Betrieb innerhalb von geschlossenen Gebäuden beschränkt werden. Durch diese Einschränkung können auf der anderen Seite bei der automatischen Kanalwahl die Kanäle flexibler gehandhabt werden.

Die Indoor-Only-Funktion kann nur zuverlässig aktiviert werden, wenn das Land eingestellt wurde, in dem der AP betrieben wird.

Die Aktivierung der Indoor-Only-Funktion ist nur erlaubt, wenn sich der AP sowie alle verbundenen Clients in einem geschlossenen Raum befinden.

13.18.2.3 Adaptive RF Optimization



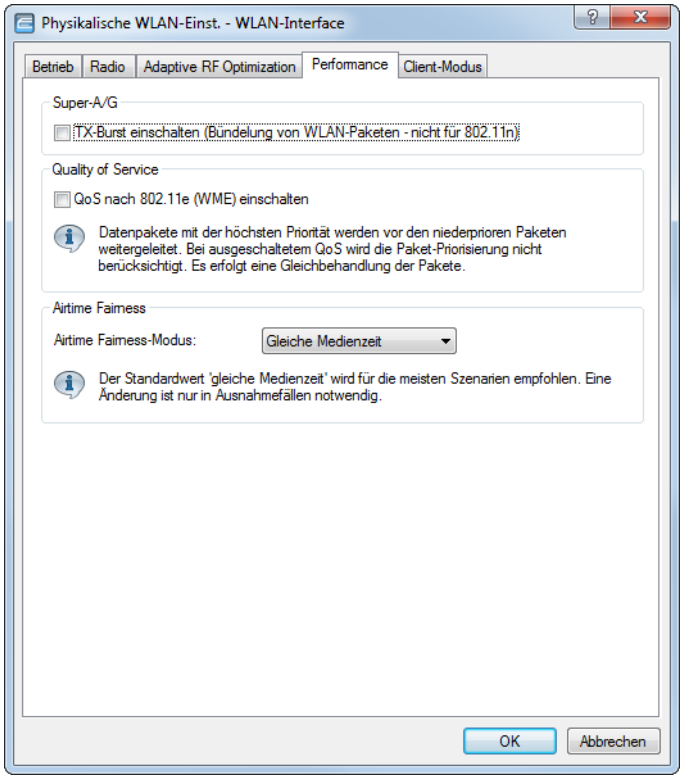
LANconfig: **Wireless LAN** > **Allgemein** > **Physikalische WLAN-Einstellungen** > **Adaptive RF Optimization**

Konfigurieren Sie hier die Einstellungen der Adaptive RF Optimization. Informationen hierzu finden Sie unter *Adaptive RF Optimization* auf Seite 978.

13.18.2.4 Performance

LANconfig: **Wireless LAN** > **Allgemein** > **Physikalische WLAN-Einstellungen** > **Performance**

Konsole: **Setup** > **Schnittstellen** > **WLAN** > **Leistung**



TX-Burst einschalten

Erlaubt / Verbietet das Paket-Bursting, was den Durchsatz erhöht, jedoch die Fairness auf dem Medium verschlechtert.

QoS nach 802.11e einschalten

Mit der Erweiterung der 802.11-Standards um 802.11e können auch für WLAN-Übertragungen definierte Dienstgüten angeboten werden (Quality of Service). 802.11e unterstützt u. a. eine Priorisierung von bestimmten Datenpaketen. Die Erweiterung stellt damit eine wichtige Basis für die Nutzung von Voice-Anwendungen im WLAN dar (Voice over WLAN – VoWLAN). Die Wi-Fi-Alliance zertifiziert Produkte, die Quality of Service nach 802.11e unterstützen, unter dem Namen WMM (Wi-Fi Multimedia, früher WME für Wireless Multimedia Extension). WMM definiert vier Kategorien (Sprache, Video, Best Effort und Hintergrund), die in Form separater Warteschlangen zur Prioritätensteuerung genutzt werden. Der 802.11e-Standard nutzt zur Steuerung der Prioritäten die VLAN-Tags bzw. die DiffServ-Felder von IP-Paketen, wenn keine VLAN-Tags vorhanden sind. Die Verzögerungszeiten (Jitter) bleiben mit weniger als zwei Millisekunden in einem Bereich, der vom menschlichen Gehör nicht wahrgenommen wird. Zur Steuerung des Zugriffs auf das Übertragungsmedium nutzt der 802.11e-Standard die Enhanced Distributed Coordination Function (EDCF).

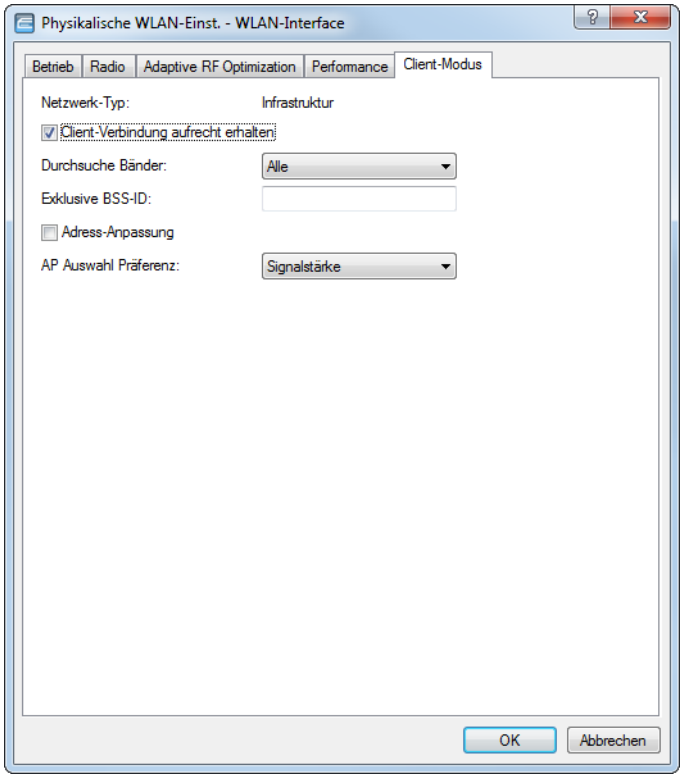
Die Steuerung der Prioritäten ist nur möglich, wenn sowohl der WLAN-Client als auch der AP den 802.11e-Standard bzw. WMM unterstützen und die Anwendungen die Datenpakete mit den entsprechenden Prioritäten kennzeichnen.

Airtime Fairness

Konfigurieren Sie hier die Einstellungen der Airtime Fairness. Informationen hierzu finden Sie unter *Airtime Fairness* auf Seite 980.

13.18.2.5 Client-Modus

Wenn das Gerät als Client betrieben wird, können auf der Registerkarte 'Client-Modus' bei den Einstellungen für die physikalischen Interfaces noch weitere Einstellungen bzgl. des Verhaltens als Client vorgenommen werden.



LANconfig: **Wireless LAN** > **Allgemein** > **Physikalische WLAN-Einstellungen** > **Client-Modus**

Konsole: **Setup** > **Schnittstellen** > **WLAN** > **Client-Einstellungen**

Client-Verbindung aufrecht erhalten

Mit dieser Option hält die Client-Station die Verbindung zur Basisstation aufrecht, auch wenn von den angeschlossenen Geräten keine Datenpakete gesendet werden. Ist diese Option ausgeschaltet, wird die Clientstation automatisch aus dem Funknetzwerk abgemeldet, wenn für eine bestimmte Zeit keine Pakete über die WLAN-Verbindung fließen.

Durchsuchte Bänder

Legen Sie hier fest, ob die Clientstation nur das 2,4-GHz-, nur das 5-GHz-Band oder alle verfügbaren Bänder absuchen soll, um eine Basisstation zu finden.

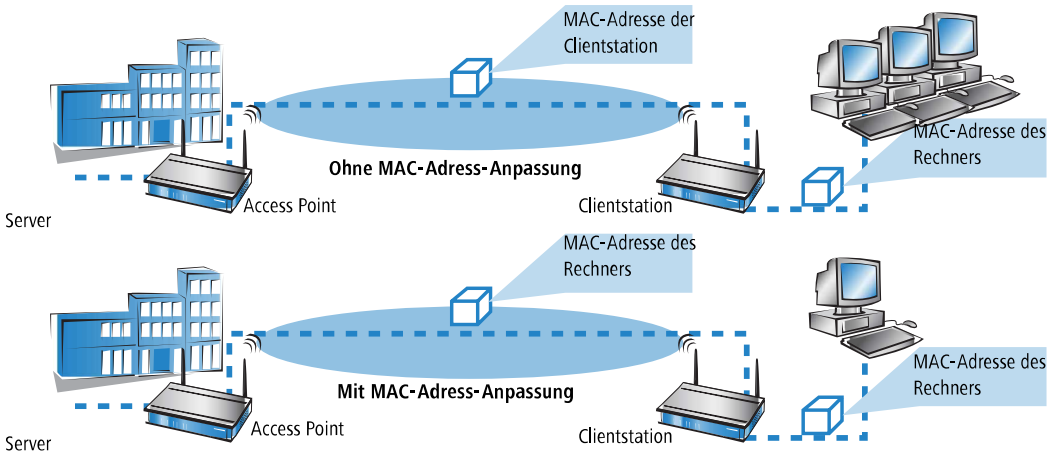
Exklusive BSS-ID

Wenn sich die Clientstation nur bei einem bestimmten AP einbuchen soll, können Sie hier die MAC-Adresse des WLAN-Moduls aus diesem AP eintragen.

Adress-Anpassung

Im Client-Modus ersetzt die Clientstation üblicherweise die MAC-Adressen in den Datenpaketen der an ihr angeschlossenen Geräte durch die eigene MAC-Adresse. Der AP auf der anderen Seite der Verbindung „sieht“

also immer nur die MAC-Adresse der Clientstation, nicht jedoch die MAC-Adresse der oder des angeschlossenen Rechners.



In manchen Installationen ist es jedoch gewünscht, dass die MAC-Adresse eines Rechners und nicht die der Clientstation an den AP übertragen wird. Mit der Option **Adress-Anpassung** wird das Ersetzen der MAC-Adresse durch die Clientstation unterbunden, die Datenpakete werden mit der originalen MAC-Adresse übertragen – der AP übernimmt im WLAN die MAC-Adresse des Clients.

Die Adress-Anpassung funktioniert nur, wenn an die Clientstation nur **ein** Rechner angeschlossen ist!

AP Auswahl Präferenz

Stehen mehrere APs zur Auswahl, die mit unterschiedlichen Profilen übereinstimmen, können folgende Kriterien zur Auswahl des APs herangezogen werden.

Profile

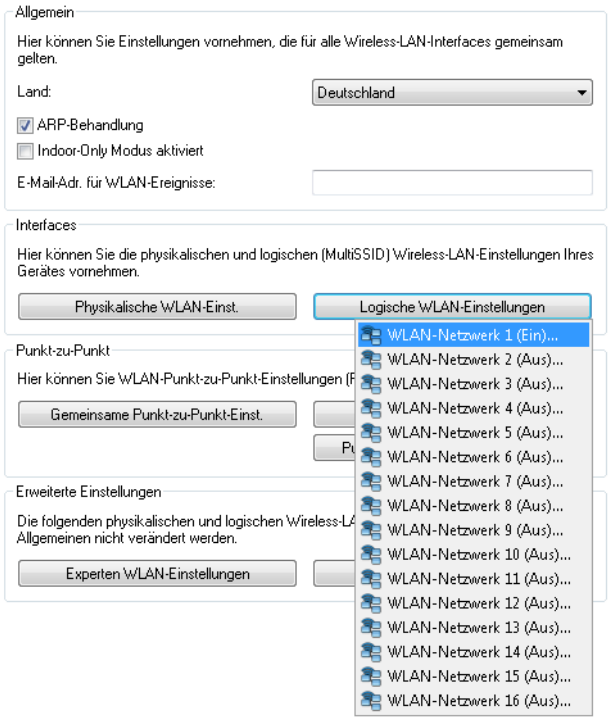
Das Profil mit dem kleinsten Index wird gewählt, auch wenn ein stärkerer AP zur Verfügung steht, der mit einem Profil eines höheren Indexes übereinstimmt.

Signalstärke

Die Signalstärke wird zum wichtigsten Auswahlkriterium.

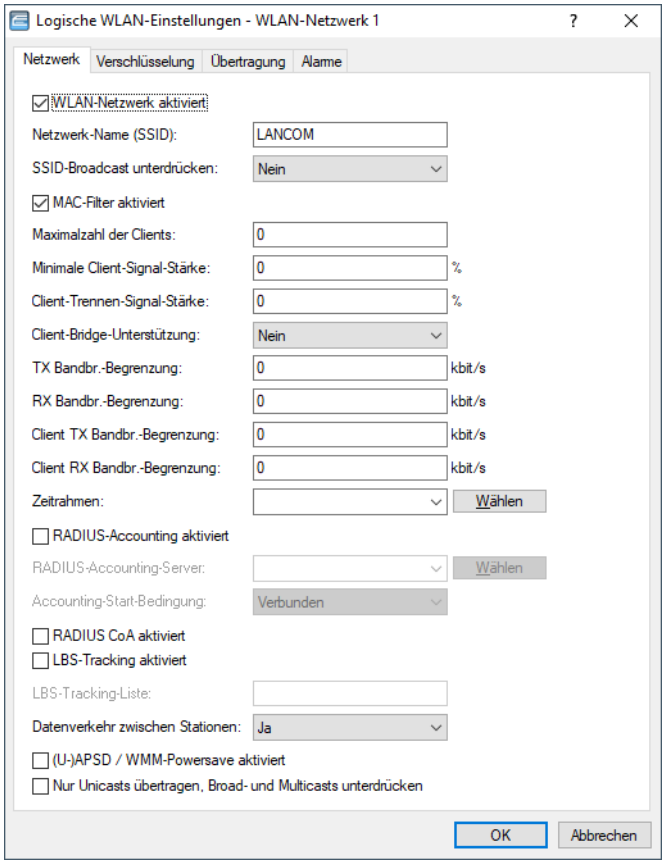
13.18.3 Die logischen WLAN-Schnittstellen

Jede physikalische WLAN-Schnittstelle kann bis zu 16 verschiedene logische Funknetzwerke aufspannen (Multi-SSID). Für jedes dieser Funknetze können bestimmte Parameter speziell definiert werden, ohne dass zusätzliche APs benötigt werden.



13.18.3.1 Netzwerkeinstellungen

Die nachfolgenden Einstellungen nehmen Sie in LANconfig unter **Wireless-LAN** > **Allgemein** > **Logische WLAN-Einstellungen** > **Netzwerk** vor.



WLAN-Netzwerk aktiviert

Mit diesem Schalter aktivieren bzw. deaktivieren Sie das entsprechende logische WLAN.

Netzwerk-Name (SSID)

Bestimmen Sie für jedes benötigte logische Funknetzwerk eine eindeutige SSID (den Netzwerknamen). Nur solche Clients, die über die gleiche SSID verfügen, können sich in diesem Funknetzwerk anmelden.

SSID-Broadcast unterdrücken

Sie können Ihr Funk-LAN entweder in einem öffentlichen oder in einem privaten Modus betreiben. Ein Funk-LAN im öffentlichen Modus kann von Mobilstationen in der Umgebung ohne weiteres kontaktiert werden. Durch Aktivieren der Option **Verschärft** versetzen Sie Ihr Funk-LAN in einen privaten Modus. In dieser Betriebsart sind Mobilstationen ohne Kenntnis des Netzwerknamens (SSID) von der Teilnahme am Funk-LAN ausgeschlossen.

Schalten Sie den „verschärften" Modus ein, wenn Sie verhindern möchten, dass sich WLAN-Clients mit der SSID „Any" oder einer leeren SSID in Ihrem Funknetzwerk anmelden.

Die Option **SSID-Broadcast unterdrücken** ermöglicht folgende Einstellungen:

Nein

Der AP veröffentlicht die SSID der Funkzelle. Sendet ein Client einen Probe Request mit leerer oder falscher SSID, antwortet der AP mit der SSID der Funkzelle (öffentliches WLAN).

Ja

Der AP veröffentlicht die SSID der Funkzelle nicht. Sendet ein Client einen Probe Request mit leerer SSID, antwortet der AP ebenfalls mit einer leeren SSID.

Verschärft

Der AP veröffentlicht die SSID der Funkzelle nicht. Sendet ein Client einen Probe Request mit leerer oder falscher SSID, antwortet der AP überhaupt nicht.

Das einfache Unterdrücken der SSID bietet keinen ausreichenden Zugriffsschutz, da der AP diese bei der Anmeldung berechtigter WLAN-Clients im Klartext überträgt und sie somit für alle im WLAN-Netz befindlichen WLAN-Clients kurzfristig sichtbar ist.

MAC-Filter aktiviert

In der MAC-Filterliste (**Wireless-LAN** > **Stationen/LEPS** > **LEPS-MAC** > **Stationsregeln**) sind die MAC-Adressen der Clients hinterlegt, die sich bei einem AP einbuchen dürfen. Mit dem Schalter **MAC-Filter aktiviert** können Sie die Verwendung der MAC-Filterliste gezielt für einzelne logische Netzwerke ausschalten.

Die Verwendung der MAC-Filterliste ist auf jeden Fall erforderlich für logische Netzwerke, in denen sich die Clients mit einer individuellen Passphrase über LEPS-MAC anmelden. Die bei LEPS-MAC verwendete Passphrase wird ebenfalls in der MAC-Filterliste eingetragen. Für die Anmeldung mit einer individuellen Passphrase beachtet der AP daher immer die MAC-Filterliste, auch wenn Sie diese Option hier deaktivieren.

Maximalzahl der Clients

Legen Sie hier die maximale Anzahl der Clients fest, die sich bei diesem AP einbuchen dürfen. Weitere Clients, die sich über diese Anzahl hinaus anmelden wollen, lehnt der AP ab.

Minimale Client-Signal-Stärke

Mit diesem Eintrag bestimmen Sie den Schwellenwert in Prozent für die minimale Signalstärke für Clients beim Einbuchen. Unterschreitet ein Client diesen Wert, sendet der AP keine Probe-Responses mehr an diesen Client und verwirft die entsprechenden Anfragen.

Ein Client mit schlechter Signalstärke findet den AP somit nicht und kann sich nicht darauf einbuchen. Das sorgt beim Client für eine optimierte Liste an verfügbaren APs, da keine APs aufgeführt werden, mit denen der Client an der aktuellen Position nur eine schwache Verbindung aufbauen könnte.

Client-Trennen-Signal-Stärke

Wenn dieser Schwellenwert unterschritten wird, dann wird der Client disassoziiert. Dadurch lässt sich vermeiden, dass der Client an einer aufgrund der geringen Signalstärke de facto bereits unbrauchbaren WLAN-Verbindung hängen bleibt anstatt auf eine am Client oft ebenfalls verfügbare Mobiltelefon-Verbindung umzuschalten – ein Verhalten, welches sich bei Mobiltelefonen immer wieder beobachten lässt und für den Benutzer ärgerlich ist.

Dieser Schwellenwert funktioniert nur, wenn auch der Wert **Minimale Client-Signal-Stärke** gesetzt ist und außerdem **Client-Trennen-Signal-Stärke** kleiner als dieser Wert ist.

Client-Bridge-Unterstützung

Aktivieren Sie diese Option für einen AP, wenn Sie im WLAN-Client-Modus für eine Client-Station die Client-Bridge-Unterstützung aktiviert haben.

Sie können den Client-Bridge-Modus ausschließlich zwischen zwei LANCOM Geräten verwenden.

TX Bandbr.-Begrenzung

Über diese Einstellung definieren Sie die zur Verfügung stehende Gesamtbandbreite in Senderichtung für die betreffende SSID (Limit in kBit/s). Der Wert `0` deaktiviert die Begrenzung.

RX Bandbr.-Begrenzung

Über diese Einstellung definieren Sie die zur Verfügung stehende Gesamtbandbreite in Empfangsrichtung für die betreffende SSID (Limit in kBit/s). Der Wert `0` deaktiviert die Begrenzung.

Client TX Bandbr.-Begrenzung

Hier begrenzen Sie die Bandbreite (Limit in kBit/s) in Senderichtung, die jedem WLAN-Client auf dieser SSID zur Verfügung steht. Der Wert `0` deaktiviert die Begrenzung.

Client RX Bandbr.-Begrenzung

Hier begrenzen Sie die Bandbreite (Limit in kBit/s) in Empfangsrichtung, die jedem WLAN-Client auf dieser SSID zur Verfügung steht. Der Wert `0` deaktiviert die Begrenzung.

Zeitrahmen

Wählen Sie hier einen der in *Zeitrahmen* auf Seite 1708 definierten Zeitrahmen aus. Über diesen kann die Ausstrahlung dieser SSID auf die dort definierten Zeiten eingeschränkt werden. Somit lässt sich z. B. in einer Schule ein WLAN nur während der Unterrichtszeiten aktivieren.

RADIUS-Accounting aktiviert

Aktivieren Sie die Option, um RADIUS-Accounting für diese SSID einzuschalten.

RADIUS-Accounting-Server

Wenn Sie RADIUS zur zentralen Verwaltung von Konto- und Zugangsinformationen in Ihren WLANs einsetzen, übernimmt standardmäßig der Access Point zentral das Weiterleiten der Anfragen für die Authorisierung und das Accounting an den RADIUS-Server. Sofern Sie für die Verwaltung der Access Points einen WLAN-Controller einsetzen, kann auch der WLAN-Controller die RADIUS-Anfragen von allen angeschlossenen Access Points an den entsprechenden RADIUS-Server weiterleiten.

In manchen Anwendungsfällen möchte der Betreiber von Access Points oder WLAN-Controllern jedoch unterschiedliche RADIUS-Server für einzelne logische WLANs (SSIDs) einsetzen. Das ist z. B. dann der Fall, wenn mehrere Kunden die technische WLAN-Infrastruktur gemeinsam nutzen, dabei jedoch eigene Systeme zur Authentifizierung einsetzen (zum Beispiel bei Wireless as a Service – WaaS).

In diesen Fällen haben Sie die Möglichkeit, für jedes logische WLAN (also jede SSID) ein separates RADIUS-Profil zu wählen. Das RADIUS-Profil enthält alle notwendigen Angaben zur Nutzung der entsprechenden RADIUS-Server inklusive der optionalen Backup-Lösung.

Geben Sie hier einen RADIUS-Accounting-Server für die betreffende SSID an. Die hier auswählbaren Server definieren Sie in der Tabelle **Wireless-LAN** > **Stationen/LEPS** > **RADIUS-Accounting** > **RADIUS-Accounting-Server**.

Accounting-Start-Bedingung

Im Normalfall sendet der WLAN-Stack eine RADIUS-Accounting-Start-Nachricht, sobald der WLAN-Client verbunden ist. Vielfach hat der WLAN-Client zu diesem Zeitpunkt noch keine IP-Adresse, weil sie u. U. vom DHCP-Server noch nicht zur Verfügung gestellt wurde. Das Attribut `Framed-IP-Address` innerhalb der RADIUS-Accounting-Nachricht kann somit nicht sinnvoll befüllt werden.

Verbunden

Das Accounting beginnt mit dem Moment, in dem der WLAN-Client in den Status „Verbunden“ wechselt. Diese Einstellung ist als Standardwert definiert.

Gültige IP-Adresse

Das Accounting beginnt mit dem Moment, in dem der WLAN-Client eine gültige IP-Adresse erhält (IPv4 oder IPv6).

Gültige IPv4-Adresse

Das Accounting beginnt mit dem Moment, in dem der WLAN-Client eine gültige IPv4-Adresse erhält.

Gültige IPv6-Adresse

Das Accounting beginnt mit dem Moment, in dem der WLAN-Client eine gültige IPv6-Adresse erhält.

APIPA-Adressen (`169.254.1.0` bis `169.254.254.255` sowie `fe80:`) werden nicht als gültige IP-Adressen anerkannt.

RADIUS CoA aktiviert

Mit RADIUS CoA (Change of Authorization) ist es möglich, aktuelle WLAN-Sitzungen zu bearbeiten. Dazu übermittelt der jeweilige CoA Client eine CoA Nachricht an das NAS. Diese Nachricht enthält neben der identifizierenden Merkmale für die Session, die Sie ändern möchten, die zu bearbeitenden Attribute und deren neue Werte.

Zudem besteht die Möglichkeit, die jeweilige Sitzung zu trennen. Dies erfolgt durch eine Disconnect Message (DM), die an das NAS gesendet wird – das NAS trennt daraufhin die gewünschte Verbindung.

Weitere Informationen zur Konfiguration von RADIUS CoA finden Sie im Abschnitt *Dynamische Autorisierung mit LANconfig konfigurieren* auf Seite 1608.

LBS-Tracking aktiviert

Diese Option gibt an, ob der LBS-Server die Client-Informationen nachverfolgen darf.

Diese Option konfiguriert das Tracking aller Clients einer SSID. Im Public Spot-Modul bestimmen Sie, ob der LBS-Server die am Public Spot angemeldeten Benutzer tracken darf.

LBS-Tracking-Liste

Mit diesem Eintrag legen Sie den Listennamen für das LBS-Tracking fest. Bei einem erfolgreichen Einbuchen eines Clients in diese SSID überträgt der AP den angegebenen Listennamen, die MAC-Adresse des Clients und die eigene MAC-Adresse an den LBS-Server.

Datenverkehr zwischen Stationen

Aktivieren Sie diese Option, wenn alle Stationen, die an dieser SSID angemeldet sind, untereinander kommunizieren dürfen.

(U-)APSD / WMM-Powersave aktiviert

Aktivieren Sie diese Option, um Stationen die Unterstützung für den Stromsparmechanismus (U-)APSD ([Unscheduled] Automatic Power Save Delivery) zu signalisieren.

(U-)APSD ist im Standard 802.11e verankert und hilft VoWLAN-Geräten dabei, ihre Akkulaufzeit zu erhöhen. Die betreffenden Geräte schalten dafür nach der Anmeldung an einem (U-)APSD-fähigen AP in den Energiesparmodus um. Erhält der AP nun Datenpakete für das betreffende Gerät, speichert es die Daten kurz zwischen und wartet, bis das VoWLAN-Gerät wieder verfügbar ist. Erst dann leitet er die Daten weiter. (U-)APSD erhöht demnach die Latenzzeit des Funkmoduls, wodurch es letztlich weniger Strom verbraucht. Die einzelnen Ruhezeiten können dabei so kurz ausfallen, dass ein VoWLAN-Gerät selbst im Gesprächszustand noch den Stromsparmechanismus benutzen kann. Die betreffenden Geräte müssen (U-)APSD allerdings ebenfalls unterstützen.

Bei WWM (Wi-Fi Multimedia) Power Save handelt es sich um einen Stromsparmechanismus der Wi-Fi Alliance, welcher auf U-APSD basiert. Bestimmte LANCOM APs sind von der Wi-Fi Alliance WMM® Power Save CERTIFIED.

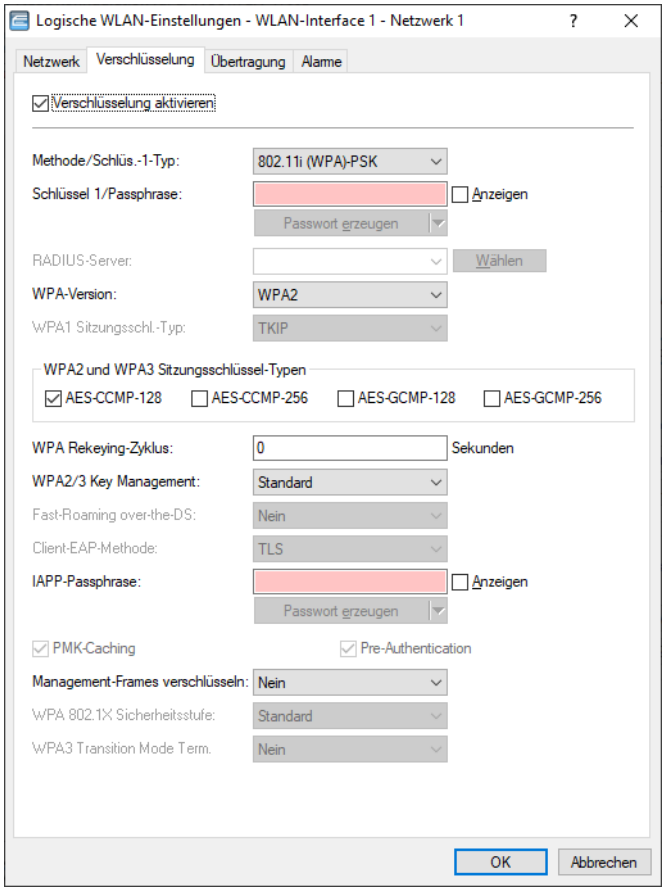
Nur Unicasts übertragen, Broad- und Multicasts unterdrücken

Multi- und Broadcast-Sendungen innerhalb einer WLAN-Funkzelle bedeuten eine Belastung für die Bandbreite dieser Funkzelle, zumal die WLAN-Clients mit diesen Sendungen oft nichts anfangen können. Der AP fängt durch ARP-Spoofing bereits einen Großteil der Multi- und Broadcast-Sendungen in die Funkzelle ab. Mit der Beschränkung auf Unicast-Sendungen filtert er z. B. überflüssige IPv4-Broadcasts wie Bonjour aus den Anfragen heraus.

Die Unterdrückung von Multi- und Broadcast-Sendungen ist zudem eine Forderung der HotSpot-2.0-Spezifikation.

13.18.3.2 Einstellungen für die Verschlüsselung

Die Details für die Verschlüsselung auf dem logischen Interface stellen Sie in LANconfig unter **Wireless-LAN** > **Allgemein** > **Logische WLAN-Einstellungen** > **Verschlüsselung** ein.



Verschlüsselung aktivieren

Aktivieren bzw. deaktivieren Sie die Verschlüsselung für diese WLAN-Schnittstelle.

Methode/Schlüssel-1-Typ

Stellen Sie hier das zu verwendende Verschlüsselungsverfahren ein. Mögliche Werte sind:

802.11i (WPA)-PSK

Die Verschlüsselung nach dem 802.11i-Standard bietet die höchste Sicherheit. Die dabei eingesetzte 128-Bit-AES-Verschlüsselung entspricht der Sicherheit einer VPN-Verbindung. Wählen Sie diese Einstellung, wenn kein RADIUS-Server zur Verfügung steht und die Authentifizierung mit Hilfe eines Preshared Keys erfolgt.

802.11i (WPA)-802.1X

Wenn die Authentifizierung über einen RADIUS-Server erfolgt, wählen Sie diese Option. Achten Sie bei dieser Einstellung darauf, auch den RADIUS-Server bei den 802.1X-Einstellungen zu konfigurieren.

WEP 152, WEP 128, WEP 64

Verschlüsselung nach dem WEP-Standard mit Schlüssellängen von 128, 104 bzw. 40 Bit. Diese Einstellung sollte nur genommen werden , wenn die verwendeten WLAN-Clients die modernen Verfahren nicht unterstützen.

WEP 152-802.1X, WEP 128-802.1X, WEP 64-802.1X

Verschlüsselung nach dem WEP-Standard mit Schlüssellängen von 128, 104 bzw. 40 Bit und zusätzlicher Authentifizierung über 802.1X/EAP. Auch diese Einstellung kommt i.d.R. dann zum Einsatz, wenn die verwendete Hardware der WLAN-Clients den 802.11i-Standard nicht unterstützt. Durch die 802.1X/EAP-Authentifizierung bietet diese Einstellung eine höhere Sicherheit als eine reine WEP-Verschlüsselung.

Enhanced Open

Hotspots werden bisher hauptsächlich unverschlüsselt betrieben, wodurch auf der Funkschnittstelle keinerlei Vertraulichkeit der übertragenen Daten gegeben ist. Auch die verbreitete Praxis, einen Hotspot mit WPA2-PSK abzusichern und den gemeinsamen Schlüssel etwa durch einen Aushang bekannt zu machen, bietet nur eingeschränkte Sicherheit – Da WPA2-PSK keine Perfect Forward Secrecy bietet, kann ein Angreifer, dem dieser Schlüssel bekannt ist, nachträglich damit abgesicherten Datenverkehr entschlüsseln. Das Enhanced Open-Verfahren kann verwendet werden, um diese Risiken zu minimieren. Es bietet verschlüsselte Kommunikation für alle Clients, die dieses Verfahren unterstützen, so dass nicht jeder in der gleichen Funkzelle alles einfach mitlesen kann. Es bleibt das Risiko einer Man-in-the-Middle-Attacke, aber im Vergleich zu einem unverschlüsselten offenen Hotspot ist es ein deutlich geringeres Risiko. Es muss nur die Verschlüsselungsmethode eingestellt werden. Mehr ist nicht notwendig, um die Kommunikation mit Clients, dieses Verfahren unterstützen, zu verschlüsseln. Zur Verwendung von Enhanced Open bei Public Spot siehe auch *Einrichtung eines sicheren Hotspots mit Enhanced Open* auf Seite 1398.

Enhanced Open Transitional

Der Enhanced Open Transition Mode kann verwendet werden, um gleichzeitig Clients anzubinden, die bereits Enhanced Open unterstützen, sowie solche, die noch nicht Enhanced Open unterstützen. Wird der Transition Mode konfiguriert, wird zusätzlich zu der regulären Enhanced Open-SSID automatisch parallel eine unverschlüsselte / offene SSID mit gleichem Namen und identischen sonstigen Einstellungen aktiviert.

Hierfür ist es erforderlich, dass auf dem gewählten Radio-Modul noch mindestens eine weitere SSID zu diesem Zeitpunkt unbelegt / nicht in Nutzung ist. Je nach Gerät stehen je Radio-Modul insgesamt 15 oder 16 SSIDs zur Verfügung. Steht keine SSID zur Verfügung, wird sowohl die offene Transition-SSID, als auch die eigentliche Enhanced Open-SSID nicht aktiviert.

Schlüssel-1/Passphrase

Je nach eingestelltem Verschlüsselungsverfahren können Sie hier einen speziellen WEP-Schlüssel für das jeweilige logische WLAN-Interface bzw. eine Passphrase bei der Verwendung von WPA-PSK eintragen:

- Die Passphrase – also das „Passwort" für das WPA-PSK-Verfahren – wird als Kette aus mindestens 8 und maximal 63 ASCII-Zeichen eingetragen.

  Bitte beachten Sie, dass die Sicherheit des Verschlüsselungssystems bei der Verwendung einer Passphrase von der vertraulichen Behandlung dieses Kennworts abhängt. Die Passphrase sollte nicht einem größeren Anwenderkreis bekannt gemacht werden.

- Der WEP-Schlüssel-1, der nur speziell für das jeweilige logische WLAN-Interface gilt, kann je nach Schlüssellänge unterschiedlich eingetragen werden. Die Regeln für die Eingabe der Schlüssel finden Sie bei der Beschreibung der WEP-Gruppenschlüssel.

RADIUS-Server

Wenn Sie RADIUS zur zentralen Verwaltung von Konto- und Zugangsinformationen in Ihren WLANs einsetzen, übernimmt standardmäßig der Access Point zentral das Weiterleiten der Anfragen für die Authorisierung und das Accounting an den RADIUS-Server. Sofern Sie für die Verwaltung der Access Points einen WLAN-Controller einsetzen, kann auch der WLAN-Controller die RADIUS-Anfragen von allen angeschlossenen Access Points an den entsprechenden RADIUS-Server weiterleiten.

In manchen Anwendungsfällen möchte der Betreiber von Access Points oder WLAN-Controllern jedoch unterschiedliche RADIUS-Server für einzelne logische WLANs (SSIDs) einsetzen. Das ist z. B. dann der Fall, wenn mehrere Kunden die technische WLAN-Infrastruktur gemeinsam nutzen, dabei jedoch eigene Systeme zur Authentifizierung einsetzen (zum Beispiel bei Wireless as a Service – WaaS).

In diesen Fällen haben Sie die Möglichkeit, für jedes logische WLAN (also jede SSID) ein separates RADIUS-Profil zu wählen. Das RADIUS-Profil enthält alle notwendigen Angaben zur Nutzung der entsprechenden RADIUS-Server inklusive der optionalen Backup-Lösung.

Wenn Sie unter **Methode/Schlüssel-1-Typ** eine Authentifizierung nach dem Standard IEEE 802.1X auswählen, geben Sie hier das Profil eines RADIUS-Servers an.

WPA-Version

WPA-Version, die der Access Point den WLAN-Clients zur Verschlüsselung anbietet.

WPA1

Nur WPA1

WPA2

Nur WPA2

WPA1/2

Sowohl WPA1 als auch WPA2 in einer SSID (Funkzelle)

WPA2/3

Sowohl WPA2 als auch WPA3 in einer SSID (Funkzelle)

WPA3

Nur WPA3

WPA1/2/3

WPA1, WPA2 und WPA3 in einer SSID (Funkzelle)

WPA1 Sitzungs-Schlüssel-Typ

Wenn als Verschlüsselungsmethode '802.11i (WPA)-PSK' eingestellt wurde, kann hier das Verfahren zur Generierung des Sitzungs- bzw. Gruppenschlüssels für WPA1 ausgewählt werden:

AES

Es wird das AES-Verfahren verwendet.

TKIP

Es wird das TKIP-Verfahren verwendet.

AES/TKIP

Es wird das AES-Verfahren verwendet. Falls die Client-Hardware das AES-Verfahren nicht unterstützt, wird TKIP eingesetzt.

WPA2 und WPA3 Sitzungs-Schlüssel-Typen

Wählen Sie hier die Verfahren aus, welche zur Generierung der WPA2- bzw. WPA3-Sitzungs- bzw. -Gruppen-Schlüssel angeboten werden sollen. Es können die folgenden Verfahren des Advanced Encryption Standard (AES) angeboten werden: AES-CCMP-128, AES-CCMP-256, AES-GCMP-128, AES-GCMP-256.

WPA Rekeying-Zyklus

Konfigurieren Sie hier die Zeit in Sekunden, nach der der Access Point bei Verwendung einer WPA-Version einen Austausch der verwendeten Schlüssel durchführt. In der Standardeinstellung ist der Wert auf „0" eingestellt, so dass keine erneute Aushandlung des Schlüssels erfolgt.

WPA2/3 Key Management

Bestimmen Sie hier, nach welchem Standard das WPA2/3-Schlüsselmanagement funktionieren soll. Mögliche Werte sind:

Standard

Aktiviert das Schlüsselmanagement gemäß dem Standard IEEE 802.11i ohne Fast Roaming und mit SHA-1-basierten Schlüsseln. Die WLAN-Clients müssen in diesem Fall je nach Konfiguration Opportunistic Key Caching, PMK Caching oder Pre-Authentifizierung verwenden.

Fast Roaming

Aktiviert Fast Roaming über 802.11r

SHA256

Aktiviert das Schlüsselmanagement gemäß dem Standard IEEE 802.11w mit SHA-256-basierten Schlüsseln.

Kombinationen dieser drei Einstellungen

Aktiviert eine entsprechende Kombination.

Obwohl eine Mehrfachauswahl möglich ist, sollten Sie diese nur vornehmen, wenn sichergestellt ist, dass sich nur entsprechend geeignete Clients am AP anmelden wollen. Ungeeignete Clients verweigern ggf. eine Verbindung, wenn eine andere Option als **Standard** aktiviert ist.

Fast-Roaming over-the-DS

Mit Fast Roaming over-the-DS (Distribution System) können Sie eine Option des Standards IEEE 801.11r aktivieren, der sich die Verbindung der Access Points über LAN zunutze macht. Der Wechselwunsch wird an den Access Point gesendet, mit dem der Client noch verbunden ist. Dieser leitet den Wunsch an den neuen Access Point weiter und der Wechsel wird durchgeführt. Dies beschleunigt den Wechsel im Vergleich zur normalen „Over-the-Air fast transition" nochmals deutlich, was insbesondere Echtzeitanwendungen wie z. B. VoIP zugute kommt.

Client-EAP-Methode

APs in der Betriebsart als WLAN-Client können sich über EAP/802.1X bei einem anderen AP authentifizieren. Zur Aktivierung der EAP/802.1X-Authentifizierung im Client-Modus wird bei den Verschlüsselungsmethoden für das erste logische WLAN-Netzwerk die Client-EAP-Methode ausgewählt.

Beachten Sie, dass die gewählte Client-EAP-Methode zu den Einstellungen des Access Points passen muss, bei dem sich der AP einbuchen will.

Beachten Sie neben der Einstellung der Client-EAP-Methode auch die entsprechende Einstellung der Betriebsart als WLAN-Client. Bei anderen logischen WLAN-Netzwerken als WLAN-1 ist die Einstellung der Client-EAP-Methode ohne Funktion.

IAPP-Passphrase

Diese Passphrase wird verwendet, um verschlüsseltes Opportunistic Key Caching zu realisieren. Siehe *Opportunistic Key Caching (OKC)* auf Seite 1010.

PMK-Caching

Beim Verbindungsaufbau eines WLAN-Clients zu einem AP handeln die beiden Gegenstellen im Rahmen der 802.1X-Authentifizierung einen gemeinsamen Schlüssel für die nachfolgende Verschlüsselung aus, den Pairwise Master Key (PMK). Bei Anwendungen mit bewegten WLAN-Clients (Notebooks in größeren Büro-Umgebungen, bewegte Objekte mit WLAN-Anbindung im Industriebereich, Smartphones) wechseln die WLAN-Clients häufig den AP, bei dem sie sich in einem WLAN-Netz anmelden. Die WLAN-Clients roamen also zwischen verschiedenen, aber in der Regel immer den gleichen APs hin und her.

APs speichern üblicherweise einen ausgehandelten PMK für eine bestimmte Zeit. Auch ein WLAN-Gerät in der Betriebsart als WLAN-Client speichert den PMK. Sobald ein WLAN-Client einen Anmeldevorgang bei einem AP startet, zu dem zuvor schon einer Verbindung bestand, kann der WLAN-Client direkt den vorhandenen PMK zur Prüfung an den AP übermitteln. Die beiden Gegenstellen überspringen so die Phase der PMK-Aushandlung während des Verbindungsaufbaus, WLAN-Client und AP stellen die Verbindung deutlich schneller her.

Pre-Authentication

Die schnelle Authentifizierung über den Pairwise Master Key (PMK) funktioniert nur, wenn der WLAN-Client sich bereits zuvor am AP angemeldet hat. Um die Dauer für die Anmeldung am AP schon beim ersten Anmeldeversuch zu verkürzen, nutzt der WLAN-Client die Prä-Authentifizierung.

Normalerweise scannt ein WLAN-Client im Hintergrund die Umgebung nach vorhandenen APs, um sich ggf. mit einem von ihnen neu verbinden zu können. APs, die WPA2/802.1X unterstützen, können ihre Fähigkeit zur Prä-Authentifizierung den anfragenden WLAN-Clients mitteilen. Eine WPA2-Prä-Authentifizierung unterschiedet sich dabei von einer normalen 802.1X-Authentifizierung in den folgenden Abläufen:

- Der WLAN-Client meldet sich am neuen AP über das Infrastruktur-Netzwerk an, das die APs miteinander verbindet. Das kann eine Ethernet-Verbindung, ein WDS-Link (Wireless Distribution System) oder eine Kombination beider Verbindungen sein.
- Ein abweichendes Ethernet-Protokoll (EtherType) unterscheidet eine Prä-Authentifizierung von einer normalen 802.1X-Authentifizierung. Damit behandeln der aktuelle AP sowie alle anderen Netzwerkpartner die Prä-Authentifizierung als normale Datenübertragung des WLAN-Clients.
- Nach erfolgreicher Prä-Authentifizierung speichern jeweils der neue AP und der WLAN-Client den ausgehandelten PMK.

  Die Verwendung von PMKs ist eine Voraussetzung für Prä-Authentifizierung. Andernfalls ist eine Prä-Authentifizierung nicht möglich.
- Sobald der Client sich später mit dem neuen AP verbinden möchte, kann er sich dank des gespeicherten PMKs schneller anmelden. Der weitere Ablauf entspricht dem PMK-Caching.

Client-seitig ist die Anzahl gleichzeitiger Prä-Authentifizierungen auf vier begrenzt, um in Netzwerk-Umgebungen mit vielen APs die Netzlast für den zentralen RADIUS-Server gering zu halten.

Management-Frames verschlüsseln

Die in einem WLAN übertragenen Management-Informationen zum Aufbau und Betrieb von Datenverbindungen sind standardmäßig unverschlüsselt. Jeder innerhalb einer WLAN-Zelle kann diese Informationen empfangen und auswerten, selbst wenn er nicht an einem Access Point angemeldet ist. Das birgt zwar keine Gefahren für eine verschlüsselte Datenverbindung, kann aber die Kommunikation innerhalb einer WLAN-Zelle durch gefälschte Management-Informationen empfindlich stören.

Der Standard IEEE 802.11w verschlüsselt die übertragenen Management-Informationen (Protected Management Frames, PMF), so dass ein Angreifer, der nicht im Besitz des entsprechenden Schlüssels ist, die Kommunikation nicht mehr stören kann.

Ab WPA3 müssen Management Frames verschlüsselt werden. Bei WPA2 ist diese Option optional.

WPA 802.1X Sicherheitsstufe

Bei WPA3-Enterprise kann zusätzlich die Unterstützung für Commercial National Security Algorithm (CNSA) Suite B-Kryptographie eingeschaltet werden, welche ein optionaler Teil von WPA3-Enterprise für Hochsicherheitsumgebungen ist. Suite B stellt sicher, dass alle Glieder in der Verschlüsselungskette aufeinander abgestimmt sind. Suite B bildet Klassen von Bitlängen für Hash-, symmetrische und asymmetrische Verschlüsselungsverfahren, die passende Schutzniveaus bieten. So passt zum Beispiel zu AES mit 128 Bit ein SHA-2-Hash mit 256 Bit. Wenn Suite B zum Einsatz kommt, ist die Unterstützung aller anderen Kombinationen ausdrücklich ausgeschlossen. In der Verschlüsselungskette gibt es folglich nur noch gleich starke Glieder.

Weitere Informationen zu CNSA Suite B finden Sie unter folgendem Link: *CNSA Algorithm Suite Factsheet*

Mit dem Schalter **WPA 802.1X Sicherheitsstufe** unter **Wireless-LAN** > **Allgemein** > **Interfaces** > **Logische WLAN-Einstellungen** kann die Suite B-Kryptographie optional eingeschaltet werden. Wird die Unterstützung für „Suite B 192 Bits“ eingeschaltet, werden die folgenden EAP Cipher-Suiten erzwungen:

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

Andere Cipher-Suiten können nicht verwendet werden. Ebenfalls wird eine Mindest-Schlüssellänge von 3072 Bit für die RSA- und Diffie-Hellman-Schlüsselaustauschverfahren, sowie 384 Bit für die ECDSA- und ECDHE-Schlüsselaustauschverfahren erzwungen. Zusätzlich wird der Sitzungschlüssel-Typ AES-GCMP-256 erzwungen.

Werden diese Cipher-Suiten von den verwendeten WLAN-Clients oder der restlichen Infrastruktur (z. B. RADIUS-Server) nicht unterstützt, dann ist keine Verbindung möglich!

Wird die Unterstützung für „Suite B 128 Bits“ eingeschaltet, werden die folgenden EAP Cipher-Suiten erzwungen:

- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

Andere Cipher-Suiten können nicht verwendet werden. Ebenfalls wird eine Mindest-Schlüssellänge von 3072 Bit für die RSA- und Diffie-Hellman-Schlüsselaustauschverfahren, sowie 384 Bit für die ECDSA- und ECDHE-Schlüsselaustauschverfahren erzwungen. Zusätzlich wird der Sitzungschlüssel-Typ AES-GCMP-128 erzwungen.

Da die Sitzunggschlüssel-Typen AES-GCMP-128 und AES-GCMP-256 nicht von allen WLAN-Modulen unterstützt werden, kann die Verwendung der Suite B-Kryptographie je nach Gerätetyp eingeschränkt oder nicht möglich sein.

Werden diese Cipher-Suiten von den verwendeten WLAN-Clients oder der restlichen Infrastruktur (z. B. RADIUS-Server) nicht unterstützt, dann ist keine Verbindung möglich!

Diese Option wird nur angezeigt, wenn sie vom Gerät unterstützt wird.

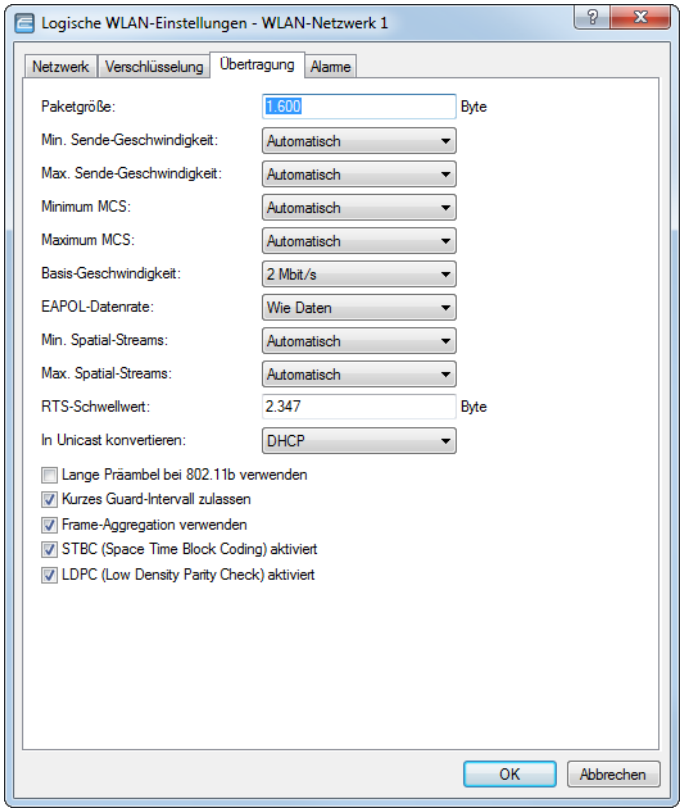
WPA3 Transition Mode Term.

Durch Setzen des Schalters wird WLAN-Clients über ein zusätzliches Info-Element explizit signalisiert, dass im gemischten WPA2/3-Modus die WPA3-PSK (SAE)-Verschlüsselungsmethode unterstützt wird. Unterstützt der Client seinerseits das „Transition Mode Termination“-Feature, wird er für das Einbuchen an dieser SSID

immer WPA3-PSK (SAE) verwenden. So wird ein Downgrade auf WPA2-PSK, was im gemischten WPA2/3-Modus ansonsten ebenfalls erlaubt ist, ausgeschlossen.

13.18.3.3 Einstellungen für die Übertragung

Die Details für die Übertragung auf dem logischen Interface stellen Sie in LANconfig unter **Wireless-LAN** > **Allgemein** > **Logische WLAN-Einstellungen** > **Übertragung** ein.



Paketgröße

Bei kleinen Datenpaketen ist die Gefahr für Übertragungsfehler geringer als bei großen Paketen, allerdings steigt auch der Anteil der Header-Informationen am Datenverkehr, die effektive Nutzlast sinkt also. Erhöhen Sie den voreingestellten Wert nur, wenn das Funknetzwerk überwiegend frei von Störungen ist und nur wenig Übertragungsfehler auftreten. Reduzieren Sie den Wert entsprechend, um die Übertragungsfehler zu vermeiden.

Minimale und maximale Geschwindigkeit

Der AP handelt mit den angeschlossenen WLAN-Clients die Geschwindigkeit für die Datenübertragung normalerweise fortlaufend dynamisch aus. Dabei passt der AP die Übertragungsgeschwindigkeit an die Empfangslage an. Alternativ können Sie hier die minimalen und maximalen Übertragungsgeschwindigkeiten fest vorgeben, wenn Sie die dynamische Geschwindigkeitsanpassung verhindern wollen.

Modulation Coding Scheme (MCS) (Nur verfügbar für 802.11n)

Eine bestimmte MCS-Nummer bezeichnet eine eindeutige Kombination aus Modulation der Einzelträger (BPSK, QPSK, 16QAM, 64QAM), Coding-Rate (d. h. Anteil der Fehlerkorrekturbits an den Rohdaten) und Anzahl der Spatial Streams. 802.11n verwendet diesen Begriff anstelle von „Datenrate“ bei älteren WLAN-Standards, weil die Rate keine eindeutige Beschreibung mehr ist.

MCS-Index	Datenströme	Modulation	Coding-Rate	Datendurchsatz (GI=0,4 s, 40 MHz)
0	1	BPSK	1/2	15
1	1	QPSK	1/2	30
2	1	QPSK	3/4	45
3	1	16QAM	1/2	60
4	1	16QAM	3/4	90
5	1	64QAM	1/2	120
6	1	64QAM	3/4	135
7	1	64QAM	5/6	150
8	2	BPSK	1/2	30
9	2	QPSK	1/2	60
10	2	QPSK	3/4	90
11	2	16QAM	1/2	120
12	2	16QAM	3/4	180
13	2	64QAM	1/2	240
14	2	64QAM	3/4	270
15	2	64QAM	5/6	300

Die Auswahl des MCS gibt also an, welche Modulationsparameter bei einem oder zwei Spatial-Datenströmen minimal bzw. maximal verwendet werden sollen. Innerhalb dieser Grenzen wird das passende MCS je nach den vorliegenden Bedingungen beim Verbindungsaufbau gewählt und während der Verbindung bei Bedarf angepasst. Damit wird auch der maximal erreichbare Datendurchsatz definiert, der in der letzten Spalte der Tabelle angegeben ist (hier für das kurze Guard-Intervall GI = 0,4 s mit Nutzung des 40 MHz-Kanals).

Basis-Geschwindigkeit

Die eingestellte Basis-Geschwindigkeit sollte es auch unter ungünstigen Bedingungen erlauben, die langsamsten Clients im WLAN zu erreichen. Stellen Sie hier nur dann eine höhere Geschwindigkeit ein, wenn alle Clients in diesem logischen WLAN auch "schneller" zu erreichen sind. Bei automatischer Festlegung der Übertragungsrate sammelt der AP die Informationen über die Übertragungsraten der einzelnen WLAN-Clients. Die Rate teilen die Clients dem AP automatisch bei jeder Unicast-Kommunikation mit. Aus der Liste der angemeldeten Clients wählt der AP nun ständig die jeweils niedrigste Übertragungsrate aus und überträgt damit die Multicast- und Broadcast-Sendungen.

EAPOL-Datenrate (EAP over LAN)

WLAN-Clients nutzen EAPOL zur Anmeldung an APs über WPA und 802.1X. Dazu kapseln sie die EAP-Pakete zum Austausch der Authentifizierungs-Informationen in Ethernet-Frames, um die EAP-Kommunikation über eine Layer-2-Verbindung zu ermöglichen

In manchen Fällen ist es sinnvoll, die Datenrate für die Übertragung der EAPOL-Pakete niedriger zu wählen als die Datenrate für die Nutzdaten. Bei beweglichen WLAN-Clients kann z. B. eine zu hohe Datenrate der EAPOL-Pakete zu Paketverlusten führen und so den Anmeldevorgang deutlich verzögern. Durch die gezielte Auswahl der EAPOL-Datenrate verläuft dieser Vorgang stabiler.

Die Standard-Auswahl "Wie Daten" behandelt EAPOL-Pakete wie normale Datenpakete und wählt die für Datenpakete übliche Übertragungsrate bzw. aktiviert die für Datenpakete übliche Ratenadaption.

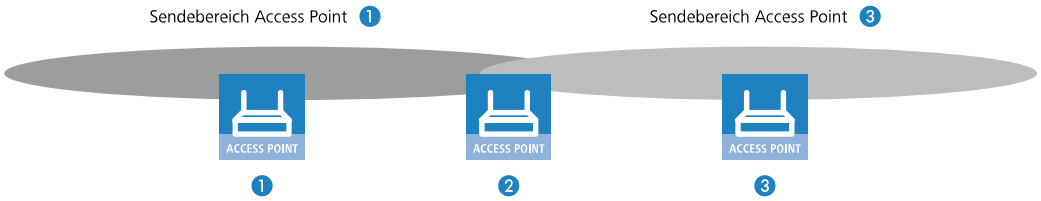
Anzahl Spatial-Streams (Nur verfügbar für 802.11n)

Mit der Funktion des Spatial-Multiplexing können mehrere separate Datenströme über separate Antennen übertragen werden, um so den Datendurchsatz zu verbessern. Der Einsatz dieser Funktion ist nur dann zu empfehlen, wenn die Gegenstelle die Datenströme mit entsprechenden Antennen verarbeiten kann.

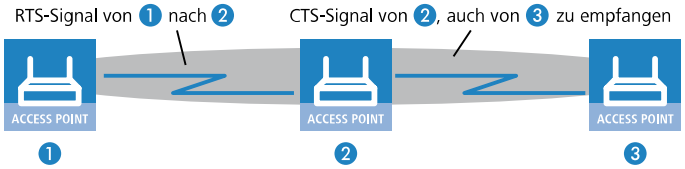
Mit der Einstellung 'Auto' werden alle Spatial-Streams genutzt, die von dem jeweiligen WLAN-Modul unterstützt werden.

RTS-Schwellwert

Mit dem RTS-Schwellenwert wird das Phänomen der „Hidden-Station" vermieden.



Dabei sind drei APs **1**, **2**, und **3** so positioniert, dass zwischen den beiden äußeren Geräten keine direkte Funkverbindung mehr möglich ist. Wenn nun **1** ein Paket an **2** sendet, bemerkt **3** diesen Vorgang nicht, da er außerhalb des Sendebereichs von **1** steht. **3** sendet also möglicherweise während der laufenden Übertragung von **1** ebenfalls ein Paket an **2**, denn **3** hält das Medium (in diesem Falle die Funkverbindung) für frei. Es kommt zur Kollision, keine der beiden Übertragungen von **1** oder **3** nach **2** ist erfolgreich. Um diese Kollisionen zu vermeiden, wird das RTS/CTS-Protokoll eingesetzt.



Dazu schickt **1** vor der eigentlichen Übertragung ein RTS-Paket an **2**, das **2** mit einem CTS beantwortet. Das von **2** ausgestrahlte CTS ist jetzt aber in „Hörweite" von **3**, so dass **3** mit seinem Paket an **2** warten kann. Die RTS- und CTS-Signale beinhalten jeweils eine Zeitangabe, wie lange die folgende Übertragung dauern wird.

Eine Kollision bei den recht kurzen RTS-Paketen ist sehr unwahrscheinlich, die Verwendung von RTS/CTS erhöht aber dennoch den Overhead. Der Einsatz dieses Verfahrens lohnt sich daher nur für längere Datenpakete, bei denen Kollisionen wahrscheinlich sind. Mit dem RTS-Schwellenwert wird eingestellt, ab welcher Paketlänge das RTS/CTS eingesetzt werden soll. Der passende Wert ist in der jeweiligen Umgebung im Versuch zu ermitteln.

Der RTS/CTS-Schwellenwert muss auch in den WLAN-Clients entsprechend den Möglichkeiten des Treibers bzw. des Betriebssystems eingestellt werden.

In Unicast konvertieren

Sie haben folgende Optionen für die Umwandlung von Datenströmen in Unicast:

Keine

Es werden keine Datenströme in Unicast umgewandelt.

DHCP

Wandelt Antwort-Nachrichten des DHCP-Servers in Unicasts um, sofern der Server sie als Broadcast versendet hat. Dies steigert die Zuverlässigkeit der Zustellung, da als Broadcast gesendete Datenpakete keinen speziellen

Adressaten, keine optimierten Sendetechniken wie ARP-Spoofing oder IGMP/MLD-Snooping und eine niedrige Datenrate aufweisen.

Multicast

Multicast-Datenströme, die über WLAN-Interfaces übertragen werden sollen, werden nach Aktivierung des Features in einzelne Unicast-Datenströme je Client auf dem MAC-Layer bzw. WLAN-Layer konvertiert. Die Pakete werden zwar je Client dupliziert, können aber, da es sich nun um Unicasts handeln, mit der für diesen Client höchstmöglichen Datenrate übertragen werden. Auch wenn die Pakete nun dupliziert werden, wird durch die viel schnellere Übertragung in den meisten Szenarien insgesamt deutlich weniger Airtime verbraucht, die dann für andere Übertragungen zur Verfügung steht.

Damit das Feature funktioniert ist es erforderlich, das IGMP-Snooping auf dem Gerät zu aktivieren und korrekt zu konfigurieren Über das IGMP-Snooping ermittelt das Gerät, welcher Client welchen Multicast-Strom empfangen möchte. Der Multicast-Konvertierung stehen somit die passenden Ziel-Clients bzw -Adressen für die Konvertierung zur Verfügung.

DHCP und Multicast

Wandelt DHCP- und Multicast-Datenstöme in Unicast um.

Lange Präambel bei 802.11b verwenden

Normalerweise handeln die Clients im 802.11b-Modus die Länge der zu verwendenden Präambel mit dem AP selbst aus. Stellen Sie hier die „lange Präambel" nur dann fest ein, wenn die Clients diese feste Einstellung verlangen.

Kurzes Guard-Interval zulassen (Nur verfügbar für 802.11n)

Mit dieser Option wird die Sendepause zwischen zwei Signalen von 0,8 s (Standard) auf 0,4 s (Short Guard Interval) reduziert. Dadurch steigt die effektiv für die Datenübertragung genutzte Zeit und damit der Datendurchsatz. Auf der anderen Seite wird das WLAN-System anfälliger für Störungen, welche durch die Interferenzen zwischen zwei aufeinanderfolgenden Signalen auftreten können.

Im Automatik-Modus wird das kurze Guard-Intervall aktiviert, sofern die jeweilige Gegenstelle diese Betriebsart unterstützt. Alternativ kann die Nutzung des kurzen Guard-Intervalls auch ausgeschaltet werden.

Frame-Aggregation verwenden (Nur verfügbar für 802.11n)

Bei der Frame-Aggregation werden mehrere Datenpakete (Frames) zu einem größeren Paket zusammengefasst und gemeinsam versendet. Durch dieses Verfahren kann der Overhead der Pakete reduziert werden, der Datendurchsatz steigt.

Die Frame-Aggregation eignet sich weniger gut bei schnell bewegten Empfängern oder für zeitkritische Datenübertragungen wie Voice over IP.

STBC (Space Time Block Coding) aktiviert (Nur verfügbar für 802.11n.)

STBC ist ein Kodierverfahren nach IEEE 802.11n. Die Funktion 'STBC' (Space Time Block Coding) variiert den Versand von Datenpaketen zusätzlich über die Zeit, um auch zeitliche Einflüsse auf die Daten zu minimieren. Durch den zeitlichen Versatz der Sendungen besteht für den Empfänger eine noch bessere Chance, fehlerfreie Datenpakete zu erhalten, unabhängig von der Anzahl der Antennen. Dadurch kommt es in einem MIMO-System zu besseren Empfangsbedingungen.

LDPC (Low Density Parity Check) aktiviert (Nur verfügbar für 802.11n.)

LDPC ist eine Methode zur Fehlerkorrektur. IEEE 802.11n nutzt als Standard-Methode zur Fehlerkorrektur Convolution Coding (CC) und ermöglicht optional jedoch auch eine Fehlerkorrektur nach der effektiveren LDPC-Methode.

Im Unterschied zur CC-Kodierung nutzt die LDPC-Kodierung größere Datenpakete zur Checksummenberechnung und kann zusätzlich mehr Bit-Fehler erkennen. Die LDPC-Kodierung ermöglicht also bereits durch ein besseres Verhältnis von Nutz- zu Checksummen-Daten eine höhere Datenübertragungsrate.

Hard-Retries (Nur im WEBconfig)

Dieser Wert gibt an, wie oft die Hardware versuchen soll, Pakete zu verschicken, bevor sie als Tx-Fehler gemeldet werden. Kleinere Werte ermöglichen es so, dass ein nicht zu versendendes Paket den Sender weniger lange blockiert.

Soft-Retries (Nur mit WEBconfig)

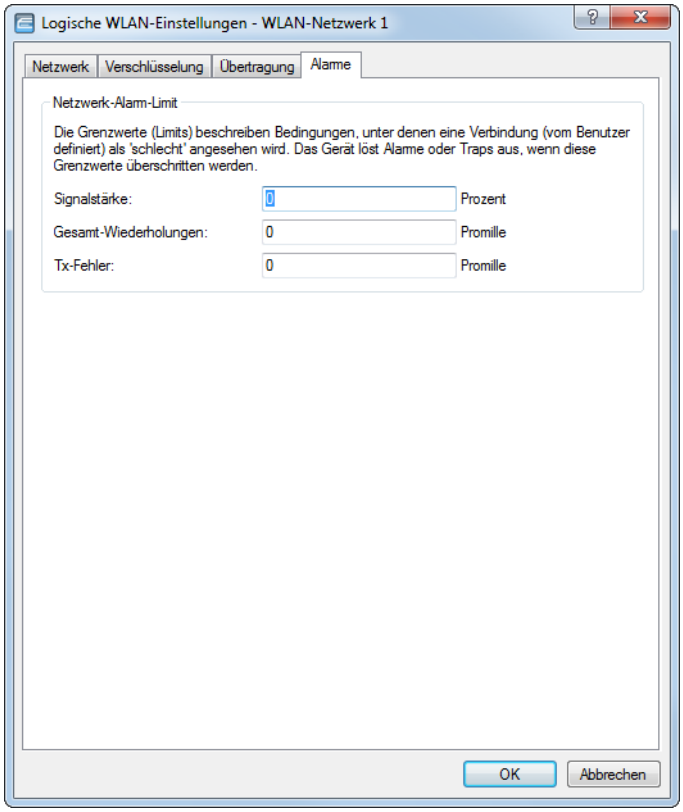
Wenn ein Paket von der Hardware nicht verschickt werden konnte, wird mit der Anzahl der Soft-Retries festgelegt, wie oft der gesamte Sendeversuch wiederholt werden soll.

Die Gesamtzahl der Versuche ist also (Soft-Retries + 1) * Hard-Retries.

Der Vorteil von Soft-Retries auf Kosten von Hard-Retries ist, dass aufgrund des Raten-Adaptionalgorithmus die nächste Serie von Hard-Retries direkt mit einer niedrigeren Rate beginnt.

13.18.3.4 Einstellungen für die Alarme

Die Details für die Alarme auf dem logischen Interface stellen Sie in LANconfig unter **Wireless-LAN** > **Allgemein** > **Logische WLAN-Einstellungen** > **Alarme** ein.



Typische Situationen, welche sich im WLAN-Umfeld meist für Probleme verantwortlich zeigen, sind ein Absinken der Signalstärke unter einen gewissen Grenzwert, der Prozentsatz der Anzahl an verlorenen Paketen überschreitet einen gewissen Grenzwert oder Pakete müssen sehr oft erneut versendet werden, was die effektiv zur Verfügung stehende Bandbreite stark reduziert.

Um diese Situationen zu erkennen und darauf zu reagieren bietet LANCOM auf WLAN Geräten diverse Konfigurationsmöglichkeiten für Grenzwerte, die beim Über- bzw. Unterschreiten einen Alarm auslösen.

Eine Verbindung wird nicht absolut als schlecht bewertet, die Bewertung hängt immer von den Parametern ab, die angegeben werden. Hierbei ist insbesondere zu beachten, dass zu hohe oder zu niedrige Grenzwerte eine Verbindung auch falsch bewerten können und unnötige Alarme in einer sehr großen Anzahl erzeugen können.

Ein gewisses Mass an Paketverlusten und eine schwankende Signalstärke sind auch bei stabilen WLAN-Verbindungen zu erwarten.

Es können hier die Grenzwerte für die einzelnen SSIDs eingestellt werden. Für Punkt-zu-Punkt-Verbindungen eines APs lassen+ sich ebenfalls Grenzwerte festlegen. Diese werden zur Bewertung der Verbindung jedes Clients zu der entsprechenden SSID und bei der Verbindung zu einem entsprechenden P2P-Partner genutzt.

Signalstärke

Der Parameter gibt das Minimum der erforderlichen Signalstärke in Prozent an. Der Alarm wird ausgelöst, wenn die Signalstärke unter den konfigurierten Wert fällt. Ein Alarm-Limit muss zwischen 1 und 100 liegen. Die Null schaltet den Alarm ab.

Im Falle von Client- und P2P-Verbindungen werden für Beacon- und Daten-Signalstärke separate Werte ausgewertet. Wenn verfügbar, wird das Beacon-Signal für den Vergleich preferiert, weil die Werte aktuell sind, auch wenn gerade kein Datenverkehr auf der Verbindung stattfindet.

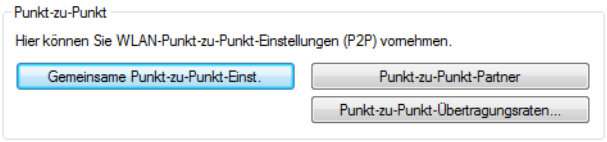
Gesamt-Wiederholungen

Der Parameter gibt den maximalen Grenzwert der Wiederhol-Rate in Promille an. Der Alarm wird ausgelöst, wenn das Verhältnis von Gesamt-Wiederholungen und Tx-Paketen den konfigurierten Wert erreicht. Ein Alarm-Limit muss zwischen 1 und 1000 liegen. Die Null schaltet den Alarm ab.

Tx-Fehler

Der Parameter gibt den maximalen Grenzwert der Transmit-Fehler-Rate in Promille an. Der Alarm wird ausgelöst, wenn das Verhältnis von Tx-Fehlern und Tx-Paketen den konfigurierten Wert erreicht. Ein Alarm-Limit muss zwischen 1 und 1000 liegen. Die Null schaltet den Alarm ab.

13.18.4 Punkt-zu-Punkt

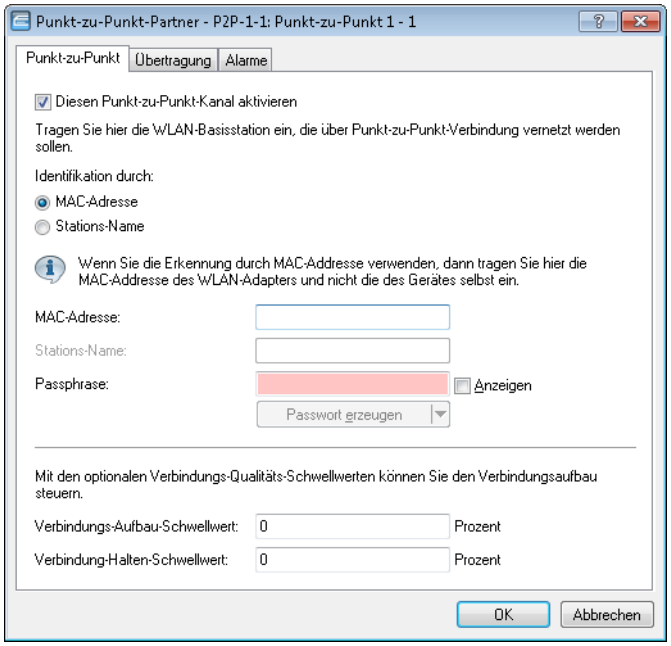


LANconfig: **Wireless LAN** > **Allgemein** > **Punkt-zu-Punkt**

Konfigurieren Sie hier die Einstellungen eines AP für eine Punkt-zu-Punkt-Verbindung. Informationen hierzu finden Sie unter *Aufbau von Punkt-zu-Punkt-Verbindungen* auf Seite 999.

13.18.5 Die Punkt-zu-Punkt-Partner

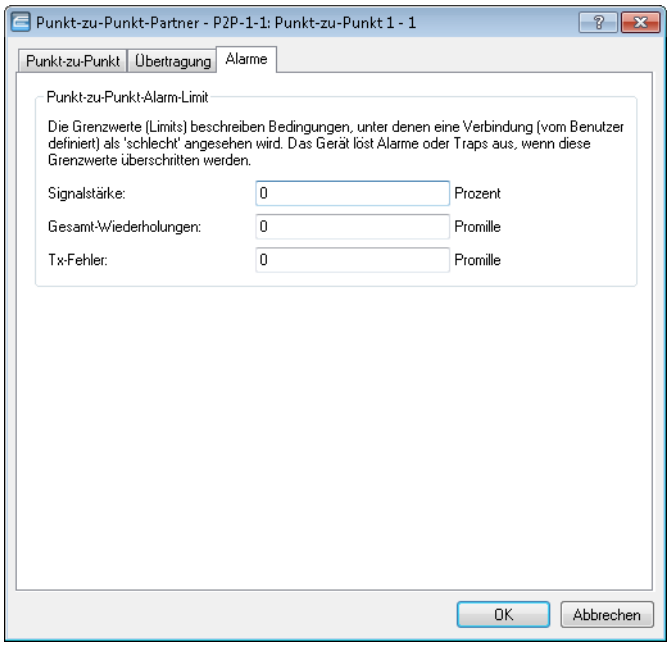
Für jedes WLAN-Modul sind bis zu 16 Punkt-zu-Punkt-Verbindungen aktivierbar. In LANconfig finden Sie diese Einstellungen unter **Wireless-LAN** > **Allgemein** > **Punkt-zu-Punkt** > **Punkt-zu-Punkt-Partner**



Für die Einrichtung einer Punkt-zu-Punkt-Verbindung gehen Sie wie folgt vor:

1. Markieren Sie die Option **Diesen Punkt-zu-Punkt-Kanal aktivieren**.
2. Wählen Sie, ob Sie die P2P-Gegenstelle anhand ihrer **MAC-Adresse** oder ihres **Stations-Namens** identifizieren.
3. Das entsprechende Textfeld wird aktiviert. Geben Sie die MAC-Adresse oder den Stations-Namen ein.

Wenn Sie die Erkennung durch MAC-Addresse verwenden, dann tragen Sie hier die MAC-Addresse des WLAN-Moduls und nicht die des Gerätes selbst ein.



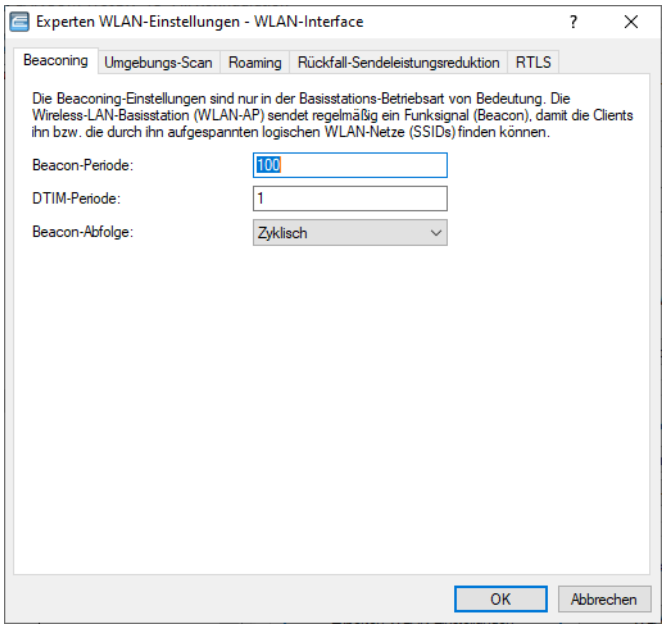
Auf dem Reiter **Alarm** sind Grenzwerte für **Signalstärke**, **Gesamtwiederholungen** und **Tx-Fehler** der Punkt-zu-Punkt-Verbindung definierbar. Bei deren Über-oder Unterschreitung löst der AP Alarme oder Traps aus.

Schließen Sie Ihre Eingaben mit einem Klick auf **OK** ab.

13.18.6 Experten-WLAN-Einstellugnen

13.18.6.1 Die Beaconing-Tabelle

Die Einstellungen in der Beaconing-Tabelle beeinflussen, wie die im AP-Modus vom AP ausgestrahlten Beacons (Leuchtfeuer) versendet werden. Teilweise kann damit das Roaming-Verhalten von Clients beeinflusst werden, teilweise dient dies der Optimierung des MultiSSID-Betriebes für ältere WLAN-Clients.



LANconfig: **Wireless-LAN** > **Allgemein** > **Erweiterte Einstellungen** > **Experten WLAN-Einstellungen** > **Beaconing**

Konsole: **Setup** > **Schnittstellen** > **WLAN** > **Beaconing**

>Beacon-Periode

Dieser Wert gibt den zeitlichen Abstand in K s an, in dem Beacons verschickt werden (1 K s entspricht 1024 Mikrosekunden und stellt eine Recheneinheit des 802.11-Standard dar – 1 K s wird auch als Timer Unit TU bezeichnet). Niedrigere Werte ergebenen kleinere Beacon-Timeout-Zeiten auf dem Client und erlauben damit ein schnelleres Roaming beim AP-Ausfall, erhöhen aber den Overhead auf dem WLAN.

DTIM-Periode

Dieser Wert gibt an, nach welcher Anzahl von Beacons die gesammelten Multicasts ausgesendet werden. Höhere Werte erlauben längere Sleep-Intervalle der Clients, verschlechtern aber die Latenzzeiten.

Beacon-Abfolge

Die Beacon-Abfolge bezeichnet die Reihenfolge, in der die Beacons zu den verschiedenen WLAN-Netzen versendet werden. Wenn z. B. drei logische WLAN-Netze aktiv sind und die Beacon-Periode 100 K s beträgt, so werden alle 100 K s die Beacons für die drei WLANs verschickt. Je nach Beacon-Abfolge werden die Beacons zu folgenden Zeitpunkten versendet:

Zyklisch

In diesem Modus beginnt der AP beim ersten Beacon-Versand (0 K s) mit WLAN-1, gefolgt von WLAN-2 und WLAN-3. Beim zweiten Beacon-Versand (100 K s) wird zuerst WLAN-2 versendet, dann WLAN-3 und erst dann kommt wieder WLAN-1 an die Reihe. Beim dritten Beacon-Versand (200 K s) entsprechend WLAN-3, WLAN-1, WLAN-2 – dann beginnt die Reihe wieder von vorne.

Gestaffelt

In diesem Modus werden die Beacons nicht gemeinsam zu einem Zeitpunkt verschickt, sondern auf die verfügbare Beacon-Periode aufgeteilt. Zum Start bei 0 K s wird nur WLAN-1 verschickt, nach 33,3 K s kommt WLAN-2, nach 66,6 K s WLAN-3 – mit Beginn einer neuen Beacon-Periode startet der Versand wieder mit WLAN-1.

Einfach-Burst

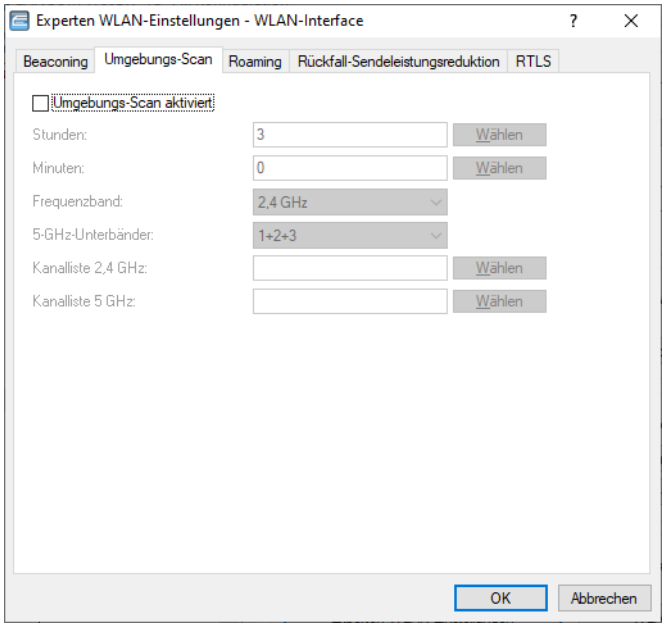
In diesem Modus verschickt der AP die Beacons für die definierten WLAN-Netze immer in der gleichen Abfolge. Beim ersten Beacon-Versand (0 K s) mit WLAN-1, WLAN-2 und WLAN-3, beim zweiten Versand nach dem gleichen Muster und so weiter.

Ältere WLAN-Clients sind manchmal nicht in der Lage, die schnell aufeinander folgenden Beacons richtig zu verarbeiten, wie sie bei einem einfachen Burst auftreten. In der Folge erkennen diese Clients oft nur die ersten Beacons und können sich daher auch nur bei diesem einen Netz einbuchen.

Die gestaffelte Aussendung der Beacons führt zum besten Ergebnis, erhöht aber die Prozessorlast für den AP. Die voreingestellte zyklische Aussendung stellt sich als guter Kompromiss dar, weil hier jedes Netz einmal als erstes ausgesendet wird.

13.18.6.2 Umgebungs-Scan

Die Umgebung Ihres WLAN kann regelmäßig nach Rogue APs abgesucht werden. Siehe hierzu auch *Umgebungsscan zu einer konfigurierbaren Zeit starten* auf Seite 972. Die Einstellugen hierzu sind in LANconfig unter **Wireless-LAN** > **Allgemein** > **Erweiterte Einstellungen** > **Experten WLAN-Einstellungen** > **Umgebungs-Scan**.



Umgebungs-Scan aktiviert

Aktiviert / deaktiviert den Umgebungs-Scan.

Die nachfolgenden Parameter sind ausgegraut, falls der Umgebungs-Scan deaktiviert ist.

Stunden

Enthält den Stundenwert der Uhrzeit für den Umgebungs-Scan.

Minuten

Enthält den Minutenwert der Uhrzeit für den Umgebungs-Scan.

Frequenzband

Enthält die Frequenzbänder für den Umgebungs-Scan.

Mögliche Werte:

2,4 GHz

Das 2,4-GHz-Frequenzband wird gescannt.

5 GHz

Das 5-GHz-Frequenzband wird gescannt.

2,4/5 GHz

Das 2,4-GHz- und das 5-GHz-Frequenzband werden gescannt.

5-GHz-Unterbänder

Enthält die Unterbänder des 5-GHz-Frequenzbandes.

Kanalliste 2,4 GHz

Legt fest, für welche 2,4-GHz-Kanäle der Umgebungs-Scan durchgeführt werden soll.

Falls Sie hier keine Eintragungen vornehmen, wird der Umgebungsscan für sämtliche Kanäle des 2,4-GHz-Frequenzbandes durchgeführt.

Mögliche Werte (Mehrfachauswahl erlaubt):

1 bis 13

In Schritten von 1.

Kanalliste 5 GHz

Legt fest, für welche 5-GHz-Kanäle der Umgebungs-Scan durchgeführt werden soll.

Falls Sie hier keine Eintragungen vornehmen, wird der Umgebungsscan für sämtliche Kanäle des 5-GHz-Frequenzbandes durchgeführt.

Mögliche Werte (Mehrfachauswahl erlaubt):

36 bis 64

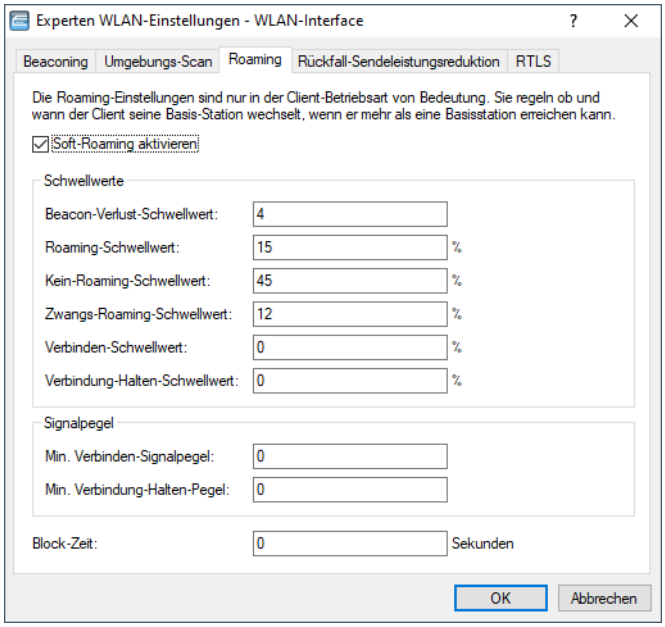
In Schritten von 4.

100 bis 140

In Schritten von 4.

13.18.6.3 Die Roaming-Tabelle

Zur genauen Steuerung, wie sich ein WLAN-Gerät in der Betriebsart 'Client' beim Roaming verhält, dienen verschiedene Schwellenwerte in der Roaming Tabelle.



LANconfig: **Wireless-LAN** > **Allgemein** > **Erweiterte Einstellungen** > **Experten WLAN-Einstellungen** > **Roaming**

Konsole: **Setup** > **Schnittstellen** > **WLAN** > **Roaming**

Soft-Roaming aktivieren

Diese Option ermöglicht dem Client, anhand verfügbarer Scan-Informationen ein Roaming zu einem stärkeren AP durchzuführen (Soft-Roaming). Roaming aufgrund eines Verbindungsverlustes (Hard-Roaming) bleibt davon natürlich unbeeinflusst. Die eingestellten Roaming-Schwellenwerte haben nur eine Funktion, wenn Soft-Roaming aktiviert ist.

Beacon-Verlust-Schwellwert

Der Beacon-Verlust-Schwellwert gibt an, wieviele Beacons des APs empfangsgestört sein dürfen, bevor ein eingebuchter Client eine erneute Suche beginnt.

Je höher der eingestellte Wert ist, desto eher kann es unbemerkt zu einer Unterbrechung der Verbindung kommen, gefolgt von einem zeitverzögerten Wiederaufbau der Verbindung.

Je kleiner der eingestellte Wert ist, desto eher kann eine möglicherweise folgende Unterbrechung erkannt werden, der Client kann frühzeitig mit dem Suchen nach einem alternativen AP beginnen.

Zu kleine Werte können dazu führen, dass der Client unnötig oft einen Verbindungsverlust erkennt.

Roaming-Schwellwert

Dieser Schwellwert gibt an, um wieviel Prozent die Signalstärke eines anderen APs besser sein muss, damit der Client auf den anderen AP wechselt.

In anderem Zusammenhang wird die Signalstärke teilweise in dB angegeben. In diesen Fällen gilt für die Umrechnung:

64dB – 100%

32dB – 50%

0dB – 0%

Kein-Roaming-Schwellwert

Dieser Schwellwert gibt die Feldstärke in Prozent an, ab welcher der aktuelle AP als so gut betrachtet wird, dass auf keinen Fall auf einen anderen AP gewechselt wird.

Zwangs-Roaming-Schwellwert

Dieser Schwellwert gibt die Feldstärke in Prozent an, ab welcher der aktuelle AP als so schlecht betrachtet wird, dass auf jeden Fall auf einen anderen, besseren AP gewechselt wird.

Verbinden-Schwellwert

Dieser Schwellwert gibt die Feldstärke in Prozent an, die ein AP mindestens aufweisen muss, damit ein Client einen Versuch zum Einbuchen bei diesem AP startet.

Verbindung-Halten-Schwellwert

Dieser Schwellwert gibt die Feldstärke in Prozent an, die der aktuelle AP mindestens aufweisen muss, damit die Verbindung nicht als abgerissen betrachtet wird.

Min. Verbinden-Signalpegel

Analog zum Verbinden-Schwellwert, Angabe jedoch als absolute Signalstärke.

Min. Verbindung-Halten-Signalpegel

Analog zum Verbindung-Halten-Schwellwert, Angabe jedoch als absolute Signalstärke.

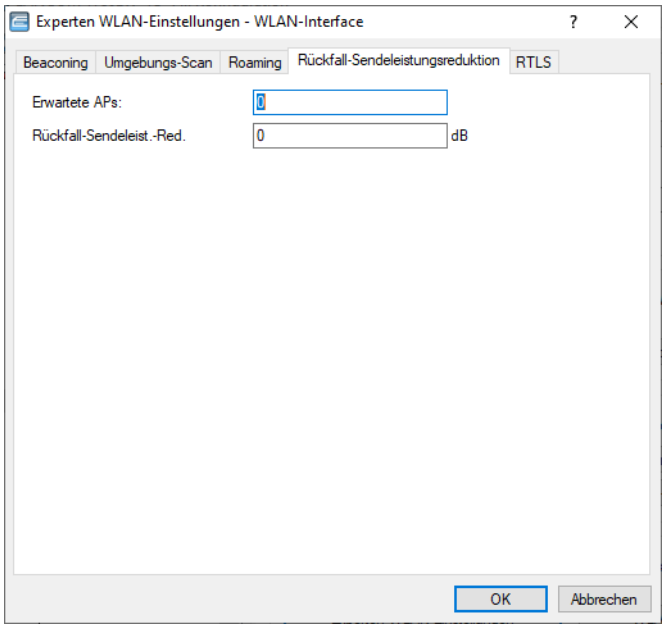
Blockzeit

In der Betriebsart als WLAN-Client und bei mehreren gleichen WLAN-Zugangspunkten (gleiche SSID auf mehreren APs) können Sie hier einen Zeitraum definieren, in dem sich der WLAN-Client nicht mehr mit einem AP verbindet, nachdem die Anmeldung an diesem AP abgelehnt wurde (Association-Reject).

Mögliche Werte sind 0 bis 4294967295 Sekunden.

Der Standardwert ist 0 Sekunden. Die Anmeldung des Clients wird nicht blockiert.

13.18.6.4 Rückfall-Sendeleistungsreduktion (Adaptive Transmission Power)



LANconfig: **Wireless-LAN** > **Allgemein** > **Erweiterte Einstellungen** > **Experten WLAN-Einstellungen** > **Rückfall-Sendeleistungsreduktion**

Konfigurieren Sie hier die Einstellungen der Rückfall-Sendeleistungsreduktion. Informationen hierzu finden Sie unter *Adaptive Transmission Power* auf Seite 1010.

Erwartete APs

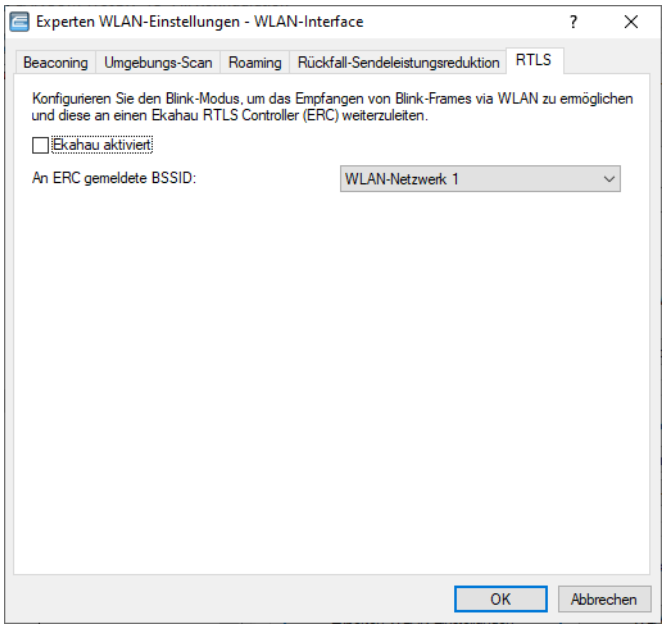
Geben Sie an, wie viele APs sich innerhalb einer Broadcast-Domäne befinden.

Rückfall-Sendeleist.-Red.

Geben Sie hier die Sendeleistungs-Reduktion in dB an, die der AP nutzen soll, falls ein AP aus der konfigurierten Gruppe nicht mehr erreichbar sein sollte.

Die standardmäßige Sendeleistungs-Reduktion konfigurieren Sie unter **Wireless-LAN** > **Allgemein** mit der Schaltfläche **Physikalische WLAN-Einst.** (und ggf. Auswahl der WLAN-Schnittstelle) im Dialog unter **Radio**.

13.18.6.5 RTLS



LANconfig: **Wireless-LAN** > **Allgemein** > **Erweiterte Einstellungen** > **Experten WLAN-Einstellungen** > **RTLS**

Konfigurieren Sie hier die Einstellungen für den AiRISTA Flow Blink Modus. Informationen hierzu finden Sie unter *AiRISTA Flow Blink Modus (vormals Ekahau Blink Modus)* auf Seite 1056.

Ekahau aktiviert

Aktivieren bzw. deaktivieren Sie hier den Blink-Modus für diese Schnittstelle.

An ERC gemeldete BSSID

Wählen Sie hier die logische WLAN-Schnittstelle aus, die das Gerät an den ERC melden soll.

Der ERC hat diese BSSID mit einem Ort "gemappt" (z. B. Serverraum) und weiß entsprechend, dass z. B. Wi-Fi Tag "A" sich in diesem Moment im Serverraum befindet, wenn der "Blink" über die BSSID des entsprechenden APs hereinkommt.

13.18.7 Konfigurierbare Datenraten je WLAN-Modul

Um in Anwendungsszenarien bestimmte Datenraten auszuschließen (z. B. bei ungünstigen Umgebungsbedingungen), ist es möglich, die Datenraten pro SSID oder P2P-Strecke genau nach den speziellen Anforderungen zu konfigurieren.

In den meisten Anwendungsfällen sind keine Änderungen an den Standard-Einstellungen notwendig. Stellen Sie sicher, dass nur WLAN-Experten diese Einstellungen ändern, da unsachgemäße Änderungen zu Problemen im WLAN-Netzwerk führen können.

Die Konfiguration von Datenraten je WLAN-Modul legt fest, welche Datenraten der AP zur Kommunikation mit Clients verwendet (Tx) und welche Datenraten der AP dem Client „ankündigt", die dieser zur Kommunikation mit dem AP verwenden soll oder darf (Rx).

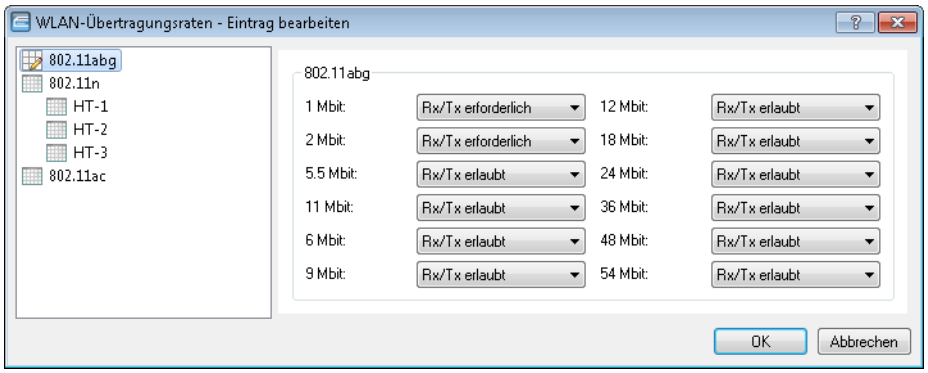
Die Ratenadaption richtet sich entsprechend nicht nur nach einer minimalen und einer maximalen Datenrate, sondern der AP verwendet auch deaktivierte Datenraten innerhalb dieser Grenzwerte nicht mehr.

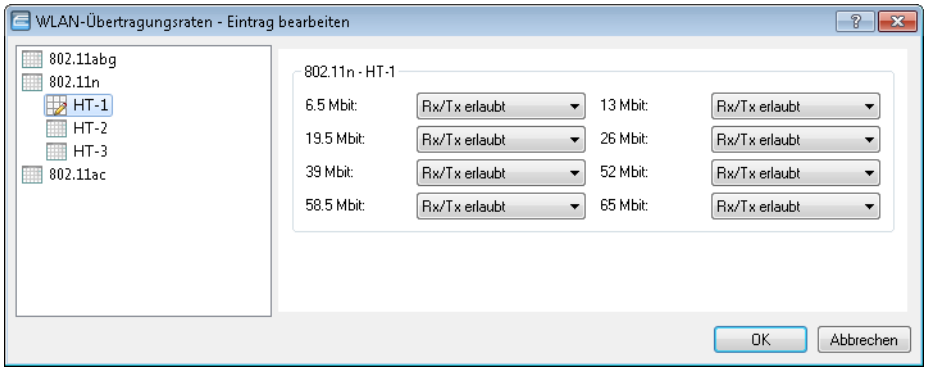
Die Konfiguration von Datenraten ist nur bei Stand-Alone-APs möglich. Für den Einsatz in WLC-Szenarien sind entsprechende Skripte notwendig, die der WLC an die APs ausrollt.

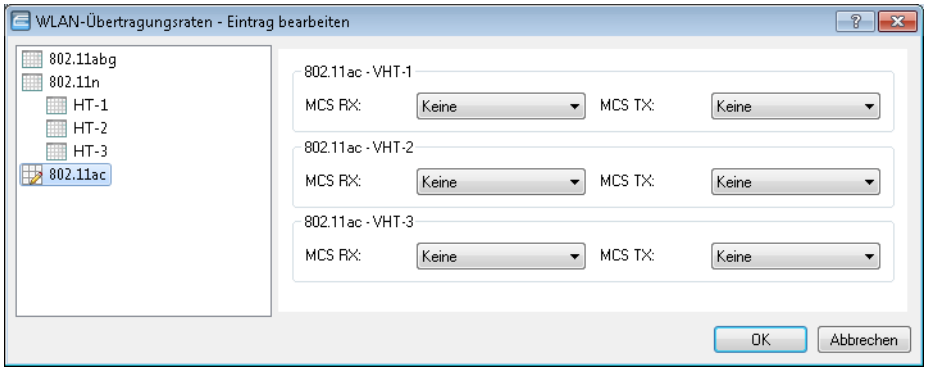
13.18.7.1 Konfiguration der Datenraten

Um die Datenraten mit LANconfig zu konfigurieren, wechseln Sie in die Ansicht **Wireless-LAN** > **Allgemein** > **Erweiterte Einstellungen** > **WLAN-Übertragungsraten**. LANconfig listet die Einstellungen aller verfügbaren Schnittstellen auf. Um die Einstellung für eine Schnittstelle zu ändern, markieren Sie die entsprechende Schnittstelle und klicken Sie auf **Bearbeiten**.

Wählen Sie links den zu konfigurierenden Standard aus.







Die Konfiguration ist separat möglich für die Standards

- 802.11abg
- 802.11n
  - HT-1
  - HT-2
  - HT-3
- 802.11ac
  - VHT-1
  - VHT-2
  - VHT-3

Je nach Standard sind für jede Übertragungsrate je SSID und P2P-Strecke explizit die folgenden Einstellungen verfügbar:

Rx/Tx erforderlich

Der AP kündigt dem Client die Rate als „unterstützt" und „erforderlich" in Beacons und Probe Responses an und nutzt sie selber auch zur Kommunikation mit dem Client. Unterstützt der Client die entsprechende Rate nicht, nimmt der AP ihn bei einer Verbindungsanfrage nicht an.

Rx/Tx erlaubt

Der AP kündigt dem Client die Rate als „unterstützt" an und nutzt sie selber auch zur Kommunikation mit dem Client. Der AP akzeptiert jedoch auch Anfragen von Clients, die die entsprechende Rate nicht unterstützen.

Rx erforderlich

Der AP kündigt dem Client die Rate als „unterstützt" und „erforderlich" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

Rx erlaubt

Der AP kündigt dem Client die Rate als „unterstützt" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

Deaktiviert

Der AP kündigt diese Rate nicht an und verwendet sie nicht zur Kommunikation mit dem Client.

MCS-9/8/7

Bei 802.11ac-Modulen ist für die Datenraten lediglich pro Stream-Variante (1, 2 oder 3 Streams) die maximale MCS auswählbar.

Keine

Bei 802.11ac-Modulen ist die jeweilige Stream-Variante für die entsprechende Datenrichtung deaktiviert.

13.18.8 RTLS (Real-Time Location System)

Unter RTLS versteht man die Möglichkeit zur Echtzeit-Lokalisierung eines Geräts. Dieses Gerät ist ein spezieller WLAN-Sender, der speziell kodierte WLAN-Pakete aussendet. Die Access Points in der Umgebung empfangen diese Pakete und leiten sie mit weiteren Daten an das verwendete System zur Echtzeit-Lokalisierung. Dadurch kann der Aufenthaltsort des WLAN-Senders genau bestimmt werden. Implizit erhält man dann den Aufenthaltsort von Gegenständen und Personen, die diesen WLAN-Sender tragen.

13.18.8.1 Stanley AeroScout RTLS

Das AeroScout RTLS-System ermöglicht u.a. Asset Management, Umgebungsmonitoring und Staff Workflow mittels spezieller via WLAN angebundener Sensoren und „Tags“. Mittels dieses Features ist die Weiterleitung der speziell kodierten WLAN-Pakete der AeroScout-Tags über eine LANCOM WLAN-Infrastruktur an die AeroScout Location Engine möglich.

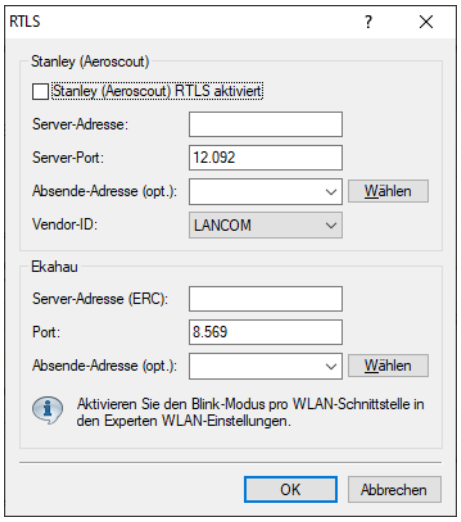
Folgende Betriebsarten werden unterstützt:

- Weiterleiten von AeroScout Tag Messages

  Es wird der WDS-Modus unterstützt. Achten Sie darauf, dass die Tags im AeroScout-System für den WDS-Modus konfiguriert sind. Der IBSS-Modus wird nicht unterstützt.
- Wi-Fi Client Reports

Stanley AeroScout RTLS konfigurieren

Um den Zugriff auf den Stanley AeroScout RTLS-Server mit LANconfig zu konfigurieren, öffnen Sie die Ansicht **Wireless-LAN** > **Allgemein** > **Erweiterte Einstellungen** > **RTLS** und konfigurieren Sie im Bereich **Stanley (AeroScout)**.



Stanley (AeroScout) RTLS aktiviert

Aktivieren Sie diese Option, um die Weiterleitung an die Aeroscout Location Engine einzuschalten.

Dieses Feature wird immer für alle WLAN-Module eines Access Points eingeschaltet.

Server-Adresse

Konfigurieren Sie hier die IP-Adresse der Aeroscout Location Engine.

Server-Port

Konfigurieren Sie bei Abweichungen vom Standardwert den Server-Port der Aeroscout Location Engine.

Absende-Adresse (optional)

Konfigurieren Sie optional das Absende-Netzwerk für die Verbindung zur AeroScout Location Engine. Dies ist nur dann erforderlich, wenn mehrere ARF-Netzwerke konfiguriert sind.

Vendor-ID

Konfigurieren Sie hier die Vendor-ID, die der Access Point an die Aeroscout Location Engine meldet. Sollte Ihre Version der AeroScout Location Engine noch nicht die dedizierte LANCOM-Vendor-ID unterstützen, ist hier ein Umschalten auf die Vendor-ID „Motorola" möglich.

13.18.8.2 AiRISTA Flow Blink Modus (vormals Ekahau Blink Modus)

Die Firma Ekahau bietet mit ihrem "Real Time Location Service" (RTLS) die Möglichkeit, den Aufenthaltsort von Gegenständen und Personen über ein vorhandenes WLAN zu bestimmen. Dazu befinden sich am Gerät oder am Körper der Person spezielle WLAN-Sender, sogenannte "Wi-Fi Tags", die speziell kodierte WLAN-Pakete aussenden. Die APs in der Umgebung empfangen diese Pakete, versehen sie mit zusätzlichen Informationen (z. B. RSSI) und leiten diese Informationen innerhalb des "TaZmen Sniffer Protocols" (TZSP) gekapselt an den im Netzwerk installierten "Ekahau RTLS Controller" (ERC). Der ERC wertet diese Daten aus und bestimmt dadurch die Position des Wi-Fi Tags.

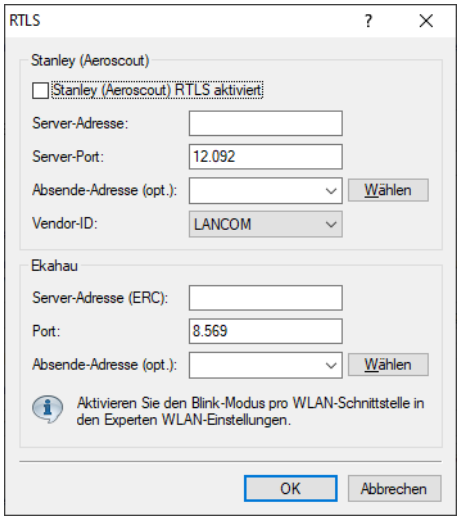
Die Wi-Fi Tags unterstützen beim Senden der WLAN-Pakete drei Modi:

- **Associated-Modus**: Im "Associated-Modus" funktioniert das Wi-Fi Tag wie ein WLAN-Client. Es loggt sich in einen umliegenden AP ein und ist somit ständig mit dem entsprechenden AP verbunden. Einerseits ermöglicht das eine nahtlose Positionsbestimmung, andererseits verbraucht dieser Modus mehr Strom, so dass die Batterie des Wi-Fi Tags eine kürzere Lebensdauer besitzt. Im "Associated-Modus" verwenden die Wi-Fi Tags das "Ekahau Location Protocol" (ELP).
- **Blink-Modus**: Im "Blink-Modus" sendet das "Wi-Fi Tag" nur kurze WLAN-Pakete, ohne sich mit einem AP zu verbinden. Im "Blink-Modus" verwenden die Wi-Fi Tags das "Ekahau Blink Protocol" (EBP).
- **Mixed-Modus**: Im "Mixed-Modus" nutzen die Wi-Fi Tags EBP zur Übermittlung des RSSI und ELP zur Übermittlung von Zustandsmeldungen an den ERC.

AiRISTA Flow Blink Modus (vormals Ekahau Blink Modus) konfigurieren

Der 'Blink-Modus' funktioniert nur mit 802.11n-WLAN-Modulen, nicht mit 802.11ac-WLAN-Modulen. Entsprechend ist es nicht möglich, im LANconfig den 'Blink-Modus' für 802.11ac-WLAN-Module zu aktivieren. Die Option ist bei den jeweiligen Geräten in diesem Fall dauerhaft deaktiviert.

Um den Zugriff auf den RTLS-Server (ERC) mit LANconfig zu konfigurieren, öffnen Sie die Ansicht **Wireless-LAN** > **Allgemein** > **Erweiterte Einstellungen** > **RTLS** und konfigurieren Sie im Bereich **Ekahau**.



Server-Adresse (ERC)

Geben Sie die Adresse des ERC an. Möglich ist die Angabe einer IP-Adresse oder eines Hostnamens.

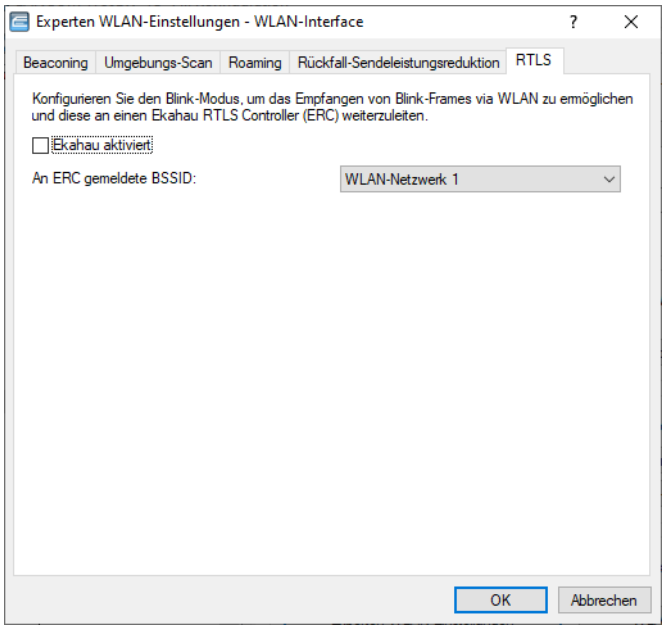
Port

Enthält den Standard-UDP-Port (8569) für die Kommunikation mit dem ERC. Ändern Sie diesen Wert nur in Ausnahmefällen.

Absende-Adresse (optional)

Geben Sie optional eine Absendeadresse an.

Um den Blink-Modus für die jeweilige physikalische WLAN-Schnittstelle zu konfigurieren, klicken Sie unter **Wireless-LAN** > **Allgemein** > **Erweiterte Einstellungen** auf die Schaltfläche **Experten WLAN-Einstellungen**, wählen Sie ggf. in der erscheinenden Drop-Down-Liste die gewünschte WLAN-Schnittstelle aus und wechseln Sie in den Reiter **RTLS**.



Ekahau aktiviert

Aktivieren bzw. deaktivieren Sie hier den Ekahau-Blink-Modus für diese Schnittstelle.

An ERC gemeldete BSSID

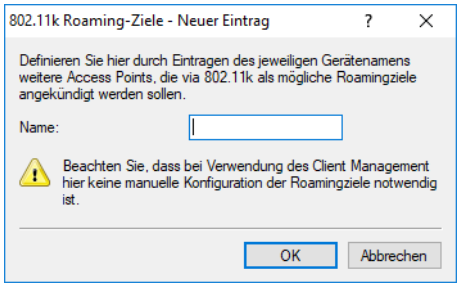
Wählen Sie hier die logische WLAN-Schnittstelle aus, die das Gerät an den ERC melden soll.

Der ERC hat diese BSSID mit einem Ort "gemappt" (z. B. Serverraum) und weiß entsprechend, dass z. B. Wi-Fi Tag "A" sich in diesem Moment im Serverraum befindet, wenn der "Blink" über die BSSID des entsprechenden APs hereinkommt.

13.18.9 IEEE 802.11k-Roaming-Ziele

Der Standard IEEE 802.11k beschreibt einen Weg, WLAN-Clients über potentielle Roaming-Ziele, also weitere Access Points der selben SSID in Reichweite, zu informieren. Diese Information an den Client erfolgt durch den im Standard definierten „Neighbour Report". Bisher kommt 802.11k bereits im Rahmen des Client Managements zum Einsatz – hierzu ist keine gesonderte Konfiguration erforderlich. In Einzelfällen bzw. speziellen Szenarien kann es notwendig sein, auf das automatische Client Management zu verzichten und das Teilfeature 802.11k separat zu verwenden.

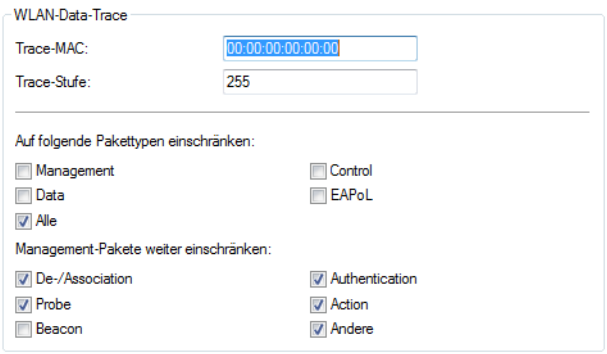
Sie finden die neue Tabelle unter **Wireless-LAN** > **Allgemein** > **Erweiterte Einstellungen** > **802.11k Roaming-Ziele**. Tragen Sie hier die potentiellen Roaming-Ziele ein.



13.18.10 WLAN-Data-Trace

Bei Problemen hilft häufig ein Trace. Hier lassen sich dafür spezielle Einstellungen für WLAN-Traces vornehmen. Siehe auch *Trace-Ausgaben* auf Seite 308.

LANconfig: **Wireless-LAN** > **Allgemein** > **Erweiterte Einstellungen** > **Trace**



Trace-MAC

Für den WLAN-Data-Trace kann die Ausgabe von Tracemeldungen auf einen bestimmten Client eingestellt werden, dessen WLAN-MAC-Adresse hier eingetragen wird.

Jede Netzwerkkarte hat eine eigene, weltweit eindeutige MAC-Adresse. Diese Adresse ist eine 12-stellige Hexadezimalzahl (z. B. 00A057010203). Sie finden diese Adresse meistens als Aufdruck auf der Netzwerkkarte selbst.

Die Eingabe von '000000000000' deaktiviert diese Funktion und gibt die Tracemeldungen von allen Clients aus.

Trace-Stufe

Für den WLAN-Data-Trace lässt sich die Ausgabe von Tracemeldungen auf einen bestimmten Inhalt beschränken. Der hier eingetragene Wert schränkt die Pakete im WLAN-DATA-Trace bis zur entsprechenden Stufe ein.

Mögliche Werte:

0 bis 255

Besondere Werte:

0: nur die Meldung, dass ein Paket überhaupt empfangen/gesendet wurde

1: zusätzlich die physikalischen Parameter der Pakete (Datenrate, Signalstärke etc.)

2: zusätzlich der MAC-Header

3: zusätzlich der Layer3-Header (z. B. IP)

4: zusätzlich der Layer4-Header (TCP, UDP...)

5: zusätzlich die TCP/UDP-Payload

255: keine Beschränkung des Inhalts. Der Trace gibt die kompletten Pakete aus.

Default:

255

Pakettypen

Ähnlich wie bei der Trace-MAC und der Trace-Stufe lassen sich die Ausgaben im WLAN-DATA-Traces anhand des Typs der empfangenen bzw. gesendeten Pakete einschränken, z. B. Management (Authenticate, Association, Action, Probe-Request/Response), Control (z. B. Powersave-Poll), EAPOL (802.1X-Verhandlung, WPA-Key-Handshake).

Mögliche Werte:

Management

Control

Daten

EAPOL

Alle

Default:

Alle

Management-Pakete

Mit dieser Auswahl lässt sich einstellen, welche Klassen von Management-Frames im WLAN-DATA-Trace auftauchen sollen.

Mögliche Werte:

Assoziierung: (Re)Association Request/Response, Disassociate

Authentisierung: Authentication, Deauthentication

Probes: Probe Request, Probe Response

Action

Beacon

Andere: alle restlichen Management-Frametypen

Default:

Assoziierung

Authentisierung

Probes

Action

Andere

13.18.11 Client Management

Mit Client Management werden WLAN-Clients stets auf den für sie idealen Access Point sowie das beste Frequenzband gesteuert. Dieses Feature steigert somit die Qualität drahtloser Netzwerke jeder Größenordnung - egal ob im stand-alone-Betrieb oder orchestriert über die LANCOM Management Cloud. Die beliebten, aber bislang getrennten Funktionen Band Steering und Client Steering werden hiermit kombiniert und auch ohne den Betrieb mit einem WLAN-Controller bereitgestellt.

Im Vergleich zum bisherigen WLC-gestützten Client Steering funktioniert Client Management autark und ohne WLC. die Access Points kommunizieren dazu untereinander mittels des Protokolls IAPP.

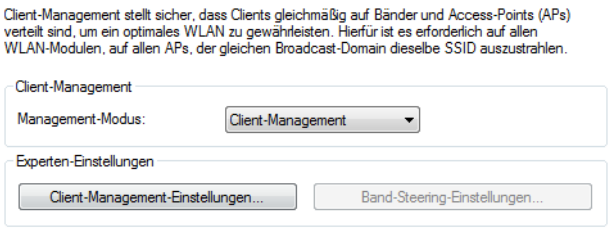
Damit die Kommunikation der Access Points untereinander funktioniert, ist es erforderlich, dass alle Access Points IAPP-Nachrichten austauschen können. IAPP-Nachrichten werden als Multicast übertragen. Gegebenenfalls sind auf Infrastrukturseite, insbesondere auf Switches, passende Ausnahmeregelungen im IGMP-Snooping oder anderen Filtermechanismen zu schaffen. IAPP verwendet die Multicast-Gruppe 224.0.1.76.

LANCOM Switches in der Defaulteinstellung sind bereits korrekt für das Client Management eingestellt.

Client Management stellt somit sicher, dass Clients gleichmäßig auf Frequenzbänder und Access Points verteilt sind, um ein optimales WLAN zu gewährleisten. Hierfür ist es erforderlich, dass sowohl auf allen WLAN-Modulen als auch auf allen Access Points der gleichen Broadcast-Domäne dieselbe SSID ausgestrahlt wird.

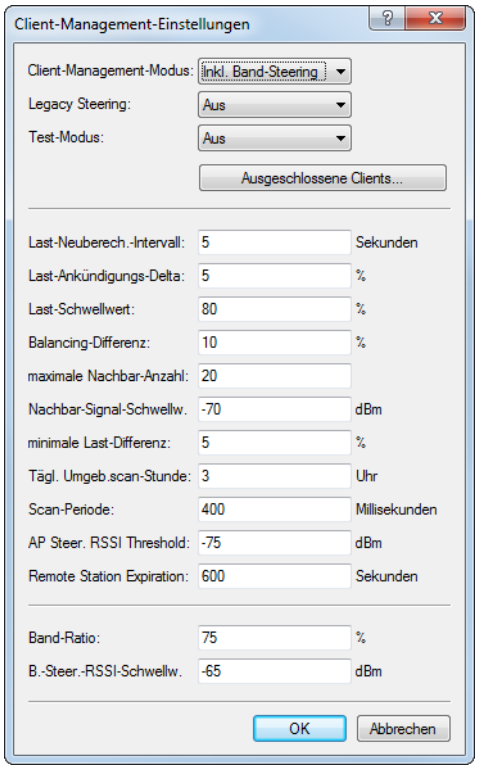
13.18.11.1 Konfiguration des Client Managements

Das Client Management können Sie unter **Wireless-LAN** > **Client-Management** > **Client-Management** > **Management-Modus** ein- bzw. ausschalten. Auf Neuinstallationen ist es per Voreinstellung eingeschaltet und benötigt normalerweise keine besonderen Einstellungen. Bei einem Access Point mit mehreren WLAN-Modulen kann alternativ auch das **AP-basierte Band-Steering** aktiviert werden. Siehe hierzu *WLAN Band Steering* auf Seite 982.



Experten-Einstellungen

Konfigurieren Sie unter **Wireless-LAN** > **Client-Management** > **Experten-Einstellungen** > **Client-Management** die Einstellungen des Client Managements. Mit den Voreinstellungen funktioniert das Client Management optimal in Büro- und Schulumgebungen.



Client-Management-Modus

Bei Access Point mit mehreren WLAN-Modulen kann das Client Management mit und ohne Band Steering durchgeführt werden.

Standardeinstellung: inkl. Band Steering

Legacy-Steering

Konfiguriert, ob auch Clients, die 802.11v nicht oder nicht korrekt unterstützen, vom Client Management auf andere Access Points geleitet werden sollen. Auch bei aktivem Legacy-Steering wird das Client Management weiterhin erst 802.11v-fähige Clients auf andere Access Points leiten; erst anschließend werden Clients, die 802.11v nicht unterstützen, geleitet. Legacy-Steering erzwingt das Umleiten dieser Clients durch eine erzwungene Trennung des Clients vom WLAN. Anschließend wird das erneute Einbuchen des Clients am aktuellen AP für eine gewisse Zeit blockiert, damit der Client seibsttätig einen anderen Access Point wählt. Dies kann im Gegensatz zum Leiten der Clients mittels 802.11v zu einer verschlechterten Benutzererfahrung führen. Dies ist vorrangig vom Verhalten der Legacy-Clients abhängig.

Standardeinstellung: Aus

Test-Modus

Betreibt Client-Management im Test-Modus: Umgebungs-Scans werden durchgeführt, Steering-Entscheidungen werden vom System getroffen und im Syslog verzeichnet, aber es findet kein tatsächliches Steering der Clients statt. Verwenden Sie den Test-Modus, um das Verhalten des Client Managements zu prüfen ohne tatsächliche Änderungen an Ihrem Netzwerk durchzuführen.

Standardeinstellung: Aus

Ausgeschlossene Clients

In vielen Umgebungen gibt es spezielle Clients, von denen bekannt ist, dass sie sich nicht gut verhalten. Stellen Sie sich ein Krankenhaus mit kundenspezifischen VoIP-Telefonen vor, die nicht in der Lage sind, Verbindungsabbrüche ordnungsgemäß zu behandeln, und die dazu neigen, sich an einen bestimmten Access Point zu halten. Um nun nicht das Client Management komplett abschalten zu müssen, kann man diese Clients von der Steuerung ausnehmen.

Konfigurieren Sie in der Tabelle die MAC-Adressen der Clients, die von einer Steuerung ausgenommen werden sollen. Als Wildcard-Zeichen kann der `*` verwendet werden, der für beliebige Zeichen steht. Dieses darf aber nicht als einziges Zeichen einer MAC-Adresse verwendet werden. Möglich sind also z. B. `01:23:45:12:34:56`, `01:*:56` oder `01:23:*`.

Last-Neuberechnungs-Intervall

Konfiguriert das Intervall, in dem die Last auf dem AP berechnet wird und Entscheidungen zum Steering der Clients getroffen werden. Erhöhen Sie den Wert, um die Last im Netzwerk zu reduzieren. Verringern Sie den Wert, um schneller eine Neuverteilung der Clients zu erreichen. Werte < 2 Sekunden werden aufgrund von negativen Effekten in der Netzwerk-Laufzeit nicht empfohlen. Werten von > 10 Sekunden werden nicht empfohlen, da das Steering der Clients sonst nicht rechtzeitig erfolgt. Es wird empfohlen, den standardmäßig eingestellten Wert nicht zu ändern.

Standardwert: 5 Sekunden

Last-Ankündigungs-Delta

Konfiguriert, bei welcher prozentualen Änderung der aktuellen Last ein Access Point diese auch außerhalb des regulären Ankündigungs-Intervalls an andere Access Points kommuniziert. Erhöhen Sie den Wert in Installationen mit vielen mobilen Clients. Verringern Sie den Wert in Installationen mit wenig beweglichen Clients. Die Standardeinstellung wurde in Hinblick auf Büro- und Schulumgebungen gewählt. Beachten Sie, dass dieser Wert unterhalb des für die Balancing-Differenz konfigurierten Wertes liegen sollte, um Fehlberechnungen zu vermeiden.

Standardwert: 5 %

Last-Schwellenwert

Konfiguriert den Last-Schwellenwert, ab dem der Access Point unabhängig vom Last-Schwellenwert der Nachbar-Access-Points mit dem Steering beginnt. Erhöhen Sie den Wert in low-quality/high-density-Szenarien wie Stadien. Verringern Sie den Wert in high-quality/high-throughput-Szenarien wie Büro/Schule.

Standardwert: 80 %

Balancing-Differenz

Konfiguriert die Last-Differenz zwischen Access Points, ab der Clients zum weniger belasteten Access Point geleitet werden. Hohe Werte führen zu weniger ausgeglichenen Installationen, niedrige Werte zu mehr Steering der Clients. Erhöhen Sie den Wert, wenn zu viel Client Steering betrieben wird. Verringern Sie den Wert, wenn eine maximal ausgeglichene Installation erforderlich ist. Die Standardeinstellung wurde in Hinblick auf Büro- und Schulumgebungen gewählt.

Standardwert: 10 %

maximale Nachbar-Anzahl

Konfiguriert die Anzahl an Nachbar-Access Points, die vom Client Management auf dem aktuellen Access Point berücksichtigt werden. In High-Density-Szenarien kann eine niedrige Anzahl Vorteile bringen, da Clients so vorrangig auf in der Nähe befindliche Access Points geleitet werden und weniger Management-Kommunikation zwischen den einzelnen Access Points notwendig ist. Werte < 4 werden nicht empfohlen, da so keine ausreichende Anzahl an Access Points für eine sinnvolle Steering-Entscheidung zur Verfügung steht. Werte > 72 werden aufgrund von Limitierungen des 802.11-Protokolls nicht unterstützt.

Standardwert: 20 APs

Nachbar-Signal-Schwellenwert

Konfiguriert die Signalstärke, mit der ein AP gesehen werden muss, um als Nachbar-Access Point eingestuft zu werden. Erhöhen Sie den Wert für High-Density-Szenarien (z. B: -60, -50). Verringern Sie den Wert für Szenarien, in der eine große Abdeckung gefordert ist (z. B. -80,-90).

Standardwert: -70 dBm

minimale Last-Differenz

Konfiguriert die minimale Last-Differenz zwischen benachbarten Access Points, ab der zwischen diesen Access Points ein Steering durchgeführt wird. Das Steering wird nur durchgeführt, wenn der konfigurierte Last-Schwellenwert überschritten wurde. Zur Vermeidung von Fehlberechnung sollte die minimale Last-Differenz die konfigurierte Balancing-Differenz nicht überschreiten. Erhöhen Sie den Wert, um weniger Steering in der Installation zu betreiben. Verringern Sie den Wert, um mehr Steering in der Installation zu betreiben.

Standardwert: 5 %

Täglicher Umgebungsscan zu Stunde

Konfiguriert die Uhrzeit (00-23), zu der täglich der Umgebungs-Scan ausgeführt wird, welcher für das Client Management benötigt wird. Der genaue Zeitpunkt des Scans wird über ein Zeitfenster von 30 Minuten verteilt, um Konflikte zwischen gleichzeitig laufenden Umgebungs-Scans zu minimieren. Der Umgebungs-Scan dauert ca. 15 Sekunden an. Währenddessen können keine WLAN-Daten über das scannende WLAN-Modul übertragen werden.

Standardwert: 3 Uhr

Scan-Periode

Konfiguriert die Laufzeit des Umgebungs-Scans, der zur Identifikation von Nachbar-Access Points dient. Die Scan-Periode sollte das 2- bis 2,5-fache des konfigurierten Beacon-Intervalls betragen; der Standardwert wurde bereits für das Standard-Beacon-Intervall passend gewählt. Dieser Wert ist von 200 ms bis 1000 ms konfigurierbar.

Standardwert: 400 ms

AP Steer. RSSI Threshold

Die Signalstärke, die ein Client auf einem entferntem Access Point haben muss, damit er zu diesem gesteuert wird.

Eine höhere Signalschwelle bewirkt einen niedrigeren Wert potentiell steuerbarer Clients und limitiert somit die Möglichkeiten des Client Managements. Gleichzeitig wäre sie in Umgebungen mit hohen Qualtitätsanforderungen sinnvoll, z. B. bei starker Verwendung von VoIP. Dafür wird eine sehr gute Ausleuchtung und höhere Dichte der Access Points benötigt.

Eine niedrigere Signalschwelle bewirkt einen höheren Wert potentiell steuerbarer Clients, allerdings kann der Algorithmus hierbei auch Clients Access Points mit schlechter Signalqualität zuweisen. Es kann sogar passieren, dass sich Clients weigern, zu einem Access Point mit schlechterer Signalqualität gesteuert zu werden. Es würde in Umgebungen helfen, in denen ein großes Areal abgedeckt werden soll. Werte unterhalb von -80 dBm führen zu einem sehr schlechten Ergebnis, da die Wahrscheinlichkeit steigt, dass Clients sich nicht mit dem Access Point verbinden können, zu dem sie gesteuert werden sollen.

Der Standardwert passt für Büroumgebungen.

Standardwert: -75 dBm

Remote Station Expiration

Zeit, in der ein Access Point sich die Informationen über die Clients eines benachbarten Access Points merkt. Diese Informationen werden zur Beschleunigung der Lenkentscheidungen verwendet. Der Standardwert passt für Büroumgebungen mit einem relativ statischen Aufbau und wenigen sich bewegenden Clients. In Umgebungen mit vielen sich bewegenden oder nur kurzzeitig verbundenen Clients sollte man niedrigere Werte setzen. Zu hohe Werte führen zu Fehlsteuerungen, wenn die Informationen des Caches nicht mehr gültig sind.

Standardwert: 600 Sekunden

Band-Ratio

Konfiguriert die gewünschte Verteilung der Clients zwischen den Radio-Bändern. Das konfigurierte Verhältnis spezifiziert, welcher Anteil an Clients auf das 5-GHz-Band geleitet werden soll.

Standardwert: 75 %

Band-Steering-RSSI-Schwellenwert

Konfiguriert die Signalstärke (RSSI), mit der ein Client auf dem jeweils anderen Radio-Band „gesehen" werden muss, damit er auf dieses Band geleitet wird. Die Standardeinstellung wurde in Hinblick auf Büro-Umgebungen gewählt.

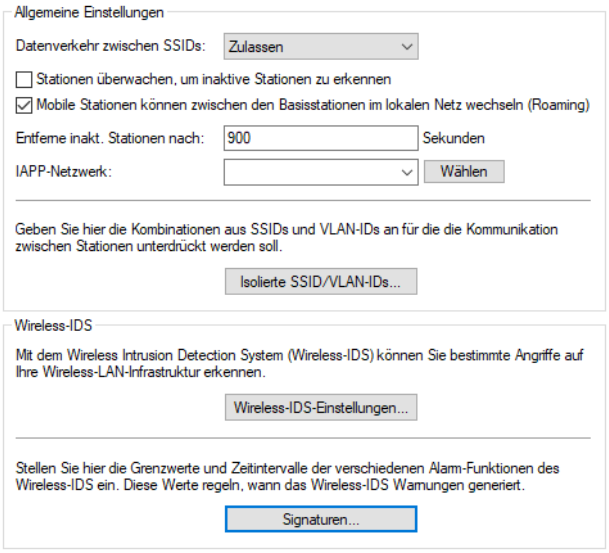
Standardwert: -65 dBm

13.18.12 WLAN-Sicherheit

In diesem Konfigurationsbereich schränken Sie die Kommunikation der Teilnehmer im Funknetzwerk ein. Dazu wird die Datenübertragung zwischen bestimmten Teilnehmer-Gruppen, nach einzelnen Stationen oder nach verwendetem Protokoll begrenzt.

13.18.12.1 Allgemeine Einstellungen

Hier finden Sie allgemeine Einstellungen zur Sicherheit im WLAN.



LANconfig: **Wireless-LAN** > **Security**

Datenverkehr zwischen SSIDs

Je nach Anwendungsfall ist es gewünscht oder eben auch nicht erwünscht, dass die an einem AP angeschlossenen WLAN-Clients mit anderen Clients kommunizieren. Die Kommunikation der Clients in unterschiedlichen SSIDs kann mit dieser Option erlaubt oder verhindert werden. Bei Modellen mit mehreren WLAN-Modulen gilt diese Einstellung global für alle WLANs aller Module.

Die Kommunikation der Clients innerhalb eines logischen WLANs wird separat bei den logischen WLAN-Einstellungen gesteuert (Inter-Station-Verkehr). Wenn der Inter-SSID-Verkehr aktiviert ist und der Inter-Station-Verkehr deaktiviert, kann ein Client aus einem logischen WLAN mit den Clients in

anderen logischen WLANs kommunizieren. Diese Möglichkeit kann über VLAN-Einstellungen oder Protokollfilter verhindert werden.

Stationen überwachen, um inaktive Stationen zu erkennen

Besonders bei öffentlichen WLAN-Zugriffspunkten (Public Spots) ist es für die Abrechnung der Nutzungsgebühren erforderlich, nicht mehr aktive Stationen zu erkennen. Dazu kann der AP zur Überwachung in regelmäßigen Abständen Pakete an die eingebuchten Stationen schicken. Kommen von einer Station keine Antworten mehr auf diese Pakete, wird sie als nicht mehr aktiv an das Abrechnungssystem gemeldet.

Mobile Stationen können zwischen den Basisstationen im lokalen Netz wechseln (Roaming)

Neben der Kommunikation der Clients untereinander kann hier auch eingestellt werden, ob die benachbarten APs beim Roaming Informationen über das Inter Access Point Protocol (IAPP) austauschen. Das IAPP ist ein Protokoll zur Kommunikation zwischen APs. Der „abgebende AP" bekommt so die Nachricht, dass ein bei ihm eingebuchter WLAN-Client nun zu einem anderen AP wechselt und kann den Client sofort aus seiner Liste entfernen.

Entferne inaktive Stationen nach … Sekunden

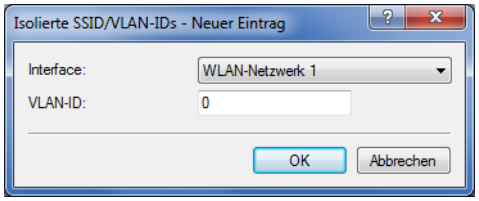
Definieren Sie eine Dauer in Sekunden, nach der inaktive Stationen aus der Liste der aktuell verbundenen Stationen entfernt werden können.

IAPP-Netzwerk

Durch Roaming-Informationen, die über das IAPP-Protokoll ausgetauscht werden, kann unter Umständen eine hohe Netzwerkbelastung hervorgerufen werden. Deshalb ist es empfehlenswert, hier ein ARF-Netzwerk auszuwählen, auf dem die IAPP-Kommunikation stattfinden soll.

13.18.12.2 Isolierte SSID/VLAN-IDs

Über dieses Menü ist es möglich, ein „Sammel-VLAN" abzubilden, in dem WLAN-Clients nicht untereinander kommunizieren dürfen, sondern eine Kommunikation nur zwischen WLAN-Client und AP möglich ist (Hotspot-Szenario). Außerhalb dieses „Sammel-VLANs" kann eine Kommunikation von Clients untereinander erlaubt werden. Dies funktioniert vollkommen transparent innerhalb derselben SSID, in der den Clients unterschiedliche VLANs zugewiesen werden.



LANconfig: **Wireless-LAN** > **Security** > **Isolierte SSID/VLAN-IDs**

Hier definieren Sie, für welche Kombinationen aus SSIDs und VLANs der Datenverkehr zwischen den Clients verboten wird. Diese Tabelle funktioniert also als Blacklist, da man üblicherweise nur wenige VLANs definieren will, in denen die Kommunikation verboten wird, aber mehrere, in denen sie erlaubt wird.

Dieser Mechanismus funktioniert auch dann, wenn die Clients an verschiedenen APs eingebucht sind (wobei auf übereinstimmende Konfiguration der Tabelle geachtet werden sollte). Voraussetzung dafür ist, dass die APs via IAPP kommunizieren können.

Interface

Die Liste der verfügbaren WLAN-Netzwerke.

VLAN-ID

Die Identifikationsnummer des VLANs.

Datenverkehr zulassen zwischen Stationen dieser SSID muss generell erlaubt sein, damit er mit diesem Feature wieder beschränkt werden kann.

13.18.12.3 Wireless Intrusion Detection System (WIDS)

Ein Intrusion Detection System (IDS) erkennt Angriffe auf ein Netzwerk und meldet diese Angriffe an ein übergeordnetes Netzwerk-Management-System. Gerade in Unternehmens-Netzwerken ist der Einsatz eines IDS unerlässlich, um eventuelle Angriffe oder Störungen sofort erkennen und abstellen zu können.

Das Wireless Intrusion Detection System (WIDS) in LCOS-Geräten überprüft die verfügbaren WLANs anhand umfangreicher, definierter Grenzwerte. Damit Sie im Falle eines Angriffes rechtzeitig reagieren können, meldet das WIDS Angriffe über E-Mail, SYSLOG oder SNMP-Traps.

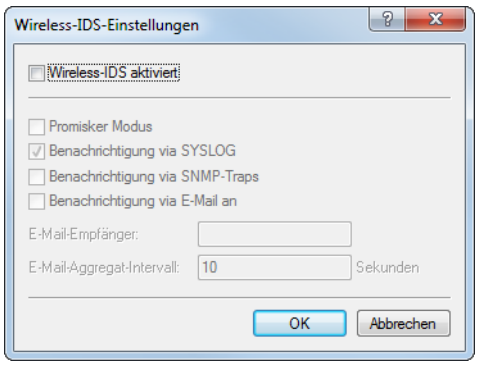
Die Erkennung von Angriffen erfolgt dabei auf Basis von bekannten oder gleichartigen Mustern.

Die WIDS-Konfiguration erfolgt entweder direkt im AP oder über die Zuordnung eines WIDS-Profils zum AP in einem WLC.

Beachten Sie bitte, dass die Erkennung von Angriffsmustern (Heuristik) auch zu Fehlalarmen („False Positive") führen kann!

WIDS im AP konfigurieren

Um das Wireless Intrusion Detection System (WIDS) mit LANconfig zu konfigurieren, wechseln Sie in die Ansicht **Wireless-LAN** > **Security** > **Wireless-IDS-Einstellungen**.



Wireless-IDS aktiviert

Aktiviert oder deaktiviert das Wireless Intrusion Detection System (WIDS).

Promisker Modus

Bei aktiviertem Modus („promiscuous mode") empfängt der AP auch Pakete, die nicht an ihn gerichtet sind, sondern an andere Netzwerkteilnehmer.

Dieser Modus ist erforderlich, um einige der unten genannten Angriffe erkennen zu können. Der promiscuous mode beeinflusst allerdings die Leistung. Daher wird mit der Aktivierung des promiscuous mode automatisch die Frame Aggregation abgeschaltet.

Benachrichtigung via SYSLOG

Aktiviert oder deaktiviert die WIDS-Meldungen über SYSLOG.

Die generierte SYSLOG-Meldung besitzt den Severity Level „INFO" und enthält den Zeitpunkt, die betroffene Schnittstelle sowie den Auslöser (Art des Angriffes und überschrittener Grenzwert).

Benachrichtigung via SNMP-Traps

Aktiviert oder deaktiviert die SNMP-Traps für WIDS-Meldungen.

Benachrichtigung via E-Mail an

Aktiviert oder deaktiviert die WIDS-Meldungen über E-Mail.

Zur Nutzung dieser Benachrichtigungen muss ein SMTP-Konto eingerichtet sein.

E-Mail-Empfänger

Geben Sie einen E-Mail-Empfänger an, wenn die Benachrichtigung über E-Mail aktiviert ist.

Das Feld muss eine gültige E-Mail-Adresse enthalten.

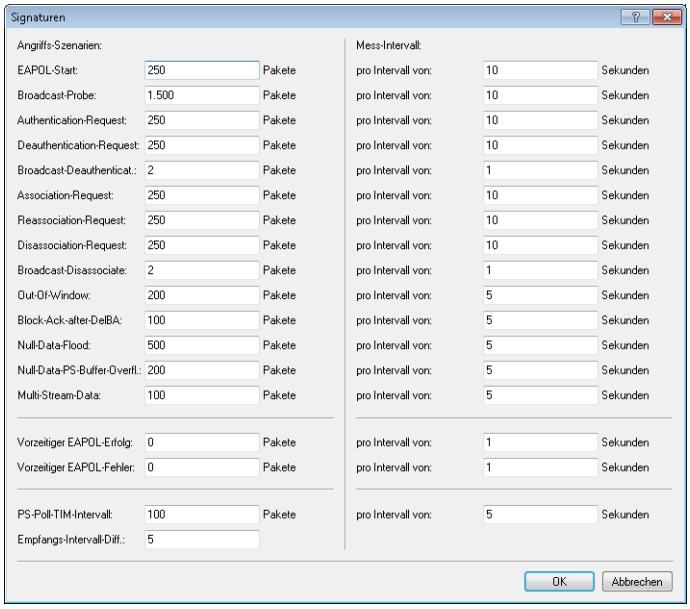
E-Mail-Aggregat-Intervall

Legen Sie die Verzögerung in Sekunden vor dem Versenden einer E-Mail fest, in der das WIDS nach dem Eintreffen eines ersten Wireless-IDS-Ereignisses weitere Ereignisse sammelt.

Diese Funktion verhindert, dass eine Flut von Angriffen eine E-Mail-Flut verursacht.

Signaturen

Um die Grenzwerte und Zeitintervalle (Datenpakete pro Sekunde) der verschiedenen Alarm-Funktionen des WIDS zu konfigurieren, wechseln Sie in die Ansicht **Wireless-LAN** > **Security** > **Signaturen**. Diese Werte regeln, wann das WIDS Warnungen generiert.



Die Angabe von Grenzwerten und Zeitintervallen für die folgenden Angriffs-Szenarien ist möglich:

- EAPOL-Start
- Broadcast-Probe
- Authentication-Request
- Deauthentication-Request (*)
- Broadcast-Deauthenticate
- Association-Request
- Reassociation-Request
- Disassociation-Request (*)
- Broadcast-Disassociate
- Out-Of-Window

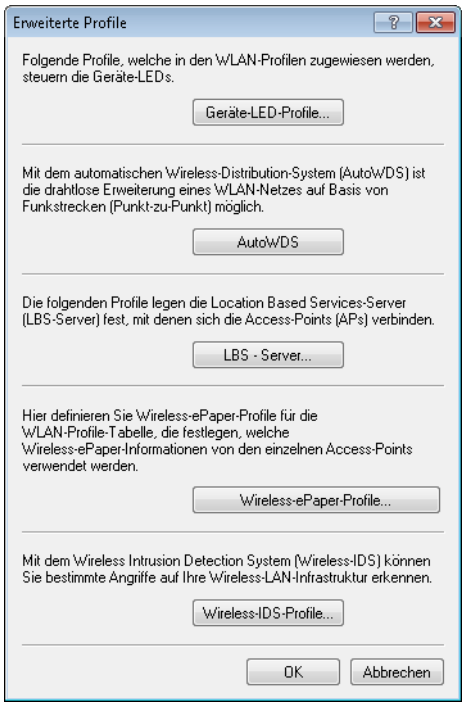
- Block-Ack-after-DelBA
- Null-Data-Flood
- Null-Data-PS-Buffer-Overflow
- Multi-Stream-Data
- Vorzeitiger EAPOL-Erfolg (*)
- Vorzeitiger EAPOL-Fehler (*)
- PS-Poll-TIM-Intervall
- Empfangs-Intervall-Differenz

Alle Felder sind bereits mit für das jeweilige Angriffs-Szenario typischen Werten vorbelegt.

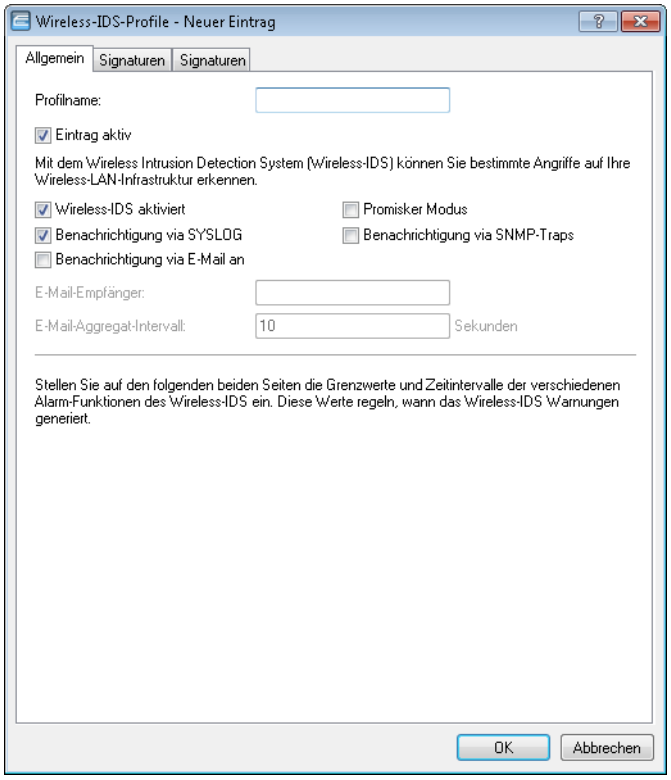
(*) Diese Angriffe werden nur bei aktivem promiscuous mode erkannt!

WIDS-Profile im WLC konfigurieren

Um ein Profil für das Wireless Intrusion Detection System (WIDS) mit LANconfig zu konfigurieren, wechseln Sie in die Ansicht **WLAN-Controller** > **Profile** und klicken Sie auf **Erweiterte Profile**.



Unter **Wireless-IDS-Profile** erstellen oder bearbeiten Sie die WIDS-Profile.



Profilname

Vergeben Sie eine Bezeichnung für das Profil. Diesen Profilnamen geben Sie bei der Zuordnung zu einem WLAN-Profil unter **WLAN-Controller** > **Profile** > **WLAN-Profile** an.

Die Angabe eines Profilnamens ist für die Konfiguration der WIDS-Signaturen notwendig.

Wireless-IDS aktiviert

Aktiviert oder deaktiviert das Wireless Intrusion Detection System (WIDS).

Promisker Modus

Bei aktiviertem Modus („promiscuous mode“) empfängt der AP auch Pakete, die nicht an ihn gerichtet sind, sondern an andere Netzwerkteilnehmer.

Dieser Modus ist erforderlich, um einige der unten genannten Angriffe erkennen zu können. Der promiscuous mode beeinflusst allerdings die Leistung. Daher wird mit der Aktivierung des promiscuous mode automatisch die Frame Aggregation abgeschaltet.

Benachrichtigung via SYSLOG

Aktiviert oder deaktiviert die WIDS-Meldungen über SYSLOG.

Die generierte SYSLOG-Meldung besitzt den Severity Level „INFO“ und enthält den Zeitpunkt, die betroffene Schnittstelle sowie den Auslöser (Art des Angriffes und überschrittener Grenzwert).

Benachrichtigung via SNMP-Traps

Aktiviert oder deaktiviert die SNMP-Traps für WIDS-Meldungen.

Benachrichtigung via E-Mail an

Aktiviert oder deaktiviert die WIDS-Meldungen über E-Mail.

Zur Nutzung dieser Benachrichtigungen muss ein SMTP-Konto eingerichtet sein.

E-Mail-Empfänger

Geben Sie einen E-Mail-Empfänger an, wenn die Benachrichtigung über E-Mail aktiviert ist.

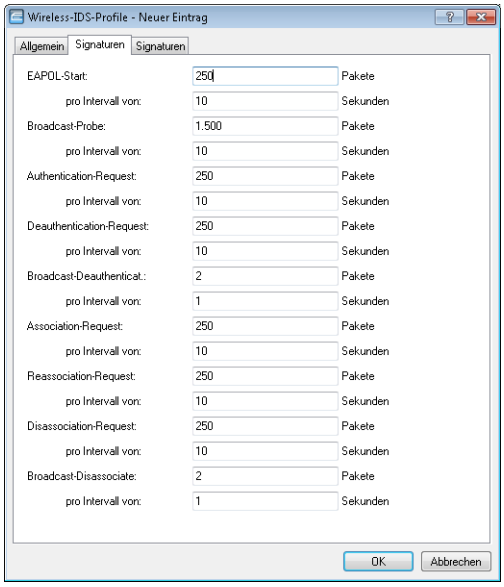
Das Feld muss eine gültige E-Mail-Adresse enthalten.

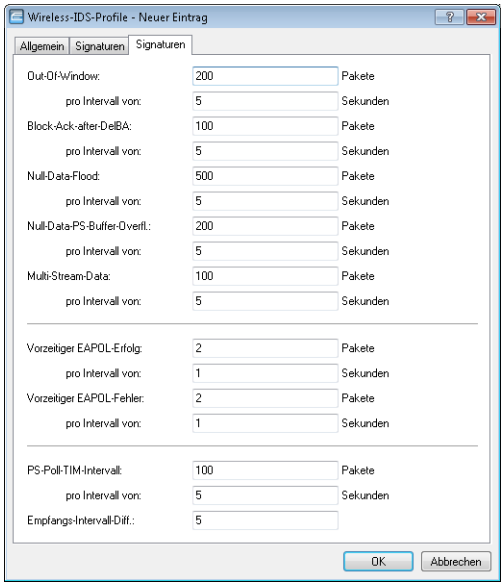
E-Mail-Aggregat-Intervall

Legen Sie die Verzögerung in Sekunden vor dem Versenden einer E-Mail fest, in der das WIDS nach dem Eintreffen eines ersten Wireless-IDS-Ereignisses weitere Ereignisse sammelt.

Diese Funktion verhindert, dass eine Flut von Angriffen eine E-Mail-Flut verursacht.

Auf den Reitern „Signaturen" konfigurieren Sie die Grenzwerte und Zeitintervalle (Datenpakete pro Sekunde) der verschiedenen Alarm-Funktionen des WIDS. Diese Werte regeln, wann das WIDS Warnungen generiert.





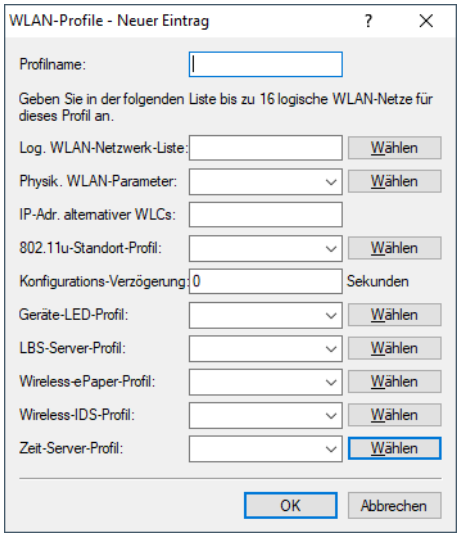
Die Angabe von Grenzwerten und Zeitintervallen für die folgenden Angriffs-Szenarien ist möglich:

- EAPOL-Start
- Broadcast-Probe
- Authentication-Request
- Deauthentication-Request (*)
- Broadcast-Deauthenticate
- Association-Request
- Reassociation-Request
- Disassociation-Request (*)
- Broadcast-Disassociate
- Out-Of-Window
- Block-Ack-after-DelBA
- Null-Data-Flood
- Null-Data-PS-Buffer-Overflow
- Multi-Stream-Data
- Vorzeitiger EAPOL-Erfolg (*)
- Vorzeitiger EAPOL-Fehler (*)
- PS-Poll-TIM-Intervall
- Empfangs-Intervall-Differenz

Alle Felder sind bereits mit für das jeweilige Angriffs-Szenario typischen Werten vorbelegt.

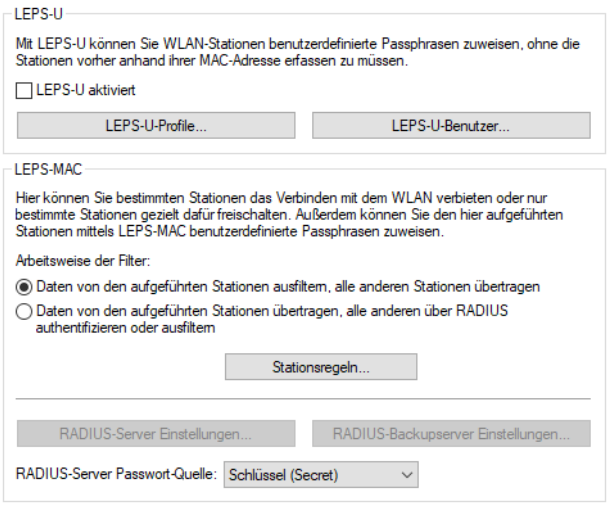
(*) Diese Angriffe werden nur bei aktivem promiscuous mode erkannt!

Speichern Sie das WIDS-Profil und ordnen Sie es anschließend unter **WLAN-Controller** > **Profile** > **WLAN-Profile** einem WLAN-Profil zu.



13.18.13 Auswahl der im WLAN zulässigen Stationen

In LANconfig konfigurieren Sie die Stationen (Clients), die sich über WLAN anmelden können, unter **Wireless-LAN** > **Stationen/LEPS**.



13.18.13.1 LEPS-U

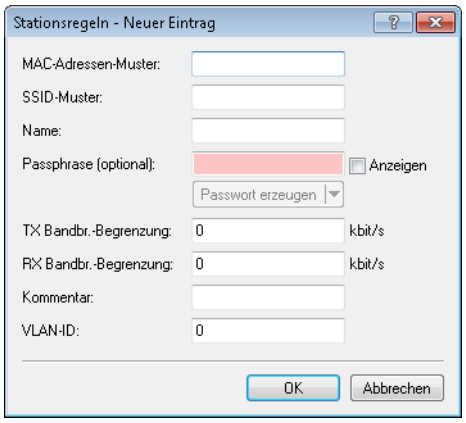
Siehe *LANCOM Enhanced Passphrase Security User (LEPS-U)* auf Seite 968.

13.18.13.2 Access Control List (LEPS-MAC)

Mit der **A**ccess **C**ontrol **L**ist (ACL) gewähren oder untersagen Sie einzelnen WLAN-Clients den Zugriff auf Ihr WLAN. Die Festlegung erfolgt anhand der fest programmierten MAC-Adressen der WLAN-Adapter.

Bei der zentralen Verwaltung der LANCOM WLAN-Router und LANCOM APs über einen WLC finden Sie die Stationstabelle unter **WLAN-Controller** > **Stationen/LEPS** > **LEPS-MAC** unter der Schaltfläche **Stationsregeln**.

Kontrollieren Sie unter **Wireless-LAN** > **Stationen/LEPS** > **LEPS-MAC**, ob die Einstellung **Daten von den aufgeführten Stationen übertragen, alle anderen über RADIUS authentifizieren oder ausfiltern** aktiviert ist. Fügen Sie neue Stationen, die an Ihrem Funk-Netzwerk teilnehmen sollen, ggf. über die Schaltfläche **Stationsregeln** hinzu.



MAC-Adressen-Muster

MAC-Adresse des WLAN-Clients, für den dieser Eintrag gilt. Die folgenden Eingaben sind möglich:

einzelne MAC-Adresse

Eine MAC-Adresse im Format `00a057112233`, `00-a0-57-11-22-33` oder `00:a0:57:11:22:33`.

Wildcards

Wildcards '*' und '?' für die Angabe von MAC-Adressbereichen, z. B. `00a057*`, `00-a0-57-11-??-??` oder `00:a0:??:11:*`.

Vendor-ID

Das Gerät hat eine Liste der gängigen Hersteller-OUIs (Organizationally Unique Identifier) gespeichert. Der MAC-Adressbereich ist gültig, wenn dieser Eintrag den ersten drei Bytes der MAC-Adresse des WLAN-Clients entspricht.

Die Verwendung von Wildcards ist möglich.

SSID-Muster

Dieser Eintrag begrenzt den Zugriff der WLAN-Clients mit den entsprechenden MAC-Adressen auf diese SSID.

Die Verwendung von Wildcards ist möglich, um den Zugriff auf mehrere SSIDs zu erlauben.

Name

Sie können zu jedem WLAN-Client einen beliebigen Namen und einen Kommentar eingeben. Dies ermöglicht Ihnen eine einfachere Zuordnung der MAC-Adressen zu bestimmten Stationen oder Benutzern.

Passphrase

Hier können Sie optional für jede physikalische Adresse (MAC) eine separate Passphrase eintragen, die in den 802.11i / WPA / AES-PSK gesicherten Netzwerken benutzt wird. Ohne die Angabe einer gesonderten Passphrase für diese MAC-Adresse werden die im Bereich **802.11i/WEP** für jedes logische Wireless-LAN-Netzwerk hinterlegten Passphrasen verwendet.

TX Bandbreitenbegrenzung

Sende-Bandbreiten-Begrenzung für die sich einbuchenden WLAN-Clients. Ein LANCOM Access Point im Client Modus übermittelt seine eigene Einstellung bei der Anmeldung an den Access Point. Dieser bildet daraus zusammen mit dem hier eingestellten Wert das Bandbreiten-Minimum als Bandbreiten-Begrenzung.

RX Bandbreitenbegrenzung

Empfangs-Bandbreiten-Begrenzung für die sich einbuchenden WLAN-Clients. Ein LANCOM Access Point im Client Modus übermittelt seine eigene Einstellung bei der Anmeldung an den Access Point. Dieser bildet daraus zusammen mit dem hier eingestellten Wert das Bandbreiten-Minimum als Bandbreiten-Begrenzung.

Die RX-Bandbreiten-Begrenzung ist nur aktiv für WLAN-Geräte im Client-Modus. Für normale WLAN-Clients wird dieser Wert nicht verwendet.

Kommentar

Hier können Sie einen Kommentar eintragen.

VLAN-ID

Diese VLAN-ID wird Paketen zugewiesen, die von dem Client mit der eingetragenen MAC-Adresse empfangen wurden. Bei der VLAN-ID '0' wird der Station keine spezielle VLAN-ID zugewiesen, es gilt die VLAN-ID der Funkzelle (SSID).

Falls sich Filterregeln widersprechen, hat die individuellere Regel eine höhere Priorität: Eine Regel ohne Wildcards in der MAC-Adresse oder SSID hat Vorrang vor einer Regel mit Wildcards. Ansonsten hat der Anwender beim Anlegen von

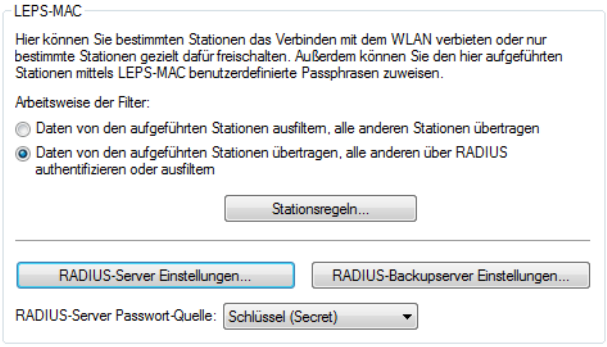
Einträgen darauf zu achten, dass sich die Filterregeln nicht widersprechen. Mit dem Trace-Aufruf `trace WLAN-ACL` in einer Telnet-Sitzung lassen sich die Filterangaben kontrollieren.

Die Filterkriterien in der Stationsliste erlauben oder verweigern den Zugriff von WLAN-Clients auf das WLAN-Netzwerk. Die Einträge **Name**, **Bandbreiten-Begrenzung**, **VLAN-ID** und **Passphrase** sind bedeutungslos, wenn das Gerät bei gültigen Filterkriterien den WLAN-Zugriff verweigert.

13.18.13.3 WLAN und RADIUS

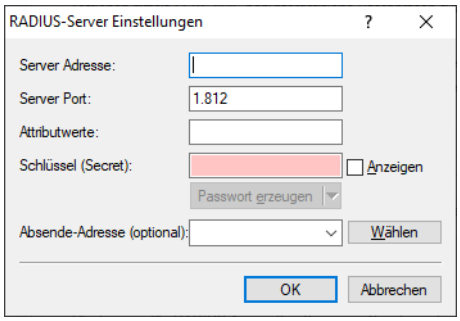
RADIUS wird für Nutzerauthentifizierung und Abrechnung verwendet. Näheres zu diesem Protokoll finden Sie im Kapitel *RADIUS* auf Seite 1219.

Bei der Verwendung eines RADIUS-Servers zur Authentifizierung von WLAN-Clients prüft der RADIUS-Server die Berechtigungen der Clients über die MAC-Adresse.



Zur Nutzung der RADIUS-Funktion für WLAN-Clients muss im Bereich **LEPS-MAC** die Arbeitsweise der Filter auf die Option „Daten von den aufgeführten Stationen übertragen, alle anderen über RADIUS authentifizieren oder ausfiltern“ ausgewählt sein.

Die Konfiguration erfolgt im LANconfig unter **Wireless-LAN** > **Stationen/LEPS** Konfigurieren Sie hier die **RADIUS-Server Einstellungen** sowie die Einstellungen für einen **RADIUS-Backupserver**.



Server Adresse

Geben Sie hier die IP-Adresse (IPv4, IPv6) oder den Host-Namen des RADIUS-Servers an, mit dem Sie zentral die Benutzer verwalten.

Server Port

Geben Sie hier den Port an, über den Sie mit Ihrem RADIUS-Server kommunizieren (Default: 1.812).

Attributwerte

LCOS ermöglicht es, die RADIUS-Attribute für die Kommunikation mit einem RADIUS-Server (sowohl Authentication als auch Accounting) zu konfigurieren.

Die Angabe der Attribute erfolgt als semikolon-separierte Liste von Attribut-Nummern oder -Namen und einem entsprechenden Wert in der folgenden Form:

`<Attribut_1>=<Wert_1>;<Attribut_2>=<Wert_2>`

Da die Anzahl der Zeichen begrenzt ist, lässt sich der Name abkürzen. Das Kürzel muss dabei eindeutig sein. Beispiele:

- `NAS-Port=1234` ist nicht erlaubt, da das Attribut nicht eindeutig ist (`NAS-Port`, `NAS-Port-Id` oder `NAS-Port-Type`).
- `NAS-Id=ABCD` ist erlaubt, da das Attribut eindeutig ist (`NAS-Identifier`).

Als Attribut-Wert ist die Angabe von Namen oder RFC-konformen Nummern möglich. Für das Gerät sind die Angaben `Service-Type=Framed` und `Service-Type=2` identisch.

Die Angabe eines Wertes in Anführungszeichen (`"<Wert>"`) ist möglich, um Sonderzeichen wie Leerzeichen, Semikolon oder Gleichheitszeichen mit angeben zu können. Das Anführungszeichen innerhalb des Wertes erhält einen umgekehrten Schrägstrich vorangestellt (`\"`), der umgekehrte Schrägstrich ebenfalls (`\\`).

Als Werte sind auch die folgenden Variablen erlaubt:

`%n`

Gerätename

`%e`

Seriennummer des Gerätes

`%%`

Prozentzeichen

`%{name}`

Original-Name des Attributes, wie ihn die RADIUS-Anwendung überträgt. Damit lassen sich z. B. Attribute mit originalen RADIUS-Attributen belegen: `Called-Station-Id=%{NAS-Identifier}` setzt das Attribut `Called-Station-Id` auf den Wert, den das Attribut `NAS-Identifier` besitzt.

Schlüssel (Secret)

Geben Sie hier den Schlüssel an, mit dem die Kodierung der Daten vorgenommen werden soll. Der Schlüssel muss ebenfalls im RADIUS-Server konfiguriert sein.

Backup-Server Adresse

Geben Sie hier die IP-Adresse (IPv4, IPv6) oder den Host-Namen des Backup-RADIUS-Servers an, mit dem Sie zentral die Benutzer verwalten.

Backup-Server Port

Geben Sie hier den Port an, über den Sie mit Ihrem Backup-RADIUS-Server kommunizieren (Default: 1.812).

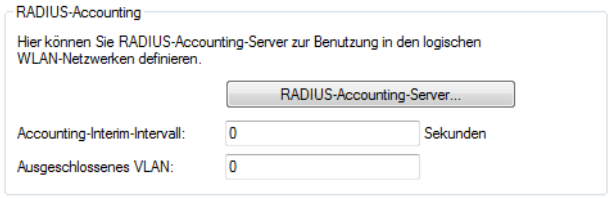
Absende-Adresse

Das Gerät ermittelt automatisch die richtige Absende-IP-Adresse für das Zielnetzwerk. Wollen Sie stattdessen eine fest definierte Absende-IP-Adresse verwenden, tragen Sie diese symbolisch oder direkt hier ein.

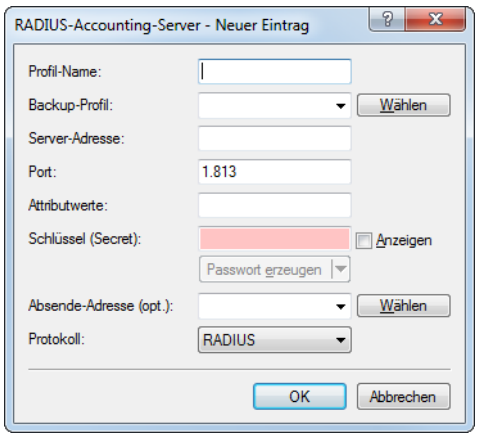
RADIUS-Server Passwort-Quelle

Stellen Sie ein, ob Sie als Passwort-Quelle für den RADIUS-Server einen **Schlüssel (Secret)** oder die **MAC-Adresse** verwenden wollen.

RADIUS-Accounting



Bei der Verwendung eines RADIUS-Servers zur Abrechnung muss dieser konfiguriert werden. Die Konfiguration erfolgt im LANconfig unter **Wireless-LAN** > **Stationen/LEPS** > **RADIUS-Accounting**. Konfigurieren Sie hier die die Einstellungen für einen **RADIUS-Accounting-Server**.



Profil-Name

Name des RADIUS-Servers, welcher das Accounting von WLAN-Clients durchführt. Sie verwenden den hier eingetragenen Namen, um aus anderen Tabellen auf den betreffenden Server zu referenzieren.

Backup-Profil

Name des RADIUS-Backup-Servers, welcher das Accounting von WLAN-Clients durchführt, falls der eigentliche Accounting-Server nicht verfügbar ist. Auf diese Weise lassen sich auch Backup-Server miteinander verketten, um mehrere Ausfall-Server festzulegen („Backup-Chaining").

Server-Adresse

Geben Sie hier die IPv4- oder IPv6-Adresse oder den Host-Namen des RADIUS-Servers an, mit dem der RADIUS-Client das Accounting von WLAN-Clients durchführt.

- Der RADIUS-Client erkennt automatisch, um welchen Adresstyp es sich handelt.
- Die allgemeinen Werte für Wiederholung und Timeout müssen Sie im RADIUS-Bereich ebenfalls festlegen.

Port

Port zur Kommunikation mit dem RADIUS-Server beim Accounting (Default: 1.812).

Attributwerte

Hier können sie RADIUS-Attribute mit benutzerdefinierten Werten versehen. Die einzelnen Namen-Werte-Paare müssen der Form <Name>=<Wert> entsprechen und sind durch Semikola voneinander getrennt.

<Name> identifiziert dabei das RADIUS-Attribut durch seinen Namen oder seine Nummer. Die zugehörigen Attributnamen finden Sie in den entsprechenden RADIUS RFCs. Attributsnamen können abgekürzt werden, solange die Bezeichner eindeutig sind.

Attributswerte können in Anführungsstriche gesetzt werden, um Leerzeichen oder Semikola in Wert-Definitionen zu benutzen. Um Anführungsstriche selbst als Zeichen zu nutzen, muß ein Backslash vorangestellt werden. Der Backslash als Zeichen wird durch ein Doppel-Backslash verfügbar.

Zusätzlich ist es möglich eine Reihe von Platzhalter einzusetzen:

- %n – wird ersetzt durch den konfigurierten Gerätenamen.
- %e – wird ersetzt mit der Seriennummer des Gerätes, wie man sie aus dem sysinfo des Gerätes kennt.
- %% – wird ersetzt durch ein einzelnes %-Zeichen.
- %{name} – wird ersetzt durch den ursprünglichen Wert des entsprechenden RADIUS-Attributes. Etwaige Neu / Um-Definitionen innerhalb dieser Attributsliste werden nicht beachtet! Der Bezeichner kann gekürzt werden, solange er eindeutig bleibt.

Mehr Informationen zu RADIUS-Attributen finden Sie unter *RADIUS-Attribute* auf Seite 1601.

Schlüssel (Secret)

Geben Sie hier den Schlüssel (Shared Secret) für den Zugang zum Accounting-Server an. Stellen Sie sicher, dass dieser Schlüssel im entsprechenden Accounting-Server übereinstimmend festgelegt ist.

Absende-Adresse

Hier können Sie optional eine Absendeadresse konfigurieren, die statt der ansonsten automatisch für die Zieladresse gewählten Absendeadresse verwendet wird.

Falls Sie z. B. Loopback-Adressen konfiguriert haben, können Sie diese hier als Absendeadresse angeben.

Als Adresse werden verschiedene Eingabeformen akzeptiert:

- Name des IP-Netzwerks (ARF-Netz), dessen Adresse eingesetzt werden soll.
- „INT“ für die Adresse des ersten Intranets.
- „DMZ“ für die Adresse der ersten DMZ.

  Wenn es eine Schnittstelle Namens „DMZ“ gibt, dann wird deren Adresse genommen.

- LB0 … LBF für eine der 16 Loopback-Adressen oder deren Name.
- Desweiteren kann eine beliebige IPv4- oder IPv6-Adresse in der üblichen Form angegeben werden.

Sofern die hier eingestellte Absendeadresse eine Loopback-Adresse ist, wird diese auch auf maskiert arbeitenden Gegenstellen unmaskiert verwendet.

Protokoll

Wählen Sie das Protokoll aus. Entweder **RADIUS** oder **RADSEC**. Mehr Informationen zu RADSEC finden Sie unter *RADSEC* auf Seite 1609.

Accounting-Interim-Intervall

Die Accounting-Funktion im Gerät kann u. a. dazu genutzt werden, das Budget von angeschlossenen WLAN-Clients zu kontrollieren. Wireless Internet Service Provider (WISPs) nutzen diese Möglichkeit teilweise zur Abrechnung ihrer Kunden. Da die Abrechnungsintervalle üblicherweise zum Monatsende wechseln, kann über eine entsprechende Aktion der Neustart aller aktuellen Accounting-Sitzungen ausgelöst werden – die eigentliche WLAN-Verbindung bleibt dabei bestehen. Mit Hilfe eines Cron-Jobs kann dieser Neustart komfortabel automatisiert werden, indem dort die Funktion `do /Setup/WLAN/RADIUS-Accounting/Neustart-Accounting` aufgerufen wird.

Ausgeschlossenens VLAN

Geben Sie hier die ID des VLANs ein, welches das Gerät vom RADIUS-Accounting ausschließen soll. Der RADIUS-Server erhält dann keine Informationen über den Verkehr dieses VLANs.

13.18.14 Verschlüsselungs-Einstellungen

Die APs der LANCOM-Familie unterstützen die aktuellsten Verfahren zur Verschlüsselung und Absicherung der Daten, die über eine WLAN-Verbindung übertragen werden.

- Der IEEE-Standard 802.11i/WPA steht für die höchste Sicherheit, die derzeit für WLAN-Verbindungen erreicht werden kann. Dieser Standard setzt u. a. auf ein neues Verschlüsselungsverfahren (AES-CCM) und erreicht im Zusammenspiel mit einigen anderen Methoden eine Sicherheit, die bisher nur von VPN-Verbindungen erzielt werden konnte. Beim Einsatz von AES-fähiger Hardware ist die Übertragung jedoch deutlich schneller als bei einer entsprechenden VPN-Absicherung.
- Aus Gründen der Kompatibilität zu älterer Hardware wird auch weiterhin das WEP-Verfahren unterstützt. WEP (**W**ired **E**quivalent **P**rivacy) war das ursprünglich im 802.11-Standard vorgesehene Verfahren zur Verschlüsselung der Daten bei Funkübertragungen. Dabei kommen Schlüssel von 40 (WEP64), 104 (WEP128) oder 128 Bit (WEP152) Länge zum Einsatz. Im Laufe der Zeit sind bei WEP jedoch einige Sicherheitslücken bekannt geworden, weshalb nach Möglichkeit nur noch die jeweils aktuellste 802.11i/WPA-Methode eingesetzt werden sollte.

Zur Vereinfachung der Konfiguration befinden sich die WLAN-Verschlüsselungseinstellungen ab LCOS 10.20 als zusätzlicher Reiter im Dialog zur Konfiguration der logischen WLAN-Einstellungen. Bei der Konfiguration einer SSID entfällt somit nun das aufwändige Wechseln zwischen dem Dialog der logischen WLAN-Einstellungen und dem Dialog der WLAN-Verschlüsselungseinstellungen.

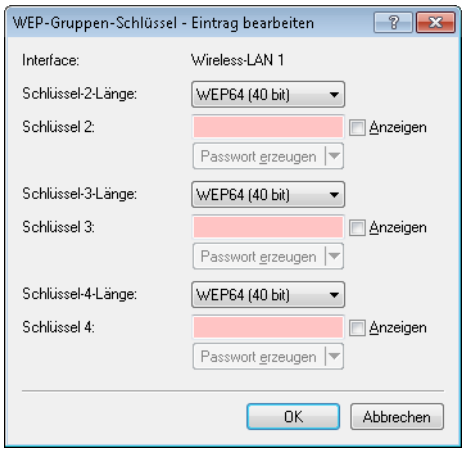
Die logischen WLAN-Einstellungen finden Sie unter **Wireless-LAN** > **Allgemein** > **Interfaces** > **Logische WLAN-Einstellungen**.

13.18.14.1 WEP-Gruppen-Schlüssel

Bei WEP kommen Schlüssel von 40 (WEP64), 104 (WEP128) oder 128 Bit (WEP152) Länge zum Einsatz. Für jedes WLAN-Interface stehen vier WEP-Schlüssel zur Verfügung: ein spezieller Schlüssel für jedes logische WLAN-Interface und drei gemeinsame Gruppen-WEP-Schlüssel für jedes physikalische WLAN-Interface.

Wenn bei der Verwendung von 802.1X/EAP unter **Wireless LAN** > **802.1X** > **Interfaces** die **Dynamische Schlüssel-Erzeugung und -Übertragung** aktiviert ist, werden die Gruppen-Schlüssel von 802.1X/EAP verwendet und stehen damit für die WEP-Verschlüsselung nicht mehr zur Verfügung.

Ab LCOS 9.00 stellt das System WPA- sowie WEP-Gruppen-Schlüssel an der Konsole nicht mehr im Klartext, sondern als Passworteingabe dar (********). In Folge dessen ist es nicht mehr möglich, diese Schlüssel z. B. per SNMP auszulesen.



LANconfig: **Wireless LAN** > **Verschlüsselung** > **WEP-Gruppen-Schlüssel**

Konsole: **Setup** > **Schnittstellen** > **WLAN** > **Gruppen-Schluessel**

Regeln für die Eingabe von WEP-Schlüsseln

Die WEP-Schlüssel können als ASCII-Zeichen oder in Hexadezimaler Darstellung eingetragen werden. Die hexadezimale Darstellung beginnt jeweils mit den Zeichen '0x'. Die Schlüssel haben je nach WEP-Verfahren folgende Länge:

Verfahren	ASCII	HEX
WEP 64	5 Zeichen Beispiel: 'aR45Z'	10 Zeichen Beispiel: '0x0A5C1B6D8E'
WEP 128	13 Zeichen	26 Zeichen
WEP 152	16 Zeichen	32 Zeichen

Der ASCII-Zeichensatz umfasst die Zeichen '0' bis'9', 'a' bis 'z', 'A' bis 'Z' sowie die folgenden Sonderzeichen: ! " # $ % & ´ () * + , - ./ : ; < = > ? @ [\ ] ^ _ ‘ { | } ~

In der HEX-Darstellung wird jedes Zeichen durch ein Zeichenpaar aus den Ziffern '0' bis'9' und den Buchstaben 'A' bis 'F' dargestellt, daher benötigen die HEX-Schlüssel die doppelte Anzahl an Zeichen zur Darstellung.

Wählen Sie die Länge und das Format (ASCII oder HEX) der Schlüssel immer nach den Möglichkeiten der Funknetzwerkkarten aus, die sich in Ihrem WLAN anmelden sollen. Wenn Sie im AP eine Verschlüsselung nach WEP 152 eingestellt haben, können manche Clients sich nicht mehr in diesem WLAN anmelden, weil sie die entsprechende Schlüssellänge nicht unterstützen.

13.18.14.2 Gruppenschlüssel pro VLAN

In einer VLAN-Umgebung weist die zentrale Netzwerkverwaltung jedem virtuellen Netz in der Regel eine eindeutige VLAN-ID zu. Die Zugehörigkeit zu einem VLAN ergibt sich meist über den physikalischen Anschluss, der den Netzwerk-Client mit dem Netz verbindet.

Die zentrale, das Netz verwaltende Station (z. B. ein VLAN-fähiger Switch) weist ihren Ports intern bestimmte VLAN-IDs zu. Trifft nun ein Datenpaket an einem Port ein, geschieht die interne Weiterleitung ausschließlich an Ports mit korrespondierenden VLAN-IDs. Alle anderen Netzteilnehmer, die an Ports mit abweichenden oder ohne VLAN-IDs angeschlossen sind, erhalten diese Datenpakete nicht.

Bei mehreren vorhandenen VLANs mit differenziertem Dienstumfang erfolgt die Trennung der Datenkommunikation meistens über die Zuweisung zu unterschiedlichen logischen WLAN-Netzen (SSIDs). Mitarbeiter erhalten z. B. über eine

spezielle SSID Zugriff auf das Firmennetzwerk und das Internet. Gäste hingegen erhalten über eine andere SSID eingeschränkten Zugriff auf das Internet.

LANCOM APs verwalten darüber hinaus in VLAN-Netzwerk-Tabellen die Zuordnung von WLAN-Clients zu einzelnen VLANs. In umfangreichen Netzwerkumgebungen übernimmt meist ein RADIUS-Server die Rechteverwaltung und Zuordnung der Clients zu genutzten VLANs. Nach erfolgreicher Authentifizierung übergibt der RADIUS-Server die Daten zurück an den entsprechenden AP. Für die Dauer der Client-Anmeldung speichert er sie in seiner VLAN-Netzwerk-Tabelle.

Bei Bedarf erhalten die verschiedenen WLAN-Clients, die am gleichen AP angemeldet sind, unterschiedliche VLAN-IDs. Dies geschieht durch die dynamischen VLAN-Netzwerk-Tabellen in den APs. Die VLAN-interne Kommunikation erfolgt abgesichert über einen bei der Anmeldung am AP ausgehandelten Sitzungsschlüssel. Somit ist die Datenübertragung der Clients in unterschiedlichen VLANs voneinander isoliert, obwohl jeder Client zur Kommunikation mit dem AP dasselbe logische WLAN-Netz (SSID) verwendet.

Meldet sich ein Client an einem AP eines WLAN-Netzes an, erhält er vom AP außerdem einen Gruppenschlüssel für den Empfang von Broad- oder Multicast-Nachrichten.

Broad- und Multicast-Nachrichten unterstützen kein VLAN-Tagging. Deshalb können WLAN-Clients, die sich in einem isolierten VLAN befinden, nicht vom Empfang dieser Nachrichten ausgeschlossen werden. Im Idealfall ignorieren die WLAN-Clients die Kommunikation über VLAN-fremde Broad- und Multicast-Nachrichten.

Da diese Nachrichten jedoch besonders zur Netzwerk-Konfiguration vermehrt zum Einsatz kommen, ergeben sich folgende Probleme:

- Netzwerkprotokolle wie „UPnP“ und „Bonjour“ nutzen diese Nachrichten, um neue Dienste im Netzwerk anzukündigen.

  Es ist also möglich, dass WLAN-Clients den Zugang zu Servern einrichten, auf die sie überhaupt nicht zugreifen können.

- Der Internetstandard IPv6 verwendet Multicast-Sendungen, um Routerinformationen an die Clients zu übermitteln.

  Die Gefahr besteht, dass VLAN-fremde WLAN-Clients diese Informationen übernehmen und sich damit den Zugriff auf das VLAN entziehen, für das sie eigentlich registriert sind.

Mit der zunehmenden Verbreitung von IPv6 werden auch diese Client-Probleme zunehmen.

Um diese Probleme zu vermeiden, kann der AP statt eines für alle WLAN-Clients gültigen Gruppenschlüssels jedem verwendeten VLAN einen separaten Gruppenschlüssel zuweisen. Er schickt somit seine Broad- und Multicast-Sendungen nicht mehr an alle vorhandenen WLAN-Clients, sondern ausschließlich an ein bestimmtes VLAN und an die dort registrierten Clients. Die WLAN-Clients anderer VLANs können diese Sendungen nun nicht mehr entschlüsseln.

Der IEEE 802.11-Standard sieht die Verwaltung von 4 unterschiedlichen Schlüsseln vor. Ein Schlüssel ist dabei immer für die gesicherte Unicast-Kommunikation zwischen dem AP und einem WLAN-Client reserviert.

Es können prinzipiell also maximal 3 separate VLANs über eigene Gruppenschlüssel verwaltet werden. Die jeweiligen Gruppenschlüssel werden dabei entweder automatisch vom AP oder manuell vom Netzwerk-Administrator verwaltet. Während der Anmeldung des WLAN-Clients am Netzwerk überträgt der AP ihm den zugehörigen VLAN-Gruppenschlüssel zur Entschlüsselung aller für sein VLAN bestimmten Broad- und Multicast-Sendungen.

Damit ergeben sich 2 mögliche Szenarien:

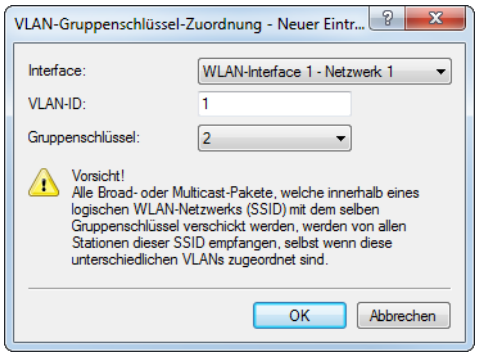
- Höchstens 3 VLANs sind im Bereich eines APs eingerichtet: Durch die 3 spezifischen VLAN-Gruppenschlüssel sind diese VLANs sicher voneinander getrennt.
- Mehr als 3 VLANs existieren im Bereich eines APs: Hierbei teilen sich mindestens 2 VLANs einen Gruppenschlüssel. Der Administrator muss die geteilten Gruppenschlüssel optimal auf die VLANs aufteilen.

Die Verwaltung der VLAN-Gruppenschlüssel erfolgt in 2 Tabellen:

- Die Konfigurations-Tabelle, in der die Zuordnung manuell durch den Administrator erfolgt.
- Die Status-Tabelle, in der die automatische Gruppenschlüssel-Zuordnung durch den AP abzulesen ist.

Verwaltung von VLAN-Gruppenschlüsseln

Wenn Sie vorhaben, verschiedene VLAN-IDs auf einem logischen WLAN-Netzwerk (SSID) zu verwenden, besteht die Möglichkeit den entsprechenden Gruppenschlüssel für Broad- und Multicast-Sendungen zuzuordnen. In LANconfig finden Sie diese Einstellung unter **Wireless-LAN** > **Verschlüsselung** > **VLAN-Gruppenschlüssel-Zuordnung**



Die automatische Zuordnung der Gruppenschlüssel durchläuft folgende Schritte:

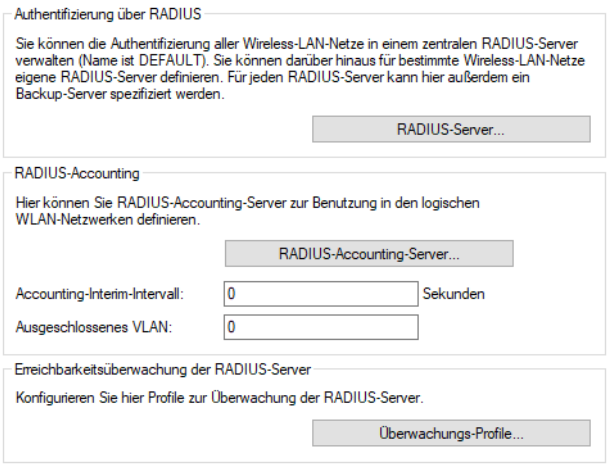
1. Wenn sich ein WLAN-Client anmeldet, überprüft der AP, ob dessen VLAN-ID bereits in der Statustabelle gelistet und entsprechend einem Gruppenschlüssel zugeordnet ist.
2. Falls nicht, überprüft der AP anhand der Konfigurationstabelle, ob eine manuelle Zuordnung besteht. In diesem Fall erstellt er einen entsprechend gemappten Eintrag in dieser Tabelle.
3. Falls auch keine manuelle Zuordnung besteht, fügt der AP einen neuen Eintrag hinzu und ordnet diesem Client den Gruppenschlüssel mit den wenigsten Teilnehmern zu.

Die Statustabelle mit den aktuellen automatischen VLAN-Gruppenschlüssel-Zuordnungen je SSID finden Sie auf der Konsole unter **Status** > **WLAN** > **VLAN-Gruppenschlüssel-Abbildung**

13.18.15 IEEE 802.1X / EAP

Der internationale Industrie-Standard IEEE 802.1X und das Extensible **A**uthentication **P**rotocol (EAP) ermöglichen Basis-Stationen die Durchführung einer zuverlässigen und sicheren Zugangskontrolle. Die Zugangsdaten können zentral auf einem RADIUS-Server verwaltet und von der Basis-Station bei Bedarf von dort abgerufen werden. RADIUS wird für Nutzerauthentifizierung und Abrechnung verwendet. Näheres zu diesem Protokoll finden Sie im Kapitel *RADIUS* auf Seite 1219.

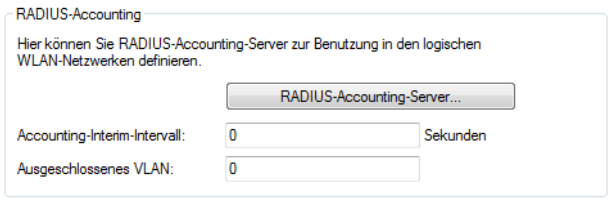
In LANconfig konfigurieren Sie die RADIUS-Server unter **Wireless-LAN** > **802.1X**.



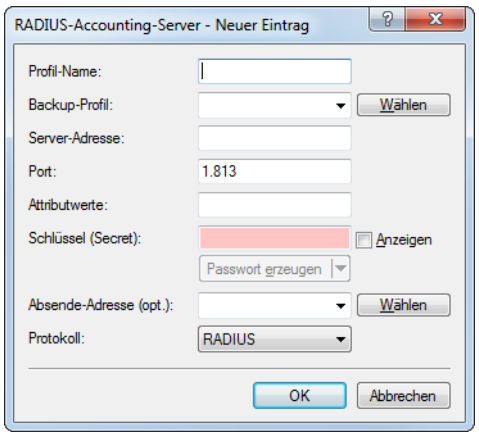
Eine Beschreibung der Konfiguration eines RADIUS-Servers für IEEE 802.1X finden Sie unter *Einwahl über 802.1X und RADIUS* auf Seite 1580.

13.18.15.1 RADIUS-Accounting

RADIUS wird für Nutzerauthentifizierung und Abrechnung verwendet. Näheres zu diesem Protokoll finden Sie im Kapitel *RADIUS* auf Seite 1219.



Bei der Verwendung eines RADIUS-Servers zur Abrechnung muss dieser konfiguriert werden. Die Konfiguration erfolgt im LANconfig unter **Wireless-LAN** > **802.1X** > **RADIUS-Accounting**. Konfigurieren Sie hier die die Einstellungen für einen **RADIUS-Accounting-Server**.



Profil-Name

Name des RADIUS-Servers, welcher das Accounting von WLAN-Clients durchführt. Sie verwenden den hier eingetragenen Namen, um aus anderen Tabellen auf den betreffenden Server zu referenzieren.

Backup-Profil

Name des RADIUS-Backup-Servers, welcher das Accounting von WLAN-Clients durchführt, falls der eigentliche Accounting-Server nicht verfügbar ist. Auf diese Weise lassen sich auch Backup-Server miteinander verketten, um mehrere Ausfall-Server festzulegen („Backup-Chaining").

Server-Adresse

Geben Sie hier die IPv4- oder IPv6-Adresse oder den Host-Namen des RADIUS-Servers an, mit dem der RADIUS-Client das Accounting von WLAN-Clients durchführt.

- Der RADIUS-Client erkennt automatisch, um welchen Adresstyp es sich handelt.
- Die allgemeinen Werte für Wiederholung und Timeout müssen Sie im RADIUS-Bereich ebenfalls festlegen.

Port

Port zur Kommunikation mit dem RADIUS-Server beim Accounting (Default: 1.812).

Attributwerte

Hier können sie RADIUS-Attribute mit benutzerdefinierten Werten versehen. Die einzelnen Namen-Werte-Paare müssen der Form <Name>=<Wert> entsprechen und sind durch Semikola voneinander getrennt.

<Name> identifiziert dabei das RADIUS-Attribut durch seinen Namen oder seine Nummer. Die zugehörigen Attributnamen finden Sie in den entsprechenden RADIUS RFCs. Attributsnamen können abgekürzt werden, solange die Bezeichner eindeutig sind.

Attributswerte können in Anführungsstriche gesetzt werden, um Leerzeichen oder Semikola in Wert-Definitionen zu benutzen. Um Anführungsstriche selbst als Zeichen zu nutzen, muß ein Backslash vorangestellt werden. Der Backslash als Zeichen wird durch ein Doppel-Backslash verfügbar.

Zusätzlich ist es möglich eine Reihe von Platzhalter einzusetzen:

- %n – wird ersetzt durch den konfigurierten Gerätenamen.
- %e – wird ersetzt mit der Seriennummer des Gerätes, wie man sie aus dem sysinfo des Gerätes kennt.
- %% – wird ersetzt durch ein einzelnes %-Zeichen.
- %{name} – wird ersetzt durch den ursprünglichen Wert des entsprechenden RADIUS-Attributes. Etwaige Neu / Um-Definitionen innerhalb dieser Attributsliste werden nicht beachtet! Der Bezeichner kann gekürzt werden, solange er eindeutig bleibt.

Mehr Informationen zu RADIUS-Attributen finden Sie unter *RADIUS-Attribute* auf Seite 1601.

Schlüssel (Secret)

Geben Sie hier den Schlüssel (Shared Secret) für den Zugang zum Accounting-Server an. Stellen Sie sicher, dass dieser Schlüssel im entsprechenden Accounting-Server übereinstimmend festgelegt ist.

Absende-Adresse

Hier können Sie optional eine Absendeadresse konfigurieren, die statt der ansonsten automatisch für die Zieladresse gewählten Absendeadresse verwendet wird.

Falls Sie z. B. Loopback-Adressen konfiguriert haben, können Sie diese hier als Absendeadresse angeben.

Als Adresse werden verschiedene Eingabeformen akzeptiert:

- Name des IP-Netzwerks (ARF-Netz), dessen Adresse eingesetzt werden soll.
- „INT“ für die Adresse des ersten Intranets.
- „DMZ“ für die Adresse der ersten DMZ.

  Wenn es eine Schnittstelle Namens „DMZ“ gibt, dann wird deren Adresse genommen.

- LB0 … LBF für eine der 16 Loopback-Adressen oder deren Name.
- Desweiteren kann eine beliebige IPv4- oder IPv6-Adresse in der üblichen Form angegeben werden.

Sofern die hier eingestellte Absendeadresse eine Loopback-Adresse ist, wird diese auch auf maskiert arbeitenden Gegenstellen unmaskiert verwendet.

Protokoll

Wählen Sie das Protokoll aus. Entweder **RADIUS** oder **RADSEC**. Mehr Informationen zu RADSEC finden Sie unter *RADSEC* auf Seite 1609.

Accounting-Interim-Intervall

Die Accounting-Funktion im Gerät kann u. a. dazu genutzt werden, das Budget von angeschlossenen WLAN-Clients zu kontrollieren. Wireless Internet Service Provider (WISPs) nutzen diese Möglichkeit teilweise zur Abrechnung ihrer Kunden. Da die Abrechnungsintervalle üblicherweise zum Monatsende wechseln, kann über eine entsprechende Aktion der Neustart aller aktuellen Accounting-Sitzungen ausgelöst werden – die eigentliche WLAN-Verbindung bleibt dabei bestehen. Mit Hilfe eines Cron-Jobs kann dieser Neustart komfortabel automatisiert werden, indem dort die Funktion `do /Setup/WLAN/RADIUS-Accounting/Neustart-Accounting` aufgerufen wird.

Ausgeschlossenens VLAN

Geben Sie hier die ID des VLANs ein, welches das Gerät vom RADIUS-Accounting ausschließen soll. Der RADIUS-Server erhält dann keine Informationen über den Verkehr dieses VLANs.

Accounting-Statustypen "Accounting-On" und "Accounting-Off"

RADIUS-Server und AP tauschen Status-Informationen wie Start, Ende oder Update von Client-Sessions am AP aus. Diese Datenpakete orientieren sich am Verhalten des angemeldeten Clients.

Mit den Statustypen "Accounting-On" und "Accounting-Off" gibt der AP Informationen über seine generelle Eignung für das RADIUS-Accounting an den RADIUS-Server weiter:

Accounting-On

Wenn das Gerät in einen Betriebszustand wechselt, in dem es Accounting-Informationen mit einem RADIUS-Server austauschen kann, sendet es ein "Accounting-On".

Accounting-Off

Wenn das Gerät in einen Betriebszustand wechselt, in dem es keine Accounting-Informationen mit einem RADIUS-Server austauschen kann, sendet es ein "Accounting-Off".

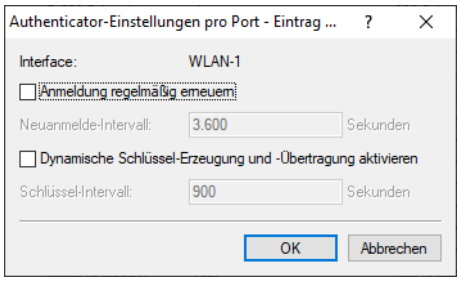
Die folgenden Bedingungen lösen die Übertragung eines "Accounting-On" oder "Accounting-Off" aus:

- Das Gerät aktiviert oder deaktiviert eine physikalische WLAN-Schnittstelle mit der entsprechenden SSID.

  Die Deaktivierung kann auch die Folge von Überhitzung, Verbindungsverlust oder fehlerhafter Link-Erkennung sein.
- Die WLAN-Schnittstelle wechselt in einen nicht-AP-Modus (also weder 'managed' noch Stand-alone-AP) oder zurück.
- Im P2P-Modus wechselt das Gerät in die Betriebsart "exklusiv", was alle SSIDs deaktiviert.
- Das Gerät aktiviert oder deaktiviert eine SSID.
- Das Gerät aktiviert oder deaktiviert das RADIUS-Accounting für eine SSID.

13.18.15.2 Automatischer Wechsel von WEP-Schlüsseln

IEEE 802.1X ermöglicht außerdem den gesicherten Versand und den regelmäßigen automatischen Wechsel von WEP Schlüsseln. Auf diese Weise verbessert IEEE 802.1X die Sicherungswirkung von WEP.



LANconfig: **Schnittstellen** > **802.1X-Authenticator** > **LAN** > **Authenticator-Einstellungen pro Port**

Konsole: **Setup** > **IEEE802.1X**

Anmeldung regelmäßig erneuern

Hier aktivieren Sie die regelmäßige Neuanmeldung. Wird eine Neuanmeldung gestartet, so bleibt der Benutzer während der Verhandlung weiterhin angemeldet.

Neuanmelde-Intervall

Intervall für die regelmäßige Neuanmeldung. Standardwert für das Neuanmelde-Intervall ist 3.600 Sekunden.

Dynamische Schlüssel-Erzeugung und Übertragung aktivieren

Hier aktivieren Sie die regelmäßige Erzeugung dynamischer WEP-Schlüssel und deren Übertragung.

Schlüssel-Intervall

Intervall für die regelmäßige Erzeugung der Schlüssel.

Spezielle Datenrate für EAPOL-Pakete

EAP over LAN (EAPOL) wird zur Anmeldung über WPA und / oder 802.1X von WLAN-Clients an APs verwendet. Dabei werden die EAP-Pakete zum Austausch der Authentisierungsinformationen in Ethernetframes gekapselt, um die EAP-Kommunikation über eine Layer-2 Verbindung zu ermöglichen.

In manchen Fällen ist es sinnvoll, die Datenrate für die Übertragung der EAPOL-Pakete niedriger zu wählen als die Datenrate für die Nutzdaten. Bei bewegten WLAN-Clients kann z. B. eine zu hohe Datenrate der EAPOL-Pakete zu Paketverlusten führen und so den Anmeldevorgang deutlich verzögern. Durch die gezielte Auswahl der EAPOL-Datenrate kann dieser Vorgang stabilisiert werden.

Konsole: **Setup** > **Schnittstellen** > **WLAN** > **Übertragung**

› **EAPOL-Rate**

Legen Sie hier die Datenrate für die Übertragung der EAPOL-Pakete fest.

Mögliche Werte:

› Wie-Daten, Auswahl aus den angebotenen Geschwindigkeiten

Default:

› Wie-Daten

Besondere Werte:

› Wie-Daten überträgt die EAPOL-Daten mit der gleichen Datenrate wie die Nutzdaten.

13.18.16 IEEE 802.11u und Hotspot 2.0

Ihr Gerät unterstützt WLAN-Verbindungen nach dem IEEE-Standard 802.11u und – darauf aufbauend – die Hotspot-2.0-Spezifikation. Über 802.11u haben Sie die Möglichkeit, in einem lokalen WLAN-Netzwerk (z. B. innerhalb Ihrer Firma) oder einem Public Spot-Netzwerk die automatische Authentisierung und Authentifizierung Ihrer Nutzer zu realisieren. Voraussetzung dafür ist, dass die betreffenden Stationen (Smartphones, Tablet-PCs, Notebooks, usw.) Verbindungen nach 802.11u und Hotspot 2.0 auch unterstützen. Folgende Funktionen bieten sich Ihnen im Detail:

› **Automatische Netzwerkwahl**

In einer 802.11u-fähigen Umgebung entfällt für einen Benutzer die manuelle Suche und Auswahl einer SSID. Stattdessen übernehmen die Stationen eigenständig die Suche und Auswahl eines geeigneten Wi-Fi-Netzwerks, indem sie selbstständig die Betreiber- und Netzwerkdaten aller 802.11u-fähigen Access Points in Reichweite erfragen und auswerten. Eine vorangehende Anmeldung am Access Point ist dabei nicht erforderlich.

Mit Hotspot 2.0 erhalten Stationen überdies die Möglichkeit, Informationen über die in einem Wi-Fi-Netzwerk verfügbaren Dienste abzurufen. Sind spezifische, für einen Benutzer aber relevante Dienste (z. B. Verbindungen via HTTP, VPN oder VoIP) für ein Wi-Fi-Netzwerk nicht verfügbar, werden alle Netzwerke, die die Kriterien nicht erfüllen, von der weiteren Suche ausgeschlossen. Somit ist sichergestellt, dass Nutzer immer das für sie optimale Netzwerk erhalten.

› **Automatische Authentisierung und Authentifizierung**

In einer 802.11u-fähigen Umgebung übernimmt die Station automatisch die Anmeldung des Benutzers, sofern die notwendigen Zugangsdaten vorliegen. Die Authentifizierung kann z. B. anhand einer SIM-Karte, eines Benutzernamens und Passworts, oder eines digitalen Zertifikats erfolgen. Ein manuelles und wiederholtes Eingeben der Zugangsdaten in eine Anmeldemaske durch den Benutzer entfällt. Nach erfolgreicher Authentifizierung kann der Nutzer die benötigten Dienste unmittelbar nutzen.

› **Unterbrechungsfreie Verbindungsübergabe (Seamless Handover)**

Verbindungen nach 802.11u ermöglichen im Zusammenspiel mit 802.21 die unterbrechungsfreie Übergabe von Datenverbindungen über verschiedene Netzwerktypen hinweg. Dies erlaubt es Nutzern, mit ihren Stationen aus dem

Mobilfunknetz unterbrechungsfrei in ein WLAN-Netz zu wechseln, sobald sie in den Empfangsbereich einer entsprechenden Hotspot-2.0-Zone kommen – und umgekehrt. Gleiches gilt für den Wechsel zwischen verschiedenen Betreibern, wenn Nutzer z. B. während einer Busfahrt von einem homogenen Netzwerk in ein anderes wechseln.

- **Automatisches Roaming**

  Verbindungen nach 802.11u ermöglichen das Roaming über unterschiedliche Betreibernetzwerke hinweg. Gelangt ein Benutzer in die Hotspot-2.0-Zone eines Betreibers, für den er keine Authentifizierungsdaten besitzt, besteht für seine Station dennoch die Option, in das Heimnetzwerk zu roamen. Die Authentifizierung an der fremden Hotspot-2.0-Zone erfolgt dann durch den Roaming-Partner des Betreibers, was den Nutzer schließlich zur Nutzung des fremden Wi-Fi-Netzwerks berechtigt. Neben Gebieten, in denen nur einzelne Netzwerkbetreiber mit Acess Points präsent sind, gewinnt diese Möglichkeit vor allem auch für Auslandsreisende an Attraktivität.

Beispiel: Angenommen, ein Nutzer ist mit seinem 802.11u-fähigen Smartphone (seiner Station) in der Stadt unterwegs und aktiviert die WLAN-Funktion, um im Internet zu surfen. Die Station beginnt daraufhin damit, alle verfügbaren Wi-Fi-Netzwerke in der Umgebung zu suchen. Bietet ein Teil der dazugehörigen Access Points 802.11u an, wählt die Station anhand der vorab erhaltenen Betreiber- und Netzinformationen dasjenige Netzwerk aus, welches am besten zum benötigten Dienst passt – z. B. einen Hotspot der eigenen Mobilfunkgesellschaft mit Internetfreigabe. Die anschließende Authentifizierung kann in diesem Fall automatisch über die SIM-Karte erfolgen, sodass der Benutzer während des gesamten Vorgangs nicht mehr einzugreifen braucht. Die für die Verbindung gewählte Verschlüsselungsmethode – z. B. WPA2 – bleibt davon unberührt.

Zusammengefasst verknüpfen Datenverbindungen nach 802.11u und mit aktiviertem Hotspot 2.0 die Sicherheitsmerkmale und Leistungsfähigkeit klassischer Wi-Fi-Hot-Spots mit der Flexibilität und Einfachheit von Datenverbindungen über Mobilfunk. Zeitgleich entlasten sie die Mobilfunknetzwerke, indem sie den Datenverkehr (und ggf. auch die Telefonie) auf die Netzstrecken und Frequenzbänder der Access Points umverteilen.

Passpoint® Release 2

Ab LCOS 10.40 ist die erweiterte Hotspot 2.0-Funktionalität Ihres WLAN-Gerätes nach dem von der Wi-Fi Alliance spezifizierten Passpoint® Release 2 konfigurierbar. Der im LCOS integrierte RADIUS-Server beinhaltet ab Version 10.32 RU4 die benötigten Features.

Passpoint® Release 2 vereinfacht das Onboarding von Geräten in ein Netz mit der Verschlüsselungsmethode WPA2-Enterprise (802.1X). Mittels eigener Onboarding-SSID kann ein Benutzer sich ein Profil auf Passpoint® Release 2-fähige Endgeräte installieren und dann automatisch mit den hinterlegten Anmeldedaten ins verschlüsselte Netz wechseln. Somit lassen sich Hotspots realisieren, die verschlüsselte drahtlose Kommunikation ermöglichen. Hierbei können die Gäste über eine offene Onboarding-SSID mit zeitlich begrenzten Zugangsdaten ausgestattet werden.

Ebenso kann ein Mobilfunkanbieter sein Mobilfunknetz entlasten, indem er Wi-Fi Offloading einführt und mobile Endgeräte, die mit einer SIM-Karte ausgestattet sind, automatisch in sein WLAN-Netz einbuchen lässt. Die Endgeräte der Kunden finden das WLAN-Netz des Mobilfunkanbieters automatisch und buchen sich mit den hinterlegten Benutzerdaten der SIM-Karte automatisch in das WLAN-Netz des Betreibers ein.

Mit Passpoint® Release 2 wird die Hotspot 2.0-Funktionalität um die folgenden Features erweitert:

- Online Sign-Up (OSU) – Mit Passpoint® Release 2 bekommen Unternehmen und Netzbetreiber die Möglichkeit, Benutzerprofile über einen so genannten „Online Sign-Up"-Server (OSU-Server) zur Verfügung zu stellen. Über eine offene OSU-SSID hat der Benutzer die Möglichkeit, verschiedene OSU-Server anhand von hinterlegten Icons zu identifizieren und somit den für ihn passenden auszuwählen. Der OSU-Server kann ggf. Benutzerdaten abfragen, bevor er ein passendes Profil für das Endgerät des Benutzers bereitstellt. Neben der offenen OSU-SSID kann auch eine verschlüsselte SSID genutzt werden, welche mittels „anonymous EAP-TLS" die Benutzerdaten verschlüsselt abfragt und bereitstellt. Hierfür wird ein entsprechender RADIUS-Server mit „anonymous EAP-TLS" Unterstützung benötigt.

  Ein OSU-Server ist kein Bestandteil des LCOS. Es gibt allerdings Lösungen von LANCOM Partnern.

- OSU-Icons – Für die unterstützten OSU-Server können im LCOS über die WEBconfig im Bereich **Dateimanagement** entsprechende Icons als Datei hochgeladen werden. Als Dateiformat empfehlen wir PNG.

- Benachrichtigungsmöglichkeit – Auf Netzseite gibt es die Möglichkeit, den Benutzer zu benachrichtigen, wenn eine Abmeldung seitens RADIUS-Server kurz bevor steht. Dies kann z. B. der Fall sein, wenn die Benutzerdaten nicht mehr länger gültig sind oder die festgelegte Verbindungsdauer erreicht wurde.
- QoS Map – Ein Access Point kann über die Funktion „QoS Map Set" seine Clients anweisen, eine bestimmte QoS Map zu verwenden. Hierbei werden die Werte für das Contention Window (Medienzugriff via EDCA) der verschiedenen Access Categories für Voice, Video, Best Effort und Background-Datenpakete und deren zugehörige DSCP-Werte definiert. Gleichzeitig nutzt auch der Access Points die in der QoS Map hinterlegten Werte.

  Aktuell stehen neben den zwei durch die Wi-Fi Alliance vorgegebenen QoS Maps nur die Standard-QoS-Map des LCOS zur Verfügung.

13.18.16.1 Hotspot-Betreiber und -Service-Provider

Die Hotspot-2.0-Spezifikation der Wi-Fi Alliance unterscheidet zwischen Hotspot-Betreibern und Hotspot-Service-Providern: Ein **Hotspot-Betreiber** unterhält lediglich ein Wi-Fi-Netzwerk, während ein **Hotspot-Service-Provider** (SP) die Verbindung der Nutzer ins Internet oder Mobilfunknetz realisiert. Natürlich ist es möglich, dass ein Betreiber gleichzeitig ein SP ist. In allen anderen Fällen jedoch benötigt ein Hotspot-Betreiber entsprechende Roaming-Vereinbarungen mit einem SP oder einem Zusammenschluss mehrerer SP (Roaming-Konsortium genannt). Erst wenn ein Betreiber diese Vereinbarungen getroffen hat, sind Kunden der entsprechenden Roaming-Partner dazu in der Lage, sich am Hotspot des Betreibers zu authentifizieren. Jeder Service-Provider betreibt dazu seine eigene AAA-Infrastruktur. Die Liste der möglichen Roaming-Partner und der Name des Hotspot-Betreibers teilt ein Hotspot den Stationen über ANQP mit (siehe Funktionsbeschreibung).

13.18.16.2 Funktionsbeschreibung

Bei 802.11u handelt es sich um den Basis-Standard der IEEE. Dieser Standard erweitert Access Points bzw. Hotspots im Wesentlichen um die Fähigkeit, sogenannte „ANQP-Datenpakete" (Advanced Message Queuing Protocol) in seinen Funksignalen auszustrahlen. ANQP ist ein Query / Response-Protokoll, mit dem ein Gerät eine Reihe von Informationen über den Hotspot abfragen kann. Hierzu gehören sowohl Metadaten, wie z. B. Angaben zum Betreiber und dem Standort, als auch Angaben zum dahinterliegenden Netzwerk, wie z. B. Angaben zu Betreiber-Domänen, Roaming-Partnern, den Authentifizierungsmethoden, Weiterleitungsadressen, usw. Alle 802.11u-fähigen Geräte in Reichweite haben die Möglichkeit, diese Datenpakete ohne vorangehende Anmeldung am Access Point abzufragen, um anhand ihrer die Netzwerkwahl und den -beitritt zu entscheiden.

Die Wi-Fi Alliance hat dem Standard weitere ANQP-Elemente hinzugefügt und vermarktet diese Spezifikation als **Hotspot 2.0**. Die Hotspot-2.0-Funktion ist somit lediglich eine Erweiterung des Standards um zusätzliche Elemente, die Geräte bei ihrer Netzwerkwahl als Kriterien heranziehen können. Hierzu gehören z. B. Angaben zu den am Hotspot verfügbaren Diensten und WAN-Metriken. Das dazugehörige Zertifizierungsprogramm heisst Passpoint®, welches in verschiedenen Ausbaustufen gibt. Bestimmte LANCOM Access Points sind von der Wi-Fi Alliance Passpoint® CERTIFIED (Release 1 und / oder 2).

ANQP-Datenpakete stellen also das zentrale Informationselement des 802.11u-Standards dar. Um die Unterstützung für 802.11u zu signalisieren und die Datenpakete zu übertragen, bedarf es allerdings noch weiterer Elemente, die für den Betrieb von 802.11u essentiell sind:

- Die Signalisierung der 802.11u-Unterstützung in den Beacons und Probes eines Hotspots erfolgt durch das sogenannte „Interworking-Element". In ihm sind bereits erste grundlegende Netzwerkinformationen – wie z. B. die Netzklassifikation, die Internetverfügbarkeit (Internet-Bit) und die OI des Roaming-Konsortiums und / oder des Betreibers – enthalten. Zugleich dient es 802.11u-fähigen Geräten als erstes Filterkriterium bei der Netzsuche.
- Die Übertragung der ANQP-Datenpakete erfolgt innerhalb der sogenannten GAS-Container. GAS steht für Generic Advertisement Service und bezeichnet generische Container, welche einem Gerät erlauben, vom Hotspot – ergänzend zu den Informationen in den Beacons – erweiterte interne und externe Informationen für die Netzwahl abzufragen. Die GAS-Container werden ihrerseits durch sogenannte Public Action Frames auf Layer 2 übermittelt.

Anmeldung eines 802.11u-fähigen Clients an einem Hotspot 2.0

Diese Funktionsbeschreibung erläutert schematisch Auswahl und Anmeldevorgang eines 802.11u-fähigen Geräts an einem Hotspot 2.0.

Anmeldung via Benutzername / Passwort oder digitalem Zertifikat

1. Die Hotspots antworten daraufhin mit einem ANQP-Response, der u. a. jeweils den Namen des Hotspot-Betreibers sowie eine Liste der NAI-Realms enthält, welche alle verfügbaren Roaming-Partner (Service-Provider, kurz SP) auflistet.
2. Das Gerät lädt die auf ihm lokal abgespeicherten Zugangsdaten aus den vom Benutzer eingerichten WLAN-Profilen oder installierten Zertifikaten, und gleicht die dortigen Realms mit den unter (2) erhaltenen NAI-Realm-Listen ab.
   a. Erzielt das Gerät hierbei einen Treffer, weiß es, dass es sich bei betreffenden Wi-Fi-Netzwerk erfolgreich authentisieren kann.
   b. Erzielt das Gerät mehrere Treffer, erfolgt die Auswahl eines Wi-Fi-Netzwerks anhand einer vom Benutzer eingerichteten Präferenzliste. Diese Liste legt die Reihenfolge der bevorzugten Betreiber im Zusammenhang mit den möglichen Roaming-Partnern fest. Das Gerät vergleicht hierbei die unter (2) erhaltenen Betreiber-Namen mit der Liste und wählt jenen Betreiber aus, der die höchste Priorität besitzt.
3. Das Gerät authentisiert sich mit seinen lokalen Zugangsdaten am Hotspot des bevorzugten Betreibers für den passenden SP. Der Access Point übermittelt diese Daten seinerseits über die SSPN-Schnittstelle (Subscription Service Provider Network) an ein für die Authentifizierung zuständiges AAA-System. Die Authentisierung erfolgt dabei über die vom SP festgelegte Authentifizierungsmethode; bei der Authentisierung via Benutzername / Passwort umfasst dies EAP-TTLS, bei der Authentisierung via digitalem Zertifikat EAP-TLS.

Anmeldung via (U)SIM

1. Im Unterschied zur Anmeldung via Benutzername / Passwort oder digitalem Zertifikat fragt ein Gerät bei vorliegen einer (U)SIM in seinen ANQP-Requests nicht nach der Liste der NAI-Realms, sondern der 3GPP Cellular Network Information. In den ANQP-Responses beinhaltet diese Cellular-Netzwerk-Informations-Liste alle Mobilfunkanbieter, für die der Access Point eine Authentisierung ermöglicht.
2. Das Gerät lädt aus seiner lokalen (U)SIM-Karte die Kennwerte für das Mobilfunknetzwerk und gleicht diese Daten mit den erhaltenen Cellular-Netzwerk-Informations-Listen ab. Der Listenabgleich sowie die Auswahl eines bevorzugten Betreibernetzwerkes erfolgen synonym zur Anmeldung via Benutzername/Passwort oder digitalem Zertifikat.
3. Das Gerät authentisiert sich mit seinen lokalen Zugangsdaten am Hotspot des bevorzugten Betreibers für die passende Mobilfunkgesellschaft. Der Hotspot übermittelt diese Daten seinerseits über die SSPN-Schnittstelle (Subscription Service Provider Network) an ein für die Authentifizierung zuständiges AAA-System. Durch das Vorhandensein einer (U)SIM-Karte ändert sich die mögliche Authentifizierungsmethode für das Gerät zu EAP-SIM oder EAP-AKA.
4. Das AAA-System erkundigt sich für die Authentifizierung über die MAP-Schnittstelle (Mobile Application Part) beim HLR-Server (Home Location Register) der Mobilfunkgesellschaft, um die Zugangsdaten zu verifizieren.

Im Falle einer erfolgreichen Authentisierung erhält das Gerät den Zugriff auf das WLAN-Netzwerk entweder via Hotspot (Zugangsdaten für das Betreiber-Netzwerk liegen vor) oder automatischem Roaming (Zugangsdaten für das Betreiber-Netzwerk liegen nicht vor).

Stehen dem Gerät mehrere Authentifizierungsmöglichkeiten zur Auswahl (z. B. SIM-Karte und Benutzername / Passwort), hat es die Möglichkeit, anhand der NAI-Realm- bzw. Cellular-Netzwerk-Informations-Liste die bevorzugte EAP-Authentifizierungsmethode und damit die bevorzugten Zugangsdaten auszuwählen.

13.18.16.3 Empfohlene allgemeine Einstellungen

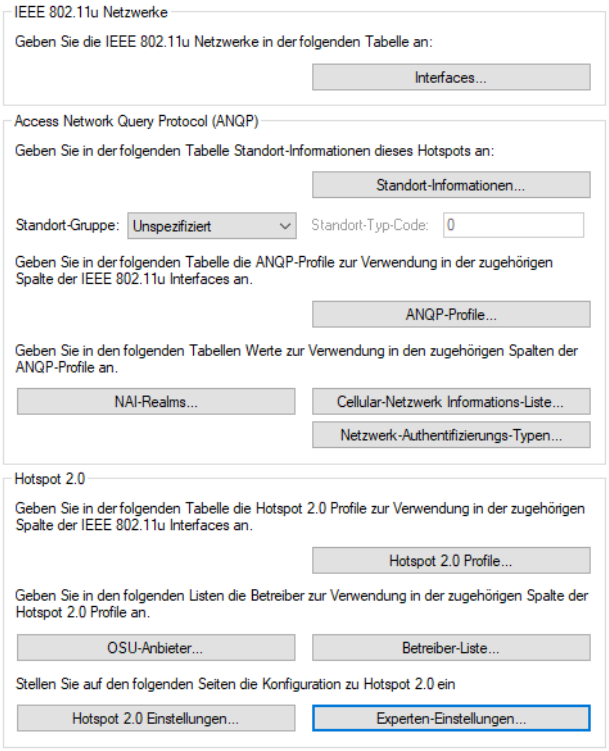
Die Hotspot-2.0-Spezifikation empfiehlt für den 802.11u-Betrieb folgende allgemeine Einstellungen:

- Aktivierte WPA2-Enterprise Sicherheit (802.1X)
- Authentifizierung via EAP mit der entsprechenden Variante:
  - EAP-SIM/EAP-AKA bei Authentifizierung mit SIM/USIM-Karte
  - EAP-TLS bei Authentifizierung mit digitalem Zertifikat
  - EAP-TTLS bei Authentifizierung mit Benutzername und Passwort
- Aktiviertes und eingerichtetes Proxy-ARP
- Deaktivierte Multicast- und Broadcasts in Funkzellen

- Nicht-zugelassener Datenverkehr zwischen den einzelnen mobilen Endgeräten (Layer-2 Traffic-Inspection & Filtering). Die dazugehörigen Schalter finden Sie im LANconfig unter **Wireless-LAN** > **Securtity** > **Datenverkehr zwischen SSIDs**.
- Aktivierte und eingerichtete Firewall auf dem Access-Router, welcher den Internetzugang zur Verfügung stellt

13.18.16.4 Konfigurationsmenü für IEEE 802.11u / Hotspot 2.0

Das Konfigurationsmenü für IEEE 802.11u und Hotspot 2.0 finden Sie unter **Wireless-LAN** > **IEEE 802.11u**.



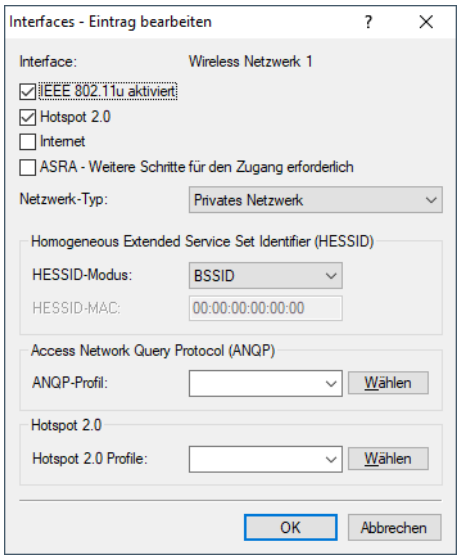
Das Gerät bietet Ihnen über die Schaltfläche **Interfaces** die Möglichkeit, die Unterstützung für den IEEE-802.11u-Standard sowie die Hotspot-2.0-Funktionalität für jede logische WLAN-Schnittstelle separat zu aktivieren bzw. zu deaktivieren sowie zu konfigurieren.

Ein Teil der zu konfigurierenden Parameter ist in sogenannte „Profile" ausgelagert. Über Profile gruppieren Sie Reihen unterschiedlicher Parameter in Listen, auf die Sie aus den einzelnen Dialogen lediglich referenzieren. Im Wesentlichen handelt es sich dabei um Profile für ANQP-Datenpakete sowie Hotspot 2.0. Die Beziehungen zwischen den Profillisten untereinander stellen sich wie folgt dar:

```
|-- Interfaces
  |-- ANQP-Profile
    |-- NAI-Realms
    |-- Cellular-Netzwerk Informations-Liste
    |-- Netzwerk-Authentifizierungs-Typen
  |-- Hotspot 2.0 Profile
    |-- Betreiber-Liste
    |-- OSU-Anbieter
```

Aktivierung für Interfaces

Die Tabelle **Interfaces** ist die höchste Verwaltungsebene für IEEE 802.11u und Hotspot 2.0. Hier haben Sie die Möglichkeit, die Funktionen für jede Schnittstelle ein- oder auszuschalten, ihnen unterschiedliche Profile zuzuweisen oder allgemeine Einstellungen vorzunehmen.



Interface

Name der logischen WLAN-Schnittstelle, die Sie gerade bearbeiten.

IEEE 802.11u aktiviert

Aktivieren oder deaktivieren Sie an der betreffenden Schnittstelle die Unterstützung für Verbindungen nach IEEE 802.11u. Wenn Sie die Unterstüzung aktivieren, sendet das Gerät für die Schnittstelle – bzw. für die dazugehörige SSID – das Interworking-Element in den Beacons / Probes. Dieses Element dient als Erkennungsmerkmal für IEEE-802.11u-fähige Verbindungen: Es enthält z. B. das Internet-Bit, das ASRA-Bit, die HESSID sowie den Standort-Gruppen-Code und den Standort-Typ-Code. Diese Einzelelemente nutzen 802.11u-fähige Geräte als erste Filterkriterien bei der Netzsuche.

Hotspot 2.0

Aktivieren oder deaktivieren Sie an der betreffenden Schnittstelle die Unterstützung für Hotspot 2.0 der Wi-Fi Alliance®. Hotspot 2.0 erweitert den IEEE-802.11u-Standard um zusätzliche Netzwerkinformationen, welche Stationen über einen ANQP-Request abfragen können. Dazu gehören z. B. der betreiberfreundliche Name, die Verbindungs-Fähigkeiten, die Betriebsklasse und die WAN-Metriken. Über diese zusätzlichen Informationen sind Stationen dazu in der Lage, die Wahl eines Wi-Fi-Netzwerkes noch selektiver vorzunehmen.

Internet

Wählen Sie aus, ob das Internet-Bit gesetzt wird. Über das Internet-Bit informieren Sie alle Stationen explizit darüber, dass das Wi-Fi-Netzwerk den Internetzugang erlaubt. Aktivieren Sie diese Einstellung, sofern über Ihr Gerät nicht nur interne Dienste erreichbar sind.

Über diese Funktion teilen Sie lediglich die Verfügbarkeit einer Internetverbindung mit. Die entsprechenden Regularien konfigurieren Sie unabhängig von dieser Option über die Firewall!

ASRA – Weitere Schritte für den Zugang erforderlich

Wählen Sie aus, ob das ASRA-Bit (Additional Step Required for Access) gesetzt wird. Über das ASRA-Bit informieren Sie alle Stationen explizit darüber, dass für den Zugriff auf das Wi-Fi-Netzwerk noch weitere Authentifizierungsschritte notwendig sind. Aktivieren Sie diese Einstellung, wenn Sie z. B. eine Online-Registrierung, eine zusätzliche Web-Authentifikation oder eine Zustimmungswebseite für Ihre Nutzungsbedingungen eingerichtet haben.

Denken Sie daran, in der Tabelle **Netzwerk-Authentifizierungs-Typen** eine Weiterleitungsadresse für die zusätzliche Authentifizierung anzugeben und / oder **WISPr** für das Public Spot-Modul zu konfigurieren, wenn Sie das ASRA-Bit setzen.

Netzwerk-Typ

Wählen Sie aus der vorgegebenen Liste einen Netzwerk-Typ aus, der das Wi-Fi-Netzwerk hinter der ausgewählten Schnittstelle am ehesten charakterisiert. Anhand der hier getroffenen Einstellung haben Nutzer die Wahl, die Netzsuche ihrer Geräte auf bestimmte Netzwerk-Typen zu beschränken. Mögliche Werte sind:

Privates Netzwerk

Beschreibt Netzwerke, in denen unauthorisierte Benutzer nicht erlaubt sind. Wählen Sie diesen Typ z. B. für Heimnetzwerke oder Firmennetzwerke, bei denen der Zugang auf die Mitarbeiter beschränkt ist.

Privat mit Gast-Zugang

Wie **Privates Netzwerk**, doch mit Gast-Zugang für unauthorisierte Benutzer. Wählen Sie diesen Typ z. B. für Firmennetzwerke, bei denen neben den Mitarbeitern auch Besucher das Wi-Fi-Netzwerk nutzen dürfen.

Kostenpflichtiges Öffentliches Netzwerk

Beschreibt öffentliche Netzwerke, die für jedermann zugänglich sind und deren Nutzung gegen Entgelt möglich ist. Informationen zu den Gebühren sind evtl. auf anderen Wegen abrufbar (z. B: IEEE 802.21, HTTP/HTTPS- oder DNS-Weiterleitung). Wählen Sie diesen Typ z. B. für Hotspots in Geschäften oder Hotels, die einen kostenpflichtigen Internetzugang anbieten.

Kostenloses öffentliches Netzwerk

Beschreibt öffentliche Netzwerke, die für jedermann zugänglich sind und für deren Nutzung kein Entgelt anfällt. Wählen Sie diesen Typ z. B. für Hotspots im öffentlichen Nah- und Fernverkehr oder für kommunale Netzwerke, bei denen der Wi-Fi-Zugang eine inbegriffene Leistung ist.

Persönliches Geräte-Netzwerk

Beschreibt Netzwerke, die drahtlose Geräte im Allgemeinen verbinden. Wählen Sie diesen Typ z. B. bei angeschlossenen Digital-Kameras, die via WLAN mit einem Drucker verbunden sind.

Netzwerk für Notdienste

Beschreibt Netzwerke, die für Notdienste bestimmt und auf diese beschränkt sind. Wählen Sie diesen Typ z. B. bei angeschlossenen ESS- oder EBR-Systemen.

Test oder experimentell

Beschreibt Netzwerke, die zu Testzwecken eingerichtet sind oder sich noch im Aufbaustadium befinden.

Wildcard

Platzhalter für bislang undefinierte Netzwerk-Typen.

HESSID-Modus

Geben Sie an, woher das Gerät seine HESSID für das homogene ESS bezieht. Als homogenes ESS bezeichnet man den Verbund einer bestimmten Anzahl von Access Points, die alle dem selben Netzwerk angehören. Als weltweit eindeutige Kennung (HESSID) dient die MAC-Adresse eines angeschlossenen Access Points. Die SSID taugt in diesem Fall nicht als Kennung, da in einer Hotspot-Zone unterschiedliche Netwerkbetreiber die gleiche SSID vergeben haben können, z. B. durch Trivialnamen wie „HOTSPOT". Mögliche Werte für den HESSID-Modus sind:

BSSID

Wählen Sie diesen Eintrag, um die BSSID des Gerätes als HESSID für Ihr homogenes ESS festzulegen.

Benutzer

Wählen Sie diesen Eintrag, um eine HESSID manuell zu vergeben.

Keiner

Wählen Sie diesen Eintrag, um die Schnittstelle keinem homogenen ESS zuzuordnen und aus dem Geräteverbund zu isolieren.

HESSID-MAC

Sofern Sie als **HESSID-Modus** die Einstellung `Benutzer` gewählt haben, tragen Sie hier die HESSID Ihres homogenen ESS in Form einer 6-oktettigen MAC-Adresse ein. Wählen Sie für die HESSID die BSSID eines beliebigen Access Apoints in Ihrem homogenen ESS in Großbuchstaben und ohne Trennzeichen, z. B. „008041AEFD7E“ für die MAC-Adresse 00:80:41:ae:fd:7e.

Sofern Ihr Gerät nicht in mehreren homogenen ESS vertreten ist, ist die HESSID für alle Schnittstellen identisch!

ANQP-Profil

Wählen Sie aus der Liste ein ANQP-Profil aus. ANQP-Profile legen Sie im Konfigurationsmenü über die gleichnamige Schaltfläche an.

Hotspot 2.0 Profile

Wählen Sie aus der Liste ein Hotspot-2.0-Profil aus. Hotspot-2.0-Profile legen Sie im Konfigurationsmenü über die gleichnamige Schaltfläche an.

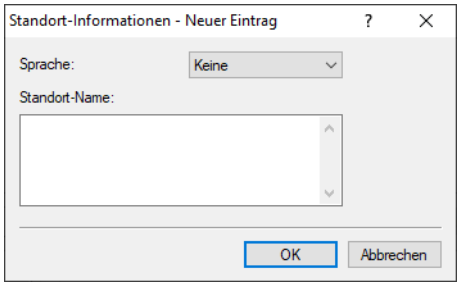
ANQP-Datenpakete konfigurieren

Standort-Informationen und -Gruppe

Über die Tabelle **Standort-Informationen** sowie den nachgelagerten Dialogabschnitt zur **Standort-Gruppe** und zum **Standort-Typ-Code** verwalten Sie die Angaben zum Standort des Access Points.

Mit Angaben zu den **Standort-Informationen** unterstützen Sie einen Nutzer bei der Auswahl des richtigen Hotspots im Falle einer manuellen Suche. Verwenden in einer Hotspot-Zone mehrere Betreiber (z. B. mehrere Cafés) die gleiche SSID, kann der Nutzer mit Hilfe der Standort-Informationen die passende Lokalität eindeutig identifizieren.

Über die **Standort-Gruppe** und den **Standort-Typ-Code** ordnen Sie dagegen Ihr Gerät – im Gegensatz zu den frei definierbaren Standort-Informationen – in eine vorgegebene Kategorie ein.



Sprache

Sie haben die Möglichkeit, für jede Sprache individuelle Informationen zum Standort des Access Points anzugeben. Ihre Nutzer bekommen dann die zur ihrer Sprache passenden Standort-Namen angezeigt. Ist eine Sprache für einen Nutzer nicht vorhanden, entscheidet seine Station, z. B. anhand der Default-Sprache.

Standort-Name

Tragen Sie hier für die ausgewählte Sprache eine kurze Beschreibung zum Standort des Gerätes ein, z. B.

```
Eiscafé Valenzia
Am Markt 3
12345 Musterstadt
```

Die **Standort-Gruppe** beschreibt das Umfeld, in dem Sie den Access Point einsetzen. Sie definieren sie global für alle Sprachen. Die möglichen Werte, festgelegt durch den „Venue Group Code", werden durch den 802.11u-Standard vorgegeben.

Über den **Standort-Typ-Code** haben Sie die Möglichkeit, die Standort-Gruppe weiter zu spezifizieren. Auch hier sind die Werte durch den Standard spezifiziert. Die möglichen Typ-Codes entnehmen Sie bitte der nachfolgenden Tabelle.

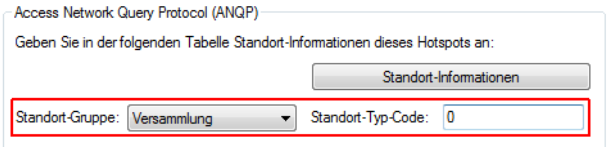


Tabelle 29: Übersicht möglicher Werte für Standort-Gruppen und -Typen

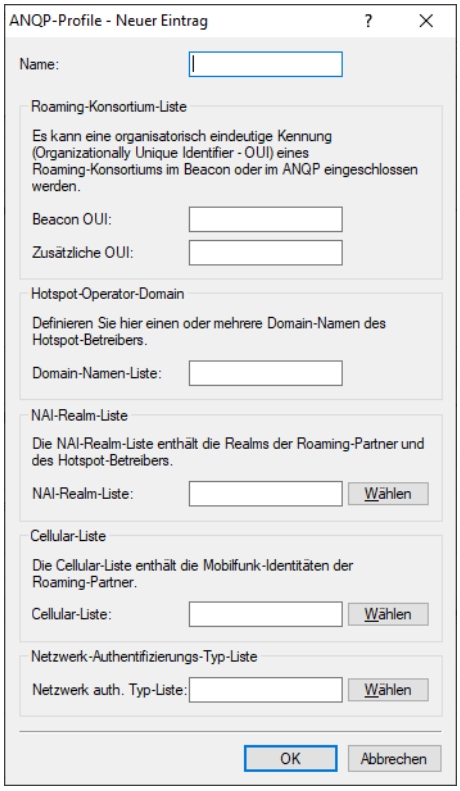
Standort-Gruppe	Standort-Typ-Code
Unspezifiziert	
Versammlung	› 0 = Unspezifizierte Versammlung › 1 = Bühne › 2 = Stadion › 3 = Passagier-Terminal (z. B. Flughafen, Busbahnhof, Fähranleger, Bahnhof) › 4 = Amphitheater › 5 = Vergnügungspark › 6 = Andachtsstätte › 7 = Kongresszentrum › 8 = Bücherei › 9 = Museum › 10 = Restaurant › 11 = Schauspielhaus › 12 = Bar › 13 = Café › 14 = Zoo, Aquarium › 15 = Notfallleitstelle
Geschäft	› 0 = Unspezifiziertes Geschäft › 1 = Arztpraxis › 2 = Bank › 3 = Feuerwache › 4 = Polizeiwache › 6 = Post › 7 = Büro › 8 = Forschungseinrichtung › 9 = Anwaltskanzlei
Ausbildung	› 0 = Unspezifizierte Ausbildung › 1 = Grundschule › 2 = Weiterführende Schule › 3 = Hochschule

Standort-Gruppe	Standort-Typ-Code
Fabrik und Industrie	› 0 = Unspezifizierte Fabrik und Industrie › 1 = Fabrik
Institutional	› 0 = Unspezifizierte Institution › 1 = Krankenhaus › 2 = Langzeit-Pflegeeinrichtung (z. B. Seniorenheim, Hospiz) › 3 = Entzugsklinik › 4 = Einrichtungsverbund › 5 = Gefängnis
Handel	› 0 = Unspezifizierter Handel › 1 = Ladengeschäft › 2 = Lebensmittelmarkt › 3 = KFZ-Werkstatt › 4 = Einkaufszentrum › 5 = Tankstelle
Wohnheim	› 0 = Unspezifiziertes Wohnheim › 1 = Privatwohnsitz › 2 = Hotel oder Motel › 3 = Studentenwohnheim › 4 = Pension
Lager	› 0 = Unspezifiziertes Lager
Dienste und sonstiges	› 0 = Unspezifizierter Dienst und sonstiges
Fahrzeug	› 0 = Unspezifiziertes Fahrzeug › 1 = Personen- oder Lastkraftwagen › 2 = Flugzeug › 3 = Bus › 4 = Fähre › 5 = Schiff oder Boot › 6 = Zug › 7 = Motorrad
Außen	› 0 = Unspezifizierter Außenbereich › 1 = Städtisches Wi-Fi-Netzwerk (Muni-Mesh-Netzwerk) › 2 = Stadtpark › 3 = Rastplatz › 4 = Verkehrsregelung › 5 = Bushaltestelle › 6 = Kiosk

ANQP-Profile

Über diese Tabelle verwalten Sie die Profillisten für ANQP. **ANQP-Profile** bieten Ihnen die Möglichkeit, bestimmte ANQP-Elemente zu gruppieren und sie in der Tabelle **Interfaces** unabhängig voneinander logischen WLAN-Schnittstellen

zuzuweisen. Zu diesen Elementen gehören z. B. Angaben zu Ihren OIs, Domains, Roaming-Partnern und deren Authentifizierungsmethoden. Ein Teil der Elemente ist in weitere Profillisten ausgelagert.



Name

Vergeben Sie hierüber einen Namen für das ANQP-Profil. Dieser Name erscheint später innerhalb der Interfaces-Tabelle in der Auswahlliste für die ANQP-Profile.

Beacon OUI

Organizationally Unique Identifier, abgekürzt OUI, vereinfacht OI. Als Hotspot-Betreiber tragen Sie hier die OI des Roaming-Partners ein, mit dem Sie einen Vertrag abgeschlossen haben. Sind Sie als Hotspot-Betreiber gleichzeitig der Service-Provider, tragen Sie hier die OI Ihres Roaming-Konsortiums oder Ihre eigene OI ein. Ein Roaming-Konsortium besteht aus einer Gruppe von Service-Providern, die untereinander Vereinbarungen zum gegenseitigen Roaming getroffen haben. Um eine OI zu erhalten, muss sich ein solches Konsortium – ebenso wie ein einzelner Service-Provider – bei der IEEE registrieren lassen.

Es besteht die Möglichkeit, bis zu 3 OIs parallel anzugeben, z. B. für den Fall, dass Sie als Betreiber Verträge mit mehreren Roaming-Partnern haben. Mehrere OIs trennen Sie durch eine kommaseparierte Liste, z. B. `00105E,00017D,00501A`.

Das Gerät strahlt die eingegebene(n) OI(s) in seinen Beacons aus. Soll das Gerät mehr als 3 OIs übertragen, lassen sich diese unter **Zusätzliche OUI** konfigurieren. Zusätzliche OIs werden allerdings erst nach dem GAS-Request einer Station übertragen; sie sind für die Stationen also nicht unmittelbar sichtbar!

Zusätzliche OUI

Tragen Sie hier die OI(s) ein, die das Gerät nach dem GAS-Request einer Station zusätzlich aussendet. Mehrere OIs trennen Sie durch eine kommaseparierte Liste, z. B. `00105E,00017D,00501A`.

Domain-Namen-Liste

Tragen Sie hier eine oder mehrere Domains ein, über die Sie als Hotspot-Betreiber verfügen. Mehrere Domain-Namen trennen Sie durch eine kommaseparierte Liste, z. B. `providerX.org,provx-mobile.com,wifi.mnc410.provX.com`. Für Subdomains reicht es aus, lediglich den obersten gültigen Domain-Namen anzugeben. Hat ein Nutzer z. B. providerX.org als Heimat-Provider in seinem Gerät konfiguriert, werden dieser Domain auch Access Points mit dem Domain-Namen wi-fi.providerX.org zugerechnet. Bei der Suche nach passenden Hotspots bevorzugt eine Station immer den Hotspot seines Heimat-Providers, um mögliche Roaming-Kosten über den Access Point eines Roaming-Partners zu vermeiden.

NAI-Realm-Liste

Wählen Sie aus der Liste ein NAI-Realm-Profil aus. Profile für NAI-Realms legen Sie im Konfigurationsmenü über die Schaltfläche **NAI-Realms** an.

Cellular-Liste

Wählen Sie aus der Liste eine Mobilfunk-Identität aus. Identitäten für Mobilfunknetzwerke legen Sie – wie bei einem Profil – im Konfigurationsmenü über die Schaltfläche **Cellular-Netzwerk Informations-Liste** an.

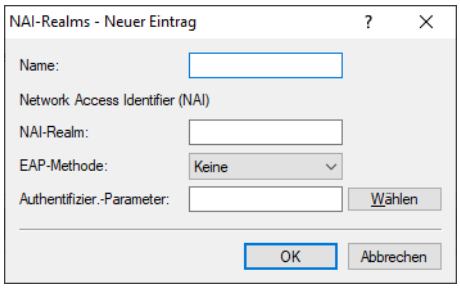
Netzwerk auth. Typ-Liste

Wählen Sie aus der Liste einen Authentifizierungs-Profil aus. Profile zur Netzwerk-Authentifizierung legen Sie im Konfigurationsmenü über die Schaltfläche **Netzwerk-Authentifizierungs-Typen** an.

Zusätzlich haben Sie über die Konsole die Möglichkeit, Ihren Nutzern auch den Typ der verfügbaren IP-Adresse anzuzeigen, den diese nach einer erfolgreichen Authentifizierung vom Netzwerk erhalten können. Sie erreichen die betreffenden Parameter **IPv4-Addr-Type** und **IPv6-Addr-Type** über den Pfad **Setup** > **IEEE802.11u** > **ANQP-General**.

NAI-Realms

Über diese Tabelle verwalten Sie die Profillisten für die NAI-Realms. Mit diesen Listen haben Sie die Möglichkeit, bestimmte ANQP-Elemente zu gruppieren. Hierzu gehören die Realms des Hotspot-Betreibers und seiner Roaming-Partner mitsamt der zugehörigen Authentifizierungs-Methoden und -Parameter. Stationen nutzen diese Liste, um anhand der hier hinterlegten Angaben festzustellen, ob sie für den Hotspot-Betreiber oder einen seiner Roaming-Partner über gültige Anmeldedaten verfügen.



Name

Vergeben Sie hierüber einen Namen für das NAI-Realm-Profil, z. B. den Namen des Service-Providers oder Dienstes, zu dem der NAI-Realm gehört. Dieser Name erscheint später im ANQP-Profil in der Auswahl für die **NAI-Realm-Liste**.

NAI-Realm

Geben Sie hier den Realm für das Wi-Fi-Netzwerk an. Der NAI-Realm selbst ist ein Identifikationspaar aus einem Benutzernamen und einer Domäne, welches durch reguläre Ausdrücke erweitert werden kann. Die Syntax für einen NAI-Realm wird in *RFC 2486* definiert und entspricht im einfachsten Fall

`<username>@<realm>`; für `user746@providerX.org` lautet der entsprechende Realm also `providerX.org`.

EAP-Methode

Wählen Sie aus der Liste eine Authentifizierungsmethode für den NAI-Realm aus. EAP steht dabei für das Authentifizierungs-Protokoll (Extensible Authentication Protocol), gefolgt vom jeweiligen Authentisierungsverfahren. Mögliche Werte sind:

EAP-TLS

Authentifizierung via Transport Layer Security (TLS). Wählen Sie diese Einstellung, wenn die Authentifizierung über den betreffenden NAI-Realm durch ein digitales Zertifikat erfolgt, das der Nutzer installiert.

EAP-SIM

Authentifizierung via Subscriber Identity Module (SIM). Wählen Sie diese Einstellung, wenn die Authentifizierung über den betreffenden NAI-Realm durch das GSM Subscriber Identity Module (die SIM-Karte) der Station erfolgt.

EAP-TTLS

Authentifizierung via Tunneled Transport Layer Security (TTLS). Wählen Sie diese Einstellung, wenn die Authentifizierung über den betreffenden NAI-Realm durch einen Benutzernamen und ein Passwort erfolgt. Zur Sicherheit wird die Verbindung bei diesem Verfahren getunnelt.

EAP-AKA

Authentifizierung via Authentication and Key Agreement (AKA). Wählen Sie diese Einstellung, wenn die Authentifizierung über den betreffenden NAI-Realm durch das UTMS Subscriber Identity Module (die USIM-Karte) der Station erfolgt.

Keine

Wählen Sie diese Einstellung, wenn der betreffende NAI-Realm keine Authentifizierung erfordert.

Authentifizierungs-Parameter

Klicken Sie die zur EAP-Methode passenden Authentifizierungs-Parameter, z. B. für EAP-TTLS

`NonEAPAuth.MSCHAPV2,Credential.UserPass`

oder für EAP-TLS `Credentials.Certificate`.

Mögliche Werte sind:

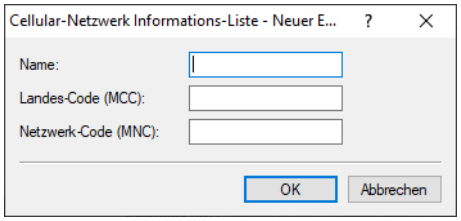
Tabelle 30: Übersicht der möglichen Authentifizierungs-Parameter

Parameter	Sub-Parameter	Erläuterung
NonEAPAuth.		Bezeichnet das Protokoll, welches der Realm für die Phase-2-Authentifizierung erfordert:
	PAP	Password Authentication Protocol
	CHAP	Challenge Handshake Authentication Protocol, ursprüngliche CHAP-Implementierung, spezifiziert im *RFC 1994*
	MSCHAP	CHAP-Implementierung von Microsoft v1, spezifiziert im *RFC 2433*
	MSCHAPV2	CHAP-Implementierung von Microsoft v2, spezifiziert im *RFC 2759*
Credentials.		Beschreibt die Art der Authentifizierung, die der Realm akzeptiert:

Parameter	Sub-Parameter	Erläuterung
	SIM	SIM-Karte
	USIM	USIM-Karte
	NFCSecure	NFC-Chip
	HWToken*	Hardware-Token
	SoftToken*	Software-Token
	Certificate	Digitales Zertifikat
	UserPass	Benutzername und Passwort
	None	Keine Zugangsdaten erforderlich
TunnelEAPCredentials.*		
	SIM*	SIM-Karte
	USIM*	USIM-Karte
	NFCSecure*	NFC-Chip
	HWToken*	Hardware-Token
	SoftToken*	Software-Token
	Certificate*	Digitales Zertifikat
	UserPass*	Benutzername und Passwort
	Anonymous*	Anonyme Anmeldung

Cellular-Netzwerk Informations-Liste

Über diese Tabelle verwalten Sie die Identitätslisten für die Mobilfunknetze. Mit diesen Listen haben Sie die Möglichkeit, bestimmte ANQP-Elemente zu gruppieren. Hierzu gehören die Netzwerk- und Landes-Codes des Hotspot-Betreibers und seiner Roaming-Partner. Stationen mit SIM- oder USIM-Karte nutzen diese Liste, um anhand der hier hinterlegten Angaben festzustellen, ob der Hotspot-Betreiber zu ihrer Mobilfunkgesellschaft gehört oder einen Roaming-Vertrag mit ihrer Mobilfunkgesellschaft hat.



Name

Vergeben Sie hierüber einen Namen für die Mobilfunk-Identität, z. B. ein Kürzel des Netzanbieters in Kombination mit dem verwendeten Mobilfunkstandard. Dieser Name erscheint später im ANQP-Profil in der Auswahl für die **Cellular-Liste**.

Landes-Code (MCC)

Geben Sie hier den Mobile Country Code (MCC) des Hotspot-Betreibers oder seiner Roaming-Partner ein, bestehend aus 2 oder 3 Zeichen, z. B. `262` für Deutschland.

* Der betreffende Parameter oder Sub-Parameter ist im Rahmen der Passpoint™-Zertifizierung für zukünftige Einsatzzwecke reserviert worden, findet gegenwärtig jedoch keine Verwendung.

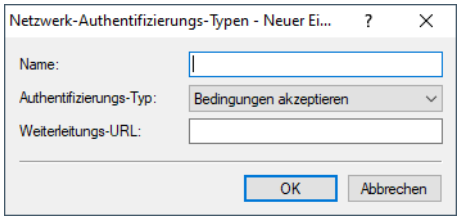
Netzwerk-Code (MNC)

Geben Sie hier den Mobile Network Code (MNC) des Hotspot-Betreibers oder seiner Roaming-Partner ein, bestehend aus 2 oder 3 Zeichen.

Netzwerk-Authentifizierungs-Typen

Über diese Tabelle verwalten Sie Adressen, an die das Gerät Stationen für einen zusätzlichen Authentifizierungsschritt weiterleitet, nachdem sich die Station bereits beim Hotspot-Betreiber oder einem seiner Roaming-Partner erfolgreich authentisiert hat. Pro Authentifizierungs-Typ ist nur eine Weiterleitungsangabe erlaubt.

Denken Sie daran, das ASRA-Bit in der Tabelle **Interfaces** zu setzen, wenn Sie einen zusätzlichen Authentifizierungsschritt einrichten!



Name

Vergeben Sie hierüber einen Namen für den Listeneintrag, z. B. `AGB akzeptieren`. Dieser Name erscheint später im ANQP-Profil in der Auswahl für die **Netzwerk auth. Typ-Liste**.

Authentifizierungs-Typ

Wählen Sie aus der Auswahlliste den Kontext, vor dem die Weiterleitung gilt. Mögliche Werte sind:

Bedingungen akzeptieren

Es ist ein zusätzlicher Authentifizierungsschritt eingerichtet, bei dem ein Benutzer die Nutzungsbedingungen des Betreibers akzeptieren muss.

Online Registrierung

Es ist ein zusätzlicher Authentifizierungsschritt eingerichtet, bei dem sich ein Benutzer erst online registrieren muss.

HTTP-Weiterleitung

Es ist ein zusätzlicher Authentifizierungsschritt eingerichtet, zu dem ein Benutzer via HTTP weitergeleitet wird.

DNS-Weiterleitung

Es ist ein zusätzlicher Authentifizierungsschritt eingerichtet, zu dem ein Benutzer via DNS weitergeleitet wird.

Weiterleitungs-URL

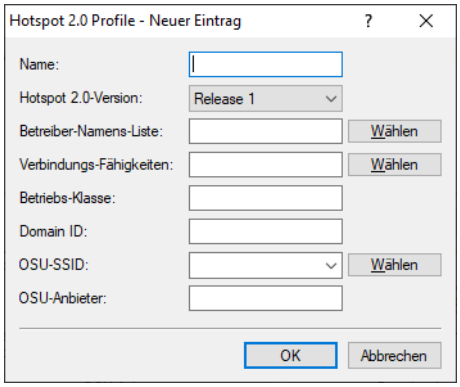
Geben Sie die Adresse an, an die das Gerät Stationen für den zusätzlichen Authentifizierungsschritt weiterleitet.

Hotspot 2.0 konfigurieren

Hotspot 2.0 Profile

Über diese Tabelle verwalten Sie die Profillisten für Hotspot 2.0. **Hotspot 2.0 Profile** bieten Ihnen die Möglichkeit, bestimmte ANQP-Elemente (die der Hotspot-2.0-Spezifikation) zu gruppieren und sie in der Tabelle **Interfaces** unabhängig voneinander logischen WLAN-Schnittstellen zuzuweisen. Zu diesen Elementen gehören z. B. der betreiberfreundliche

Name, die Verbindungs-Fähigkeiten, die Betriebsklasse und die WAN-Metriken. Ein Teil der Elemente ist in weitere Profillisten ausgelagert.



Name

Vergeben Sie hierüber einen Namen für das Hotspot-2.0-Profil. Dieser Name erscheint später innerhalb der Interfaces-Tabelle in der Auswahlliste für die Hotspot-2.0-Profile.

Hotspot 2.0 Version

Stellen Sie das in diesem Profil unterstützte Release von Hotspot 2.0 ein.

Ein Client muss das entsprechende Release beherrschen, um sich verbinden zu können.

Betreiber-Namens-Liste

Wählen Sie aus der Liste das Profil eines Hotspot-Betreibers aus. Profile für Hotspot-Betreiber legen Sie im Konfigurationsmenü über die Schaltfläche **Betreiber-Liste** an.

Verbindungs-Fähigkeiten

Wählen Sie für jeden Dienst die Verbindungs-Fähigkeit aus. Stationen nutzen diese Liste, um anhand der hier hinterlegten Angaben vor einem Netzbeitritt festzustellen, ob Ihr Hotspot die benötigten Dienste (z. B. Internetzugang, SSH, VPN) überhaupt erlaubt. Aus diesem Grund sollten so wenig Einträge wie möglich den Status „unbekannt" tragen. Mögliche Statuswerte für die einzelnen Dienste sind „closed" (`-C`), „open" (`-O`) oder „unknown" (`-U`):

- `ICMP`: Geben Sie an, ob Sie den Austausch von Informations- und Fehlermeldungen via ICMP erlauben.
- `TCP-FTP`: Geben Sie an, ob Sie Dateiübertragungen via FTP erlauben.
- `TCP-SSH`: Geben Sie an, ob Sie verschlüsselte Verbindungen via SSH erlauben.
- `TCP-HTTP`: Geben Sie an, ob Sie Internetverbindungen via HTTP/HTTPS erlauben.
- `TCP-TLS`: Geben Sie an, ob Sie verschlüsselte Verbindungen via TLS erlauben.
- `TCP-PPTP`: Geben Sie an, ob Sie das Tunneln von VPN-Verbindungen via PPTP erlauben.
- `TCP-VOIP`: Geben Sie an, ob Sie Internettelefonie via VoIP (TCP) erlauben.
- `UDP-IPSEC-500`: Geben Sie an, ob Sie IPsec via UDP und Port 500 erlauben.
- `UDP-VOIP`: Geben Sie an, ob Sie Internettelefonie via VoIP (UDP) erlauben.
- `UDP-IPSEC-4500`: Geben Sie an, ob Sie IPsec via UDP und Port 4500 erlauben.
- `ESP`: Geben Sie an, ob Sie ESP (Encapsulating Security Payload) für IPsec erlauben.

Wenn Sie nicht wissen, ob in Ihrem Netzwerk ein Dienst verfügbar und seine Ports offen oder geschlossen sind, oder Sie gegenüber einer Station bewusst keine Angabe zum Status machen wollen, wählen Sie eine `-U`-Einstellung.

Über diesen Dialog legen Sie keine Berechtigungen fest! Die Angaben dienen den Stationen lediglich dazu, den Netzbeitritt über Ihr Gerät zu entscheiden. Spezifische Zugangsberechtigungen für Ihr Netzwerk konfigurieren Sie über andere Gerätefunktionen, wie z. B. die Firewall / QoS.

Betriebs-Klasse

Geben Sie hier den Code für die globale Betriebsklasse des Access Points an. Über die Betriebs-Klasse teilen Sie einer Station mit, auf welchen Frequenzbändern und Kanälen Ihr Access-Point verfügbar ist. Beispiel:

- `81`: Betrieb bei 2,4 GHz mit Kanälen 1–13
- `116`: Betrieb bei 40 MHz mit Kanälen 36 und 44

Die für Ihr Gerät passende Betriebsklasse entnehmen Sie bitte dem IEEE Standard 802.11-2012, Anhang E, Tabelle E-4: Global operating classes; erhältlich unter *standards.ieee.org*.

Domain ID

Die Domain-ID gibt an, welcher ANQP-Server verwendet wird. Alle Access Points bzw. SSIDs mit gleicher Nummer / Domain-ID (16-Bit-Wert) verwenden den gleichen ANQP-Server.

Ein Client würde somit auf eine ANQP-Anfrage auf Access Points / SSIDs mit identischer Domain-ID immer die gleiche Antwort erhalten. Um unterschiedliche Antworten zu erhalten, müsste der Client nach unterschiedlichen Domain-IDs Ausschau halten.

OSU-SSID

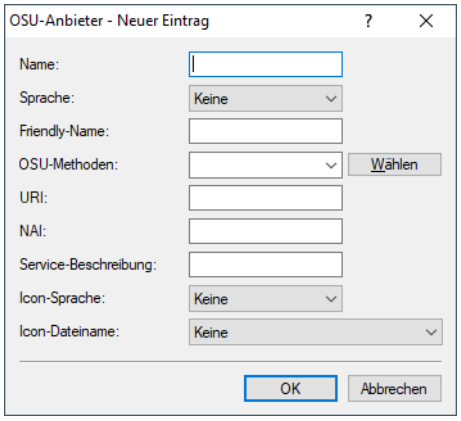
Name der SSID, die Zugang zum OSU-Server bietet.

OSU-Anbieter

Liste der OSU-Providernamen aus *OSU-Anbieter* auf Seite 1101, die im Profil unterstützt werden.

OSU-Anbieter

In dieser Tabelle konfigurieren Sie die OSU-Provider für Online Sign-Up bei Passpoint® Release 2.



Name

Geben Sie diesem OSU-Provider einen Namen, über den Sie ihn später referenzieren können. Wenn der gleiche Name erneut verwendet wird, dann kann dieser Provider z. B. für mehrere Spachen verwendet werden.

Sprache

Stellen Sie die von diesem OSU-Provider unterstützte Sprache ein.

Friendly-Name

Geben Sie diesem OSU-Provider einen sprechenden Namen.

OSU-Methoden

Stellen Sie hier die von diesem OSU-Provider verwendeten OSU-Methoden ein. Möglich sind „OMA-DM“ oder „SOAP-XML-SPP“.

Mögliche Methoden innerhalb des Online Sign-Up-Servers bei Passpoint® Release 2:

- OMA – Open Mobile Alliance
- DM – Device Management
- SOAP – Simple Object Access Protocol
- XML – eXtended Markup Language
- SPP – Subscription Provisioning Protocol

URI

Geben Sie eine URI ein, unter der ein Client den OSU-Server erreicht.

NAI

Geben Sie den Network Access Identifier (NAI) für diesen OSU-Provider ein.

Service-Beschreibung

Geben Sie hier einen Beschreibungstext für diesen Dienst ein.

Icon-Sprache

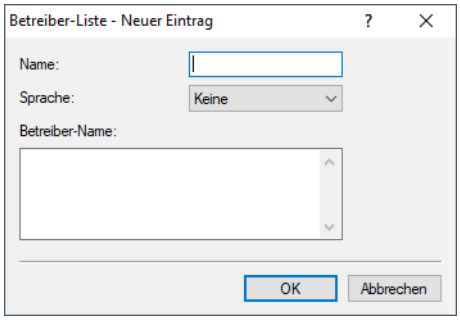
Stellen Sie hier die Sprache des ausgewählten Icons ein.

Icon-Dateiname

Wählen Sie ein Icon für diesen OSU-Provider aus. Die Icons können über die WEBconfig im Bereich ***Dateimanagement*** als Datei hochgeladen werden. Als Dateiformat empfehlen wir PNG.

Betreiber-Liste

Über diese Tabelle verwalten Sie die Klartext-Namen der Hotspot-Betreiber. Ein Eintrag in dieser Tabelle bietet Ihnen die Möglichkeit, einen benutzerfreundlichen Betreiber-Namen an die Stationen zu senden, den diese dann anstelle der Realms anzeigen können. Ob sie das allerdings tatsächlich tun, ist abhängig von der Implementierung.



Name

Vergeben Sie hierüber einen Namen für den Eintrag, z. B. eine Indexnummer oder Kombination aus Betreiber-Name und Sprache.

Sprache

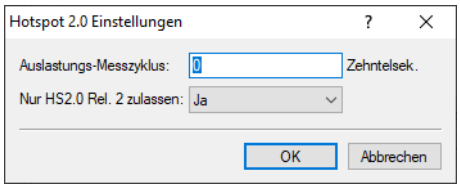
Wählen Sie aus der Liste eine Sprache für den Hotspot-Betreiber aus.

Betreiber-Name

Geben Sie hier den Klartext-Namen des Hotspot-Betreibers ein.

Hotspot 2.0 Einstellungen

In dieser Tabelle konfigurieren Sie spezielle Einstellungen für Hotspot 2.0.



Auslastungs-Messzyklus

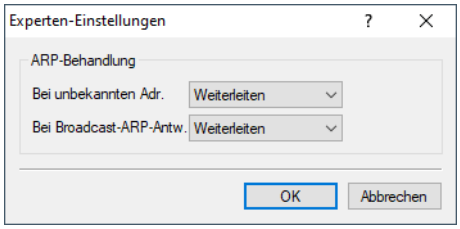
Messzyklus der WAN-Down- / Uplink-Geschwindigkeiten in Zehntelsekunden.

Nur Hotspot 2.0 Release 2 zulassen

Für HotSpot 2.0 Release 2 wird gefordert, nur Release 2-Clients zuzulassen. Dies kann durch diesen Schalter ausgeschaltet werden.

Experten-Einstellungen

In dieser Tabelle konfigurieren Sie Experten-Einstellungen für Hotspot 2.0. Die Einstellungen in diesem Menü dienen der Unterdrückung von ARP (IPv4) bzw. Neighbor Solicitation (IPv6) innerhalb der SSID zwischen den Clients. Alternativ kann dies i.d.R. auch durch die Unterdrückung von Broad- / Multicasts via **Nur Unicasts übertragen, Broad- und Multicasts unterdrücken** in den logischen WLAN-Netzwerkeinstellungen gelöst werden.



Bei unbekannten Adressen

Bei unbekannten Adressen wird das Paket entweder weitergeleitet oder verworfen.

Bei Broadcast-ARP-Antworten

Bei Broadcasts wird das Paket entweder weitergeleitet oder verworfen.

13.18.17 Statischer WLAN-Controller

Der weit verbreitete Einsatz von APs und Wireless Routern hat zu einem deutlich komfortableren und flexibleren Zugang zu Netzwerken in Firmen, Universitäten und anderen Organisationen geführt.

Bei allen Vorzügen der WLAN-Strukturen bleiben einige offene Aspekte:

› Alle APs benötigen eine Konfiguration und ein entsprechendes Monitoring zur Erkennung von unerwünschten WLAN-Clients etc. Die Administration der APs erfordert gerade bei größeren WLAN-Strukturen mit entsprechenden

Sicherheitsmechanismen eine hohe Qualifikation und Erfahrung der Verantwortlichen und bindet erhebliche Ressourcen in den IT-Abteilungen.

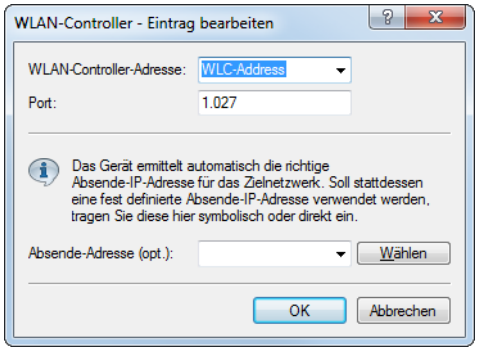
- Die manuelle Anpassung der Konfigurationen in den APs bei Änderungen in der WLAN-Struktur zieht sich ggf. über einen längeren Zeitraum hinweg, sodass es zur gleichen Zeit unterschiedliche Konfigurationen im WLAN gibt.
- Durch die gemeinsame Nutzung des geteilten Übertragungsmediums (Luft) ist eine effektive Koordination der APs notwendig, um Frequenzüberlagerungen zu vermeiden und die Netzwerkperformance zu optimieren.
- APs an öffentlich zugänglichen Orten stellen ein potenzielles Sicherheitsrisiko dar, weil mit den Geräten auch die darin gespeicherten, sicherheitsrelevanten Daten wie Kennwörter etc. gestohlen werden können. Außerdem können ggf. unbemerkt fremde APs mit dem LAN verbunden werden und so die geltenden Sicherheitsrichtlinien umgehen.

Mit einem zentralen WLAN-Management werden diese Probleme gelöst. Die Konfiguration der APs wird dabei nicht mehr in den Geräten selbst vorgenommen, sondern in einer zentralen Instanz, dem WLAN-Controller (WLC). Der WLC authentifiziert die APs und überträgt den zugelassenen Geräten eine passende Konfiguration. Dadurch kann die Konfiguration des WLANs komfortabel von einer zentralen Stelle übernommen werden und die Konfigurationsänderungen wirken sich zeitgleich auf alle APs aus. Da die vom WLC zugewiesene Konfiguration in den APs optional **nicht** im Flash, sondern im RAM abgelegt wird, können in besonders sicherheitskritischen Netzen bei einem Diebstahl der Geräte auch keine sicherheitsrelevanten Daten in unbefugte Hände geraten. Nur im „autarken Weiterbetrieb" wird die Konfiguration für eine definierte Zeit optional im Flash gespeichert (in einem Bereich, der nicht mit LANconfig oder anderen Tools auszulesen ist).

Geben Sie hier die WLC an, mit denen dieser gemanagte AP vornehmlich Verbindung aufnehmen soll. Damit der AP seine Konfiguration von einem WLC erhält, muss unter **Wireless-LAN** > **Allgemein** > **Physikalische WLAN-Einst.** > **Betrieb** die **WLAN-Betriebsart** auf **Managed** eingestellt sein.

Befinden sich der AP und der WLC im gleichen IP-Netzwerk, dann ist hier keine Einstellung erforderlich

LANconfig: **Wireless-LAN** > **WLC** > **WLAN-Controller**



WLAN-Controller-Adresse

Hier wird der Name oder die IP-Adresse des WLAN-Controllers angegeben.

Der Standardname 'WLC-Address' der LANCOM WLAN-Controller ist voreingestellt, so dass Sie hier in der Regel nichts ändern müssen. Ist eine DNS-Adressauflösung nicht möglich, so geben Sie hier die IP-Adresse des WLAN-Controllers an.

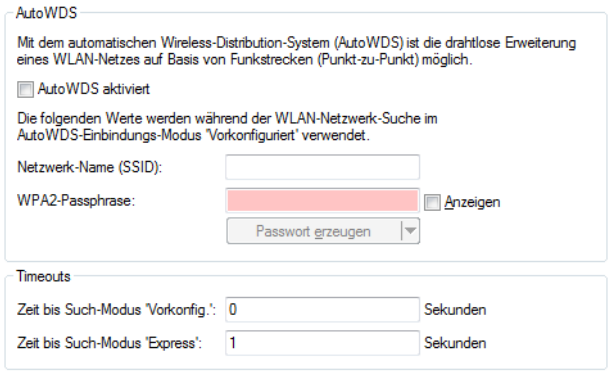
Port

Der Port, über den mit dem WLC kommuniziert wird. Default: 1027

Absende-Adresse

Hier können Sie optional eine Absendeadresse konfigurieren, die statt der ansonsten automatisch für die Zieladresse gewählten Absendeadresse verwendet wird.

13.18.18 AutoWDS



LANconfig: **Wireless LAN** > **AutoWDS**

Konfigurieren Sie hier die Einstellungen eines AP für ein automatisches Wireless-Distribution-System (AutoWDS). Informationen hierzu finden Sie unter *AutoWDS – Kabellose Integration von APs über P2P-Verbindungen* auf Seite 1196.

13.18.19 Erweiterte WLAN-Parameter

- **ProbeRsp-Retries**

  Konsole: **Setup** > **Schnittstellen** > **WLAN** > **Übertragung**

  Dies ist die Anzahl der Hard-Retries für Probe-Responses, also Antworten, die ein AP als Antwort auf einen Probe-Request von einem Client schickt.

  Mögliche Werte:

  - 0 bis 15

  Default:

  - 3

  Default:

  - Werte größer als 15 werden wie 15 behandelt.

- **Sperrzeit**

  Konsole: **Setup** > **Schnittstellen** > **WLAN** > **Roaming**

  In der Betriebsart als WLAN-Client und bei mehreren gleichen WLAN-Zugangspunkte (gleiche SSID auf mehreren APs) können Sie hier einen Zeitraum zu definieren, in dem sich der WLAN-Client nicht mehr mit einem AP verbindet, nachdem die Anmeldung an diesem AP abgelehnt wurde (Association-Reject).

  Mögliche Werte:

  - 0 bis 4294967295 in Sekunden

  Default:

  - 0

13.18.19.1 Rausch-Offsets

Die Funkmodule der WLAN-Geräte können Rausch- und Signalpegel als absolute Werte (in dBm) angeben. Die Empfangsteile sind jedoch ab Werk nicht kalibriert. Um die Genauigkeit der Angaben für Rausch- und Signalpegel zu optimieren, können in der Rausch-Offset-Tabelle abhängig von Funkband (2,4 / 5 GHz), Kanal und WLAN-Schnittstelle

Korrekturwerte (in dB) angegeben werden, die zu den von den Funkmodulen gelieferten Werten für Rausch- und Signalpegel addiert werden.

Konsole: **Setup** > **WLAN** > **Rausch-Offsets**

- **Band**

  Frequenzband, für das der Rausch-Offset-Wert angegeben wird.

  Mögliche Werte:

  - 2,4 oder 5 GHz

  Default:

  - 2,4 GHz

- **Kanal**

  Kanal, für den der Rausch-Offset-Wert angegeben wird.

  Mögliche Werte:

  - Gültige Kanalbezeichnung für das gewählte Frequenzband, maximal 5 Zeichen

  Default:

  - leer

- **Schnittstelle**

  Physikalische WLAN-Schnittstelle, für die der Rausch-Offset-Wert angegeben wird.

  Mögliche Werte:

  - Auswahl aus der Liste der möglichen WLAN-Interfaces.

  Default:

  - WLAN-1

- **Wert**

  Rausch-Offset-Wert in dB, der zu den vom Funkmodul übermittelten Werten addiert wird.

  Mögliche Werte:

  - Maximal 4 Ziffern.

  Default:

  - leer



Die Ermittlung der geeigneten Offset-Werte mit einem entsprechenden Meßaufbau obliegt dem Betreiber der WLAN-Geräte. Die Werte können durch produktionsbedingte Streuungen, Alterung und Umwelteinflüsse schwanken und müssen je nach Gerät einzeln ermittelt sowie ggf. regelmäßig überprüft werden, sofern der Bedarf für die exakten Signalpegel-Angaben dies rechtfertigt. LANCOM liefert nur für einige Modelle Standard-Werte. Aufgrund der genannten Schwankungen übernimmt LANCOM keine Gewähr für die Genauigkeit dieser Werte.

13.18.19.2 UUID-Info-Element für LANCOM WLAN Access Points

Alle aktuellen LANCOM APs sind Multi-SSID-fähig. D. h., sie können mehreren WLAN-Clients gleichzeitig unterschiedliche 'virtuelle' APs anbieten.

Bei Geräten mit zwei Funkmodulen (Dual Radio) beziehen sich darüber hinaus die BSSIDs der logischen Netzwerke zwar auf das entsprechende Funkmodul, die MAC-Adressen der beiden Funkmodule sind jedoch völlig unabhängig voneinander. Somit lassen sich logische Netzwerke mit unterschiedlicher BSSID nicht eindeutig einem Gerät zuordnen.

Zur Netzwerk-Überwachung und -Planung ist es jedoch sinnvoll, die logischen Netzwerke den entsprechenden Geräten (bzw. Funkmodulen) zuordnen zu können.

LANCOM APs unterstützen unter anderem ein Aironet-kompatibles Info-Element, das den vom Administrator vergebenen Namen des Gerätes beinhaltet. Die Übertragung dieser Information ist jedoch optional, wobei viele Anwender sie deaktivieren, weil sie z. B. aus Sicherheitsgründen so wenig Informationen wie möglich über den AP im Netzwerk veröffentlichen möchten.

Bei der Überwachung des Netzwerkes taucht diese Information also entweder gar nicht auf, oder sie identifiziert das Gerät je nach Eingabe nicht zwingend als AP.

Darüber hinaus besitzen LANCOM Access Points eine UUID (Universally Unique Identifier), die aus Geräte-Typ und Seriennummer errechnet wird und das Gerät eindeutig im Netzwerk identifizieren kann. Durch eine Verschlüsselung bei der UUID-Erzeugung ist jedoch ein Rückschluss auf Gerät oder Seriennummer nur mit hohem Aufwand (Brute-Force-Angriff über alle möglichen Geräte-Typen und Seriennummern) möglich.

Sie können die Übertragung der UUID je Funkmodul und logischem Netzwerk unabhängig voneinander ein- oder ausschalten.

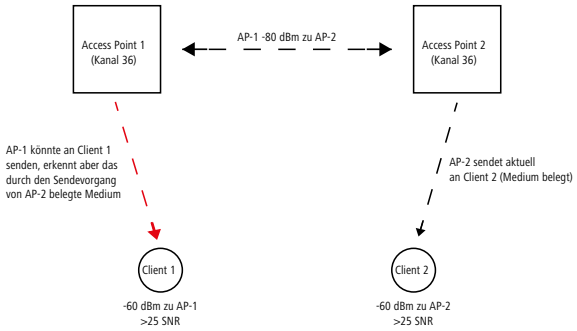
13.18.19.3 Ratenadaptionsalgorithmus

Eine WLAN-Verbindung nutzt, im Gegensatz zu einer Ethernet-Verbindung, variable Bitraten. Höhere Bitraten bieten einen besseren Durchsatz, setzen allerdings auch eine höhere Signalqualität beim Empfänger voraus. Dies ist Voraussetzung für eine fehlerlose Dekodierung. WLAN-Geräte passen die Bitrate an, wenn sich Eigenschaften des Mediums ändern oder eine erste Verbindung hergestellt wird. Dadurch wird sichergestellt, dass das Gerät die beste verfügbare Bitrate nutzt.

Der bekannte Minstrel-Algorithmus prüft im Gegensatz zum Standard-Algorithmus nicht ausschließlich die benachbarten Bitraten sondern alle Bitraten. Somit wird die optimale Bitrate schneller bestimmt.

13.18.19.4 Reduzierung der Empfindlichkeit für empfangene Pakete

In High Density-Szenarien wie Stadien, Messehallen oder Auditorien kommt es unausweichlich zu einer hohen Auslastung des Mediums durch Access Points, die den gleichen Kanal benutzen. Dadurch kann eine Situation entstehen, bei der die Access Points ihre Übertragungen an die Clients zurückhalten, weil der Kanal häufiger als belegt erkannt wird.



Durch eine ab LCOS 10.30 RU1 mögliche Reduzierung der Empfangssempfindlichkeit kann ein Access Points künstlich „tauber" eingestellt werden. Hierdurch werden Übertragungen, die weiter entfernt sind, vom Access Point „überhört" und der Kanal wird somit öfter als „frei" erkannt. Es sind somit vereinfacht gesprochen mehr gleichzeitige Übertragungen auf dem gleichen Kanal möglich. Einserseits steigt dadurch der Gesamtdurchsatz eines Systems, aber auf der anderen Seite steigt auch die Interferenz auf Seiten der Clients.

Ein Client weiß nämlich nichts von der künstlichen Schwerhörigkeit. Er empfängt weiterhin die gewollten Signale seines Access Points sowie die Signale der anderen Access Points auf dem gleichen Kanal. Nur wenn der Signal-zu-Rauschabstand (SNR) weiterhin gut bleibt, werden die zusätzlichen Übertragungen dank dieses Features auch sauber vom Client empfangen. Ein weiterer Nebeneffekt des Unwissens der Clients ist, dass ein zu hoch eingestellter Wert den Effekt ins Gegenteil verkehren kann. Da der Access Point nicht zwischen Übertragungen von eigenen Clients und von anderen Geräten – sowohl Access Points als auch Clients – unterscheiden kann, wird nur das gehört, was über dem eingestellten

Schwellenwert liegt – egal von wem es kommt. Es kann somit passieren, dass die Übertragung eines verbundenen Clients vom Access Point nicht mehr „gehört" wird. Hierduch ensteht eine asymmetrische Verbindung, der Client wird den Access Point möglicherweise noch gut empfangen und geht daher von einer guten Verbindung aus, während der Access Point vom Client nichts mehr mitbekommt und ihn somit ignoriert. Empfehlenswert ist, die Reduzierung so einzustellen, dass dadurch keine Benachteiligung von Clients entsteht.

Die Reduzierung stellen Sie über die Konsole im Wert **Setup** > **Schnittstellen** > **WLAN** > **Radio-Einstellungen** > **Rx-Paket-Empf.-Reduktion** ein. Der Wertebereich von 0-20 entspricht dabei einer minimalen Empfangsstärke im Bereich von -95 dBm (0) bis -75 dBm (20). Prinzipiell treten bei den WLAN-Funkmodulen herstellungsbedingt Streuungen auf. Dadurch kann die reale Empfangsstärke geringfügig abweichen.

Für WLAN-Controller kann diese Einstellung ebenfalls über die Konsole im Profil eines Access Points vorgenommen werden. Also unter **Setup** > **WLAN-Management** > **AP-Konfiguration** > **Basisstationen** die Werte **Modul-1-Rx-Paket-Empf.-Reduktion** resp. **Modul-2-Rx-Paket-Empf.-Reduktion** entsprechend anpassen.

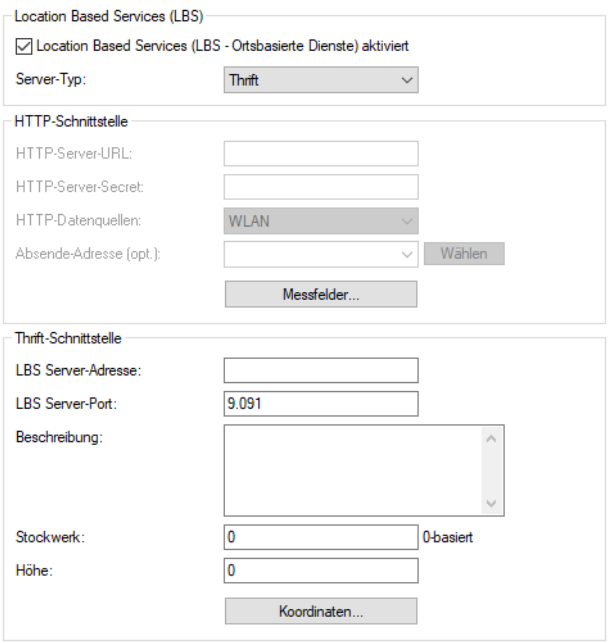
Dieses Feature ist für Experten! Wie in der Beschreibung bereits gesagt, kann es statt einem Mehrwert auch das Gegenteil bewirken und Übertragungen auf der Seite des Access Points stören. Einerseits sollte die Reduzierung mit einem Puffer zu den üblichen RSSI-Werten der Clients auf Seiten des Access Points konfiguriert werden. Andererseits sind die Retries bzw. die WLAN-Quality-Indizes zu beachten. Wenn diese sich nach Erhöhung dieses Wertes deutlich verschlechtern, dann deutet dies auf einen zu hohen Wert hin.

13.18.20 Location Based Services (LBS)

Die LANCOM Access Points können als LBS-Client mit einem LBS-Server zusammen arbeiten. Dann melden Sie an den LBS-Server alle verbundenen Clients, sodass der LBS-Server entsprechend diesen Clients ortsbasierte Dienste anbieten kann. Unterstützt werden ab LCOS 10.42 eine HTTP-Schnittstelle und eine schon länger unterstützte Thrift-Schnittstelle.

Mittels der HTTP-Schnittstelle können Access Points LBS-Daten direkt an einen frei konfigurierbaren HTTP-Endpunkt senden. Da die Daten im JSON-Format vorliegen, wird eine einfache Verarbeitung auf der Empfängerseite sichergestellt.

LANconfig: **Sonstige Dienste** > **Dienste** > **Location Based Services (LBS)**



Location Based Services (LBS – Ortsbasierte Dienste) aktiviert

Aktiviert oder deaktiviert die ortsbasierenden Dienste.

Server-Typ

Konfigurieren Sie hier, ob die HTTP-Schnittstelle oder die Thrift-Schnittstelle verwendet werden soll.

13.18.20.1 HTTP-Schnittstelle

Mittels der HTTP-API können Access Points LBS-Daten direkt an einen frei konfigurierbaren HTTP-Endpunkt senden. Da die Daten im JSON-Format vorliegen, wird eine einfache Verarbeitung auf der Empfängerseite sichergestellt.

HTTP Server-URL

Konfigurieren Sie hier die URL des HTTP-Endpunkts.

Es werden HTTP und HTTPS unterstützt. Bei der Verwendung von HTTPS kann entweder keine Zertifikatsprüfung, eine Prüfung des Server-Zertifikat oder eine beidseite Prüfung mit Server- und Client-Authentisierung stattfinden. Dazu kann ein PKCS#12-Container mit CA- und Client-Zertifikat auf das Gerät hochgeladen werden, der das CA-Zertifikat oder das CA- und Client-Zertifikat enthält. Dies kann über LANconfig oder WEBconfig erfolgen.Wird kein PKCS#12-Container hochgeladen, wird bei Verwendung von HTTPS keine Zertifikatsprüfung durchgeführt.

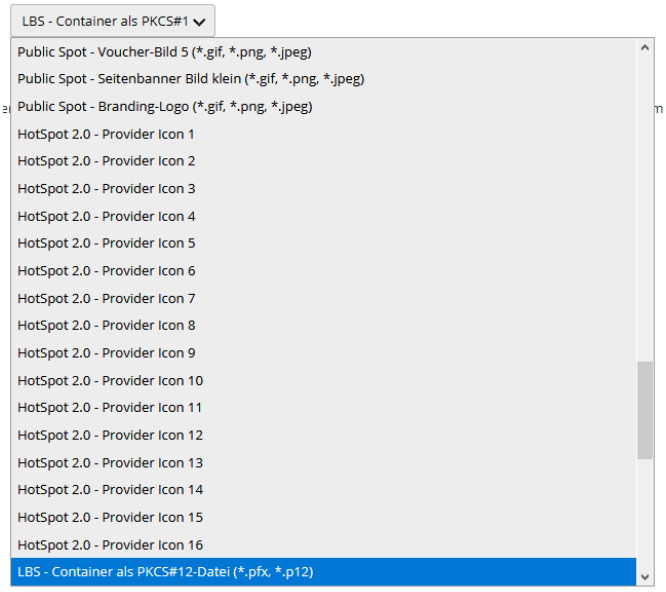


Abbildung 19: Screenshot WEBconfig

HTTP-Server-Secret

Das HTTP-Server-Secret wird in den JSON-Nachrichten des Access Points zum Endpunkt übertragen und kann dazu dienen, die Nachrichten zusätzlich zu authentifizieren.

HTTP-Datenquellen

Konfigurieren Sie hier, ob WLAN-, BLE- oder beide Arten von LBS-Daten gesendet werden sollen.

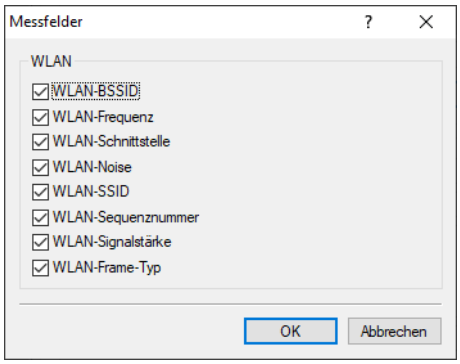
Die Einstellung **BLE** ist nur bei Geräten mit mit verbautem BLE-Modul unterstützt.

Absende-Adresse

Konfigurieren Sie hier, welche Absendeadresse für die Kommunikation mit dem HTTP-Endpunkt verwendet werden soll. Dies kann erforderlich sein, wenn auf dem Gerät mehrere IP-Netzwerke konfiguriert sind.

Messfelder

Konfigurieren Sie hier im Detail, welche Messfelder bzw. vom Access Point ermittelten Daten in den Nachrichten an den HTTP-Endpunkt enthalten sein sollen. Es empfiehlt sich, diese auf den tatsächlich benötigten Umfang anzupassen, um das Datenaufkommen gering zu halten.



Datenformat der an den Endpunkt gesendeten Nachrichten

› Für **WLAN**:

```
{
  "version": "1.0",
  "secret": "geheim",
  "type": "WLAN",
  "deviceMac": "00a057000000",
  "measurements": [
    {
      "clientMac": "334455667788",
      "seenTime": 1579792598996,
      "frameSeqNum": 1074,
      "ssid": "",
      "module": 0,
      "bssid": "00a057000000",
      "rssi": -56,
      "frequency": 2462,
      "noise": -70,
      "frameType": "PROBE"
    },
    {
      "clientMac": "554433aabbcc",
      "seenTime": 1579792601334,
      "frameSeqNum": 2742,
      "ssid": "",
      "module": 0,
      "bssid": "00a057000000",
      "rssi": -45,
      "frequency": 2462,
      "noise": -70,
      "frameType": "PROBE"
    }
  ]
}
```

version

Die Version der verwendeten API. Aktuell ist dies immer 1.0.

secret

Das in der Konfiguration des Access Points festgelegte HTTP-Server-Secret.

type

Der Typ der gesendeten Daten. Kann entweder WLAN oder BLE sein.

deviceMac

Die LAN-MAC-Adresse des Access Points.

measurements

Hierin ist mindestens ein Messwert enthalten. Es können aber auch mehrere enthalten sein.

clientMac

Die MAC-Adresse des WLAN-Clients.

seenTime

Der Zeitstempel (in Unix-Zeit), zu dem der WLAN-Frame vom Client am Access Point empfangen wurde.

frameSeqNum

Die Sequenznummer des empfangenen WLAN-Frames.

ssid

Die im WLAN-Frame enthaltene SSID, sofern vorhanden.

module

Beschreibt, von welcher WLAN-Schnittstelle des Access Points der WLAN-Frame empfangen wurde. Typischerweise 0 für die erste WLAN-Schnittstelle oder 2 für die zweite WLAN-Schnittstelle.

bssid

Die im WLAN-Frame enthaltene BSSID.

rssi

Die Signalstärke in dBm des empfangenen WLAN-Frames.

frequency

Die Frequenz in MHz des WLAN-Kanals, auf dem der WLAN-Frame empfangen wurde.

noise

Der Rauschpegel in dBm auf dem Kanal, auf dem der WLAN-Frame empfangen wurde.

frameType

Der Frame-Typ des empfangenen WLAN-Frame. Folgende Typen sind möglich: `PROBE`, `AUTHENTICATION`, `ASSOCIATION`, `DEAUTHENTICATION` oder `DEASSOCIATION`.

› Für **BLE**:

```
{
  "version": "1.0",
  "secret": "geheim",
  "type": "BLE",
  "deviceMac": "00a057000000",
  "measurements": [
    {
      "deviceAddress": "001122334455",
      "seenTime": 1579792601269,
      "addressType": "Random",
      "rssi": -77
    },
    {
      "deviceAddress": "ffeeddccbbaa",
      "seenTime": 1579792601273,
      "addressType": "Random",
      "rssi": -61
      "name": "test",
      "advertisingData": "1eff0600010920024bab81ba8815c5dc61c38449a886740a1ddb09b9e2ad8e",
      "scanResponseData": "050974657374"
    }
  ]
}
```

version

Die Version der verwendeten API. Aktuell ist dies immer 1.0.

secret

Das in der Konfiguration des AP festgelegte HTTP-Server-Secret.

type

Der Typ der gesendeten Daten. Kann entweder WLAN oder BLE sein.

deviceMac

Die LAN-MAC-Adresse des AP.

measurements

Hierin ist mindestens ein Messwert enthalten. Es können aber auch mehrere enthalten sein.

deviceAddress

Die Adresse des BLE-Gerätes bzw. -Clients.

seenTime

Der Zeitstempel (in Unix-Zeit), zu dem der BLE-Frame vom Client am AP empfangen wurde.

addressType

Der BLE-Adresstyp. Folgende Adresstypen sind möglich: `Public` oder `Random`.

rssi

Die Signalstärke in dBm des empfangenen BLE-Frames.

name

Der vom BLE-Gerät übermittelte Name. Kann nur übermittelt werden, wenn der aktive BLE-Scan in den BLE-Betriebseinstellungen aktiviert ist.

advertisingData

Das komplette vom BLE-Gerät übermittelte Advertisement.

scanResponseData

Die komplette vom BLE-Gerät übermittelte Scan-Response. Kann nur übermittelt werden, wenn der aktive BLE-Scan in den BLE-Betriebseinstellungen aktiviert ist.

13.18.20.2 Thrift-Schnittstelle

LBS Server-Adresse

Geben Sie hier die Adresse des LBS-Servers ein.

LBS Server-Port

Geben Sie hier den Port des LBS-Servers ein.

Beschreibung

Geben Sie hier eine Beschreibung des Gerätes ein.

Stockwerk

Geben Sie hier die Etage ein, auf der sich das Gerät befindet. So differenzieren Sie z. B. zwischen Ober- und Untergeschoss.

Höhe

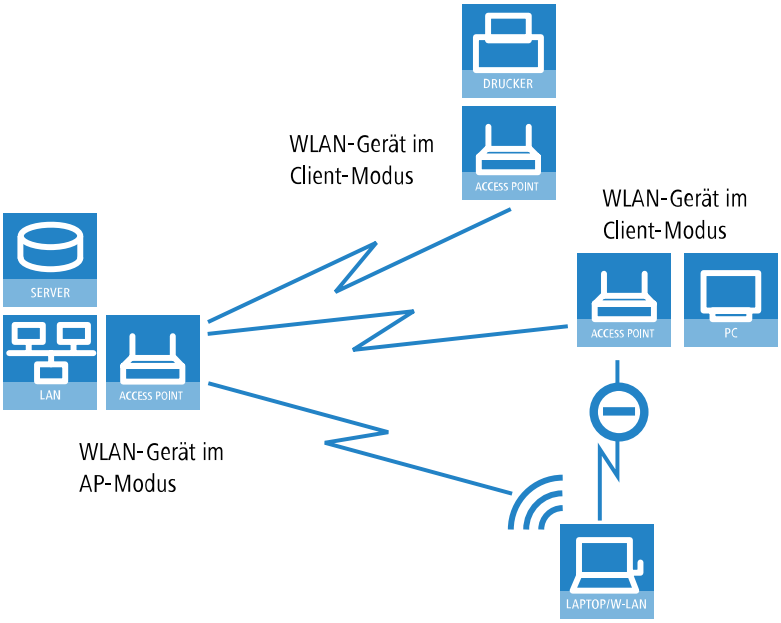
Geben Sie hier die Höhe ein, auf der sich das Gerät befindet. Die Angabe eines negativen Wertes ist möglich, so dass Sie zwischen einer Position über und unter dem Meeresspiegel differenzieren können.

Koordinaten

Standortkoordinaten des Gerätes. Die Angabe erfolgt im geographischen Koordinatensystem über den **Breitengrad** und **Längengrad**.

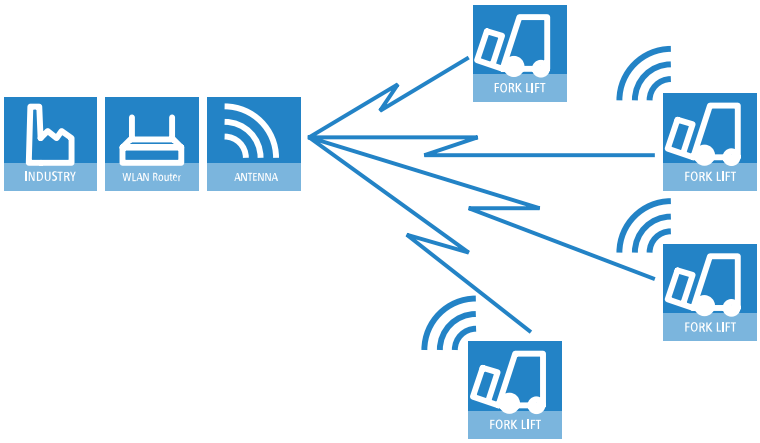
13.19 Konfiguration des Client-Modus

Zur Anbindung von einzelnen Geräten mit einer Ethernet-Schnittstelle in ein Funk-LAN können LANCOM Geräte mit WLAN-Modul in den sogenannten Client-Modus versetzt werden, in dem sie sich wie ein herkömmlicher Funk-LAN-Adapter verhalten und nicht wie ein Access Point (AP). Über den Client-Modus ist es also möglich, auch Geräte wie PCs oder Drucker, die ausschließlich über eine Ethernet-Schnittstelle verfügen, in ein Funk-LAN einzubinden.



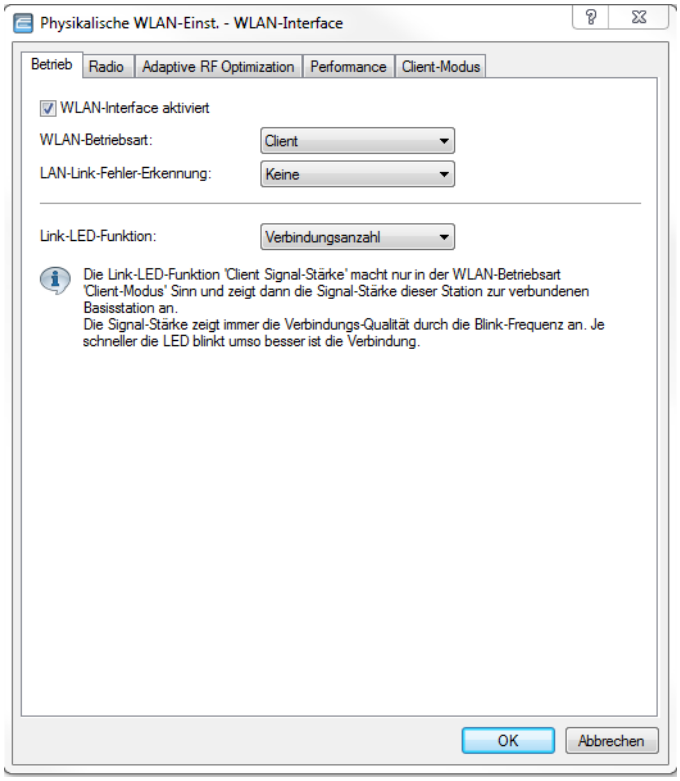
Bei einem WLAN-Gerät im AP-Modus können sich weitere WLAN-Clients anmelden, bei einem WLAN-Gerät im Client-Modus jedoch nicht.

In industriellen Anwendungen können die WLAN-Clients auch mobil eingesetzt werden, z. B. auf einem Gabelstapler, der über die drahtlose Verbindung ständig Kontakt zu seiner Leitstelle hält.



13.19.1 Client-Modus mit LANconfig aktivieren

Um Ihr Gerät mittels LANconfig in den Client-Modus zu versetzen, wechseln Sie in die Ansicht **Wireless-LAN** > **Allgemein** > **Physikalische WLAN-Einst.** und wählen Sie im Reiter **Betrieb** die WLAN-Betriebsart **Client**. Bestätigen Sie Ihre Auswahl mit einem Klick auf die Schaltfläche **OK**.



13.19.2 Client-Einstellungen

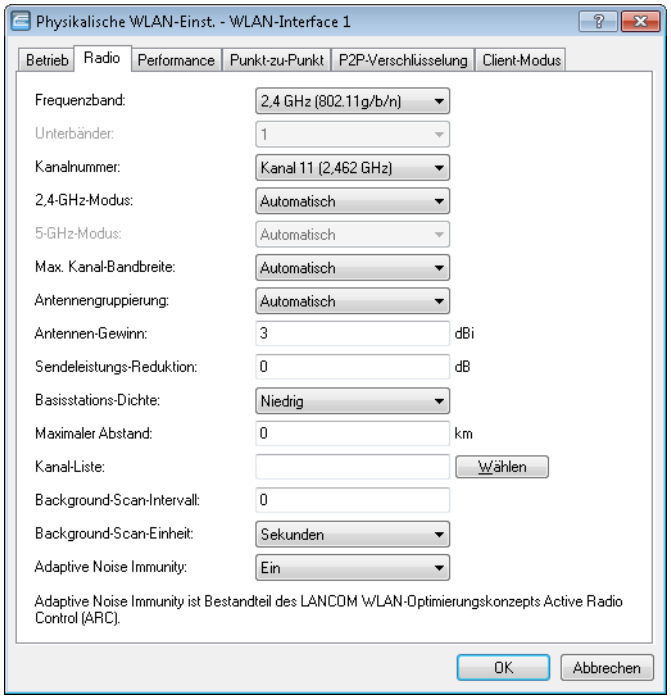
Für LANCOMAPs und LANCOM Wireless Router im Client-Modus können auf der Registerkarte 'Client-Modus' bei den Einstellungen für die physikalischen Interfaces (**Wireless-LAN** > **Allgemein** > **Physikalische WLAN-Einst.**) weitere Einstellungen bzgl. des Verhaltens als Client vorgenommen werden. Siehe *Client-Modus* auf Seite 1027.

Die Konfiguration der Client-Einstellungen kann auch mit dem WLAN-Assistenten von LANconfig erfolgen.

13.19.3 Radio-Einstellungen

Damit der WLAN-Client eine Verbindung zu einem AP aufbauen kann, muss er geeignete Frequenzbänder bzw. Kanäle verwenden.

1. Zum Bearbeiten der Radio-Einstellungen wechseln Sie unter LANconfig bei den physikalischen WLAN-Einstellungen für das gewünschte WLAN-Interface auf die Registerkarte 'Radio'.



2. Stellen Sie das Frequenz-Band, die Kanäle und den 2,4-GHz- bzw. 5-GHz-Modus passend zu den Einstellungen des APs ein.

Je nach Modell entfällt die Auswahl des Frequenzbandes und der Kanäle, z. B. wenn das Gerät nur ein Frequenzband unterstützt.

13.19.3.1 Greenfield-Modus für Access Points mit IEEE 802.11n

Bei APs nach dem Standard IEEE 802.11n haben Sie in den physikalischen WLAN-Einstellungen die Möglichkeit, die Datenübertragung nach den Standards IEEE 802.11a/b/g/n gezielt zu erlauben oder einzuschränken.

Neben der Auswahl der einzelnen Standards a/b/g/n und verschiedenen gemischten Betriebsarten erlauben die APs auch die Auswahl des Greenfield-Modus. Wenn Sie in den physikalischen WLAN-Einstellungen einer WLAN-Schnittstelle den Greenfield-Modus aktivieren, können sich nur WLAN-Clients in die zugehörigen logischen WLANs (SSIDs) einbuchen, die ihrerseits den Standard IEEE 802.11n unterstützen. Andere WLAN-Clients, die ausschließlich nach den Standards IEEE 802.11a/b/g arbeiten, können sich nicht in diese WLANs einwählen.

Der Standard IEEE 802.11n erlaubt nur Verschlüsselungen nach WPA2 / AES und unverschlüsselte Verbindungen. WEP- und TKIP-basierte Verschlüsselungen sind in IEEE 802.11n nicht erlaubt. Bitte beachten Sie je nach Einstellungen der physikalischen und logischen WLAN-Einstellungen die folgenden Einschränkungen:

› Wenn Sie in den physikalischen Einstellungen einen gemischten Modus mit Unterstützung für den Standard IEEE 802.11n aktivieren und einzelne WLAN-Clients in einem logischen Netzwerk nur WEP-Verschüsselung erlauben,

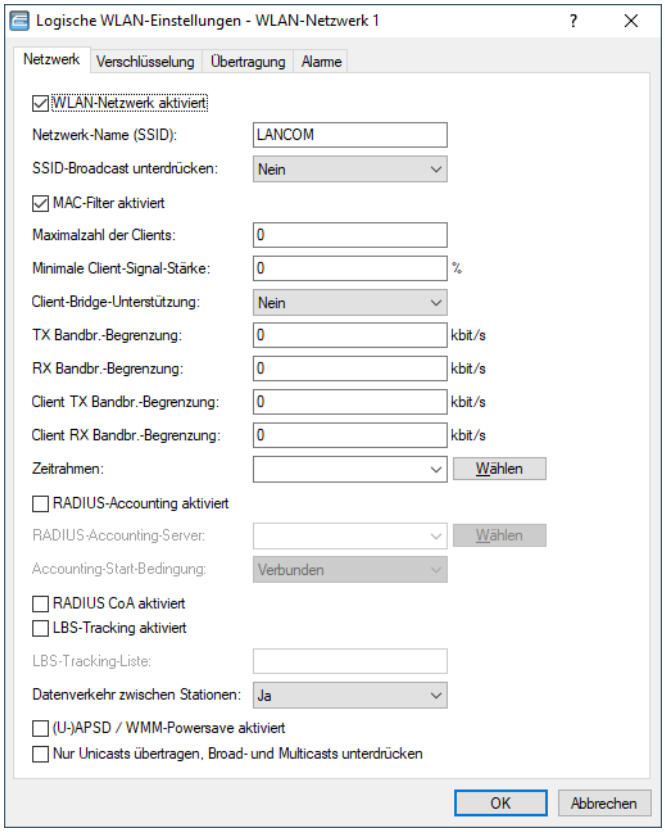
reduziert der AP die Übertragungsrate auf den Standard 802.11a/b/g, weil die höheren Übertragungsraten nach IEEE 802.11n in Kombination mit WEP nicht erlaubt sind.

- Wenn Sie in den Verschlüsselungseinstellungen eines logischen WLANs neben AES auch andere Sitzungsschlüssel nach TKIP erlauben, verwendet der AP für dieses WLAN ausschließlich den Sitzungsschlüssel nach AES, weil TKIP nach IEEE 802.11n nicht erlaubt ist.
- Wenn Sie in den Verschlüsselungseinstellungen eines logischen WLANs ausschließlich Sitzungsschlüssel nach TKIP erlauben, reduziert der AP die Übertragungsrate auf den Standard 802.11a/b/g, weil die höheren Übertragungsraten nach IEEE 802.11n in Kombination mit TKIP nicht erlaubt sind.

13.19.4 SSID des verfügbaren Netzwerks einstellen

In den WLAN-Clients muss die SSID des Netzwerks eingetragen werden, zu dem sich die Clientstationen verbinden soll.

1. Zum Eintragen der SSID wechseln Sie unter LANconfig nach **Wireless-LAN** > **Allgemein**. Nach einem Klick auf **Logische WLAN-Einstellungen** wählen Sie das **erste** WLAN-Interface aus.

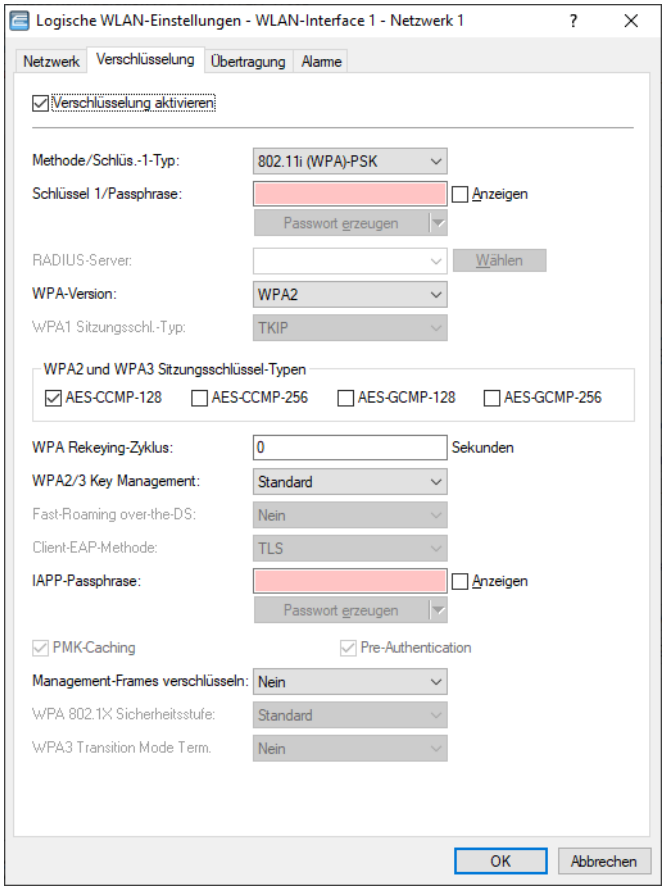


2. Aktivieren Sie auf der Registerkarte **Netzwerk** das WLAN-Netzwerk und tragen Sie die SSID des Netzwerks ein, bei dem sich die Clientstation einbuchen soll.

13.19.5 Verschlüsselungseinstellungen

Für den Zugriff auf ein WLAN müssen in der Clientstation die entsprechenden Verschlüsselungsmethoden und Schlüssel eingestellt werden.

1. Zum Eintragen der Schlüssel wechseln Sie unter LANconfig nach **Wireless LAN** > **Allgemein** > **Logische WLAN-Einstellungen** > **Verschlüsselung**.



2. Aktivieren Sie die Verschlüsselung und passen Sie die Verschlüsselungsmethode an die Einstellungen des APs an.
3. LANCOM APs und LANCOM Wireless Router in der Betriebsart als WLAN-Client können sich über EAP / 802.1X bei einem anderen AP authentifizieren. Wählen Sie dazu hier die gewünschte Client-EAP-Methode aus. Beachten Sie, dass die gewählte Client-EAP-Methode zu den Einstellungen des APs passen muss, bei dem sich das Gerät einbuchen will.

Je nach gewählter EAP-Methode müssen im Gerät die entsprechenden Zertifikate hinterlegt werden:

- Für TTLS und PEAP nur das EAP / TLS-Root-Zertifikat, als Schlüssel wird dabei die Kombination Benutzername:Kennwort eingetragen.
- Für TLS zusätzlich das EAP / TLS-Gerätezertifikat samt privatem Schlüssel.

Bei der Verwendung von WPA bzw. 802.1X sind evtl. weitere Einstellungen im RADIUS-Server notwendig.

13.19.6 PMK-Caching im WLAN-Client-Modus

Beim Verbindungsaufbau eines WLAN-Clients zu einem AP handeln die beiden Gegenstellen im Rahmen der 802.1X-Authentifizierung einen gemeinsamen Schlüssel für die nachfolgende Verschlüsselung aus, den Pairwise Master Key (PMK). Bei Anwendungen mit bewegten WLAN-Clients (Notebooks in größeren Büro-Umgebungen, bewegte Objekte mit WLAN-Anbindung im Industriebereich) wechseln die WLAN-Clients häufig den AP, bei dem sie sich in einem WLAN-Netz anmelden. Die WLAN-Clients roamen also zwischen verschiedenen, aber in der Regel immer den gleichen APs hin und her.

APs speichern üblicherweise einen ausgehandelten PMK für eine bestimmte Zeit. Auch ein WLAN-Gerät in der Betriebsart als WLAN-Client speichert den PMK. Sobald ein WLAN-Client einen Anmeldevorgang bei einem AP startet, zu dem zuvor schon eine Verbindung bestand, kann der WLAN-Client direkt den vorhandenen PMK zur Prüfung an den AP übermitteln. Die beiden Gegenstellen überspringen so die Phase der PMK-Aushandlung während des Verbindungsaufbaus, WLAN-Client und AP stellen die Verbindung deutlich schneller her.

13.19.7 Prä-Authentifizierung im WLAN-Client-Modus

Die schnelle Authentifizierung über den Pairwise Master Key (PMK) funktioniert nur, wenn der WLAN-Client sich bereits zuvor am AP angemeldet hat. Um die Dauer für die Anmeldung am AP schon beim ersten Anmeldeversuch zu verkürzen, nutzt der WLAN-Client die Prä-Authentifizierung.

Normalerweise scannt ein WLAN-Client im Hintergrund die Umgebung nach vorhandenen APs, um sich ggf. mit einem von ihnen neu verbinden zu können. APs, die WPA2 / 802.1X unterstützen, können ihre Fähigkeit zur Prä-Authentifizierung den anfragenden WLAN-Clients mitteilen. Eine WPA2-Prä-Authentifizierung unterschiedet sich dabei von einer normalen 802.1X-Authentifizierung in den folgenden Abläufen:

- Der WLAN-Client meldet sich am neuen AP über das Infrastruktur-Netzwerk an, das die APs miteinander verbindet. Das kann eine Ethernet-Verbindung, ein WDS-Link (Wireless Distribution System) oder eine Kombination beider Verbindungen sein.
- Ein abweichendes Ethernet-Protokoll (EtherType) unterscheidet eine Prä-Authentifizierung von einer normalen 802.1X-Authentifizierung. Damit behandeln der aktuelle AP sowie alle anderen Netzwerkpartner die Prä-Authentifizierung als normale Datenübertragung des WLAN-Clients.
- Nach erfolgreicher Prä-Authentifizierung speichern jeweils der neue AP und der WLAN-Client den ausgehandelten PMK.

  Die Verwendung von PMKs ist eine Voraussetzung für Prä-Authentifizierung. Andernfalls ist eine Prä-Authentifizierung nicht möglich.
- Sobald der Client sich später mit dem neuen AP verbinden möchte, kann er sich dank des gespeicherten PMKs schneller anmelden. Der weitere Ablauf entspricht dem *PMK-Caching*.

Client-seitig ist die Anzahl gleichzeitiger Prä-Authentifizierungen auf vier begrenzt, um in Netzwerk-Umgebungen mit vielen APs die Netzlast für den zentralen RADIUS-Server gering zu halten.

13.19.8 Mehrere WLAN-Profile im Client-Modus

13.19.8.1 Einleitung

Zur Anbindung von einzelnen Geräten mit einer Ethernet-Schnittstelle in ein WLAN können APs in den sogenannten Client-Modus versetzt werden, in dem sie sich wie ein herkömmlicher WLAN-Client verhalten und nicht wie ein AP.

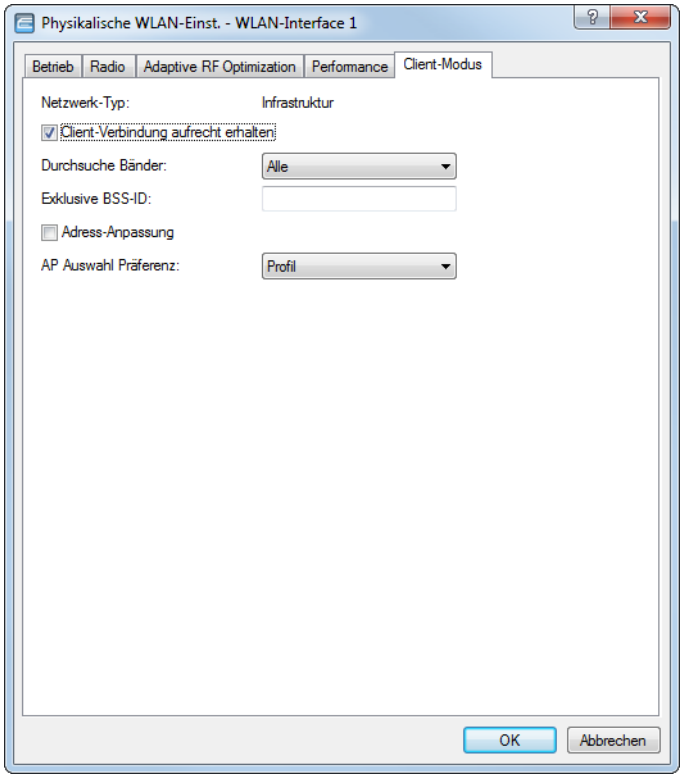
WLAN-Clients wie Notebooks können in der Regel über das Betriebssystem oder über die gerätespezifische Software verschiedene Profile speichern und verwalten, um je nach Umgebung auf verschiedene APs zuzugreifen (z. B. für ein WLAN im Unternehmen und für ein weiteres WLAN im Home-Office). In diesen Profilen sind u. a. die SSID des entsprechenden WLANs und die benötigten Schlüssel gespeichert. Der WLAN-Client wählt dann automatisch aus den verfügbaren WLANs das passende Profil für das stärkste oder das bevorzugte WLAN.

LANCOM APs können bis zu 16 verschiedene WLAN-Profile für die Verwendung im Client-Modus speichern. Für die Profile werden im Client-Modus die Netzwerk- sowie Übertragungsparameter für die logischen WLANs sowie die Verschlüsselungseinstellungen verwendet.

Bitte beachten Sie, dass Sie ein WLAN-Modul im Client-Modus sich zu jeder Zeit nur mit einem AP verbinden kann, auch wenn mehrere WLAN-Profile definiert sind.

13.19.8.2 Konfiguration

Neben den Netzwerk-, Übertragungs- und Verschlüsselungsparametern kann für jedes WLAN-Modul separat definiert werden, nach welchem Kriterium das zu verwendende Client-Profil ausgewählt werden soll.



LANconfig: **Wireless-LAN** > **Allgemein** > **Physikalische WLAN-Einst.** > **Client-Modus**

Konsole: **Setup** > **Schnittstellen** > **WLAN** > **Client-Einstellungen** > **WLAN-1**

AP Auswahl Präferenz

Wählen Sie hier aus, wie diese Schnittstelle verwendet werden soll.

Mögliche Werte:

Signalstärke

Wählt das Profil, dessen WLAN aktuell das stärkste Signal bietet. In dieser Einstellung wechselt das WLAN-Modul im Client-Modus automatisch in ein anderes WLAN, sobald diese ein stärkeres Signal bietet.

Profil

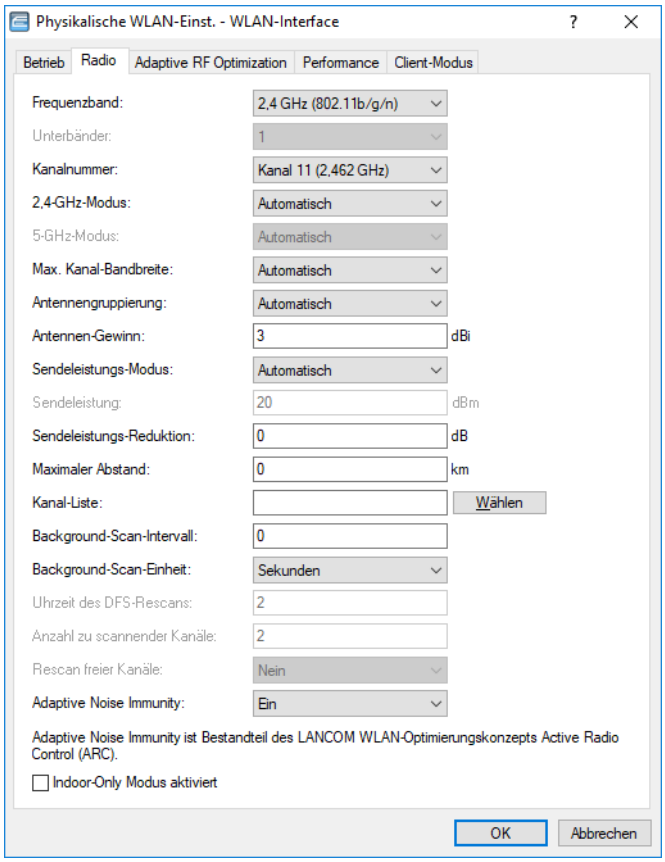
Wählt aus den verfügbaren WLANs das zu verwendende Profil in der Reihenfolge der definierten Einträge (WLAN-Index, z. B. WLAN-1, WLAN-1-2 etc.), auch wenn ein anderes WLAN ein stärkeres Signal bietet. In dieser Einstellung wechselt das WLAN-Modul im Client-Modus automatisch in ein anderes WLAN, sobald ein WLAN mit einem niedrigeren WLAN-Index erkannt wird (unabhängig von der Signalstärke dieses WLANs).

13.19.9 Roaming

Mit Roaming bezeichnet man den Übergang eines WLAN-Clients zu einem anderen AP, wenn er keine Verbindung zum bisherigen AP mehr aufrecht erhalten kann. Um das Roaming zu ermöglichen, muss sich mindestens ein weiterer AP in der Reichweite des Clients befinden, der ein Netzwerk mit der gleichen SSID und den passenden Radio- und Verschlüsselungs-Einstellungen anbietet.

Normalerweise würde der WLAN-Client sich nur dann bei einem anderen AP einbuchen, wenn er die Verbindung zu dem bisherigen AP vollständig verloren hat (Hard-Roaming). Das Soft-Roaming ermöglicht dem Client hingegen, anhand verfügbarer Scan-Informationen ein Roaming zu einem stärkeren AP durchzuführen. Mit der Funktion des Background-Scanning kann das Gerät im Client-Modus schon vor Verbindungsverlust Informationen über andere verfügbare APs sammeln. Die Umschaltung auf einen anderen AP erfolgt dann nicht erst, wenn die bisherige Verbindung vollständig verloren wurde, sondern wenn ein anderer AP in Reichweite über ein stärkeres Signal verfügt.

1. Zum Aktivieren des Soft-Roaming wechseln Sie auf **Wireless-LAN** > **Allgemein** > **Erweiterte Einstellungen** > **Experten WLAN-Einstellungen** > **Roaming** und schalten das Soft-Roaming für die gewählte Schnittstell ein und stellen Sie ggf. die weiteren Parameter wie die Schwellenwerte und Signalpegel ein.
2. Zur Konfiguration des Background-Scanning wechseln Sie unter LANconfig bei den physikalischen WLAN-Einstellungen für das gewünschte WLAN-Interface auf die Registerkarte 'Radio'.



3. Tragen Sie als Background-Scan-Intervall die Zeit ein, in welcher das Gerät zyklisch die aktuell ungenutzten Frequenzen des aktiven Bandes nach erreichbaren APs absucht. Um ein schnelles Roaming zu erzielen, wird die Scan-Zeit auf z. B. 260 Sekunden (2,4 GHz) bzw. 720 Sekunden (5 GHz) eingestellt.

13.19.9.1 ARF-Netzwerk für IAPP

APs nutzen das IAPP-Protokoll, um sich über die Roaming-Vorgänge der eingebuchten WLAN-Clients zu informieren. Die APs senden dazu regelmäßig bestimmte Multicast-Nachrichten aus (Announces), mit deren Hilfe die Geräte die BSSIDs und IP-Adressen der anderen APs lernen. Bei einem Roaming-Vorgang informiert der WLAN-Client den neuen AP darüber, bei welchem AP er bisher eingebucht war. Der neue AP kann mit den aus den IAPP-Announces gelernten Informationen den bisherigen AP informieren, der den WLAN-Client umgehend aus seiner Tabelle der eingebuchten Clients entfernen kann.

Wenn in einem AP mehrere ARF-Netzwerke definiert sind, werden die IAPP-Announces in alle ARF-Netze ausgesendet. Um diese Multicasts auf ein bestimmtes ARF-Netz zu reduzieren, kann gezielt ein IAPP-IP-Netzwerk definiert werden.

Konsole: **Setup** > **WLAN**

- **IAPP-IP-Netzwerk**

  Wählen Sie hier aus, welches ARF-Netzwerk als IAPP-IP-Netzwerk verwendet werden soll.

  Mögliche Werte:

  - Auswahl aus der Liste der im Gerät definierten ARF-Netzwerke, maximal 16 alphanumerische Zeichen.

  Default:

  - leer

  Besondere Werte:

  - leer: Wenn kein IAPP-IP-Netzwerk definiert ist, werden die IAPP-Announces in alle definierten ARF-Netze versendet.

14 WLAN-Management

14.1 Ausgangslage

Der weit verbreitete Einsatz von Wireless Access Points (APs) und Wireless Routern hat zu einem deutlich komfortableren und flexibleren Zugang zu Netzwerken in Firmen, Universitäten und anderen Organisationen geführt.

Bei allen Vorzügen der WLAN-Strukturen bleiben einige offene Aspekte:

- Alle APs benötigen eine Konfiguration und ein entsprechendes Monitoring zur Erkennung von unerwünschten WLAN-Clients etc. Die Administration der APs erfordert gerade bei größeren WLAN-Strukturen mit entsprechenden Sicherheitsmechanismen eine hohe Qualifikation und Erfahrung der Verantwortlichen und bindet erhebliche Ressourcen in den IT-Abteilungen.
- Die manuelle Anpassung der Konfigurationen in den APs bei Änderungen in der WLAN-Struktur zieht sich ggf. über einen längeren Zeitraum hinweg, sodass es zur gleichen Zeit unterschiedliche Konfigurationen im WLAN gibt.
- Durch die gemeinsame Nutzung des geteilten Übertragungsmediums (Luft) ist eine effektive Koordination der APs notwendig, um Frequenzüberlagerungen zu vermeiden und die Netzwerkperformance zu optimieren.
- APs an öffentlich zugänglichen Orten stellen ein potenzielles Sicherheitsrisiko dar, weil mit den Geräten auch die darin gespeicherten, sicherheitsrelevanten Daten wie Kennwörter etc. gestohlen werden können. Außerdem können ggf. unbemerkt fremde APs mit dem LAN verbunden werden und so die geltenden Sicherheitsrichtlinien umgehen.

14.2 Technische Konzepte

Mit einem zentralen WLAN-Management lassen sich diese Probleme lösen. Die Konfiguration der APs wird dabei nicht mehr in den Geräten selbst vorgenommen, sondern in einer zentralen Instanz, dem WLAN-Controller (WLC). Der WLC authentifiziert die APs und überträgt den zugelassenen Geräten eine passende Konfiguration. Dadurch kann die Konfiguration des WLANs komfortabel von einer zentralen Stelle übernommen werden und die Konfigurationsänderungen wirken sich zeitgleich auf alle APs aus. Da die vom WLC zugewiesene Konfiguration in den APs optional **nicht** im Flash, sondern im RAM abgelegt wird, können in besonders sicherheitskritischen Netzen bei einem Diebstahl der Geräte auch keine sicherheitsrelevanten Daten in unbefugte Hände geraten. Nur im "autarken Weiterbetrieb" wird die Konfiguration für eine definierte Zeit optional im Flash gespeichert (in einem Bereich, der nicht mit LANconfig oder anderen Tools auszulesen ist).

14.2.1 WLC-Funktionen im LANCOM vRouter

Ab LCOS 10.30 unterstützt der LANCOM vRouter zusätzlich die Funktionen eines WLAN-Controllers. Entscheiden Sie selbst und flexibel, welche Rolle Ihr LANCOM vRouter übernehmen soll: VPN-Gateway oder WLAN-Controller. Der LANCOM vRouter unterstützt ab sofort die Rolle eines virtuellen WLCs (vWLC) und kann somit Access Points verwalten. Damit können die WLAN-Controller-Funktionalitäten vollständig auf einer Virtualisierungsplattform wie VMWare ESXi oder Microsoft Hyper-V virtualisiert werden. Die Anzahl der verwalteten Access Points ist abhängig von der Lizenzkategorie des vRouters. Alle vRouter-Lizenzen, die ab dem Release von LCOS 10.30 ausgestellt wurden, enthalten eine vWLC-Option.

Produkt	VPN-Lizenzen	AP-Lizenzen
vRouter 50	10	10
vRouter 250	50	50
vRouter 500	100	100

Produkt	VPN-Lizenzen	AP-Lizenzen
vRouter 1000	200	200
vRouter unlimited	1000	1000

LANCOM Systems GmbH empfiehlt den Betrieb einer vRouter-Instanz entweder hauptsächlich als VPN-Gateway / Router oder als WLAN-Controller. Die empfohlene Nutzung kann auch anteilig erfolgen; zum Beispiel bei der Lizenzstufe „vRouter 1000“ (200 VPN-Lizenzen und 200 AP-Lizenzen):

- 100 gleichzeitige VPN-Verbindungen und 100 verwaltete APs oder
- 150 gleichzeitige VPN-Verbindungen und 50 verwaltete APs.

14.2.2 Der CAPWAP-Standard

Mit dem CAPWAP-Protokoll (Control And Provisioning of Wireless Access Points) stellt die IETF (Internet Engineering Task Force) einen Standard für das zentrale Management großer WLAN-Strukturen vor.

CAPWAP verwendet zwei Kanäle für die Datenübertragung:

- Kontrollkanal, verschlüsselt mit Datagram Transport Layer Security (DTLS). Über diesen Kanal werden die Verwaltungsinformationen zwischen dem WLC und dem AP ausgetauscht.

  DTLS ist ein auf TLS basierendes Verschlüsselungsprotokoll, welches im Gegensatz zu TLS auch über verbindungslose, ungesicherte Transportprotokolle wie UDP übertragen werden kann. DTLS verbindet so die Vorteile der hohen Sicherheit von TLS mit der schnellen Übertragung über UDP. DTLS eignet sich damit – anders als TLS – auch für die Übertragung von VoIP-Paketen, da hier nach einem Paketverlust die folgenden Pakete wieder authentifiziert werden können.
- Über diesen Datenkanal werden die Nutzdaten aus dem WLAN vom AP über den WLC ins LAN übertragen – gekapselt in das CAPWAP-Protokoll.

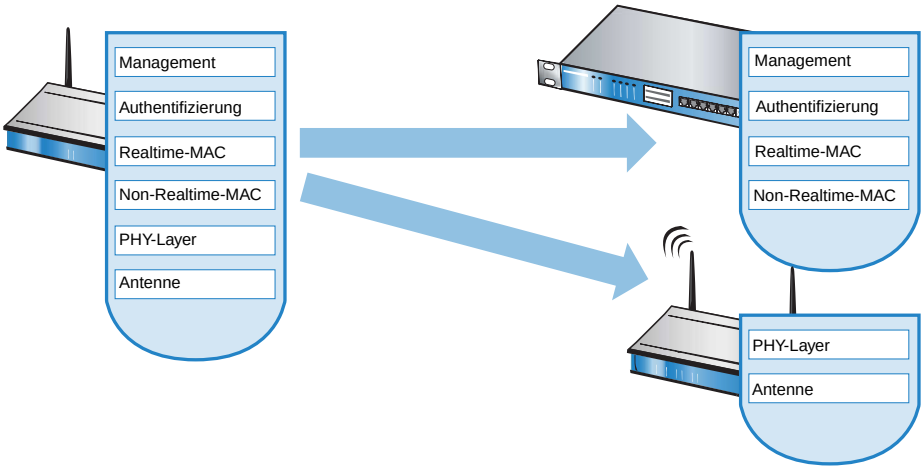
14.2.3 Die Smart-Controller-Technologie

In einer dezentralen WLAN-Struktur mit autonomen APs (Stand-Alone-Betrieb als so genannte "Rich Access Points") sind alle Funktionen für die Datenübertragung auf dem PHY-Layer, die Kontroll-Funktionen auf dem MAC-Layer sowie die Management-Funktionen in den APs enthalten. Mit dem zentralen WLAN-Management werden diese Aufgaben auf zwei verschiedene Geräte aufgeteilt:

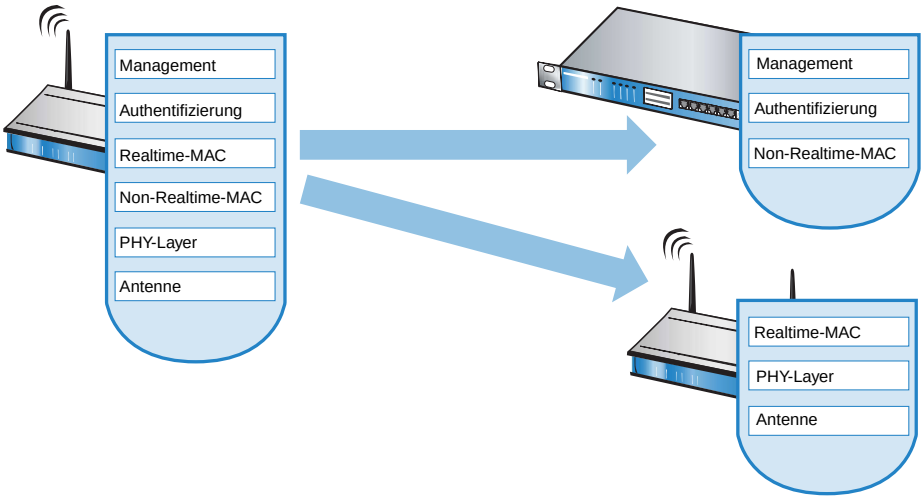
- Der zentrale WLC übernimmt die Verwaltungsaufgaben.
- Die verteilten APs übernehmen die Datenübertragung auf dem PHY-Layer und die MAC-Funktionen.
- Als dritte Komponenten kommt ggf. ein RADIUS- oder EAP-Server zur Authentifizierung der WLAN-Clients hinzu (was in autonomen WLANs aber auch der Fall sein kann).

CAPWAP beschreibt drei unterschiedliche Szenarien für die Verlagerung von WLAN-Funktionen in den zentralen WLC.

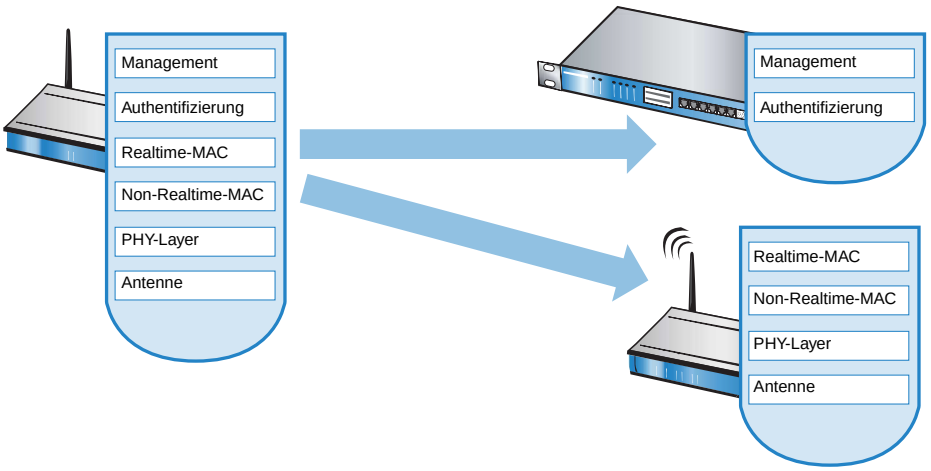
- Remote-MAC: Hier werden alle WLAN-Funktionen vom AP an den WLC übertragen. Die APs dienen hier nur als "verlängerte Antennen" ohne eigene Intelligenz.



- Split-MAC: Bei dieser Variante wird nur ein Teil der WLAN-Funktionen an den WLC übertragen. Üblicherweise werden die zeitkritischen Anwendungen (Realtime-Applikationen) weiterhin auf dem AP abgearbeitet, die nicht zeitkritischen Anwendungen (Non-Realtime-Applikationen) werden über den zentralen WLC abgewickelt.



- Local-MAC: Die dritte Möglichkeit sieht eine vollständige Verwaltung und Überwachung des WLAN-Datenverkehrs direkt in den APs vor. Zwischen dem AP und dem WLC werden lediglich Nachrichten zur Sicherung einer einheitlichen Konfiguration der APs und zum Management des Netzwerks ausgetauscht.



Die Smart-Controller-Technologie von LANCOM setzt das Local-MAC-Verfahren ein. Durch die Reduzierung der zentralisierten Aufgaben bieten die WLAN-Strukturen eine optimale Skalierbarkeit. Gleichzeitig wird der WLC in einer solchen Struktur nicht zum zentralen Flaschenhals, der große Teile des gesamten Datenverkehrs verarbeiten muss. In Remote-MAC- und Split-MAC-Architekturen müssen immer **alle** Nutzdaten zentral über den WLC laufen. In Local-MAC-Architekturen können die Daten jedoch alternativ auch direkt von den APs in das LAN ausgekoppelt werden, sodass eine hochperformante Datenübertragung ermöglicht wird. Bei der Auskopplung in das LAN können die Daten auch direkt in spezielle VLANs geleitet werden, die Einrichtung von geschlossenen Netzwerken z. B. für Gast-Zugänge sind so leicht möglich.

Layer-3-Tunneling und Layer-3-Roaming

WLCs mit LCOS unterstützen ebenfalls die Übertragung der Nutzdaten durch einen CAPWAP-Tunnel. Auf diese Weise können z. B. ausgewählte Applikationen wie VoIP über den zentralen WLC geleitet werden. Beim Wechsel der WLAN-Clients in eine andere Funkzelle bleibt so die zugrundeliegende IP-Verbindung ohne Unterbrechung, da sie fortlaufend vom zentralen WLC verwaltet wird (Layer-3-Roaming). Mobile SIP-Telefone können auf diese Weise auch während eines Gesprächs komfortabel "roamen" – über die Subnetzgrenzen im Ethernet hinweg.

Die zentrale Verwaltung der Datenströme kann in Umgebungen mit zahlreichen VLANs auch die Konfiguration der VLANs auf den Switch-Ports überflüssig machen, da alle CAPWAP-Tunnel zentral auf dem WLC verwaltet werden.

14.2.4 Kommunikation zwischen Access Point und WLAN-Controller

Die Kommunikation zwischen einem AP und dem WLC wird immer vom AP aus eingeleitet. Die Geräte suchen in folgenden Fällen nach einem WLC, der ihnen eine Konfiguration zuweisen kann:

- Bei LANCOM APs sind im Auslieferungszustand die WLAN-Module auf die Betriebsart 'Managed' eingestellt. In diesem Modus suchen die APs nach einem zentralen WLC, der ihnen eine Konfiguration zuweisen kann, und bleiben so lange im "Such-Modus", bis sie einen passenden WLC gefunden haben oder die Betriebsart für die WLAN-Module manuell geändert wird.
- Während der AP nach einem WLC sucht, sind dessen WLAN-Module ausgeschaltet.
- Bei LANCOM Wireless Routern sind im Auslieferungszustand die WLAN-Module auf die Betriebsart 'Access-Point' eingestellt. In diesem Modus arbeiten die Wireless Router als autarke Access Points mit einer lokal im Gerät gespeicherten Konfiguration. Um Teilnehmer einer zentral über WLAN-Controller verwalteten WLAN-Struktur zu werden, muss die Betriebsart für die WLAN-Module in den gewünschten Wireless Routern auf 'Managed' umgestellt werden.

Die Kommunikation zwischen Access Point und dem WLAN-Controller erfolgt per **CAPWAP** sowie per **SCEP**. Für **CAPWAP** wird in der Standard-Konfiguration der **UDP-Port 1027** verwendet (kann in der Konfiguration des WLAN-Controllers angepasst werden). Für die Kommunikation per **SCEP** wird das Protokoll **HTTP** (**TCP-Port 80**) verwendet.

Der AP sendet zu Beginn der Kommunikation eine "Discovery Request Message", um die verfügbaren WLCs zu ermitteln. Dieser Request wird grundsätzlich als Broadcast versendet. Da in manchen Strukturen ein potenzieller WLC aber nicht über Broadcast zu erreichen ist, können auch spezielle Adressen von weiteren WLCs in die Konfiguration der APs eingetragen werden.

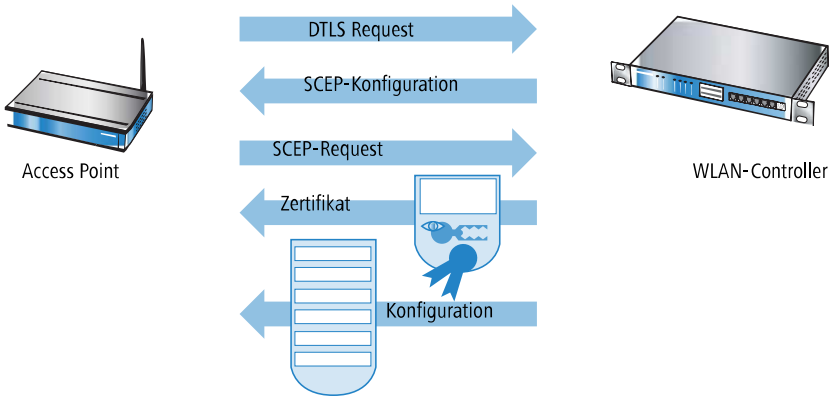
Außerdem können auch DNS-Namen von WLCs aufgelöst werden. Alle APs mit LCOS 7.22 oder höher haben den Standardnamen 'WLC-Address' bereits konfiguriert, sodass ein DNS-Server diesen Namen zu einem WLC auflösen kann. Gleiches gilt auch für die über DHCP gelernten DHCP-Suffixe. Somit können auch WLCs erreicht werden, die nicht im gleichen Netz stehen, ohne die APs konfigurieren zu müssen.

Aus den verfügbaren WLCs wählt der AP den besten aus und fragt bei diesem nach dem Aufbau der DTLS-Verbindung an. Der "beste" WLC ist für den AP derjenige mit der geringsten Auslastung, also dem kleinsten Verhältnis von gemanagten APs zu den maximal möglichen APs. Bei zwei oder mehreren gleich "guten" WLCs wählt der AP den im Netzwerk nächsten, also den mit der geringsten Antwortzeit.

Der WLC ermittelt daraufhin mit einer internen Zufallszahl einen eindeutigen und sicheren Sitzungsschlüssel, mit dem er die Verbindung zum AP schützt. Die CA im WLC stellt dem AP ein Zertifikat mittels SCEP aus. Das Zertifikat ist mit einem Kennwort für einmalige Verwendung als "Challenge" gesichert, der AP kann sich mit diesem Zertifikat gegenüber dem WLC für die Abholung des Zertifikats authentifizieren.

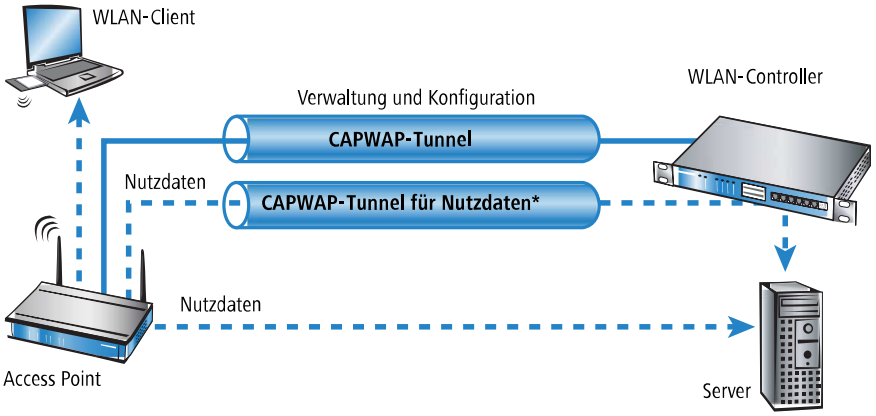
Über die gesicherte DTLS-Verbindung wird dem AP die Konfiguration für den integrierten SCEP-Client mitgeteilt – der AP kann dann über SCEP sein Zertifikat bei der SCEP-CA abholen. Anschließend wird die dem AP zugewiesene Konfiguration übertragen.

SCEP steht für Simple Certificate Encryption Protocol, CA für Certification Authority.



Sowohl Authentifizierung als auch Konfiguration können entweder automatisch vorgenommen werden oder nur bei passendem Eintrag der MAC-Adresse des AP in der AP-Tabelle des WLC. Sofern bei dem AP die WLAN-Module bei Beginn der DTLS-Kommunikation ausgeschaltet waren, werden diese nach erfolgreicher Übertragung von Zertifikat und Konfiguration eingeschaltet (sofern sie nicht in der Konfiguration explizit ausgeschaltet sind).

In der Folgezeit werden über den CAPWAP-Tunnel die Verwaltungs- und Konfigurationsdaten übertragen. Die Nutzdaten vom WLAN-Client werden im AP direkt in das LAN ausgekoppelt und z. B. an den Server übertragen.



14.2.5 Zero-Touch-Management

Mit der Möglichkeit, einem anfragenden AP ein Zertifikat und eine Konfiguration automatisch zuzuweisen, realisieren WLCs ein echtes "Zero-Touch-Management". Neue APs brauchen nur noch mit dem LAN verbunden werden; weitere Konfigurationsschritte sind erforderlich. Diese Reduzierung auf die reine Installation der Geräte entlastet die IT-Abteilungen gerade bei verteilten Strukturen, da in den entfernten Standorten kein spezielles IT- oder WLAN-Know-How zur Inbetriebnahme erforderlich ist.

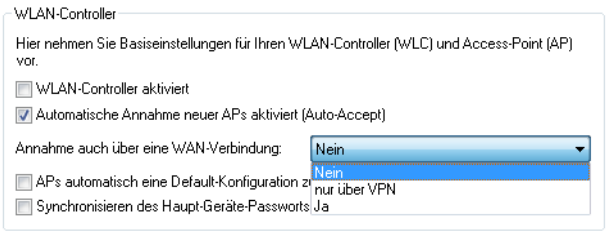
14.2.6 Split-Management

APs sind fähig, ihren WLC auch in entfernten Netzen zu suchen – eine einfache IP-Verbindung z. B. über eine VPN-Strecke reicht aus. Da die WLCs ausschließlich den WLAN-Teil der Konfiguration im AP beeinflussen, lassen sich alle anderen Funktionen separat verwalten. Durch diese Aufteilung der Konfigurationsaufgaben eignen sich WLCs ideal für den Aufbau einer firmenweiten WLAN-Infrastruktur in der Zentrale inklusive aller angeschlossenen Niederlassungen und Home-Offices.

14.2.7 Schutz vor unberechtigtem CAPWAP-Zugriff aus dem WAN

Der WLC oder LANCOM Router mit aktiver WLC-Option behandelt CAPWAP-Anfragen aus dem LAN und dem WAN identisch. Bei von WAN-Gegenstellen stammenden Anfragen übernimmt er die APs in seine AP-Verwaltung und übergibt ggf. eine Default-Konfiguration. Entsprechend konfiguriert wird der CAPWAP-Dienst auf WAN-Gegenstellen nicht mehr angeboten, so dass keine Annahme von APs und Konfigurationsvergabe auf WAN-Gegenstellen mehr stattfindet.

Die Konfiguration erfolgt unter **WLAN-Controller** > **Allgemein** im Bereich **WLAN-Controller**. Ist die automatische Annahme neuer APs aktiviert, können Sie unter **Annahme auch über eine WAN-Verbindung** wählen, ob der CAPWAP-Dienst auch auf WAN-Gegenstellen angeboten wird.



Nein

Das Gerät nimmt keine neuen APs über die WAN-Verbindung an.

Nur über VPN

Das Gerät nimmt nur neue APs an, wenn die WAN-Verbindung über VPN erfolgt.

Ja

Das Gerät nimmt alle neuen APs über die WAN-Verbindung an.

14.3 Grundkonfiguration der WLAN-Controller-Funktion

Für den Start benötigt ein WLC zur weitestgehend automatisierten Konfiguration der APs die beiden folgenden Informationen:

- Eine aktuelle Zeitinformation (Datum und Uhrzeit), damit die Gültigkeit der benötigten Zertifikate sichergestellt werden kann.
- Ein WLAN-Profil, welches der WLC den APs zuweisen kann.

Weiterführende, optionale Konfigurationsbeispiele schließen das Einrichten von redundanten WLCs, das manuelle Trennen und Verbinden von APs sowie das Durchführen eines Backups der notwendigen Zertifikate ein.

Standardmäßig wartet der WLC auf dem UDP-Port 1027 (konfigurierbar) auf Verbindungen. Die Verteilung der Zertifikate erfolgt über SCEP, welches den TCP-Port 80 (HTTP) nutzt.

14.3.1 Zeitinformation für den WLAN-Controller einstellen

Die Verwaltung von APs in einer WLAN-Infrastruktur basiert auf der automatischen Verteilung von Zertifikaten über Simple Certificate Enrollment Protocol (SCEP).

Der WLC kann die Gültigkeit dieser zeitlich beschränkten Zertifikate nur dann prüfen, wenn er über eine aktuelle Zeitinformation verfügt. Solange der WLC nicht über eine aktuelle Zeitinformation verfügt, leuchtet die WLAN-LED dauerhaft rot, das Gerät ist nicht betriebsbereit.

Router mit WLC-Option verfügen über keine WLAN-LED.

Um dem Gerät eine Zeit zuzuweisen, klicken Sie in LANconfig mit der rechten Maustaste auf den Eintrag für den WLC und wählen im Kontext-Menü den Eintrag **Datum/Zeit setzen**. Alternativ klicken Sie in WEBconfig im Bereich **Extras** den Link **Datum und Uhrzeit einstellen**.

Die WLCs können die aktuelle Zeit alternativ auch automatisch über das Network Time Protocol (NTP) von einem Zeit-Server beziehen. Informationen über NTP und die entsprechende Konfiguration finden Sie im LCOS-Referenzhandbuch.

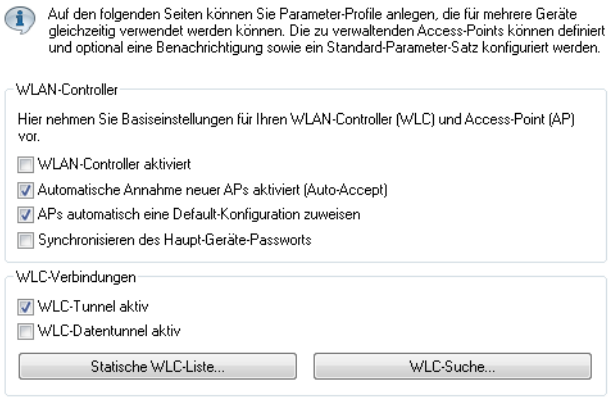
Sobald der WLC über eine gültige Zeitinformation verfügt, beginnt die Erstellung der Zertifikate (Root- und Geräte-Zertifikat). Wenn die Zertifikate erfolgreich erzeugt wurden, meldet der WLC Betriebsbereitschaft, die WLAN-LED blinkt dann rot.

Nach Herstellung der Betriebsbereitschaft sollten Sie eine Sicherung der Zertifikate anlegen (*Sicherung der Zertifikate*)

14.3.2 Beispiel einer Default-Konfiguration

1. Öffnen Sie die Konfiguration des WLCs durch einen Doppelklick auf den entsprechenden Eintrag in LANconfig.

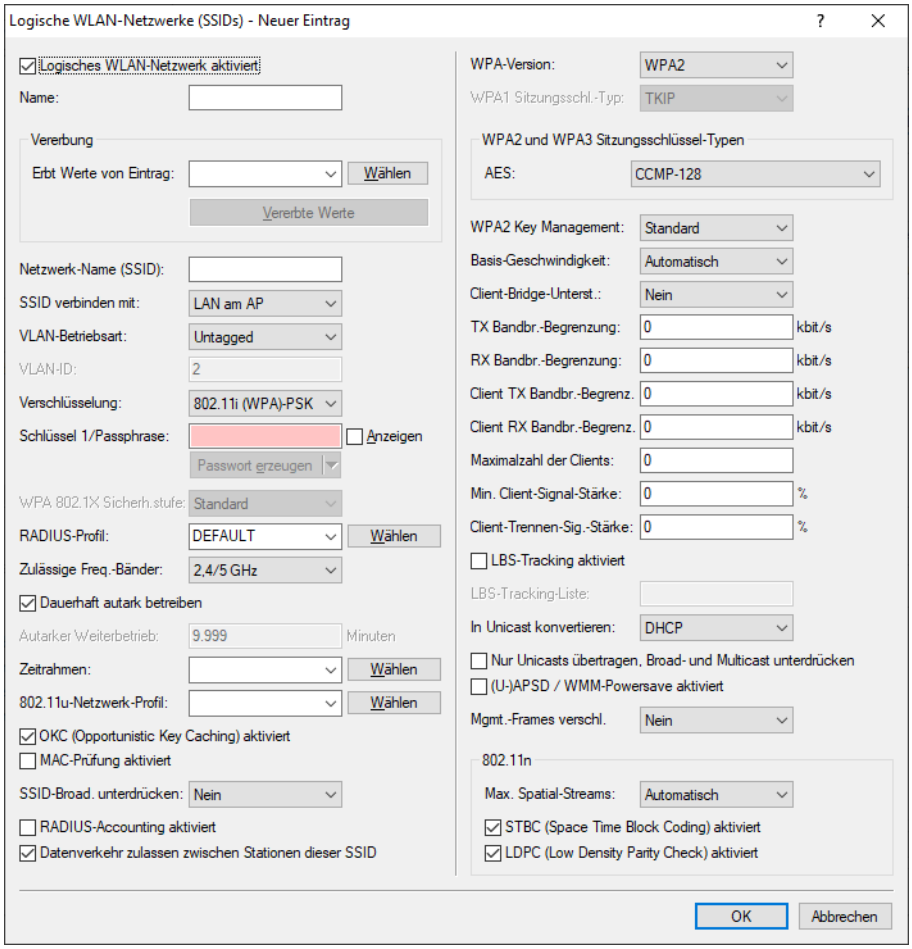
2. Aktivieren Sie unter **WLAN-Controller** > **Allgemein** die Optionen für die automatische Annahme neuer APs sowie die Zuweisung einer Default-Konfiguration.



- **Automatische Annahme neuer APs aktiviert (Auto-Accept)**: Ermöglicht dem WLC, allen neuen APs ohne gültiges Zertifikat ein solches Zertifikat zuzuweisen. Dazu muss entweder für den AP eine Konfiguration in der AP-Tabelle eingetragen sein oder die Automatische Zuweisung der Default-Konfiguration ist aktiviert.
- **APs automatisch eine Default-Konfiguration zuweisen** : Ermöglicht dem WLC, allen neuen APs eine Default-Konfiguration zuzuweisen, auch wenn für diese keine explizite Konfiguration hinterlegt wurde.

Durch die Kombination dieser beiden Optionen kann der WLC alle im LAN gefundenen APs im Managed-Modus automatisch in die von ihm verwaltete WLAN-Struktur aufnehmen, z. B. temporär während der Rollout-Phase einer WLAN-Installation.

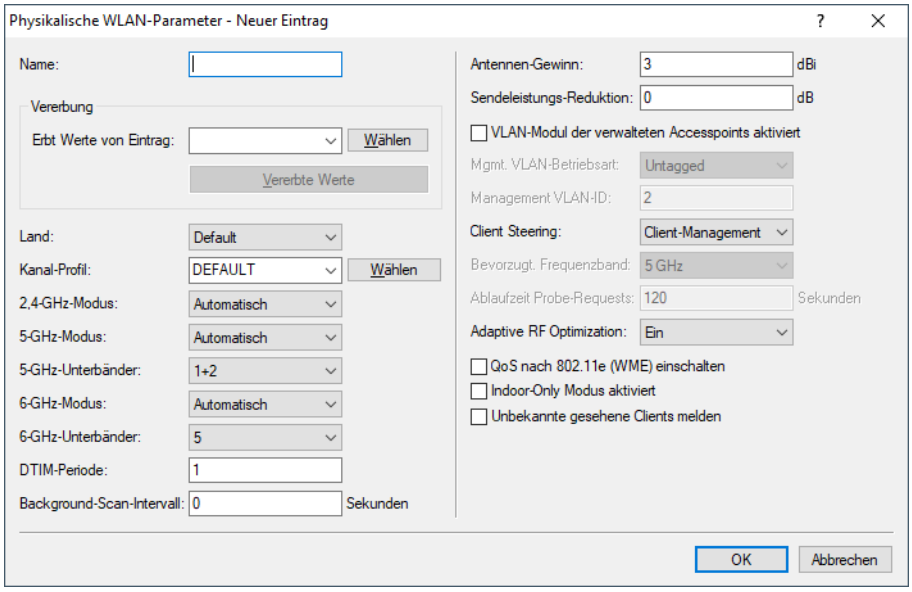
3. Wechseln Sie in der Ansicht **Profile** in die logischen WLAN-Netzwerke. Erstellen Sie einen neuen Eintrag mit folgenden Werten:



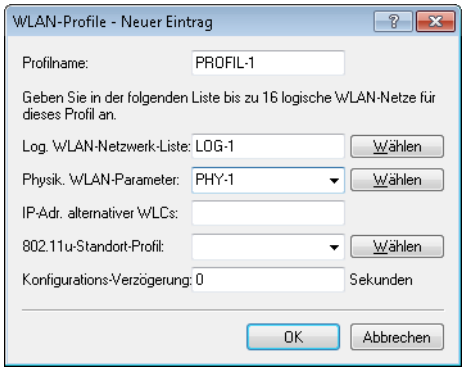
- **Netzwerkname**: Geben Sie dem WLAN einen Namen. Dieser Name wird nur für die Verwaltung im WLC verwendet.
- **SSID**: Mit dieser SSID verbinden sich die WLAN-Clients.
- **Verschlüsselung**: Wählen Sie die Verschlüsselung passend zu den Möglichkeiten der verwendeten WLAN-Clients und geben Sie ggf. einen Schlüssel bzw. eine Passphrase ein.
- Deaktivieren Sie die MAC-Prüfung. Hinweise zur Nutzung der MAC- Filterlisten in gemanagten WLAN-Strukturen finden Sie unter *Prüfung der WLAN-Clients über RADIUS (MAC-Filter)*.

4. Erstellen Sie auch bei den physikalischen WLAN-Parametern einen neuen Eintrag. Für die Default-Konfiguration reicht hier in vielen Fällen nur die Angabe eines Namens. Die restlichen Einstellungen können bei Bedarf angepasst werden.

In normalen AP-Anwendungen sollten Sie nur die 5-GHz-Unterbänder 1 und 2 verwenden. Das Unterband 3 steht nur für besondere Anwendungen zur Verfügung (z. B. BFWA – Broadband Fixed Wireless Access).

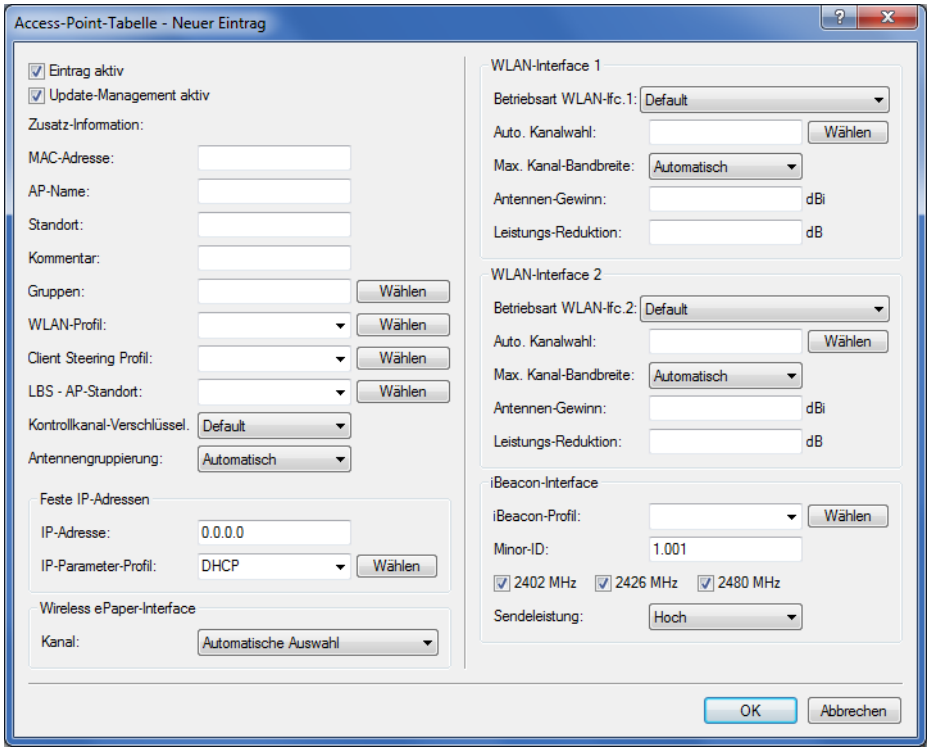


5. Erstellen Sie ein neues WLAN-Profil, geben Sie ihm einen eindeutigen Namen und weisen Sie ihm das eben erstellte logische WLAN-Netzwerk sowie die physikalischen WLAN-Parameter zu.



6. Wechseln Sie auf in Ansicht **AP-Konfiguration**, öffnen Sie die **Access-Point-Tabelle** und erstellen Sie einen neuen Eintrag mit einem Klick auf die Schaltfläche **Default**. Weisen Sie dabei dem Eintrag das eben erstellte WLAN-Profil zu, **AP-Name** und **Standort** sollten frei bleiben.

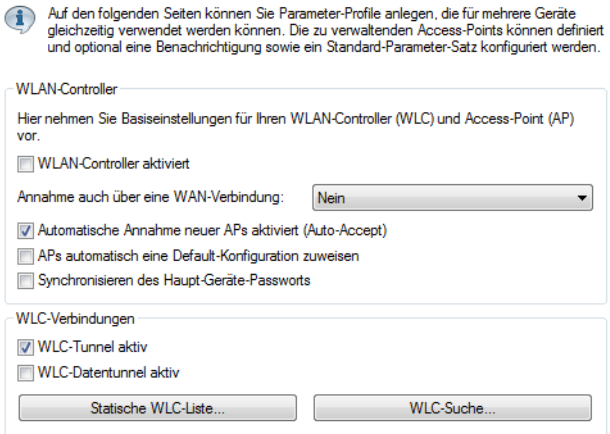
Die **MAC-Adresse** wird für die Default-Konfiguration auf 'ffffffffffff' gesetzt und ist nicht editierbar. Damit gilt dieser Eintrag als Standard für alle APs, die nicht mit ihrer MAC-Adresse explizit in dieser Tabelle eingetragen sind.



14.3.3 Zuweisung der Default-Konfiguration zu den neuen Access Points

Mit diesen Einstellungen haben Sie alle erforderlichen Werte definiert, damit der WLC den APs die erforderlichen WLAN-Parameter zuweisen kann. Mit dieser Konfigurations-Zuweisung ändern die APs in der Verwaltung des WLCs ihren Status von "Neuer Access Point" auf "Erwarteter Access Point", die im Display des Gerätes unter **Exp. APs** aufgeführt werden. Sobald allen neuen APs die Default-Konfiguration zugewiesen wurde, erlischt die New-APs-LED.

Nach der ersten Startphase kann die Option **Automatische Annahme neuer APs** wieder deaktiviert werden, damit keine weiteren APs automatisch in das Netzwerk aufgenommen werden.



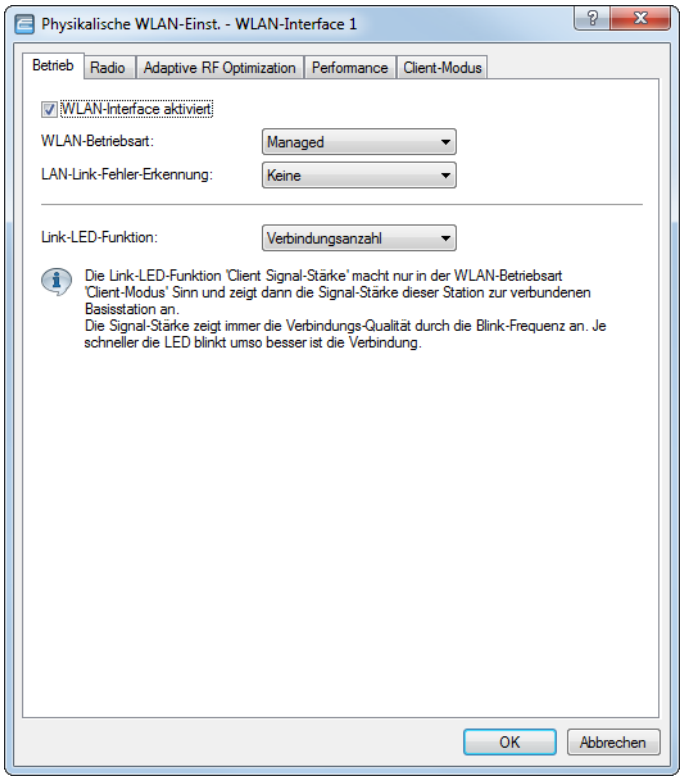
14.3.4 Konfiguration der Access Points

LANCOM Access Points und LANCOM Wireless Router unterscheiden sich bzgl. der Einstellung der WLAN-Module im Auslieferungszustand.

- Bei APs sind im Auslieferungszustand die WLAN-Module auf die Betriebsart 'Managed' eingestellt. In diesem Modus suchen die APs nach einem zentralen WLC, der ihnen eine Konfiguration zuweisen kann, und bleiben so lange im "Such-Modus", bis sie einen passenden WLC gefunden haben oder die Betriebsart für die WLAN-Module manuell geändert wird.
- Bei Wireless Routern sind im Auslieferungszustand die WLAN-Module auf die Betriebsart 'Access-Point' eingestellt. In diesem Modus arbeiten die Wireless Router als autarke APs mit einer im Gerät lokal gespeicherten Konfiguration. Um Teilnehmer einer zentral über WLC verwalteten WLAN-Struktur zu werden, muss die Betriebsart für die WLAN-Module in den gewünschten Wireless Routern auf 'Managed' umgestellt werden.

Die Betriebsart kann für jedes WLAN-Modul separat eingestellt werden. Bei Modellen mit zwei WLAN-Modulen kann so ein Modul mit einer lokalen Konfiguration arbeiten, das zweite kann zentral über den WLC verwaltet werden.

Für einzelne Geräte finden Sie die Betriebsart der WLAN-Module in LANconfig über **Wireless LAN** > **Allgemein** > **Physikalische WLAN-Einstellungen** > **Betrieb**:



Wenn Sie die Betriebsart für mehrere Geräte gleichzeitig umstellen möchten, können Sie auf die Geräte ein einfaches Script anwenden mit folgenden Zeilen:

```
# Script
lang English
flash 0
cd Setup/Interfaces/WLAN/Operational
set WLAN-1 0 managed-AP 0
# done
exit
```

14.4 Konfiguration

Die meisten Parameter zur Konfiguration der WLAN-Controller entsprechen denen der Access Points. In diesem Abschnitt werden daher nicht alle WLAN-Parameter explizit beschrieben sondern nur die für den Betrieb der WLAN-Controller erforderlichen Aspekte.

14.4.1 Allgemeine Einstellungen

In diesem Bereich nehmen Sie die Basiseinstellungen für Ihren WLC vor.

- Automatische Annahme neuer APs (Auto-Accept)

  Ermöglicht dem WLC, allen neuen APs eine Konfiguration zuzuweisen, auch wenn diese nicht über ein gültiges Zertifikat verfügen.

  Ermöglicht dem WLC, allen neuen APs **ohne** gültiges Zertifikat ein solches Zertifikat zuzuweisen. Dazu muss eine der beiden Bedingungen erfüllt sein:

  - Für den AP ist unter seiner MAC-Adresse eine Konfiguration in der AP-Tabelle eingetragen.
  - Die Option 'Automatische Zuweisung der Default-Konfiguration' ist aktiviert.

- Automatische Zuweisung der Default-Konfiguration

  Ermöglicht dem WLC, allen neuen APs (also **ohne** gültiges Zertifikat) eine Default-Konfiguration zuzuweisen, auch wenn für diese keine explizite Konfiguration hinterlegt wurde. Im Zusammenspiel mit dem Auto-Accept kann der WLC alle im LAN gefundenen APs im Managed-Modus automatisch in die von ihm verwaltete WLAN-Struktur aufnehmen (bis zur maximalen Anzahl der auf einem WLC verwalteten APs). Per Default aufgenommene APs werden auch in die MAC-Liste aufgenommen.

  Mit dieser Option können möglicherweise auch unbeabsichtigte APs in die WLAN-Struktur aufgenommen werden. Daher sollte diese Option nur während der Startphase bei der Einrichtung einer zentral verwalteten WLAN-Struktur aktiviert werden.

Mit der Kombination der Einstellungen für Auto-Accept und Default-Konfiguration können Sie verschiedene Situationen für die Einrichtung und den Betrieb der APs abdecken:

Auto-Accept	Default-Konfiguration	Geeignet für
Ein	Ein	Rollout-Phase: Verwenden Sie diese Kombination nur dann, wenn **keine APs unkontrolliert** mit dem LAN verbunden werden können und so unbeabsichtigt in die WLAN-Struktur aufgenommen werden.
Ein	Aus	Kontrollierte Rollout-Phase: Verwenden Sie diese Kombination, wenn Sie alle erlaubten APs mit ihrer MAC-Adresse in die AP-Tabelle eingetragen haben und diese automatisch in die WLAN-Struktur aufgenommen werden sollen.
Aus	Aus	Normalbetrieb: Es werden keine neuen APs ohne Zustimmung der Administratoren in die WLAN-Struktur aufgenommen.

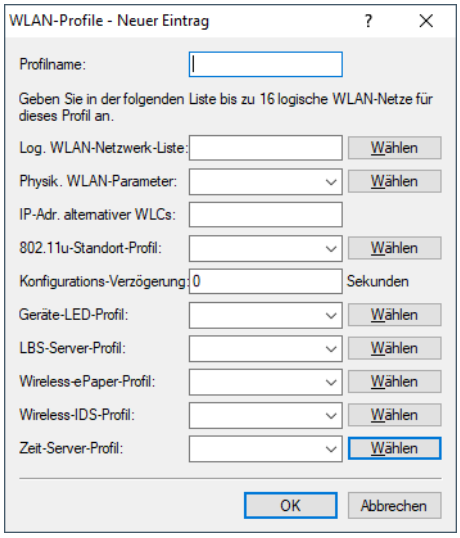
14.4.2 Profile

Im Bereich der Profile definieren Sie die logischen WLAN-Netzwerke, die physikalischen WLAN-Parameter sowie die WLAN-Profile, die eine Kombination aus den beiden vorgenannten Elementen darstellen.

14.4.2.1 WLAN-Profile

In den WLAN-Profilen werden die Einstellungen zusammengefasst, die den APs zugewiesen werden. Die Zuordnung der WLAN-Profile zu den Access Points erfolgt in der Access Point-Tabelle.

Für jedes WLAN-Profil können Sie unter **WLAN-Controller** > **Profile** > **WLAN-Profile** die folgenden Parameter definieren:



Profil-Name

Name des Profils, unter dem die Einstellungen gespeichert werden.

Log. WLAN-Netzwerk-Liste

Liste der logischen WLAN-Netzwerke, die über dieses Profil zugewiesen werden.

Die APs nutzen aus dieser Liste nur die ersten 16 Einträge, die mit der eigenen Hardware kompatibel sind. Somit können in einem Profil z. B. jeweils 16 WLAN-Netzwerke für reinen 2,4 GHz-Betrieb und 16 für reinen 5 GHz-Betrieb definiert werden. Für jeden AP – sowohl Modelle mit 2,4 GHz- als auch die mit 5 GHz-Unterstützung – stehen damit die maximal möglichen 16 logischen WLAN-Netzwerke zur Verfügung.

Physik. WLAN-Parameter

Ein Satz von physikalischen Parametern, mit denen die WLAN-Module der APs arbeiten sollen.

IP-Adr. alternativer WLCs

Liste der WLCs, bei denen der AP eine Verbindung versuchen soll. Der AP leitet die Suche nach einem WLC über einen Broadcast ein. Wenn nicht alle WLCs über einen solchen Broadcast erreicht werden können (WLC steht z. B. in einem anderen Netz), dann ist die Angabe von alternativen WLCs sinnvoll.

802.11u-Standort-Profil

Wählen Sie aus der Liste ein Hotspot-2.0-Profil aus. Hotspot-2.0-Profile legen Sie im Konfigurationsmenü über die gleichnamige Schaltfläche an.

Konfigurations-Verzögerung

Geben Sie hier die Verzögerung an, nach der ein vom WLAN-Controller gemanagter AP die übertragene Konfiguration übernimmt.

Dies ist insbesondere in AutoWDS-Szenarien sinnvoll, in denen mehrere gemanagte APs über Punkt-zu-Punkt-Strecken hintereinander verbunden sind. Durch eine vorzeitige Konfigurations-Änderung auf einem AP, welcher die Verbindung zu einem entfernteren AP herstellt, könnte sonst die Verbindung zu dem entfernteren AP abgeschnitten werden.

Eine grobe Regel für die Berechnung der Verzögerung ist (unabhängig von der Topologie): Eine Sekunde pro gemanagtem AP, also z. B. 200 Sekunden bei 200 APs.

Die Verzögerung gilt nicht für übertragene Skripte.

Geräte-LED-Profil

Wählen Sie aus der Liste der Geräte-LED-Profile das Profil aus, das im WLAN-Profil gelten soll. Die Geräte-LED-Profile verwalten Sie unter **WLAN-Controller** > **Profile** > **Geräte-LED-Profile**.

LBS-Allgemein-Profil

Wählen Sie hier aus der Liste der allgemeinen LBS-Profile das Profil aus, das im WLAN-Profil gelten soll. Die allgemeinen LBS-Profile verwalten Sie unter **WLAN-Controller** > **Profile** > **Erweiterte Profile** mit der Schaltfläche **LBS - Allgemein**.

Wireless-ePaper-Profil

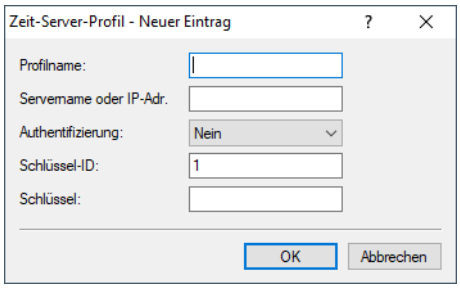
Wählen Sie hier aus der Liste der Wireless-ePaper-Profile das Profil aus, das im WLAN-Profil gelten soll. Die Wireless-ePaper-Profile verwalten Sie unter **WLAN-Controller** > **Profile** > **Erweiterte Profile** mit der Schaltfläche **Wireless-ePaper-Profile**.

Wireless-IDS-Profil

Wählen Sie hier aus der Liste der Wireless-IDS-Profile das Profil aus, das im WLAN-Profil gelten soll. Die Wireless-IDS-Profile verwalten Sie unter **WLAN-Controller** > **Profile** > **Erweiterte Profile** mit der Schaltfläche **Wireless-IDS-Profile**.

Zeit-Server-Profil

Wählen Sie hier aus der Liste der Zeit-Server-Profile das Profil aus, das im WLAN-Profil gelten soll. Die Zeit-Server-Profile verwalten Sie unter **WLAN-Controller** > **Profile** > **Erweiterte Profile** mit der Schaltfläche **Zeit-Server-Profil**.



Profilname

Der Name dieses NTP-Profils.

Servername oder IP-Adresse

Der Servername oder die IP-Adresse des NTP-Servers.

Authentifizierung

Aktiviert bzw. deaktiviert die MD5-Authentifizierung für den Server.

Schlüssel-ID

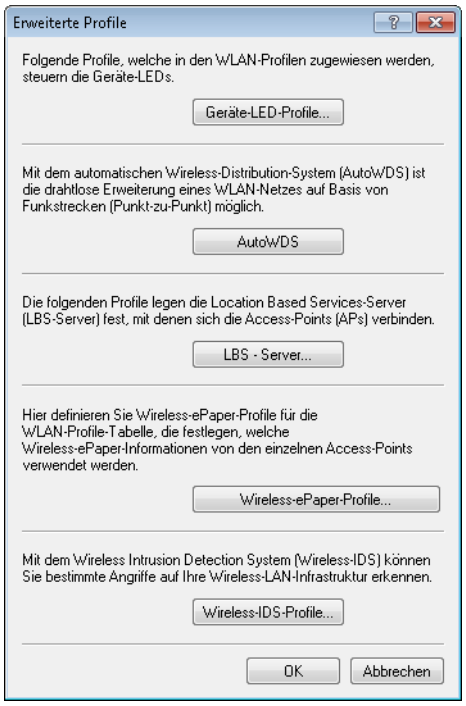
Kennzeichnet den zur MD5-Authentifizierung verwendeten Schlüssel für den Server.

Schlüssel

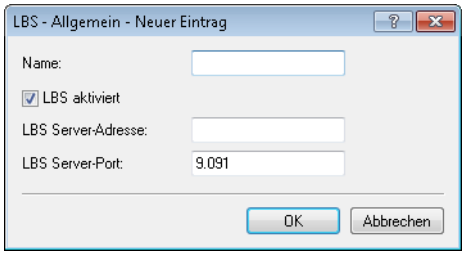
Der Wert des Schlüssels für die Authentifizierung mit dem NTP-Server.

14.4.2.2 Allgemeines LBS-Profil und Gerätestandort-Profil

Um die Einstellungen von Location Based Services-Servern (LBS-Servern) und AP-Standorten komfortabel über einen WLC zu verwalten, erstellen Sie über **WLAN-Controller** > **Profile** mit der Schaltfläche **Erweiterte Profile** das entsprechende Profil für den LBS-Server.



Mit der Schaltfläche **LBS – Server** erstellen Sie ein allgemeines LBS-Server-Profil.



Name

Vergeben Sie einen aussagekräftigen Namen für das Profil.

LBS aktiviert

Aktivieren oder deaktivieren Sie LBS.

LBS Server-Adresse

Geben Sie hier die Adresse des LBS-Servers ein.

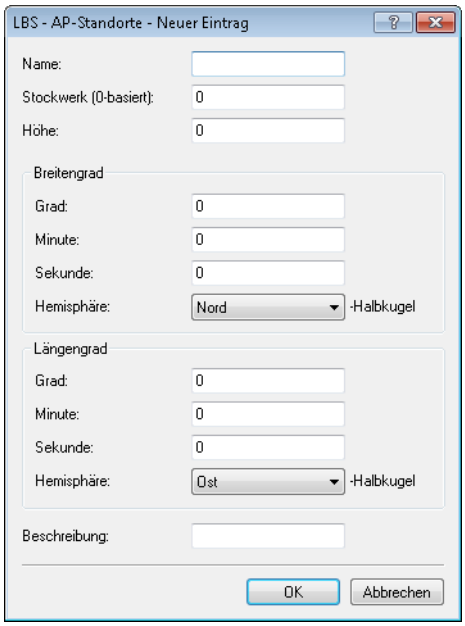
LBS Server-Port

Geben Sie hier den Port des LBS-Servers ein (Default: 9091).

Sie erstellen das entsprechende Profil für Standorte der LBS APs über **WLAN-Controller** > **AP-Konfiguration** mit der Schaltfläche **Erweiterte Einstellungen**.



Mit der Schaltfläche **LBS-AP-Standorte** erstellen Sie ein Standort-Profil der LBS-APs.



Name

Vergeben Sie einen aussagekräftigen Namen für das Profil.

Stockwerk (0-basiert)

Geben Sie hier die Etage ein, auf der sich das Gerät befindet. So differenzieren Sie z. B. zwischen Ober- und Untergeschoss.

Höhe

Geben Sie hier die Höhe ein, auf der sich das Gerät befindet. Die Angabe eines negativen Wertes ist möglich, so dass Sie zwischen einer Position über und unter dem Meeresspiegel differenzieren können.

Grad (Breitengrad)

Dieses Feld gibt den Winkel in Grad des geographischen Koordinatensystems an.

Minute (Breitengrad)

Dieses Feld gibt die Minute des geographischen Koordinatensystems an.

Sekunde (Breitengrad)

Dieses Feld gibt die Sekunde des geographischen Koordinatensystems an.

Hemisphäre (Breitengrad)

Dieses Feld gibt die Orientierung des geographischen Koordinatensystems an. Für die geographische Breite (Latitude) sind folgende Werte möglich:

- Nord: nördliche Breite
- Süd: südliche Breite

Grad (Längengrad)

Dieses Feld gibt den Winkel in Grad des geographischen Koordinatensystems an.

Minute (Längengrad)

Dieses Feld gibt die Minute des geographischen Koordinatensystems an.

Sekunde (Längengrad)

Dieses Feld gibt die Sekunde des geographischen Koordinatensystems an.

Hemisphäre (Längengrad)

Dieses Feld gibt die Orientierung des geographischen Koordinatensystems an. Für die geographische Länge (Longitude) sind folgende Werte möglich:

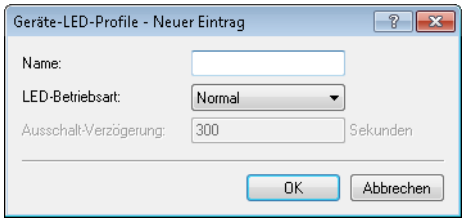
- Ost: östliche Länge
- West: westliche Länge

Beschreibung

Geben Sie hier eine Beschreibung des Gerätes ein.

14.4.2.3 Geräte-LED-Profile

Die Geräte-LEDs lassen sich am Gerät konfigurieren, um den AP unauffällig betreiben zu können. Um diese Konfiguration auch über einen WLC durchzuführen, erstellen Sie unter **WLAN-Controller** > **Profile** > **Erweiterte Profile** > **Geräte-LED-Profile** entsprechende Profile, die Sie anschließend einem WLAN-Profil zuordnen.



Name

Vergeben Sie hier einen Namen für das Geräte-LED-Profil.

LED-Betriebsart

Die folgenden Optionen stehen zur Auswahl:

- **Normal**: Die LEDs sind immer aktiviert, auch nach einem Neustart des Gerätes.
- **Verzögert aus**: Nach einem Neustart sind die LEDs für einen bestimmten Zeitraum aktiviert, danach schalten sie sich aus. Das ist dann hilfreich, wenn die LEDs während des Neustartes auf kritische Fehler hinweisen.
- **Alle aus**: Die LEDs sind alle deaktiviert. Auch nach einem Neustart des Gerätes bleiben die LEDs deaktiviert.

Ausschalt-Verzögerung

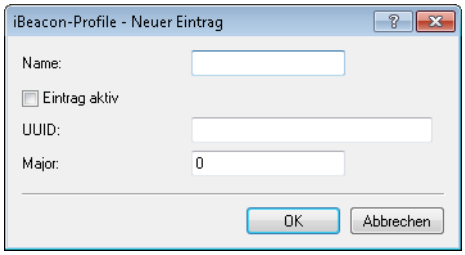
In der Betriebsart **Verzögert aus** können Sie im Feld **LED-Ausschalt-Verzögerung** die Dauer in Sekunden festlegen, nach der das Gerät die LEDs bei einem Neustart deaktivieren soll.

14.4.2.4 ESL- und iBeacon-Profile

Um die Einstellungen von Wireless-ePaper-Informationen und iBeacon-Informationen der einzelnen APs komfortabel über einen WLC zu verwalten, erstellen Sie über **WLAN-Controller** > **AP-Konfiguration** mit der Schaltfläche **Erweiterte Einstellungen** die entsprechenden Profile für Wireless-ePapaper und iBeacon.



Mit der Schaltfläche **iBeacon-Profile** erstellen Sie iBeacon-Profile für die Zuweisungsgruppen und die AP-Tabelle, die festlegen, welche iBeacon-Informationen die einzelnen APs ausstrahlen.



Name

Name des Profils

Eintrag aktiv

Aktiviert oder deaktiviert dieses Profil.

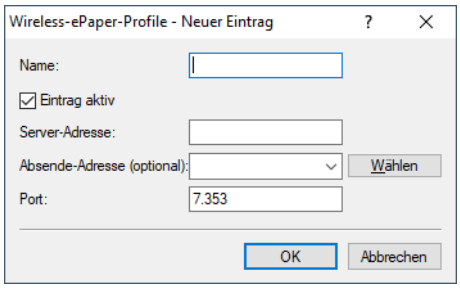
UUID

Eindeutige Kennzeichnung des Senders

Major

Gibt den Major-Wert des iBeacons an.

Mit der Schaltfläche **Wireless-ePaper-Profile** erstellen Sie Wireless-ePaper-Profile für die WLAN-Profile-Tabelle, die festlegen, welche Wireless-ePaper-Informationen die einzelnen APs ausstrahlen.



Name

Name des Profils

Eintrag aktiv

Aktiviert oder deaktiviert dieses Profil.

Server-Adresse

IP-Adresse des Wireless ePaper Servers.

Absende-Adresse (optional)

Geben Sie hier die Loopback-Adresse an.

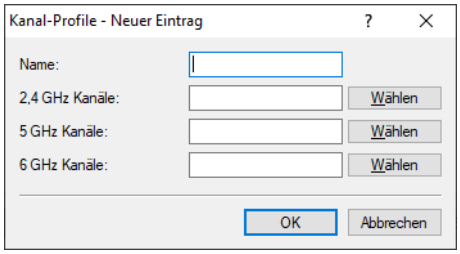
Port

Gibt den Port an.

14.4.2.5 Kanal-Profil-Tabelle

Die Konfiguration der WLAN-Kanäle erstellen Sie unter **WLAN-Controller** > **Profile** > **Erweiterte Profile** > **Kanal-Profile**. Innerhalb des Kanal-Profils können die WLAN-Kanäle je Frequenzband festgelegt werden. Auf diese Weise lassen sich auch Kanäle eindeutig definieren, deren Nummerierung sich in verschiedenen Frequenzbändern wiederholt (z. B. bei 2,4 GHz und 6 GHz). Verknüpfen Sie neu erzeugte Kanalprofile anschließend innerhalb des physikalischen WLAN-Profils.

Das DEFAULT-Profil aktiviert alle erlaubten Kanäle.



Name

Name des Profils.

2,4 GHz Kanäle

Wählen Sie die 2,4 GHz-Kanäle für dieses Profil aus.

5 GHz Kanäle

Wählen Sie die 5 GHz-Kanäle für dieses Profil aus.

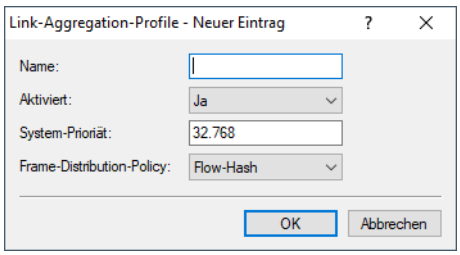
6 GHz Kanäle

Wählen Sie die 6 GHz-Kanäle für dieses Profil aus.

14.4.2.6 Link-Aggregation-Profile

LACP nach IEEE 802.1AX erlaubt es, mehrere Ethernet-Verbindungen in einer sogenannten LAG (Link Aggregation Group) zu bündeln, um innerhalb der LAG den erreichbaren Datendurchsatz zu erhöhen. Hierzu werden auf der sendenden Seite die ausgehenden Pakete anhand der konfigurierten Frame-Distribution-Policy auf die verschiedenen einzel-Links innerhalb der LAG verteilt.

Die Konfiguration der Link-Aggregation-Profile erstellen Sie unter **WLAN-Controller** > **Profile** > **Erweiterte Profile** > **Link-Aggregation-Profile**.



Name

Der Name dieser LAG (Link Aggregation Group).

Aktiviert

Aktiviert bzw. deaktiviert diese LAG (Link Aggregation Group).

System-Priorität

Die Systempriorität dieser LAG (Link Aggregation Group).

Frame-Distribution-Policy

Frame-Distribution-Policy dieser LAG (Link Aggregation Group).Mögliche Optionen:

Flow-Hash

Für ausgehende Pakete wird ein Flow-Hash über die enthaltenen IP-Adressen und TCP/UDP-Ports gebildet und anhand dessen die Pakete auf die einzelnen Links der LAG verteilt. Hiermit erreicht man eine Verteilung auf Session-Ebene, so dass auch Sessions eines einzelnen Clients auf mehrere Links verteilt werden können. Diese Einstellung wird für die meisten Szenarien empfohlen.

Quell-Ziel-MAC

Ausgehende Pakete werden anhand des enthaltenen Paares aus Quell-MAC-Adresse und Ziel-MAC-Adresse auf die einzelnen Links der LAG verteilt.

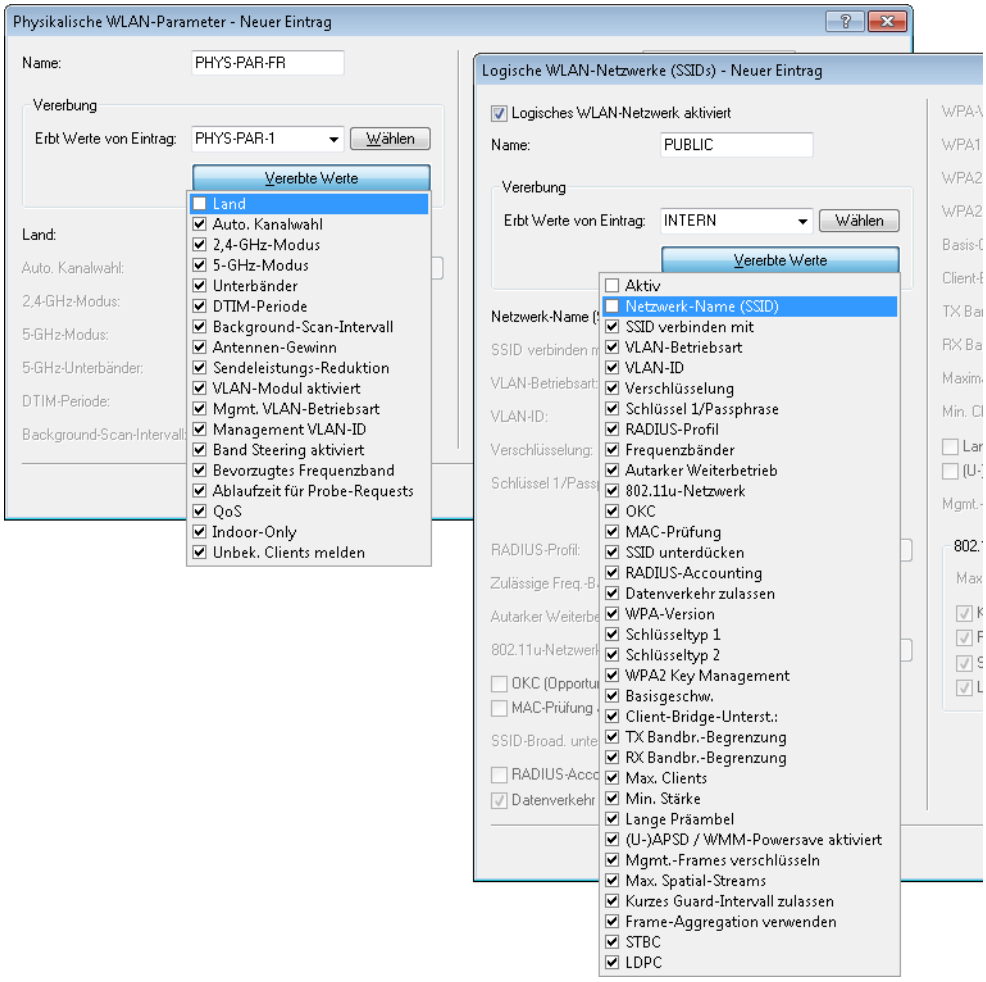
14.4.2.7 Vererbung von Parametern

Mit einem WLC können sehr viele unterschiedliche APs an verschiedenen Standorten verwaltet werden. Nicht alle Einstellungen in einem WLAN-Profil eignen sich dabei für jeden der verwalteten APs gleichermaßen. Unterschiede gibt es z. B. in den Ländereinstellungen oder bei den Geräteeigenschaften.

Damit auch in komplexen Anwendungen die WLAN-Parameter nicht in mehreren Profilen redundant je nach Land oder Gerätetyp gepflegt werden müssen, können die logischen WLAN-Netzwerke und die physikalischen WLAN-Parameter ausgewählte Eigenschaften von anderen Einträgen "erben".

1. Erstellen Sie dazu zunächst die grundlegenden Einstellungen, die für die meisten verwalteten APs gültig sind.

2. Erzeugen Sie danach Einträge für die spezifischeren Werte, z. B. physikalische Einstellungen für ein bestimmtes Land oder ein logisches WLAN-Netzwerk für den öffentlichen Zugang von mobilen Clients.



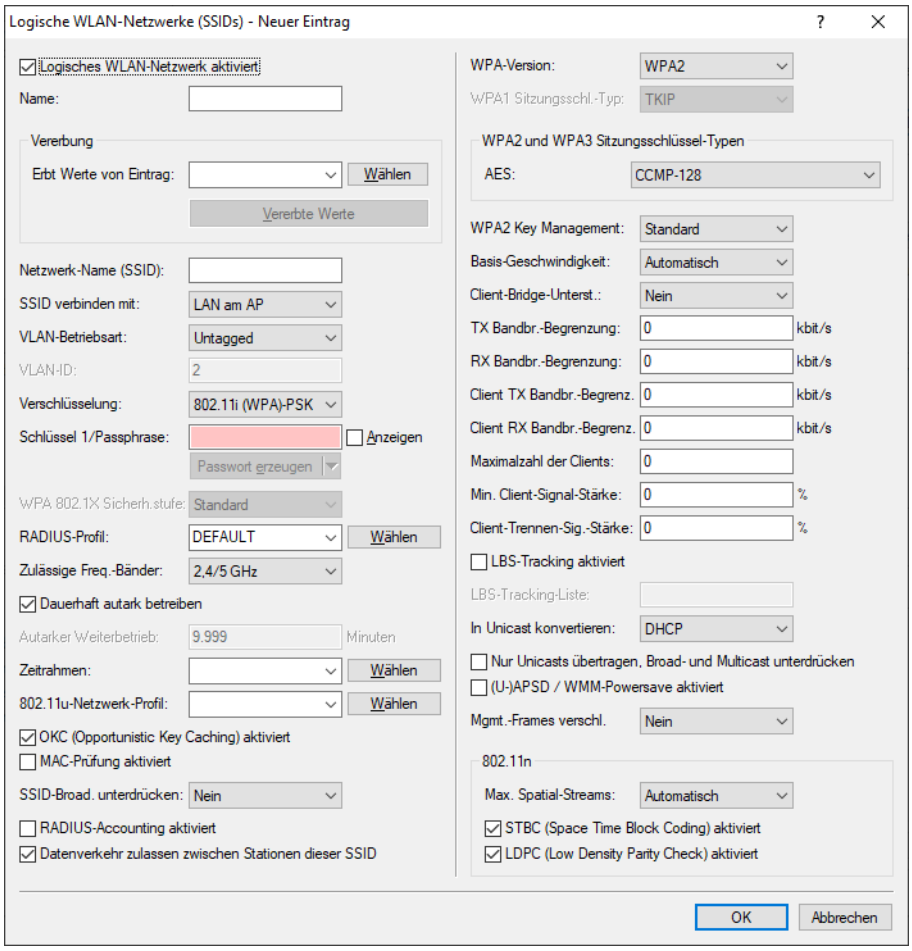
3. Wählen Sie aus, von welchem Eintrag Werte geerbt werden sollen und markieren Sie die vererbten Werte. Die so übernommenen Parameter werden im Konfigurationsdialog grau dargestellt und können nicht verändert werden.
4. Die so zusammengestellten WLAN-Einstellungen werden dann je nach Verwendung zu separaten Profilen zusammengefasst, die wiederum gezielt den jeweiligen Access Points zugewiesen werden.

Bei der Vererbung sind grundsätzlich Ketten über mehrere Stufen (Kaskadierung) möglich. So können z. B. länder- und gerätespezifische Parameter komfortabel zusammengestellt werden.

Auch Rekursionen sind möglich – Profil A erbt von Profil B, gleichzeitig erbt B aber auch von A. Die verfügbaren Parameter für die Vererbung beschränken sich dabei aber auf eine "Vererbungsrichtung" pro Parameter.

14.4.2.8 Logische WLAN-Netzwerke

Unter **WLAN-Controller** > **Profile** > **Logische WLAN-Netzwerke** können Sie die Parameter für die logischen WLAN-Netzwerke einstellen, die der WLC den APs zuweisen soll. Für jedes logische WLAN-Netzwerk können Sie die folgenden Parameter definieren:



Logisches WLAN-Netzwerk aktiviert

Aktivieren Sie das logische WLAN-Netzwerk, indem Sie diese Option anklicken.

Name

Geben Sie hier einen Namen an, der das logische WLAN-Netzwerk eindeutig kennzeichnet.

Vererbung

Möchten Sie Einträge erzeugen, die sich nur in wenigen Werten von vorhandenen Einträgen unterscheiden, können Sie einen "Eltern"-Eintrag sowie die zu übernehmenden Einträge hier gezielt auswählen.

Auch ein "Eltern"-Eintrag kann selber geerbte Einträge enthalten. Achten Sie darauf, dass die Konstruktionen für geerbte Einträge nicht zu komplex und damit schwer nachvollziehbar und konfigurierbar sind.

Netzwerk-Name (SSID)

Geben Sie hier die SSID des WLAN-Netzwerkes an. Alle Stationen, die zu diesem WLAN-Netz gehören, müssen dieselbe SSID verwenden.

SSID verbinden mit

Wählen Sie hier aus, mit welcher logischen Schnittstelle des APs die SSID verknüpft sein soll bzw. wohin der AP Datenpakete dieser SSID leiten soll.

- „LAN“: Der AP lädt die Datenpakete standardmäßig lokal ins LAN weiter (LAN-1). Dazu muss er entsprechend konfiguriert sein.
- „WLC-Tunnel-x“: Die SSID ist mit einem WLC-Bridge-Layer-3-Tunnel verbunden. Der AP liefert alle Datenpakete in diesen Tunnel und damit zum WLC. Dieser Tunnel muss auf dem WLC konfiguriert sein.
- „L2TP-ETHERNET-x“: Die SSID ist mit einem L2TPv3-Ethernet-Tunnel verbunden. Dies ermöglicht ein automatisches Auskoppeln von WLAN-SSIDs in L2TP-Ethernet-Tunnel. Allgemeine Informationen zum Thema L2TPv3 finden Sie im Abschnitt *Layer 2 Tunneling Protocol (L2TP)* auf Seite 838. Die Verwendung von L2TPv3-Tunneln als Alternative zum klassischen WLC-Layer-3-Tunnel empfiehlt sich, wenn der WLAN-Durchsatz durch diesen begrenzt wird, da mittels L2TPv3 ein höherer Maximaldurchsatz erzielt werden kann. Passen Sie anschließend noch die Verwendung der gewählten L2TP-ETHERNET-x-Schnittstelle auf dem WLC an, z. B. zur weiteren Verwendung im IP-Router oder in der LAN-Bridge.

  Sowohl der WLC als auch die verwalteten Access Points müssen LCOS 10.50 oder höher unterstützen.

Beachten Sie, dass Sie bei Weiterleitung aller Datenpakete zum WLC zwar zentrale Routen und Filter definieren können, dieses jedoch eine hohe Last auf dem WLC erzeugt. Dafür müssen dort entsprechend hohe Bandbreiten zur Verfügung stehen, um den gesamten Datenverkehr dieser und ggf. weiterer über WLC-Tunnel mit diesem WLC verbundenen SSIDs übertragen zu können.

VLAN-Betriebsart

Stellen Sie hier die VLAN-Betriebsart des APs für Pakete dieses WLAN-Netzwerkes (SSID) ein. Die Verwendung von VLAN-IDs ist abhängig davon, ob das VLAN-Modul in den physikalischen WLAN-Parametern des APs aktiviert ist. Ansonsten ignoriert der AP alle VLAN-Einstellungen in den logischen Netzwerken. Es ist möglich, das Netzwerk trotz aktiviertem VLAN auch ungetagged zu betreiben:

- „Untagged“: Der AP markiert Datenpakete dieser SSID nicht mit einer VLAN-ID.

  Es ist möglich ein WLAN-Netzwerk trotz aktiviertem VLAN auch ungetagged zu betreiben. Intern ist dafür die VLAN-ID "1" reserviert.
- „Tagged“: Der AP markiert die Datenpakete mit der nachfolgend bestimmten VLAN-ID.

VLAN-ID

VLAN-ID für dieses logische WLAN-Netzwerk.

Bitte beachten Sie, dass für die Nutzung der VLAN-IDs in einem logischen WLAN-Netzwerk die Einstellung einer Management-VLAN-ID erforderlich ist (siehe Physikalische WLAN Parameter)!

Verschlüsselung

Bestimmen Sie hier das Verschlüsselungsverfahren bzw. bei WEP die Schlüssellänge für die Verschlüsselung von Datenpaketen in diesem WLAN.

Schlüssel 1 / Passphrase

Sie können die Schlüssel oder Passphrasen als ASCII-Zeichenkette eingeben. Bei WEP ist alternativ die Eingabe einer Hexadezimalzahl durch ein vorangestelltes "0x" möglich. Folgende Zeichenkettenlängen ergeben sich für die verwendeten Formate:

- WPA-PSK: 8 bis 63 ASCII-Zeichen
- WEP128 (104 Bit): 13 ASCII- oder 26 Hexadezimal-Zeichen
- WEP64 (40 Bit): 5 ASCII- oder 10 Hexadezimal-Zeichen

RADIUS-Profil

Geben Sie an, welches RADIUS-Profil der AP für dieses Netzwerk erhalten soll, damit dieser bei Bedarf eine direkte Verbindung zum RADIUS-Server aufbauen kann. Lassen Sie dieses Feld leer, wenn der WLC RADIUS-Anfragen abwickeln soll.

Die RADIUS-Profile müssen Sie in der entsprechenden Tabelle konfigurieren.

Zulässige Freq.-Bänder

Bestimmen Sie das Frequenzband, das die Netzwerkteilnehmer zur Übertragung von Daten im WLAN verwenden sollen. Sie können sowohl das 2,4 GHz-Band, das 5 GHz-Band als auch beide Bänder auswählen. Zusätzlich gibt es das 6 GHz-Band.

Dauerhaft autark betreiben

Ist am WLC der autarke Weiterbetrieb für WLAN-Netwerke so konfiguriert, dass Netzwerke dauerhaft ausgestrahlt werden (Wert: 9999), so gilt dies gleichermaßen für lokal am LAN ausgekoppelte Netzwerke, als auch für via WLC-Tunnel verbundene Netzwerke. Im Falle eines Ausfalls des WLC werden beide Arten von Netzen somit weiter ausgestrahlt; sinnvoll ist dies aber nur für via LAN ausgekoppelte Netzwerke, da via WLC-Tunnel angebundenen Netzwerken ihr Endpunkt in Form des WLCs fehlt und diese damit nicht einsatzfähig sind.

Mit diesem Schalter können die beiden Arten von Netzwerken getrennt behandelt werden.

- Ist der Schalter gesetzt, werden lokal ausgekoppelte Netzwerke dauerhaft autark weiterbetrieben. Über einen WLC-Tunnel ausgekoppelte Netzwerke werden hingegen nur ausgestrahlt, wenn der WLC erreichbar ist.
- Ist der Schalter nicht gesetzt, wird weiterhin die unter **Autarker Weiterbetrieb** angegebene Zeit verwendet.

Autarker Weiterbetrieb

Zeit in Minuten, für die der AP im Managed-Modus mit seiner aktuellen Konfiguration weiterarbeitet.

Der WLC weist dem AP die Konfiguration zu, der sie optional im Flash speichert (in einem Bereich, der nicht mit LANconfig oder anderen Tools auszulesen ist). Falls die Verbindung zum WLC abbricht, arbeitet der AP für die hier eingestellte Zeit mit seiner Konfiguration aus dem Flash weiter. Auch nach einem eigenen Stromausfall kann der AP mit der Konfiguration aus dem Flash weiterarbeiten.

Wenn die eingestellte Zeit abgelaufen ist, bevor die Verbindung zum WLC wiederhergestellt ist, löscht der AP die Konfiguration im Flash – der AP stellt seinen Betrieb ein. Sobald der WLC wieder erreichbar ist, überträgt der WLC die Konfiguration erneut zum AP.

Diese Maßnahme stellt einen wirksamen Schutz gegen Diebstahl dar, da der AP die sicherheitsrelevanten Parameter der Konfiguration nach Ablauf der eingestellten Zeit automatisch löscht.

Stellt der AP im Backup-Fall eine Verbindung zu einem sekundären WLC her, so unterbricht der AP den Count-Down für den autarken Weiterbetrieb. Der AP bleibt also mit seinen WLAN-Netzwerken auch über diese eingestellte Zeit hinaus aktiv, solange er eine Verbindung zu einem WLC hat.

Bitte beachten Sie, dass der AP die Konfigurationsdaten im Flash erst nach Ablauf der eingestellten Zeit für den autarken Weiterbetrieb löscht, nicht jedoch durch die Trennung vom Stromnetz!

Zeitrahmen

Wählen Sie hier einen der in **WLAN-Controller** > **Allgemein** > **Zeitrahmen** definierten Zeitrahmen aus. Über diesen kann die Ausstrahlung dieser SSID auf die dort definierten Zeiten eingeschränkt werden. Somit lässt sich z. B. in einer Schule ein WLAN nur während der Unterrichtszeiten aktivieren. Die Konfiguration der Zeitrahmen für den WLAN-Controller erfolgt analog zu den Einstellungen in *Zeitrahmen* auf Seite 1708.

802.11u-Netzwerk-Profil

Wählen Sie aus der Liste ein Hotspot-2.0-Profil aus.

OKC aktiviert

Mit dieser Option aktivieren Sie das opportunistische Schlüssel-Caching (Opportunistic Key Caching). Das OKC ermöglicht es WLAN-Clients, schnell und komfortabel in WLAN-Umgebungen mit WPA2-Enterprise-Verschlüsselung zwischen WLAN-Zellen zu wechseln (Roaming).

MAC-Prüfung aktiviert

In der MAC-Filterliste (**Wireless-LAN** > **Stationen/LEPS** > **LEPS-MAC** > **Stationsregeln**) sind die MAC-Adressen der Clients hinterlegt, die sich bei einem AP einbuchen dürfen. Mit dem Schalter **MAC-Filter aktiviert** können Sie die Verwendung der MAC-Filterliste gezielt für einzelne logische Netzwerke ausschalten.

SSID-Broad. unterdrücken

Sie können Ihr Funk-LAN entweder in einem öffentlichen oder in einem privaten Modus betreiben. Ein Funk-LAN im öffentlichen Modus kann von Mobilstationen in der Umgebung ohne weiteres kontaktiert werden. Durch Aktivieren der Closed-Network-Funktion versetzen Sie Ihr Funk-LAN in einen privaten Modus. In dieser Betriebsart sind Mobilstationen ohne Kenntnis des Netzwerknamens (SSID) von der Teilnahme am Funk-LAN ausgeschlossen.

Schalten Sie den "Closed-Network-Modus" ein, wenn Sie verhindern möchten, dass sich WLAN-Clients mit der SSID "Any" oder einer leeren SSID in Ihrem Funknetzwerk anmelden.

Die Option **SSID-Broadcast unterdrücken** ermöglicht folgende Einstellungen:

- **Nein**: Der AP veröffentlicht die SSID der Funkzelle. Sendet ein Client einen Probe Request mit leerer oder falscher SSID, antwortet der AP mit der SSID der Funkzelle (öffentliches WLAN).
- **Ja**: Der AP veröffentlicht die SSID der Funkzelle nicht. Sendet ein Client einen Probe Request mit leerer SSID, antwortet der AP ebenfalls mit einer leeren SSID.
- **Verschärft**: Der AP veröffentlicht die SSID der Funkzelle nicht. Sendet ein Client einen Probe Request mit leerer oder falscher SSID, antwortet der AP überhaupt nicht.



Das einfache Unterdrücken der SSID bietet keinen ausreichenden Zugriffsschutz, da der AP diese bei der Anmeldung berechtigter WLAN-Clients im Klartext überträgt und sie somit für alle im WLAN-Netz befindlichen WLAN-Clients kurzfristig sichtbar ist.

RADIUS-Accounting aktiviert

Aktivieren Sie diese Option, wenn Sie das RADIUS-Accounting in diesem logischen WLAN-Netzwerkm aktivieren wollen.

Datenverkehr zulassen zwischen Stationen dieser SSID

Aktivieren Sie diese Option, wenn alle Stationen, die an dieser SSID angemeldet sind, untereinander kommunizieren dürfen.

WPA-Version

Wählen Sie hier die WPA-Version aus, die der AP den WLAN-Clients zur Verschlüsselung anbieten soll.

- WPA1: Nur WPA1
- WPA2: Nur WPA2
- WPA3: Nur WPA3
- WPA1/2: Sowohl WPA1 als auch WPA2 in einer SSID (Funkzelle)
- WPA2/3: Sowohl WPA2 als auch WPA3 in einer SSID (Funkzelle)
- WPA1/2/3: WPA1, WPA2 und WPA3 in einer SSID (Funkzelle)

WPA1 Sitzungsschl.-Typ

Wenn Sie als Verschlüsselungsmethode "802.11i (WPA)-PSK" nutzen, können Sie hier das Verfahren zur Generierung des Sitzungs- bzw. Gruppenschlüssels für WPA1 auswählen:

- AES: Der AP verwendet das AES-Verfahren.

- TKIP: Der AP verwendet das TKIP-Verfahren.
- AES/TKIP: Der AP verwendet das AES-Verfahren. Falls die Client-Hardware das AES-Verfahren nicht unterstützt, wechselt der AP zum TKIP-Verfahren.

WPA2 und WPA3 Sitzungsschlüssel-Typen

Wählen Sie hier das Verfahren zur Generierung des Sitzungs- bzw. Gruppenschlüssels für WPA2 und WPA3 aus.

Basis-Geschwindigkeit

Die eingestellte Basis-Geschwindigkeit sollte es auch unter ungünstigen Bedingungen erlauben, die langsamsten Clients im WLAN zu erreichen. Stellen Sie hier nur dann eine höhere Geschwindigkeit ein, wenn alle Clients in diesem logischen WLAN auch "schneller" zu erreichen sind. Bei automatischer Festlegung der Übertragungsrate sammelt der AP die Informationen über die Übertragungsraten der einzelnen WLAN-Clients. Die Rate teilen die Clients dem AP automatisch bei jeder Unicast-Kommunikation mit. Aus der Liste der angemeldeten Clients wählt der AP nun ständig die jeweils niedrigste Übertragungsrate aus und überträgt damit die Multicast- und Broadcast-Sendungen.

Client-Bridge-Unterst.

Aktivieren Sie diese Option für einen AP, wenn Sie im WLAN-Client-Modus für eine Client-Station die Client-Bridge-Unterstützung aktiviert haben.

Der Client-Bridge-Modus ist ausschließlich zwischen zwei LANCOM-Geräten verwendbar.

TX Bandbr.-Begrenzung

Über diese Einstellung definieren Sie die zur Verfügung stehende Gesamtbandbreite in Senderichtung für die betreffende SSID. Der Wert `0` deaktiviert die Begrenzung.

RX Bandbr.-Begrenzung

Über diese Einstellung definieren Sie die zur Verfügung stehende Gesamtbandbreite in Empfangsrichtung für die betreffende SSID. Der Wert `0` deaktiviert die Begrenzung.

Client TX Bandbr.-Begrenzung

Hier begrenzen Sie die Bandbreite (Limit in kBit/s) in Senderichtung, die jedem WLAN-Client auf dieser SSID zur Verfügung steht. Der Wert `0` deaktiviert die Begrenzung.

Client RX Bandbr.-Begrenzung

Hier begrenzen Sie die Bandbreite (Limit in kBit/s) in Empfangsrichtung, die jedem WLAN-Client auf dieser SSID zur Verfügung steht. Der Wert `0` deaktiviert die Begrenzung.

Maximalzahl der Clients

Legen Sie hier die maximale Anzahl der Clients fest, die sich bei diesem AP einbuchen dürfen. Weitere Clients, die sich über diese Anzahl hinaus anmelden wollen, lehnt der AP ab.

Min. Client-Signal-Stärke

Mit diesem Eintrag bestimmen Sie den Schwellwert in Prozent für die minimale Signalstärke für Clients beim Einbuchen. Unterschreitet ein Client diesen Wert, sendet der AP keine Probe-Responses mehr an diesen Client und verwirft die entsprechenden Anfragen.

Ein Client mit schlechter Signalstärke findet den AP somit nicht und kann sich nicht darauf einbuchen. Das sorgt beim Client für eine optimierte Liste an verfügbaren APs, da keine APs aufgeführt werden, mit denen der Client an der aktuellen Position nur eine schwache Verbindung aufbauen könnte.

Client-Trennen-Signal-Stärke

Wenn dieser Schwellenwert unterschritten wird, dann wird der Client disassoziiert. Dadurch lässt sich vermeiden, dass der Client an einer aufgrund der geringen Signalstärke de facto bereits unbrauchbaren WLAN-Verbindung hängen bleibt anstatt auf eine am Client oft ebenfalls verfügbare Mobiltelefon-Verbindung umzuschalten – ein Verhalten, welches sich bei Mobiltelefonen immer wieder beobachten lässt und für den Benutzer ärgerlich ist.

Dieser Schwellenwert funktioniert nur, wenn auch der Wert **Minimale Client-Signal-Stärke** gesetzt ist und außerdem **Client-Trennen-Signal-Stärke** kleiner als dieser Wert ist.

LBS-Tracking aktiviert

Diese Option gibt an, ob der LBS-Server die Client-Informationen nachverfolgen darf.

Diese Option konfiguriert das Tracking aller Clients einer SSID. Im Public Spot-Modul bestimmen Sie, ob der LBS-Server die am Public Spot angemeldeten Benutzer tracken darf.

LBS-Tracking-Liste

Mit diesem Eintrag legen Sie den Listennamen für das LBS-Tracking fest. Bei einem erfolgreichen Einbuchen eines Clients in diese SSID überträgt der AP den angegebenen Listennamen, die MAC-Adresse des Clients und die eigene MAC-Adresse an den LBS-Server.

Lange Präambel bei 802.11b verwenden

Normalerweise handeln die Clients im 802.11b-Modus die Länge der zu verwendenden Präambel mit dem AP selbst aus. Stellen Sie hier die "lange Präambel" nur dann fest ein, wenn die Clients diese feste Einstellung verlangen.

(U-)APSD / WMM-Powersave aktiviert

Aktivieren Sie diese Option, um Stationen die Unterstützung für den Stromsparmechanismus (U-)APSD ([Unscheduled] Automatic Power Save Delivery) zu signalisieren.

(U-)APSD ist im Standard 802.11e verankert und hilft VoWLAN-Geräten dabei, ihre Akkulaufzeit zu erhöhen. Die betreffenden Geräte schalten dafür nach der Anmeldung an einem (U-)APSD-fähigen AP in den Energiesparmodus um. Erhält der AP nun Datenpakete für das betreffende Gerät, speichert es die Daten kurz zwischen und wartet, bis das VoWLAN-Gerät wieder verfügbar ist. Erst dann leitet er die Daten weiter. (U-)APSD erhöht demnach die Latenzzeit des Funkmoduls, wodurch es letztlich weniger Strom verbraucht. Die einzelnen Ruhezeiten können dabei so kurz ausfallen, dass ein VoWLAN-Gerät selbst im Gesprächszustand noch den Stromsparmechanismus benutzen kann. Die betreffenden Geräte müssen (U-)APSD allerdings ebenfalls unterstützen.

Bei WWM (Wi-Fi Multimedia) Power Save handelt es sich um einen Stromsparmechanismus der Wi-Fi Alliance, welcher auf U-APSD basiert. Bestimmte LANCOM APs sind von der Wi-Fi Alliance WMM® Power Save CERTIFIED.

Max. Spatial-Streams

Mit der Funktion des Spatial-Multiplexing kann der AP mehrere separate Datenströme über separate Antennen übertragen, um so den Datendurchsatz zu verbessern. Der Einsatz dieser Funktion ist nur dann zu empfehlen, wenn die Gegenstelle die Datenströme mit entsprechenden Antennen verarbeiten kann.

In der Einstellung 'Automatisch' nutzt der AP alle Spatial-Streams, die das jeweilige WLAN-Modul unterstützt.

Kurzes Guard-Intervall zulassen

Dieser Option reduziert die Sendepause zwischen zwei Signalen von 0,8 s (Standard) auf 0,4 s (Short Guard Interval). Dadurch steigt die effektiv für die Datenübertragung genutzte Zeit und damit der Datendurchsatz. Auf der anderen Seite ist das WLAN-System damit anfälliger für Störungen, welche durch die Interferenzen zwischen zwei aufeinanderfolgenden Signalen auftreten können.

Im Automatik-Modus wird das kurze Guard-Intervall aktiviert, sofern die jeweilige Gegenstelle diese Betriebsart unterstützt. Alternativ kann die Nutzung des kurzen Guard-Intervalls auch ausgeschaltet werden.

Frame-Aggregation verwenden

Bei der Frame-Aggregation werden mehrere Datenpakete (Frames) zu einem größeren Paket zusammengefasst und gemeinsam versendet. Dieses Verfahren reduziert den Overhead der Pakete, der Datendurchsatz steigt.

Die Frame-Aggregation eignet sich weniger gut bei schnell bewegten Empfängern oder für zeitkritische Datenübertragungen wie Voice over IP.

STBC (Space Time Block Coding) aktiviert

Aktivieren Sie hier das Space Time Block Coding.

STBC ist ein Kodierverfahren nach IEEE 802.11n. Die Funktion „STBC" (Space Time Block Coding) variiert den Versand von Datenpaketen zusätzlich über die Zeit, um auch zeitliche Einflüsse auf die Daten zu minimieren. Durch den zeitlichen Versatz der Sendungen besteht für den Empfänger eine noch bessere Chance, fehlerfreie Datenpakete zu erhalten, unabhängig von der Anzahl der Antennen. Dadurch kommt es in einem MIMO-System zu besseren Empfangsbedingungen.

LDPC (Low Density Parity Check) aktiviert

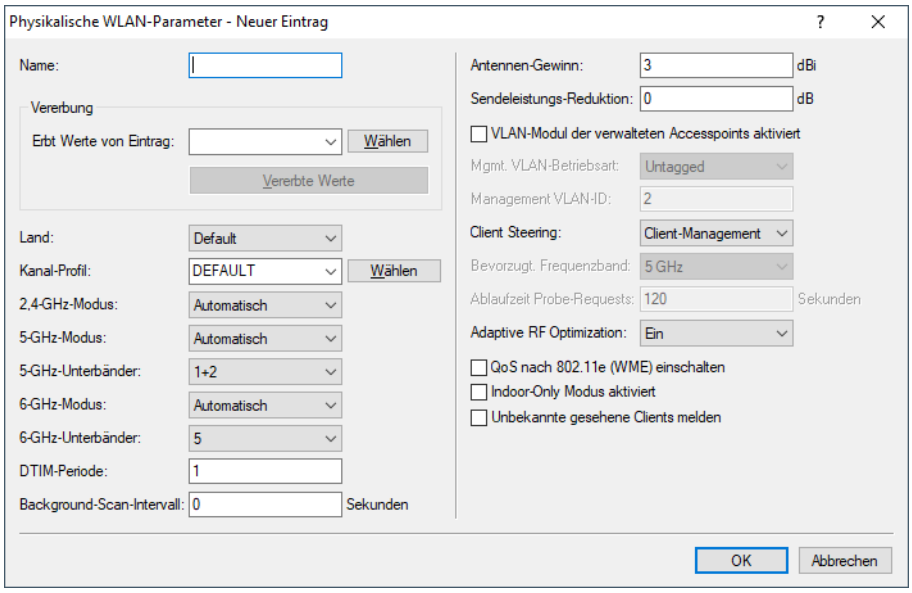
Aktivieren Sie hier den Low Density Parity Check.

Bevor der Sender die Datenpakete abschickt, erweitert er den Datenstrom abhängig von der Modulationsrate um Checksummen-Bits, um dem Empfänger damit die Korrektur von Übertragungsfehlern zu ermöglichen. Standardmäßig nutzt der Übertragungsstandard IEEE 802.11n das bereits aus den Standards 802.11a und 802.11g bekannte 'Convolution Coding' (CC) zur Fehlerkorrektur, ermöglicht jedoch auch eine Fehlerkorrektur nach der LDPC-Methode (Low Density Parity Check).

Im Unterschied zur CC-Kodierung nutzt die LDPC-Kodierung größere Datenpakete zur Checksummenberechnung und kann zusätzlich mehr Bit-Fehler erkennen. Die LDPC-Kodierung ermöglicht also bereits durch ein besseres Verhältnis von Nutz- zu Checksummen-Daten eine höhere Datenübertragungsrate.

14.4.2.9 Physikalische WLAN-Parameter

Hier werden die physikalischen WLAN-Parameter eingestellt, die den Access Points zugewiesen werden. Für jeden Satz von physikalischen WLAN-Parametern können Sie unter **WLAN-Controller** > **Profile** > **Physikalische WLAN-Parameter** die folgenden Parameter definieren:



Name

Eindeutiger Name für diese Zusammenstellung von physikalischen WLAN-Parametern.

Vererbung

Auswahl eines schon definierten Satzes von physikalischen WLAN-Parametern, von dem die Einstellungen übernommen werden sollen.

Land

Land, in dem die Access Points betrieben werden sollen. Aufgrund dieser Information werden landesspezifische Einstellungen wie die erlaubten Kanäle etc. festgelegt.

Kanal-Profil

Wählen Sie ein Kanal-Profil aus. Siehe *Kanal-Profil-Tabelle* auf Seite 1141.

Das DEFAULT-Profil aktiviert alle erlaubten Kanäle des eingestellten Landes.

DTIM-Periode

Sobald mindestens ein mobiles Endgerät (Client) Stromsparmechanismen verwendet, werden Broad- und Multicasts nicht mehr unmittelbar in die Funkzelle gesendet, sondern gesammelt nach den regelmäßig von dem Access Point ausgestrahlten Beacon. Da den Clients das nächste relevante Beacon bekannt gegeben wird und sie sich daher auf die Aussendung der Broad- und Multicasts synchronisieren können, ermöglicht ihnen dies, ihr Funkmodul die meiste Zeit ausgeschaltet zu lassen und es nur zu diesen Zeitpunkten zu aktivieren.

Die DTIM-Periode gibt an, nach jeweils wievielen Beacons gesammelte Broad- und Multicasts ausgestrahlt werden. Höhere Werte erlauben Clients, mehr Energie zu sparen, erhöhen aber auch die Latenz bei der Zustellung dieser Pakete.

Der Standard-Wert ist 1, d .h. gesammelte Broad- und Multicasts werden nach jedem Beacon ausgestrahlt.

Management VLAN-ID

Die VLAN-ID, die für das Management-Netz der APs verwendet wird.

Die Management-VLAN-ID **muss** auf einen Wert ungleich null eingestellt werden, um VLANs auf den WLAN-Netzwerken nutzen zu können. Das gilt auch dann, wenn das Management-Netz selbst nicht mit VLAN-IDs getaggt werden soll (Mgmt-VLAN-ID = 1).

Die VLAN-Aktivierung gilt jeweils nur für logischen WLAN-Netzwerke, die mit diesen physikalischen WLAN-Parametern verbunden sind.

Client Steering

Dieser Eintrag bestimmt die Art des Client Steerings und ob der AP das Band-Steering aktivieren soll. In diesem Fall kann ein Dual-Port-Access-Point einen WLAN-Client auf ein bevorzugtes Frequenzband umleiten.

Das Client-Steering ermöglicht den APs, die im Sendebereich befindlichen WLAN-Clients anhand bestimmter Kriterien zu veranlassen, sich immer mit dem für sie idealen AP zu verbinden. Die Kriterien sind zentral im WLAN-Controller definiert. Die verwalteten Access Point melden ständig die aktuellen Werte an den WLAN-Controller, der aufgrund der Kriterien entscheidet, welche Access Points die Anfragen von WLAN-Clients beantworten dürfen. Deshalb ist das Client-Steering auch nur mit Access Points möglich, die ein WLAN-Controller zentral verwaltet.

Aus

Das Client-Steering ist deaktiviert.

Ein

Der AP lässt das Client-Steering vom WLC durchführen.

Client Management

Das Client Steering wird dezentral von den APs durchgeführt. Siehe *Client Management* auf Seite 983.

AP-basiertes Band-Steering

Der AP leitet den WLAN-Client eigenständig auf ein bevorzugtes Frequenzband.

Unbekannte gesehene Clients melden

Der Access-Point meldet standardmäßig nur bekannte (also assoziierte) Clients an den WLC. Sollen darüber hinaus auch alle übrigen gesehenen (also unbekannte und nicht assoziierte) Clients gemeldet werden, so können Sie diesen Schalter aktivieren. Dies erhöht natürlich den Datenverkehr im Netz. Sie sollten diesen Schalter daher nur vorübergehend oder zu Testzwecken aktivieren.

Wenn mit einer Vielzahl von unbekannten Clients zu rechnen ist (z. B. bei einem Public Spot oder in Bereichen mit regem Publikumsverkehr), sollten Sie diesen Schalter nicht aktivieren, da Sie ansonsten von den eingehenden Meldungen überflutet werden.

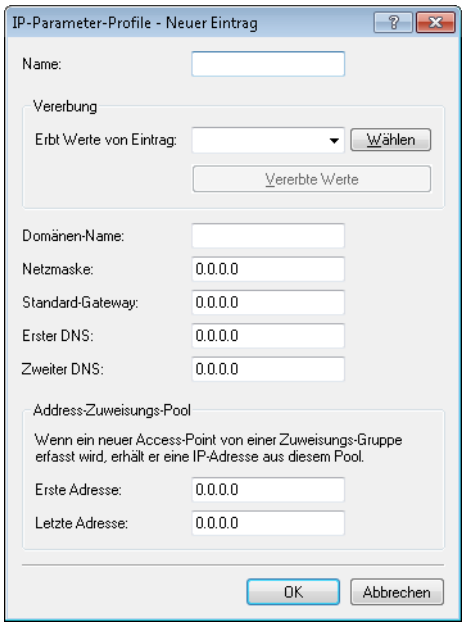
Alle weiteren physikalischen WLAN-Parameter entsprechen denen der üblichen Konfiguration für APs.

Für den erfolgreichen Profilbezug ist es erforderlich, dass der HTTP-Zugriff auf den WLC aus dem lokalen Netz erlaubt ist.

14.4.3 Access Point Konfiguration

14.4.3.1 IP-Parameter-Profile

In dieser Tabelle definieren Sie bestimmte Netzprofile, welche sich einem AP zuweisen lassen, den der WLC nicht automatisch via DHCP konfigurieren soll. Auf diese Weise legen Sie gezielt fest, welche IP-Parameter ein AP nutzt.



Name

Name des IP-Parameter-Profils.

Vererbung

Auswahl eines schon definierten IP-Parameter-Profils, von dem die Einstellungen übernommen werden sollen (siehe *Vererbung von Parametern* auf Seite 1143).

Domänen-Name

Name der Domäne (DNS-Suffix), die dieses Profil nutzen soll.

Netzmaske

Netzmaske des Profils.

Standard-Gateway

Standard-Gateway, welches das Profil verwendet.

Erster DNS

Der DNS (Domain Name System), den das Profil verwenden soll.

Zweiter DNS

Zweiter, alternativer DNS, sollte der erste nicht erreichbar sein.

Erste Adresse

Anfang des IPv4-Adressbereichs, aus dem ein neuer AP eine IP-Adresse erhält, wenn der WLC den AP einer Zuweisungs-Gruppe zuordnen kann und Sie für den betreffenden AP in der AP-Tabelle keine konkrete IP-Adresse definiert haben.

Letzte Adresse

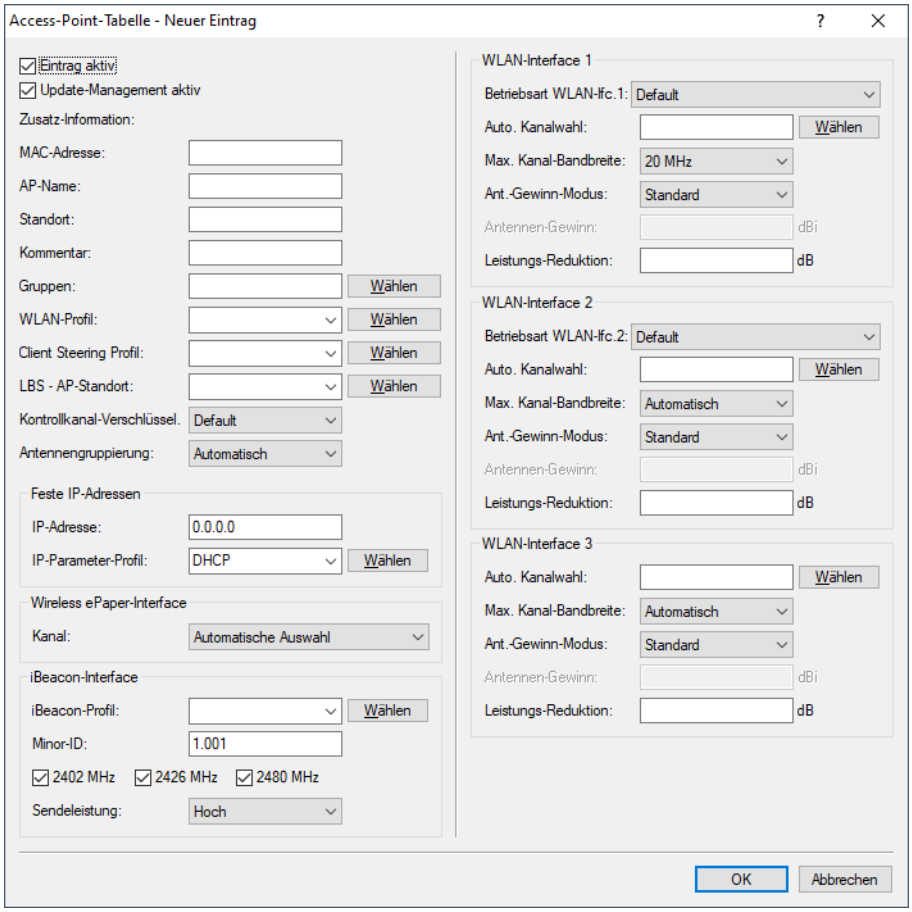
Ende des IPv4-Adressbereichs, aus dem ein neuer AP eine IP-Adresse erhält, wenn der WLC den AP einer Zuweisungs-Gruppe zuordnen kann und Sie für den betreffenden AP in der AP-Tabelle keine konkrete IP-Adresse definiert haben.

Weitere Informationen zu den Zuweisungs-Gruppen finden Sie im Abschnitt *IP-abhängige Autokonfiguration und Tagging von APs* auf Seite 1190.

14.4.3.2 Liste der Access Points

Die Access Point-Tabelle ist ein zentraler Aspekt der Konfiguration für WLCs. Hier ordnet der WLC den Access Points über WLAN-Profile (also Kombinationen aus logischen und physikalischen WLAN-Parametern) ihre MAC-Adresse zu. Außerdem hat die reine Existenz eines Eintrages in der Access Point-Tabelle für einen bestimmten Access Point Auswirkungen auf

die Möglichkeit, eine Verbindung zu einem WLC aufbauen zu können. Für jeden Access Point können Sie unter **WLAN-Controller** > **AP-Konfiguration** > **Access-Point-Tabelle** die folgenden Parameter definieren:



Eintrag aktiv

Aktiviert bzw. deaktiviert diesen Eintrag.

Update-Management aktiv

Wenn Sie für diesen Access Point das Update-Management aktivieren, kann er neue Firmware- oder Script-Versionen automatisch laden. Nehmen Sie alle weiteren Einstellungen unter Access Point-Update vor (*Zentrales Firmware- und Skript-Management*).

MAC-Adresse

MAC-Adresse des Access Points.

AP-Name

Name des Access Points im Managed-Modus.

Standort

Standort des Access Points im Managed-Modus.

Kommentar

Geben Sie einen Kommentar für diesen Eintrag ein.

Gruppen

Ordnet den Access Point einer oder mehrerer Gruppen zu

WLAN-Profil

WLAN-Profil aus der Liste der definierten Profile.

Client Steering Profil

Client Steering-Profile legen die Bedingungen fest, nach denen der WLC entscheidet, welche Access Points beim nächsten Anmeldeversuch einen Client annehmen.

LBS - AP-Standort

LBS-Standort-Profil aus der Liste der definierten Profile.

Kontrollkanal-Verschlüsselung

Verschlüsselung für die Kommunikation über den Kontrollkanal. Ohne Verschlüsselung tauschen Access Point und WLC die Kontrolldaten im Klartext aus. Eine Authentifizierung mittels Zertifikat findet in beiden Fällen statt.

Antennengruppierung

Um den Gewinn durch Spatial-Multiplexing zu optimieren, kann die Antennengruppierung konfiguriert werden.

IP-Adresse

Spezifizieren Sie hier eine feste IP-Adresse des Access Points.

IP-Parameter-Profil

Geben Sie hier den Profilnamen an, über den der WLC die IP-Einstellungen für den Access Point referenzieren muss. Wenn Sie den Standardwert DHCP beibehalten, ignoriert der WLC die Angabe der festen IP-Adresse, so dass der Access Point seine IP-Adresse über DHCP beziehen muss.

Kanal (Wireless ePaper-Interface)

Bestimmen Sie hier, wie die Kanalwahl der Wireless ePaper-Schnittstelle erfolgen soll.

iBeacon-Profil (iBeacon-Interface)

Wählen Sie ein iBeacon-Profil aus der Liste der angelegten Profile aus.

iBeacon-Profile erstellen Sie unter **WLAN-Controller** > **AP-Konfiguration** > **Erweiterte Einstellungen** > **iBeacon-Profile**.

Minor

Legen Sie eine Minor-ID für das iBeacon-Modul fest.

2402 MHz, 2426 MHz, 2480 MHz

Definieren Sie hier, welche Sendekanäle das iBeacon-Modul verwenden soll.

Sendeleistung

Geben Sie an, Mit welcher Leistung das iBeacon-Modul senden soll. Folgende Werte sind möglich:

- **Hoch**: Das Modul sendet mit maximaler Leistung (Default).
- **Mittel**: Das Modul sendet mit durchschnittlicher Leistung.
- **Gering**: Das Modul sendet mit minimaler Leistung.

Betriebsart WLAN-Ifc. 1

Über diese Einstellung konfigurieren Sie das Frequenzband, in dem der Access Point die 1. physikalische WLAN-Schnittstelle betreibt. In der Einstellung **Default** wählt der Access Point das Frequenzband für die physikalische WLAN-Schnittstelle selbstständig aus. Dabei behandelt der Access Point das 2,4-GHz-Band bevorzugt, sofern dieses verfügbar ist.

Betriebsart WLAN-Ifc. 2

Über diese Einstellung konfigurieren Sie das Frequenzband, in dem der Access Point die 2. physikalische WLAN-Schnittstelle betreibt. In der Einstellung **Default** wählt der Access Point das Frequenzband für die physikalische WLAN-Schnittstelle selbstständig aus. Dabei behandelt der Access Point das 5-GHz-Band bevorzugt, sofern dieses verfügbar ist.

Sofern ein verwalteter Access Point lediglich über eine physikalische WLAN-Schnittstelle verfügt, ignoriert der Access Point die Einstellungen für die 2. physikalische WLAN-Schnittstelle.

Auto. Kanalwahl

Die Kanalauswahl erfolgt vom Access Point grundsätzlich automatisch für das Frequenzband des eingestellten Landes, wenn hier kein Eintrag erfolgt.

Tragen Sie hier die Kanäle ein, auf die sich die automatische Auswahl für das erste WLAN-Modul beschränken soll. Geben Sie hier nur einen Kanal an, so verwendet der Access Point nur diesen und es findet keine automatische Auswahl statt. Achten Sie deshalb darauf, dass die angegebenen Kanäle wirklich im Frequenzband des eingestellten Landes zur Verfügung stehen. Für das jeweilige Frequenzband ungültige Kanäle ignoriert der Access Point.

Max. Kanal-Bandbreite

Geben Sie an, wie und in welchem Umfang der Access Point die Kanal-Bandbreite für die physikalische(n) WLAN-Schnittstelle(n) festlegt. Folgende Werte sind möglich:

- **Automatisch**: Der Access Point ermittelt automatisch die maximale Kanal-Bandbreite (Default).
- **20 MHz**: Der Access Point benutzt auf 20 MHz gebündelte Kanäle.
- **40 MHz**: Der Access Point benutzt auf 40 MHz gebündelte Kanäle.
- **80 MHz**: Der Access Point benutzt auf 80 MHz gebündelte Kanäle.
- **80+80 MHz**: Der Access Point benutzt zwei auf 80 MHz gebündelte Kanäle.
- **160 MHz**: Der Access Point benutzt auf 160 MHz gebündelte Kanäle.
- **320 MHz** (Nur WLAN-Interface 3): Der Access Point benutzt auf 320 MHz gebündelte Kanäle.

Standardmäßig bestimmt die physikalische WLAN-Schnittstelle den Frequenzbereich, in dem die zu übertragenen Daten auf die Trägersignale aufmoduliert werden, automatisch. 802.11a/b/g nutzen 48 Trägersignale in einem 20 MHz-Kanal. Durch die Nutzung des doppelten Frequenzbereiches von 40 MHz können 96 Trägersignale eingesetzt werden, was zu einer Verdoppelung des Datendurchsatzes führt.

802.11n kann in einem 20 MHz-Kanal 52, in einem 40 MHz-Kanal sogar 108 Trägersignale zur Modulation nutzen. Für 802.11n bedeutet die Nutzung der 40 MHz-Option also einen Performance-Gewinn auf mehr als das Doppelte.

Ant.-Gewinn-Modus

Bei der Inbetriebnahme von Access Points an einem WLAN-Controller wurden diese bisher immer mit einem Antennengewinn von 3 dBi je Modul eingerichtet, da dieser Wert für die meisten Indoor-Access Points mit Standardantennen passend ist. Insbesondere für Outdoor-Access Points mit integrierten Antennen musste der Wert aber in der Vergangenheit manuell angepasst werden, die hier häufig interne Antennen mit einem hohen Antennengewinn zum Einsatz kommen. Ab LCOS 10.30 wird der Standard-Antennengewinn eines verwalteten Access Points an den WLAN-Controller übertragen und dort automatisch verwendet. Für diese Funktion müssen sowohl der Access Point als auch der WLAN-Controller, mindestens den Firmware-Stand 10.30 aufweisen. Mit dieser Einstellung für den Modus des Antennengewinns wird verhindert, dass man nach einem Rollout einige Access Points noch manuell korrigieren muss.

Mögliche Werte:

Standard

Der im Access Point voreingestellte Wert für den Antennengewinn wird verwendet.

Benutzerdefiniert

Der im Feld **Antennen-Gewinn** eingestellte Wert wird verwendet.

Antennen-Gewinn

Mit diesem Eintrag können Sie den Antennen-Verstärkungsfaktor (Gewinn in dBi) abzüglich der Dämpfungen für Kabel und ggf. Blitzschutz angeben. Hieraus errechnet der Access Point die im jeweiligen Land und für das jeweilige Frequenzband maximal zulässige Sendeleistung.

Wenn Sie das Feld leer lassen, verwendet der Access Point die Default-Einstellung der Konfigurationsgruppe im verwendeten WLAN-Profil.

Sie können die Sendeleistung auf minimal 0,5 dBm im 2,4-GHz-Band bzw. 6,5 dBm im 5-GHz-Band reduzieren. Das begrenzt den maximal einzutragenden Wert im 2,4-GHz-Band auf 17,5 dBi, im 5-GHz-Band auf 11,5 dBi.

Achten Sie darauf, dass Ihr Antennen-, Kabel- und Blitzschutz-Aufbau unter diesen Bedingungen den Regulierungsanforderungen des Landes entspricht, in dem Sie das System einsetzen.

Die Empfindlichkeit des Empfängers bleibt hiervon unbeeinflusst.

Die aktuelle Sendeleistung können Sie mit Hilfe von WEBconfig bzw. Telnet unter **Status** > **WLAN-Statistik** > **WLAN-Parameter** > **Sendeleistung** oder per LANmonitor unter **System-Informationen** > **WLAN-Karte** > **Sendeleistung** einsehen.

Leistungs-Reduktion

Wenn Sie eine Antenne mit einem hohen Verstärkungsfaktor verwenden, können Sie mit diesem Eintrag die Sendeleistung des Access Points auf die in verwendeten Land und die im jeweiligen Frequenzband zulässige Sendeleistung herunterdämpfen.

Wenn Sie das Feld leer lassen, verwendet der Access Point die Default-Einstellung der Konfigurationsgruppe im verwendeten WLAN-Profil.

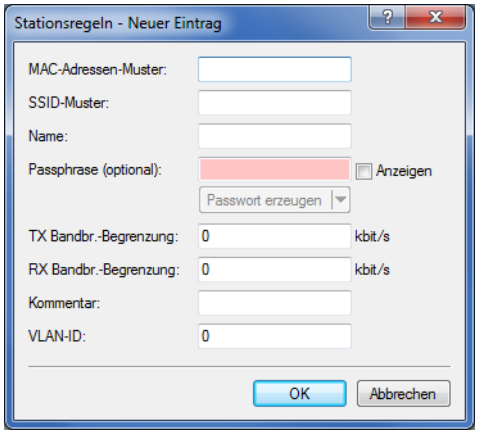
Es gelten dieselben Werte und Einschränkungen wie im Feld **Antennen-Gewinn**.

14.4.3.3 Stationen

Mit Hilfe der Stationsregeln legen Sie fest, welche WLAN-Clients sich in den WLAN-Netzwerken der APs anmelden können, die durch den WLC zentral verwaltet werden. Außerdem können Sie den einzelnen WLAN-Clients auf diesem Wege sehr komfortabel eine individuelle Passphrase zur Authentifizierung und eine VLAN-ID zuweisen.

Zur Nutzung der Stationsregeln unter **WLAN-Controller** > **Stationen/LEPS** > **LEPS-MAC** > **Stationsregeln** muss grundsätzlich der RADIUS-Server im WLC aktiviert sein. Alternativ kann auch eine Weiterleitung zu einem anderen RADIUS-Server konfiguriert werden. Weitere Information zu RADIUS finden Sie unter *RADIUS*.

Für jedes logische WLAN-Netzwerk, in dem die WLAN-Clients über RADIUS geprüft werden sollen, muss die MAC-Prüfung aktiviert werden.



MAC-Adresse

MAC-Adresse des WLAN-Clients, für den dieser Eintrag gilt. Die folgenden Eingaben sind möglich:

einzelne MAC-Adresse

Eine MAC-Adresse im Format `00a057112233`, `00-a0-57-11-22-33` oder `00:a0:57:11:22:33`.

Wildcards

Wildcards '*' und '?' für die Angabe von MAC-Adressbereichen, z. B. `00a057*`, `00-a0-57-11-??-??` oder `00:a0:??:11:*`.

Vendor-ID

Das Gerät hat eine Liste der gängigen Hersteller-OUIs (Organizationally Unique Identifier) gespeichert. Der MAC-Adressbereich ist gültig, wenn dieser Eintrag den ersten drei Bytes der MAC-Adresse des WLAN-Clients entspricht.

Die Verwendung von Wildcards ist möglich.

SSID-Muster

Dieser Eintrag begrenzt den Zugriff der WLAN-Clients mit den entsprechenden MAC-Adressen auf diese SSID.

Die Verwendung von Wildcards ist möglich, um den Zugriff auf mehrere SSIDs zu erlauben.

Name

Sie können zu jedem WLAN-Client einen beliebigen Namen und einen Kommentar eingeben. Dies ermöglicht Ihnen eine einfachere Zuordnung der MAC-Adressen zu bestimmten Stationen oder Benutzern.

Passphrase

Hier können Sie optional für jede physikalische Adresse (MAC) eine separate Passphrase eintragen, die in den 802.11i / WPA / AES-PSK gesicherten Netzwerken benutzt wird. Ohne die Angabe einer gesonderten Passphrase für diese MAC-Adresse werden die im Bereich **802.11i / WEP** für jedes logische Wireless-LAN-Netzwerk hinterlegten Passphrasen verwendet.

TX Bandbreitenbegrenzung

Sende-Bandbreiten-Begrenzung für die sich einbuchenden WLAN-Clients. Ein WLAN-Gerät im Client-Modus übermittelt seine eigene Einstellung bei der Anmeldung an den AP. Dieser bildet daraus zusammen mit dem hier eingestellten Wert das Bandbreiten-Minimum.

RX Bandbreitenbegrenzung

Empfangs-Bandbreiten-Begrenzung für die sich einbuchenden WLAN-Clients. Ein WLAN-Gerät im Client-Modus übermittelt seine eigene Einstellung bei der Anmeldung an den AP. Dieser bildet daraus zusammen mit dem hier eingestellten Wert das Bandbreiten-Minimum.

Die RX-Bandbreiten-Begrenzung ist nur aktiv für WLAN-Geräte im Client-Modus. Für normale WLAN-Clients wird dieser Wert nicht verwendet.

Kommentar

Hier können Sie einen Kommentar eintragen.

VLAN-ID

Die ID des VLANs, zu welchem dieser Client gehört. Das heißt, der Client kann nur von Paketen erreicht werden, die dem selben VLAN entstammen. Pakete, welche der Client selbst versendet, werden mit dieser VLAN-ID markiert. Sie brauchen diesen Wert nur zu setzen, wenn dieser Client zu einem anderen VLAN gehören soll, als das logische WLAN-Netzwerk (SSID), mit dem er verbunden ist. Gültige VLAN-IDs liegen im Bereich 0 bis 4094. Eine 0 bedeutet, dass der Client zu dem VLAN seines logischen WLAN-Netzwerks (SSID) gehört, sofern dieses überhaupt einem VLAN angehört.

Nutzen Sie IPv6 oder wird in einem VLAN auch Multicast verwendet, müssen den verschiedenen VLANs einer SSID zwingend verschiedene Gruppenschlüssel zugeordnet werden. Ansonsten können die verschiedenen Multicasts nicht den richtigen Clients zugeordnet werden. Dies führt zum Beispiel bei Nutzung von IPv6 dazu, dass den Clients auch IPv6-Präfixe bekannt gegeben werden, die auf der genutzten VLAN-ID nicht funktionieren! Die Gruppenschlüssel können Sie unter **WLAN** > **Verschlüsselung** > **VLAN-Gruppenschlüssel** konfigurieren.

Falls sich Filterregeln widersprechen, hat die individuellere Regel eine höhere Priorität: Eine Regel ohne Wildcards in der MAC-Adresse oder SSID hat Vorrang vor einer Regel mit Wildcards. Ansonsten hat der Anwender beim Anlegen von Einträgen darauf zu achten, dass sich die Filterregeln nicht widersprechen. Mit dem Trace-Aufruf `trace WLAN-ACL` in einer Telnet-Sitzung lassen sich die Filterangaben kontrollieren.

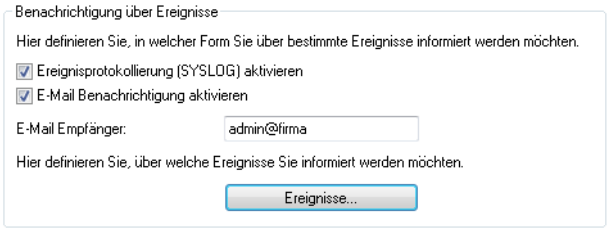
Die Filterkriterien in der Stationsliste erlauben oder verweigern den Zugriff von WLAN-Clients auf das WLAN-Netzwerk. Die Einträge **Name**, **Bandbreiten-Begrenzung**, **VLAN-ID** und **Passphrase** sind bedeutungslos, wenn das Gerät bei gültigen Filterkriterien den WLAN-Zugriff verweigert.

14.4.3.4 Optionen für den WLAN-Controller

Im Bereich der **Optionen** werden die Benachrichtigungen bei Ereignissen im WLC eingestellt sowie einige Defaultwerte definiert.

Benachrichtigungen über Ereignisse

Die Benachrichtigungen können über SYSLOG oder E-Mail erfolgen. Dazu können Sie die folgenden Parameter definieren:





LANconfig: **WLAN-Controller** > **Optionen**

Ereignisprotokollierung (SYSLOG) aktivieren

Aktiviert die Benachrichtigung über SYSLOG.

E-Mail-Benachrichtigung aktivieren

Aktiviert die Benachrichtigung über E-Mail.

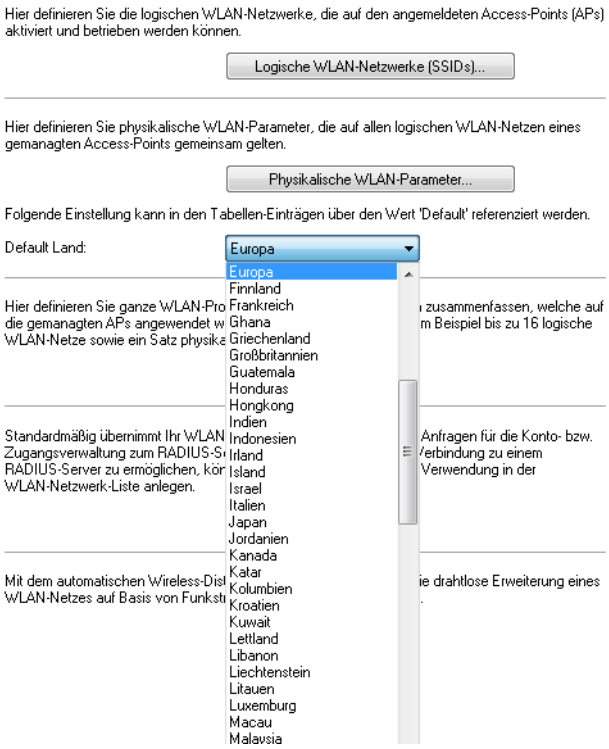
Ereignisse

Wählt die Ereignisse, die über die eine Benachrichtigung erfolgen soll. Mögliche Werte:

- Aktiven AP melden
- Verlorenen AP melden
- Neuen AP melden

Default-Parameter

Für einige Parameter können zentral Default-Werte definiert werden, die an anderen Stellen der Konfiguration als 'Default' referenziert werden können.



LANconfig: **WLAN-Controller** > **Profile** > **Default Land**

› **Default Land**

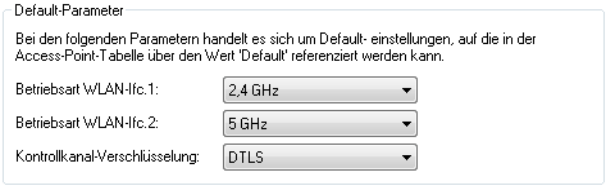
Land, in dem die Access Points betrieben werden sollen. Aufgrund dieser Information werden landesspezifische Einstellungen wir die erlaubten Kanäle etc. festgelegt.

› Mögliche Werte:

› Auswahl aus den verfügbaren Ländern

› Default:

› Europa



LANconfig: **WLAN-Controller** > **AP-Konfig** >

WEBconfig: **LCOS-Menübaum** > **Setup** > **WLAN-Management** > **AP-Konfiguration**

› **WLAN-Interface 1**

Frequenzband für das erste WLAN-Modul. Mit diesem Parameter kann das WLAN-Modul auch deaktiviert werden.

› **WLAN-Interface 2**

Frequenzband für das zweite WLAN-Modul. Mit diesem Parameter kann das WLAN-Modul auch deaktiviert werden.

- **Verschlüsselung**

  Verschlüsselung für die Kommunikation über den Kontrollkanal. Ohne Verschlüsselung werden die Kontrolldaten im Klartext ausgetauscht. Eine Authentifizierung mittels Zertifikat findet in beiden Fällen statt.

14.4.3.5 Virtualisierung und Gastzugang über WLAN Controller mit VLAN

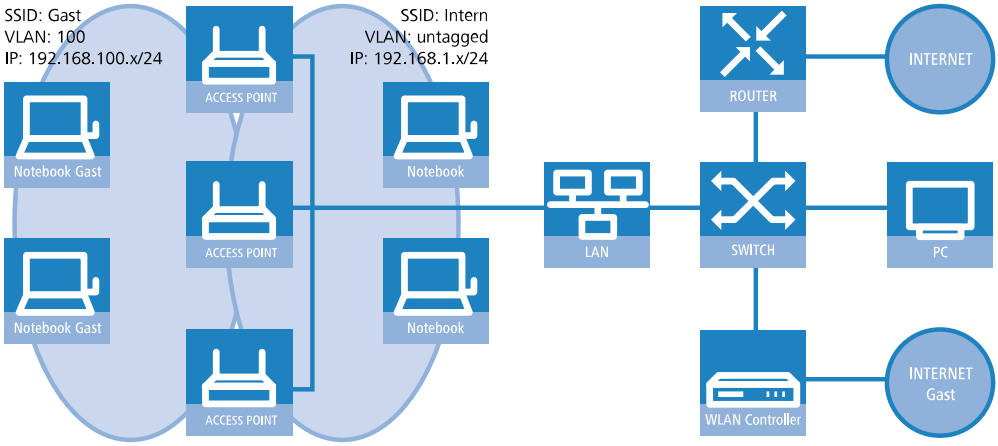
In vielen Unternehmen ist es erwünscht, den Besuchern für die mitgebrachten Notebooks o. ä. einen Internetzugang über WLAN anzubieten. In einem größeren Netzwerk mit mehreren Access Points kann die Konfiguration der nötigen Einstellungen zentral im WLAN Controller erfolgen.

Ziele

- Nutzung der WLAN-Infrastruktur für interne Mitarbeiter und Gäste
- Nutzung der gleichen physikalischen Komponenten (Kabel, Switche, Access Points)
- Trennung der Netzwerke über VLAN und ARF
- Auskopplung der Datenströme zu bestimmten Zielnetzwerken:
  - Gäste: nur Internet
  - Interne Mitarbeiter: Internet sowie alle lokalen Geräte und Dienste
- Gäste melden sich über ein Webformular am WLAN an.
- Interne Mitarbeiter nutzen die WLAN-Verschlüsselung zur Authentifizierung.

Aufbau

- Die Verwaltung der Access Points erfolgt zentral über den WLC.
- Der WLC dient als DHCP-Server für die WLAN-Clients des Gastnetzes.
- Für das Gastnetz wird der Internetzugang vom WLC (z. B. separater DSL Zugang oder Internetzugang über Firmen-DMZ) bereitgestellt.
- Die kabelgebundene Infrastruktur basiert auf gemanagten VLAN-fähigen Switches:
  - Das VLAN-Management der Access Points erfolgt über den WLC.
  - Das VLAN-Management der Switches erfolgt separat über die Switch-Konfiguration.
- Die Access Points werden innerhalb des internen VLANs betrieben.

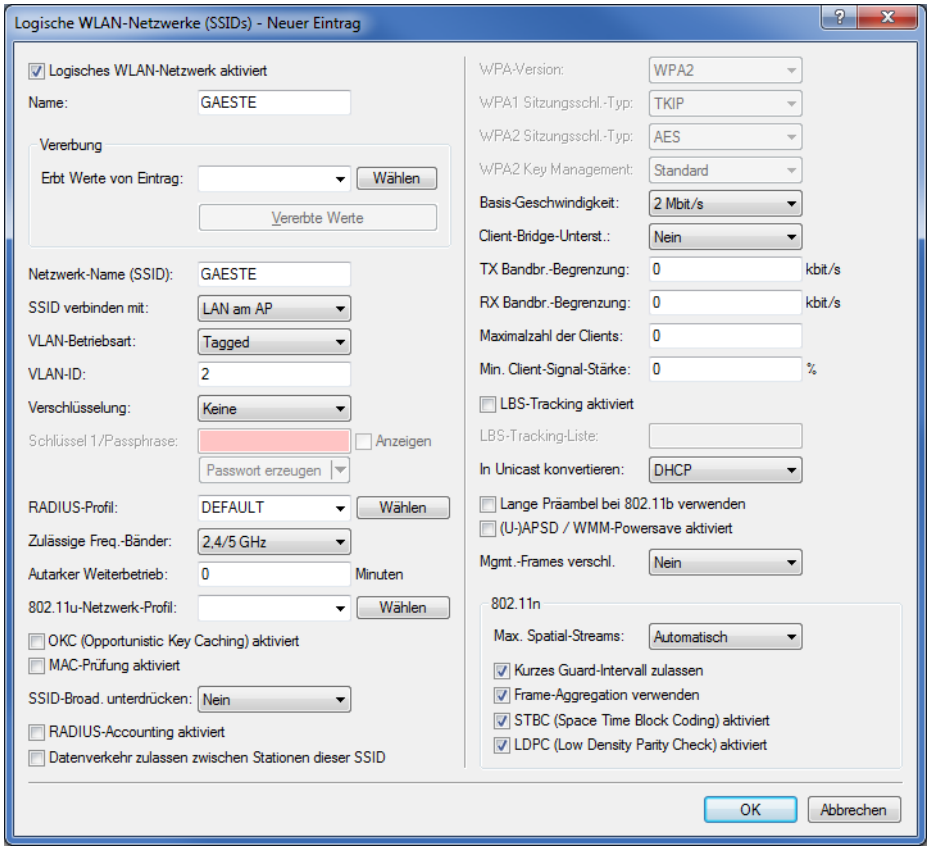


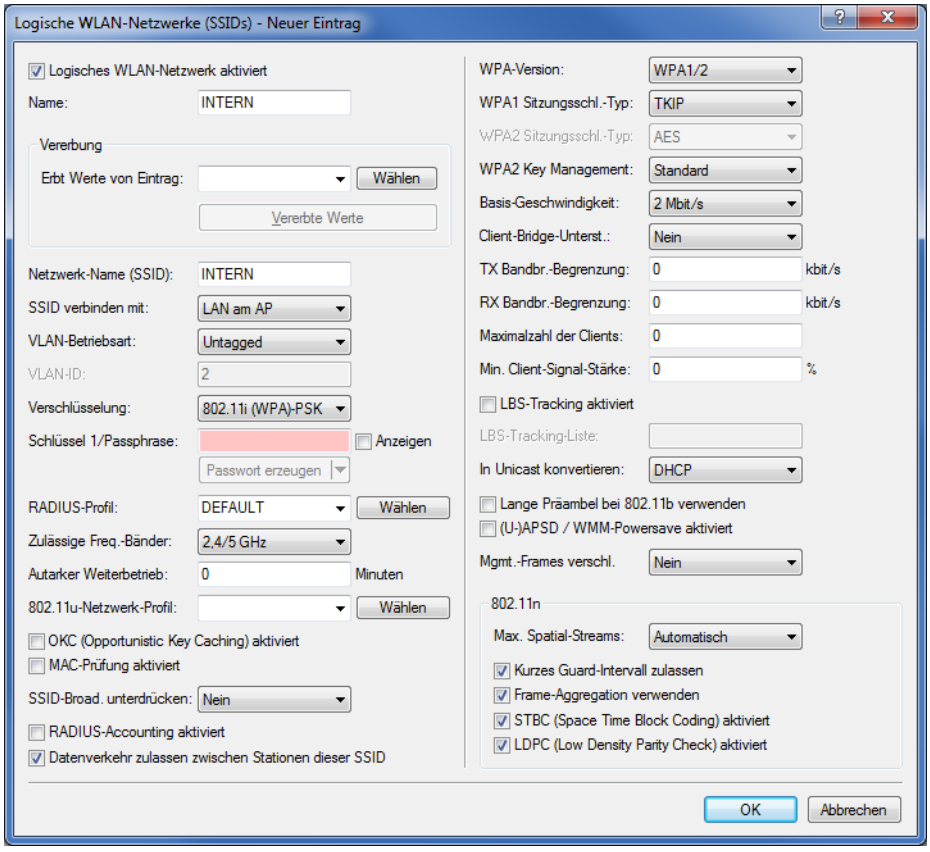
WLAN-Konfiguration des WLAN Controllers

Bei der WLAN-Konfiguration definieren Sie die benötigten WLAN-Netzwerke und weisen sie zusammen mit den physikalischen WLAN-Einstellungen den vom Controller verwalteten Access Points zu.

1. Erstellen Sie ein logisches WLAN für die Gäste und eines für die internen Mitarbeiter.
   - Das WLAN mit der SSID `GAESTE` erhält die VLAN-ID `100` (VLAN-Betriebsart **Tagged**) und verwendet **Keine** Verschlüsselung.
   - Das WLAN mit der SSID `INTERN` erhält keine VLAN-ID (VLAN-Betriebsart **Untagged**, d. h. Datenpakete werden ohne VLAN-Tag in das Ethernet übertragen) und verwendet eine Verschlüsselung nach WPA, z. B. **802.11i (WPA)-PSK**.

› LANconfig: **WLAN-Controller** > **Profile** > **Logische WLAN-Netzwerke (SSIDs)**

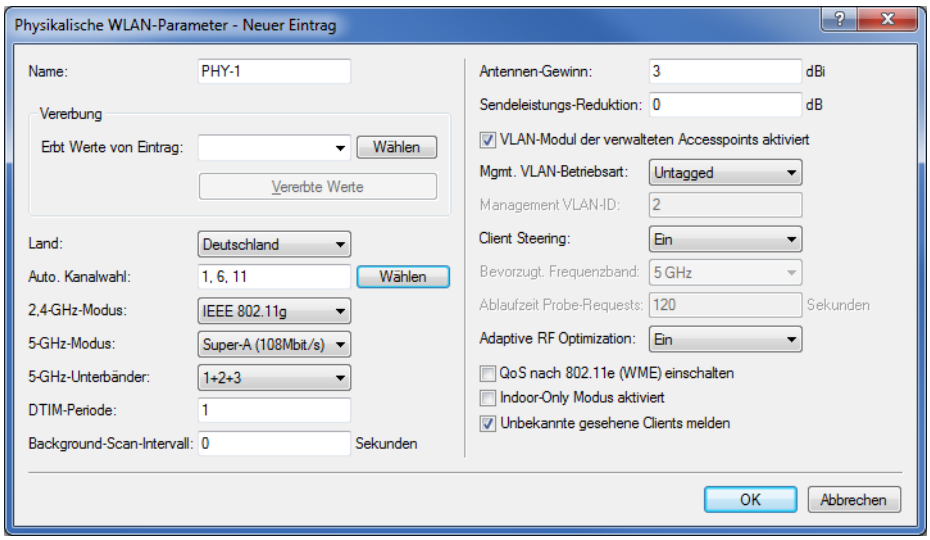




Wenn Sie die **VLAN-Betriebsart** auf **Untagged** stellen, graut LANconfig das Eingabefeld **VLAN-ID** im oben gezeigten Hinzufügen-/Bearbeiten-Dialog aus. Die dazugehörige Tabelle **Logische WLAN-Netzwerke (SSIDs)** zeigt als zugewiesene VLAN aber trotzdem den im ausgegrauten Feld ausgewiesenen Wert an. Dieser Eintrag ist lediglich programmintern, da der zulässige Wertebereich zwischen 2 und 4094 liegt. Letztlich entscheidend ist die VLAN-Betriebsart: Wenn diese auf **Untagged** steht, wird in keinem Fall eine VLAN-ID übertragen.

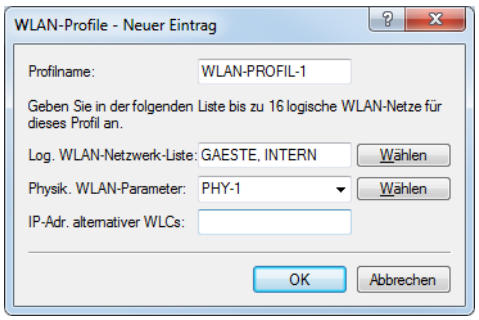
2. Erstellen Sie einen Satz von physikalischen Parametern für die verwendeten Access Points.
Dabei wird die Management-VLAN-ID auf `1` gesetzt, um die VLAN-Nutzung generell zu aktivieren (jedoch ohne separates Management-VLAN für das Gerät; der Management-Datenverkehr wird ungetagged übertragen).

   › LANconfig: **WLAN-Controller** > **Profile** > **Physikalische WLAN-Parameter**



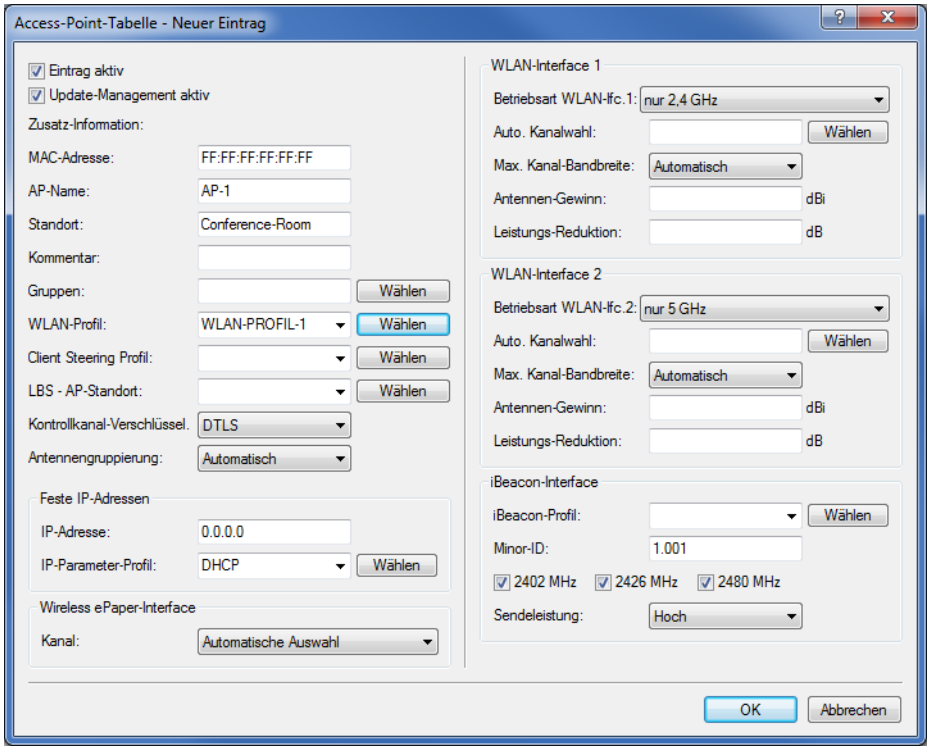
3. Erstellen Sie ein WLAN-Profil, welches Sie den Access Points zuweisen.
   Unter diesem WLAN-Profil vereinen Sie die beiden zuvor erstellten logischen WLAN-Netzwerke und den zuvor erstellten Satz von physikalischen Parametern.

   › LANconfig: **WLAN-Controller** > **Profile** > **WLAN-Profile**



4. Ordnen Sie das WLAN-Profil den vom Controller verwalteten Access Points zu.
   Tragen Sie dazu die einzelnen Access Points mit der MAC-Adresse in die Access-Point-Tabelle ein. Alternativ können Sie über die Schaltfläche **Default** auch ein Standardprofil anlegen, das für alle Access Points gilt.

   › LANconfig: **WLAN-Controller** > **AP-Konfig.** > **Access-Point-Tabelle**



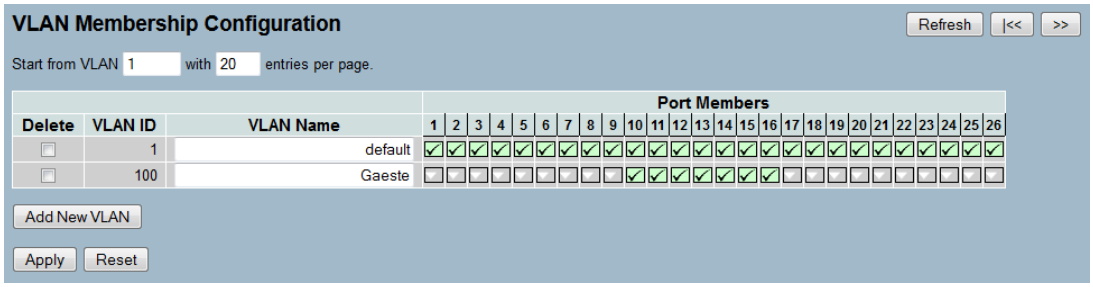
Konfiguration des Switches (LANCOM GS-2326P)

In diesem Kapitel beschreiben die Konfiguration des Switches am Beispiel eines LANCOM GS-2326P.

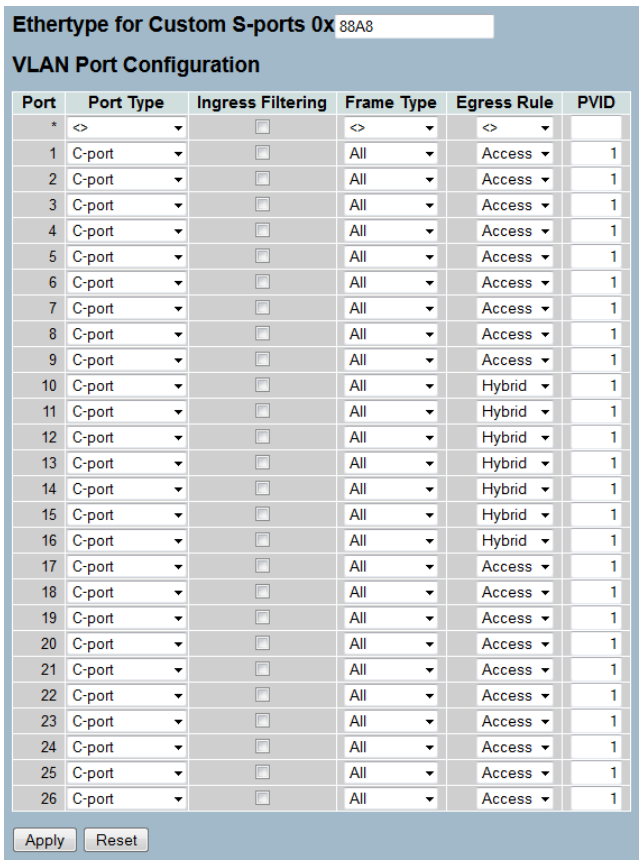
1. Legen Sie unter **Configuration** > **VLAN** > **VLAN-Membership** für das eingerichtete Gäste-Netz eine weitere VLAN-Gruppe an.

   Zur Unterscheidung der VLANs im Switch werden zwei Gruppen verwendet. Das interne Netz für die Mitarbeiter wird in der Gruppe `default` abgebildet, das der Gäste in der Gruppe `Gaeste`.

- Die VLAN-Gruppe für die internen Mitarbeiter verwendet die Default-VLAN-ID `1`. Diese zur internen Verwaltung eingesetzte VLAN-ID gilt auf allen Ports und wird ungetagged betrieben; d. h. alle ungetaggt eingehenden Datenpakete erhalten für das interne Routing die VLAN-ID 1, welche bei ausgehenden Datenpaketen wieder entfernt wird (siehe auch "PVID" im nächsten Schritt).
- Die VLAN-Gruppe für die Gäste verwendet die VLAN-ID `100`, die Sie bereits bei der Konfiguration der WLANs im Controller eingetragen haben. Sie gilt nur auf den Ports, an denen der WLAN-Controller und die Access Points angeschlossen sind (in diesem Beispiel: Port 10 bis 16, grüner Haken unter **Port Members**). Bei ausgehenden Datenpaketen entfernt der Switch die Tags nicht; d. h. alle getaggt eingehenden Datenpakete mit der VLAN-ID 100 behalten diesen Tag und werden nur an die Ports geroutet, die Mitglied der entsprechenden Gruppe sind.



2. Stellen Sie unter **Configuration** > **VLAN** > **Ports** den **Port Type** alle Ports auf **C-port**. Details zu dieser Einstellung finden Sie in der Switch-Dokumentation.
3. Konfigurieren Sie die **Egress Rule** für die einzelnen Ports.
   - Alle Ports außer Port 10 bis 16 erhalten die Regel **Access**. Dadurch leiten diese Ports nur ungetaggte Datenpakete weiter, alle anderen werden verworfen.
   - Die Ports 10 bis 16 erhalten die Regel **Hybrid**. Dadurch leiten diese Ports sowohl ungetaggte als auch getaggte Datenpakete weiter.



Achten Sie darauf, dass die **PVID** (Port-VLAN-ID) für jeden Port den Wert `1` besitzt. Die PVID ist die VLAN-ID, die ein Port eingehenden Datenpaketen ohne VLAN-Tag zuweist; daher entspricht die PVID der VLAN-ID der `default`-Gruppe.

4. OPTIONAL: Sofern Sie den Zugang zum Gäste-Netz auch über Ethernet erlauben möchten, stellen Sie unter **Configuration** > **VLAN** > **Ports** z. B. für die Ports 17 bis 20 die **PVID** auf `100`, und weisen unter **Configuration** > **VLAN** > **VLAN-Membership** diese Ports der Gruppe `Gaeste` zu. Dadurch erhalten alle über diese Ports ungetaggt eingehenden Datenpakete die VLAN-ID 100.

Beachten Sie, dass die betreffenden Datenpakete den Switch dann lediglich über die Ports des Gäste-Netzes wieder verlassen können!

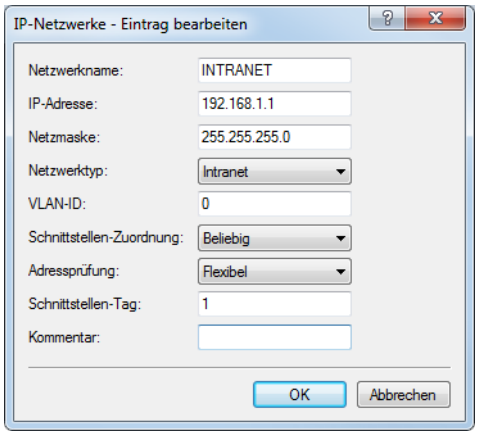
Konfiguration der IP-Netzwerke im WLAN Controller

Für die Trennung der Datenströme auf Layer 3 werden zwei verschiedene IP-Netzwerke verwendet (ARF – Advanced Routing and Forwarding).

1. Stellen Sie für das interne Netzwerk das **INTRANET** auf die Adresse `192.168.1.1` ein.

   Dieses IP-Netzwerk verwendet die **VLAN-ID** `0`. Damit werden alle ungetaggten Datenpakete diesem Netzwerk zugeordnet (das VLAN-Modul des Controllers selbst muss dazu deaktiviert sein). Das **Schnittstellen-Tag** `1` wird für die spätere Auskopplung der Daten im virtuellen Router verwendet.

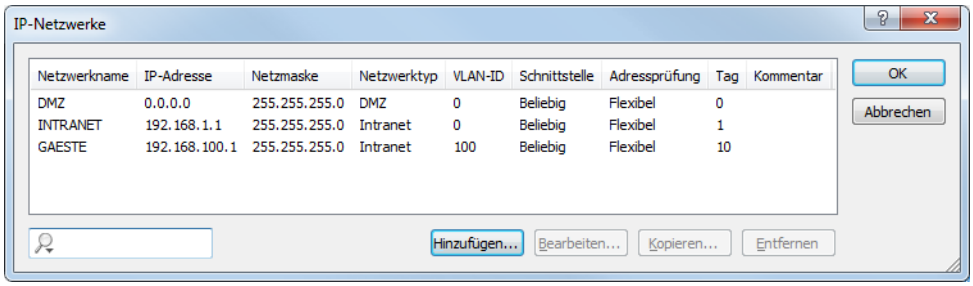
   › LANconfig: **TCP/IP** > **Allgemein** > **IP-Netzwerke**



2. Legen Sie für die Gäste ein neues IP-Netzwerk mit der Adresse `192.168.100.1` an.

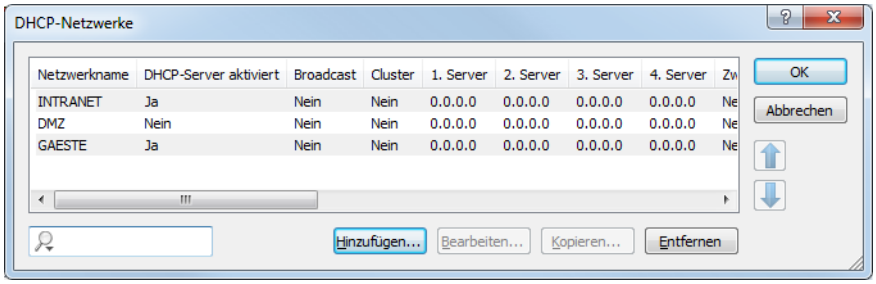
   Dieses Netzwerk verwendet die **VLAN-ID** `100`. Damit werden alle Datenpakete mit dieser ID dem Gäste-Netzwerk zugeordnet. Auch hier dient das **Schnittstellen-Tag** `10` der späteren Verwendung im virtuellen Router.

   › LANconfig: **TCP/IP** > **Allgemein** > **IP-Netzwerke**

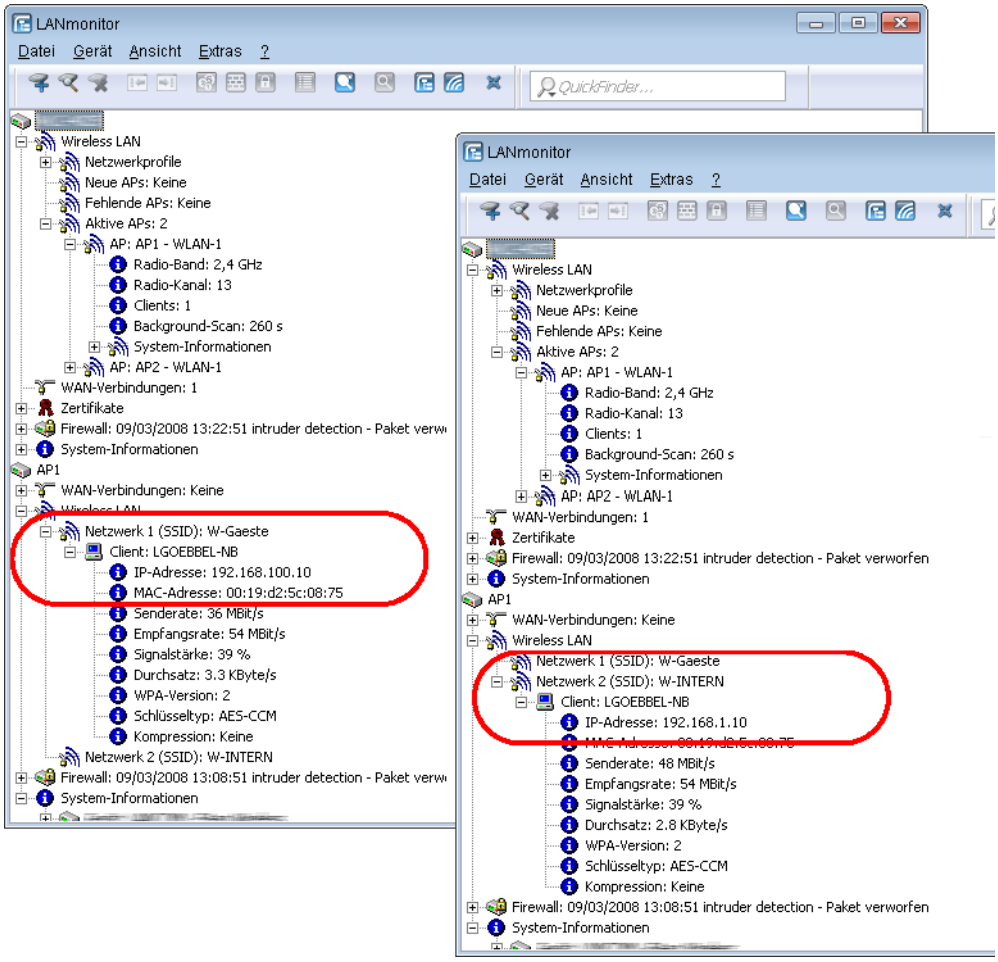


3. Aktivieren Sie für die beiden IP-Netzwerke den DHCP-Server.

› LANconfig: **TCP/IP** > **Allgemein** > **IP-Netzwerke**



Mit diesen Einstellungen können die WLAN-Clients der internen Mitarbeiter und der Gäste gezielt den jeweiligen Netzwerken zugeordnet werden.

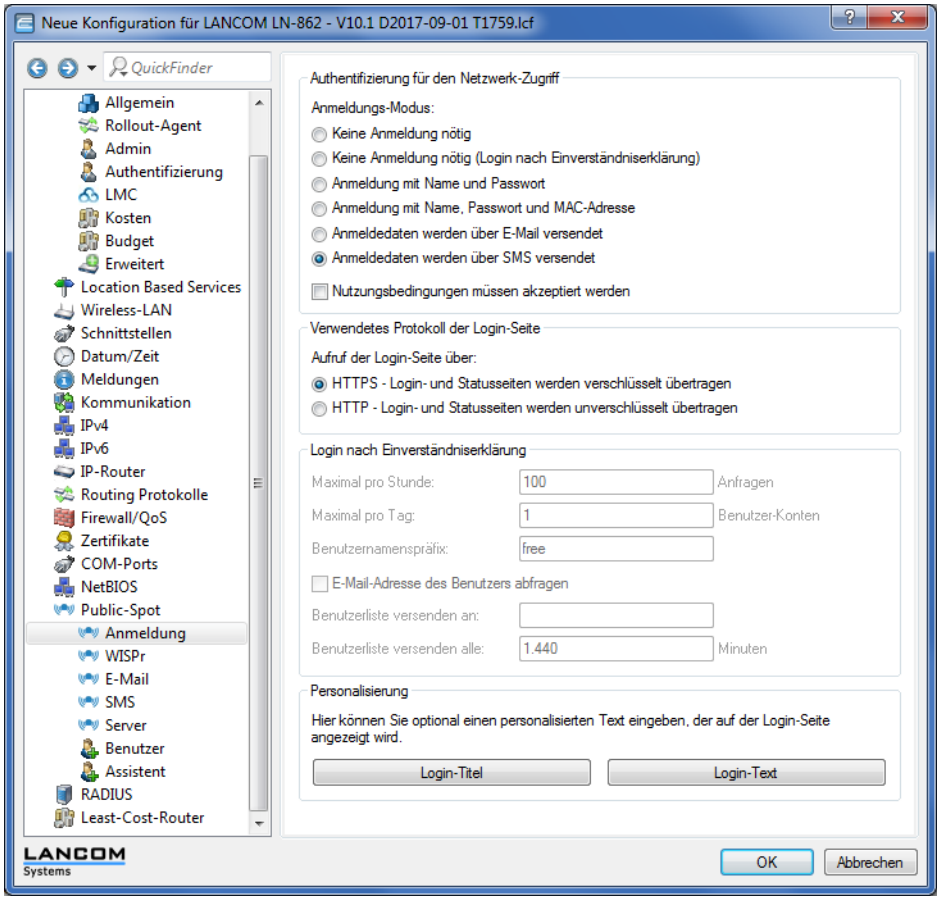


Konfiguration der Public Spot-Zugänge

Mit dem Public Spot bieten Sie einen kontrollierten Zugriffspunkt auf Ihr WLAN. Die Authentifizierung erfolgt durch Benutzerabfrage über ein Webinterface. Bei Bedarf können Sie den Zugang zeitlich begrenzen.

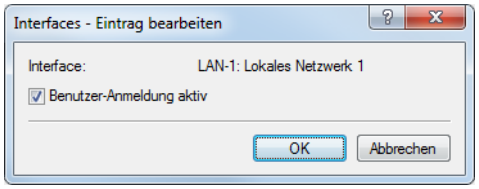
1. Aktivieren Sie die Authentifizierung für den Netzwerk-Zugriff mit Benutzername und Passwort.

› LANconfig: **Public-Spot** > **Anmeldung** > **Authentifizierung für den Netzwerk-Zugriff**



2. Aktivieren Sie die Benutzeranmeldung für das Controller-Interface, über das er mit dem Switch verbunden ist.

   › LANconfig: **Public-Spot** > **Server** > **Betriebseinstellungen** > **Interfaces**

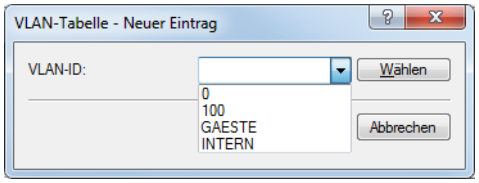


3. Regulieren Sie den Zugang zum Public Spot.

   Mit dem Eintrag der VLAN-ID "100" für das Gäste-Netzwerk in der VLAN-Tabelle beschränken Sie die Public Spot-Verwendung auf Datenpakete aus diesem virtuellen LAN. Alle Datenpakete aus anderen VLANs werden ohne Anmeldung am Public Spot weitergeleitet. Achten Sie dabei auch darauf, dass der WEBconfig-Zugang über das Public Spot-Interface auf die Authentifizierungsseiten beschränkt ist (siehe *Konfigurationszugriff einschränken*).

   Ohne die Einschränkung des Interfaces auf die VLAN-ID ist der Controller auf dem angegebenen physikalischen Ethernet-Port nicht mehr erreichbar!

› LANconfig: **Public-Spot** > **Server** > **VLAN-Tabelle**



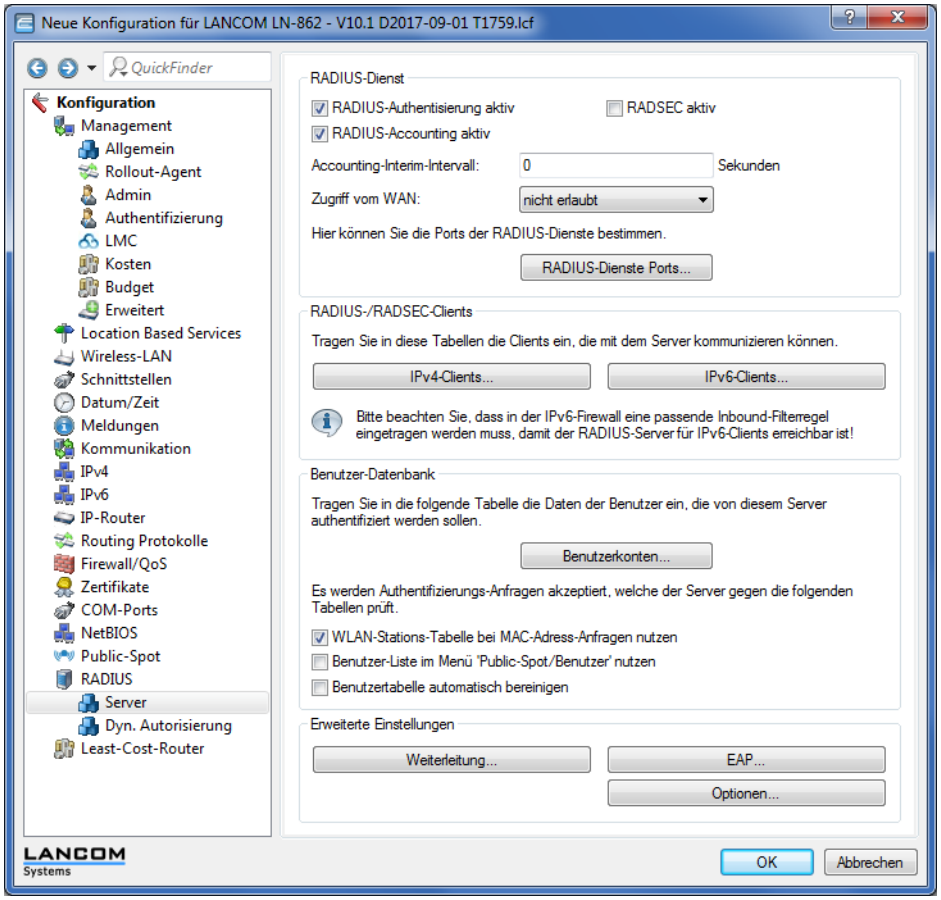
4. Aktivieren Sie die Option zum Bereinigen der Benutzertabelle, damit das Gerät nicht mehr benötigte Einträge automatisch löscht.

   › LANconfig: **RADIUS** > **Server** > **Benutzer-Datenbank** > **Benutzertabelle automatisch bereinigen**

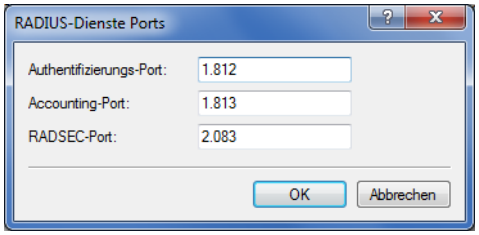
Internen RADIUS-Server für Public Spot-Nutzung konfigurieren

Der Assistent speichert die Public Spot-Zugänge in der Benutzerdatenbank des internen RADIUS-Servers. Damit Sie diese Public Spot-Zugänge nutzen können, wurde der interne RADIUS-Server standardmäßig vorkonfiguriert. Dies können Sie in **LANconfig** wie folgt einsehen:

1. Navigieren Sie zu **RADIUS** > **Server** > **RADIUS-Dienst**.
2. Stellen Sie sicher, dass die Häkchen für **RADIUS-Authentisierung aktiv** und **RADIUS-Accounting aktiv** gesetzt sind.



3. Klicken Sie die Schaltfläche **RADIUS-Dienste Ports**.

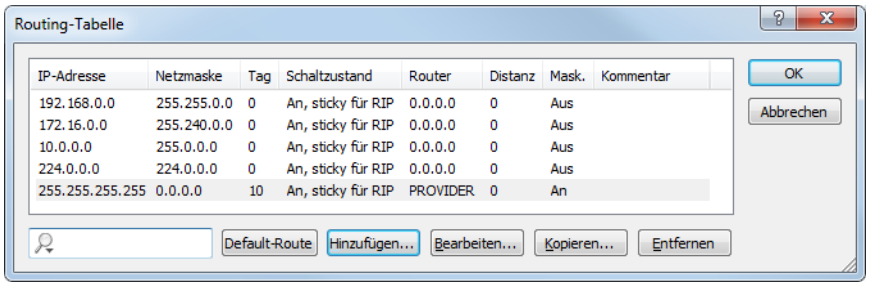


Hier sehen Sie die Default-Einstellungen.

Konfiguration des Internetzugangs für das Gästenetzwerk

1. Um den Benutzern des Gast-Netzes einen Internetzugang bereitzustellen, nutzen Sie z. B. den Assistenten für die Einrichtung eines Zugangs zum Providernetz.
2. Beschränken Sie den Zugang zum Providernetz.
   Damit dieser Zugang nur für die Benutzer im Gästenetzwerk zur Verfügung steht, vergeben Sie der entsprechenden Route das Routing-Tag "10". Damit können nur Datenpakete aus dem IP-Netzwerk "GAESTE" mit dem Schnittstellen-Tag "10" in das Netz des Providers übertragen werden. Das Routing zwischen dem Gäste-Netzwerk und dem internen Netzwerk ist aufgrund der unterschiedlichen Routing-Tags ausgeschlossen.

   › LANconfig: **IP-Router** > **Routing** > **Routing-Tabelle**



3. Optional: Laden Sie im LANconfig ggf. über **Gerät** > **Konfigurations-Verwaltung** > **Zertifikat oder Datei hochladen** eine HTML-Vorlage und ein Bild als Vorlage für die Ausgabe der Vouchers in das Gerät.
   Das Bild kann als GIF, JPEG oder PNG vorliegen und darf maximal 64 KB groß sein.

14.4.3.6 WLAN Layer-3 Tunneling

Einleitung

Der CAPWAP-Standard für das zentrale WLAN-Management bietet zwei verschiedene Übertragungskanäle an:

› Der obligatorische Kontrollkanal überträgt Verwaltungsdaten zwischen dem verwalteten AP und dem WLC.
› Der optionale Datenkanal überträgt die Nutzdaten aus den jeweiligen WLAN-Netzwerken (SSID) zwischen dem verwalteten AP und dem WLC.

Die optionale Nutzung des Datenkanals zwischen dem verwalteten AP und dem WLC entscheidet über den Weg der Nutzdaten:

› Wenn Sie den Datenkanal deaktivieren, leitet der AP die Nutzdaten direkt in das LAN weiter. In diesem Fall steuern Sie die Zuordnung von WLAN-Clients zu bestimmten LAN-Segmenten z. B. über die Zuweisung von VLAN-IDs. Der Vorteil dieser Anwendung liegt vor allem in der geringen Belastung des WLCs und des gesamten Netzwerks, weil der AP ausschließlich die Verwaltungsdaten über den CAPWAP-Tunnel überträgt, während er die Nutzdaten auf dem kürzesten Weg überträgt.

- Wenn Sie den Datenkanal aktivieren, leitet der AP auch die Nutzdaten an den zentralen WLC weiter. Dieser Ansatz hat folgende Vorteile:
  - Die APs können Netzwerke anbieten, die nur auf dem WLC verfügbar sind, z. B. einen zentralen Internetzugang für einen Public Spot.
  - Die von den APs angebotenen WLANs (SSIDs) sind auch ohne die Nutzung von VLAN voneinander separiert verfügbar. Der Verzicht auf VLAN reduziert den Aufwand für die Konfiguration der anderen Netzwerkkomponenten wie Switches etc.
  - Die an den APs in verschiedenen IP-Netzwerken angemeldeten WLAN-Clients können ohne Unterbrechung der IP-Verbindung zu einem anderen AP roamen, weil die Verbindung fortlaufen vom zentralen WLC verwaltet wird und nicht vom AP (Layer-3-Roaming).

Mit der Nutzung des Datenkanals entstehen auf der Basis der vorhandenen, physikalischen Netzwerkstruktur zusätzliche logische Netzwerke, die so genannten Overlay-Netzwerke.

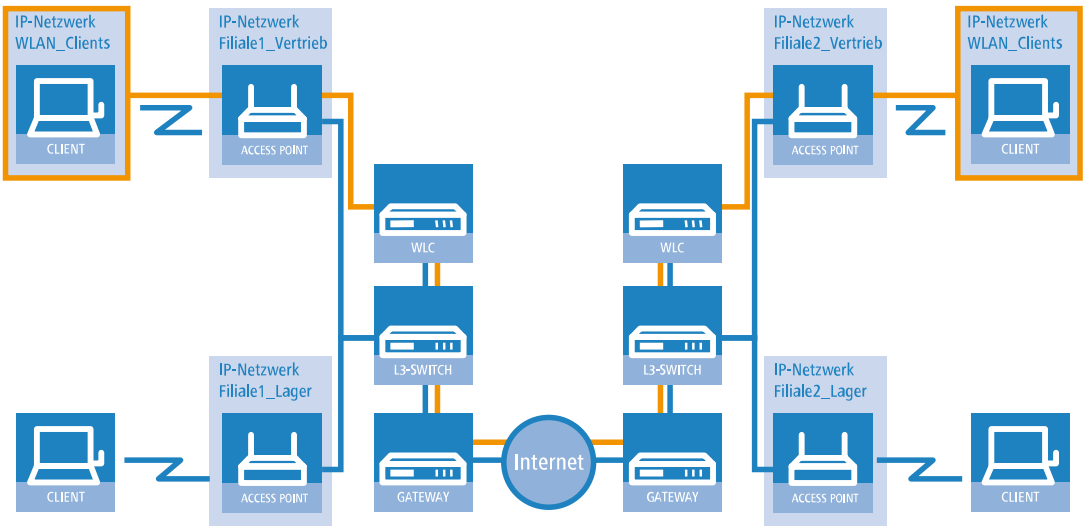


Abbildung 20: Overlay-Netzwerk über mehrere IP-Netzwerke hinweg

Über den Datenkanal können Sie so sogar über mehrere WLCs hinweg logische Overlay-Netzwerke aufspannen.

Mehrere WLCs innerhalb einer Broadcast-Domäne können das gleiche Overlay-Netzwerk unterstützen. Deaktivieren Sie den WLC-Datenkanal zwischen diesen WLCs (WEBconfig: LCOS-Menübaum > Setup > WLAN-Management > WLC-Cluster > WLC-Daten-Tunnel-aktiviert). Der mehrfache Empfang der Broadcast-Nachrichten führt ansonsten zu Schleifen. Da Router die Broadcast-Nachrichten verwerfen, haben Sie für WLC in getrennten Netzen die Möglichkeit, den CAPWAP-Datenkanal zu aktivieren.

Die APs nutzen virtuelle WLC-Schnittstellen (WLC-Tunnel), um die Datenkanäle der jeweiligen SSIDs zwischen dem AP und dem WLC zu verwalten. Jeder WLC bietet je nach Modell 16 bis 32 WLC-Tunnel an, die Sie bei der Konfiguration der logischen WLANs nutzen können.

Die Geräte bieten die virtuellen WLC-Schnittstellen in allen Dialogen zur Auswahl von logischen Schnittstellen an (LAN oder WLAN), z. B. in den Port-Tabellen der LAN- und VLAN-Einstellungen oder bei der Definition von IP-Netzwerken.

Tutorials

In den folgenden Abschnitten finden Sie konkrete Szenarien mit Schritt-für-Schritt Anleitungen für eine Reihe von Standard-Szenarien beim Einsatz von WLCs.

"Overlay Netzwerk": Netzwerke für Access Points trennen ohne VLAN

Die Trennung von Netzwerken in einer gemeinsam genutzten physikalischen Infrastruktur basiert in vielen Fällen auf dem Einsatz von VLANs. Dieses Verfahren setzt allerdings voraus, dass die eingesetzten Switches VLAN-fähig sind und dass in allen Switches die entsprechenden VLAN-Konfigurationen durchgeführt werden. Der Administrator rollt die VLAN-Konfiguration in diesem Beispiel also über das gesamte Netzwerk aus.

Mit einem WLC können Sie die Netze auch mit minimalem Einsatz von VLANs trennen. Über einen CAPWAP-Datentunnel leiten die APs die Nutzdaten der angeschlossenen WLAN-Clients direkt zum WLC, der die Daten den entsprechenden VLANs zuordnet. Die VLAN-Konfiguration beschränkt sich dabei auf den WLC und einen einzigen zentralen Switch. Alle anderen Switches arbeiten in diesem Beispiel ohne VLAN-Konfiguration.

Mit dieser Konfiguration reduzieren Sie das VLAN auf den Kern der Netzstruktur (in der Grafik blau hinterlegt dargestellt). Darüber hinaus erfordern lediglich 3 der genutzten Switch-Ports eine VLAN-Konfiguration.

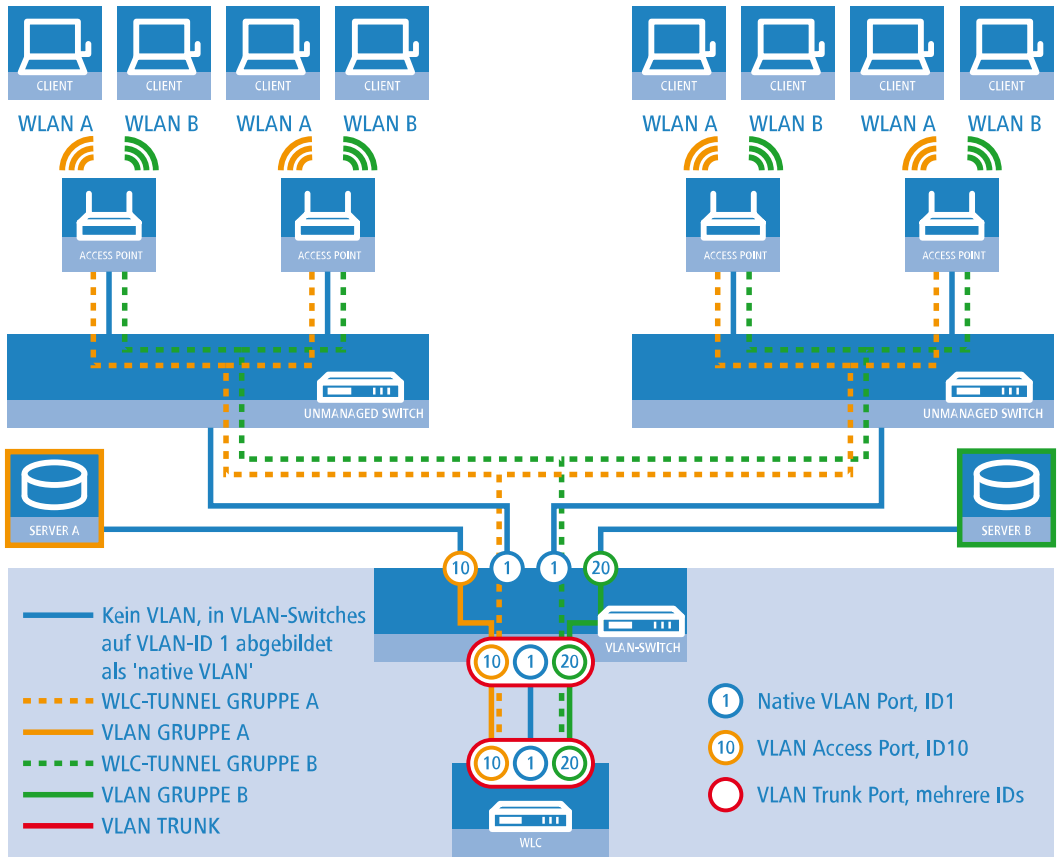


Abbildung 21: Anwendungsbeispiel Overlay-Netz

Die Grafik zeigt ein Anwendungsbeispiel mit den folgenden Komponenten:

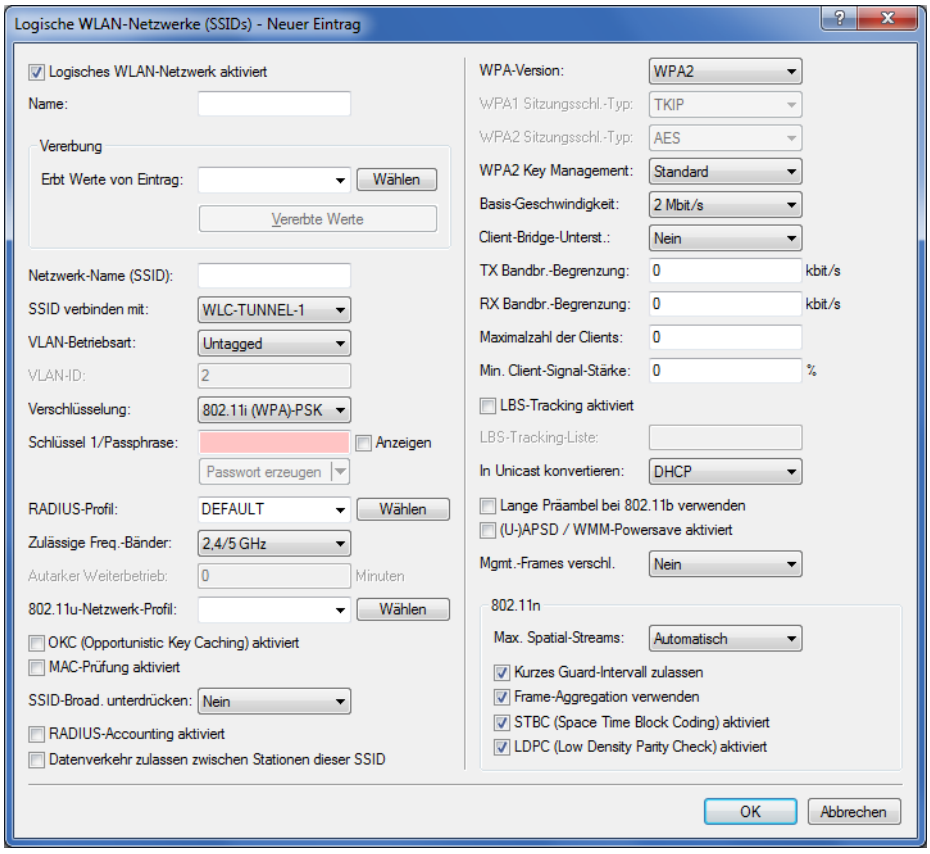
- Das Netz besteht aus zwei Segmenten mit jeweils einem eigenen (nicht unbedingt VLAN-fähigen) Switch.
- In jedem Segment stehen mehrere APs, angeschlossen an den jeweiligen Switch.
- Jeder AP bietet zwei SSIDs für die WLAN-Clients aus verschiedenen Benutzergruppen an, in der Grafik dargestellt in Grün und Orange.
- Jede der Benutzergruppen hat Zugang zu einem eigenen Server, der vor dem Zugriff aus anderen Benutzergruppen getrennt ist. Die Server sind nur durch die auf dem Switch konfigurierten Access-Ports über die entsprechenden VLANs erreichbar.
- Ein WLC verwaltet alle APs in Netz.
- Ein zentraler, VLAN-fähiger Switch verbindet die Switches der Segmente, die gruppenbezogenen Server und den WLC.

Das Ziel der Konfiguration: Ein WLAN-Client, der sich an einer bestimmten SSID anmeldet, soll Zugang zu "seinem" Server haben – unabhängig vom verwendeten AP und unabhängig vom Segment, in dem er sich gerade befindet.

Die folgende Beschreibung basiert auf einer funktionsfähigen Grundkonfiguration des WLCs. Die Konfiguration des VLAN-Switches ist nicht Bestandteil dieser Beschreibung.

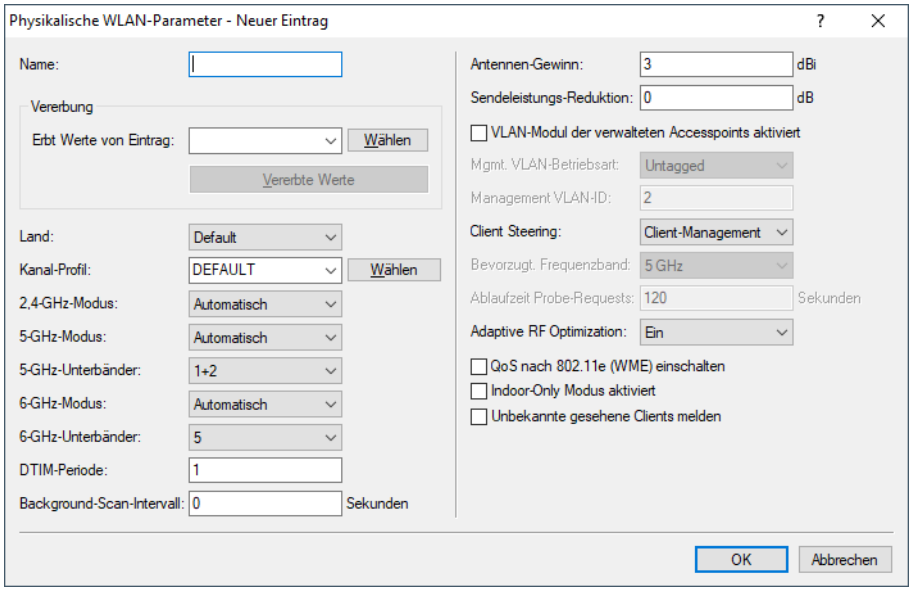
Konfiguration der WLAN-Einstellungen

1. Erstellen Sie für jede SSID einen Eintrag in der Liste der logischen Netzwerke mit einem passenden Namen und der zugehörigen SSID. Verbinden Sie diese SSID mit einem WLC-Tunnel, die erste SSID z. B. mit 'WLC-TUNNEL-1' und die zweite mit 'WLC-TUNNEL-2'. Stellen Sie die VLAN-Betriebsart jeweils auf 'Tagged' mit der VLAN-ID '10' für das erste logischen Netz und der VLAN-ID '20' für das zweite logischen Netz. In LANconfig finden Sie diese Einstellungen unter **Konfiguration** > **WLAN-Controller** > **Profile** > **Logische WLAN-Netzwerke (SSIDs)**.

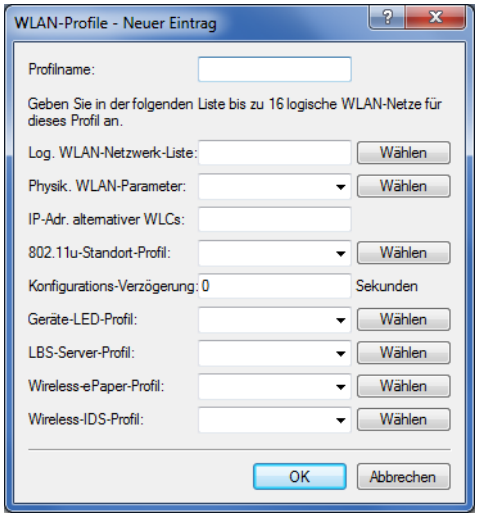


2. Erstellen Sie einen Eintrag in der Liste der physikalischen WLAN-Parameter mit den passenden Einstellungen für Ihre APs, z. B. für das Land 'Europa' mit den Kanälen 1, 6 und 11 im 802.11g/b/n und 802.11a/n gemischten Modus. Aktivieren Sie für dieses Profil der physikalischen WLAN-Parameter die Option, das VLAN-Modul auf den APs einzuschalten. Stellen Sie die Betriebsart für das Management-VLAN in den APs auf 'Ungetagged' ein. In LANconfig

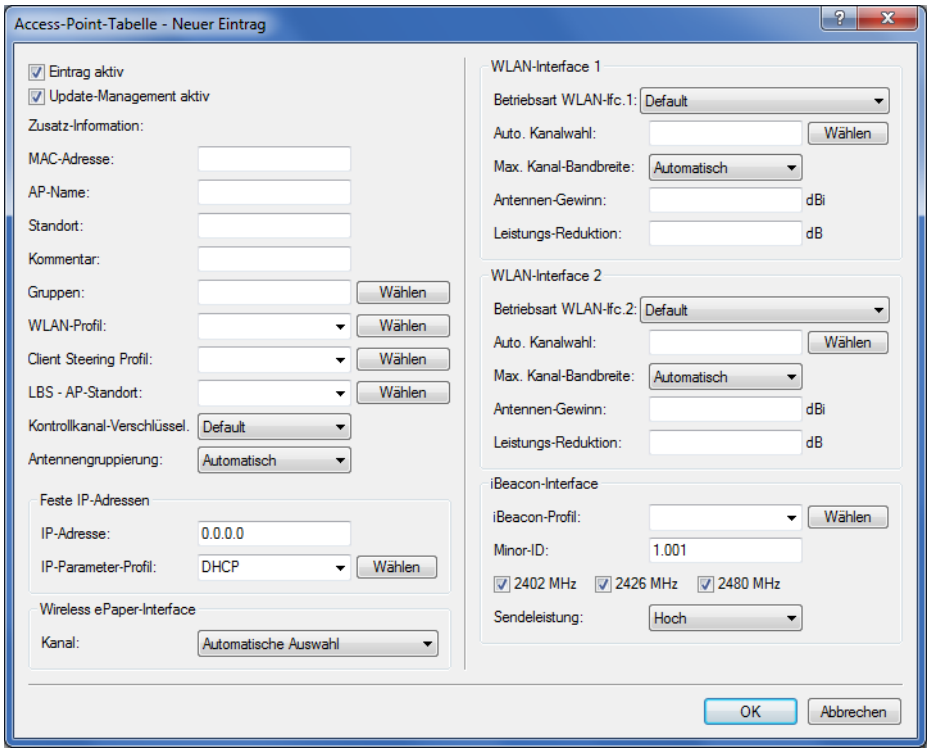
finden Sie diese Einstellungen unter **Konfiguration** > **WLAN-Controller** > **Profile** > **Physikalische WLAN-Parameter**.



3. Erstellen Sie ein WLAN-Profil mit einem passenden Namen und ordnen Sie diesem WLAN-Profil die zuvor erstellten logischen WLAN-Netzwerke und die physikalischen WLAN-Parameter zu. In LANconfig finden Sie diese Einstellungen unter **Konfiguration** > **WLAN-Controller** > **Profile** > **WLAN-Profile**.

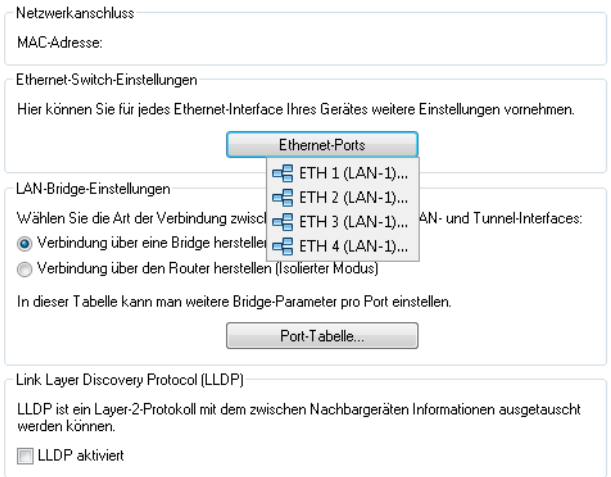


4. Erstellen Sie für jeden verwalteten AP einen Eintrag in der AP-Tabelle mit einem passenden Namen und der zugehörigen MAC-Adresse. Ordnen Sie diesem AP das zuvor erstellte WLAN-Profil zu. In LANconfig finden Sie diese Einstellungen unter **Konfiguration** > **WLAN-Controller** > **AP-Konfig.** > **Access-Point-Tabelle**.



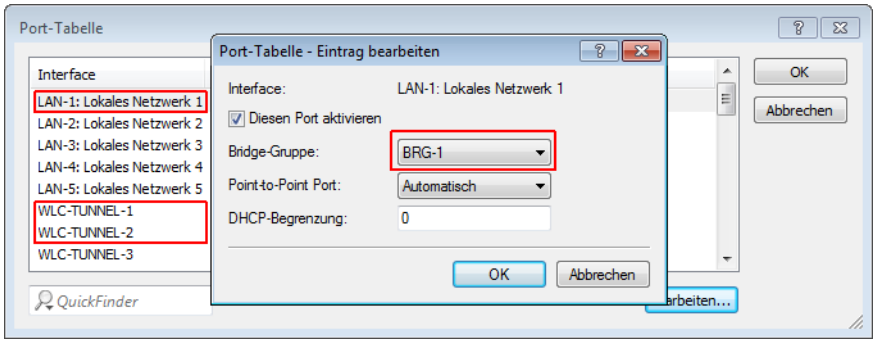
Konfiguration der Schnittstellen am WLC

5. Ordnen Sie jedem physikalischen Ethernet-Port eine separate logische LAN-Schnittstelle zu, z. B. 'LAN-1'. Stellen Sie sicher, dass die anderen Ethernet-Ports nicht der gleichen LAN-Schnittstelle zugeordnet sind. In LANconfig finden Sie diese Einstellungen unter **Konfiguration** > **Schnittstellen** > **LAN** > **Ethernet-Ports**.



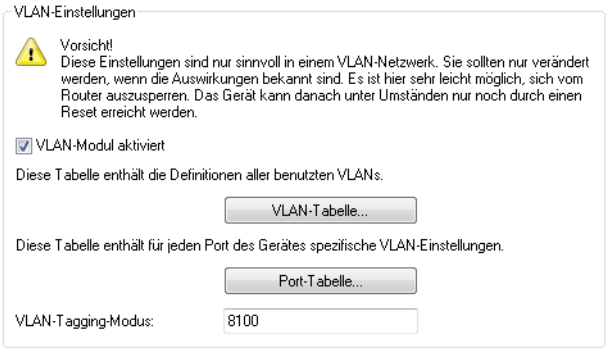
6. Ordnen Sie die logische LAN-Schnittstelle 'LAN-1' und die WLC-Tunnel 'WLC-Tunnel-1' und 'WLC-Tunnel-2' der Bridge-Gruppe 'BRG-1' zu. Stellen Sie sicher, dass die anderen LAN-Schnittstellen nicht der gleichen Bridge-Gruppe

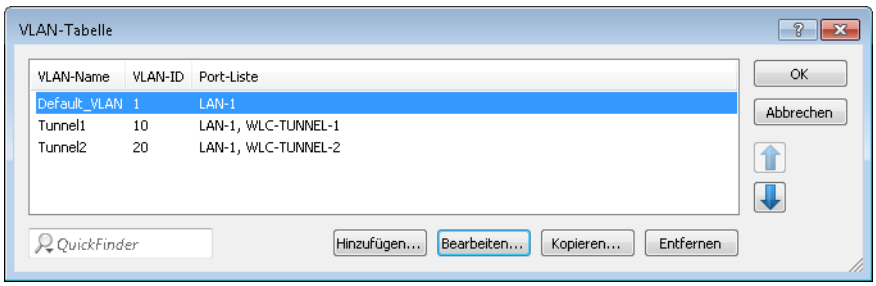
zugeordnet sind. In LANconfig finden Sie diese Einstellungen unter **Konfiguration** > **Schnittstellen** > **LAN** > **Port-Tabelle**.



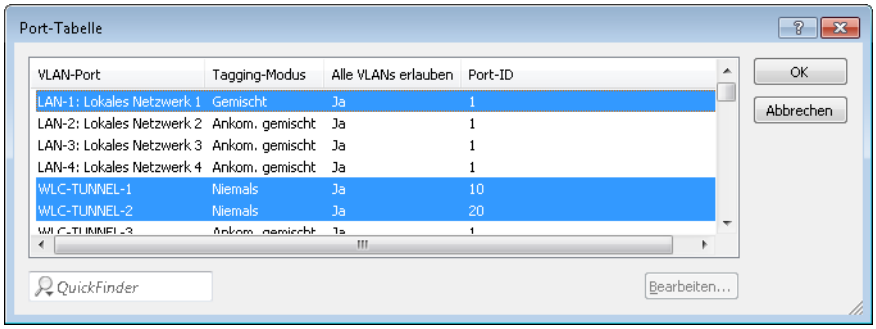
Die LAN-Schnittstellen und WLC-Tunnel gehören standardmäßig keiner Bridge-Gruppe an. Indem Sie die LAN-Schnittstelle 'LAN-1' sowie die beiden WLC-Tunnel 'WLC-Tunnel-1' und 'WLC-Tunnel-2' der Bridge-Gruppe 'BRG-1' zuordnen, leitet das Gerät alle Datenpakete zwischen LAN-1 und den WLC-Tunneln über die Bridge weiter.

7. Aktivieren Sie unter **Schnittstellen** > **VLAN** das VLAN-Modul des WLC und ordnen Sie unter **VLAN-Tabelle** dem gewünschten VLAN den oben gewählten LAN-Port (LAN-1) sowie den passenden WLC-Tunnel zu.





8. Stellen Sie unter **Schnittstellen** > **VLAN** > **Port-Tabelle** den Tagging-Modus der Tunnel-Interfaces sowie des LAN-Interfaces korrekt ein und setzen Sie die passende Port-VLAN-ID.



Je nach Schaltung des Switches konfigurieren Sie den Tagging-Modus des LAN-Interfaces auf 'Gemischt' oder 'Immer'.

Im Normalfall betreibt man die Tunnel-Interfaces im Modus 'Niemals', da Pakete hier (aus dem WLAN) immer ungetaggt ankommen und der WLC sie mit der Port-VLAN-ID versieht.

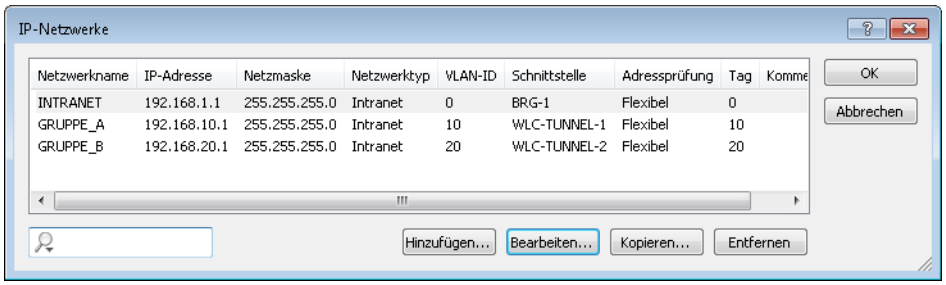
Bitte beachten Sie, dass bei Aktivierung des VLAN-Moduls die auf dem WLC angelegten ARF-Netze eine VLAN-ID erhalten müssen. Soll der WLC das Netz ohne VLAN-Tag erreichen, setzen Sie bei oben stehender VLAN-Konfiguration die '1' als VLAN-ID für das IP-Netz.

Eine ähnliche Konfiguration ist möglich, indem Sie schon am Access Point ein VLAN-Tag für die durch den Tunnel zu leitenden Pakete setzen und das VLAN-Modul des WLC nicht nutzen.

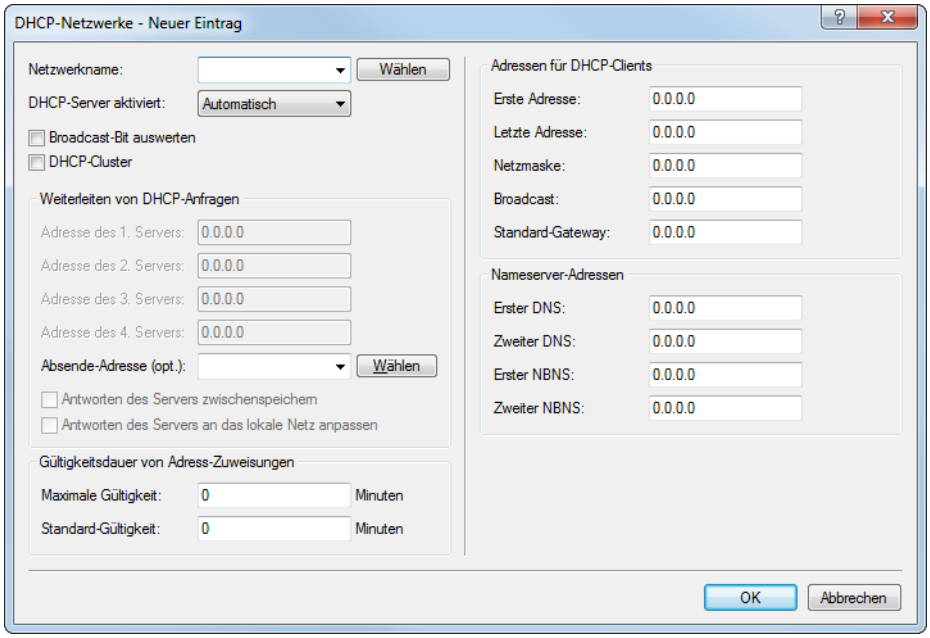
Dabei würde der WLC allerdings durch das Bridgen der verschiedenen WLC-Tunnel untereinander auch Broadcasts in alle Tunnel weiterleiten, was ab einer bestimmten Menge von Tunneln/SSIDs und APs zu Lastproblemen im Netz und auf dem WLC führen kann. Die vorliegende Konfiguration des VLAN-Moduls verhindert das.

9. Ergänzend konfigurieren Sie unter **IPv4** > **Allgemein** > **IP-Netzwerke** für die auf Layer 2 getrennten Netzwerke die IP-Einstellungen.

Damit das Gerät die Netzwerke nicht wieder auf Layer 3 verbindet, ist auch eine Trennung auf Layer 3 erforderlich, z. B. durch ein Schnittstellen-Tag oder durch die Firewall.



10. Der WLC kann optional als DHCP-Server für die APs fungieren. Aktivieren Sie dazu den DHCP-Server für das 'INTRANET'. In LANconfig finden Sie diese Einstellungen unter **IPv4** > **DHCPv4** > **DHCP-Netzwerke**.



"Layer-3-Roaming"

Die Durchleitung der Nutzdaten aus den WLANs über WLC-Tunnel bis zum WLC ermöglicht das Roaming auch über die Grenzen von Broadcast-Domänen hinweg. In diesem Anwendungsbeispiel verhindert ein Layer-3-Switch zwischen den Etagen die Weiterleitung der Broadcasts und trennt so die Broadcast-Domänen.

In diesem Beispiel haben zwei Benutzergruppen A und B jeweils Zugang zu einem eigenen WLAN (SSID). Die APs in mehreren Etagen des Gebäudes bieten die beiden SSIDs 'GRUPPE_A' und 'GRUPPE_B' an.

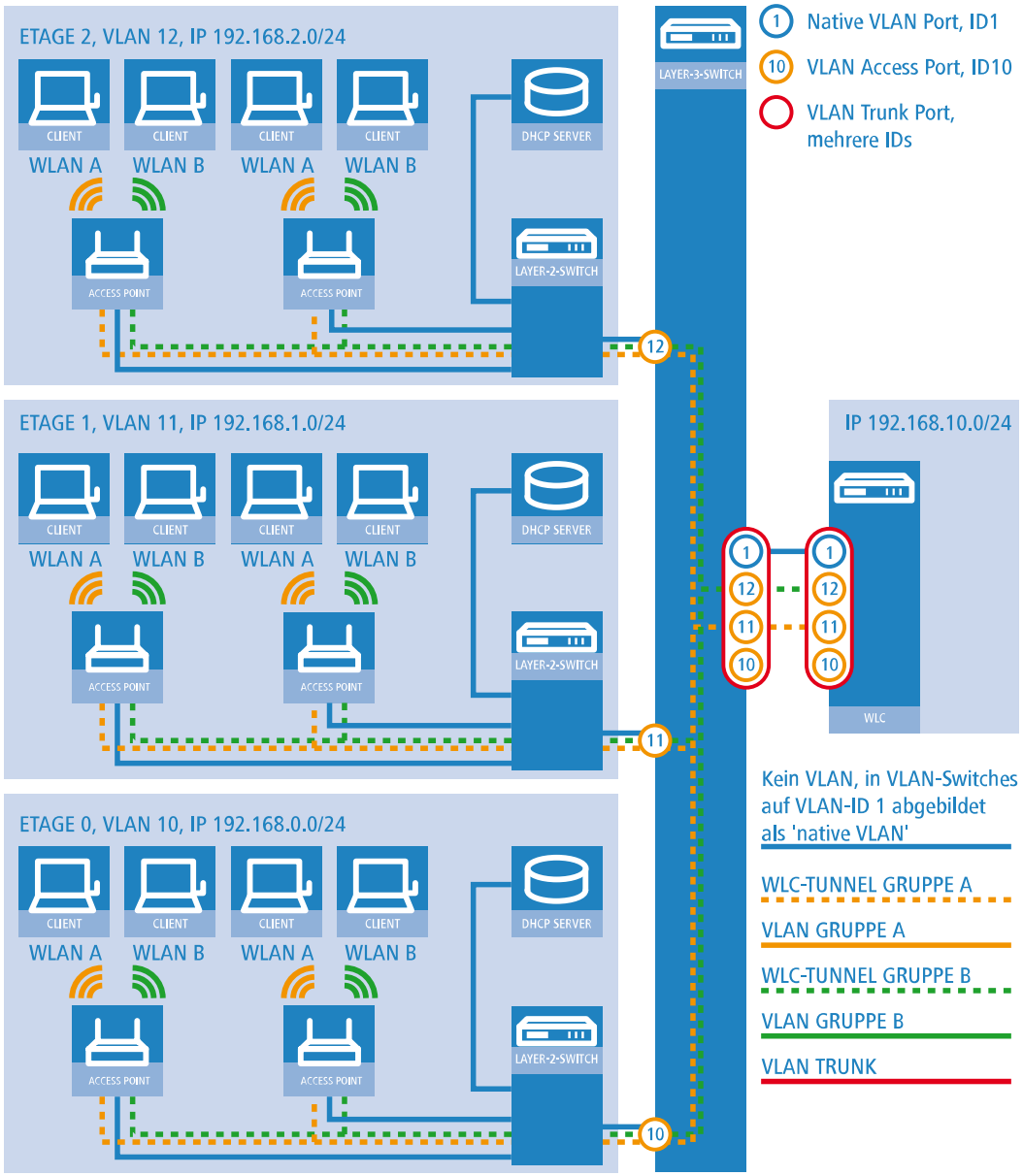


Abbildung 22: Anwendungsbeispiel Layer-3-Roaming

Die Grafik zeigt ein Anwendungsbeispiel mit den folgenden Komponenten:

- Das Netz besteht aus 3 Segmenten in separaten Etagen eines Gebäudes.
- Ein zentraler Layer-3-Switch verbindet die Segmente und teilt das Netzwerk in 3 Broadcast-Domänen auf.
- Jedes Segment nutzt einen eigenen IP-Adressbereich und ein eigenes VLAN.
- In jedem Segment arbeitet ein lokaler DHCP-Server, der den APs die folgenden Informationen übermittelt:
  - IP-Adresse des Gateways
  - IP-Adresse des DNS-Servers
  - Domänen-Suffix

  Die Bereitstellung dieser Informationen ermöglicht es den APs, Kontakt mit dem WLC in einer anderen Broadcast-Domäne aufzunehmen.

Das Ziel der Konfiguration: Ein WLAN-Client, der sich an einer bestimmten SSID anmeldet, soll beim Wechsel der Etage nahtlos Zugang zu "seinem" WLAN behalten – unabhängig vom verwendeten AP und unabhängig vom Segment, in dem er sich gerade befindet. Da die Segmente in diesem Beispiel unterschiedliche IP-Adresskreise nutzen, gelingt das nur durch die Verwaltung der APs auf Layer 3 direkt über den zentralen WLC über die Grenzen der VLANs hinweg.

Die Konfiguration entspricht dem Beispiel *"Overlay Netzwerk": Netzwerke für Access Points trennen ohne VLAN* auf Seite 1175.

WLAN-Controller mit Public Spot

Dieses Szenario basiert auf dem ersten Szenario (Overlay-Netzwerk) und erweitert es um spezifische Einstellungen für eine Benutzer-Authentifizierung.

Die Durchleitung der Nutzdaten aus den WLANs über WLC-Tunnel bis zum WLC ermöglicht eine besonders einfache Konfiguration von Public Spots z. B. für Gäste parallel zu einem intern genutzten WLAN.

In diesem Beispiel haben die Mitarbeiter einer Firma Zugang zu einem eigenen WLAN (SSID), die Gäste erhalten über einen Public Spot ebenfalls Zugang zum Internet. Die APs in allen Bereichen des Gebäudes bieten die beiden SSIDs 'FIRMA' und 'GAESTE' an.

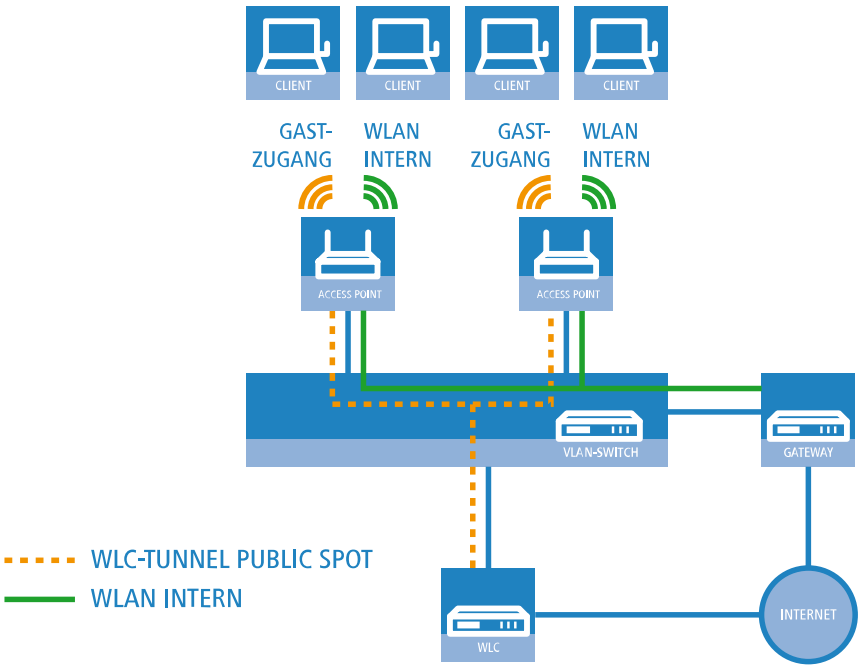
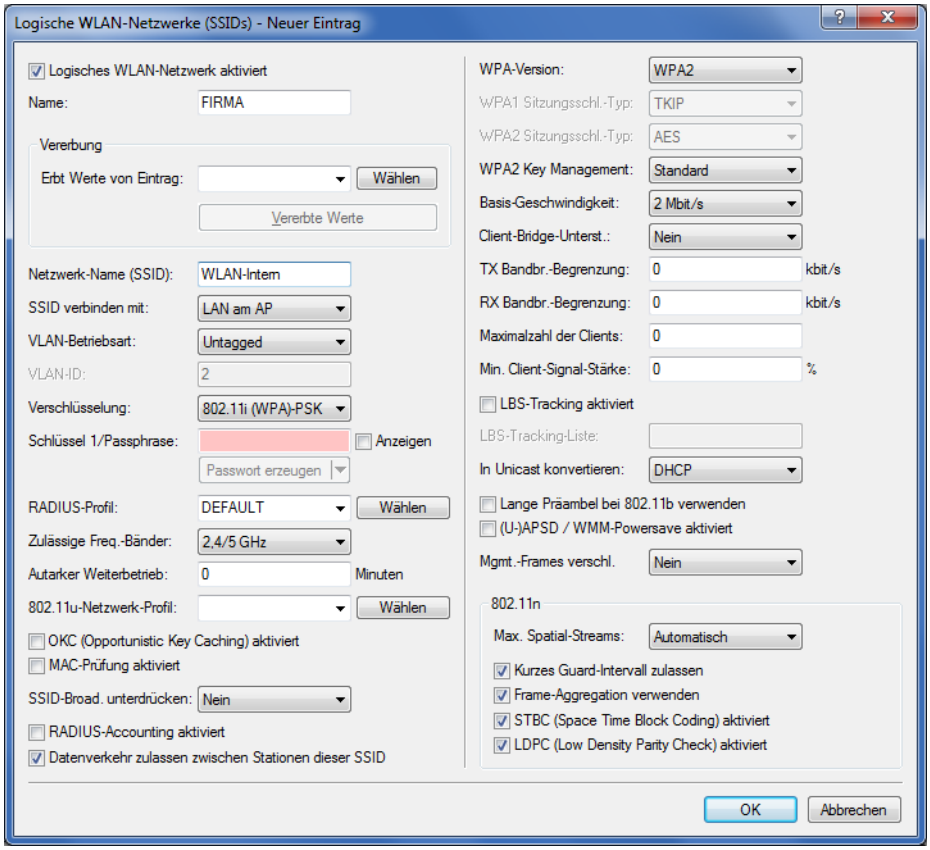


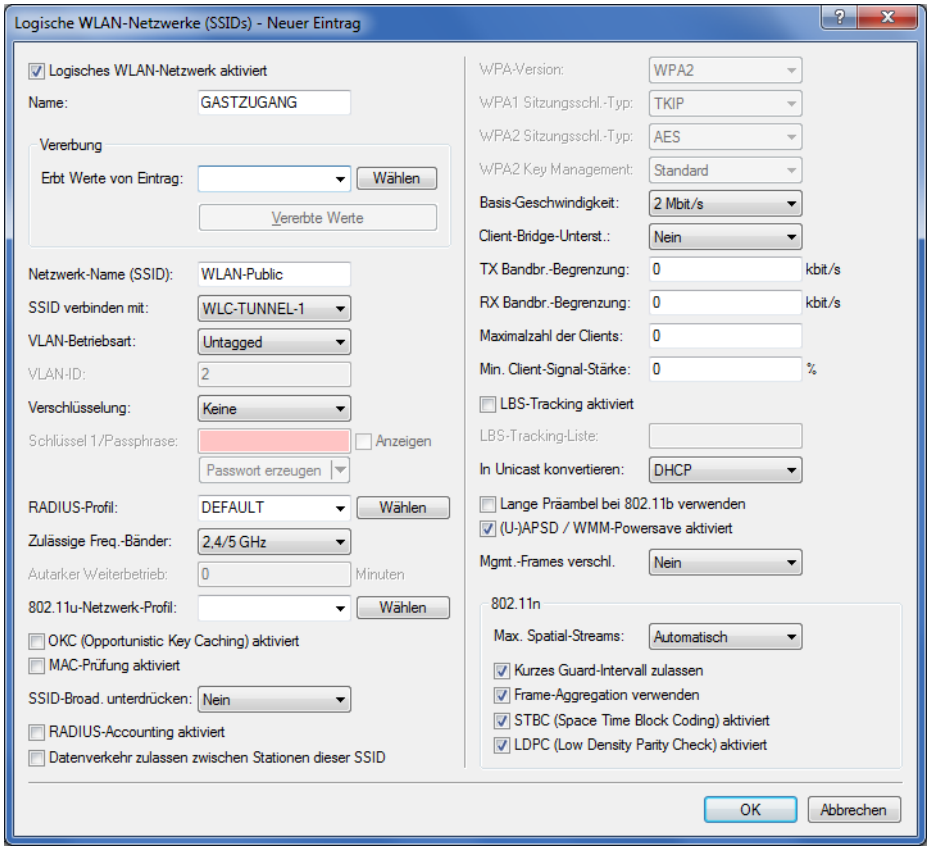
Abbildung 23: Anwendungsbeispiel WLAN-Controller mit Public Spot

Das Ziel der Konfiguration: Ein WLAN-Client, der sich an der internen SSID anmeldet, soll Zugang zu allen internen Ressourcen und zum Internet über das zentrale Gateway erhalten. Die APs koppeln die Nutzdaten der internen Clients lokal aus und leiten sie direkt in das LAN weiter. Die WLAN-Clients der Gäste melden sich am Public Spot an. Die APs leiten die Nutzdaten der Gäste-Clients über einen WLC-Tunnel direkt zum WLC, der über eine separate WAN-Schnittstelle Zugang zum Internet ermöglicht.

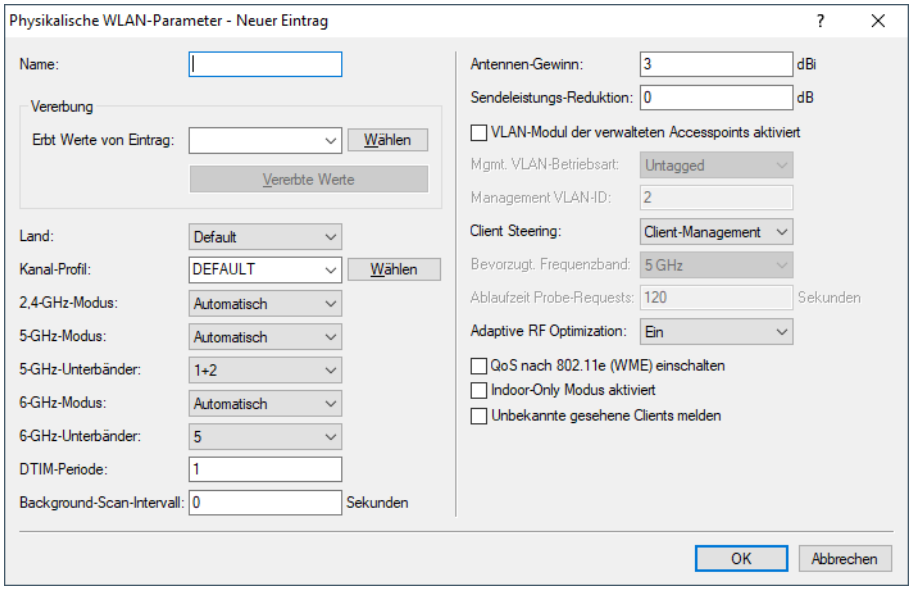
1. Erstellen Sie für das interne WLAN und das Gäste-WLAN jeweils einen Eintrag in der Liste der logischen Netzwerke mit einem passenden Namen und der zugehörigen SSID. Verbinden Sie die SSID für die interne Nutzung mit dem 'LAN am AP', die SSID für die Gäste z. B. mit 'WLC-TUNNEL-1'. Deaktivieren Sie bei der SSID für das Gästenetzwerk die Verschlüsselung, damit sich die WLAN-Clients der Gäste beim Public Spot anmelden können. Unterbinden Sie

für diese SSID außerdem den Datenverkehr der Stationen untereinander (Interstation-Traffic). In LANconfig finden Sie diese Einstellung unter **Konfiguration** > **WLAN-Controller** > **Profile** > **Logische WLAN-Netzwerke (SSIDs)**.

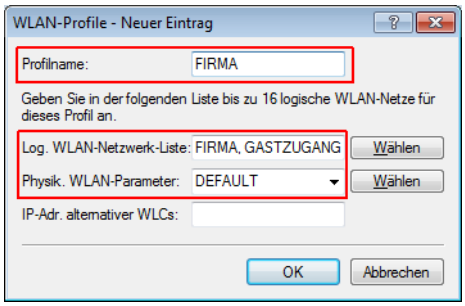




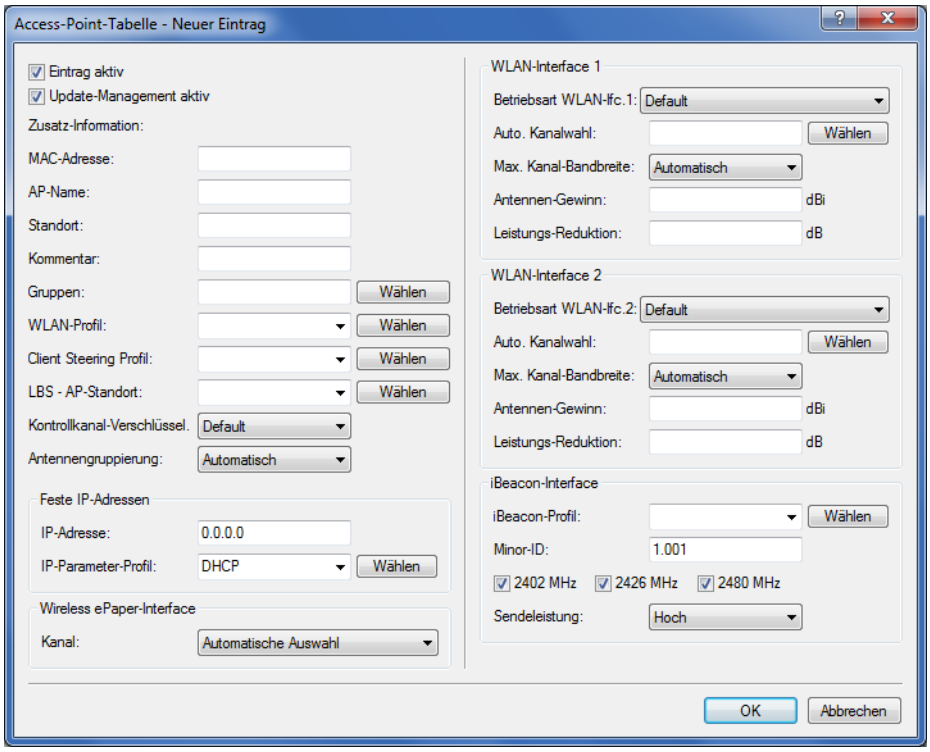
2. Erstellen Sie einen Eintrag in der Liste der physikalischen WLAN-Parameter mit den passenden Einstellungen für Ihre APs, z. B. für das Land 'Europa' mit den Kanälen 1, 6 und 11 im 802.11g/b/n und 802.11a/n gemischten Modus. In LANconfig finden Sie diese Einstellung unter **Konfiguration** > **WLAN-Controller** > **Profile** > **Physikalische WLAN-Parameter**.



3. Erstellen Sie ein WLAN-Profil mit einem passenden Namen und ordnen Sie diesem WLAN-Profil die zuvor erstellten logischen WLAN-Netzwerke und die physikalischen WLAN-Parameter zu. In LANconfig finden Sie diese Einstellung unter **Konfiguration** > **WLAN-Controller** > **Profile** > **WLAN-Profile**.

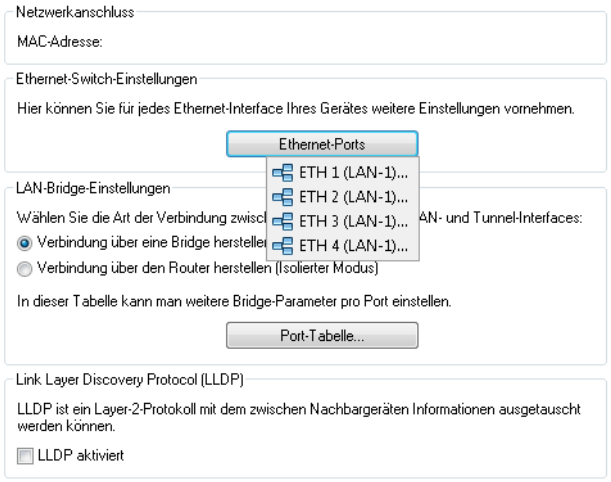


4. Erstellen Sie für jeden verwalteten AP einen Eintrag in der AP-Tabelle mit einem passenden Namen und der zugehörigen MAC-Adresse. Ordnen Sie diesem AP das zuvor erstellte WLAN-Profil zu. In LANconfig finden Sie diese Einstellung unter **Konfiguration** > **WLAN-Controller** > **AP-Konfig** > **Access-Point-Tabelle**.

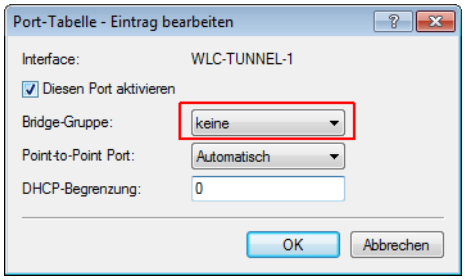


5. Ordnen Sie jedem physikalischen Ethernet-Port eine separate logische LAN-Schnittstelle zu, z. B. 'LAN-1'. Stellen Sie den 4. Ethernet-Port auf die logische LAN-Schnittstelle 'DSL-1' ein. Der WLC verwendet diese LAN-Schnittstelle später

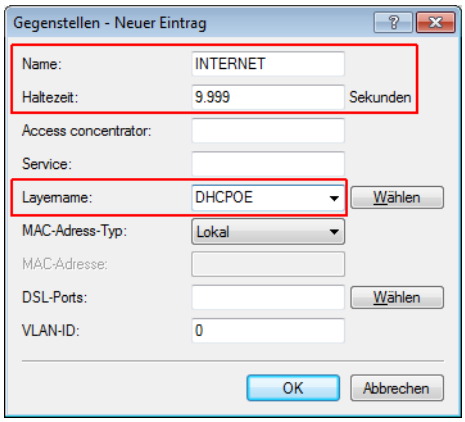
für den Internetzugang des Gästenetzes. In LANconfig finden Sie diese Einstellung unter **Konfiguration** > **Schnittstellen** > **LAN** > **Ethernet-Ports**.



6. Überprüfen Sie, dass die logische LAN-Schnittstelle 'WLC-Tunnel 1' keiner Bridge-Gruppe zugeordnet ist. So stellen Sie sicher, dass die anderen LAN-Schnittstellen keine Daten zum Public Spot-Netzwerk übertragen. In LANconfig finden Sie diese Einstellung unter **Konfiguration** > **Schnittstellen** > **LAN** > **Port-Tabelle**.

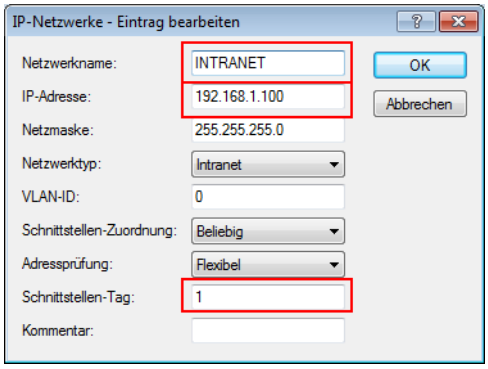


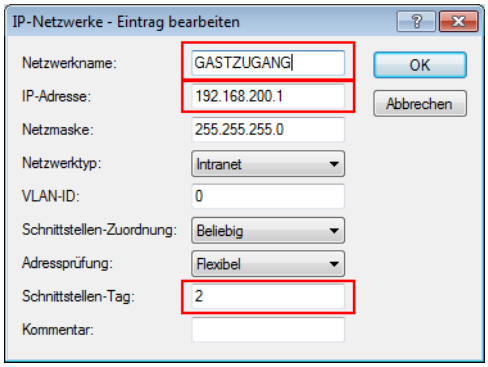
7. Erstellen Sie für den Internetzugang der Gäste einen Eintrag in der Liste der DSL-Gegenstellen mit der Haltezeit '9999' und dem vordefinierten Layer 'DHCPOE'. Dieses Beispiel setzt voraus, dass ein Router mit aktiviertem DHCP-Server den Internetzugang bereitstellt. In LANconfig finden Sie diese Einstellung unter **Konfiguration** > **Kommunikation** > **Gegenstellen** > **Gegenstellen**.



8. Erstellen Sie für die interne Nutzung das IP-Netzwerk 'INTRANET' z. B. mit der IP-Adresse '192.168.1.100' und mit dem Schnittstellen-Tag '1', für die Gäste das IP-Netzwerk 'GASTZUGANG' z. B. mit der IP-Adresse '192.168.200.1' und mit dem Schnittstellen-Tag '2'. Der virtuelle Router im WLC nutzt die Schnittstellen-Tags, um die Routen für die

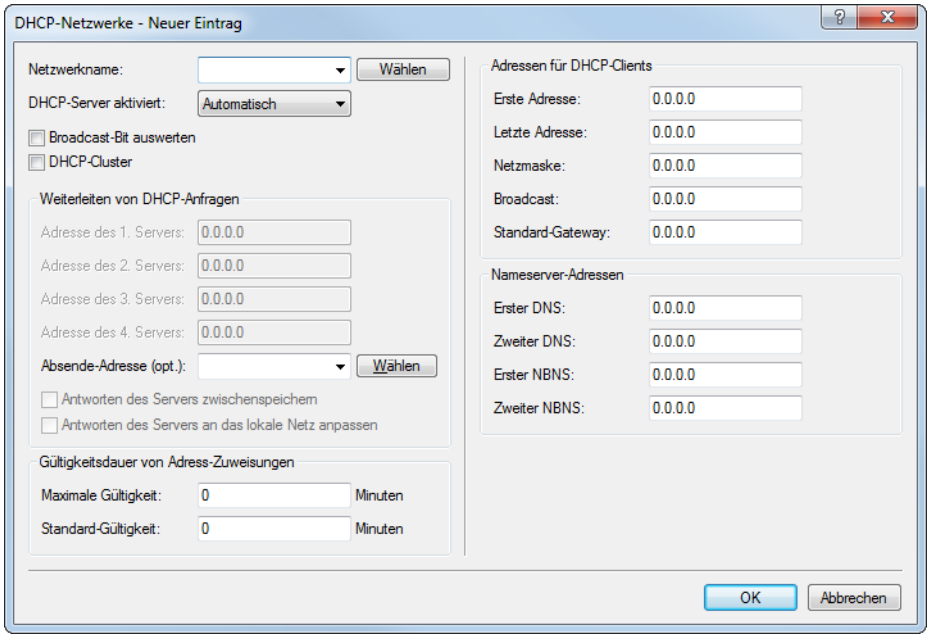
beiden Netzwerke zu trennen. In LANconfig finden Sie diese Einstellung unter **Konfiguration** > **TCP/IP** > **Allgemein** > **IP-Netzwerke**.



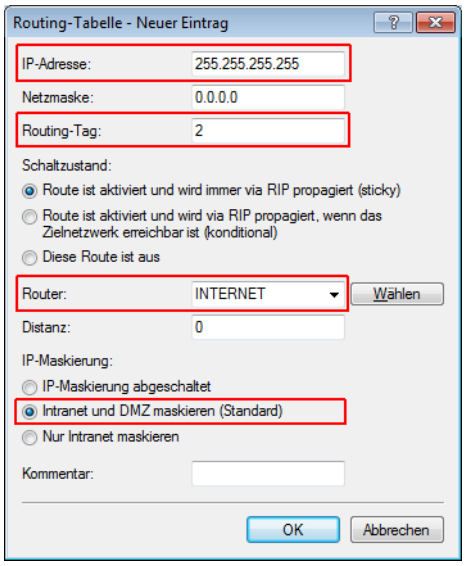


9. Der WLC kann als DHCP-Server für die APs und die angemeldeten WLAN-Clients fungieren. Aktivieren Sie dazu den DHCP-Server für das 'INTRANET' und den 'GASTZUGANG. In LANconfig finden Sie diese Einstellung unter **Konfiguration** > **TCP/IP** > **DHCP** > **DHCP-Netzwerke**.

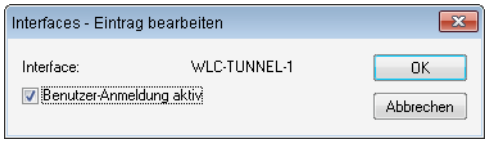
Die Aktivierung des DHCP-Servers ist für das Gästenetz zwingend, für das interne Netz optional. Für das interne Netz können Sie den DHCP Server auch anders realisieren.



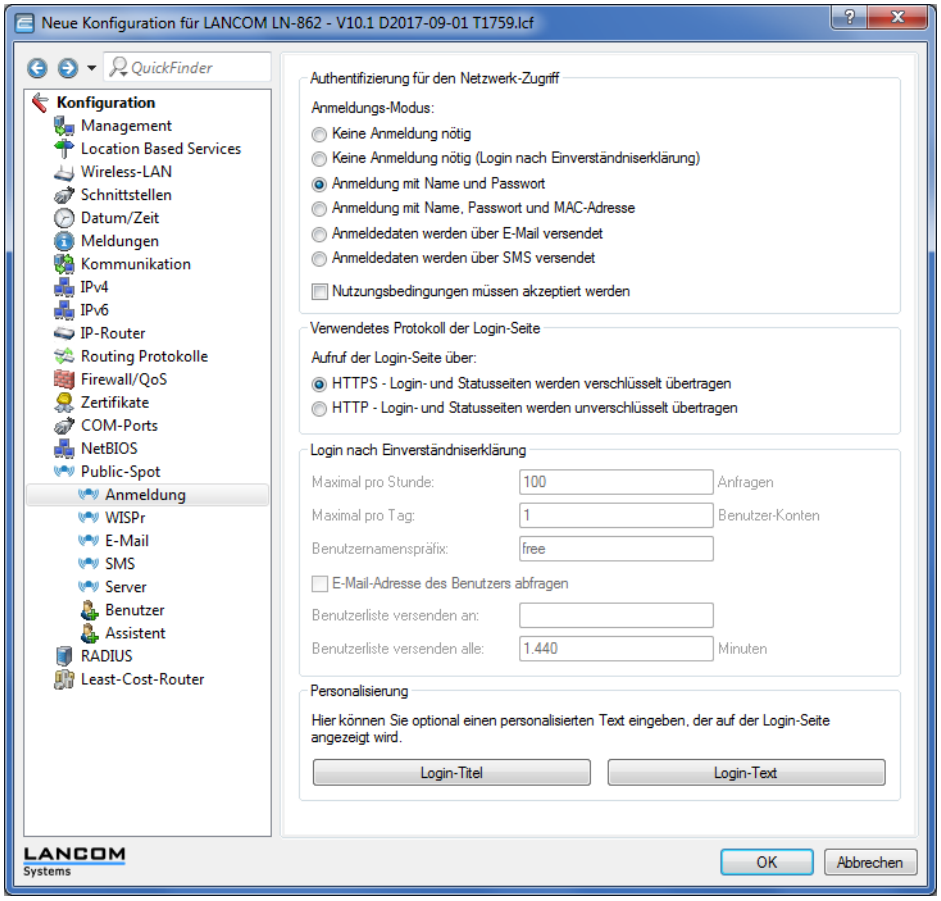
10. Erstellen Sie eine neue Standard-Route in der Routing-Tabelle, welche die Daten aus dem Gästenetzwerk auf den Internet-Zugang des WLCs leitet. Wählen Sie dazu das Routing-Tag '2' und den Router 'Internet'. Aktivieren Sie außerdem die Option 'Intranet und DMZ maskieren (Standard)'. In LANconfig finden Sie diese Einstellung unter **Konfiguration** > **IP-Router** > **Routing** > **Routing-Tabelle**.



11. Aktivieren Sie die Public Spot-Anmeldung für die logische LAN-Schnittstelle 'WLC-Tunnel 1'. In LANconfig finden Sie diese Einstellung unter **Konfiguration** > **Public-Spot** > **Server** > **Betriebseinstellungen** > **Interfaces**.



12. Aktivieren Sie im letzten Schritt die Anmeldung über den Public-Spot für den WLC. In LANconfig finden Sie diese Einstellung unter **Konfiguration** > **Public-Spot** > **Anmeldung**.



Neben der Konfiguration des WLCs konfigurieren Sie den Public Spot nach Ihren Wünschen entweder für die interne Benutzerliste oder für die Verwendung eines RADIUS-Servers.

14.4.4 IP-abhängige Autokonfiguration und Tagging von APs

Sämtliche APs, die Sie einem gemanagten Netz hinzufügen, verwalten Sie im einfachsten Falle in einer flachen Hierarchie. In größeren Installationen mit Hunderten von APs über mehrere Standorte hinweg wird diese Form der Organisation jedoch schnell unübersichtlich und erzeugt einen hohen Administrationsaufwand. Über die Einrichtung von **Zuweisungs-Gruppen** haben Sie daher die Möglichkeit, das Management verteilter APs zu vereinfachen. Hierbei lassen Sie neue APs in Abhängigkeit von der erhaltenen IP-Adresse automatisch vom WLC konfigurieren. Dadurch entfällt die manuelle Zuweisung eines IP-Parameter-Profils, eines WLAN-Profils und eines Client Steering-Profils durch einen Administrator.

Die Anwendung einer Zuweisungs-Gruppe bei Anmeldung eines neuen APs an einem zentralen WLC läuft nach folgendem Schema ab: Nachdem die neuen APs am gewünschten Einsatzort (z. B. einem Firmen- bzw. Filialnetz) installiert sind, versuchen diese, eine Verbindung zum eingetragenen WLC aufzubauen und via CAPWAP eine Konfiguration zu beziehen. Der WLC erkennt die Verbindungsanfragen und prüft für jeden neuen AP, ob in der AP-Tabelle ein geeignetes AP-Profil (z. B. das Default-Profil) vorliegt oder/und eine geeignete Zuweisungs-Gruppe definiert ist. Liegen eine oder mehrere Konfigurationsmöglichkeiten vor, prüft der WLC diese auf folgende Zustände:

1. Für einen neuen AP existiert eine Zuweisungs-Gruppe, jedoch kein AP-Profil. In diesem Fall weist der WLC dem neuen AP die innerhalb der Zuweisungs-Gruppe definierten Profile zu.
2. Für einen neuen AP existiert sowohl eine Zuweisungs-Gruppe als auch ein AP-Profil. In diesem Fall ignoriert der WLC die Zuweisungs-Gruppe und weist dem neuen AP die innerhalb des AP-Profils definierten Profile zu.

3. Für einen neuen AP existiert ein AP-Profil, aber keine Zuweisungs-Gruppe. Das Verhalten entspricht dem von Punkt (2).

Existieren für einen neuen AP weder ein AP-Profil, noch eine Zuweisungs-Gruppe, gibt der WLC eine Warnung aus, welche den Administrator auf die Fehlkonfiguration hinweist.

Nach der erfolgreichen Gruppenzuweisung legt der WLC in der Access-Point-Tabelle automatisch ein AP-Profil für jeden neuen AP an. Im Feld **Gruppen** referenziert der WLC die Zuweisungs-Gruppen, die er beim Hinzufügen des neuen AP angewandt hat.

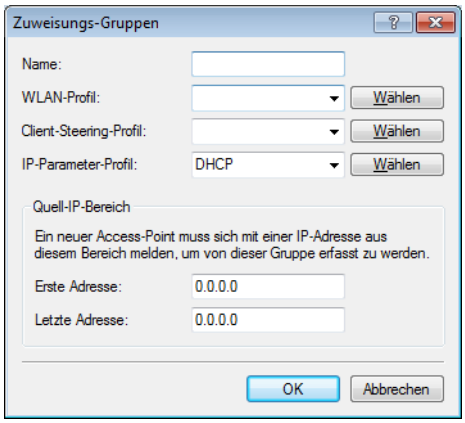
Ein AP darf immer nur eine Zuweisungsgruppe erhalten. Sobald sich Anwendungsbereiche von Zuweisungsgruppen überschneiden, erkennt LCOS derartige Konfigurationsfehler und schreibt die Meldungen in die entsprechende Status-Tabelle unter **Status** > **WLAN-Management** > **AP-Konfiguration**.

Über das Gruppen-Feld haben Sie ebenfalls die Möglichkeit, einen AP mit individuell definierbaren Tags zu versehen. Diese **Tag-Gruppen** lassen sich z. B. beim Ausführen von Aktionen auf dem WLC als Filterkriterien einsetzen, um eine Aktion auf eine Auswahl von APs zu beschränken.

14.4.4.1 Einrichten von Zuweisungs-Gruppen für die IP-abhängige Autokonfiguration

Das nachfolgende Tutorial zeigt Ihnen, wie Sie auf einem WLC Zuweisungs-Gruppen für die IP-abhängige Autokonfiguration neuer APs einrichten.

1. Öffnen Sie den Konfigurationsdialog für Ihr Gerät und wählen Sie **WLAN-Controller** > **AP-Konfiguration** > **Zuweisungs-Gruppen**.
2. Klicken Sie **Hinzufügen**, um eine neue Gruppe anzulegen.



3. Geben Sie als **Name** eine eindeutige Bezeichnung für die Zuweisungs-Gruppe an, z. B. `Filiale_Berlin`.
4. Wählen Sie das **WLAN-Profil** aus, welches der WLC einem neuen AP automatisch zuweist, wenn die IP-Adresse des neuen APs innerhalb des Quell-IP-Bereichs liegt.
5. Geben Sie ein **IP-Parameter-Profil** an, sofern der neue AP eine manuelle Netzkonfiguration erhalten soll. Andernfalls belassen Sie den Einzelwert **DHCP**; hierbei erhält der AP eine automatische Netzkonfiguration vom DHCP-Server. Der DHCP-Server muss dazu entsprechend konfiguriert sein.

   Sofern Sie eine manuelle Netzkonfiguration zuweisen wollen, bei der ein neuer AP eine abweichende IP-Adresse erhält, so geben Sie den entsprechenden Adressbereich im **IP-Parameter-Profil** unter **Address-Zuweisungs-Pool** an.
6. **Optional**: Geben Sie ein **Client Steering-Profil** an, um bei mehreren neuen APs die sich im Sendebereich befindlichen, künftigen WLAN-Clients auf den für sie idealen AP umzuleiten.

   Sofern Sie Client Steering aktivieren, muss dieses innerhalb der zu managenden Infrastruktur für jeden AP aktiviert sein. Weitere Informationen dazu finden Sie im Abschnitt *Client Steering über den WLC* auf Seite 1230.

7. Geben Sie den Anfang und das Ende des **Quell-IP-Bereich**s an, für den die Zuweisungs-Gruppe gilt.
   Ein neuer AP muss sich mit einer IP-Adresse aus diesem Bereich beim WLC anmelden, um die für die Gruppe hinterlegte Konfiguration zu erhalten.
8. Schließen Sie alle Dialogfenster mit **OK** und schreiben Sie die Konfiguration zurück auf Ihr Gerät.

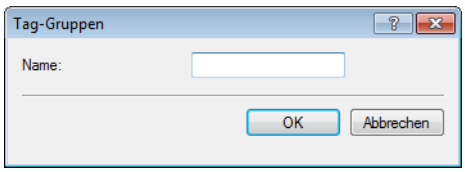
Der WLC weist fortan allen neuen APs die in den Zuweisungs-Gruppen referenzierten Profile zu. Über die LCOS-Konsole haben Sie dann die Möglichkeit, Informationen zur Kategorisierung abzurufen, siehe *Übersicht der capwap-Parameter im show-Befehl* auf Seite 69.

Achten Sie darauf, dass in der Access-Point-Tabelle kein AP-Profil (z. B. das Default-Profil) vorliegt, welches der WLC den neuen APs zuweisen könnte. Sofern ein geeignetes AP-Profil vorliegt, erhält dies gegenüber Zuweisungs-Gruppen stets die höhere Priorität.

14.4.4.2 Einrichten von Tag-Gruppen für die selektive Auswahl von APs

Das nachfolgende Tutorial zeigt Ihnen, wie Sie eine AP-Konfiguration auf einem WLC um eine Tag-Gruppe erweitern. Dazu legen Sie zunächst eine Tag-Gruppe an und weisen diese Gruppe anschließend einem WLAN-Profil zu.

1. Öffnen Sie den Konfigurationsdialog für Ihr Gerät und wählen Sie **WLAN-Controller** > **AP-Konfiguration** > **Tag-Gruppen**.
2. Klicken Sie **Hinzufügen**, um eine neue Gruppe anzulegen.



3. Geben Sie unter **Name** den zu definierenden Tag ein und speichern Sie den Eintrag mit **OK**.
4. Wechseln Sie in den Dialog **WLAN-Controller** > **AP-Konfiguration** > **Access-Point-Tabelle**.
5. Wählen Sie ein bestehendes AP-Profil über **Bearbeiten** aus oder fügen Sie ggf. ein neues hinzu.
6. Wählen Sie unter **Gruppen** die zuvor anlegte(n) Tag-Gruppe(n) aus.
   Mehrere Tag-Gruppen trennen Sie durch eine kommaseparierte Liste.

   Die Taggruppen sind unabhängig von den Zuweisungs-Gruppen, deren Zuweisung im selben Eingabefeld erfolgt. Zuweisungs-Gruppen werden generell vom Gerät zugewiesen und bedürfen keiner nutzerseitigen Zuordnung. Das manuelle Zuordnen einer Zuweisungs-Gruppe hat gemäß der unter *IP-abhängige Autokonfiguration und Tagging von APs* auf Seite 1190 beschriebenen Zustandsprüfung keinen Effekt auf die AP-Konfiguration. Auswirkungen bestehen lediglich auf die Filterung im Befehl `show capwap group` an der Konsole.

   Das manuelle Hinzufügen von Zuweisungs-Gruppen zu Filterungszwecken ist nicht empfehlenswert. Legen Sie stattdessen separate Tag-Gruppen an.
7. Schließen Sie alle Dialogfenster mit **OK** und schreiben Sie die Konfiguration zurück auf Ihr Gerät.

Der WLC versieht fortan alle APs, die das bearbeitete WLAN-Profil erhalten, mit den darin referenzierten Tags.

14.5 Access Point Verwaltung

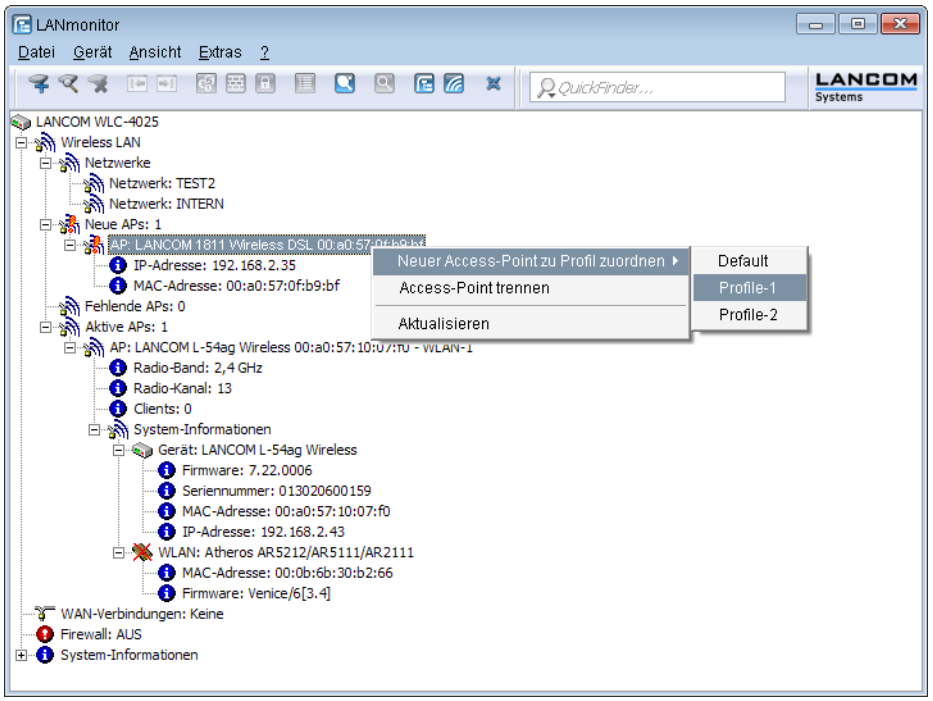
14.5.1 Neue Access Points manuell in die WLAN-Struktur aufnehmen

Wenn Sie die APs nicht automatisch in die WLAN-Struktur aufnehmen wollen, können Sie die APs auch manuell akzeptieren.

14.5.1.1 Access Points akzeptieren über den LANmonitor

Neue APs können sehr komfortabel über den LANmonitor akzeptiert werden. Dabei wird eine Konfiguration ausgewählt, welche dem AP nach der Übertragung eines neuen Zertifikats zugewiesen wird.

Klicken Sie dazu im LANmonitor mit der rechten Maustaste auf den neuen AP, den Sie in die WLAN-Struktur aufnehmen möchten. Wählen Sie dann im Kontextmenü die Konfiguration, die Sie dem Gerät zuordnen wollen.

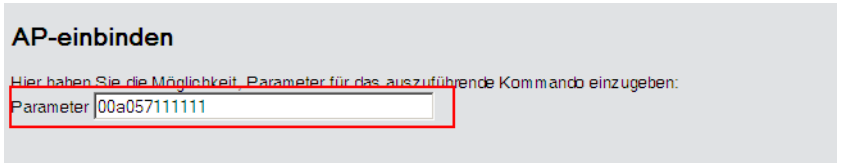


Mit dem Zuweisen der Konfiguration wird der AP in der AP-Tabelle des WLCs eingetragen. Es dauert jedoch einige Sekunden, bis der WLC dem AP auch ein Zertifikat zugewiesen hat und dieser ein aktives Element der zentralen WLAN-Struktur wird. Der neu aufgenommene AP wird also für eine kurze Zeit als "Lost AP" im LANmonitor und soweit vorhanden durch die rote Lost-AP-LED und im Gerätedisplay angezeigt, bis die Zertifikatszuweisung abgeschlossen ist.

14.5.1.2 Access Points akzeptieren über WEBconfig mit Zuweisung eines Zertifikats

Neue APs, die kein gültiges Zertifikat haben, für die jedoch ein Eintrag in der AP-Tabelle vorliegt, können über eine Aktion in WEBconfig manuell akzeptiert werden.

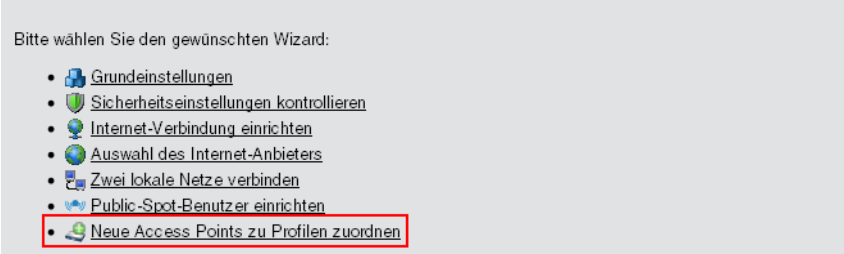
1. Öffnen Sie die Konfiguration des WLCs mit WEBconfig.
2. Wählen Sie unter **Extras** > **LCOS-Menübaum** > **Setup** > **WLAN-Management** die Aktion **AP-einbinden**.
3. Geben Sie als Parameter für die Aktion die MAC-Adresse des APs ein, den Sie akzeptieren möchten, und bestätigen Sie mit **Ausführen**.



14.5.1.3 Access Points akzeptieren über WEBconfig mit Zuweisung von Zertifikat und Konfiguration

Neue APs, die kein gültiges Zertifikat haben und für die kein Eintrag in der AP-Tabelle vorliegt, können über einen Assistenten in WEBconfig manuell akzeptiert werden. Dabei wird eine Konfiguration ausgewählt, welche dem AP nach der Übertragung eines neuen Zertifikats zugewiesen wird.

1. Öffnen Sie die Konfiguration des WLCs mit WEBconfig. Wählen Sie unter **Setup-Wizards** den Wizard **Neue Access Points zu Profilen zuordnen**.



2. Klicken Sie auf den Link, um den Assistenten zu starten. Wählen Sie den gewünschten AP anhand seiner MAC-Adresse aus und geben Sie die WLAN-Konfiguration an, die dem AP zugewiesen werden soll.



Mit dem Zuweisen der Konfiguration wird der AP in der AP-Tabelle des WLAN-Controllers eingetragen. Es dauert jedoch einige Sekunden, bis der WLC dem AP auch ein Zertifikat zugewiesen hat und er damit aktives Element der zentralen WLAN-Struktur wird. Der neu aufgenommene AP wird also für eine kurze Zeit als „Lost AP" im LANmonitor und soweit vorhanden durch die rote Lost-AP-LED und im Gerätedisplay angezeigt, bis die Zertifikatszuweisung abgeschlossen ist.

14.5.1.4 Neue APs über den WEBconfig Setup-Wizard hinzufügen

Ab LCOS 9.00 verfügen WLCs über einen überarbeiteten Setup-Wizard **Neue Access Points zu Profilen zuordnen**, der Ihnen das Hinzufügen neuer APs über WEBconfig erleichtert. Der neue Setup-Wizard erlaubt Ihnen, mit wenigen Mausklicks

- gezielt nach einem neuen AP zu suchen;
- ein oder mehrere neue APs gleichzeitig zu akzeptieren;
- einem neuen AP ein WLAN-Profil oder eine Kanalliste zuzuweisen;
- die Konfiguration eines bereits akzeptierten AP an einen neuen AP zu vererben;
- die Konfiguration eines akzeptierten fehlenden AP mit der eines neuen AP zu wechseln. Beim Wechseln einer Konfiguration erhält der neue AP die vollständige Konfiguration des akzeptierten fehlenden AP (mit Ausnahme der

MAC-Adresse). Beim Einbinden des neuen AP löscht der WLC anschließend die Konfiguration des akzeptierten fehlenden AP.



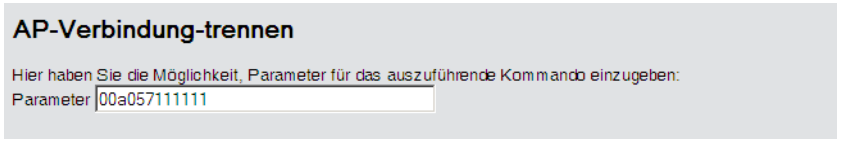
Um einen neuen AP mit den getätigten Einstellungen zu akzeptieren, klicken Sie abschließend auf **AP-einbinden**.

Sofern ein Sie einen AP über Zuweisungs-Gruppen konfigurieren lassen, brauchen Sie für den betreffenden AP keine Einstellungen in diesem Setup-Wizard vornehmen. Der WLC weist dem AP automatisch beim Einbinden die Einstellungen aus den entsprechenden Gruppen zu.

14.5.2 Access Points manuell aus der WLAN-Struktur entfernen

Um einen AP, der vom WLC verwaltet wird, aus der WLAN-Struktur zu entfernen, müssen Sie folgende Aktionen ausführen:

1. Stellen Sie im AP die WLAN-Betriebsart für die WLAN-Module von 'Managed' auf 'Client' oder 'Access-Point' um.
2. Löschen Sie im WLC die Konfiguration für den AP bzw. deaktivieren Sie die **Automatische Zuweisung der Default-Konfiguration** über **Extras** > **LCOS-Menübaum** > **Setup** > **WLAN-Management** > **AP-automatisch-einbinden**.
3. Trennen Sie die Verbindung zum AP unter WEBconfig im Bereich **Extras** > **LCOS-Menübaum** > **Setup** > **WLAN-Management** mit der Aktion **AP-Verbindung-trennen** oder alternativ im LANmonitor.
4. Geben Sie als Parameter für die Aktion die MAC-Adresse des APs ein, zu dem Sie die Verbindung trennen möchten, und bestätigen Sie mit **Ausführen**.



14.5.3 Access Point deaktivieren oder dauerhaft aus der WLAN-Struktur entfernen

In manchen Fällen ist es notwendig, einen vom WLC verwalteten AP entweder vorübergehend zu deaktivieren oder dauerhaft aus der WLAN-Struktur zu entfernen.

14.5.3.1 Access Point deaktivieren

Um einen AP zu deaktivieren, setzen Sie den entsprechenden Eintrag in der AP-Tabelle auf 'inaktiv' oder löschen Sie den Eintrag aus der Tabelle. Dadurch werden die WLAN-Module im Managed-Modus ausgeschaltet, die entsprechenden SSIDs werden im AP gelöscht.

Die WLAN-Module und die WLAN-Netzwerke (SSIDs) werden auch dann abgeschaltet, wenn der autarke Weiterbetrieb aktiviert ist.

Ein so deaktivierter AP bleibt mit dem WLC verbunden, die Zertifikate bleiben erhalten. Der WLC kann also jederzeit durch das Aktivieren des Eintrags in der AP-Tabelle oder durch einen neuen Eintrag in der AP-Tabelle für die entsprechende MAC-Adresse den AP und seine WLAN-Module im Managed-Modus wieder einschalten.

Wird die Verbindung zu einem deaktivierten AP getrennt (unbeabsichtigt z. B. durch Störung im LAN oder gezielt durch den Administrator), dann beginnt der AP eine neue Suche nach einem passenden WLC. Der bisherige WLC kann zwar das Zertifikat auf Gültigkeit prüfen, hat aber keinen (aktiven) Eintrag in der AP-Tabelle – er wird also zum sekundären WLC für diesen AP. Findet der AP einen primären WLC, so wird er sich bei diesem anmelden.

14.5.3.2 Access Point dauerhaft aus der WLAN-Struktur entfernen

Damit ein AP auf Dauer nicht mehr Mitglied der zentral verwalteten WLAN-Struktur ist, müssen die Zertifikate im SCEP-Client gelöscht oder widerrufen werden.

- Wenn Sie Zugriff auf den AP haben, können Sie die Zertifikate am schnellsten durch einen Reset des Geräts löschen.
- Wurde das Gerät gestohlen und soll aus diesem Grund aus der WLAN-Struktur entfernt werden, so müssen die Zertifikate in der CA des WLCs widerrufen werden. Wechseln Sie dazu unter WEBconfig in den Bereich **Extras** > **LCOS-Menübaum** > **Status** > **Zertifikate** > **SCEP-CA** > **Zertifikate** in die **Zertifikatsstatus-Tabelle**. Löschen Sie dort das Zertifikat für die MAC-Adresse des APs, den Sie aus der WLAN-Struktur entfernen möchten. Die Zertifikate werden dabei nicht gelöscht, aber als abgelaufen markiert.

Bei einer Backup-Lösung mit redundanten WLCs müssen die Zertifikate in allen WLCs widerrufen werden!

14.6 AutoWDS – Kabellose Integration von APs über P2P-Verbindungen

In einem zentral gemanagten WLAN sind die angeschlossenen Access Points (APs) klassischerweise über das LAN mit dem WLAN-Controller (WLC) verbunden. Diese LAN-Verbindungen geben gleichzeitig die Topologie des verwalteten Netzes vor. Eine Erweiterung des Netzes um zusätzliche APs ist jedoch auf die Reichweite der kabelgebundenen Netzarchitektur beschränkt und erfordert ggf. einen Ausbau der betreffenden Infrastruktur.

Mittels **AutoWDS** haben Sie die Möglichkeit, die Erweiterung eines WLANs auf Basis von Funkstrecken (P2P) vorzunehmen und dadurch kostengünstig und schnell sehr skalierbare Netze zu errichten. "AutoWDS" steht dabei für "Automatic Wireless Distribution System". Die Funktion erlaubt Ihnen, ein FunkNetz aus mehreren APs herzustellen, welche ausschließlich drahtlos untereinander verbunden sind: die logische Verbindung allein genügt. Die möglichen Einsatzgebiete erstrecken sich z. B. auf die flächendeckende Anbindung kleiner Areale oder ganzer Gebiete an das Internet oder ein FirmenNetz, in denen eine Verbindung über LAN nicht sinnvoll oder unpraktikabel ist.

AutoWDS wird ab LCOS 10.70 nicht mehr unterstützt. Die Funktionalität bleibt in LANCOM Geräten enthalten (außer in Routern der 18xx-Serie) und kann somit für Bestands-Installationen weiterhin verwendet werden. LANCOM Systems wird allerdings keinen Support mehr bei der Einrichtung und Analyse eines AutoWDS Szenarios leisten.

Im einfachsten Fall benötigen Sie lediglich einen WLC, der mit einem AutoWDS-fähigen AP via LAN verbunden ist. Der AP spannt das gemanagte WLAN auf und agiert gleichzeitig als "Zugangs-AP". Über den Zugangs-AP stellen hinzukommende AutoWDS-fähige APs die Verbindung zum WLC her, welcher ihnen mittels CAPWAP eine Konfiguration übermittelt. Nach Erhalt der Konfiguration und Eingliederung in das gemanagte WLAN nutzen die einzelnen APs P2P-Strecken, um Nutzerdaten weiterzuleiten, miteinander zu kommunizieren und die Topologie aufrecht zu erhalten. Weitere hinzukommende APs sind in der Lage, die eingebundenen APs ihrerseits als Zugangs-APs zu nutzen. Auf diese Weise lassen sich mehrere APs miteinander verketten und vermaschte Netze aufbauen, die optional via RSTP redundante

Verbindungen aufweisen. Aus Sicht eines hinzukommenden AP sind eingebundene APs "Master-APs". Aus Sicht des Master-AP sind hinzukommende APs "Slave-APs".

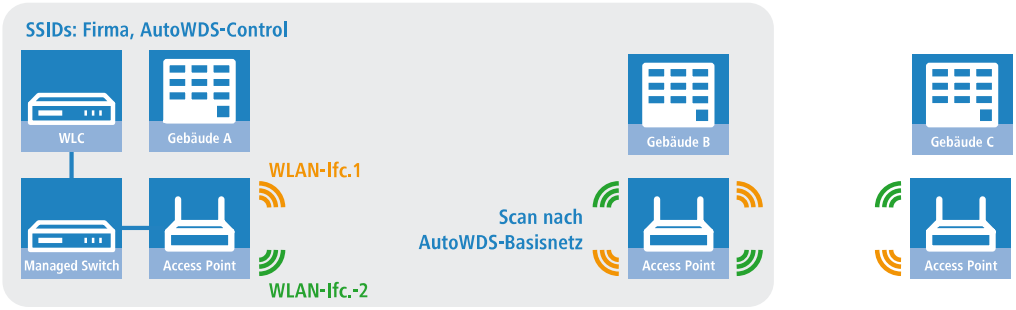


Abbildung 24: Phase 1 – Hinzukommender AP in Gebäude B sucht nach AutoWDS-Basisnetz und findet Zugangs-AP in Gebäude A



Abbildung 25: Phase 2 – Hinzukommender AP in Gebäude B findet WLC und bezieht AP-Konfiguration über CAPWAP

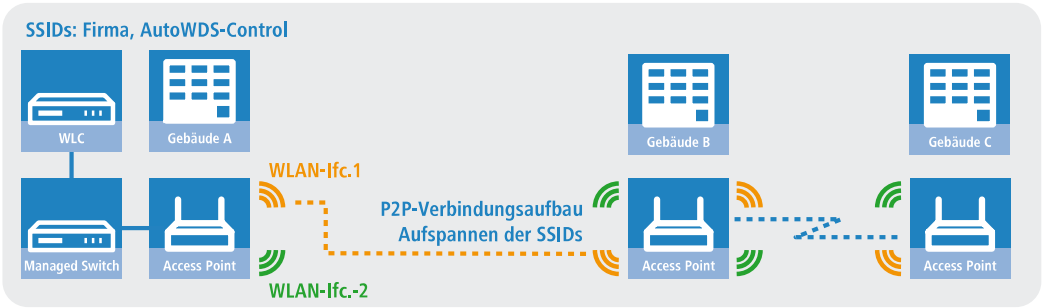


Abbildung 26: Phase 3 – Hinzukommender AP in Gebäude B integriert sich in das gemanagte WLAN. Hinzukommender AP in Gebäude C sucht nach AutoWDS-Basisnetz und findet Zugangs-AP in Gebäude B.

Genauere Informationen zum Integrationsablauf und zu den Betriebsmodi beim Topologie-Management erhalten Sie in den nachfolgenden Abschnitten zur Funktionsweise von AutoWDS.

AutoWDS eignet sich ausschließlich für statische Infrastrukturen, nicht für sich bewegende APs. Sollte ein AP aus der Reichweite seines P2P-Partners wandern und die Verbindung zum Netz verlieren, erfolgt eine temporäre Downtime mit anschließender *Rekonfiguration*. Das Roaming von WLAN-Clients zwischen einzelnen AutoWDS-APs hingegen unterscheidet sich nicht von dem zwischen normalen APs.

AutoWDS unterstützt keine Netztrennung von SSIDs auf VLANs über eine statische Konfiguration oder eine dynamische VLAN-Zuweisung über RADIUS. Soll eine Netztrennung von SSIDs erfolgen, müssen Sie diese durch Layer-3-Tunnel separieren.

Das DFS-Verhalten eines AP im 5-GHz-Betrieb ist von AutoWDS unberührt und besitzt höhere Priorität. Die DFS-Radarerkennung kann bewirken, dass der AP während des Betriebs einen plötzlichen Kanalwechsel durchführt oder das WLAN bei Ausfall der möglichen Frequenzen – aufgrund mehrerer Radarerkennungen auf verschiedenen Kanälen – für einige Zeit komplett deaktiviert. Der betroffene AP kann somit für Störungen des gesamten AutoWDS-Verbundes verantwortlich sein oder eine Zeit lang gar keine SSIDs aufspannen. Innerhalb von Gebäuden haben Sie die Möglichkeit, evtl. auftretenden Störungen durch Aktivieren des Indoor-Modus entgegenzuwirken.

Wenn Sie AutoWDS auf einem Gerät mit einer einzigen physikalischen WLAN-Schnittstelle einsetzen, drittelt sich im Betrieb deren Datenrate, da das Gerät eingehende/ausgehende Daten mehrfach senden muss: An die WLAN-Clients, an einen Master-AP und ggf. an einen Slave-AP. Um diesen Effekt zu mildern, sollten Sie ausschließlich Geräte mit mehreren physikalischen WLAN-Schnittstellen einsetzen und auf diesen eine Trennung des Datenverkehrs vornehmen. Dazu reservieren Sie eine physikalische WLAN-Schnittstelle für die Anbindung der APs und eine physikalische WLAN-Schnittstelle für die Anbindung der Clients.

MultiHop auf ein und derselben WLAN-Schnittstelle aktivieren Sie bei Bedarf in der AutoWDS-Profil-Konfiguration, da dieses aufgrund der Performance-Verluste standardmäßig deaktiviert ist.

14.6.1 Hinweise zur Nutzung von AutoWDS

Die Einsatzmöglichkeiten von AutoWDS unterliegen technischen Beschränkungen, wodurch sich die Funktion ausschließlich für bestimmte Anwendungsszenarien eignet. Bitte beachten Sie daher aufmerksam die in diesem Kapitel beschriebenen allgemeinen Hinweise, um möglichen Komplikationen vorzubeugen. Die hier gelisteten Punkte sind als Ergänzung zu den Hinweisen des übrigen AutoWDS-Kapitels zu verstehen, wobei Überschneidungen möglich sind.

- APs müssen bei Radarerkennung (5-GHz-Band, Outdoor bzw. DFS) den Kanal wechseln. Dadurch sind kurzzeitige Unterbrechungen des WLANs durch notwendigen Kanalwechsel möglich.
- Generell ist ein AutoWDS-Betrieb von bis zu maximal 3 Hops empfehlenswert.
- Bei Verwendung von AutoWDS auf ausschließlich einem Funkkanal treten Mehrfachübertragungen und Hidden-Station-Probleme auf. Empfehlenswert ist daher der Einsatz von APs mit zwei physikalischen WLAN-Schnittstellen (Dual Radio) auf separaten Funkkanälen.
- AutoWDS unterstützt keine Netztrennung von SSIDs auf VLANs über eine statische Konfiguration oder eine dynamische VLAN-Zuweisung über RADIUS. Soll eine Netztrennung von SSIDs erfolgen, müssen Sie diese durch Layer-3-Tunnel separieren.

Betreiben Sie DFS in Kombination mit AutoWDS, konfigurieren Sie für den autarken Weiterbetrieb (Continuation-Time) des AutoWDS-Profils mindestens 2 Minuten. So bleibt dem CAPWAP-Layer nach der Downtime einer P2P-Verbindung aufgrund eines DFS-Scans von einer Minute eine zusätzliche Minute Zeit, die CAPWAP-Verbindung zum WLC über die P2P-Verbindung nach dem DFS-Scan wieder herzustellen.

Achten Sie nach Möglichkeit darauf, dass alle beteiligten APs je physikalischer WLAN-Schnittstelle (WLAN-1, WLAN-2) durchgehend das gleiche Frequenzband (2,4GHz oder 5GHz) verwenden, um so eventuelle Probleme bei der automatischen Topologie-Konfiguration auszuschließen.

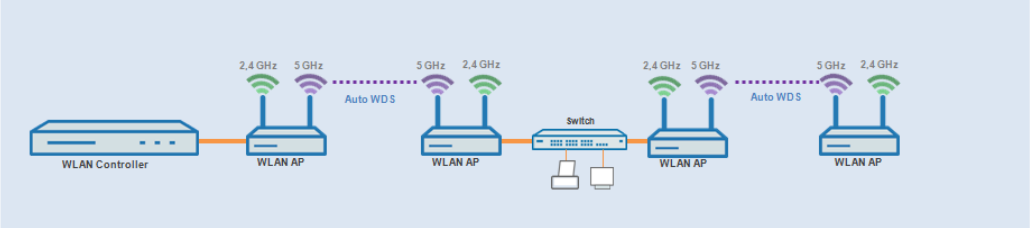
Nachfolgend finden Sie eine Bewertung der **Eignung von AutoWDS** für bestimmte von Anwendungsszenarien.

Gut geeignet:

Nutzung einer **dedizierten** physikalischen WLAN-Schnittstelle für die P2P-Strecken.

- Verwendung von unterschiedlichen Kanälen für die P2P-Strecken (Indoor)

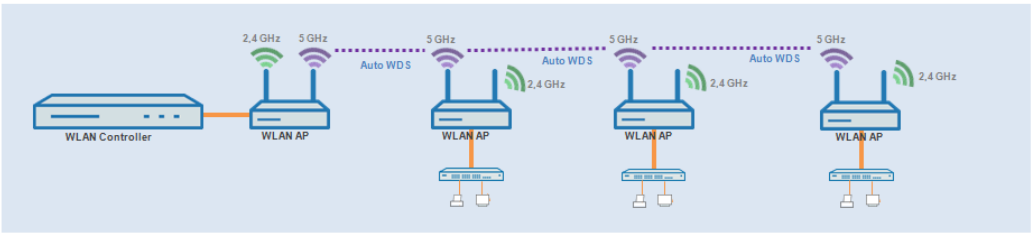
- Verwendung von AutoWDS auf bis zu 3 Hops



Bedingt geeignet:

Nutzung einer physikalischen WLAN-Schnittstelle **gleichzeitig** für AutoWDS-Uplink und -Downlink (Repeater-Modus), wobei alle P2P-Strecken den gleichen Funkkanal verwenden.

- Verwendung für Betrieb ohne DFS (Indoor)
- Verwendung von AutoWDS auf bis zu 3 Hops



Mögliche auftretende Probleme sind z. B. das sogenannte Hidden-Station-Phänomen oder die Durchsatz-Reduzierung durch Mehrfachübertragung.

- **Hidden-Station-Phänomen**: Bei größeren Entfernungen können sich weit entfernte APs des selben Netzwerkes u. U. nicht mehr gegenseitig sehen, da die Empfangsradien nicht ausreichen. In diesem Fall steigt die Wahrscheinlichkeit, dass mehrere APs gleichzeitig senden und sich in der Übertragung gegenseitig stören. Diese Kollisionen führen zu Mehrfachübertragungen und Performanz-Einbußen.

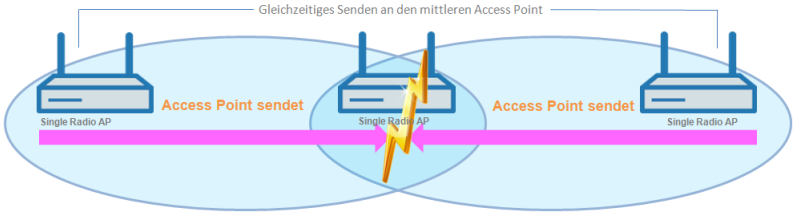


Abbildung 27: Gleichzeitiges senden an den mittleren AP: Die beiden äußeren APs erkennen die Kollision nicht.

- **Durchsatz-Reduzierung durch Mehrfachübertragung**: Überträgt ein AP Datenpakete auf dem gleichen Kanal mehrfach, reduziert sich in der Praxis der maximal erreichbare Durchsatz (Halbierung pro Hop).

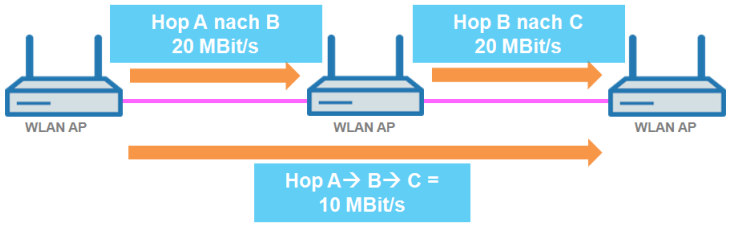
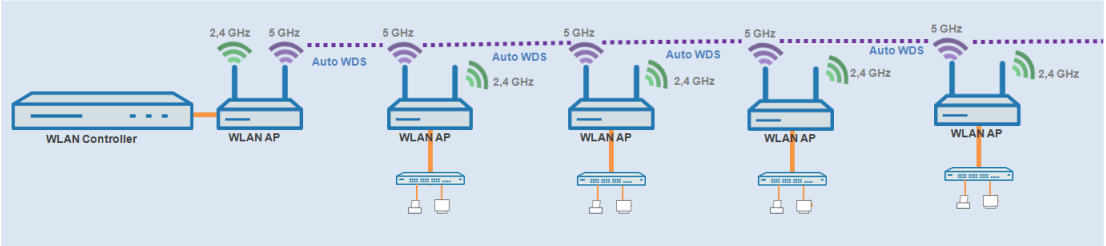


Abbildung 28: Übertragung der Datenpakete auf jedem Hop

Nicht geeignet:

Nutzung einer physikalischen WLAN-Schnittstelle **gleichzeitig** für AutoWDS-Uplink und -Downlink (Repeater-Modus) bei Outdoor-Betrieb mit mehr als 1 Hop im 5-GHz-Band.



Im Repeater-Modus nimmt die physikalische WLAN-Schnittstelle eine Doppelrolle ein: In Richtung des WLCs agiert die Schnittstelle als Master, in Richtung eines Nachbar-APs hingegen als Slave. Hierzu arbeiten alle APs notwendigerweise auf dem selben Funkkanal. Bei der Erkennung von DFS-Signalen dürfen die APs jedoch nicht mehr auf den entsprechenden Frequenzen senden. Somit kann Seitens der APs keine Meldung an den WLC über die DFS-Erkennung erfolgen und der WLC kann seinerseits keinen Frequenzwechsel für das Netz einleiten. Im Ergebnis sind die betroffenen APs ggf. permanent vom Netz getrennt.

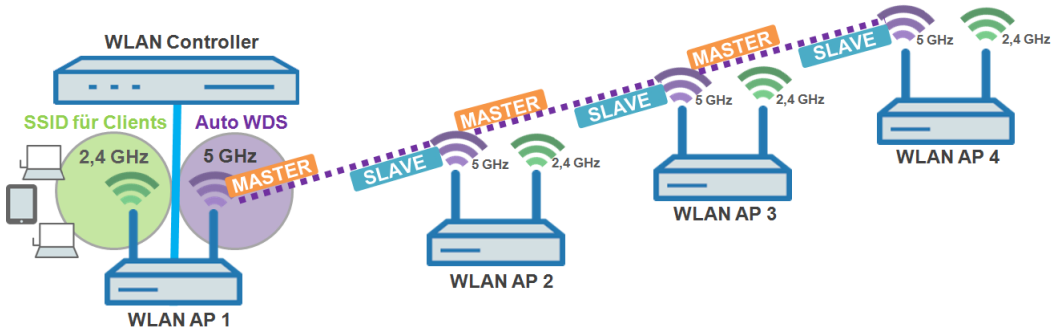


Abbildung 29: Verbindungssperre bei DFS-Erkennung

14.6.2 Funktionsweise

14.6.2.1 Aufspannen des AutoWDS-Basisnetzes

AutoWDS stellt verschiedene Integrationsmodi bereit, über die das Management von P2P-Strecken zum Errichten vermaschter Netze erfolgen kann. Den Großteil der Konfiguration nehmen Sie auf dem WLC vor, der die einzelnen logischen WLAN-Netze verwaltet. Dazu verknüpfen Sie ein aktives AutoWDS-Profil mit einem eingerichteten WLAN-Profil

Ihres gemanagten WLANs. Das AutoWDS-Profil gruppiert die Einstellungen und Grenzwerte für die Gestaltung der P2P-Topologie und des AutoWDS-Basisnetzes.

Das AutoWDS-Basisnetz bzw. die dazugehörige SSID (Vorgabename: **AutoWDS-Rollout**) ist ein reines Managementnetz: Es dient ausschließlich der Authentifizierung eines AP bei der vorkonfigurierten Integration sowie dem Aufbau des WLC-Tunnels für den Konfigurationsaustausch. Auf diese Weise lassen sich hinzukommende APs bei der Integration in das gemanagte WLAN vom operativen Betrieb isolieren. Sobald eine P2P-Verbindung zu einem Master-AP besteht, gilt ein hinzukommender AP als integriert und wickelt die weitere Kommunikation über die Bridge auf Layer 2 ab. Ähnlich wie bei klassischen P2P-Verbindungen spannen die P2P-Partner dazu eine Management-SSID auf, über die sie den Datenverkehr und den CAPWAP-Tunnel zum WLC abwickeln (siehe *Update der AP-Konfiguration und Aufbau der P2P-Strecke* auf Seite 1203).

Für WLAN-Clients wie Smartphones, Laptops, etc. ist das AutoWDS-Basisnetz nicht benutzbar. Für sie muss innerhalb der WLAN-Infrastruktur eine eigene SSID aufgespannt sein.

Nachdem Sie Ihrem gemanagten WLAN ein aktives AutoWDS-Profil zugewiesen haben, spannen die betreffenden (Zugangs-)APs das AutoWDS-Basisnetz auf und senden in ihren Beacons (sofern Sie im AutoWDS-Profil 'SSID-Broadcast' aktiviert haben) und Probe-Responses eine zusätzliche, herstellerspezifische Kennung aus. Diese auch als "AutoWDSInfoFlags" bezeichnete Kennung signalisiert hinzukommenden AutoWDS-fähigen APs die generelle Unterstützung der Funktion und teilt ihnen mit, …

- ob AutoWDS für die erkannte SSID aktiv/inaktiv ist;
- ob der AP der betreffenden SSID eine aktive/inaktive WLC-Verbindung besitzt;
- ob der WLC hinzukommende APs im Express-Modus akzeptiert oder verbietet; und
- ob sich APs für die Integration mit der äquivalenten physikalischen WLAN-Schnittstelle des Zugangs-AP verbinden müssen (strikte Schnittstellen-Paarung, d. h. mit WLAN-1 auf WLAN-1 sowie mit WLAN-2 auf WLAN-2) oder gemischte Schnittstellen-Paarungen erlaubt sind.

Ein gemanagter AP funktioniert automatisch als AutoWDS-AP, sobald er sich einmal initial mit einem WLC per LAN-Kabel gepaart und ein gültiges Zertifikat sowie ein AutoWDS-Profil mit der weiteren AP-Konfiguration korrekt übertragen hat. Ein konfigurierter AutoWDS-AP funktioniert automatisch als hinzukommender AP, sobald eine CAPWAP-Verbindung zu einem WLC nach einer vordefinierten Zeit nicht gelingt, weil z. B. keine kabelgebundene LAN Verbindung existiert. Der betreffende AP wechselt die Betriebsart daraufhin temporär in den **Client**-Modus und scannt solange die einzelnen WLANs, bis er einen geeigneten Zugangs-AP erkennt. Der Scan erfolgt sowohl im 2,4-GHz- als auch im 5-GHz-Frequenzband.

Sofern Ihr Gerät über zwei physikalische WLAN-Schnittstellen verfügt und beide aktiv sind, scannen beide WLAN-Schnittstellen gleichzeitig nach einem geeigneten AutoWDS-Basisnetz. Erkennt eine physikalische WLAN-Schnittstelle eine geeignete SSID, assoziiert sie sich mit dem Zugangs-AP, sofern es die oben erwähnte Schnittstellen-Paarung erlaubt. Die andere physikalische WLAN-Schnittstelle scannt für den Fall weiter, dass die bereits assoziierte physikalische WLAN-Schnittstelle die Verbindung wieder verliert. Die andere physikalische WLAN-Schnittstelle verbindet sich aber bis dahin mit keinem weiteren AutoWDS-Basisnetz. Sobald Ihr Gerät die WLC-Konfiguration erhalten hat, verhalten sich beide physikalischen WLAN-Schnittstellen wie im Profil festgelegt und spannen die Ihnen zugewiesenen SSIDs und das AutoWDS-Basisnetz auf.

Der Ablauf des Suchvorgangs nach einem AutoWDS-Basisnetz ist identisch mit dem der Rekonfiguration bei Verlust der WLAN-Verbindung (siehe *Verlust der Konnektivität und Rekonfiguration* auf Seite 1204).

14.6.2.2 Unterschiede der Integrationsmodi

Bei der Integration von hinzukommenden APs in Ihr gemanagtes WLAN haben Sie die Wahl zwischen zwei verschiedenen Integrationsmodi. Der Integrationsmodus legt die Bedingungen fest, unter denen Ihr WLC einen hinzukommenden AP akzeptiert:

- Die **vorkonfigurierte Integration** stellt den kontrollierten und bevorzugten Weg dar, einen hinzukommenden AP über eine Funkstrecke in ein gemanagtes WLAN zu integrieren. In diesem Modus gestattet der WLC ausschließlich die Integration von APs, die über eine lokal vorkonfigurierte SSID und gültige WPA2-Passphrase für das AutoWDS-Basisnetz verfügen.

Der Modus eignet sich für sämtliche Produktivumgebungen und dient dazu, einen vorgegebenen Bezug zwischen einem hinzukommenden AP und einem AutoWDS-Basisnetz herzustellen. Sobald der betreffende AP eine Konfiguration vom WLC erhält, priorisiert der AP diese Konfiguration höher als die lokale AutoWDS-Konfiguration, bis der WLC via CAPWAP die Konfiguration widerruft oder Sie den AP resetten.

- Die **Express-Integration** stellt den schnellen Weg dar, einen hinzukommenden AP über eine Funkstrecke in ein gemanagtes WLAN zu integrieren. In diesem Modus erlaubt der WLC sowohl die Integration vorkonfigurierter Geräte als auch die Integration vollkommen unkonfigurierter Geräte. Unkonfigurierte APs verfügen weder über eine eingetragene SSID noch über eine individuelle WPA2-Passphrase für ein AutoWDS-Basisnetz. Für die Authentifizierung an einem beliebigen AutoWDS-Basisnetz nutzen die Geräte stattdessen einen fest in die Firmware implementierten Pre-Shared-Key.

  Der Modus eignet sich zur einfachen Integration neuer APs in ein gemanagtes WLAN. Die Wahl eines AutoWDS-Basisnetzes geschieht hierbei automatisch und entzieht sich Ihrer Kontrolle. Sobald die betreffenden APs vom WLC eine Konfiguration erhalten, speichern die Geräte die Einstellungen als voreingestellte Werte, bis der WLC via CAPWAP die Konfiguration widerruft, das Gerät nach einem Verbindungsabbruch die Express-*Rekonfiguration* ausführt oder Sie das Gerät resetten.

  Achten Sie bei der Express-Integration darauf, dass sich keine anderen AutoWDS-Basisnetze in Reichweite befinden. Andernfalls ist es möglich, dass ein fremder WLC Ihren AP übernimmt und so Ihrem weiteren Fernzugriff entzieht. Ein aktivierter Express-Modus erweitert die Angriffsmöglichkeiten. Deshalb ist es ratsam, den Express-Modus zu deaktivieren, wenn er nicht unbedingt notwendig ist.

  LANCOM empfiehlt aus o. g. Sicherheitsgründen vornehmlich die vorkonfigurierte Integration. Über das Pairing von WLC und APs haben Sie die Möglichkeit, den Aufwand für die vorkonfigurierte Integration weiter zu reduzieren. Mehr dazu erfahren Sie im Abschnitt *Vorkonfigurierte Integration durch Pairing beschleunigen* auf Seite 1209.

Nach erfolgreicher Authentifizierung am AutoWDS-Basisnetz und dem Beziehen einer IP-Adresse scannen die hinzukommenden APs das Netz nach einem WLC. Sobald sie einen WLC erkannt haben, versuchen sie, sich mit ihm zu verbinden und eine Konfiguration zu beziehen. Im LANmonitor erscheinen diese APs als neue Geräte, deren Aufnahme in das gemanagte WLAN der Administrator noch bestätigen und ihnen noch ein WLAN-Profil zuweisen muss. Die Zuweisung unterscheidet sich dabei nicht von der Aufnahme normaler APs. Alternativ kann die Zuweisung durch den WLC erfolgen, wenn Sie

- ein Default-WLAN-Profil eingerichtet und die automatische Zuweisung dessen aktiviert haben; oder
- den betreffenden AP in die Access-Point-Tabelle eingetragen und mit einem WLAN-Profil verknüpft haben.

Durch gleichzeitiges Setzen der automatischen Annahme hinzukommender APs durch den WLC ("Auto Accept") lässt sich die Integration hinzukommender APs automatisieren. Für die Express-Integration sollten Sie diese Einstellung jedoch unbedingt deaktivieren, um ein Mindestmaß an Sicherheit zu erhalten und Rogue-AP-Intrusion zu erschweren.

Der Ablauf der Zertifikatserstellung und die Zertifikatsprüfung sowie die automatische Annahme oder Verweigerung von Verbindungsanfragen durch den WLC gleichen dem eines WLAN-Szenarios mit kabelgebundenen APs. Weitere Informationen dazu finden Sie im Abschnitt *Kommunikation zwischen Access Point und WLAN-Controller* auf Seite 1125.

14.6.2.3 Gestaltung der Topologie

Mit der Zuweisung des WLAN-Profils durch den WLC erhalten die Slave-APs gleichzeitig Informationen darüber, wie Ihre P2P-Strecken der Topologie des vermaschten Netzes aufzubauen sind. Die Topologie ergibt sich unmittelbar aus der Hierarchie der unter den APs aufgebauten P2P-Verbindungen. Für deren Gestaltung bietet Ihnen der WLC folgende Management-Modi an:

- **Automatisch**: Der WLC generiert automatisch eine P2P-Konfiguration. Manuell festgelegte P2P-Strecken ignoriert das Gerät.

- **Halb-automatisch**: Der WLC generiert ausschließlich dann eine P2P-Konfiguration, wenn keine manuelle P2P-Konfiguration für den hinzukommenden AP existiert. Andernfalls verwendet der WLC die manuelle Konfiguration.
- **Manuell**: Der WLC generiert selbständig keine P2P-Konfiguration. Wenn eine manuelle P2P-Konfiguration existiert, wird diese verwendet. Andernfalls überträgt der WLC keine P2P-Konfiguration zum AP.

Standardmäßig übernimmt der WLC automatisch die Berechnung der Topologie, bei der sich ein Slave-AP i. d. R. mit dem nächstgelegenen Master-AP verbindet. Die in Echtzeit berechnete Topologie protokolliert der WLC in der Status-Tabelle **AutoWDS-Auto-Topology**. Sofern Sie das halb-automatische oder manuelle Management verwenden, definieren Sie die statischen P2P-Strecken innerhalb der Setup-Tabelle **AutoWDS-Topology**. Dazu legen Sie die Beziehungen zwischen den einzelnen Master-APs und Slave-APs ähnlich einer normalen P2P-Verbindung fest. Mehr dazu finden Sie im Abschnitt *Manuelles Topologie-Mangement* auf Seite 1211.

Die automatische Berechnung einer P2P-Konfiguration (z. B. bei Initial- oder Wiederverbindung eines AP) ersetzt einen in der AutoWDS-Auto-Topology-Tabelle ggf. bereits vorhandenen Eintrag.

Die automatisch generierten Topologie-Einträge sind nicht boot-persistent. Die Tabelle leert sich bei einem Neustart des WLC.

Bei der manuellen Topologie-Konfiguration ist es wichtig, dass sich ein konfigurierter P2P-Master-AP innerhalb der Topologie näher am WLC befindet als ein entsprechender P2P-Slave-AP, da bei einer kurzzeitigen Unterbrechung der P2P-Verbindung der Slave-AP nach dem Master-AP scannt.

14.6.2.4 Update der AP-Konfiguration und Aufbau der P2P-Strecke

Hat ein hinzukommender AP vom WLC via CAPWAP das WLAN-Profil mit sämtlichen darin enthaltenen Einstellungen empfangen, versucht er, als Slave eine P2P-Strecke zu dem ihm zugewiesenen Master-AP aufzubauen. Bei diesem Prozess wechselt der AP gleichzeitig seine WLAN-Betriebsart von **Client** zurück zu **Managed**.

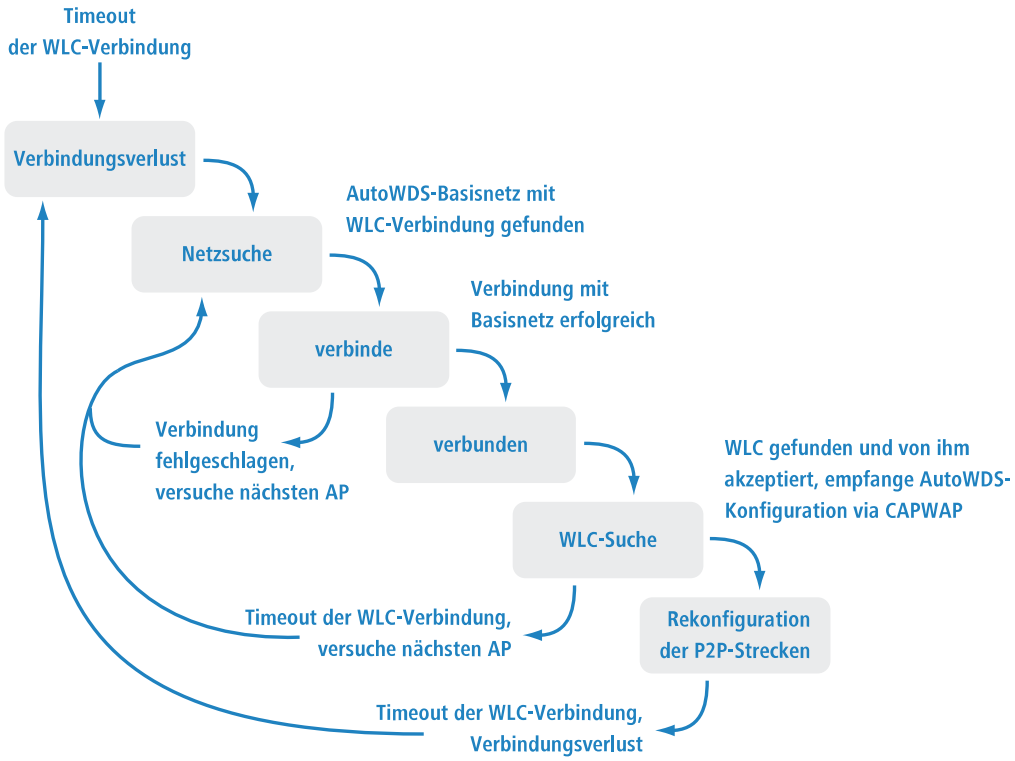
Da der Master-AP bereits im Managed-Modus agiert, erhält er vom WLC via CAPWAP lediglich ein Update seiner P2P-Konfiguration. Diese teilt dem AP neben der WPA2-Passphrase die Peer-Identifikation des AP mit. Bei einer automatisch generierten P2P-Konfiguration entspricht die Peer-Identifikation der MAC-Adresse; bei einer manuellen P2P-Konfiguration dem Namen des Slave-AP. Der Master-AP kennzeichnet derartige SSIDs mit der Kennung ***** P2P Info *****.

Sobald beide APs eine P2P-Verbindung aufgebaut haben, ist der AutoWDS-Integrationsprozess abgeschlossen. Der hinzukommende AP ist dann für Clients (Smartphones, Laptops, andere APs im Client-Modus auf der Suche nach einem Master, etc.) benutzbar.

Solange sich der hinzukommende AP im Client-Modus befindet, ist das Bridging zwischen einer physikalischen WLAN-Schnittstelle und einer LAN-Schnittstelle oder einer anderen physikalischen Funkschnittstelle während des gesamten Integrationsprozesses deaktiviert. Dazu legt das Gerät die physikalischen WLAN-Schnittstellen automatisch auf verschiedene Bridges. Erst nach dem erfolgreichen Aufbau der P2P-Verbindung schaltet der AP das Bridging wieder in den Ursprungszustand zurück.

14.6.2.5 Verlust der Konnektivität und Rekonfiguration

Sobald Sie AutoWDS auf einem hinzukommenden AP aktivieren, die Anmeldung an einem Zugangs-AP fehlschlägt oder ein eingebundener AP die Verbindung zum WLC verliert, setzt dies einen automatischen (Re-)Konfigurationsprozess in Gang, der gemäß dem abgebildeten Schema verläuft:



Ein AP durchläuft den (Re-)Konfigurationsprozess nicht, wenn er im Client-Modus zwar eine Verbindung zu einem Zugangs-AP, jedoch nicht zum WLC aufbauen kann. Der AP wartet 5 Minuten ab Verbindung zum AutoWDS-Basisnetz, ob der WLC eine Konfiguration des Gerätes durchführt. Erfolgt in dieser Zeit keine Konfiguration (z. B. weil kein Administrator den AP akzeptiert), trennt sich der AP vom AutoWDS-Basisnetz und scannt nach weiteren passenden SSIDs. Ist nur eine SSID in Reichweite, wählt der AP diese erneut für den Integrationsvorgang.

Sofern Verbindung zu einem LAN besteht, versucht der AP während der kompletten Downtime zusätzlich, per Broadcast den WLC über LAN zu erreichen. Findet der AP den WLC via LAN, erfolgt kein Aufsetzen einer neuen P2P-Strecke und der WLC löscht sämtliche automatisch generierten P2P-Strecken, die den AP als Slave festlegten.

14.6.2.6 Konfigurations-Timeouts

Sowohl die initiale Konfiguration als auch die Rekonfiguration eines hinzukommenden APs werden durch den Ablauf einzelner Zähler ausgelöst, deren Zusammenspiel das Verhalten des Gerätes steuert. Hierzu gehören, sofern festgelegt:

1. die Zeit für den autarken Weiterbetrieb der P2P-Strecke bei Verlust der CAPWAP-Verbindung (ausschließlich Rekonfiguration);
2. die Wartezeit bis zum Beginn der automatischen (Re-)Konfiguration für die vorkonfigurierte Integration; sowie
3. die Wartezeit bis zum Beginn der automatischen (Re-)Konfiguration für die Express-Integration.

Die Weiterbetriebszeit bezeichnet die Lebensdauer einer jeden P2P-Strecke für den Fall, dass der AP die CAPWAP-Verbindung zum WLC verliert. Erkennt der AP einen Verlust der CAPWAP-Verbindung, versucht er, die Verbindung innerhalb der festgelegten Weiterbetriebszeit wiederherzustellen. Während dieser Zeiten bleiben Verbindungen zu den P2P-Partnern und eingebuchten WLAN-Clients bestehen. Gelingt dem AP die Wiederherstellung nicht und ist die Weiterbetriebszeit abgelaufen, verwirft das Gerät den P2P-Teil der WLC-Konfiguration. Wenn die autarke Weiterbetriebszeit mit `0` festgelegt ist, verwirft der AP den betreffenden Konfigurationsteil sofort.

Anschließend beginnt das Gerät damit, anhand des verbliebenen Konfigurationsteils – der SSID des AutoWDS-Basisnetzes, der dazugehörigen WPA2-Passphrase sowie der Wartezeiten für die vorkonfigurierte und Express-Integration – die eingestellte Zeit bis zum Beginn der automatischen (Re-)Konfiguration für die vorkonfigurierte Integration herabzuzählen. Nach Ablauf dieser Wartezeit schaltet das Gerät seine physikalische(n) WLAN-Schnittstelle(n) in den Client-Modus um und scannt die verfügbaren SSIDs nach dem zuletzt erkannten AutoWDS-Basisnetz. Parallel dazu beginnt der Zähler bis zum Beginn der automatischen (Re-)Konfiguration für die Express-Integration herabzuzählen.

Hat das Gerät bei Ablauf des Express-Zählers das ihm bekannte AutoWDS-Basisnetz nicht gefunden, stellt das Gerät automatisch auf Express-Integration um. Anschließend sucht der AP solange nach einem beliebigen AutoWDS-fähigen Netz, bis schließlich ein geeigneter Zugangs-AP erkannt ist.

Durch intelligentes Zusammenspiel der einzelnen Wartezeiten haben Sie die Möglichkeit, das Gerät auf unvorhergesehene Ereignisse flexibel reagieren zu lassen. So lässt sich z. B. eine Fallback-Lösung für den Fall realisieren, dass Sie den Pre-Shared-Key für das AutoWDS-Basisnetz ändern, die Änderung am hinzukommenden AP jedoch fehlschlägt und sich das Gerät aufgrund einer ungültigen Konfiguration nicht mehr erreichen lässt. Bitte beachten Sie dabei die unter *Unterschiede der Integrationsmodi* auf Seite 1201 aufgeführten Hinweise.

Die betreffenden Zähler konfigurieren Sie sowohl auf dem AP (z. B. via LANconfig) als auch auf dem WLC (ausschließlich im Setup-Menü). Auf dem AP werden die Zähler ausschließlich dann beachtet, wenn noch keine WLC-Konfiguration vorliegt (initiale Konfiguration). Sobald eine Konfiguration vorliegt, sind die im AutoWDS-Profil festgelegten Zählerwerte maßgebend (Rekonfiguration). Näheres zur Prioritätensetzung der Konfigurationen finden Sie unter *Unterschiede der Integrationsmodi* auf Seite 1201.

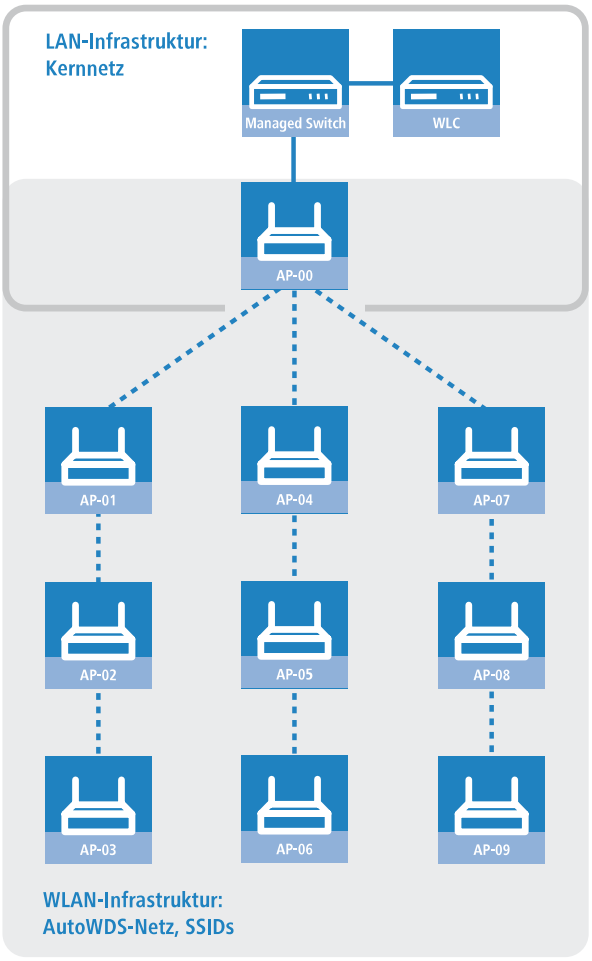
Wenn Sie den Express- oder den Vorkonfigurations-Zähler deaktivieren, überspringt das Gerät den entsprechenden Integrationsschritt. Durch Deaktivieren beider Zähler lässt sich die automatische Rekonfiguration ausschalten. Das Gerät ist dann nach einem entsprechend langen Verbindungsabbruch nicht mehr mittels AutoWDS zu erreichen. Das Gerät bleibt aber über die LAN-Schnittstelle erreichbar und sucht im LAN nach einem WLC, sofern eine entsprechende Verbindung besteht.

Der Prozess zur vorkonfigurierten Integration startet nicht, wenn die Angaben für das AutoWDS-Basisnetz (SSID, Passphrase) unvollständig sind oder der Vorkonfigurations-Zähler bei `0` liegt.

14.6.2.7 Beispiel: Ausfall eines AP

Die CAPWAP-Verbindung eines jeden AP sichert sich in einem festgelegten Intervall durch Echo-Requests zum WLC ab. Fällt ein AP aus oder ist seine Anbindung gestört, läuft ein solcher Request ins Leere. Erhalten die betreffenden APs nach mehrmaliger Wiederholung des Echo-Requests keine Antwort des WLC, gilt die CAPWAP-Verbindung als verloren und

die betreffenden APs beginnen mit dem unter *Verlust der Konnektivität und Rekonfiguration* auf Seite 1204 beschriebenen Rekonfigurationsprozess.



Für die oben abgebildete Infrastruktur hätte ein Ausfall von AP-01 die nachfolgenden Auswirkungen, sofern das automatische Topologie-Management aktiviert ist:

1. AP-01 ist defekt.
2. AP-02 und AP-03 wiederholen ihre Echo-Requests; alle Wiederholungen schlagen fehl.
3. AP-02 und AP-03 gehen in den autarken Weiterbetrieb (sofern konfiguriert) und versuchen weiterhin, den WLC zu erreichen (sowohl über WLAN als auch LAN, sofern Konnektivität besteht).
4. AP-02 und AP-03 beenden den autarken Weiterbetrieb für die P2P-Verbindungen.
5. AP-02 und AP-03 zählen die Wartezeit für den Beginn der vorkonfigurierten Integration herunter.
6. AP-02 und AP-03 schalten nach Ablauf der Wartezeit in den Client-Modus und scannen das WLAN nach dem letzten bekannten AutoWDS-Basisnetz.
7. AP-02 und AP-03 finden einen neuen Zugangs-AP (z. B. AP-05 oder AP-06) und buchen sich als Client ein.
8. AP-02 und AP-03 stellen über den **WLC-TUNNEL-AUTOWDS** die CAPWAP-Verbindung wieder her und melden dem WLC den neuen Zugangs-AP sowie die verwendeten physikalischen WLAN-Schnittstellen.
9. Der WLC generiert für die betroffenen physikalischen WLAN-Schnittstellen eine P2P-Strecke und übermittelt den APs die Konfiguration via CAPWAP.
10. Die APs setzen die neue P2P-Strecke zu den Ihnen zugewiesenen Master-APs auf und kommunizieren mit dem WLC nicht mehr über den **WLC-TUNNEL-AUTOWDS**, sondern ins LAN gebridged.

14.6.3 Einrichtung mittels vorkonfigurierter Integration

Die nachfolgenden Abschnitte zeigen Ihnen, wie Sie ein AutoWDS-Netz über die vorkonfigurierte Integration einrichten. Die Konfiguration verwendet dabei das automatische Topologie-Management des WLC.

In diesem Szenario erweitert ein Unternehmen seine Geschäftsräume um einen weiteren Gebäudekomplex. Das Unternehmen will die neuen Geschäftsräume in sein bestehendes gemanagtes WLAN integrieren. Dazu sollen die betreffenden APs ausschließlich per Funkstrecke verbunden sein. Zwischen Gebäude A (alt) und Gebäude B (neu) ist keine kabelgebundene Netzverbindung erwünscht.

Um die Konfiguration einfach zu halten, konfiguriert das Unternehmen alle APs mit einem einzelnen WLC. Die genaue Anzahl der APs in Gebäude A und Gebäude B ist nebensächlich. Besonderheiten wie mehrere physikalische WLAN-Schnittstellen berücksichtigt der WLC beim Topologie-Management automatisch.

Die Konfiguration selbst gliedert sich in zwei Teile:

1. Konfiguration des WLC in Gebäude A
2. Konfiguration aller APs in Gebäude B

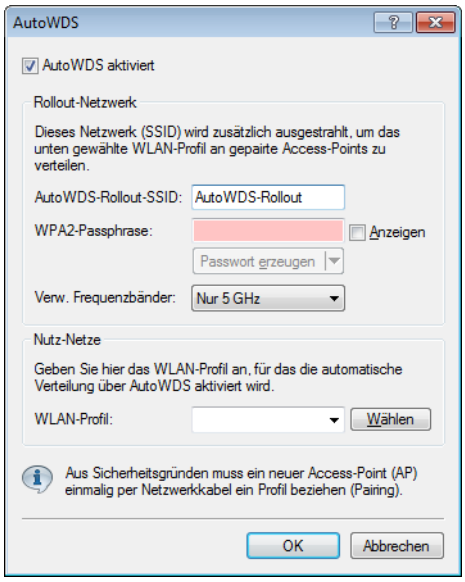
Das Anwendungsbeispiel setzt eine gültige WLAN-Konfiguration mit gültigen Zertifikaten im WLC voraus. Wie Sie ein gemanagtes WLAN einrichten, entnehmen Sie bitte dem Kapitel zum WLAN-Management.

14.6.3.1 Konfiguration des WLC

Die nachfolgenden Handlungsanweisungen beschreiben die AutoWDS-Konfiguration eines zentralen WLC für die vorkonfigurierte Integration.

Achten Sie darauf, dass die AutoWDS-APs, die sich als WLAN-Client in das Netzwerk integrieren, über das WLC-TUNNEL-AUTOWDS-Interface einen DHCP-Server erreichen. Ohne IP-Adresse werden die APs nicht nach dem WLC suchen und keine Konfiguration vom WLC erhalten.

1. Öffnen Sie den Konfigurationsdialog in LANconfig und klicken Sie **WLAN-Controller** > **Profile** > **AutoWDS**, um zum AutoWDS-Einstellungsfenster zu gelangen.



2. Klicken Sie **AutoWDS aktiviert**, um die Funktion auf dem Gerät generell zu aktivieren.
3. Geben Sie unter **AutoWDS-Rollout-SSID** den Namen des AutoWDS-Basisnetzes ein. Standardmäßig verwendet LANconfig die Bezeichnung `AutoWDS-Rollout`.

   Die hier festgelegte SSID agiert als Managementnetz für sämtliche ein AutoWDS-Netz suchenden APs und ist – bis auf die Passphrase – nicht weiter konfigurierbar. Der WLC verbindet die angegebene SSID intern automatisch mit

einem WLC-Tunnel (**WLC-TUNNEL-AUTOWDS**). Normale WLAN-Clients sind nicht in der Lage, dieses Managementnetz zu benutzen.

Vergeben Sie hier zweckmäßigerweise eine vom LANconfig-Standard abweichende individuelle AutoWDS-Rollout-SSID.

Die Einrichtung des AutoWDS-Basisnetzes reduziert die Anzahl der SSIDs, die Ihr Gerät über eine physikalische WLAN-Schnittstelle maximal aufspannen kann, um den Wert 1.

4. Geben Sie unter **WPA2-Passphrase** einen Schlüssel ein, mit dem Sie das AutoWDS-Basisnetz absichern.

   Wählen Sie dazu einen möglichst komplexen Schlüssel mit mindestens 8 und maximal 63 Zeichen. Für eine angemessene Verschlüsselung sollte der Schlüssel mindestens 32 Zeichen umfassen.

5. Geben Sie unter **Verw. Frequenzbänder** das Frequenzband an, in dem die APs das AutoWDS-Basisnetz ausstrahlen.
6. Wählen Sie das **WLAN-Profil** aus, dessen SSIDs Sie mittels AutoWDS erweitern wollen.

   Die APs des betreffenden WLAN-Profils fungieren als Zugangs-APs und spannen das AutoWDS-Basisnetz auf. Gleichzeitig erhalten via AutoWDS eingebundene APs dieses WLAN-Profil als Standardkonfiguration, unter der sie nach erfolgreicher Integration die dazugehörige SSID aussenden.

7. Schließen Sie die geöffneten Dialogfenster mit **OK** und schreiben Sie die Konfiguration zurück auf das Gerät.

Der WLC weist nun allen gemanagten AutoWDS-fähigen APs in Ihrem WLAN die AutoWDS-Einstellungen zu, woraufhin diese das AutoWDS-Basisnetz aufspannen. Für künftige Rekonfigurationsprozesse verwenden die APs ausschließlich die hier hinterlegte SSID und Passphrase, sofern nicht anders konfiguriert (siehe *Unterschiede der Integrationsmodi* auf Seite 1201).

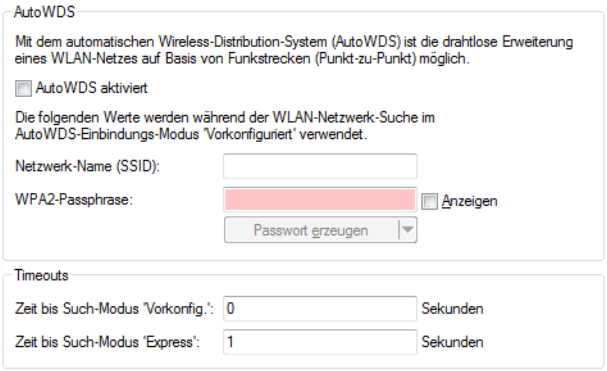
Die Konfiguration des WLC ist damit abgeschlossen. Fahren Sie nun mit der Konfiguration der APs fort.

14.6.3.2 Konfiguration der APs

Die nachfolgenden Handlungsanweisungen beschreiben die AutoWDS-Konfiguration eines AP für die vorkonfigurierte Integration. Die Konfigurationsschritte sind für sämtliche hinzukommenden APs identisch.

Die Konfiguration eines APs ist nicht notwendig, wenn der AP sich initial bereits mit einem WLC gepaired hat. Die manuelle Eingabe der SSID und der Passphrase ist optional für Geräte, die sich außerhalb der Reichweite des WLC befindet und damit ein Pairing unmöglich ist.

1. Öffnen Sie den Konfigurationsdialog in LANconfig und klicken Sie **Wireless-LAN** > **AutoWDS**, um zum AutoWDS-Einstellungsfenster zu gelangen.



2. Klicken Sie **AutoWDS aktiviert**, um die Funktion auf dem Gerät generell zu aktivieren.
3. Geben Sie unter **Netzwerk-Name (SSID)** den Namen des AutoWDS-Basisnetzes ein, das Sie auf dem WLC konfiguriert haben (z. B. `AutoWDS-Rollout`).
4. Geben Sie unter **WPA2-Passphrase** den Schlüssel des AutoWDS-Basisnetzes ein, den Sie auf dem WLC konfiguriert haben.

5. Ändern Sie die Timeout-Werte für die **Zeit bis Such-Modus 'Vorkonfig'** auf `1` und die **Zeit bis Such-Modus 'Express'** auf `0`.
6. Stellen Sie unter **Wireless LAN** > **Allgemein** > **Physikalische WLAN-Einst.** sicher, dass sich mindestens eine physikalische WLAN-Schnittstelle in der Betriebsart **Managed** befindet.
   Andernfalls sucht das Gerät zu keiner Zeit nach einem AutoWDS-Basisnetz.
7. Schließen Sie das Dialogfenster mit **OK** und schreiben Sie die Konfiguration zurück auf das Gerät.

Nach erfolgreichem Konfigurations-Update schaltet der AP seine physikalische(n) WLAN-Schnittstelle(n) in den Client-Modus und sucht nach dem eingetragenen AutoWDS-Basisnetz. Weitere Informationen zum Ablauf erhalten Sie im *Kapitel zur Funktionsweise*.

14.6.4 Vorkonfigurierte Integration durch Pairing beschleunigen

Über das einmalige Pairing von WLC und APs haben Sie die Möglichkeit, den Aufwand für die vorkonfigurierte Integration weiter zu reduzieren. Beim Pairing verbinden Sie im Vorfeld einen zurückgesetzten AP via LAN mit dem WLC, auf dem Sie Ihr gemanagtes WLAN inklusive AutoWDS eingerichtet haben. Im zurückgesetzten Zustand befindet sich der AP nach dem Einschalten automatisch im Managed-Modus. Findet der AP den WLC und akzeptiert der WLC den AP, erhält der AP automatisch sämtliche relevanten Zertifikate und Konfigurationsteile, welche die notwendigen Parameter im Gerät konfigurieren. Das Pairing ist dann abgeschlossen. Am Einsatzort installiert ein Mitarbeiter den AP und schaltet ihn ein. Das Gerät sucht dann automatisch nach dem vorkonfigurierten AutoWDS-Basisnetz.

Die nachfolgenden Schritte fassen die Vorgehensweise beim Pairing zusammen. Zusätzlich beinhalten Sie die Schritte zur automatischen Konfigurationszuweisung, um das Pairing bei einer hohen Anzahl von APs weiter zu vereinfachen.

1. Starten Sie LANconfig und richten Sie auf Ihrem WLC ein gemanagtes WLAN mit einem gültigen WLAN-Profil ein, sofern noch nicht geschehen. In LANconfig konfigurieren Sie ein solches Profil unter **WLAN-Controller** > **Profile** > **WLAN-Profile**.
2. Aktivieren Sie für dieses WLAN-Profil die AutoWDS-Funktion, wie im Abschnitt *Konfiguration des WLC* auf Seite 1207 beschrieben.
3. Legen Sie unter **WLAN-Controller** > **AP-Konfiguration** > **Access-Point-Tabelle** über die Schaltfläche **Default** ein für sämtliche APs allgemein gültiges Profil an. Weisen Sie diesem Profil dabei das zuvor eingerichtete **WLAN-Profil** zu
4. Aktivieren Sie unter **WLAN-Controller** > **Allgemein** die Option **APs automatisch eine Default-Konfiguration zuweisen**.
5. **Optional:** Um die Annahme hinzukommender APs in LANmonitor nicht manuell zu bestätigen, sondern dies durch den WLC zu automatisieren, aktivieren Sie in dem Dialog zusätzlich die Option **Automatische Annahme neuer APs aktiviert (Auto-Accept)**.

   Aus Sicherheitsgründen sollten Sie diese Option lediglich dann aktivieren, wenn Sie die hinzukommenden APs über eine LAN-Schnittstelle mit dem WLC verbunden haben. Achten Sie darauf, dass keine weiteren Geräte mit dem WLC verbunden sind, um ein mögliches Rogue-AP-Intrusion auszuschließen.
6. Übertragen Sie die Konfiguration zum WLC.
7. Resetten Sie den hinzukommenden AP und schließen Sie das Gerät via LAN an den WLC an.
   Das Gerät beginnt automatisch damit, nach einem WLC zu suchen.
8. Akzeptieren Sie im LANmonitor unter **Wireless LAN** > **Neue APs** den AP, sofern Sie keine automatische Annahme eingerichtet haben.
   Das Gerät erhält daraufhin vom WLC die benötigten Konfigurationsteile für den zukünftigen gemanagten Betrieb. Nach erfolgreicher Konfiguration listet LANmonitor das Gerät im Zweig **Aktive APs**.

Das Pairing ist damit abgeschlossen und der AP für den zukünftigen AutoWDS-Betrieb einsatzbereit.

14.6.5 Einrichtung mittels Express-Integration

Die nachfolgenden Abschnitte zeigen Ihnen, wie Sie ein AutoWDS-Netz über die Express-Integration einrichten. Die Konfiguration verwendet dabei das automatische Topologie-Management des WLC.

Das Ausgangsszenario gleicht dem der *vorkonfigurierten Integration*.

Auf einem zurückgesetzten AP ist AutoWDS standardmäßig deaktiviert, sodass Sie zunächst einen kabelgebundenen Zugriff wählen müssen, um die Funktion zu aktivieren. Eine Ausnahme besteht jedoch bei Geräten, die auf Kundenwunsch explizit auf das Feature hin getauft sind: In diesem Fall ist AutoWDS standardmäßig aktiviert. Der *2. Konfigurationteil* entfällt und die Geräte lassen sich im Express-Integrationsmodus unmittelbar in Betrieb nehmen.

Die Express-Konfiguration unterliegt sicherheitsrelevanten Besonderheiten. Lesen Sie sich daher das Kapitel *Unterschiede der Integrationsmodi* auf Seite 1201 aufmerksam durch.

14.6.5.1 Konfiguration des WLC

Die nachfolgenden Handlungsanweisungen beschreiben die AutoWDS-Konfiguration eines zentralen WLC für die Express-Integration.

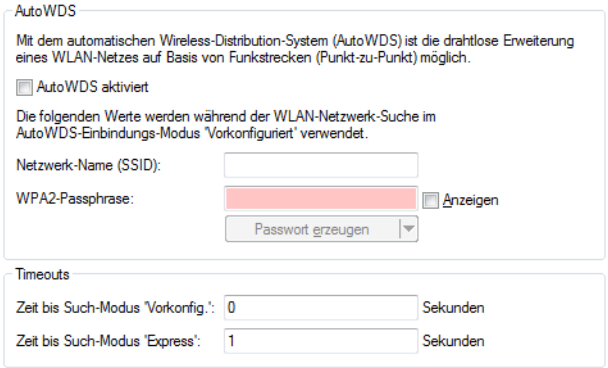
1. Führen Sie die einzelnen Handlungsschritte unter *Konfiguration des WLC* auf Seite 1207 für die vorkonfigurierte Integration aus.
2. Melden Sie sich über WEBconfig oder die Konsole an Ihrem Gerät an.
3. Wechseln Sie innerhalb des Setup-Menüs in die Tabelle **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Profile**.
4. Klicken Sie auf den Eintrag **DEFAULT**, um das AutoWDS-Standardprofil zu bearbeiten.
5. Ändern Sie den Parameter **Erlaube-Express-Integration** auf **ja** und speichern Sie die Einstellung mit einem Klick auf **Setzen**.

Die Konfiguration des WLC ist damit abgeschlossen. Fahren Sie nun mit der Konfiguration der APs fort.

14.6.5.2 Konfiguration der APs

Die nachfolgenden Handlungsanweisungen beschreiben die AutoWDS-Konfiguration eines AP für die Express-Integration. Die Konfigurationsschritte sind für sämtliche hinzukommenden APs identisch.

1. Öffnen Sie den Konfigurationsdialog in LANconfig und klicken Sie **Wireless-LAN** > **AutoWDS**, um zum AutoWDS-Einstellungsfenster zu gelangen.



2. Klicken Sie **AutoWDS aktiviert**, um die Funktion auf dem Gerät generell zu aktivieren.
3. Stellen Sie unter **Wireless LAN** > **Allgemein** > **Physikalische WLAN-Einst.** sicher, dass sich mindestens eine physikalische WLAN-Schnittstelle in der Betriebsart **Managed** befindet.
   Andernfalls sucht das Gerät zu keiner Zeit nach einem AutoWDS-Basisnetz.
4. Schließen Sie das Dialogfenster mit **OK** und schreiben Sie die Konfiguration zurück auf das Gerät.

Nach erfolgreichem Konfigurations-Update schaltet der AP seine physikalische(n) WLAN-Schnittstelle(n) in den Client-Modus und sucht nach einem beliebigen AutoWDS-Basisnetz. Weitere Informationen zum Ablauf erhalten Sie unter *Aufspannen des AutoWDS-Basisnetzes* auf Seite 1200.

14.6.6 Umschalten von Express- zu vorkonfigurierter Integration

Um nach einem Netz-Rollout mittels Express-Integration auf eine vorkonfigurierte Integration umzuschalten, deaktivieren Sie die Express-Integration auf dem WLC. Ein gezieltes Umschalten der APs entfällt, da die APs im Rahmen der Express-Integration bereits eine AutoWDS-Konfiguration erhalten haben, die ein AutoWDS-Netz für spätere Rekonfigurationsprozesse vorkonfiguriert.

1. Melden Sie sich über WEBconfig oder die Konsole an Ihrem Gerät an.
2. Wechseln Sie innerhalb des Setup-Menüs in die Tabelle **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Profile**.
3. Klicken Sie auf den Eintrag **DEFAULT**, um das AutoWDS-Standardprofil zu bearbeiten.
4. Ändern Sie den Parameter **Erlaube-Express-Integration** auf **nein** und speichern Sie die Einstellung mit einem Klick auf **Setzen**.

Damit haben Sie die Express-Integration für weitere hinzukommende APs deaktiviert.

14.6.7 Manuelles Topologie-Mangement

Die Einrichtungsbeispiele für AutoWDS verfolgen das automatische Topologie-Management durch den WLC, um die Konfiguration zu vereinfachen. Je nach Einsatzszenario kann es jedoch erforderlich sein, einzelne oder sämtliche P2P-Strecken manuell zu definieren.

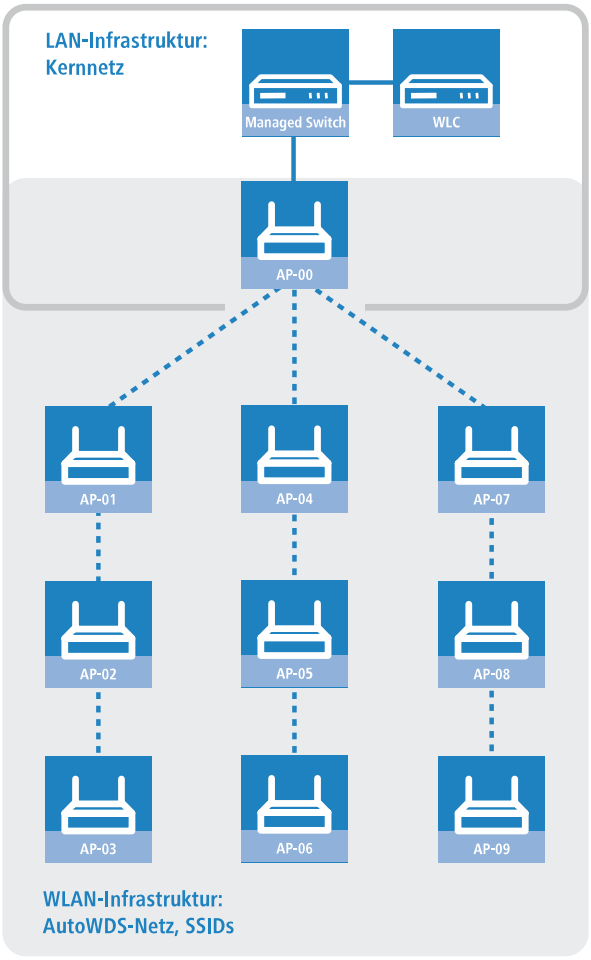
Der nachfolgende Abschnitt zeigt Ihnen, wie Sie das automatische Topologie-Management auf dem WLC deaktivieren und eine manuelle P2P-Konfiguration anlegen. Für die Konfiguration der P2P-Strecken ordnen Sie den APs zunächst eindeutige Namen zu, die Sie anschließend mit der Topologiekonfiguration und den verwendeten physikalischen WLAN-Schnittstellen verknüpfen. Das Kapitel geht davon aus, dass Sie die unter *Einrichtung mittels vorkonfigurierter Integration* auf Seite 1207 beschriebenen Schritte für den WLC bereits ausgeführt haben, um die Basis-Konfiguration abzuschließen und AutoWDS auf dem WLC generell zu aktivieren.



Generell ist ein AutoWDS-Betrieb von bis zu maximal 3 Hops empfehlenswert.

Änderungen am Ausgangsszenario

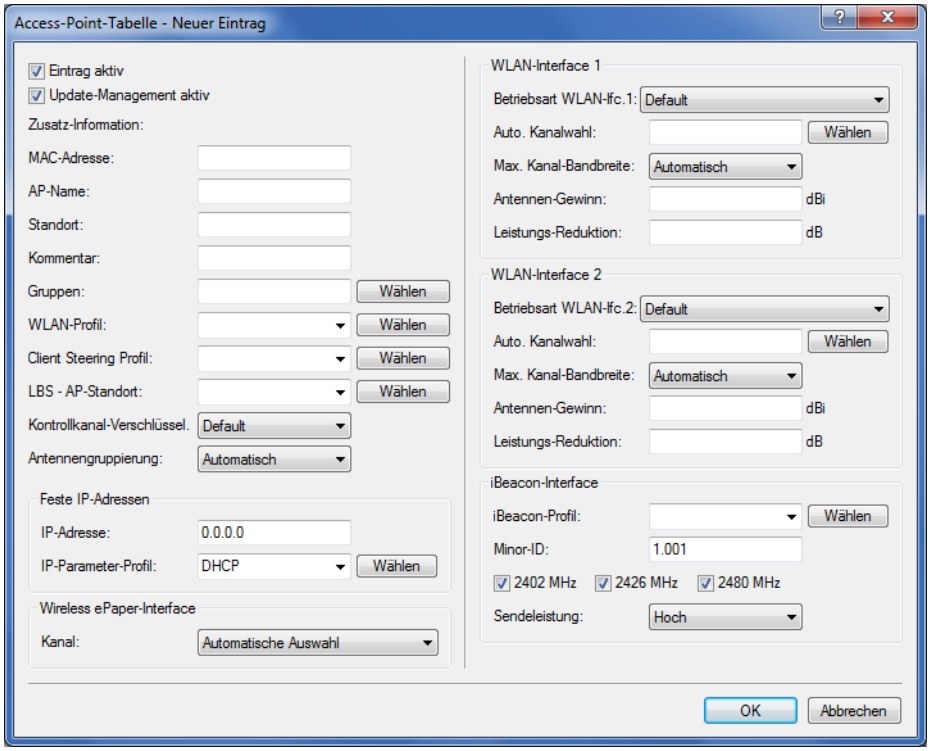
Das Ausgangsszenario gleicht dem der vorkonfigurierten Integration. Für die gesamte WLAN-Infrastruktur kommen ausschließlich Dual-Radio-APs zum Einsatz, die entsprechend der untenstehenden Grafik angeordnet sind. Das gemanagte WLAN besteht zu Beginn aus einem einzigen AP, der den hinzukommenden APs als initialer Zugangs-AP dient.



14.6.7.1 Konfiguration des WLC

Die nachfolgenden Handlungsanweisungen beschreiben die Deaktivierung des automatischen Topologie-Managements und die Konfiguration manueller P2P-Strecken gemäß des unter *Manuelles Topologie-Mangement* auf Seite 1211 beschriebenen Szenarios.

1. Öffnen Sie den Konfigurationsdialog in LANconfig und klicken Sie **WLAN-Controller** > **AP-Konfiguration** > **Access-Point-Tabelle**, um zur Liste der verwalteten APs zu gelangen.



2. Geben Sie für jeden hinzukommenden AP die **MAC-Adresse** und unter **AP-Name** einen eindeutigen Namen an. Auf diesen Namen referenzieren Sie später in der Topologie-Konfiguration.

   Für das Beispielszenario lauten die einzelnen Konfigurationseinträge wie folgt:

Tabelle 31: Konfiguration der hinzukommenden APs in der Access-Point-Tabelle

Eintrag	MAC-Adresse	AP-Name
01	00-80-63-a6-3d-f0	AP-00
02	00-a0-57-99-c6-4f	AP-01
03	00-80-63-b1-df-87	AP-02
04	00-a0-57-12-a8-01	AP-03
05	00-80-63-d9-ae-22	AP-04
06	00-a0-57-60-c4-3d	AP-05
07	00-a0-57-24-d4-1b	AP-06
08	00-80-63-a8-b1-37	AP-07
09	00-80-63-b1-df-99	AP-08
10	00-a0-57-33-e1-05	AP-09

Der Tabelleneintrag AP-00 bezieht sich auf Ihren bereits vorhandenen AP, welchen die hinzukommenden APs als Zugangs-AP nutzen.

3. Wählen Sie das **WLAN-Profil** aus, für das Sie AutoWDS aktiviert haben.
   Über das betreffende WLAN-Profil erhalten die APs automatisch die Einstellungen für AutoWDS und damit auch die P2P-Konfiguration zugewiesen.

4. Schließen Sie die geöffneten Dialogfenster mit **OK** und schreiben Sie die Konfiguration zurück auf das Gerät.
5. Melden Sie sich über WEBconfig oder die Konsole an Ihrem Gerät an.
6. Wechseln Sie innerhalb des Setup-Menüs in die Tabelle **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Profile**.
7. Klicken Sie auf den Eintrag **DEFAULT**, um das AutoWDS-Standardprofil zu bearbeiten.
8. Ändern Sie den Parameter **Topology-Management** auf **Manuell** und speichern Sie die Einstellung mit einem Klick auf **Setzen**.
9. Wechseln Sie in die Tabelle **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Topology** und klicken Sie **Hinzufügen**.
10. Legen Sie für jedes P2P-Paar eine manuelle P2P-Konfiguration an. Die festgelegte P2P-Strecke gilt stets aus Sicht des Slave-AP.
    a) Geben Sie im Feld **AutoWDS-Profil** das AutoWDS-Profil an, für das die manuelle P2P-Konfiguration gilt, z. B. `DEFAULT`.
    b) Setzen Sie die **Priorität** der P2P-Konfiguration auf `0` (höchste Priorität).
    c) Geben Sie für **Slave-AP-Name** und **Master-AP-Name** den Namen der APs entsprechend der von Ihnen gewählten Hierarchie ein.

       Für das Beispielszenario lauten die einzelnen Konfigurationseinträge bei strikter Schnittstellen-Paarung wie folgt:

       Tabelle 32: Konfiguration der P2P-Paare in der AutoWDS-Topology-Tabelle

Eintrag	Slave-AP-Name	Slave-AP-WLAN-Ifc.	Master-AP-Name	Master-AP-WLAN-Ifc.
01	AP-01	WLAN-1	AP-00	WLAN-1
02	AP-02	WLAN-2	AP-01	WLAN-2
03	AP-03	WLAN-1	AP-02	WLAN-1
04	AP-04	WLAN-2	AP-00	WLAN-2
05	AP-05	WLAN-1	AP-04	WLAN-1
06	AP-06	WLAN-2	AP-05	WLAN-2
07	AP-07	WLAN-1	AP-00	WLAN-1
08	AP-08	WLAN-2	AP-07	WLAN-2
09	AP-09	WLAN-1	AP-08	WLAN-1

    d) Geben Sie unter **Schluessel** die WPA2-Passphrase an, mit der die P2P-Partner die P2P-Strecke verschlüsseln.

       Wählen Sie dazu einen möglichst komplexen Schlüssel mit mindestens 8 und maximal 63 Zeichen. Für eine angemessene Verschlüsselung sollte der Schlüssel mindestens 32 Zeichen umfassen. Wenn Sie das Eingabefeld leer lassen, erzeugt das Gerät automatisch eine Passphrase mit einer Länge von 32 Zeichen.
    e) Schalten Sie den Eintrag **Aktiv** auf **Ja**.
    f) Speichern Sie den jeweiligen Eintrag mit einem Klick auf **Setzen**.

Waren bereits APs angeschlossen, übermittelt der WLC die neue Konfiguration an die APs und löst damit einen Rekonfigurationsprozess auf diesen aus. Waren noch keine APs angeschlossen, überträgt der WLC die P2P-Konfiguration beim ersten Verbindungsaufbau der hinzukommenden APs.

14.6.8 Redundante Strecken mittels RSTP

Das manuelle Topologie-Management eröffnet Ihnen in Kombination mit dem Rapid Spanning Tree Protocol (RSTP) die Möglichkeit, redundante P2P-Strecken einzurichten, um die Ausfallsicherheit Ihres gesamten AutoWDS-Basisnetzes zu verbessern. Hierzu müssen Sie RSTP zunächst im Setup-Menü eines jeden APs aktivieren, da sich die Management-Einstellungen des WLC nicht auf diesen Konfigurationsteil erstrecken. Um den Konfigurationsaufwand zu

reduzieren, ist der Einsatz eines Skripts empfehlenswert, welches Sie über das Skript-Management des WLC an sämtliche APs übertragen.

Die nachfolgenden Schritte zeigen Ihnen, wie Sie dabei vorgehen. Die Schritte implizieren, dass Sie ein AutoWDS-Basisnetz bereits erfolgreich eingerichtet haben. Nach seiner Aktivierung führt RSTP die Pfadsuche vollautomatisch durch.

1. Erstellen Sie eine Textdatei mit dem Namen `WLC_Script_1.lcs`.
2. Kopieren die folgenden Codezeilen in die Textdatei und speichern Sie.

```
# Script (9.000.0000 / 15.07.2014)

lang English
flash No

set /Setup/LAN-Bridge/Spanning-Tree/Protocol-Version        Rapid
set /Setup/LAN-Bridge/Spanning-Tree/Path-Cost-Computation   Rapid
set /Setup/LAN-Bridge/Spanning-Tree/Operating               yes

flash Yes

# done
exit
```

3. Melden Sie sich an der WEBconfig-Oberfläche Ihres WLCs an und wählen Sie **Extras** > **Dateimanagement** > **Zertifikat oder Datei hochladen**.
4. Wählen Sie in der Auswahlliste **Dateityp** den Eintrag **CAPWAP – WLC_Script_1.lcs** und über die Schaltfläche **Durchsuchen** die zuvor angelegte Skriptdatei aus. Klicken Sie anschließend auf **Upload starten**.
   Den erfolgreichen Upload des Skripts in den WLC prüfen Sie z. B. über das Status-Menü unter **Dateisystem** > **Inhalt**.
5. Wechsel Sie im Setup-Menü zum Menüpunkt **WLAN-Management** > **Zentrales-Firmware-Management** > **Skriptverwaltung** und klicken Sie **Hinzufügen**.
6. Geben Sie als **Profil** Ihr entsprechendes WLAN-Profil an und als **Name** `WLC_Script_1.lcs` ein, um das AutoWDS-Profil mit dem Skriptnamen zu verbinden und an die APs auszurollen.
7. Weisen Sie – wie in Kapitel *Konfiguration des WLC* auf Seite 1212 beschrieben – den APs im WLC eindeutige Namen zu und richten Sie die manuellen P2P-Strecken ein.

Damit haben Sie die Konfiguration erfolgreich abgeschlossen.

14.7 Zentrales Firmware- und Skript-Management

Mit einem WLC kann die Konfiguration von mehreren LANCOM Wireless Routern und APs von einer Stelle aus komfortabel und konsistent verwaltet werden. Mit dem zentralen Firmware- und Skript-Management können auch Firmware- und Skript-Uploads auf allen verwalteten WLAN-Geräten automatisch ausgeführt werden.

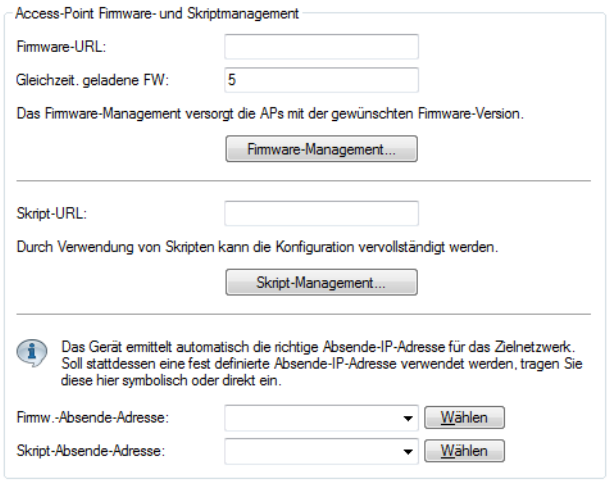
Dazu werden die Firmware- und Skript-Dateien auf einem Web-Server abgelegt (Firmware als *.UPX, Skripte als *.LCS). Der WLC prüft einmal täglich oder aufgrund einer entsprechenden Benutzeraktion den Bestand und vergleicht die verfügbaren Dateien mit den Versionen in den Geräten – alternativ kann dieser Vorgang auch über einen Cron-Job z. B. nachts erledigt werden. Wenn ein Update durchgeführt werden kann oder nicht die gewünschte Version auf dem AP läuft, lädt der WLC diese vom Webserver herunter und spielt sie in die entsprechenden Wireless Router und APs ein.

Mit der Konfiguration des Firmware- und Skript-Managements kann die Distribution der Dateien gezielt gesteuert werden. So kann die Nutzung von bestimmten Firmware-Versionen z. B. auf bestimmte Gerätetypen oder MAC-Adressen beschränkt werden.

Das Update kann in zwei möglichen Zuständen ausgeführt werden:

- Beim Verbindungsaufbau, danach startet der AP automatisch neu.
- Wenn der AP schon verbunden ist, startet das Gerät danach **nicht** automatisch neu. In diesem Fall wird der AP manuell über die Menüaktion **Setup** > **WLAN-Management** > **Zentrales-Firmware-Management** > **Aktualisierte-APs-neustarten** oder zeitgesteuert per Cron-Job neu gestartet.

- Mit der Aktion **Setup** > **WLAN-Management** > **Zentrales-Firmware-Management** > **Aktualisiere-Firmware-und-Skript-Information** können Skript- und Firmwareverzeichnisse aktualisiert werden.



Sie finden die Parameter zur Konfiguration auf folgenden Pfaden:

LANconfig: **WLAN-Controller** > **AP-Update**

WEBconfig: **Setup** > **WLAN-Management** > **Zentrales-Firmware-Management**

14.7.1 Allgemeine Einstellungen für das Firmware-Management

- **Firmware-URL**

  Pfad zum Verzeichnis mit den Firmware-Dateien.

  - Mögliche Werte: URL in der Form `Server/Verzeichnis` oder `http://Server/Verzeichnis`
  - Default: leer

  Beachten Sie, dass der angegebene Web-Server das Directory Listing erlauben muss. Das Firmware-Management bezieht auf diese Weise die Information über die angebotenen Firmwares.

- **Gleichzeitig geladene FW**

  Anzahl der gleichzeitig im Arbeitsspeicher des WLCs vorgehaltenen Firmware-Versionen.

  Die hier vorgehaltenen Fimrware-Versionen werden nur einmal vom Server geladen und anschließend für alle passenden Update-Prozesse genutzt.

  - Mögliche Werte: 1 bis 10
  - Default: 5

- **Firmware-Absende-IP-Adresse**

  Hier können Sie optional eine Absendeadresse konfigurieren, die statt der automatisch für die Zieladresse gewählten Absendeadresse verwendet wird.

  Mögliche Werte:

  - Name eines definierten IP-Netzwerks.
  - 'INT' fur die IP-Adresse im ersten Netzwerk mit der Einstellung 'Intranet'.
  - 'DMZ' für die IP-Adresse im ersten Netzwerk mit der Einstellung 'DMZ'.
  - Name einer Loopback-Adresse.
  - Beliebige andere IP-Adresse.

  Default:

- leer

Wenn in der Liste der IP-Netzwerke oder in der Liste der Loopback-Adressen ein Eintrag mit dem Namen 'INT' oder 'DMZ' vorhanden ist, wird die IP-Adresse des IP-Netzwerks bzw. der Loopback-Adresse mit dem Namen 'INT' bzw. 'DMZ' verwendet.

14.7.1.1 Firmware-Management-Tabelle

In dieser Tabelle wird hinterlegt, welche Geräte (MAC-Adresse) und Gerätetypen mit welcher Firmware betrieben werden sollen.

Gerätetypen

Wählen Sie hier aus, für welchen Gerätetyp die in diesem Eintrag spezifizierte Firmware-Version verwendet werden soll.

- Mögliche Werte: Alle oder Auswahl aus der Liste der verfügbaren Gerätetypen.
- Default: Alle

MAC-Adresse

Wählen Sie hier aus, für welches Gerät (identifiziert anhand der MAC-Adresse) die in diesem Eintrag spezifizierte Firmware-Version verwendet werden soll.

- Mögliche Werte: Gültige MAC-Adresse.
- Default: Leer

Version

Firmware-Version, welche für die in diesem Eintrag spezifizierten Geräte oder Gerätetypen verwendet werden soll. Auf diese Version der Firmware wird ggf. ein Update für die spezifizierten Geräte bzw. Gerätetypen erfolgen. Die Angabe erfolgt in der Form: „xx.yy“, z. B. 10.40. Default: Leer

Datum

Das Datum ermöglicht ein Downgrade auf eine spezifische Firmware-Version innerhalb einer Release, z. B. von einem Release-Upgrade (RU) auf ein früheres Upgrade.

- Mögliche Werte: 8 Zeichen aus 0123456789. Der Eintrag muss dem Format des UPX-Headers entsprechen, also z. B. „01092014“ für den 01.09.2014.
- Default: Leer

14.7.1.2 Allgemeine Einstellungen für das Skript-Management

- **Skript-URL**

  Pfad zum Verzeichnis mit den Skript-Dateien.

  Mögliche Werte:

  - URL in der Form `Server/Verzeichnis` oder `http://Server/Verzeichnis`
  - Default: Leer

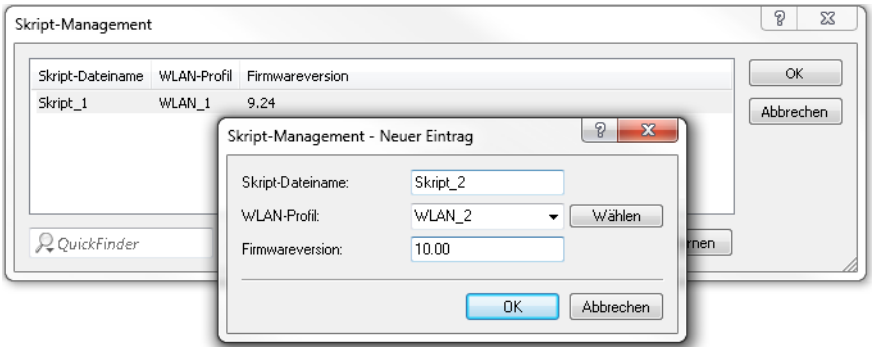
14.7.1.3 Skript-Management-Tabelle

In dieser Tabelle werden Skripte anhand ihres Dateinamens einem WLAN-Profil zugeordnet.

Die Konfiguration eines Wireless Routers und Access Points in der Betriebsart „Managed“ erfolgt über WLAN-Profile. Mit einem Skript können auch diejenigen Detail-Parameter der gemanagten Geräte eingestellt werden, die nicht im Rahmen der vorgegebenen Parameter eines WLAN-Profils verwaltet werden. Dabei erfolgt die Zuordnung ebenfalls über

die WLAN-Profile, um für die Wireless Router und APs mit gleicher WLC-Konfiguration auch das gleiche Skript zu verwenden.

Da für jedes WLAN-Profil nur eine Skript-Datei angegeben werden kann, ist hier keine Versionierung möglich. Bei der Zuweisung eines Skripts zu einem Wireless Router oder Access Point wird allerdings eine MD5-Prüfsumme der Skript-Datei gespeichert. Über diese Prüfsumme kann der WLC bei einer neuen oder geänderten Skript-Datei mit gleichem Dateinamen feststellen, ob die Skript-Datei erneut übertragen werden muss.



Skript-Dateiname

Tragen Sie den CAPWAP-Slot ein, den Sie beim Upload des Skriptes in den WLAN-Controller ausgewählt haben (WLC_Script_1.lcs, WLC_Script_2.lcs oder WLC_Script_3.lcs). Bezieht der WLAN-Controller das Skript von einem Web-Server, muss der Skript-Name des Skriptes auf dem Web-Server hinterlegt werden. Mögliche Werte: Dateiname in der Form `*.lcs`. Default: Leer.

WLAN-Profil

Wählen Sie hier aus, für welches WLAN-Profil die in diesem Eintrag spezifizierte Skript-Datei verwendet werden soll. Mögliche Werte: Auswahl aus der Liste der definierten WLAN-Profile. Default: Leer

Firmwareversion

Mit der Angabe einer Firmwareversion legen Sie fest, für welche LCOS-Version das entsprechende Skript ausgerollt werden soll.

Bitte beachten Sie, die Firmware in der Form „xx.yy“ anzugeben, z. B. 10.00 oder 9.24.

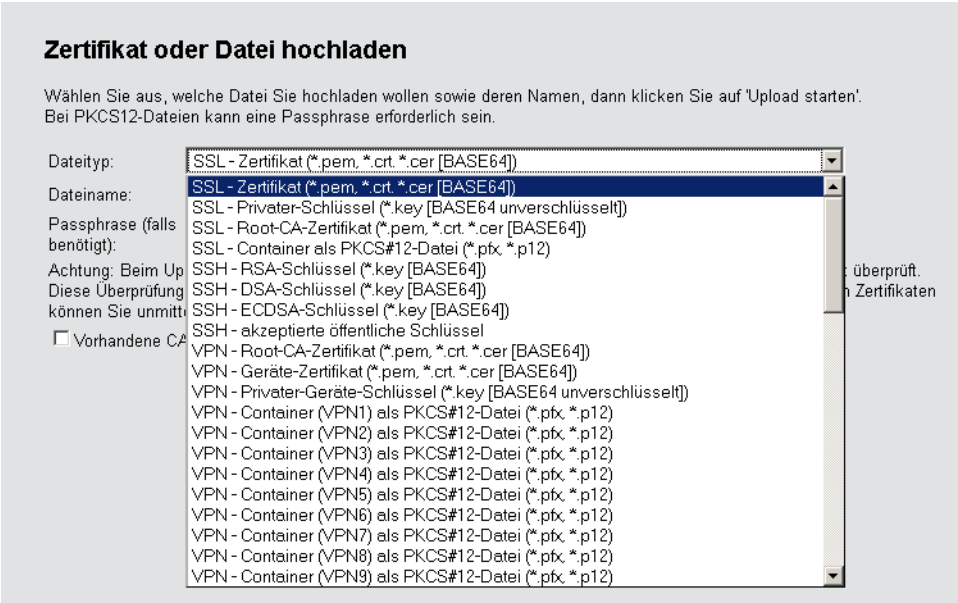
14.7.1.4 Interner Skript-Speicher (Skript-Management ohne HTTP-Server)

Skripte haben im Gegensatz zu Firmware-Dateien oft nur ein geringes Datenvolumen. Im internen Skript-Speicher der WLCs können drei Skripte mit maximal je 64kB Größe gespeichert werden. Wenn der Bedarf für Skripte nicht über dieses Volumen hinausgeht, kann die Einrichtung eines HTTP-Servers für diesen Zweck entfallen.

Die Skript-Dateien werden dazu einfach über WEBconfig auf den vorgesehenen Speicherplatz geladen. Nach dem Upload muss die Liste der verfügbaren Skripte mit der Aktion **Setup** > **WLAN-Management** > **Zentrales-Firmware-Management** > **Aktualisiere-Firmware-und-Skript-Information** aktualisiert werden.

Aus der Skript-Management-Tabelle können diese internen Skripte den entsprechenden Namen referenziert werden (WLC_Script_1.lcs, WLC_Script_2.lcs oder WLC_Script_3.lcs).

Bitte beachten Sie bei der Angabe der Script-Namen die Groß- und Kleinschreibung!



14.8 RADIUS

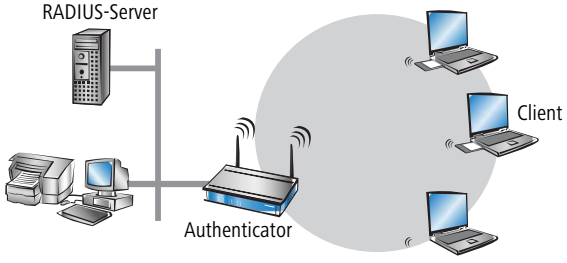
RADIUS steht für „Remote Authentication Dial-In User Service" und wird als „Triple-A-Protokoll" bezeichnet. Dabei stehen die drei „A" für

- Authentication (Authentifizierung)
- Authorization (Autorisierung)
- Accounting (Abrechnung)

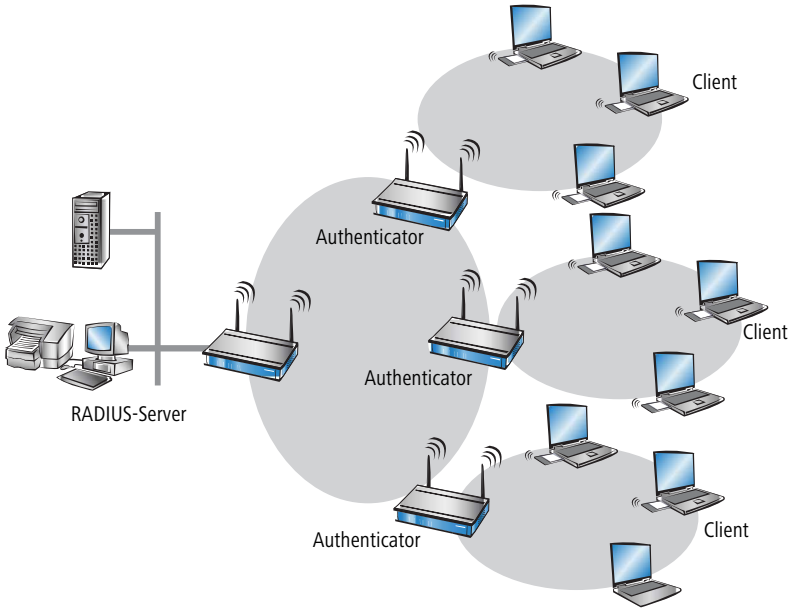
Sie können mit diesem Protokoll Benutzern Zugang zu einem Netz gewähren, ihnen bestimmte Rechte zuweisen und ihre Aktionen verfolgen. Gegebenenfalls können Sie auch die in Anspruch genommenen Leistungen gegenüber dem Benutzer mit Hilfe des RADIUS-Servers abrechnen (z. B. bei WLAN Hotspots). Für jede Aktion, die vom Benutzer durchgeführt wird, kann der RADIUS-Server eine Autorisierung durchführen, und so den Zugriff auf Netzwerkressourcen je nach Benutzer freigeben oder sperren.

Damit RADIUS funktioniert, sind 3 verschiedene Geräte nötig.

- Client: Das ist ein Gerät (PC, Notebook etc.) über das der Benutzer sich in das Netz einwählen möchte.
- Authenticator: Eine Netzwerkkomponente, welche die Authentifizierung weiterleitet und zwischen dem Netz und dem Client liegt. Diese Aufgabe kann z. B. ein Access Point übernehmen. Der Authenticator wird auch als Network Access Server (NAS) bezeichnet.



- Authentication-Server: RADIUS-Server, auf dem die Daten für die Benutzer konfiguriert sind. Dieser steht gewöhnlich in dem Netz, für das er Zugangsberechtigungen erteilen soll. Er ist für den Client über den Authenticator erreichbar. Auch für diese Aufgabe kann in entsprechenden Szenarien ein Access Point eingesetzt werden.



Der Authenticator hat zunächst keine Informationen über die Clients, die sich anmelden wollen. Diese sind alle in einer Datenbank des RADIUS-Servers gespeichert. Welche Anmeldeinformationen der RADIUS-Server für die Authentifizierung benötigt, ist dort in der Datenbank hinterlegt und kann von Netzwerk zu Netzwerk variieren. Der Authenticator hat nur die Aufgabe, die Informationen zwischen dem Client und dem RADIUS-Server zu übertragen.

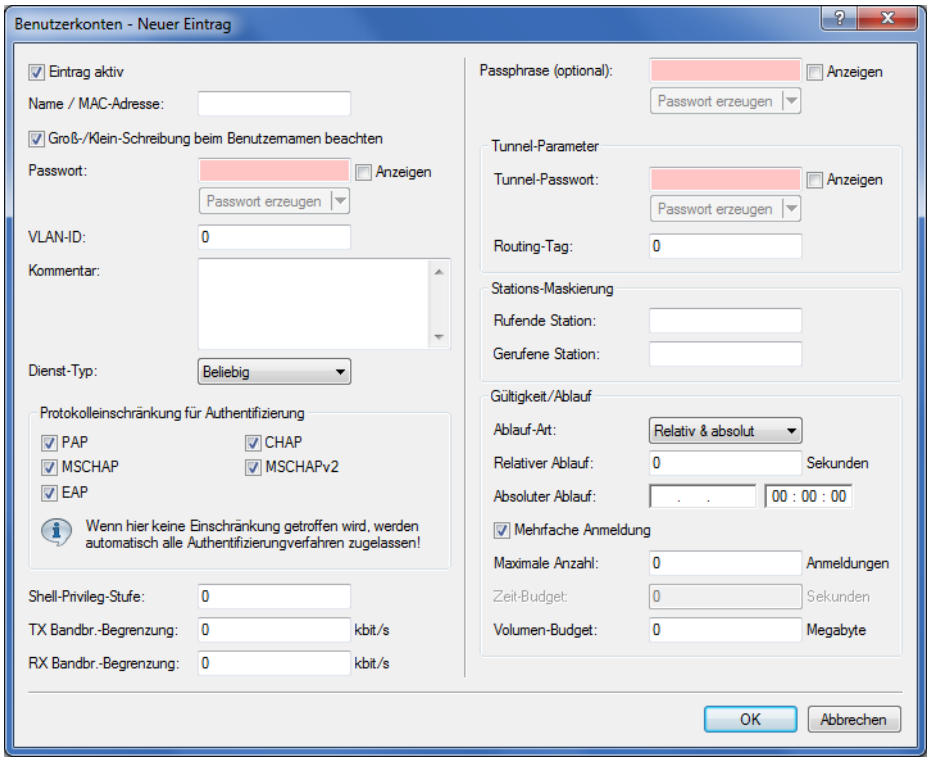
Der Zugang zu einem RADIUS-Server kann über verschiedene Wege aufgebaut werden:

- Über PPP bei der Einwahl in ein Netzwerk
- Über WLAN
- Über einen Public Spot für Benutzer, die sich per Browser anmelden
- über das 802.1X-Protokoll

14.8.1 Prüfung der WLAN-Clients über RADIUS (MAC-Filter)

Bei der Nutzung von RADIUS zur Authentifizierung der WLAN-Clients kann neben einem externen RADIUS-Server auch die interne Benutzertabelle der WLC genutzt werden, um nur bestimmten WLAN-Clients anhand ihrer MAC-Adresse den Zugang zum WLAN zu erlauben.

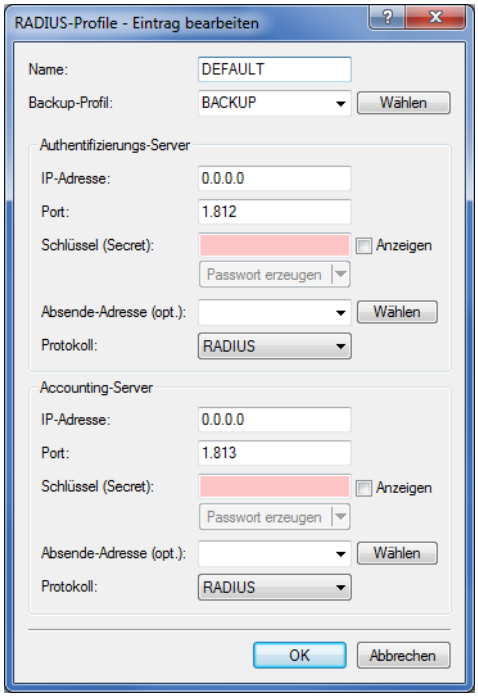
Tragen Sie die zugelassenen MAC-Adressen über LANconfig in die RADIUS-Datenbank im Konfigurationsbereich **RADIUS** > **Server** auf der Registerkarte **Allgemein** ein. Verwenden Sie dabei die MAC-Adresse als **Name** und ebenso als **Passwort** und wählen Sie als Authentifizierungsmethode **Alle**.



14.8.2 Externer RADIUS-Server

Standardmäßig übernimmt der WLC die Weiterleitung von Anfragen für die Konto- bzw. Zugangsverwaltung an einen RADIUS-Server. Damit die APs den RADIUS-Server direkt ansprechen können, müssen entsprechenden Server-Informationen hier definiert werden. Somit funktioniert die RADIUS-Anwendung auch dann noch, wenn der WLC nicht erreichbar ist. Allerdings müssen dafür Einstellungen für jeden einzelnen AP im adressierten RADIUS-Server vorgenommen werden und

die managed APs müssen den RADIUS-Server aus ihrem Management-Netz heraus erreichen können. Ist der RADIUS-Server in einem anderen IP-Netz, muss über das IP-Parameter-Profil insbesondere das Gateway definiert werden.



LANconfig: **WLAN-Controller** > **Profile** > **RADIUS-Profile**

Name

Geben Sie eine Bezeichnung für diesen Eintrag ein.

Backup-Profil

Wählen Sie aus der Liste der RADIUS-Server-Profile ein Profil als Backup-Server.

Authentifizierungs-Server

IP-Adresse

Tragen Sie die IP-Adresse des Authentifizierungs-Servers ein.

Port

Tragen Sie den Port des Authentifizierungs-Servers ein.

Schlüssel (Secret)

Dieser Eintrag enthält den Schlüssel (Shared Secret) zur Autorisierung.

Anzeigen

Ativiert / deaktiviert die Anzeige des Schlüssels.

Absende-Adresse (optional)

Geben Sie hier ggf. die Loopback-Adresse des Gerätes an.

Protokoll

Wählen Sie aus dem Drop-Down-Menü zwischen dem normalen RADIUS-Protokoll und dem sicheren RADSEC-Protokoll für die RADIUS-Anfrage.

Accounting-Server

IP-Adresse

Tragen Sie die IP-Adresse des Accounting-Servers ein.

Port

Tragen Sie den Port des Accounting-Servers ein.

Schlüssel (Secret)

Dieser Eintrag enthält den Schlüssel (Shared Secret) zur Autorisierung.

Anzeigen

Ativiert / deaktiviert die Anzeige des Schlüssels.

Absende-Adresse (optional)

Geben Sie hier ggf. die Loopback-Adresse des Gerätes an.

Protokoll

Wählen Sie aus dem Drop-Down-Menü zwischen dem normalen RADIUS-Protokoll und dem sicheren RADSEC-Protokoll für die RADIUS-Anfrage.

14.8.3 Dynamische VLAN-Zuweisung

In einer größeren WLAN-Struktur ist es oft sinnvoll, den einzelnen WLAN-Clients ein bestimmtes Netzwerk zuzuweisen. Solange sich die WLAN-Clients immer in der Reichweite des gleichen APs befinden, kann diese Zuweisung über die SSID in Verbindung mit einem bestimmten IP-Netzwerk realisiert werden. Wechseln die WLAN-Clients hingegen häufig die Position und buchen sich dann bei unterschiedlichen APs ein, befinden sie sich je nach Konfiguration in einem anderen IP-Netzwerk.

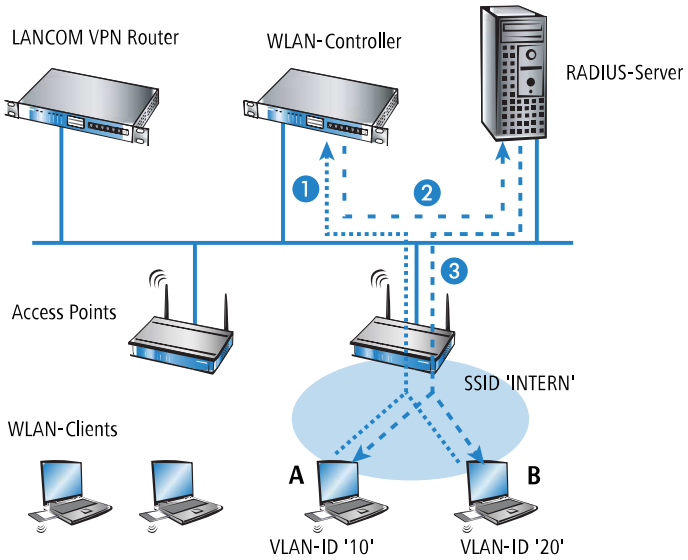
Um die WLAN-Clients **unabhängig** von dem WLAN-Netzwerk, in dem sie sich gerade eingebucht haben, in ein bestimmtes Netzwerk zu leiten, können dynamisch zugewiesene VLANs genutzt werden. Anders als bei den statisch konfigurierten VLAN-IDs für eine bestimmte SSID wird die VLAN-ID dabei dem WLAN-Client von einem RADIUS-Server direkt zugewiesen.

Beispiel:

- Die WLAN-Clients der Mitarbeiter buchen sich über einen AP in das WPA2-gesicherte WLAN mit der SSID 'INTERN' ein. Bei der Anmeldung werden die RADIUS-Anfragen der WLAN-Clients an den AP gestellt. Wenn sich das entsprechende WLAN-Interface in der Betriebsart 'Managed' befindet, werden die RADIUS-Anfragen automatisch an den WLC weitergereicht. Dieser leitet die Anfragen seinerseits an den konfigurierten RADIUS-Server weiter. Der RADIUS-Server kann die Zugangsberechtigung der WLAN-Clients prüfen. Darüber hinaus kann er allerdings auch z. B. anhand der MAC-Adresse eine bestimmte VLAN-ID für die jeweilige Abteilung zuweisen. Dabei erhält z. B. der WLAN-Client aus dem Marketing die VLAN-ID '10' und WLAN-Client aus der Entwicklung die '20'. Wenn für den Benutzer keine VLAN-ID definiert ist, wird die Haupt-VLAN-ID der SSID verwendet.
- Die WLAN-Clients der Gäste buchen sich über den gleichen AP in das nicht gesicherte WLAN mit der SSID 'PUBLIC' ein. Diese SSID ist statisch auf die VLAN-ID '99' gebunden und leitet die Gäste so in einen bestimmtes Netzwerk. Statische und dynamische VLAN-Zuweisung können also sehr elegant parallel genutzt werden.

Die Zuweisung der VLAN-ID kann im RADIUS-Server auch anhand von anderen Kriterien erfolgen, z. B. über die Kombination aus Benutzername und Kennwort. Auf diese Weise kann z. B. den unbekannten MAC-Adressen der Besucher in einer Firma eine VLAN-ID zugewiesen werden, die für den Gastzugang z. B. nur die Internetnutzung erlaubt, jedoch keinen Zugang zu anderen Netzwerkressourcen.

Alternativ zu einem externen RADIUS-Server kann den WLAN-Clients auch über den internen RADIUS-Server oder die Stationstabelle im WLC eine VLAN-ID zugewiesen werden.



1. Aktivieren Sie das VLAN-Tagging für den WLC. Tragen Sie dazu als Management-VLAN-ID in den physikalischen Parametern des Profils einen Wert größer als '0' ein.
2. Für eine Authentifizierung über 802.1X wählen Sie in den Verschlüsselungseinstellungen für das logische WLAN-Netzwerk des Profils eine Einstellung, die eine Authentifizierungsanfrage auslöst.
3. Für eine Prüfung der MAC-Adressen aktivieren Sie für das logische WLAN-Netzwerk des Profils die MAC-Prüfung.

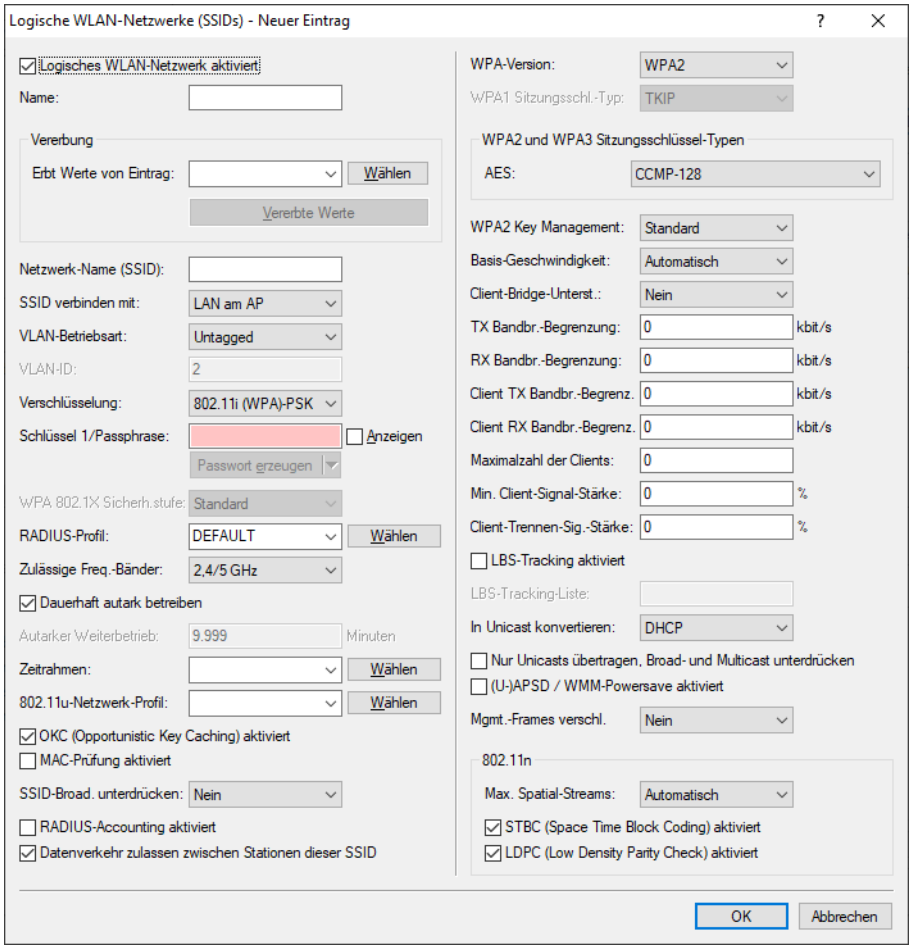
   Sowohl für die Authentifizierung über 802.1X als auch für die Prüfung der MAC-Adressen ist bei der Verwaltung von WLAN-Modulen über einen WLC ein RADIUS-Server erforderlich. Der WLC trägt sich dabei automatisch in den von ihm verwalteten APs als RADIUS-Server ein – alle RADIUS-Anfragen an die APs werden daher direkt an den WLC weitergeleitet, der die Anfragen entweder selbst bearbeiten oder sie alternativ an einen externen RADIUS-Server weiterleiten kann.
4. Für eine Weiterleitung der RADIUS-Anfragen an einen anderen RADIUS-Server tragen Sie dessen Adresse über LANconfig in die Liste der Forwarding-Server im Konfigurationsbereich 'RADIUS-Server' auf der Registerkarte **Forwarding** ein. Alternativ tragen Sie die externen RADIUS-Server über WEBconfig ein unter **Menübaum** > **LCOS-Setup** > **RADIUS** > **Server** > **Weiterleit-Server**. Stellen Sie außerdem den Standard-Realm sowie den leeren Realm ein, um auf unterschiedliche Benutzerinformationen (mit unbekanntem oder ganz ohne Realm) gezielt reagieren zu können.
5. Konfigurieren Sie die Einträge im RADIUS-Server entsprechend, damit den anfragenden WLAN-Clients anhand bestimmter Merkmale die richtigen VLAN-IDs zugewiesen werden.

Weitere Information zu RADIUS finden Sie in der Dokumentation Ihres RADIUS-Servers.

14.8.4 RADIUS-Accounting im WLAN-Controller für logische WLANs aktivieren

Die Konfiguration der logischen WLAN-Netzwerke finden Sie in folgendem Menü:

LANconfig: **WLAN-Controller** > **Profile** > **Logische WLAN-Netzwerke (SSIDs)**



RADIUS-Accounting aktiviert

Stellen Sie hier ein, ob das RADIUS-Accounting in diesem logischen WLAN-Netzwerk aktiviert werden soll.

Mögliche Werte:

› ja, nein

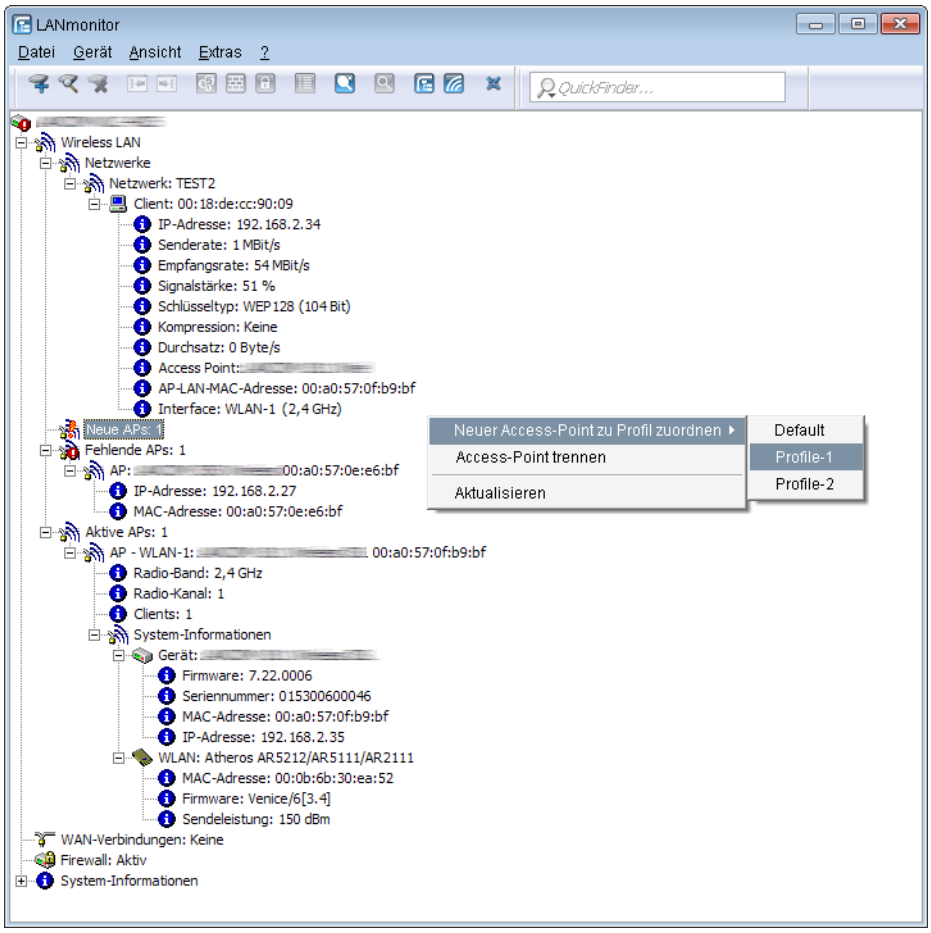
Default:

› nein

Die APs, die der WLC mit diesem logischen WLAN-Netzwerk konfiguriert, müssen eine LCOS-Version 8.00 oder höher verwenden.

14.9 Anzeigen und Aktionen im LANmonitor

Über den LANmonitor haben Sie einen schnellen Überblick über die WLC im Netzwerk und die APs in der WLAN-Struktur. LANmonitor zeigt dabei u. a. die folgenden Informationen:



- Aktive WLAN-Netzwerke mit den eingebuchten WLAN-Clients sowie der Bezeichnung des APs, bei dem der WLAN-Client eingebucht ist.
- Anzeige der neuen APs mit IP- und MAC-Adresse
- Anzeige der fehlenden APs mit IP- und MAC-Adresse
- Anzeige der gemanagten APs mit IP- und MAC-Adresse, verwendetem Frequenzband und Kanal

> Falls der AP wegen einer älteren Firmware diese Daten nicht überträgt, entnimmt der WLC den Kanal und die Frequenz aus der Status-Tabelle **Aktive-Radios** unter **Status** > **Aktive-Radios** > **WLAN-Management** > **AP-Status**.

Über die rechte Maustaste kann auf den APs ein Kontext-Menü geöffnet werden, in dem folgende Aktionen zur Auswahl stehen:

- **Neuen Access Point zu Profil zuordnen**

  Bietet die Möglichkeit, einem neuen AP eine Konfiguration zuzuordnen und ihn so in die WLAN-Struktur aufzunehmen.

- **Access Point trennen**

Trennt die Verbindung zwischen AP und WLC. Der AP sucht dann erneut nach einem zuständigen WLC. Diese Aktion wird z. B. verwendet, um APs nach einem Backup-Fall vom Backup-WLC zu trennen und wieder auf den eigentlichen WLC zu leiten.

› **Aktualisieren**

Aktualisiert die Anzeige des LANmonitors.

14.10 Funkfeldoptimierung

Mit der Auswahl des Kanals in der Kanal-Liste wird der Teil des Frequenzbandes festgelegt, den ein AP für seine logischen WLANs verwendet. Alle WLAN-Clients, die sich mit einem AP verbinden wollen, müssen den gleichen Kanal im gleichen Frequenzband verwenden. Im 2,4-GHz-Band stehen je nach Land die Kanäle 1 bis 13, im 5-GHz-Band die Kanäle 36 bis 64 zur Verfügung. Auf einem Kanal kann dabei zeitgleich jeweils nur ein AP Daten übertragen. Um in der Funkreichweite eines anderen APs ein WLAN mit maximaler Bandbreite betreiben zu können, muss jeder AP einen separaten Kanal nutzen – anderenfalls müssen sich die WLANs die Bandbreite des Kanals teilen.

Bei einer völlig offenen Kanalliste werden die APs möglicherweise automatisch Kanäle wählen, die sich gegenseitig teilweise überlappen und so die Signalqualität reduzieren. Außerdem könnten die APs evtl. Kanäle wählen, welche die WLAN-Clients aufgrund der Ländereinstellung nicht nutzen können. Um die APs gezielt auf bestimmte Kanäle zu leiten, können z. B. die überlappungsfreien Kanäle 1, 6, 11 in der Kanalliste aktiviert werden.

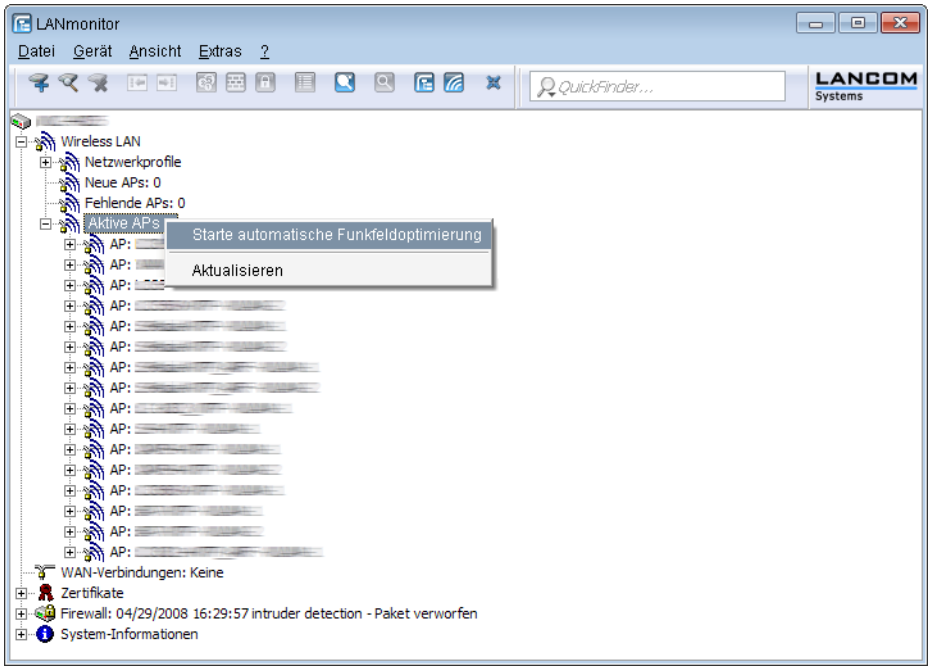
In größeren Installationen mit mehreren APs ist es manchmal schwierig, für jeden AP einen geeigneten Kanal einzustellen. Mit der automatischen Funkfeldoptimierung bieten die WLCs ein Verfahren, um die optimalen Kanäle der APs für das 2,4-GHz- und 5-GHz-Band automatisch einzustellen.

Für APs, die im 5-GHz-Band funken, muss sichergestellt sein, dass der "Indoor-Only"-Modus aktiviert ist.

Konsole: **Setup** > **WLAN-Management** > **Starte-automatische-Funkfeldoptimierung**

Sie können die Optimierung auch gezielt für einen einzelnen AP starten, indem Sie die MAC-Adresse als Parameter für die Aktion eintragen.

LANmonitor: Klicken Sie mit der rechten Maustaste auf die Liste der aktiven APs oder auf ein bestimmtes Gerät und wählen Sie danach im Kontextmenü **Starte automatische Funkfeldoptimierung**.



Die Optimierung läuft dann in den folgenden Schritten ab:

1. Der WLC weist allen APs den gleichen Kanal zu. Hierbei verwendet er den Kanal, der von den meisten APs genutzt wird.
2. Die APs führen einen "Background-Scan" durch und melden das Ergebnis an den WLC.
3. Der WLC bestimmt für jeden AP auf Basis der im "Background-Scan" erkannten Geräte einen Interferenzwert.
4. Anschließend löscht er die AP-Kanalliste aller APs. Da die Kanalliste nun leer ist, erhalten die APs über ein Konfigurations-Update die neue Kanalliste ihres jeweiligen Profils.
5. Der WLC deaktiviert die Funkmodule aller APs.
6. Die einzelnen APs durchlaufen nun nacheinander die folgenden Schritte. Es beginnt der AP mit dem höchsten Interferenzwert, um sicherzustellen, dass dieser AP zuerst einen Kanal wählen kann.
7. In der Reihenfolge der Interferenzwerte aktiviert der WLC die Funkmodule der APs, die daraufhin die automatische Einmessung starten. Der jeweilige AP sucht selbstständig den für ihn besten Kanal aus der ihm zugewiesenen Kanalliste. Zur Bestimmung des am besten geeigneten Kanals führt der AP jeweils eine Interferenz-Messung durch, so dass er Signalstärken und Kanäle anderer APs entsprechend berücksichtigen kann. Da die bisherige Liste in der Konfiguration des WLCs gelöscht wurde, ist dies nun die Profilkanalliste. Wenn die Profilkanalliste leer ist, hat der AP die freie Auswahl aus den nicht durch andere Funk-Module belegten Kanälen. Der gefundene Kanal wird zurück an den WLC gesendet und dort in der AP-Kanalliste gespeichert. Somit erhält der AP beim nächsten Verbindungsaufbau wieder diesen Kanal. Die AP-Kanalliste hat so gesehen ein höheres Gewicht als die Profilkanalliste.

Verfügt ein AP über mehrere WLAN-Module, so durchläuft jedes WLAN-Modul nacheinander diesen Vorgang.

Die Funkfeldoptimierung ist Bestandteil von *LANCOM Active Radio Control (ARC)*.

14.10.1 Gruppenbezogene Funkfeldoptimierung

Ein WLC erlaubt eine Gruppierung von APs anhand von Standortinformationen, Geräteeigenschaften oder Netzgliederungen. Auf Basis dieser Gruppenzugehörigkeit lässt sich auch eine Funkfeldoptimierung durchführen. Statt also entweder für alle oder nur für einen AP eine Funkfeldoptimierung durchzuführen, können Sie z. B. alle AP innerhalb eines Gebäudetrakts mit einer speziellen Bezeichnung oder mit einer bestimmten Firmware-Version adressieren.

Die entsprechende Gruppe lässt sich sowohl über WEBconfig als auch die Konsole mit dem Gruppen-Parameter ansprechen:

```
do /Setup/WLAN-Management/start optimization <Gruppe>
```

Die APs sind über folgende Optionen des Gruppen-Parameters filterbar:

-g <Gruppenname>

APs, die der Gruppe angehören. Mehrere Gruppennamen sind durch Komma getrennt möglich.

-l <Standort>

APs, deren Standort entsprechend festgelegt ist.

Die Kombination von `-l` und einer der Standort-Optionen `-c` bis `-r` ist nicht sinnvoll.

-c <Land>

APs mit der entsprechenden Landesangabe.

-i <Stadt>

APs mit der entsprechenden Stadtangabe.

-s <Straße>

APs mit der entsprechenden Straßenangabe.

-b <Gebäude>

APs mit der entsprechenden Gebäudeangabe.

-f <Etage>

APs mit der entsprechenden Etagenangabe.

-r <Raum>

APs mit der entsprechenden Raumangabe.

-d <Gerätename>

APs mit den entsprechenden Gerätenamen.

-a <Antennen>

APs mit der entsprechenden Anzahl an Antennen.

Eine Kombination aus den Optionen `-d` und `-a` ist nicht sinnvoll.

-v <Firmware>

APs, die genau diese Firmwareversion besitzen.

-x <Firmware>

APs, deren Firmwareversion niedriger als die angegebene Version ist.

-y <Firmware>

APs, deren Firmwareversion niedriger oder gleich der angegebenen Version ist.

-z <Firmware>

APs, der Firmwareversion höher als die angegebene Version ist.

-t <Firmware>

APs, deren Firmwareversion höher oder gleich der angegebenen Version ist.

Kombinationen sind möglich, um z. B. APs mit einer Firmwareversion zwischen zwei Versionsständen zu adressieren.

-n <Intranet-Adresse>

APs, die sich im Intranet mit der angegebenen Adresse befinden.

-p <Profilname>

APs, die sich im angegebenen WLAN-Profil befinden.

14.11 Client Steering über den WLC

Das Client Steering ermöglicht den APs, die im Sendebereich befindlichen WLAN-Clients anhand bestimmter Kriterien zu veranlassen, sich immer mit dem für sie idealen AP zu verbinden. Die Kriterien sind zentral im WLC definiert. Die verwalteten APs melden ständig die aktuellen Werte an den WLC, der aufgrund der Kriterien entscheidet, welche APs die Anfragen von WLAN-Clients beantworten dürfen. Deshalb ist das Client Steering auch nur mit APs möglich, die ein WLC zentral verwaltet.

In gemanagten Netzen zentralisiert ein WLC das Client Steering aller angeschlossenen APs. Das Client Steering läuft in diesem Fall wie folgt ab:

1. Der WLC sammelt die Daten über die angemeldeten WLAN-Clients von den angeschlossenen APs. Aus diesen Daten erstellt der WLC die Bewertung für das Client Steering.
2. Alle APs sind so konfiguriert, dass das Client Steering über den WLC erfolgt.
3. Ein hinzukommender WLAN-Client sendet einen Probe-Request an die APs in seiner Reichweite.
4. Die APs übermitteln diese Anfrage zusammen mit der Signalstärke des WLAN-Clients via CAPWAP an den WLC.
5. Der WLC berechnet für jeden AP im Bereich des WLAN-Clients einen Wert, der sich aus drei Bestandteilen zusammensetzt:
   - Signalstärke-Wert
   - Wert aus der Anzahl der am AP angemeldeten Clients
   - Frequenzband-Wert

   Zusammen mit der jeweiligen Gewichtung, mit der der WLC jeden einzelnen Wert multipliziert, ergibt sich der endgültige Wert.
6. Der WLC sendet den APs mit dem höchsten oder einem maximal um ein Toleranz-Level davon abweichenden Wert die Nachricht, dass dieser den WLAN-Client beim nächsten Anmeldeversuch annehmen darf.
7. Versucht der WLAN-Client, sich noch vor der Antwort des WLC mit einem AP zu verbinden, weist ihn dieser zurück, solange die Antwort vom WLC aussteht.
8. Versucht ein WLAN-Client nicht, sich trotz einer bestehenden Verbindung mit niedriger Qualität an einem anderen AP mit höherer Verbindungsqualität zu verbinden ("Sticky Client"), kann der WLC den aktuellen AP dazu veranlassen, den WLAN-Client abzumelden. Der WLAN-Client ist daraufhin gezwungen, sich mit dem AP zu verbinden, der die bessere Verbindung anbietet.

Wenn ein AP die Verbindung zu dem WLC verliert, der für das Client Steering verantwortlich ist, lässt der AP alle Verbindungen von berechtigten WLAN-Clients zu.

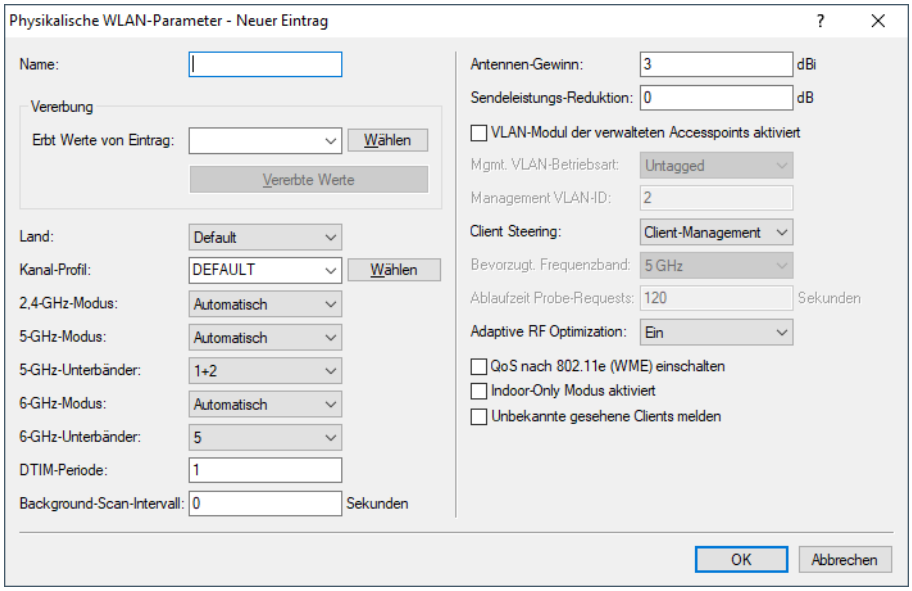
Für die optimale Funktionsweise des gemanagten Client-Steerings muss auf sämtlichen APs LCOS 9.00 oder höher installiert sein. Wenn Sie im Mischbetrieb APs mit einer älteren LCOS-Version einsetzen, kann in Ihrem WLAN keine sinnvolle Verteilung der Clients erfolgen.

In Szenarien mit zeitkritischem Roaming, z. B. bei VoIP-Telefonen, sollten Sie Client Steering nicht einsetzen, da Client Steering den Einbuchvorgang eines Clients verzögern kann.

14.11.1 Konfiguration

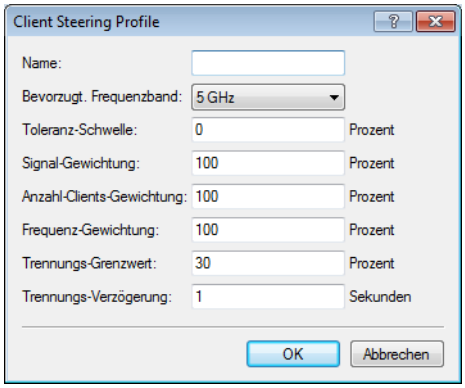
Mit LANconfig konfigurieren Sie das Client Steering wie folgt:

1. Aktivieren Sie zunächst im WLC das Client Steering für einen AP unter **WLAN-Controller** > **Profile** > **Physikalische WLAN-Parameter** über die Auswahlliste **Client Steering**.
   - **Aus**: Das Client Steering ist deaktiviert.
   - **AP-basiertes Band Steering**: Der AP leitet den WLAN-Client eigenständig auf ein bevorzugtes Frequenzband.
   - **Ein**: Der AP lässt das Client Steering vom WLC durchführen.



2. Im Menü **WLAN-Controller** > **AP-Konfiguration** > **Client Steering Profile** sind bereits zwei Standard-Profile vorkonfiguriert (High-Density, Default), die für die meisten Anwendungsfälle genügen. Optional erstellen Sie dort mit einem Klick auf **Hinzufügen** ein neues Client Steering-Profil.

   Client Steering-Profile legen die Bedingungen fest, nach denen der WLC entscheidet, welche APs beim nächsten Anmeldeversuch einen Client annehmen.



Die Einträge haben folgende Bedeutung:

Name

Bezeichnung des Client Steering-Profils.

Bevorzugt. Frequenzband

Gibt das Frequenzband vor, auf welches der WLC den WLAN-Client leitet.

- **2,4GHz**: Der WLC leitet den WLAN-Client auf das 2,4 GHz Frequenzband.
- **5GHz**: Der WLC leitet den WLAN-Client auf das 5 GHz Frequenzband.

Toleranz-Schwelle

Um diesen Prozentwert darf der errechnete Wert für einen AP vom maximal errechneten Wert abweichen, so dass der AP die Erlaubnis erhält, den Client beim nächsten Anmeldeversuch anzunehmen.

Signal-Gewichtung

Gibt an, mit wie viel Prozent der Signalstärke-Wert in den endgültigen Wert eingeht.

Anzahl-Clients-Gewichtung

Gibt an, mit wie viel Prozent der Wert für die Anzahl angemeldeter Clients bei einem AP in den endgültigen Wert eingeht.

Frequenzband-Gewichtung

Gibt an, mit wie viel Prozent der Wert für das Frequenzband in den endgültigen Wert eingeht.

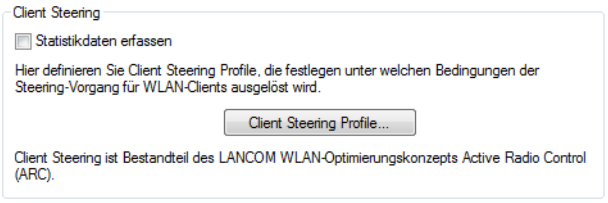
Trennungs-Grenzwert

Gibt den Prozentwert vom maximal gesehenen Signalstärkewert an, unter den der aktuelle Wert sinken muss, bevor der AP die Verbindung zum Client trennt.

Trennungs-Verzögerung

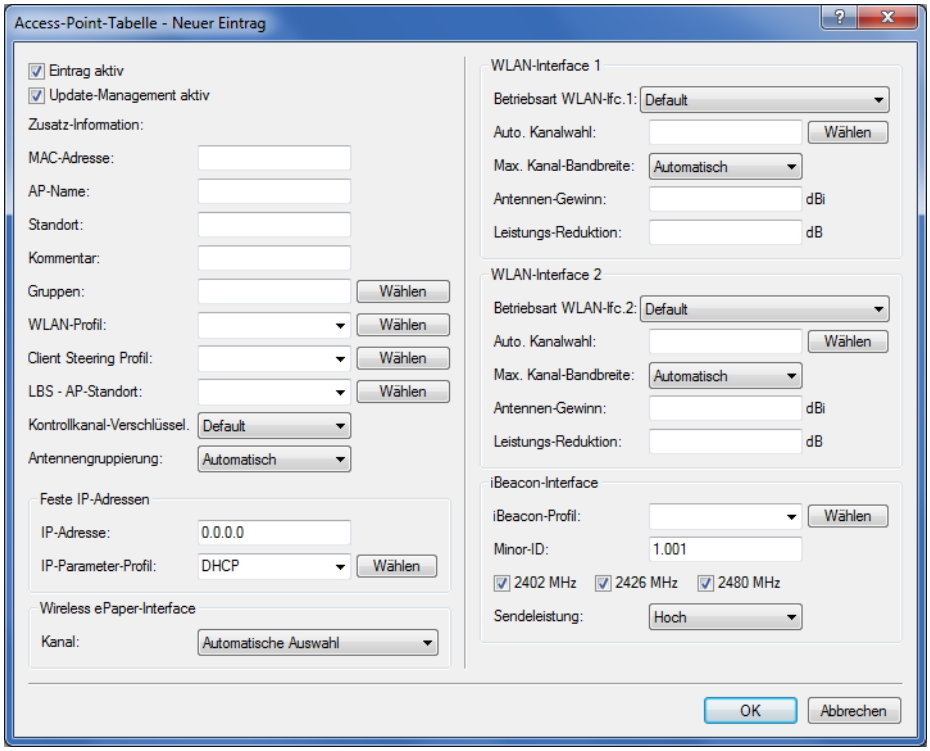
Gibt die Anzahl der Sekunden an, in denen keine Datenübertragung zwischen AP und Client stattfinden darf, bevor der AP den Client trennt.

3. Optional: Aktivieren Sie über den Parameter **Statistikdaten erfassen** die Aufzeichnung von Client Steering-Statistiken. Die Statistikdaten lassen sich anschließend z. B. mittels LANmonitor auswerten.

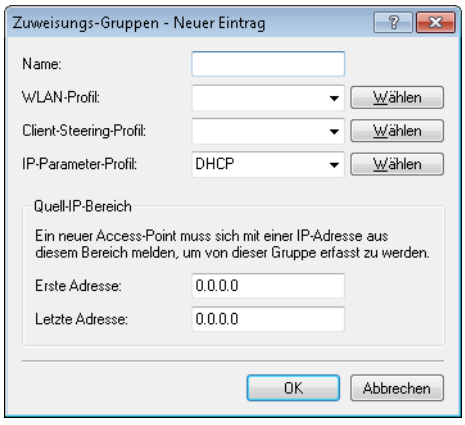


Die Statistikaufzeichnung erhöht die Last auf dem WLC. LANCOM empfiehlt daher, die Statistikaufzeichnung nicht dauerhaft zu aktivieren.

4. Weisen Sie jetzt unter **WLAN-Controller** > **AP-Konfiguration** > **Access-Point-Tabelle** dem entsprechenden AP eines der Client Steering-Profile zu.



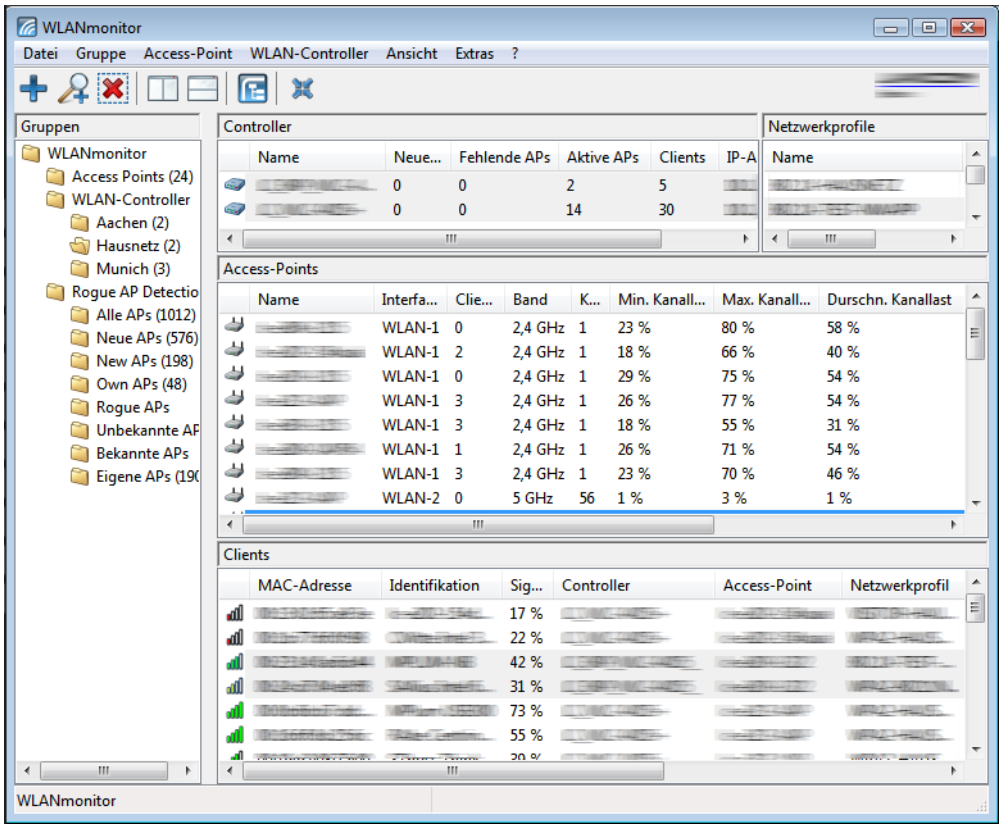
5. Optional: Ordnen Sie ggf. definierten Zuweisungs-Gruppen ein entsprechendes Client Steering-Profil zu.



Damit haben Sie die Konfiguration des Client-Steerings abgeschlossen.

14.12 Kanallastanzeige im WLC-Betrieb

Für die von einem WLC verwalteten APs wird die Last auf den verwendeten Kanälen in drei Werten als minimale, maximale und durchschnittliche Kanallast angezeigt. Die angezeigten Werte werden in einem Messintervall von drei Minuten ermittelt. Die ersten Werte werden demnach auch erst nach drei Minuten angezeigt.



14.13 Sicherung der Zertifikate

Ein WLC erzeugt beim ersten Systemstart die grundlegenden Zertifikate für die Zuweisung der Zertifikate an die APs – darunter die Root-Zertifikate für die CA (Certification Authority) und die RA (Registration Authority). Auf der Grundlage dieser beiden Zertifikate stellt der WLC die Geräte-Zertifikate für die APs aus.

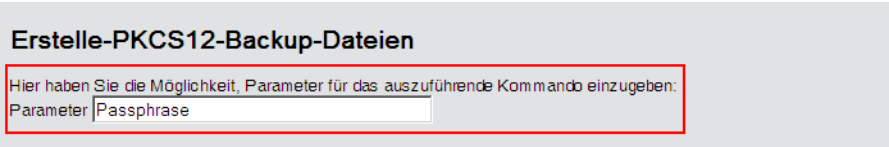
Wenn mehrere WLCs in der gleichen WLAN-Infrastruktur parallel eingesetzt werden (Load-Balancing) oder wenn ein Gerät ersetzt bzw. neu konfiguriert werden muss, sollten immer die gleichen Root-Zertifikate verwendet werden, um einen reibungslosen Betrieb der verwalteten APs zu gewährleisten.

14.13.1 Backup der Zertifikate anlegen

Für die Wiederherstellung der CA bzw. der RA werden die jeweiligen Root-Zertifikate mit den privaten Schlüsseln benötigt, die beim Systemstart automatisch vom WLC erzeugt werden. Außerdem sollten folgende noch weitere Dateien mit Informationen über die ausgestellten Geräte-Zertifikate gesichert werden. Damit diese vertraulichen Daten auch beim Export aus dem Gerät heraus geschützt bleiben, werden sie zunächst in einen PCKS12-Container gespeichert, der mit einer Passphrase geschützt ist.

WEBconfig

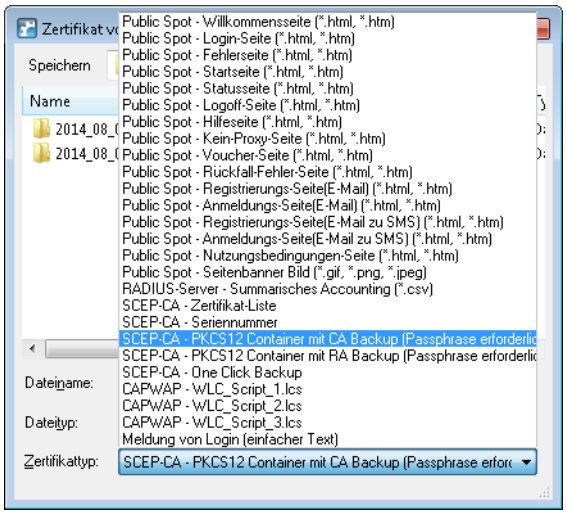
1. Öffnen Sie die Konfiguration des WLCs mit WEBconfig im Bereich **Extras** > **LCOS-Menübaum** > **Setup** > **Zertifikate** > **SCEP-CA** > **CA-Zertifikate**.
2. Wählen Sie den Befehl **Erstelle-PKCS12-Backup-Dateien** und geben Sie als Parameter die Passphrase für die PKCS12-Container an.



Mit dieser Aktion werden die Zertifikate und privaten Schlüssel in die PKCS12-Dateien gespeichert und können dann aus dem Gerät heruntergeladen werden.

LANconfig

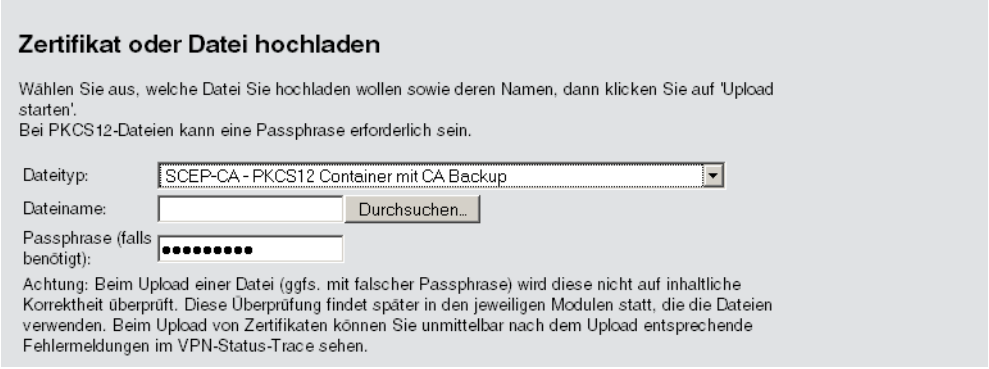
1. Markieren Sie den entsprechenden WLC in der Geräteübersicht und wählen Sie im Menü **Gerät** > **Konfigurations-Verwaltung** den Punkt **Zertifikat als Datei sichern.**.
2. Wählen Sie in der Liste **Zertifikattyp** den gewünschten PKCS12-Container aus und klicken Sie auf **Speichern**.



14.13.2 Zertifikats-Backup in das Gerät einspielen

1. Wählen Sie **Extras** > **Dateimanagement** > **Zertifikat oder Datei hochladen**.
2. Wählen Sie dann als Dateityp nacheinander die beiden Einträge für die SCEP-CA:
   - PKCS12-Container mit CA-Backup
   - PKCS12-Container mit RA-Backup

3. Geben Sie dazu jeweils den Dateinamen mit Speicherort an und die Passphrase, die beim Erstellen der Sicherungsdateien definiert wurde. Bestätigen Sie mit **Upload starten**:



4. Nach dem Einspielen der CA Sicherung muss die Datei `controller_rootcert` im Verzeichnis **Status** > **File-System** > **Contents** gelöscht werden.
   Geben Sie dazu an der Konsole die folgenden Befehle ein:

```
cd /Status/File-System/Contents
del controller_rootcert
```

5. Löschen Sie nach dem Zurückspielen des Backups alle Dateien, die mit `controller_` oder `eaptls_` beginnen.

6. Danach muss im Verzeichnis **Setup** > **Certificates** > **SCEP-Client** der Befehl `Reinit` aufgerufen werden:

```
cd /Setup/Certificates/SCEP-Client
do Reinit
```

14.13.3 Sichern und Wiederherstellen weiterer Dateien der SCEP-CA

Um die SCEP-CA vollständig wiederherstellen zu können, sind auch die Informationen über die von der SCEP-CA ausgestellten Geräte-Zertifikate für die einzelnen APs wichtig.

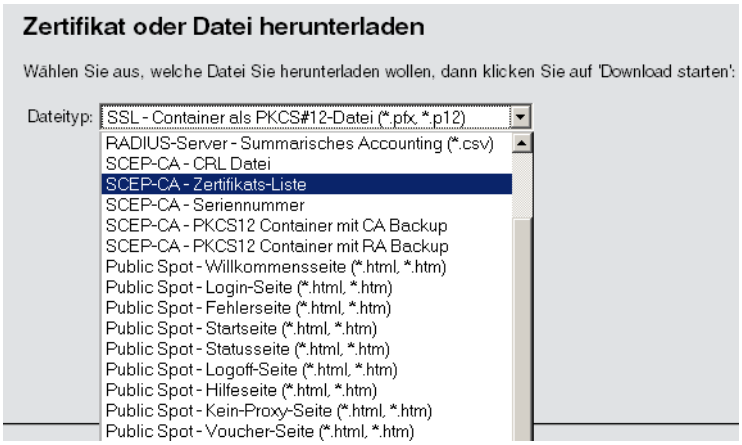
Wenn nur die Root-Zertifikate gesichert werden, können die ausgestellten Geräte-Zertifikate nicht mehr zurückgerufen werden!

Daher müssen Sie neben den Zertifikaten selbst noch folgende Dateien sichern:

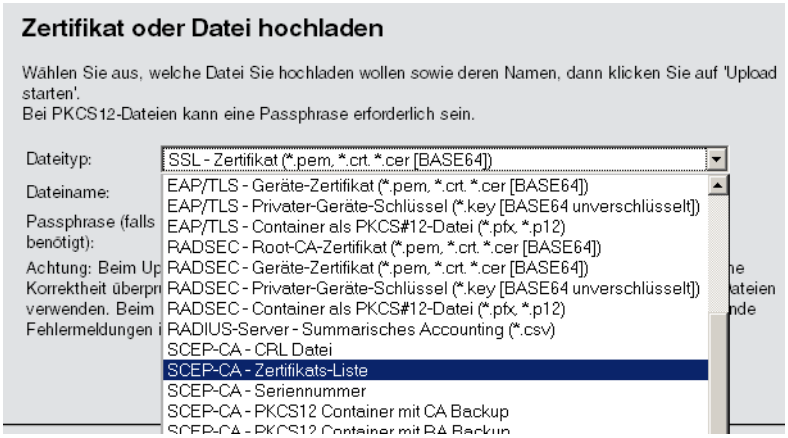
- SCEP-Zertifikatsliste: Liste aller von der SCEP-CA jemals ausgestellten Zertifikate.
- SCEP-Seriennummern: Enthält die Seriennummer für das nächste Zertifikat.

1. Wählen Sie **Extras** > **Dateimanagement** > **Zertifikat oder Datei herunterladen**.

2. Wählen Sie dann als Dateityp nacheinander die oben aufgeführten Einträge und bestätigen Sie mit **Download starten**.



3. Zum Einspielen dieser Dateien in das Gerät wählen Sie auf der Startseite von WEBconfig den Befehl **Zertifikat oder Datei hochladen**.
4. Wählen Sie dann als Dateityp nacheinander die oben aufgeführten Einträge, geben Sie dazu jeweils den Dateinamen mit Speicherort an und bestätigen Sie mit **Upload starten**.



Nach dem Einspielen einer neuen Zertifikatsliste werden abgelaufene Zertifikate entfernt und eine neue CRL erstellt. Weiterhin reinitialisiert sich die CA automatisch, wenn nach dem Einspielen der Zertifikatsbackups erfolgreich Zertifikate und Schlüssel extrahiert wurden.

14.13.4 One Click Backup der SCEP-CA

Um das Backup der im WLC vorliegenden CA zu vereinfachen, bietet Ihnen das Gerät die Möglichkeit, mit einer einzigen Aktion einen kompletten Zertifikats-Datensatz zu erzeugen (One Click Backup). Dieser Datensatz erlaubt Ihnen die vollständige Sicherung und Wiederherstellung der CA und vermeidet das Auftreten von Zertifikats-Konflikten.

Derartige Konflikte können dann auftreten, wenn Sie die einzelnen PKCS12-Container separat vom Gerät heruntergeladen haben und anschließend wieder einspielen: Hat der WLC in der Zwischenzeit eine neue CA aufgesetzt und neue Zertifikate ausgestellt, führen die abweichenden CAs temporär zu Authentisierungsproblemen bei den verschiedenen Diensten im LCOS. Sofern nicht gewartet werden kann, bis die einzelnen Dienste neue Zertifikate anfordern, erfordert die manuelle Konfliktlösung ein Löschen der SCEP-Dateien aus dem LCOS-Dateisystem und eine Reinitialisierung des SCEP-Clienten. Mit dem Zurückspielen eines One Click Backups dagegen führt das LCOS die notwendigen Schritte automatisch aus.

Erstellen einer Backup-Datei

Um einen Zertifikats-Datensatz zu erzeugen, führen Sie die Aktion **Erstelle-PKCS12-Backup-Dateien** unter **Setup** > **Zertifikate** > **SCEP-CA** > **CA-Zertifikate** aus. Diese Aktion erzeugt eine Zip-Datei innerhalb des LCOS-Dateisystems, die alle notwendigen Dateien enthält. Zum Schutz der enthaltenen Zertifikate und Schlüssel ist die Zip-Datei automatisch mit dem Gerätepasswort geschützt, sofern Sie kein gesondertes Passwort angeben. Die erzeugte Zip-Datei lässt sich anschließend z. B. im WEBconfig über **Extras** > **Dateimanagement** > **Zertifikat oder Datei herunterladen** > **SCEP-CA – One Click Backup** herunterladen.

Zurückspielen der Backup-Datei

Um einen Zertifikats-Datensatz zurückzuspielen, laden Sie die gesicherte Zip-Datei unter Angabe der Passphrase direkt in das Gerät. Im WEBconfig z. B. erfolgt dies über die Auswahl **Extras** > **Dateimanagement** > **Zertifikat oder Datei hochladen** > **SCEP-CA – One Click Backup**. Setzen Sie dabei die Option **Vorhandene CA Zertifikate ersetzen**, damit das Gerät den Zertifikats-Datensatz nach dem Hochladen automatisch zurückspielt.

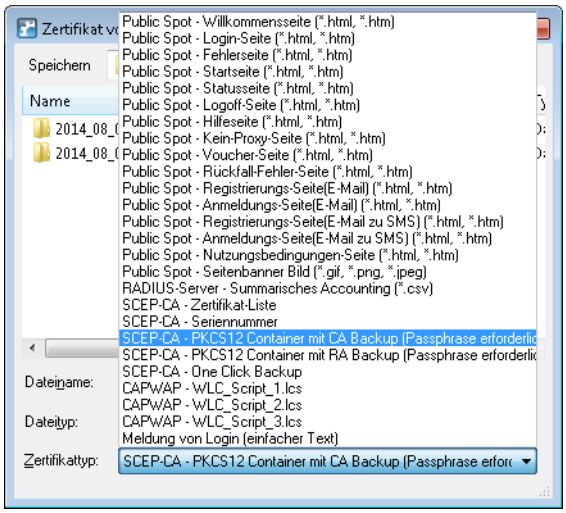
Sofern Sie die Option nicht setzen oder die Backup-Datei auf andere Weise ins Gerät laden, müssen Sie nach dem Hochladen die Aktion *2.39.2.2.11 Zertifikate-aus-Backup-wiederherstellen* ausführen, damit das Gerät den Zertifikats-Datensatz zurückspielt.

14.13.5 Backup und Einspielen der Zertifikate über LANconfig

Um die Zertifikate über LANconfig zu speichern und hochzuladen, gehen Sie wie folgt vor:

Speichern

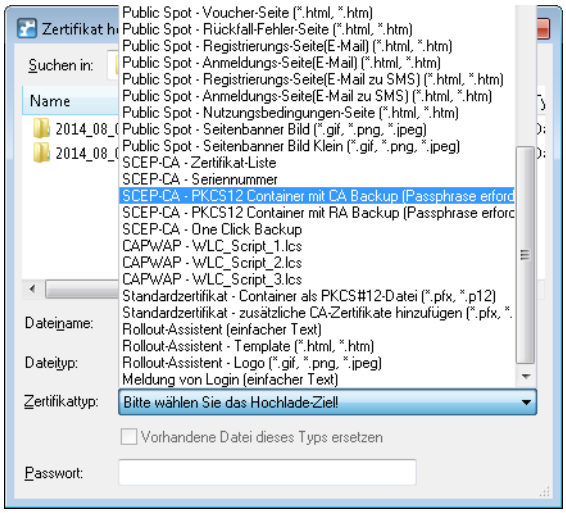
1. Markieren Sie den entsprechenden WLC in der Geräteübersicht und wählen Sie im Menü **Gerät** > **Konfigurations-Verwaltung** den Punkt **Zertifikat als Datei sichern**.
2. Wählen Sie in der Liste **Zertifikattyp** den gewünschten PKCS12-Container-Typ aus und klicken Sie auf **Speichern**.



Hochladen

1. Markieren Sie den entsprechenden WLC in der Geräteübersicht und wählen Sie im Menü **Gerät** > **Konfigurations-Verwaltung** den Punkt **Zertifikat oder Datei hochladen**.
2. Wählen Sie in der Liste **Zertifikattyp** den gewünschten PKCS12-Container-Typ aus.

3. Navigieren Sie anschließend zur gewünschten Datei, geben Sie ggf. ein Passwort an und klicken Sie auf **Öffnen**.



One Click Backup

Für das One Click Backup wählen Sie aus der Dialogliste jeweils den Eintrag "SCEP-CA – One Click Backup" aus.

14.14 Backuplösungen

WLCs verwalten eine große Zahl von APs, bei denen wiederum zahlreiche WLAN-Clients eingebucht sein können. Die WLC haben daher eine zentrale Bedeutung für die Funktionsfähigkeit der gesamten WLAN-Struktur – die Einrichtung einer Backup-Lösung für den vorübergehenden Ausfall eines WLCs ist daher in vielen Fällen unverzichtbar.

In einem Backup-Fall soll sich ein gemanagter AP mit einem anderen WLC verbinden. Da diese Verbindung nur gelingen kann, wenn das Zertifikat des APs von dem Backup-Controller authentifiziert wird, müssen alle WLCs in einer Backup-Lösung auf jeden Fall identische Root-Zertifikate verwenden.

14.14.1 WLC-Cluster

Sofern Sie in Ihrem Netz mehrere WLCs einsetzen, haben Sie die Möglichkeit, diese Geräte zu einem geschlossenen Verbund (Cluster) zusammenfassen. Die APs eines gemanagten WLANs werden dann nicht mehr von einem einzigen, zentralen WLC verwaltetet, sondern von mehreren miteinander synchronisierten WLCs. Ein solcher WLC-Cluster bietet Ihnen vor allem in größeren Netzen diverse Vorteile:

- Automatische Verteilung der Netzlast zwischen den einzelnen APs und WLCs („Load-Balancing“).
- Erhöhte Ausfallsicherheit durch die Bereitstellung von Backup-WLCs („Hot Standby“) und automatische Neuverteilung der APs im Falle eines WLC-Ausfalls.
- Aufbau einer Zertifikatshierarchie: Verwaltung der Zertifikate durch eine zentrale Zertifizierungsstelle (CA), dargestellt wahlweise durch einen Master-WLC oder eine externe Stelle (z. B. einen Server).

Ab LCOS 9.00 hat die Cluster-Funktion die im Folgenden näher beschriebenen Verbesserungen erhalten.

14.14.1.1 CAPWAP im WLC gezielt (de)aktivieren

Um mehrere WLCs in einem Verbund (Cluster) zu betreiben, müssen alle beteiligten Geräte eine identische Konfiguration aufweisen. Dies ist auf einem WLC standardmäßig jedoch nicht der Fall, da dieser bestimmte Konfigurationsbestandteile

(wie Zertifikate) automatisch generiert. Durch Deaktivieren von CAPWAP auf allen Geräten bis auf einem haben Sie die Möglichkeit, in Ihrem WLC-Cluster einen Master-Controller zu definieren, dessen Konfiguration sich anschließend auf die übrigen WLCs spiegeln lässt.

Mehr zum Spiegeln einer Konfiguration erfahren Sie im Abschnitt *Config-Sync*.

14.14.1.2 WLC-Tunnel für die interne Kommunikation

Der Einsatz von WLC-Tunneln ist ein essentieller Bestandteil eines WLC-Clusters. Die am WLC-Cluster beteiligten WLCs nutzen diese Tunnel zur Kommunikation untereinander, um die verteilten Statusinformationen im Verbund abzugleichen. Im Rahmen der Funktionserweiterungen ab LCOS 9.00 verbessert sich daher auch der LCOS-interne Umgang mit WLC-Tunneln:

- WLCs sind dazu in der Lage, sich untereinander automatisch zu finden.
- Sie haben die Möglichkeit, WLC-Tunnel statisch zu konfigurieren.
- WLCs trennen einen WLC-Tunnel erst nach Ablauf eines Timeouts.
- WLC-Tunnel lassen sich global ein- oder ausschalten.

Die Einstellungen für die WLC-Tunnel und die weiteren WLCs (Remote-WLCs) nehmen Sie in LANconfig im Abschnitt **WLAN-Controller** > **Allgemein** > **WLC-Cluster** vor. Über die Einstellung **WLC-Tunnel aktiv** deaktivieren Sie den Einsatz von WLC-Tunneln, was de facto ein Abschalten der Clustering-Funktion bewirkt.

14.14.1.3 Ermittlung des idealen WLC

Die im LCOS implementierten Algorithmen ermöglichen die intelligente Verteilung von APs auf einzelne WLCs. Dies erlaubt den APs, innerhalb von WLC-Clustern die Netzlast gleichmäßig auf alle WLCs aufzuteilen oder nach Ausfall eines WLCs ein alternatives Gerät zu wählen. Hierzu sendet ein AP zunächst einen Discovery Request ins Netz, um sämtliche verfügbaren WLCs zu ermitteln. Die WLCs antworten ihrerseits mit einem Discovery Response, anhand dessen ein AP eine Liste von WLCs erstellt. Diese Liste priorisiert ein der AP anhand verschiedener Kritieren.

Ein AP arbeitet dabei die einzelnen Kriterien sequentiell ab: Sofern nach der Anwendung eines Kriteriums mehrere WLCs für den idealen WLC in Frage kommen, zieht der AP das nächste Kriterium zur Priorisierung heran. Dieser Prozess endet, wenn im Rahmen der nachfolgend beschriebenen Priorisierung schließlich ein WLC als idealer WLC verbleibt.

Kriterien zur Priorisierung

- **Spezifität der AP-Konfiguration**: Ein AP wertet aus, ob ein WLC für den AP eine Konfiguration bereithält und ob diese ein spezifisches AP-Profil oder ein Default-Profil umfasst. Ein spezifisches AP-Profil priorisiert der AP am höchsten, gefolgt von einem Default-Profil. Ein fehlendes Profil erhält die niedrigste Priorität.
- **Höhe des Präferenzwerts**: Der AP wertet aus, welchen Präferenzwert Sie einem WLC zugewiesen haben. Je höher die betreffende Zahl zwischen 0 und 255 liegt, desto höher priorisiert der AP den WLC.

Sofern immer noch mehrere WLCs für die Rolle des idealen WLCs in Frage kommen, hängt der weitere Priorisierungsprozess vom Verbindungsstatus und der Art des Auswahlprozesses (automatisch vs. manuell initiiert) ab:

- Bei der **erstmaligen Ermittlung** bildet ein AP für jeden verbliebenen WLC einen gewichteten Wert aus der Zahl der verbundenen sowie der maximal möglichen APs (**Lizenzauslastung**). Als idealen WLC wählt ein AP schließlich den WLC mit der geringsten Lizenzauslastung.

  Hat ein WLC die maximal mögliche Anzahl von AP-Verbindungen erreicht (Lizenzkontingent erschöpft), berücksichtigt ein AP den betreffenden WLC nicht mehr für den aktuellen Auswahlprozess.
- Bei der **automatischen Überprüfung** der idealen AP-Verteilung verbleibt ein AP bei dem mit ihm verbundenen WLC, sofern sich dieser WLC in der Liste der verbliebenen WLCs befindet. Andernfalls sorgt ein **zufallsgesteuerter Algorithmus** dafür, dass der AP einen beliebigen AP auswählt.
- Bei der **manuell ausgelösten Überprüfung** der idealen AP-Verteilung sorgt ein **zufallsgesteuerter Algorithmus** dafür, dass die einzelnen APs die im Netz verfügbaren Lizenzkontingente möglichst gleichmäßig ausnutzen.

14.14.1.4 Ermittlung der idealen AP-Verteilung

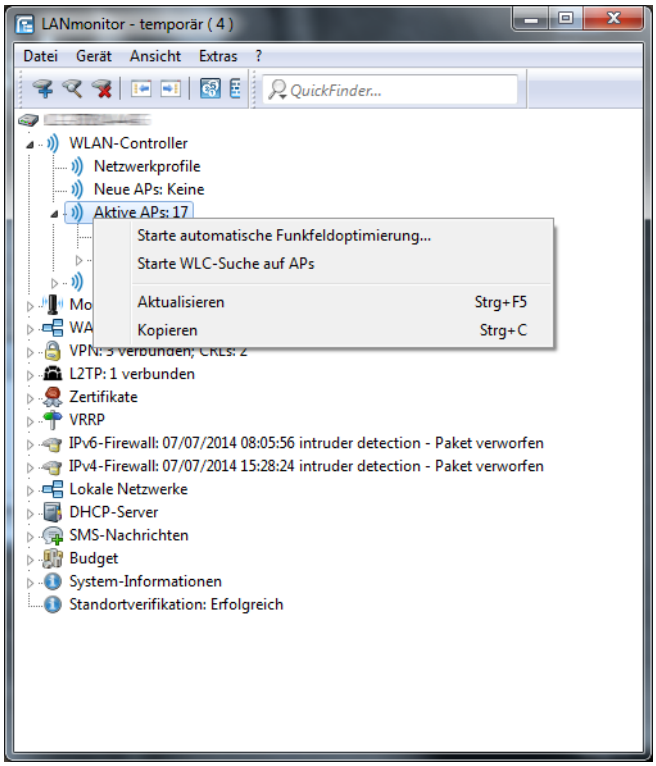
Die Ermittlung der idealen AP-Verteilung in einem WLC-Cluster und eine dadurch ggf. ausgelöste Umverteilung erfolgt grundsätzlich automatisch. Dazu durchläuft ein jeder AP in unregelmäßigen Abständen von 30 bis 60 Minuten den Prozess zur *Ermittlung des idealen WLC*. Gewinnt bei diesem Vorgang der WLC, zu dem bereits eine Verbindung besteht, erfolgt keine Umverteilung. Weist jedoch ein anderer WLC eine höhere Priorisierung auf, so versucht der AP, sich mit diesem WLC zu verbinden.

Sie haben aber auch als Administrator die Möglichkeit, via LANmonitor die Ermittlung der idealen AP-Verteilung und eine ggf. daraus resultierende Umverteilung der APs manuell auszulösen (siehe *Ideale AP-Verteilung manuell initiieren* auf Seite 1241).

14.14.1.5 Ideale AP-Verteilung manuell initiieren

Die nachfolgenden Schritte zeigen Ihnen, wie Sie die Berechnung der idealen Verteilung manuell starten und dadurch ggf. eine Neuverteilung auslösen.

1. Starten Sie LANmonitor und wählen Sie einen WLC aus.
2. Wechseln Sie in den Menüzweig **Wireless LAN** > **Aktive APs**.
3. Öffnen Sie das Kontextmenü auf einem beliebigen AP und wählen Sie **Starte WLC-Suche auf APs**.



Die betreffenden Access Points bestimmen den für sie optimalen WLC und verteilen sich entsprechend der Vorgaben über den WLC-Verbund.

14.14.1.6 Einrichten einer CA-Hierarchie

Um mehrere WLC im Verbund zu betreiben (WLC-Cluster), müssen alle beteiligten Geräte eine identische Konfiguration aufweisen. Dies umfasst auch die innerhalb des WLC-Clusters eingesetzten Zertifikate. Die Lösung liegt in dem Aufbau einer Zertifikats- bzw. CA-Hierarchie: Hierbei definieren Sie die CA eines WLC als Root-CA, von welcher die übrigen WLCs das Zertifikat für ihre (Sub-)CA beziehen.

Das nachfolgende Szenario zeigt Ihnen, welche Konfigurationsschritte für den Aufbau einer CA-Hierarchie notwendig sind. Die Konfiguration erfolgt exemplarisch anhand zweier WLCs:

- WLC-MAIN stellt das Gerät mit der Root-CA dar;
- WLC-SUB stellt das Gerät dar, welches bei der Root-CA ein Zertifikat bezieht, um als Sub-CA weitere Zertifikate ausstellen zu können.

Konfiguration der Root-CA

Der nachfolgende Abschnitt beschreibt die Einrichtung einer Root-CA auf einem WLC. Die einzelnen Handlungsschritte gehen von einem zurückgesetzten Gerät aus, bei dem Sie die Standard-Inbetriebnahme durchgeführt und die korrekte Uhrzeit gesetzt haben.

1. Melden Sie sich via WEBconfig oder über die Konsole am Gerät an.
2. Wechseln Sie in das Menü **Setup** > **Zertifikate** > **SCEP-CA** > **CA-Zertifikate**. Passen Sie hier die Namen für die Certificate Authority (CA) und die Registration Authority (RA) über die Parameter **CA-Distinguished-Name** und **RA-Distinguished-Name** an.

   Beispiel: `/CN=WLC-MAIN CA/O=LANCOM SYSTEMS/C=DE`

3. Wechsel Sie in das Menü **Setup** > **Zertifikate** > **SCEP-CA** und setzten Sie den Parameter **Aktiv** auf **Ja**.

Damit haben Sie die Konfiguration der Root-CA abgeschlossen. Mit dem Befehl `show ca cert` an der Kommendozeile lässt sich überprüfen, ob der WLC das Zertifikat korrekt erstellt hat.

Konfiguration der Sub-CA

Der nachfolgende Abschnitt beschreibt die Einrichtung einer Sub-CA auf einem WLC. Die einzelnen Handlungsschritte gehen von einem zurückgesetzten Gerät aus, bei dem Sie die Standard-Inbetriebnahme durchgeführt und die korrekte Uhrzeit gesetzt haben.

1. Melden Sie sich via WEBconfig oder über die Konsole am Gerät an.
2. Wechseln Sie in das Menü **Setup** > **Zertifikate** > **SCEP-CA** und setzten Sie den Parameter **Root-CA** auf **Nein**.
3. Wechseln Sie in das Menü **Setup** > **Zertifikate** > **SCEP-CA** > **CA-Zertifikate**. Passen Sie hier die Namen für die Certificate Authority (CA) und die Registration Authority (RA) über die Parameter **CA-Distinguished-Name** und **RA-Distinguished-Name** an.

   Beispiel: `/CN=WLC-SUB CA/O=LANCOM SYSTEMS/C=DE`

4. Wechseln Sie in das Menü **Setup** > **Zertifikate** > **SCEP-CA** > **Sub-CA** und tragen Sie für den Parameter **CADN** den Distinguished Name der Root-CA ein.

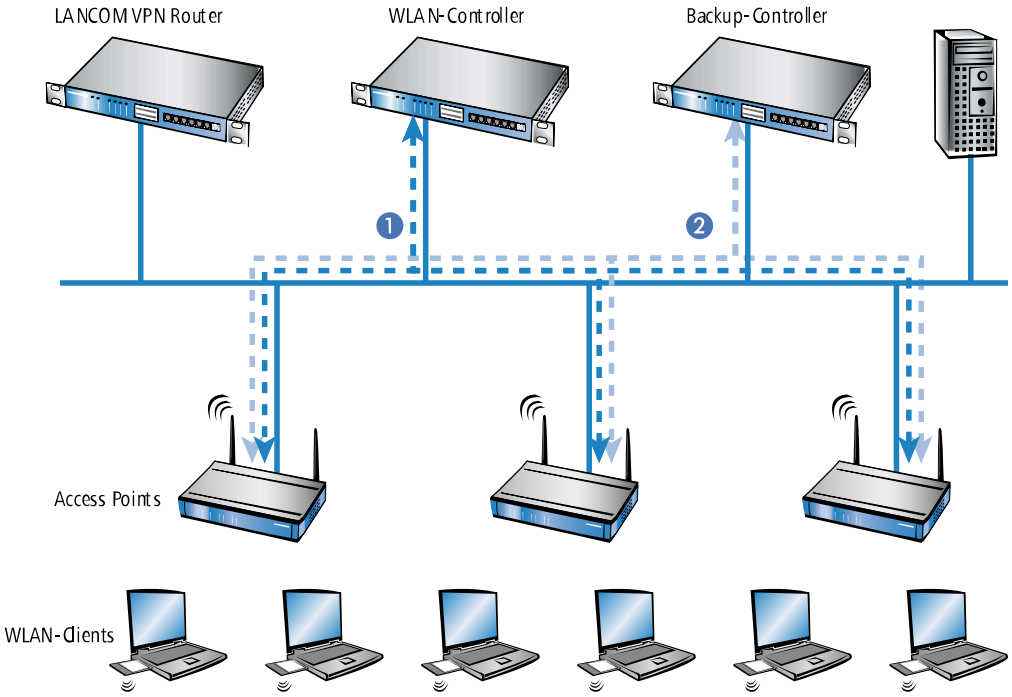
   Beispiel: `/CN=WLC-MAIN CA/O=LANCOM SYSTEMS/C=DE`

5. Tragen Sie für den Parameter **Challenge-Pwd** das Challenge-Passwort ein, das auf WLC-MAIN unter **Setup** > **Zertifikate** > **SCEP-CA** hinterlegt ist.
6. Hinterlegen im Parameter **CA-Url-Adresse** die URL (Adresse) zur Root-CA.
   Stellt ein anderer WLC mit LCOS-Betriebssystem die Root-CA zur Verfügung, müssen Sie lediglich die IP-Adresse im Default-Wert durch jene Adresse austauschen, unter der das entsprechende Gerät zu erreichen ist. Beispiel: `http://192.168.1.1/cgi-bin/pkiclient.exe`.
7. Optional: Spezifizieren Sie die **Ext-Key-Usage** und **Cert-Key-Usage**, um die Funktionen der Sub-CA einzuschränken. Weitere Informationen hierzu finden Sie in der Menüreferenz.
8. Setzten Sie den Parameter **Auto-generiert-Request** auf **ja**, um die Sub-CA zu aktivieren..
9. Wechseln Sie in das Menü **Setup** > **Zertifikate** > **SCEP-CA** und setzten Sie den Parameter **Aktiv** auf **ja**, um den CA-Server mit SCEP zu aktivieren.

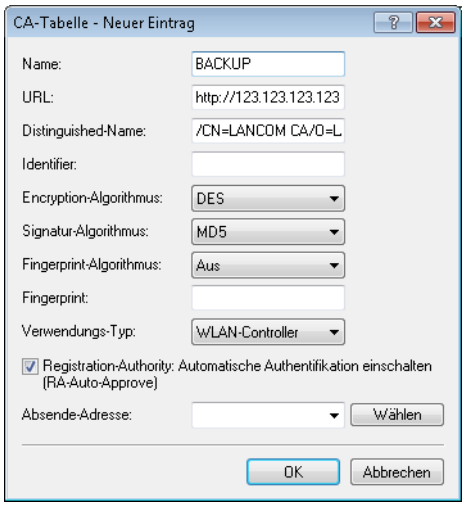
Damit haben Sie die Konfiguration der Sub-CA abgeschlossen. Mit dem Befehl `show ca cert` an der Kommendozeile lässt sich überprüfen, ob der WLC das Zertifikat korrekt erstellt hat. Die Hierarchie der Zertifikate muss hierbei sichtbar sein: Als erstes zeigt der WLC das Zertifikat der Root-CA an, dann das Zertifikat der Sub-CA.

14.14.2 Backup mit redundanten WLAN-Controllern

Diese Form des Backups bietet sich an, wenn Sie einen WLC durch einen zweiten WLC absichern und dabei jederzeit die volle Kontrolle über alle gemanagten APs behalten möchten. Der Backup-WLC wird dabei so konfiguriert, dass er die benötigten Zertifikate über SCEP vom abgesicherten Haupt-WLC bezieht.



1. Stellen Sie auf beiden WLCs **1** und **2** die gleiche Uhrzeit ein.
2. Schalten Sie die CA auf dem Backup-WLC aus (WEBconfig: LCOS-Menübaum > Setup > Zertifikate > SCEP-CA > Aktiv).
3. Erstellen Sie in der Konfiguration des SCEP-Clients im Backup-WLC einen neuen Eintrag in der CA-Tabelle (in LANconfig unter **Zertifikate** > **SCEP-Client** > **CA-Tabelle**). Darin wird die CA des Haupt-WLC eingetragen.

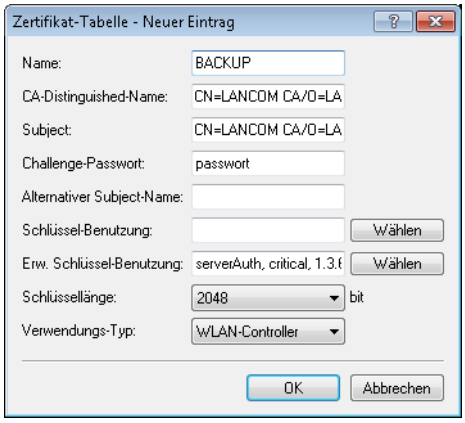


4. Geben Sie als URL die IP-Adresse oder den DNS-Namen des Haupt-WLCs ein gefolgt vom Pfad zur CA `/cgi-bin/pkiclient.exe`, also z. B. `10.1.1.99/cgi-bin/pkiclient.exe`.

   › **Distinguished-Name**: Standardname der CA (/CN=LANCOM CA/O=LANCOM SYSTEMS/C=DE) bzw. der Name der auf dem primären Controller vergeben wurde

- **RA-Auto-Approve** einschalten
- **Verwendungs-Typ**: WLAN-Controller

5. Erstellen Sie dann einen neuen Eintrag in der Zertifikats-Tabelle mit folgenden Angaben:



- **CA-Distinguished-Name**: Der Standardname, der bei der CA eingetragen wurde, also z. B. /CN=LANCOM CA/O=LANCOM SYSTEMS/C=DE
- **Subject**: Angabe der MAC-Adresse des Haupt-WLAN-Controllers in der Form: /CN=00:a0:57:01:23:45/O=LANCOM SYSTEMS/C=DE
- **Challenge**: Das allgemeine Challenge-Passwort der CA auf dem primären WLAN-Controller oder ein extra für den Controller manuell vergebenes Passwort.
- **Erweiterte Schlüsselbenutzung**: critical,serverAuth,1.3.6.1.5.5.7.3.18
- **Schlüssellänge**: 2048 Bit
- **Verwendungs-Typ**: WLAN-Controller

6. Wenn im Backup-Controller zuvor schon eine SCEP-Konfiguration aktiv war, müssen folgende Aktionen unter WEBconfig ausgeführt werden (**Experten-Konfguration** > **Setup** > **Zertifikate** > **SCEP-Client**):

- Bereinige-SCEP-Dateisystem
- Aktualisieren (2x: beim ersten Mal holt sich der SCEP-Client nur die neuen CA/RA Zertifikate, beim zweiten Mal wird das Gerätezertifikat aktualisiert)

7. Konfigurieren Sie den ersten WLC **1** wie gewünscht mit allen Profilen und der zugehörigen AP-Tabelle. Die APs bauen dann die Verbindung zum ersten WLC auf. Die APs erhalten von diesem WLC ein gültiges Zertifikat und eine Konfiguration für die WLAN-Module.
8. Übertragen Sie die Konfiguration des ersten WLCs **1** z. B. mit LANconfig auf den Backup-Controller **2**. Dabei werden auch die Profile und die AP-Tabellen mit den MAC-Adressen der APs auf den Backup-WLC übertragen. Alle APs bleiben in diesem Zustand weiterhin beim ersten WLC angemeldet. Ist die Übertragung der Konfiguration erfolgt, ist es erforderlich, dass Sie dem Backup-Controller eine neue IP-Adresse zuweisen.

Fällt der erste WLC **1** aus, suchen die APs automatisch nach einem anderen WLC und finden dabei den Backup-WLC **2**. Da dieser über die gleichen Root-Zertifikate verfügt, kann er die Zertifikate der APs auf Gültigkeit überprüfen. Da die APs außerdem mit ihrer MAC-Adresse in der AP-Tabelle des Backup-WLCs eingetragen sind, übernimmt der Backup-WLC vollständig die Verwaltung der APs. Änderungen in den WLAN-Profilen des Backup-WLCs wirken sich direkt auf die gemanagten APs aus.

Die APs bleiben in diesem Szenario so lange in der Verwaltung des Backup-WLCs, bis dieser entweder selbst einmal nicht erreichbar ist oder bis sie manuell getrennt werden.

Mit der Einstellung des autarken Weiterbetriebs können die APs auch während der Suche nach einem Backup-WLC mit der aktuellen WLAN-Konfiguration in Betrieb bleiben, und die WLAN-Clients bleiben eingebucht.

14.14.3 Backup mit primären und sekundären WLAN-Controllern

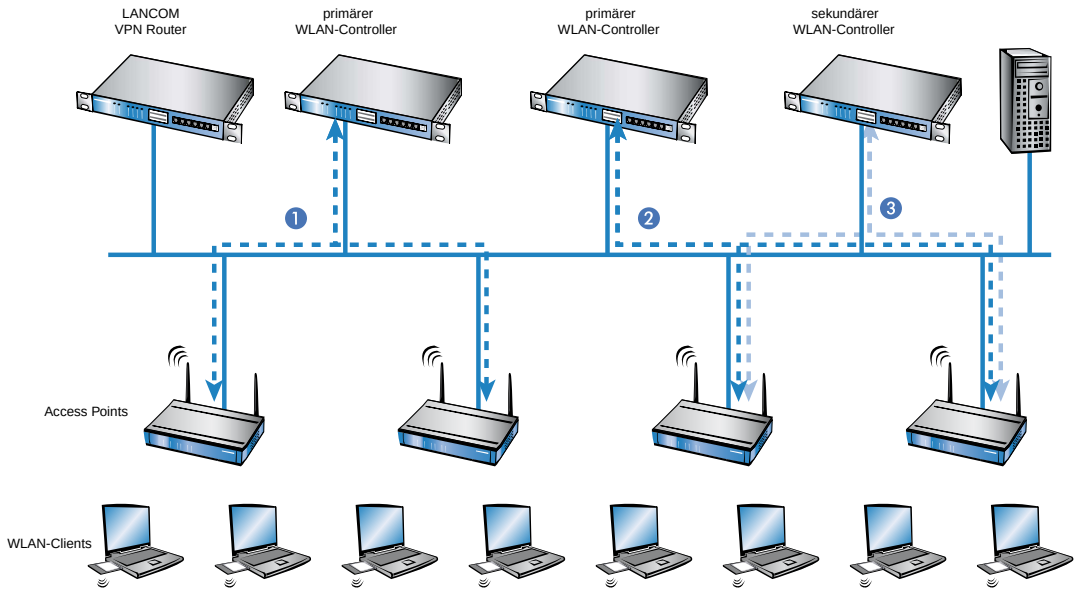
Mit einer zweiten Form des Backups können Sie für eine größere Anzahl von "primären" WLCs einen gemeinsamen, "sekundären" Backup-WLC bereitstellen. Beim Ausfall eines WLCs bleiben die APs zwar in Betrieb, arbeiten allerdings mit der aktuellen Konfiguration der WLAN-Module weiter. Der Backup-WLC kann als sekundärer WLC den APs keine veränderte Konfiguration zuweisen.

14.14.4 Primäre und sekundäre Controller

Der Verbindungsaufbau zwischen WLC und AP wird immer vom AP initiiert. Ein AP im Managed-Modus sucht in einem LAN nach einem WLC, der ihm eine Konfiguration zuweisen kann. Bei dieser Suche kann der AP unterschiedliche geeignete WLCs finden:

- Der WLC kann das **Zertifikat** des APs authentifizieren und hat für die MAC-Adresse des suchenden APs eine **Konfiguration** gespeichert. Einen solchen WLC bezeichnet man als "primären" WLC.
- Ein WLC kann das **Zertifikat** des APs authentifizieren, hat aber für die MAC-Adresse des suchenden APs **keine Konfiguration** gespeichert und auch **keine Default-Konfiguration**. Einen solchen WLC bezeichnet man als "sekundären" WLC.

Beispiel einer Backup-Lösung mit drei WLCs für 50 gemanagte APs: Zwei der WLCs verwalten jeweils 25 APs, der dritte steht als Backup-WLC bereit:



Ein WLC kann nun in seiner AP-Tabelle die fünffache Anzahl der von ihm selbst maximal verwalteten APs aufnehmen. Für jeweils fünf WLCs (mit gleicher Ausstattung) reicht also ein zusätzlicher WLC aus, um eine vollständige Absicherung bei Ausfall eines Gerätes zu realisieren.

1. Stellen Sie auf allen WLCs **1** und **2** und **3** die gleiche Uhrzeit ein.
2. Übertragen Sie die CA- und RA-Zertifikate aus dem ersten primären WLC **1** in den zweiten, primären **2** und den sekundären "Backup-WLC" **3**.
3. Konfigurieren Sie den ersten WLC **1** wie gewünscht mit den Profilen und der zugehörigen AP-Tabelle für eine Hälfte der APs. Dieser WLC wird somit zum primären WLC für die bei ihm eingetragenen APs.

Bei einer Backup-Lösung über einen sekundären WLC muss die Zeit für den autarken Weiterbetrieb auf jeden Fall so eingestellt werden, dass der AP während dieser Zeitspanne einen Backup-WLC findet, da der Backup-WLC dem AP keine neue Konfiguration zuweisen kann.

Sobald der AP eine Verbindung zu einem sekundären WLC hergestellt hat, wird der Ablauf der Zeit für den autarken Weiterbetrieb unterbrochen. Der AP bleibt also mit seinen WLAN-Netzwerken auch über diese eingestellte Zeit hinaus aktiv, solange er eine Verbindung zu einem WLC hat.

1. Konfigurieren Sie den zweiten WLC **2** für die andere Hälfte der APs, welche dann diesen WLC als primären WLC betrachten.
2. Der Backup-WLC **3** bleibt bis auf die Uhrzeit und die Root-Zertifikate ohne weitere Konfiguration.
3. Die APs suchen nach dem Start über eine Discovery-Message nach einem WLC. In diesem Fall antworten alle drei WLCs auf diese Nachricht – die APs wählen jeweils "ihren" primären WLC für die folgende DTLS-Verbindung. Die eine Hälfte der APs entscheidet sich für WLC **1**, die andere Hälfte für WLC **2**. Da WLC **3** für keinen der APs als primärer WLC fungiert, meldet sich kein AP bei ihm an.
4. Fällt z. B. der erste WLC **2** aus, suchen die APs automatisch nach einem anderen WLC. Sie finden die WLC **A** und **C**, wobei **A** schon mit seinen 25 APs vollständig ausgelastet ist. Backup-Controller **C** kann die Gültigkeit der Zertifikate prüfen, die APs also authentifizieren und als gemanagte APs annehmen. Da die APs jedoch **nicht** mit ihrer MAC-Adresse in der AP-Tabelle des Backup-WLCs eingetragen sind, kann der Backup-WLC die APs nicht weiter verwalten, sie werden nur mit der jeweiligen aktuellen WLAN-Konfiguration weiterbetrieben.

Sollte WLC **A** nicht ausgelastet sein, weil z. B. einige "seiner" APs ausgeschaltet sind, so könnten sich auch einige der suchenden APs bei diesem anmelden. WLC **A** bleibt für diese APs aber ein "sekundärer" WLC, da er nicht über Konfigurationsprofile für diese Geräte verfügt. Wird in diesem Fall einer der AP wieder eingeschaltet, der über einen Eintrag in der AP-Tabelle von WLC **A** verfügt, nimmt **A** diesen reaktivierten AP wieder auf und trennt sich dafür von einem der APs im Backup-Fall.

Mit der Einstellung des autarken Weiterbetriebs bleiben die APs auch während der Suche nach einem Backup-WLC mit der aktuellen WLAN-Konfiguration in Betrieb, die WLAN-Clients können weiterhin alle Funktionen nutzen.

14.14.5 Automatische Suche nach alternativen WLCs

Ab LCOS 9.00 versucht ein AP nicht mehr, sich bei einem Verbindungsabbruch mit dem zuletzt bekannten WLC neu zu verbinden. Stattdessen sucht der AP im Netz nach einem erreichbaren WLC, der den Kriterien für die *Ermittlung des idealen WLC* entspricht.

14.14.6 One Click Backup der SCEP-CA

Um das Backup der im WLC vorliegenden CA zu vereinfachen, bietet Ihnen das Gerät die Möglichkeit, mit einer einzigen Aktion einen kompletten Zertifikats-Datensatz zu erzeugen (One Click Backup). Dieser Datensatz erlaubt Ihnen die vollständige Sicherung und Wiederherstellung der CA und vermeidet das Auftreten von Zertifikats-Konflikten.

Derartige Konflikte können dann auftreten, wenn Sie die einzelnen PKCS12-Container separat vom Gerät heruntergeladen haben und anschließend wieder einspielen: Hat der WLC in der Zwischenzeit eine neue CA aufgesetzt und neue Zertifikate ausgestellt, führen die abweichenden CAs temporär zu Authentisierungsproblemen bei den verschiedenen Diensten im LCOS. Sofern nicht gewartet werden kann, bis die einzelnen Dienste neue Zertifikate anfordern, erfordert die manuelle Konfliktlösung ein Löschen der SCEP-Dateien aus dem LCOS-Dateisystem und eine Reinitialisierung des SCEP-Clienten. Mit dem Zurückspielen eines One Click Backups dagegen führt das LCOS die notwendigen Schritte automatisch aus.

Erstellen einer Backup-Datei

Um einen Zertifikats-Datensatz zu erzeugen, führen Sie die Aktion **Erstelle-PKCS12-Backup-Dateien** unter **Setup** > **Zertifikate** > **SCEP-CA** > **CA-Zertifikate** aus. Diese Aktion erzeugt eine Zip-Datei innerhalb des LCOS-Dateisystems, die alle notwendigen Dateien enthält. Zum Schutz der enthaltenen Zertifikate und Schlüssel ist die Zip-Datei automatisch mit dem Gerätepasswort geschützt, sofern Sie kein gesondertes Passwort angeben. Die erzeugte Zip-Datei lässt sich anschließend z. B. im WEBconfig über **Extras** > **Dateimanagement** > **Zertifikat oder Datei herunterladen** > **SCEP-CA – One Click Backup** herunterladen.

Zurückspielen der Backup-Datei

Um einen Zertifikats-Datensatz zurückzuspielen, laden Sie die gesicherte Zip-Datei unter Angabe der Passphrase direkt in das Gerät. Im WEBconfig z. B. erfolgt dies über die Auswahl **Extras** > **Dateimanagement** > **Zertifikat oder Datei hochladen** > **SCEP-CA – One Click Backup**. Setzen Sie dabei die Option **Vorhandene CA Zertifikate ersetzen**, damit das Gerät den Zertifikats-Datensatz nach dem Hochladen automatisch zurückspielt.

Sofern Sie die Option nicht setzen oder die Backup-Datei auf andere Weise ins Gerät laden, müssen Sie nach dem Hochladen die Aktion *2.39.2.2.11 Zertifikate-aus-Backup-wiederherstellen* ausführen, damit das Gerät den Zertifikats-Datensatz zurückspielt.

14.15 Automatischer Konfigurationsabgleich (Config-Sync) mit der LANCOM WLC High Availability Clustering XL Option

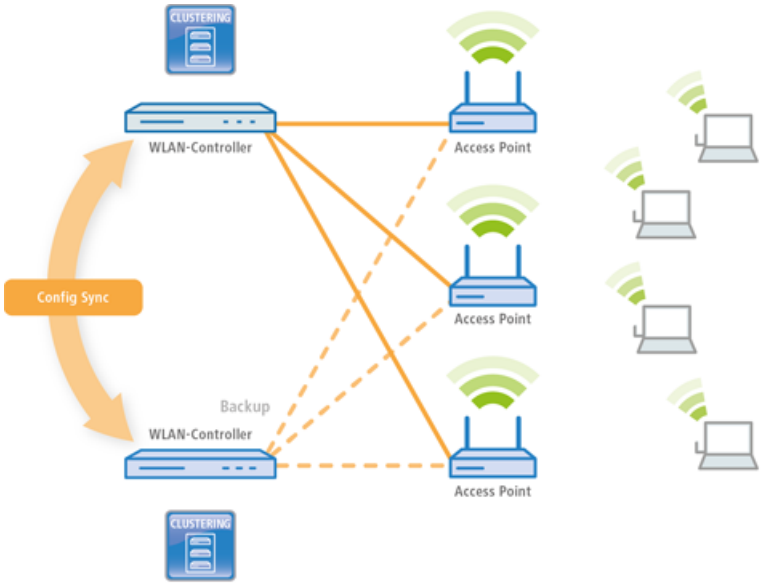
Anwendungsbeispiel WLAN-Controller:

WLAN-Infrastrukturen sind inzwischen integraler Bestandteil moderner Unternehmensnetzwerke. Mit zunehmendem Anspruch an die Verfügbarkeit einer WLAN-Lösung im Kontext des "All Wireless Office" steigt auch der Bedarf an zuverlässigen Backup- und Hochverfügbarkeitslösungen ("High Availability"). In WLAN-Infrastrukturen mit genau einem WLAN-Controller und verbundenen APs kommt es bisher bei Ausfall oder Wartung (z. B. Firmware-Update) des WLCs zu einem automatischen und autarken Weiterbetrieb der am WLC angebundenen APs. Das bedeutet, dass die APs im autarken Betriebsmodus nicht mehr auf die Funktionen zugreifen können, die auf dem WLC zentral verfügbar sind, wie z. B. Public Spot, IEEE 802.1X-Authentifizierung oder Layer-3-Tunnel.

Um dies zu vermeiden und den vollständigen Weiterbetrieb aller WLAN-Funktionen auch bei einer temporären Nichtverfügbarkeit eines WLCs aufrecht zu erhalten, können ein oder mehrere Redundanz- oder Backup-WLCs eingesetzt werden. Im Backup-Fall wechseln die APs automatisch vom temporär nicht verfügbaren WLC zu einem Backup-WLC. Hierfür ist auf dem Backup-WLC die gleiche Konfiguration (z. B. AP-Tabelle oder WLAN-Profile) wie auf dem primären WLC der APs erforderlich. Ersteinrichtung der WLCs sowie jede weitere Konfigurationsänderung muss auf den Geräten dabei jeweils separat und identisch erfolgen – für den Administrator ein enormer Aufwand. Die manuelle Pflege von Konfigurationen über mehrere identische Geräte kann im Backup-Fall mit veralteter oder nicht synchroner Konfiguration des Backup-WLCs zu einem fatalen Zustand der gesamten WLAN-Infrastruktur führen. Die dann startende Fehlersuche gestaltet sich in der Regel als Herausforderung. Auf der Anwenderseite von WLAN-Clients führt dies zu einem Ausfall der Produktivität, die unter Umständen unternehmensweit großen Schaden verursachen kann.

Neu mit der LANCOM WLC High Availability Clustering XL Option: Diese Software-Option ermöglicht die Gruppierung von mehreren WLCs zu einer hochverfügbaren Gerätegruppe (High Availability Cluster). Damit können Konfigurationsänderungen, Funktionen und Erweiterungen, die an einem WLC vorgenommen werden, automatisch auf die anderen WLCs des Clusters übertragen werden, ohne dass jedes einzelne Gerät manuell gemanagt werden muss.

Gemeinsame Parameter in einem Cluster (z. B. WLAN-Profile, AP-Tabellen oder Public Spot-Einstellungen) werden hierbei synchronisiert, individuelle Parameter (wie z. B. die IP-Adresse des WLCs) werden nicht untereinander ausgetauscht.



Mit der LANCOM WLC High Availability Clustering XL Option profitieren Sie von einer deutlich vereinfachten Administration sowie einer enormen Zeitersparnis, da Sie nur einen WLC des Clusters konfigurieren müssen. Die vorgenommenen Änderungen überträgt dieser WLC dann automatisch auf die anderen Cluster-Geräte. In Hinblick auf das oben beschriebene Szenario verbinden sich nun bei Ausfall oder Wartung (z. B. Firmware-Update) eines WLCs die APs automatisch mit einem anderen WLC, der dank Config Sync ganz ohne Zutun des Administrators bereits die identische Konfiguration besitzt. Dadurch wird eine komfortable Hochverfügbarkeit realisiert.

Die Voraussetzungen für eine gültige Gruppenmitgliedschaft eines Gerätes sind:

- Es muss eine LANCOM WLC High Availability Clustering XL Option vorhanden sein (ab LCOS-Version 9.10).
- Es muss eine IP-Kommunikation zu allen anderen Geräten möglich sein, z. B. über LAN, WAN oder VPN.
- Es muss in der Gruppenliste aufgeführt sein, die in jedem Gerät gespeichert ist.
- Es muss ein gültiges Zertifikat vorhanden sein.
- Es muss sich als Gruppenmitglied per Zertifikat authentifizieren können.

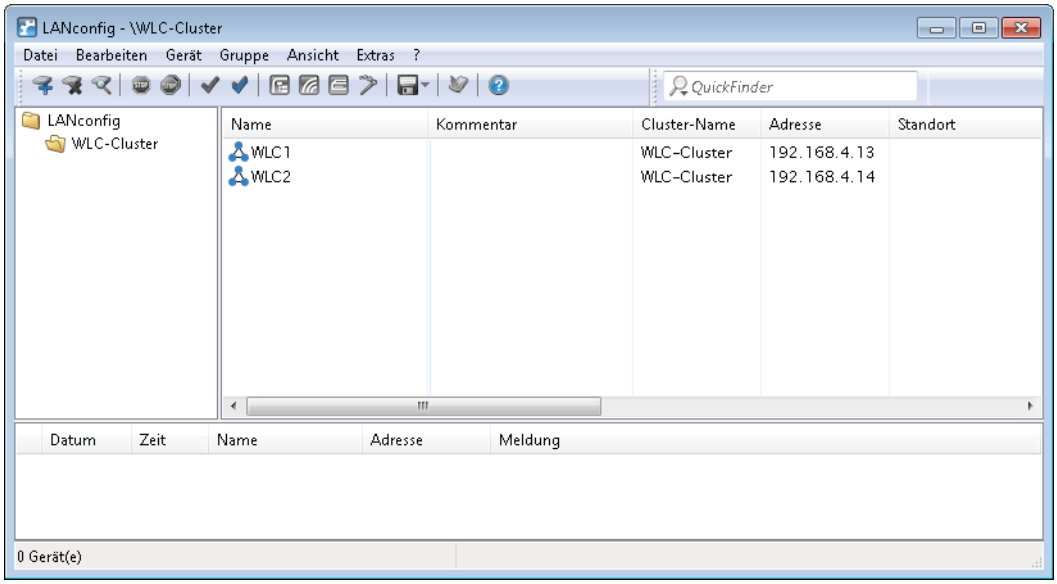
14.15.1 Spezielles LANconfig-Icon für Cluster-Geräte oder mit Config-Sync

LANconfig markiert Geräte, die ihre Konfiguration per Config-Sync teilen, mit einem eigenen Symbol. Zudem ist in der Spalte **Config Cluster** die Konfigurationsgruppe jedes Gerätes ersichtlich. Somit bietet Ihnen LANconfig die Möglichkeit, die Geräteauflistung nach Clusternamen zu sortieren und zu bearbeiten.

Möchten Sie an der Konfiguriation eines Clustermitgliedes Änderungen vornehmen, so erhalten Sie folgende Warnung:

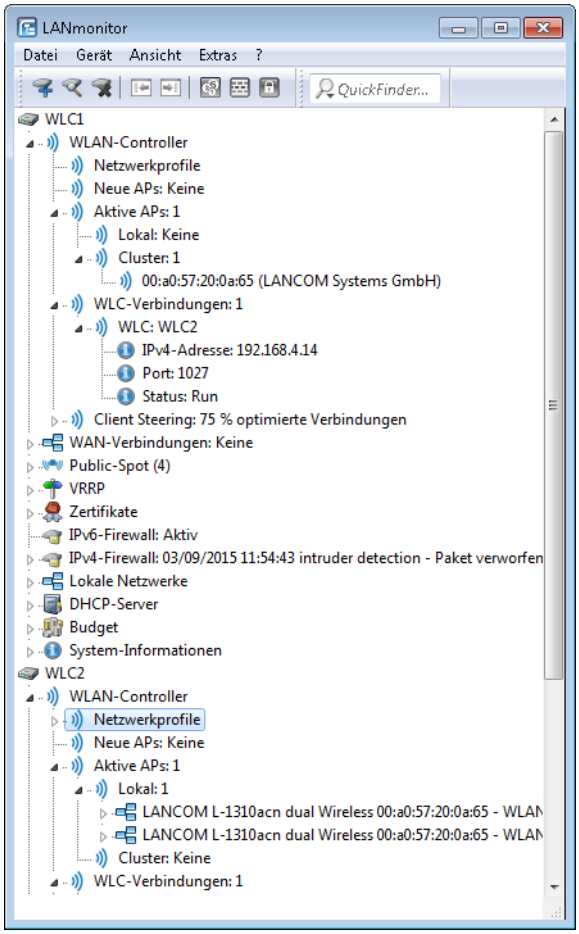
"Dieses Gerät gehört zu dem Config-Cluster: [clustername]. Das Bearbeiten dieser Konfiguration wirkt sich auch auf folgende Geräte aus: [Auflistung aller Geräte des gleichen Clusters]"

Diese Meldung können Sie bei Bedarf umgehen. Aktivieren Sie hierfür die Option **Nicht wieder anzeigen** innerhalb des angezeigten Fensters.



14.15.2 Spezielles LANmonitor-Icon für Cluster-Geräte oder mit Config-Sync

LANmonitor markiert Geräte, die ihre Konfiguration per Config-Sync teilen, mit einem eigenen Symbol. Zudem wird hinter den Gerätenamen der Name der Konfigurationsgruppe (Cluster name) angegeben. Somit können Sie mit LANmonitor die Geräte mit gleicher Konfiguration leichter zuordnen.



15 Public Spot

15.1 Einführung

Dieses Kapitel gibt Antworten auf die beiden folgenden Fragen:

- Was ist ein "Public Spot"?
- Welche Funktionen und Eigenschaften zeichnen das Public Spot-Modul aus?

15.1.1 Was ist ein "Public Spot"?

Public Spots, auch HotSpots genannt, sind Orte, an denen sich Benutzer mit ihren Endgeräten – z. B. einem Smartphone, Tablet-PC oder Notebook – in ein öffentlich zugängliches Netzwerk einwählen können. Üblicherweise stellen diese Netzwerke einen Zugang ins Internet bereit, doch kann ein Public Spot auch auf ein lokes Netzwerk beschränkt sein; z. B. um Besuchern einer musealen Einrichtung oder eines Messegeländes via Intranet zusätzliche Informationen bereitzustellen. Der Begriff wird dabei synonym zu den Geräten benutzt, über welche die Benutzer den Netzzugang schließlich herstellen, weshalb auch dieses Handbuch meistens nicht zwischen der Lokalität und dem Gerät unterscheidet.

15.1.1.1 Die Lösung: (W)LAN-Technologie

Für Public Spot-Szenarios bieten sich die bewährten (W)LAN-Technologien nach den internationalen IEEE 802.11/802.3-Standards an:

- Der Zugang über WLAN ermöglicht den schnellen und unkomplizierten Zugang über Funk: WLAN-Adapter gehören zur Standardausrüstung mobiler Endgeräte und unterstützen Bandbreiten, die selbst das ruckelfreie Abspielen von HD-Videos ermöglichen.
- Der Zugang über LAN ist – bei automatischer Adressvergabe via DHCP – ähnlich unkompliziert: Die meisten Notebooks besitzen standardmäßig einen LAN-Adapter, in den das Netzwerkkabel einzustecken ist.

Beim Zugang über LAN verliert der Anwender zwar seine stationäre und unterbrechungsfreie Flexibilität, allerdings ermöglicht diese Zugangsform – eine entsprechende Infrastruktur vorausgesetzt – selbst bei hoher Netzlast (z. B. durch Multimedia-Inhalte wie Video-on-Demand) und hoher Nutzerzahl (z. B. in einem großen Hotel) einen stabilen Netzbetrieb, wo Verbindungen via WLAN evtl. früher an ihre Grenzen stoßen. Ebenso ist es über einen Public Spot via LAN auch möglich, eine bereits bestehende, kabelgebundene Infrastruktur (z. B. in einer Hochschule) relativ kostengünstig um ein Public Spot-Angebot zu erweitern.

Besonderheiten beim Zugang über (W)LAN

Der Einsatz von herkömmlichen WLAN-Access-Points oder LAN-Routern als Public Spot wird dadurch erschwert, dass die Benutzer-Authentifizierung nur über RADIUS/802.1X möglich ist, was wiederum eine entsprechende Konfiguration erfordert. Aus diesem Grund ist der Einsatz von Geräten ohne Public Spot-Funktion nicht praktikabel, da diese Geräte nicht in der Lage sind, zwischen befugten und unbefugten Nutzern öffentlich zugänglicher Netze zu trennen und deren spezifische Netznutzung entsprechend zu protokollieren.

15.1.1.2 Benutzer-Autorisierung und -Authentifizierung

Sobald sich eine Person mit einem Endgerät in Reichweite eines Access Points befindet, kann sie zu diesem Access Point auch eine spontane Verbindung herstellen. Ähnliches gilt für frei zugängliche LAN-Anschlüsse. Daraus ergibt sich immer dann ein Problem, wenn der Zugang nicht jedermann, sondern nur bestimmten Benutzern zur Verfügung stehen soll. Genau diese Einschränkung ist beim Einsatz von Public Spots typisch.

Ein Public Spot muss daher in der Lage sein, den (W)LAN-Zugang auf Benutzerebene zu kontrollieren. Bei einfachen Public Spot-Installationen reicht es dabei aus, wenn die Benutzerdaten lokal im Router oder Access Point – oder alternativ in einem WLAN-Controller – gespeichert und verwaltet werden. Komplexere Installationen verwenden stattdessen für ein detaillierteres Accounting oder eine direkte Verwaltung Datenbankanbindungen an zentrale Authentifizierungs-Server. Solche zentralen Server arbeiten üblicherweise nach dem RADIUS-Verfahren.

15.1.1.3 Abrechnung (Accounting)

Möchte der Betreiber eines Public Spots diesen Service nicht kostenlos anbieten, muss er die Verbindungsdaten der einzelnen Nutzer erfassen und abrechnen. Üblich ist es beispielsweise, nach vorheriger Bezahlung eine befristete Benutzung zu gewähren (PrePaid-Modell), die verbrauchten Ressourcen im Nachhinein abzurechnen (PostPaid-Modell) oder die unbeschränkte Benutzung bis zu einem bestimmten Zeitpunkt zu erlauben (etwa bis zum Abreisetag in einem Hotel).

Auch für die Accounting-Funktion des Public Spots gilt bei kleinen Installationen, dass sie möglichst unkompliziert lokal im Gerät erfolgen sollte. Für größere Installationen ist eine zentrale Abrechnung über einen externen RADIUS-Server möglich. Je nach Anwendungsszenario, ist über eine Software-Schnittstelle optional auch die Anbindung an externe Systeme realisierbar, welche auf die Abrechnungsdaten zugreifen und die Authentifizierung der Anwender steuern (z. B. Hotelreservierungssysteme).

15.1.1.4 Logging

Das Public Spot-Modul stellt mittels RADIUS-Accounting und SYSLOG geeignete Schnittstellen zur Speicherung der Nutzungsdaten zur Verfügung.

Bitte beachten Sie, dass der Betrieb eines Public Spots (manchmal auch als "HotSpot" bezeichnet) in Ihrem Land rechtlichen Regulierungen unterliegen kann. Bitte informieren Sie sich vor der Einrichtung eines Public Spots über die jeweils geltenden Vorschriften. Informationen zu diesem Thema finden Sie auch im LANCOM Techpaper "Public Spot", erhältlich unter *www.lancom-systems.de*.

15.1.2 Anwendungsszenarien

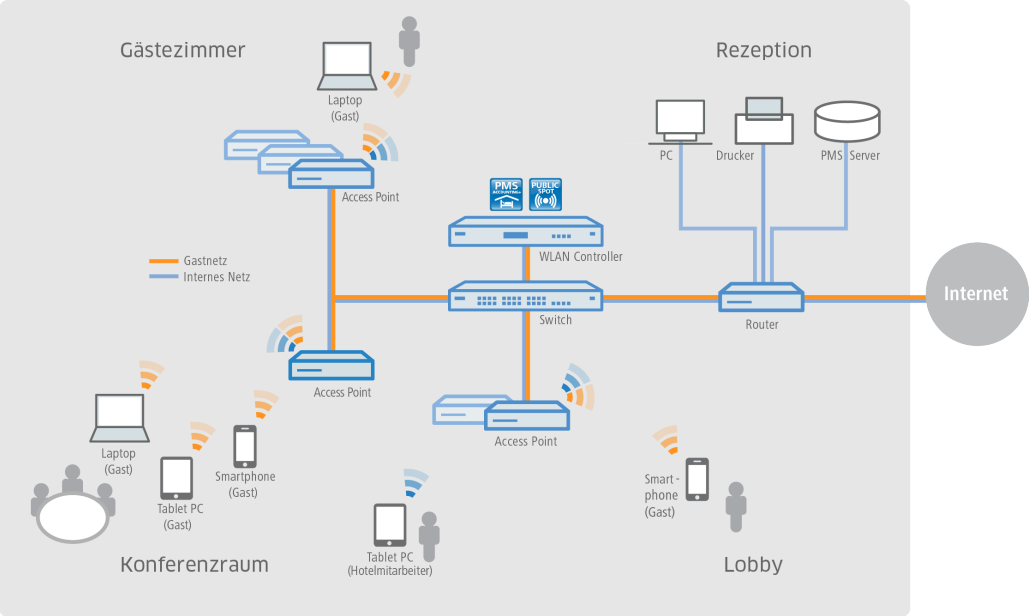
15.1.2.1 Gastzugänge im Hotel

Dank Wireless LAN ist es für Hotelbetreiber so einfach wie nie, ihren Gästen einen komfortablen Internetzugang zu bieten. Hotspot-Lösungen von LANCOM sind schnell installiert und geben Gästen die Möglichkeit, mit dem eigenem Laptop, Tablet oder Smartphone per WLAN auf das Internet zuzugreifen. Ob in der Lobby, dem Konferenzraum oder in Gästezimmern – absolut sicher getrennt vom internen Netz können überall dort, wo es gewünscht ist, Gastzugänge bereitgestellt werden.

Für die komfortable Abrechnung ist die LANCOM Public Spot PMS Accounting Plus Option ideal: Sämtliche Public Spot-Anmeldungen werden hierbei automatisch an den zentralen PMS-Server, auf welchem das Hotelabrechnungssystem installiert ist, weitergeleitet. Gäste können sich so z. B über die Zimmernummer und den Nachnamen am Hotspot anmelden. Bei kostenpflichtigen Internetzugängen können zudem die Nutzungsgebühren direkt auf die Zimmerrechnung verbucht werden. Alternativ sind natürlich auch kostenlose Gastzugänge in Hotels einfach einzurichten – je nach Bedarf.

- **Komfortable Inbetriebnahme und Konfiguration** – ein benutzerfreundlicher Einrichtungs- und Konfigurationsassistent garantiert eine einfache Inbetriebnahme des Hotspots. Genaueres erfahren Sie im Kapitel *Basis-Installation eines Public Spots für einfache Szenarien* auf Seite 1262.
- **Kein Zugriff von Unbefugten auf interne Daten möglich** – per VLAN oder Layer-3-Tunnel erfolgt innerhalb einer Infrastruktur eine sichere Trennung des Haus- und Gastnetzes. Auch auf der Luftschnittstelle lassen sich die Daten sicher verschlüsseln, damit Gäste über das WLAN nicht in das Hotelnetz eindringen können. Genaueres erfahren Sie im Kapitel *Virtualisierung und Gastzugang über WLAN Controller mit VLAN* auf Seite 1163.
- **Einfache Anmeldung des Gastes im WLAN** – durch die Smart Ticket-Funktion erhält der Gast die Zugangsdaten für den Public Spot ganz komfortabel automatisch per SMS oder E-Mail. Alternativ ist auch der Ausdruck eines Vouchers möglich oder die Anmeldung des Gastes über z. B. Zimmernummer/Nachname. Genaueres erfahren Sie im Kapitel *Alternative Anmeldeformen* auf Seite 1311.

- **Einfache Abrechnung von kostenpflichtigen Internetzugängen** – mit der Erweiterung um die LANCOM Public Spot PMS Accounting Plus Option ist die Anbindung an Hotelabrechnungssysteme (wie Micros Fidelio) möglich. Genaueres erfahren Sie im Kapitel *Schnittstelle für Property-Management-Systeme* auf Seite 1342.

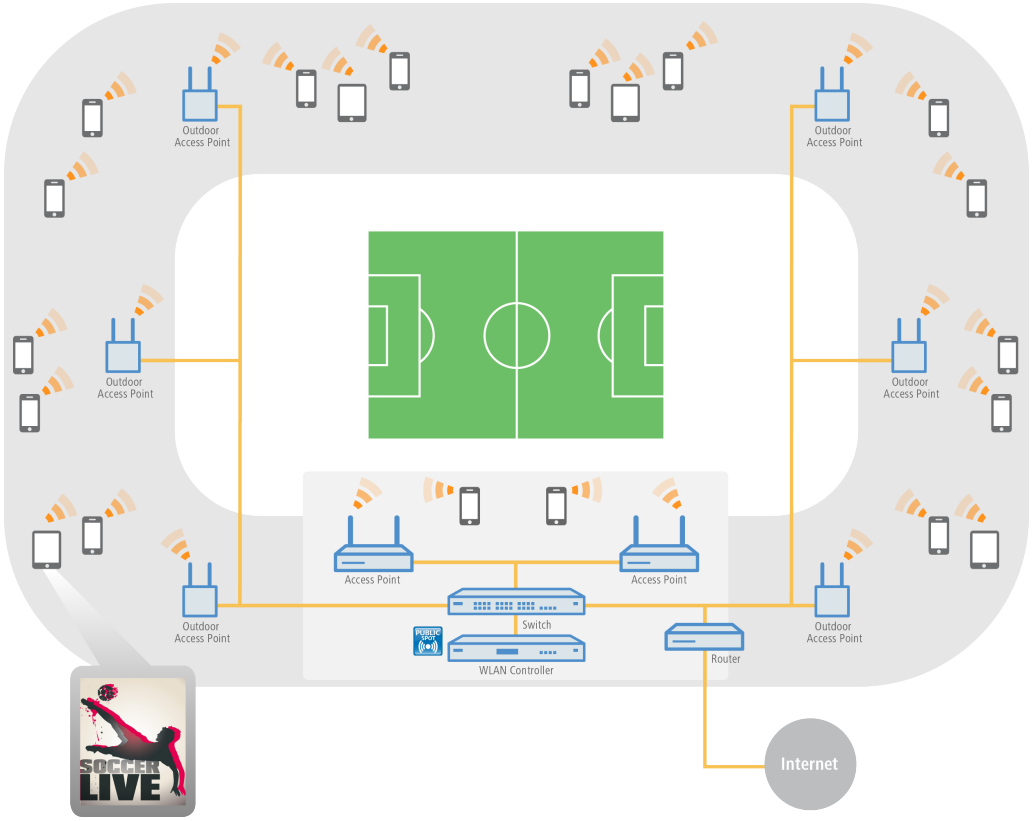


15.1.2.2 Gastzugänge in Sportstadien

Stadien, in denen große Sportveranstaltungen stattfinden, werden immer moderner und sollen auch einer sehr hohen Anzahl an Zuschauern ermöglichen, mit den eigenen Endgeräten den Komfort eines Internetzugangs zu nutzen, um z. B. Live-Content zur Veranstaltung abzurufen oder online zu surfen. Um den Gästen auf der Zuschauertribüne eine – im Vergleich zum überlasteten Mobilfunknetz – schnelle Internetverbindung zu bieten, ist ein Offloading in das Stadion-WLAN mithilfe von LANCOM Lösungen empfehlenswert. Durch die Einbindung der Clients in das Stadion-WLAN bietet sich dem Stadionbetreiber die Möglichkeit, zusätzliche Werbeflächen für Sponsoren und damit zusätzliche Einnahmequellen zu schaffen. So können beispielsweise die Hotspot-Anmeldeseite individuell gestaltet oder verschiedene Sponsoring-Websites freigeschaltet werden.

- **Multimediales Fan-Erlebnis** – durch einen WLAN-Internetzugang erhalten Fans die attraktive Möglichkeit, live aktuelle Sport-News und -informationen sowie beispielsweise Wiederholungen von Spielszenen aufzurufen.
- **Neue Werbeflächen generieren zusätzliche Einnahmen** – durch die individuelle Gestaltungsmöglichkeit der Hotspot-Anmeldeseite sowie die Konfiguration von vordefinierten Websites, die keine Anmeldung erfordern (Walled Garden-Funktion), stehen dem Stadionbetreiber zusätzliche, attraktive Werbeflächen zur Verfügung. Genaueres erfahren Sie im Kapitel *Anmeldungsfreie Netze* auf Seite 1290.

- **Komfortable Inbetriebnahme und Konfiguration** – ein benutzerfreundlicher Einrichtungs- und Konfigurationsassistent garantiert eine einfache Inbetriebnahme des Hotspots. Genaueres erfahren Sie im Kapitel *Basis-Installation eines Public Spots für einfache Szenarien* auf Seite 1262.



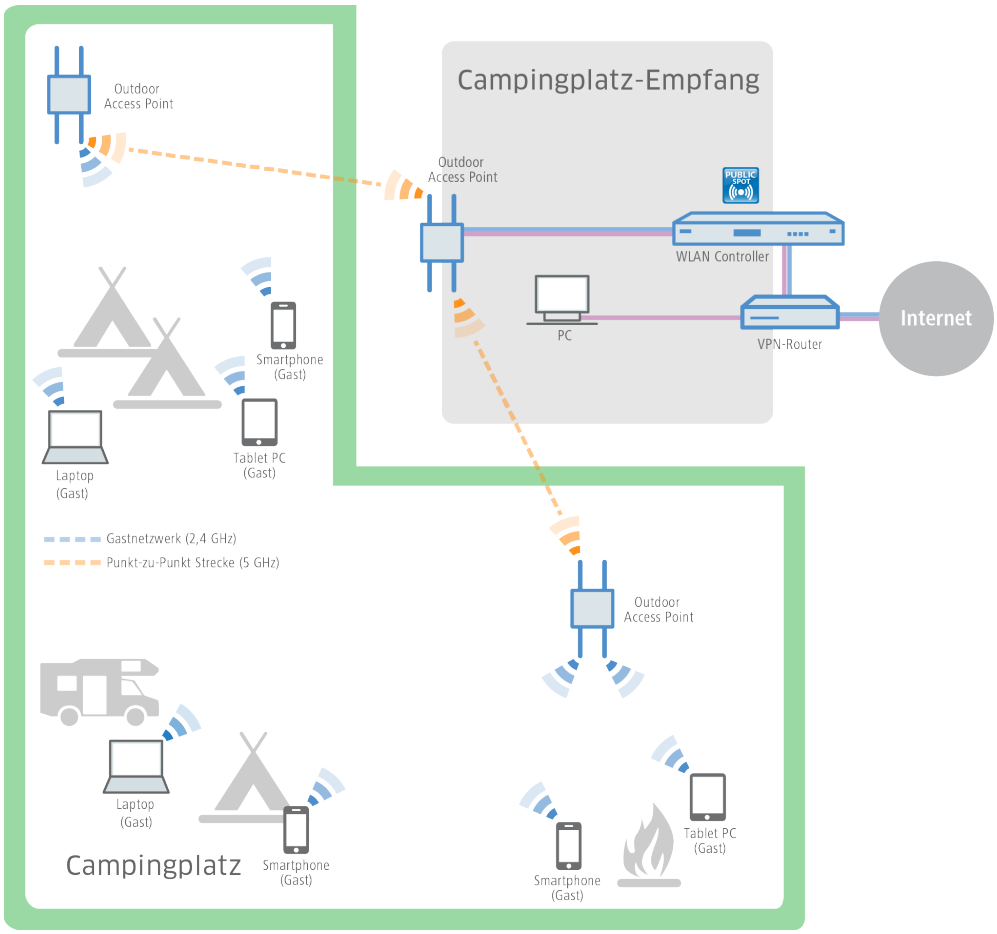
15.1.2.3 Gastzugänge auf Campingplätzen

Campingplätze befinden sich im Freien und sind meist sehr weitläufig. Trotzdem erwarten Urlauber auf modernen Campingplätzen den Komfort, mit dem eigenen Laptop, Tablet oder Smartphone jederzeit auf das Internet zuzugreifen. Ob im Zelt, im Wohnwagen oder am Lagerfeuer – ein überall verfügbarer Internetzugang ist ein echter Wettbewerbsvorteil für Campingplatzbetreiber.

Mit den robusten und wetterbeständigen Outdoor-Geräten von LANCOM und der LANCOM Public Spot Option, lassen sich auch diese anspruchsvollen Szenarien komfortabel umsetzen – ohne das aufwändige und kostenintensive Verlegen von Kabeln. So wird beispielsweise im Verwaltungsgebäude des Campingplatzes ein WLAN Controller (inkl. LANCOM Public Spot Option) mit einem LANCOM Dual Radio Outdoor Access Point verbunden. Von diesem wird das Signal nun über Punkt-zu-Punkt-Strecken im 5-GHz-Frequenzband an weitere Outdoor Access Points geleitet, welche die gewünschten Areale – wie z. B. Stellplätze oder Freizeitbereiche für die Gäste – mit WLAN im 2,4-GHz-Frequenzband abdecken. Dabei ist eine sichere Trennung des Gast- und Verwaltungsnetzes dank VLAN-Zuweisung gewährleistet.

- **Komfortabel online ohne Verlegung von Kabeln** – auch in großen Arealen können Gäste ohne aufwändige Installation mit dem Internet verbunden werden.
- **Komfortable Inbetriebnahme und Konfiguration** – ein benutzerfreundlicher Einrichtungs- und Konfigurationsassistent garantiert eine einfache Inbetriebnahme des Hotspots. Genaueres erfahren Sie im Kapitel *Basis-Installation eines Public Spots für einfache Szenarien* auf Seite 1262.
- **Einfacher Gastzugang** – durch die Smart Ticket-Funktion erhält der Client die Zugangsdaten für den Public Spot ganz komfortabel automatisch per SMS oder E-Mail. Alternativ ist auch der Ausdruck eines Vouchers möglich. Genaueres erfahren Sie im Kapitel *Alternative Anmeldeformen* auf Seite 1311.

- **Zuverlässig auch unter extremen Bedingungen** – dank der robusten IP66 Outdoor-Gehäuse und ihres erweiterten Temperaturbereichs sind die LANCOM Outdoor-Geräte zuverlässig und trotzen auch extremen Wetterbedingungen von -33 bis +70 °C.



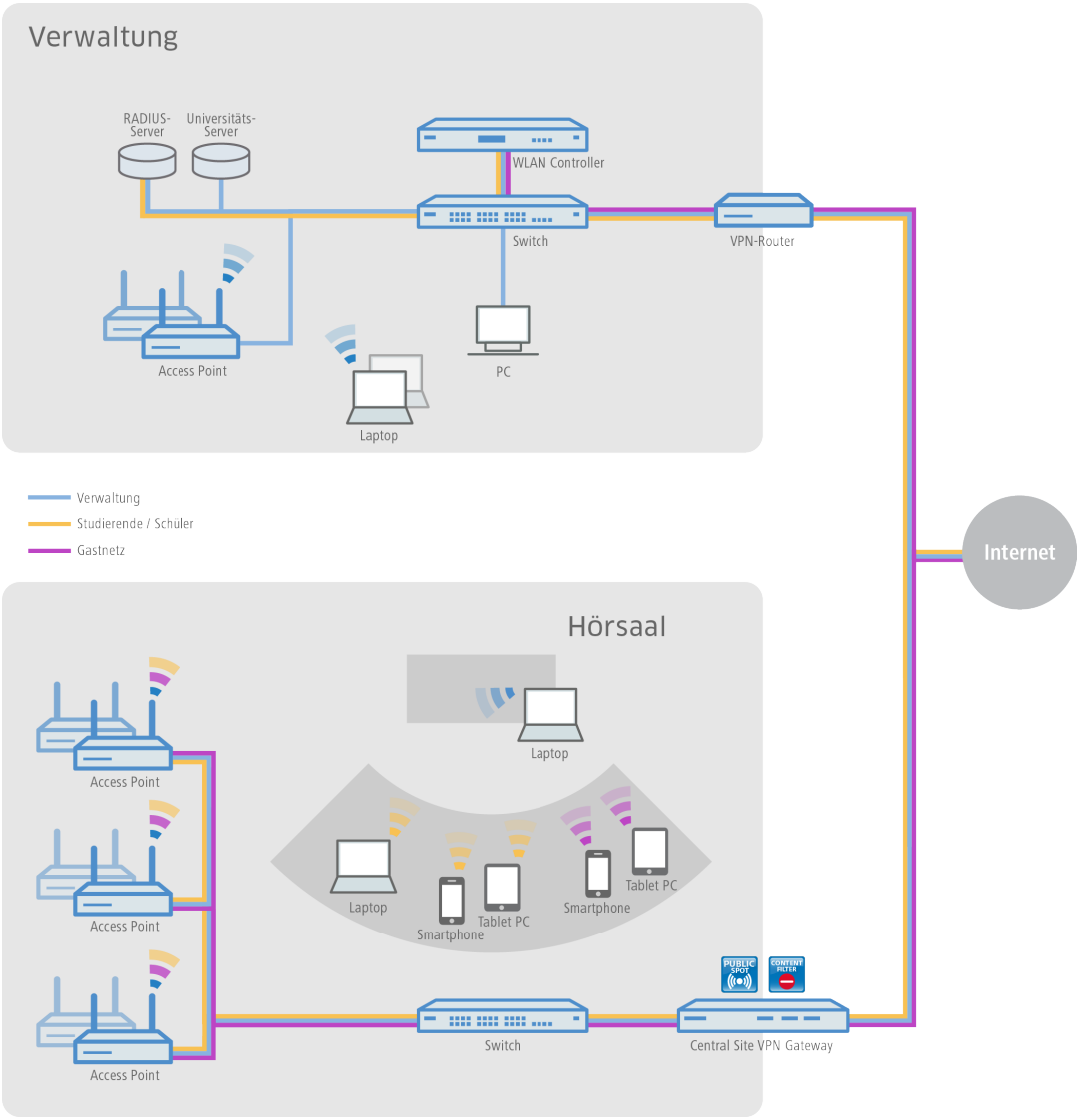
15.1.2.4 Gastzugänge in Schulen und Universitäten

Für Hausarbeiten recherchieren, für Prüfungen lernen, den Unterricht vorbereiten oder interaktiv gestalten. Die Möglichkeit der Internetnutzung ist für Schüler und Studenten sowie Lehrer und Mitarbeiter an modernen Schulen und Universitäten heute unerlässlich – und das auch in voneinander getrennten Gebäudeteilen, möglichst kabellos und mit den eigenen Endgeräten.

Mit Hilfe von LANCOM WLAN-Lösungen ist dies leicht umsetzbar. Indem separate Netze konfiguriert werden, sind die Internetzugänge der Schüler und Studenten vom Zugang der Verwaltung sicher getrennt. Dank dynamischer VLAN-Zuweisung werden die verschiedenen Benutzergruppen über nur eine SSID den für sie vorgesehenen VLANs zugewiesen. So erhält beispielsweise nur das Personal Zugriff auf den Universitätsserver. Gleichzeitig erhalten die Schüler und Studenten den heute so wichtigen Komfort eines weitreichenden WLAN-Gastzugangs. Die Authentifizierung im Schüler- und Studentennetz (z. B. Eduroam) kann beispielsweise über IEEE 802.1X erfolgen. So ist es auch für Gaststudenten von kooperierenden Unis möglich, sich in das WLAN der Gasthochschule einzuwählen. Und selbst Tagungsgästen kann z. B. mittels eines Vouchers ein temporärer Gastzugang zur Verfügung gestellt werden.

- **Sichere Anmeldung für Universitätsangehörige** – Professoren, Studenten und Angestellte der Universität können über das sicher verschlüsselte WLAN Zugang zum Internet und zu verschiedenen Online-Bibliotheken erhalten.
- **Kein Zugriff von Unbefugten auf interne Daten möglich** – per VLAN oder Layer-3-Tunnel erfolgt innerhalb einer Infrastruktur eine sichere Trennung der Verwaltungs-, Studenten- und Professoren- und Gastnetze. Genaueres erfahren Sie im Kapitel *Virtualisierung und Gastzugang über WLAN Controller mit VLAN* auf Seite 1163.

- **Kein Missbrauch des Netzwerks** – durch den LANCOM Content Filter erfolgt eine professionelle, datenbankgestützte Verifizierung von Webseiten. Unerwünschte Websites oder Webinhalte können so für definierte Benutzergruppen unzugänglich gemacht werden.
- **Komfortable, kabellose Internetzugänge** – auch in großen Arealen haben Gäste ohne aufwändige Installation mit ihren mobilen Endgeräten WLAN-Internetzugang.



15.1.2.5 Gastzugänge in Unternehmen

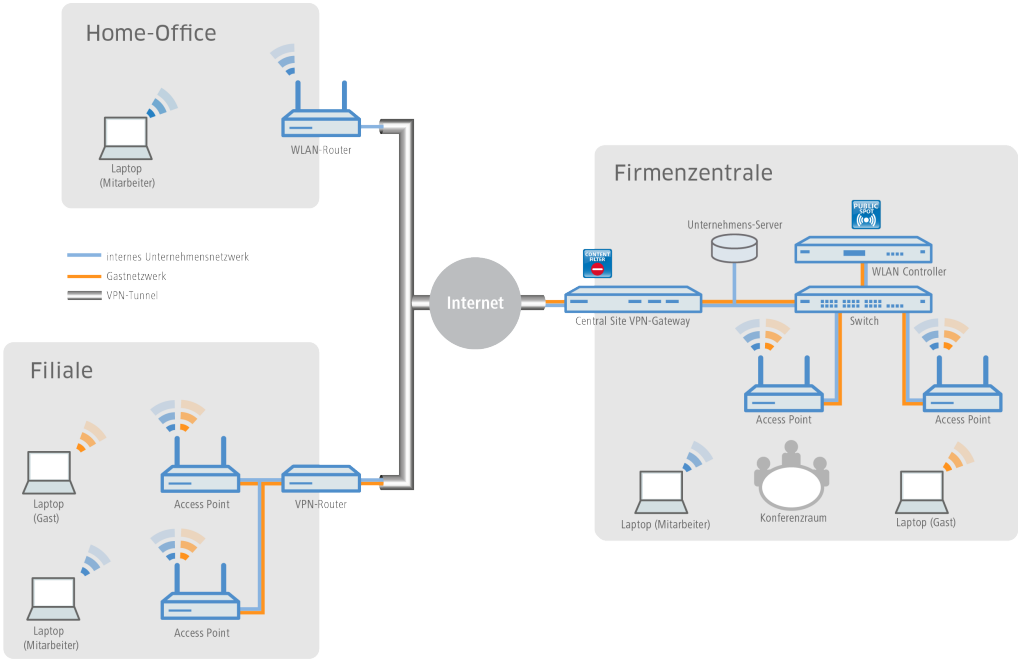
Innerhalb eines Unternehmens mit einer komplexen Netzwerkstruktur ist die Flexibilität und Stabilität des Internetzugangs extrem wichtig. Filialen müssen standortübergreifend auf das Unternehmensnetzwerk zugreifen und Home Office-Mitarbeiter benötigen ebenso Zugriff auf E-Mail-Konten und Datenbanken. Zusätzlich soll Kunden und Besuchern ein separater Gastzugang angeboten werden.

Mit den Geräten von LANCOM und der LANCOM Public Spot Option sind auch diese Szenarien leicht umzusetzen. Über VPN-Tunnel werden dabei die Standorte miteinander verbunden. Unternehmen können ihren externen Gästen durch ein separates Gastnetzwerk in der Firmenzentrale oder auch in angebundenen Filialen Zugriff auf das Internet über die eigenen mobilen Endgeräte gewähren ("Bring Your Own Device"). Dabei bleibt der Zugriff auf unternehmensinterne Daten nur den befugten Mitarbeitern vorbehalten.

- **Sichere Trennung von Unternehmens- und Gastnetz** – durch die sichere Trennung per VLAN oder Layer-3-Tunnel erfolgt innerhalb einer Infrastruktur eine sichere Trennung des Mitarbeiter- und Gastnetzes. Interne Daten sind somit

sicher vor unbefugten Zugriffen. Genaueres erfahren Sie im Kapitel *Virtualisierung und Gastzugang über WLAN Controller mit VLAN* auf Seite 1163.

- **Komfortable Inbetriebnahme und Konfiguration** – über LANCOM WLAN Controller können unterschiedliche Benutzerprofile definiert und die Konfigurationen in die verschiedenen WLAN-Geräte – selbst über entfernte Standorte hinweg – eingespielt werden.
- **Einfacher Gastzugang** – über Voucher können den Gästen am Empfang Zugangsdaten für den Public Spot ganz komfortabel für die Nutzung eigener mobiler Clients zur Verfügung gestellt werden ("Bring Your Own Device"). So erhalten nur registrierte Besucher Zugang zum Internet sowie ggf. Zugriff auf weitere Dienste wie E-Mail-Konten.
- **Kein Missbrauch des Netzwerks** – durch den LANCOM Content Filter erfolgt eine professionelle, datenbankgestützte Verifizierung von Webseiten. Unerwünschte Websites oder Webinhalte können so für definierte Benutzergruppen unzugänglich gemacht werden.



15.1.2.6 Gastzugänge für Provider

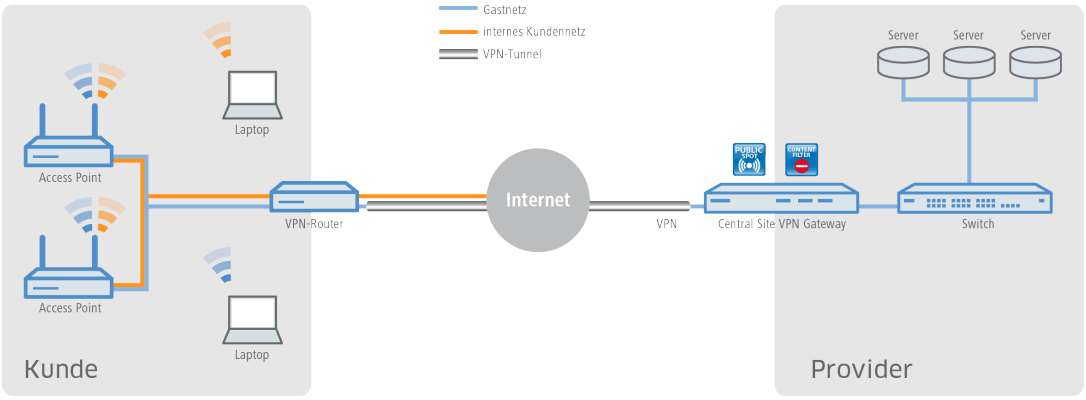
Für Internet-Provider ist es mit den Lösungen von LANCOM sehr einfach, bei ihren Kunden ein Netzwerk mit Gastzugängen anzubieten. Der Provider erhält von LANCOM alle benötigten Netzwerkprodukte aus einer Hand und managt die Netzwerke seiner Kunden zentral und komfortabel – ohne einen Techniker vor Ort.

Für die Umsetzung werden beim Kunden des Providers (beispielsweise ein Hotel, Krankenhaus oder Geschäft) LANCOM Access Points hinter einem LANCOM VPN-Router installiert. Ein separat getrenntes, internes Netz verfügt über einen direkten Internetzugang. Der Gastzugang läuft über einen sicheren VPN-Tunnel zunächst zum Central Site VPN Gateway beim Provider, der auf seinen internen Servern die ankommenden Anfragen protokollieren kann. Ebenfalls kann er mit dem LANCOM Content Filter den Zugang von unerwünschten oder illegalen Websites für die Gastzugänge des Kunden einschränken oder sperren.

- **Einfaches und zentrales Management und Rollout** – auch ohne einen Techniker vor Ort kann der Provider zentral die Netzwerke der Kunden überwachen und konfigurieren. Genaueres erfahren Sie im Kapitel *Basis-Installation eines Public Spots für einfache Szenarien* auf Seite 1262.
- **Verschiedene Redirect-Optionen** – durch Netztrennung können verschiedene Gestaltungsmöglichkeiten des Hotspot-Dienstes realisiert werden. So kann den Endkunden z. B. ausschließlich die Verwaltung ihres Hotspots angeboten werden oder auch ein Full-Service bereitgestellt werden, indem der komplette Datenverkehr vom Endkunden zum Provider getunnelt weitergeleitet wird.
- **Anbindung eigener AAA-Systeme** – LANCOM stellt verschiedene Schnittstellen (RADIUS, XML, FIAS) zur Verfügung, mit denen eigene AAA-Server kombiniert werden können. So kann die Authentifizierung und Anmeldung am Hotspot

sowie die Abrechnung providerspezifisch umgesetzt werden. Genaueres erfahren Sie im Kapitel *Alternative Anmeldeformen* auf Seite 1311.

- **Multi-Provider-Unterstützung** – LANCOM Geräte sind nicht auf das Zurückgreifen auf einen bestimmten Provider festgelegt. Hotspot-Dienstanbieter, die über Kooperationen mit verschiedenen Providern verfügen, können Ihre Software-Lösungen über verschiedene Schnittstellen mit LANCOM Geräten kombinieren. Genaueres erfahren Sie im Kapitel *Alternative Anmeldeformen* auf Seite 1311.
- **Kein Missbrauch des Netzwerks** – durch den LANCOM Content Filter erfolgt eine professionelle, datenbankgestützte Verifizierung von Webseiten. Unerwünschte Websites oder Webinhalte können so für definierte Benutzergruppen unzugänglich gemacht werden.
- **Data Offloading** – WLAN-Hotspots entlasten wirkungsvoll das Mobilfunk-Netz, indem der Datenverkehr auf andere Infrastrukturen ausgelagert wird.

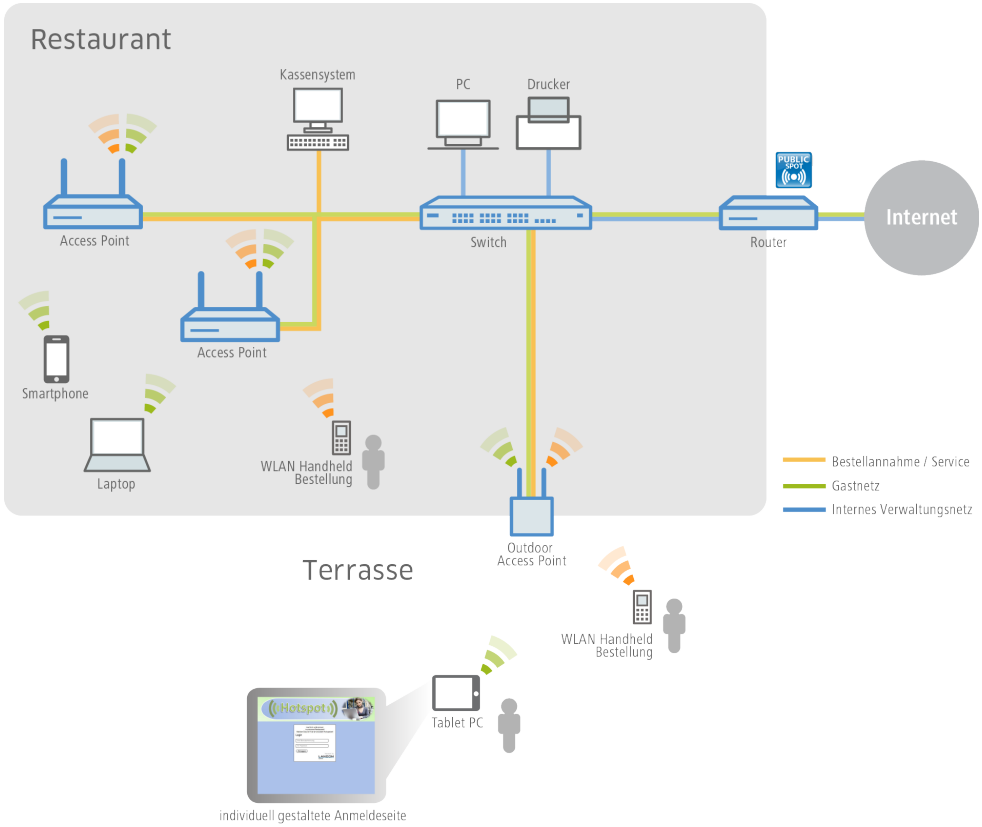


15.1.2.7 Gastzugänge in der Gastronomie

Den Gästen in einem modernen Restaurant oder Café einen Hotspot zur Verfügung zu stellen, kann die Attraktivität der Location deutlich steigern. Mit den WLAN-Lösungen von LANCOM profitieren die Gäste von einem WLAN-Gastnetz, sodass sie mit ihren mobilen Smartphones, Tablet PCs oder Laptops komfortabel das Internet nutzen können – und das absolut sicher getrennt vom internen Verwaltungsnetz. Für eine deutliche Steigerung der Effizienz im Arbeitsablauf haben die Servicekräfte zudem die Möglichkeit, Bestellungen mithilfe eines WLAN-fähigen Handhelds aufzunehmen und direkt an das Kassensystem, die Küche oder an die Getränketheke zu übertragen. Natürlich ist ein WLAN-Zugang für die Gäste als auch für die Bestellannahme ebenso im Terrassen- oder Außenbereich der Gastronomie verfügbar, denn für Bereiche im Freien eignet sich ideal ein robuster LANCOM Outdoor Access Point

- **Individueller und flexibler Gestaltungsspielraum** – ob eigene Logos, Texte oder Bilder – die Begrüßungsseite des Public Spots kann ganz einfach nach den eigenen Wünschen gestaltet werden. Auch das Aufrufen vordefinierter Websites ist möglich (Walled Garden-Funktion), sodass z. B. die Speisekarte des Restaurants oder die eigene Website ohne vorherige Anmeldung am Hotspot vom Gast besucht werden kann. Genaueres erfahren Sie im Kapitel *Geräteeigene und individuelle Voucher- und Authentifizierungsseiten (Templates)* auf Seite 1346.
- **Kein Zugriff von Unbefugten auf interne Daten möglich** – per VLAN oder Layer-3-Tunnel erfolgt innerhalb einer Infrastruktur eine sichere Trennung der Netze. Genaueres erfahren Sie im Kapitel *Virtualisierung und Gastzugang über WLAN Controller mit VLAN* auf Seite 1163.
- **Komfortable Inbetriebnahme und Konfiguration** – ein benutzerfreundlicher Einrichtungs- und Konfigurationsassistent garantiert eine einfache Inbetriebnahme von Hotspots. Genaueres erfahren Sie im Kapitel *Basis-Installation eines Public Spots für einfache Szenarien* auf Seite 1262.

› **Einfacher Gastzugang** – durch die Smart Ticket-Funktion erhält der Gast die Zugangsdaten für den Public Spot ganz komfortabel automatisch per SMS oder E-Mail. Alternativ ist auch der Ausdruck eines Vouchers möglich. Genaueres erfahren Sie im Kapitel *Alternative Anmeldeformen* auf Seite 1311.



15.1.3 Das Public Spot-Modul im Überblick

Die Ansprüche an Geräte im Public Spot-Betrieb sind so unterschiedlich, wie die Umgebungen, in denen sie eingesetzt wird. Ein Public Spot verfügt über Funktionen für die unterschiedlichsten Bedürfnisse, die in den folgenden Abschnitten genauer beschrieben sind.

15.1.3.1 Open User Authentication (OUA)

Die Open User Authentication (OUA) stellt eine web-basierte Authentisierung über ein Formular bereit und eignet sich deshalb optimal für Public Spot-Installationen.

Typischer Ablauf einer Online-Sitzung mit OUA

1. Der Benutzer eines (W)LAN-fähigen Endgerätes befindet sich in Reichweite eines Access Points bzw. einer Netzwerkdose im Public Spot-Betrieb.

   › WLAN: Nach dem Systemstart meldet sich der WLAN-Adapter automatisch an betreffenden Access Point an.
   › LAN: Nach dem Systemstart stellt der Benutzer über ein geeignetes Kabel den Netzanschluss her und lässt sich vom DHCP-Server eine Adresse zuweisen.

   Ein Internetzugang oder der Zugriff auf einen kostenpflichtigen Service ist in dieser Phase noch nicht möglich.
2. Der Benutzer startet seinen Web-Browser. Das den Public Spot-Service anbietende Gerät führt den Benutzer automatisch auf die Anmeldeseite des Public Spots. Auf dieser Seite findet er detaillierte Informationen zum angebotenen Service.

   Alternativ führt das vom Benutzer verwendete Endgerät automatisch eine Captive-Portal-Erkennung durch und präsentiert direkt nach der Einbuchung in das WLAN die Anmeldeseite des Public Spot.

In der Regel hat der Benutzer seine Anmeldedaten in Form eines Vouchers für einen zeitlich begrenzten Zugang zum Public Spot erhalten. Es sind aber auch andere Anmeldeformen denkbar, wie z. B. die Anmeldung nach Bestätigen der Nutzungsbestimmungen des Betreibers oder die selbstständige Anforderung der Zugangsdaten via E-Mail oder SMS.

3. Im Falle einer Voucher-Anmeldung trägt der Benutzer auf der Anmeldeseite seine Zugangsdaten (Benutzerkennung und Passwort) ein. Je nach Konfiguration prüft entweder der geräteinterne oder ein externer RADIUS-Server die eingegebenen Anmeldedaten. Im Erfolgsfall erhält der Benutzer den Zugang zum Public Spot, ansonsten erscheint eine Fehlermeldung. Falls die Verwendung von Zeitkontingenten gewünscht ist (PrePaid-Modell), überträgt der RADIUS-Server dem Public Spot zusätzlich Informationen zum verfügbaren Zeitguthaben des Benutzers.
4. Der Benutzer kann sich jederzeit beim Public Spot abmelden. Unabhängig davon beendet der Public Spot eine Sitzung selbstständig bei vollständigem Ablauf des Zeitguthabens, bei Erreichen eines festgelegten Ablaufdatums oder bei längerem Kontaktabbruch.

   Während und beim Beenden der Sitzung liefert der Public Spot dem Benutzer eine Übersicht über die Sitzungsdaten. Auf Wunsch meldet der Public Spot parallel dazu alle wichtigen Abrechnungsinformationen des Benutzers an den zuständigen RADIUS-Accounting-Server. Dies kann entweder der geräteinterne oder ein extern konfigurierter Server sein.

15.1.3.2 Sicherheit im (W)LAN

Bei der Betrachtung von (W)LANs entstehen oft erhebliche Sicherheitsbedenken. Solche Bedenken existieren im Zusammenhang mit Public Spots sowohl beim Betreiber als auch beim Benutzer.

Sicherheit für den Betreiber

Für den Betreiber eines Public Spots steht die Absicherung seiner Netzwerk-Infrastruktur im Vordergrund. Das Public Spot-Modul stellt dem Betreiber deshalb eine Reihe von Sicherungstechnologien und -methoden zur Verfügung:

- **Multi-SSID** (nur WLAN)**, VLAN und virtuelle Router**
  - Die sichere Abgrenzung des öffentlichen Zugangs kann durch eine oder mehrere separate Funkzellen eines Access Points erfolgen (Multi-SSID).
  - VLAN-Technik kann den öffentlichen Zugang vom privaten Netz des Betreibers trennen.
  - Die virtuelle Routing-Technologie ARF (Advanced Routing and Forwarding) von LANCOM Systems versieht eine SSID mit eigenen Sicherheits- und QoS-Einstellungen und routet darüber nur bestimmte Ziele.

  So kann der Gastzugang über einen Public Spot – sicher und effektiv vom Produktivnetz getrennt – die gemeinsame Infrastruktur mitnutzen. Die geräteinterne Firewall kann dabei z. B. die für Public Spot-Nutzer verfügbare Bandbreite im WAN auf max. 50 % begrenzen und nur auf Webseitenzugriffe (HTTP, Port 80) und Namensauflösungen (UDP 53) einschränken.
- **Traffic-Limit**

  Um Denial-of-Service- (DoS-) und Brute-Force-Angriffe auf den Public Spot zu verhindern, können Sie den zulässige Datentransfer noch nicht authentisierter Public Spot-Teilnehmer auf ein ungefährliches Volumen begrenzen.
- **Sperren des Konfigurationszugangs**

  Sie können den Web-Zugriff auf die Gerätekonfiguration (z. B. Ihres Access Points, WLAN Controllers oder Routers) aus dem Public Spot-Netzwerk heraus sperren, so dass der Konfigurationszugang nur über andere festgelegte Management-Schnittstellen möglich ist.

Sicherheit für den Benutzer

Für den Benutzer eines Public Spots steht die Vertraulichkeit der übertragenen Daten im Vordergrund. Zudem wünscht er die Sicherung seiner Benutzerdaten gegen Missbrauch. Ihn schützen folgende Sicherungstechnologien:

- **Intra-Cell Blocking** (nur WLAN)

Unterbinden Sie in Ihrem Public Spot-Netzwerk die Kommunikation der WLAN-Clients untereinander. Diese Maßnahme erschwert – über die nutzerseitig evtl. ohnehin schon bestehenden Schutzmechanismen – den Zugriff auf die Ressourcen Ihrer Public Spot-Benutzer.

› **Verschlüsselung während der Anmeldephase**

Sofern Sie über ein digitales Zertifikat verfügen, können Sie dieses in Ihr Gerät laden, um über das verschlüsselte HTTPS-Verfahren Benutzernamen und Kennwörter sicher zu schützen. Das digitale Zertifikat sollte dabei von einer anerkannten öffentlichen Stelle signiert sein, damit ein Browser es als vertrauenswürdig einstuft und Ihren Nutzern keine Sicherheitswarnung ausgibt. Ohne ein Zertifikat erfolgt die Übertragung der Anmeldedaten unverschlüsselt.

Das Zertifikat sichert lediglich den Anmeldevorgang ab; innerhalb eines Public Spot-Netzwerks werden die Daten in der Regel unverschlüsselt übertragen. Dies gilt sowohl für Verbindungen über LAN als auch über WLAN. Sofern Ihre Nutzer also den normalen Datenverkehr absichern möchten, sind sie auf eigene Verschlüsselungsmechanismen angewiesen!

Ausgenommen davon sind WLAN-Verbindungen, die über Hotspot 2.0 erfolgen: Da der Hotspot-2.0-Standard auf WPA2 (802.1X/802.11i), EAP und 802.11u basiert, werden Datenpakete sowohl bei der Autorisierung als auch während der Sitzung stets verschlüsselt übertragen.

LANCOM empfiehlt dringend, sensitive Nutzdaten immer über verschlüsselte Verbindungen zu übertragen, z. B. durch IPSec-basierte VPN-Tunnel mit dem LANCOM Advanced VPN Client oder durch normale HTTPS-gesicherte Datenverbindungen. Außerdem sollte der Public Spot-Benutzer auf die Aktivierung einer Personal Firewall auf seinem Endgerät achten.

15.1.3.3 Assistent zur Einrichtung eines Public Spots

Der Setup-Assistent **Public Spot einrichten** unterstützt Sie bei der Einrichtung und ersten Konfiguration Ihres Public Spots. Mit seiner Hilfe gelingt es Ihnen, mit wenigen Klicks ein funktionsfähiges Public Spot-Netzwerk bereitzustellen. Der Assistent gruppiert dazu die dafür notwendigen Einstellungen (z. B. Zuweisen einer Schnittstelle, Vergeben eines IP-Bereichs, Festlegen von Zugangform und Anmeldungsverfahren, Protokollierung) und bietet Ihnen darüber hinaus die Option, einen Administrator mit beschränkten Rechten anzulegen, dem ausschließlich die Einrichtung und ggf. Verwaltung von Public Spot-Nutzern erlaubt ist.

15.1.3.4 Assistent zum Einrichten und Verwalten von Benutzern

Mit Hilfe des Setup-Wizards **Public-Spot-Benutzer einrichten** (Benutzer-Erstellungs-Assistent) erstellen Sie über WEBconfig zeitlich begrenzte Zugänge zu einem Public Spot-Netzwerk mit wenigen Mausklicks. Dabei bestimmen Sie im einfachsten Fall lediglich die Dauer des Zugangs; der Assistent vergibt Benutzername und Kennwort automatisch und speichert den Zugang in der Benutzerdatenbank des geräteinternen RADIUS-Servers. Der Anwender erhält abschließend ein ausdruckbares, personalisiertes Ticket (Voucher), mit dem er sich im Public Spot-Netzwerk ab sofort bis zur definierten Ablaufzeit anmelden kann.

Alternativ lassen sich Voucher auch auf Vorrat anlegen und ausdrucken, um z. B. in Stoßzeiten die Voucher-Ausgabe zu beschleunigen oder Mitarbeitern ohne Gerätezugriff die Voucher-Ausgabe zu ermöglichen. Hierzu geben Sie im Benutzer-Erstellungs-Assistenten an, dass die Nutzungsdauer erst ab dem ersten Login des Anwenders beginnt. Außerdem definieren Sie eine maximale Gültigkeitsdauer für den Zugang – nach dieser Zeit löscht der Public Spot den Zugang automatisch, auch wenn die Nutzungsdauer noch nicht abgelaufen ist.

Der Setup-Wizard **Public-Spot-Benutzer verwalten** (Benutzer-Verwaltungs-Assistent) stellt alle eingetragenen Public Spot-Zugänge auf einer eigenen Webseite in einer tabellarischen Übersicht dar. So haben Sie mit einem Klick die wichtigsten Daten Ihrer Nutzer im Blick und können auf komfortable Weise die Gültigkeit des Zugangs verlängern / verkürzen oder das betreffende Benutzerkonto komplett löschen. Zusätzlich lassen sich über den Assistenten Informationen zum Benutzerkonto abrufen, wie z. B. das vergebene Passwort im Klartext, der Authentifizierungsstatus, die IP-Adresse, die gesendeten / empfangenen Datenmengen oder etwaige Beschränkungen, die für das Benutzerkonto gelten.

Verwalten mehrere Administratoren die Public Spot-Zugänge, haben Sie die Möglichkeit, die Anzeige der angelegten Accounts auf den jeweiligen Administrator zu beschränken. Als Folge erscheinen in der tabellarischen Übersicht lediglich die angelegten Zugänge des gerade angemeldeten Administrators.

Diese Beschränkung zeigt keine Wirkung, falls ein Administrator-Zugang existiert, dessen kompletter Name Bestandteil der übrigen Administratoren-Accounts ist. "PSpot_Admin" sieht z. B. die Einträge von "PSpot_Admin1" und "PSpot_Admin2". "PSpot_Admin" fungiert in diesem Szenario als Super-Admin. Alle anderen Administratoren ("PSpot_AdminX") dagegen sehen die Einträge der anderen nicht.

15.2 Einrichtung und Betrieb

Dieses Kapitel enthält die wichtigsten Informationen zu Einrichtung und Betrieb eines Public Spots.

- **1. Schritt: Grundkonfiguration**

  Zunächst beschreiben wir die Grundkonfiguration. Nach Abschluss der Grundkonfiguration ist der Public Spot betriebsbereit und für einfaches Anwendungsszenario (Anmeldung über Voucher) vorkonfiguriert.

- **2. Schritt: Sicherheitseinstellungen**

  Dieses Kapitel geht explizit auf sicherheitsrelevanten Einstellungen ein, mit denen Sie Angriffe auf Ihr Public Spot-Netzwerk erschweren und den stabilen Betrieb verbessern. Sofern Sie die hier beschriebenen Einstellungen nicht bereits nicht im Rahmen anderer Einrichtungsschritte getätigt haben, sollten Sie den nachfolgenden Seiten erhöhte Aufmerksamkeit schenken.

- **3. Schritt: Erweiterte Funktionen und Einstellungen**

  Schließlich richtet sich der Blick auf zahlreiche erweiterte Funktionen und Einstellungsoptionen. In detaillierten Beschreibungen erfahren Sie, wie Sie Ihr Gerät individuell an Aufgabe und Umfeld anpassen. Außerdem lernen Sie, wie Sie sich während des Betriebes einen Überblick über Zustand und Aktivitäten des Public-Spots verschaffen.

Bitte beachten Sie, dass der Betrieb eines Public Spots (manchmal auch als "HotSpot" bezeichnet) in Ihrem Land rechtlichen Regulierungen unterliegen kann. Bitte informieren Sie sich vor der Einrichtung eines Public Spots über die jeweils geltenden Vorschriften. Informationen zu diesem Thema finden Sie auch im LANCOM Techpaper "Public Spot", erhältlich unter *www.lancom-systems.de*.

15.2.1 Grundkonfiguration

Die Anleitung der Grundkonfiguration ist in mehrere separate Abschnitte aufgeteilt:

- Der erste Abschnitt beschreibt die Einrichtung eines funktionsfähigen Public Spots am Beispiel eines Wireless Routers.

  Um einen Public Spot für ein einfaches Anwendungsszenario einzurichten, können Sie einen entsprechenden Assistenten starten, der Sie bei der Inbetriebnahme des Public Spots unterstützt.

- Der zweite Abschnitt beschreibt die Konfiguration der Standardwerte für die Benutzer-Assistenten, mit denen auch Mitarbeiter ohne allgemeine Administrator-Rechte neue Public Spot-Benutzer sehr komfortabel anlegen und verwalten können. Hierzu gehört auch das Anlegen eines beschränkten Zugangs, welcher Ihren Mitarbeitern lediglich den Zugriff auf diese Assistenten gewäht.
- Der dritte Abschnitt beschreibt die Benutzerverwaltung im lokalen RADIUS-Server, wahlweise über die Benutzer-Assistenten oder manuell über LANconfig.

Die Abschnitte bauen teilweise aufeinander auf, Sie sollten also idealerweise diese Informationen in der entsprechenden Reihenfolge bearbeiten.

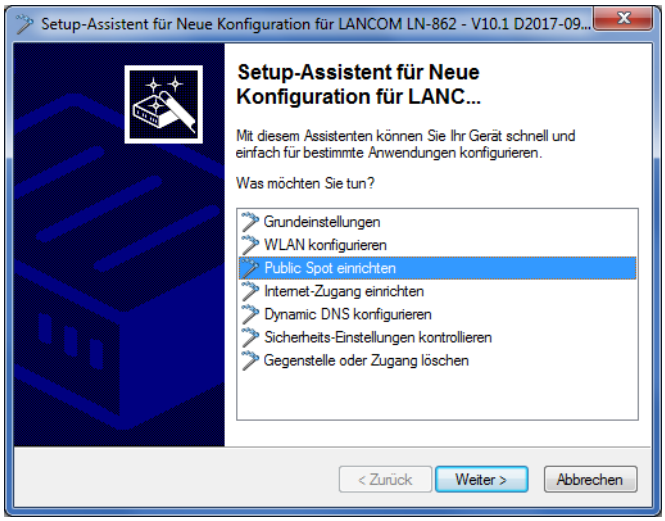
15.2.1.1 Basis-Installation eines Public Spots für einfache Szenarien

Installation über den Setup-Assistenten

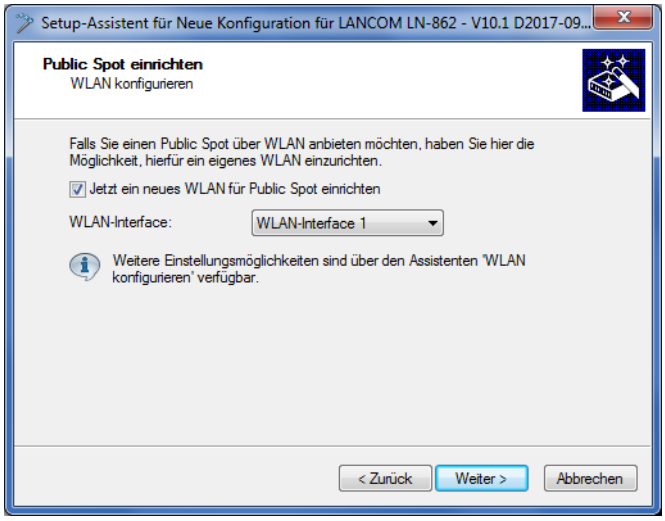
Der folgende Abschnitt beschreibt, wie Sie mit dem Einrichtungs-Assistenten die Basis-Installation eines Public Spots über LANconfig vornehmen.

Der Assistent für die Basis-Konfiguration des Public Spots zeigt je nach Gerätetyp und Verlauf verschiedene Dialoge. Dieses Tutorial stellt nur ein mögliches Beispiel dar.

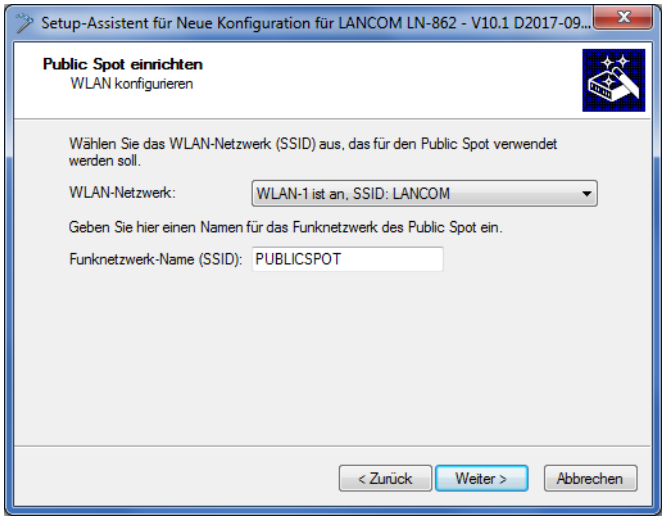
1. Starten Sie dazu LANconfig und markieren Sie das Gerät, für das Sie einen Public Spot einrichten wollen, z. B. einen Access Point.
2. Starten Sie den Setup-Assistenten über **Gerät** > **Setup Assistent**, wählen Sie die Aktion **Public Spot einrichten** und klicken Sie anschließend auf **Weiter**.



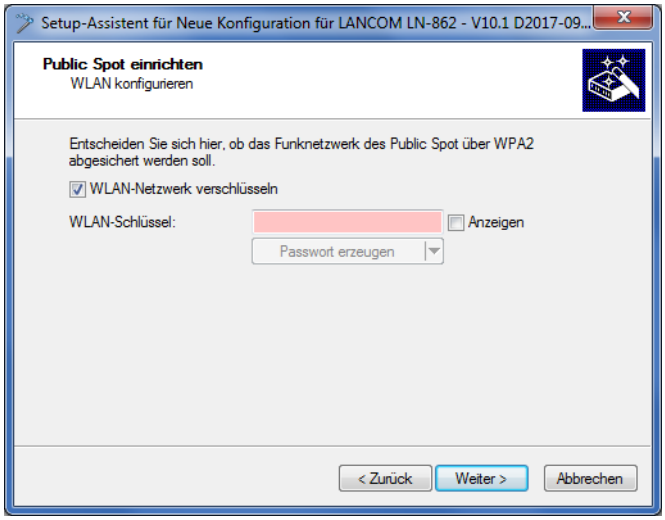
3. Falls Sie die Nutzung des Public Spots über WLAN einrichten möchten, aktivieren Sie die entsprechende Option und klicken Sie auf **Weiter**.



4. Wählen Sie aus dem Auswahlmenü die logische Schnittstelle aus, über die Sie den Public Spot anbieten wollen (z. B. WLAN-1), und geben Sie dem Funknetzwerk einen aussagekräftigen Namen (PUBLICSPOT). Klicken Sie auf **Weiter**.

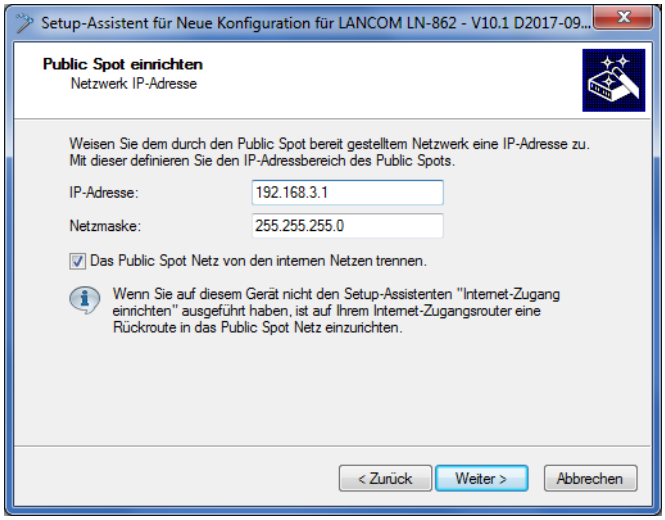


5. Legen Sie fest, ob das Funknetzwerk verschlüsselt werden soll. Geben Sie in diesem Fall einen WLAN-Schlüssel vor oder lassen Sie ihn automatisch generieren.



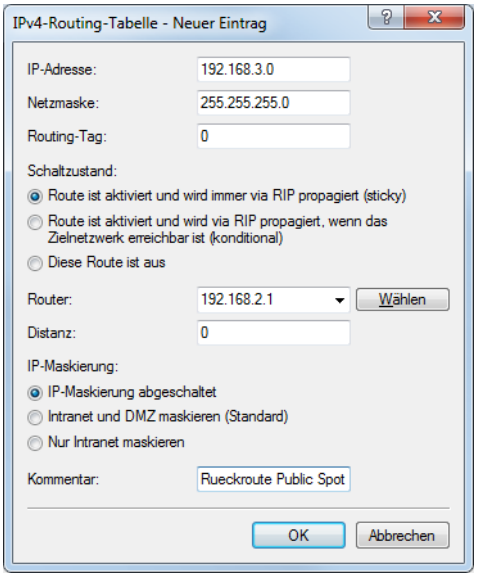
6. Weisen Sie dem Gerät die IP-Adresse und die Netzmaske zu, die Ihr Public Spot-Netzwerk spezifizieren soll, und klicken Sie auf **Weiter**.
   Das Public Spot-Modul enthält in Ihrem Netzwerk eine eigene IP-Adresse, die unabhängig von der Adresse ist, die Sie dem Gerät zugewiesen haben. Haben Sie z. B. ein 192.168.0.0/24-Netzwerk aufgespannt und Ihr Gerät besitzt darin die IP 192.168.2.1, können Sie dem Public Spot-Modul z. B. die IP `192.168.3.1` und die Subnetzmaske `255.255.255.0` vergeben, sofern diese IP nicht anderweitig belegt ist.

Wenn Sie das Public Spot-Netzwerk aus Sicherheitsgründen von den internen Netzwerken trennen möchten, achten Sie darauf, dass die entsprechende Option aktiviert ist.



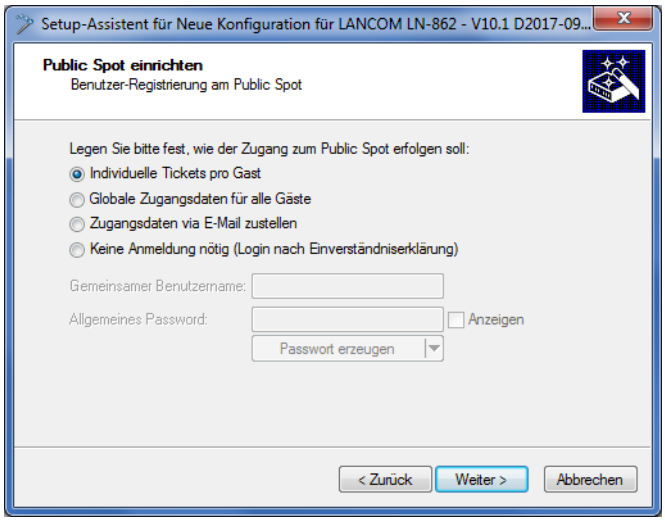
Sofern Ihr Gerät nicht direkt mit dem Internet verbunden ist und Sie für Ihr Public Spot-Netzwerk einen anderen Adresskreis aufgespannt haben, **müssen** Sie in Ihrem Internet-Gateway eine Rückroute in das Public Spot-Netzwerk einrichten. Ohne Rückroute erhalten Public Spot-Nutzer bei der Weiterleitung einen HTTP-Fehler, nachdem sie am Public Spot erfolgreich authentifiziert wurden.

Wie Sie eine Rückroute einrichten, entnehmen Sie bitte der Dokumentation Ihres Internet-Gateways. In LANconfig konfigurieren Sie diese unter **IP-Router** > **Routing** > **IPv4-Routing-Tabelle**. Legen Sie dazu einen neuen Eintrag an und tragen Sie unter **IP-Adresse** die Netzadresse Ihres Public Spot-Netzes ein sowie unter **Router** die Adresse, die der Public Spot in Ihrem lokalen Netz besitzt.

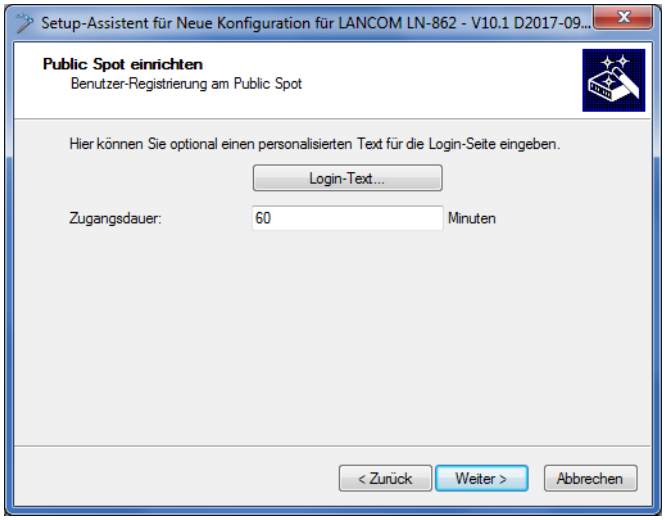


7. Legen Sie fest, mit welchen Zugangsdaten sich Ihre Benutzer am Public Spot anmelden. Außerdem können Sie die Anmeldeseite optional mit einem Login-Text personalisieren. Klicken Sie anschließend auf **Weiter**.

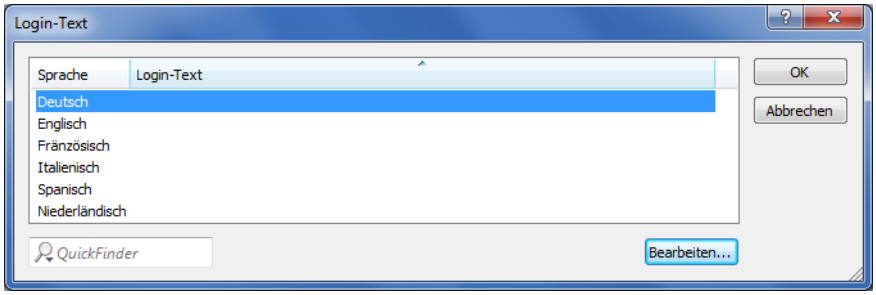
Sie können jedem Benutzer entweder eigene Zugangsdaten aushändigen oder ein allgemeines Konto einrichten, das sämtliche Benutzer für den Zugang zum Public Spot verwenden. Sofern Sie später Voucher ausgeben und feste Benutzerkonten einrichten möchten, wählen Sie die Option **Individuelle Tickets pro Gast**.

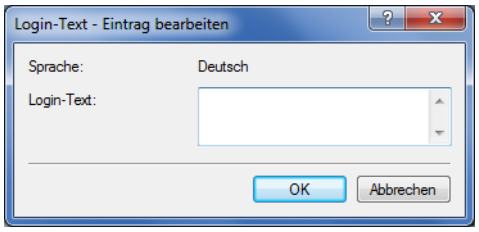


8. Wählen Sie hier optional einen Login-Text, legen Sie die Zugangsdauer fest und klicken Sie **Weiter**.



Login-Text (optional):



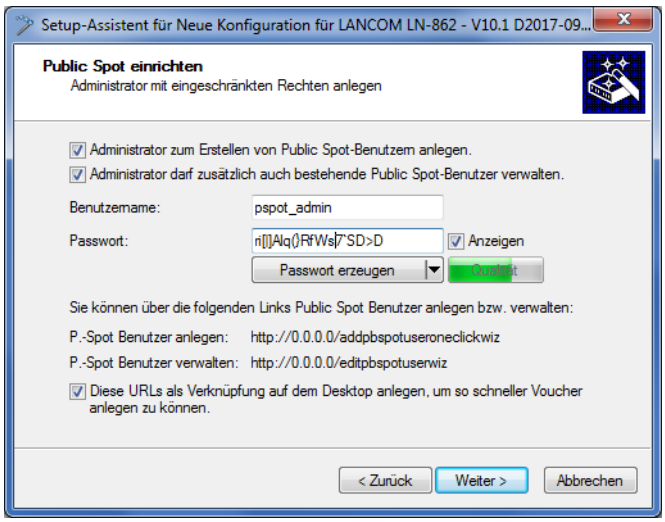


Der Login-Text ist ein individueller Text in HTML-Schreibweise in, welcher auf der Anmeldeseite innerhalb der Box des Anmeldeformulars eingeblendet wird. Sie können diesen Text auch zu einem späteren Zeitpunkt manuell hinzufügen oder ändern (siehe dazu das Kapitel *Individueller Text oder Login-Titel auf der Anmeldeseite* auf Seite 1350).

9. Erstellen Sie ggf. einen Administrator mit beschränkten Rechten, der über die Setup-Wizards in WEBconfig Public Spot-Nutzer erstellen und verwalten darf. Klicken Sie anschließend auf **Weiter**.
   Ein solcher Administrator ist z. B. dann sinnvoll, wenn Sie Ihren Mitarbeitern eine Möglichkeit an die Hand geben wollen, selbstständig Benutzerkonten zu administrieren, ohne, dass ein Geräte-Administrator in den Prozess eingebunden werden muss. Die die Erstellungsrechte aktivieren im WEBconfig den Benutzer-Erstellungs-Assistenten; die Verwaltungsrechte den Benutzer-Verwaltungs-Assistenten.

   Über den Benutzer-Erstellungs-Assistenten **Public-Spot-Benutzer einrichten** hat ein Administrator die Möglichkeit, zeitliche befristete Benutzerkonten für Public Spot-Benutzer zu erstellen und die dazugehörigen Zugangsdaten auf einem Voucher auszudrucken.

   Über den Benutzer-Verwaltungs-Assistenten **Public-Spot-Benutzer verwalten** hat ein Administrator die Möglichkeit, diese Nutzer zu admistrieren. Dabei kann er die Gültigkeit des Zugangs verlängern oder verkürzen, oder das betreffende Nutzerkonto komplett löschen. Zusätzlich kann er über den Assistenten Informationen zum Benutzerkonto abrufen, wie z. B. das vergebene Passwort im Klartext, den Authentifizierungsstatus, die IP-Adresse, die gesendeten/empfangenen Datenmengen oder etwaige Beschränkungen, die für das Konto gelten.

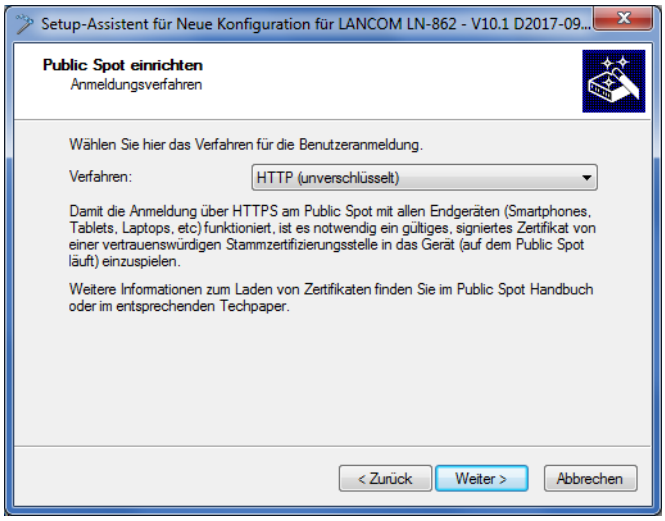


Achten Sie bei der Vergabe eines Passwortes darauf, dass es sicher ist. Der Setup-Assistent prüft während der Eingabe die Qualität des Passwortes. Bei unsicheren Passworten erscheint das Eingabefeld rot, bei erhöhter Sicherheit wechselt es zu gelb, und bei sehr sicheren Passworten erhält es einen grünen Hintergrund.

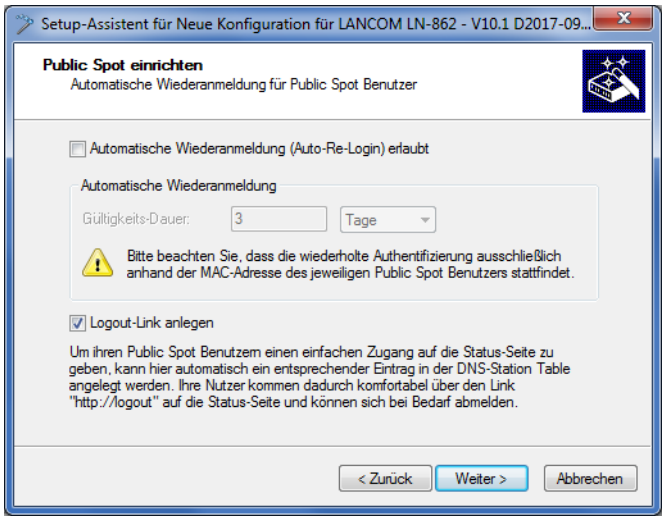
10. Wählen Sie das Verfahren für die Benutzer-Anmeldung. Klicken Sie anschließend auf **Weiter**.

    Sie können in der Drop-Down-Liste zwischen **HTTP** und **HTTPS** wählen, wobei Sie mit einer Verbindung über HTTPS die Sicherheit der Anmeldedaten der Public Spot-Benutzer gewährleisten.

Für die Verwendung von HTTPS sollte anschließend noch ein passendes Server-Zertifikat eingespielt werden. Ansonsten wird dem Benutzer bei der Anmeldung das geräteeigene Zertifikat präsentiert, was im Browser zu einer Zertifikatswarnung führt.

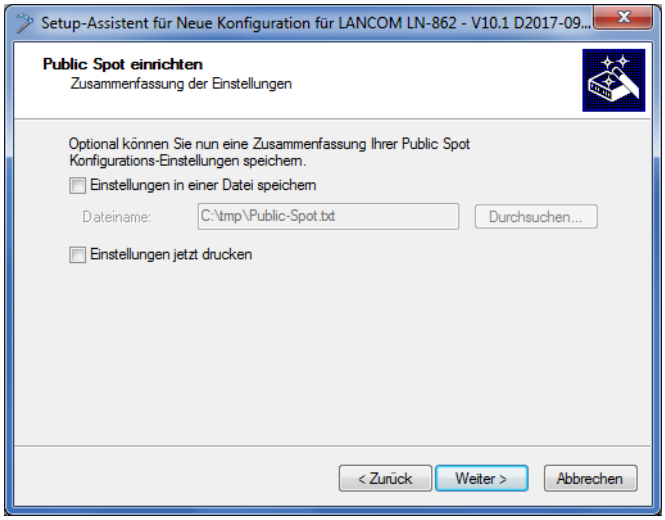


11. Legen Sie fest, ob für sämtliche Public Spot-Nutzer eine automatische Wiederanmeldung erlaubt ist und welche welche maximale Abwesenheit dafür zulässig ist, bevor sich der Nutzer erneut über die Public Spot-Webseite anmelden muss. Klicken Sie anschließend auf **Weiter**.
    Die **Automatische Wiederanmeldung** ist eine Komfort-Option, bei welcher der Public Spot ihm bekannte Nutzer bzw. Geräte automatisch authentifiziert. Da die Erkennung bekannter Geräte jedoch ausschließlich über die MAC-Adresse des Netzwerkadapters erfolgt, welche sich fälschen lässt, stellt dieser Anmeldungsweg ein potentielles Sicherheitsrisiko dar und ist deshalb standardmäßig deaktiviert.



12. Speichern Sie bei Bedarf die vorgenommenen Einstellungen.

Bevor Sie die Konfiguration auf Ihr Gerät übertragen, haben Sie die Möglichkeit, die Einstellungen lokal auf Ihrem PC zu sichern oder eine Zusammenfassung auszudrucken.



13. Klicken Sie abschließend auf **Weiter** und **Fertig stellen**, um die Basis-Installation des Public Spots abzuschließen. Der Setup-Assistent sendet die Einstellungen daraufhin an das Gerät.

Fertig! Damit haben Sie Ihr Public Spot-Modul konfiguriert. Wenn Sie sich nun mit einem WLAN-fähigen Gerät in Reichweite des Public Spots begeben, kann das Gerät die eingerichtete SSID als öffentliches Netzwerk finden und sich an diesem anmelden.

Manuelle Installation

Die nachfolgenden Konfigurationsschritte zeigen Ihnen, wie Sie manuell einen Public Spot für einfache Einsatzszenarien einrichten. Bei dem geschilderten Einsatzszenario aktivieren Sie Public Spot auf einem Interface, über das kein anderer Datenverkehr außer dem des Public Spots läuft; sich z. B. Public Spot- und normale WLAN-Benutzer kein gemeinsames Netzwerk teilen (dedizierte SSID).

Dieses Tutorial stellt nur ein mögliches Beispiel dar. Je nach Geräteart (Access Point, WLAN-Controller, etc.) oder Komplexität der Netzwerkkonfiguration (z. B. Einsatz von VLAN oder ARF) sind abweichende oder zusätzliche Schritte für die Einrichtung eines Public Spots erforderlich! Da derartige Netzwerkkonfigurationen jedoch sehr individuell sind, konzentriert sich das Tutorial bewusst auf ein einfaches Beispiel, damit Sie die notwendigen Schritte bei Bedarf adaptieren können.

1. Starten Sie dazu LANconfig und markieren Sie das Gerät, für das Sie einen Public Spot einrichten wollen, z. B. einen Access Point. Öffnen Sie anschließend den Konfigurationsdialog für das Gerät.
2. Überprüfen Sie die korrekte Uhrzeit.

   Für die Prüfung der Zertifikate und die korrekte Erfassung und Abrechnung der Sitzungsdaten ist die möglichst exakte Uhrzeit im Public Spot wichtig. Bestimmen Sie zunächst Einstellungen wie Zeitzone und Zeitumstellungen (Sommer- und Normalzeit):

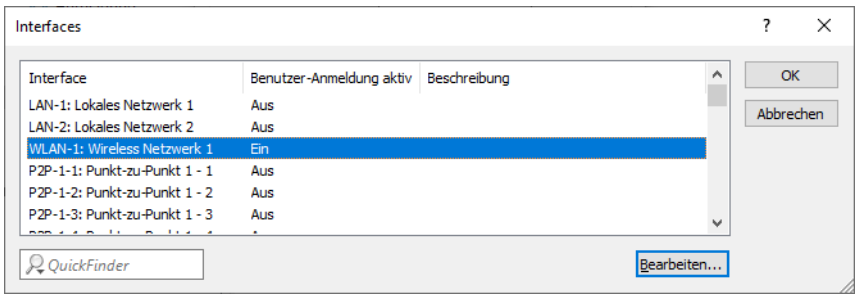
   › LANconfig: **Datum/Zeit** > **Allgemein**

   Damit die Uhrzeit des Public Spots auch später jederzeit korrekt eingestellt bleibt, sollten Sie das Gerät als NTP-Client einrichten. Den dafür notwendigen Zeit-Server tragen Sie unter **Datum/Zeit** > **Synchronisierung** > **Zeit-Server** ein. Öffnen Sie dazu den Hinzufügen-Dialog, um sich eine Liste möglicher Server-Adressen anzeigen zu lassen.
3. Wählen Sie die Schnittstellen für den Public Spot-Betrieb.

   Mit der Auswahl einer Schnittstelle legen Sie fest, auf welchen Schnittstellen die Benutzer-Anmeldung aktiviert wird. Zur Auswahl stehen neben den logischen WLAN-Interfaces, über die sich Public Spot-Benutzer direkt anmelden

können, auch die logischen LAN-Interfaces (LAN-1 etc.) und die Point-to-Point-Strecken (P2P-1 etc.). Über LAN- und P2P-Interfaces können Sie weitere Access-Points in den Public Spot eines anderen Gerätes einbeziehen. Wählen Sie für einen singulären Access-Point hingegen z. B. das logische WLAN-Interface **WLAN-1**.

› LANconfig: **Public-Spot** > **Server** > **Betriebseinstellungen** > **Interfaces**

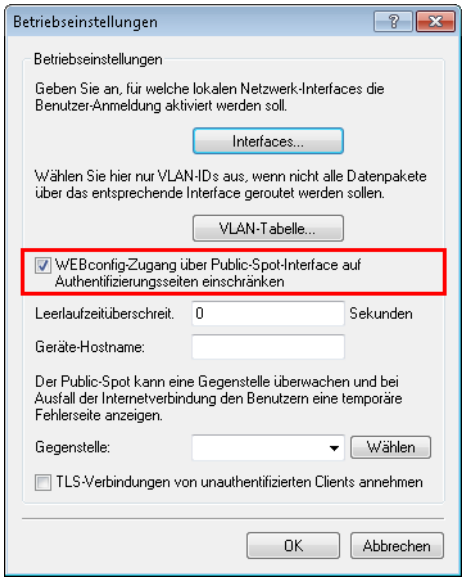


Mit der Aktivierung der Authentifizierung für eine WLAN-Schnittstelle geben Sie automatisch die zugehörige SSID für die Public Spot-Nutzung frei.

Auf einem WLC können Sie bestimmte Ethernet-Interfaces für den Public Spot aktivieren. Dabei können Sie auch eine gezielte Einschränkung auf bestimmte VLANs festlegen.

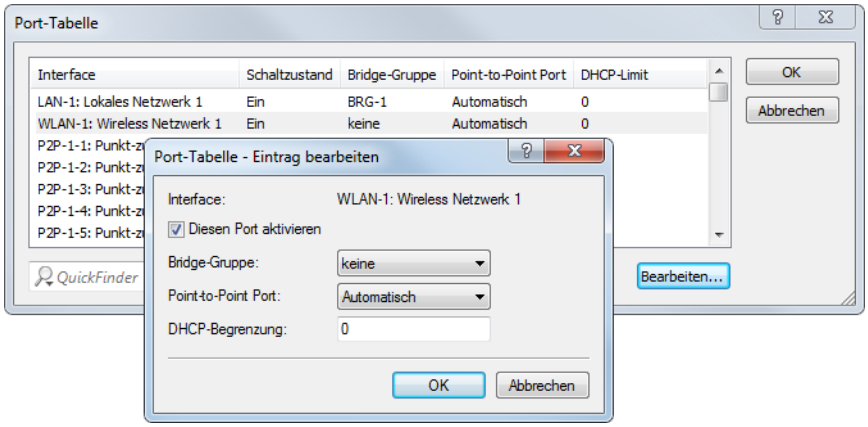
4. Beschränken Sie den Zugriff auf Ihr Gerät aus dem Public Spot-Netzwerk heraus ausschließlich auf die Authentifizierungsseiten.
   Wenn Sie den Zugriff nicht einschränken, sind Public Spot-Nutzer dazu in der Lage, auf die Konfigurationsoberfläche Ihres Gerätes (WEBconfig) zuzugreifen. Aus Sicherheitsgründen sollten Sie diese Möglichkeit jedoch ausschließen.

   › LANconfig: **Public-Spot** > **Server** > **Betriebseinstellungen** > **WEBconfig-Zugang über Public Spot-Interface auf Authentifizierungsseiten einschränken**



5. Trennen Sie die Schnittstelle, über die Sie den Public Spot-Betrieb anbieten wollen, vom übrigen Netzwerkverkehr. Damit Endgeräte über unterschiedliche Interfaces bzw. Schnittstellen eines Public Spot-Gerätes (z. B. zwischen LAN-1 und WLAN-1) miteinander kommunizieren können, sind diese Schnittstellen in Ihrem Gerät logisch miteinander verknüpft (gebridged). In einem Public Spot-Szenario ist solch ein Bridging aus Sicherheitsgründen aber oft nicht erwünscht. Um die Kommunikation zwischen der einem Public Spot zugewiesenen Schnittstelle (z. B. WLAN-1) und dem übrigen Netzwerk zu trennen, müssen Sie das Bridging aufheben. Setzen Sie dazu in der **Port-Tabelle** die **Bridge-Gruppe** für das betreffende Interface auf `keine`.

› LANconfig: **Schnittstellen** > **LAN** > **Port-Tabelle**

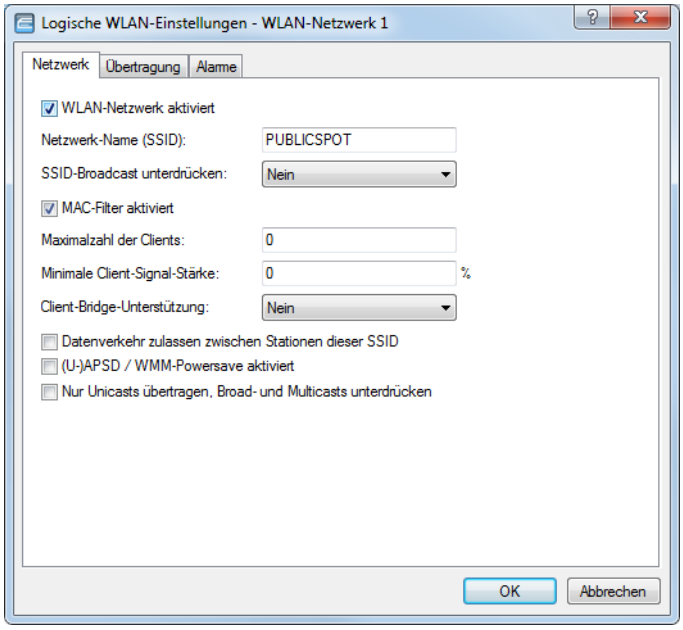


6. Aktivieren Sie WLAN für den Public Spot.

   Diese Einstellung betrifft nicht: Router, WLAN Controller, Central Site Gateways.

   Aktivieren Sie das logische WLAN, welches Sie zuvor für die Public Spot-Anmeldung freigegeben haben, und geben Sie diesem Netzwerk einen aussagekräftigen Namen (SSID).

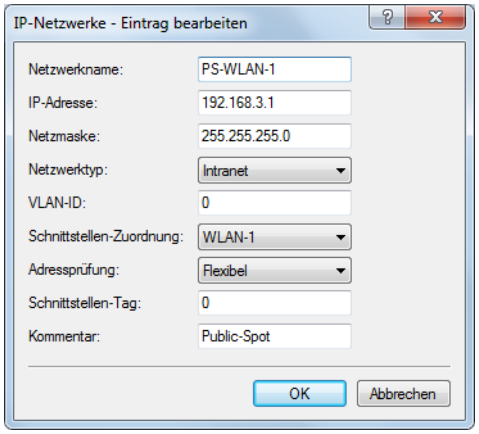
   › LANconfig: **Wireless-LAN** > **Allgemein** > **Logische WLAN-Einstellungen** > **WLAN-Netzwerk <Nummer>** > **Netzwerk**



Sofern Sie kein privates WLAN einrichten, sollten Sie aus Sicherheitsgründen die Einstellung **Datenverkehr zulassen zwischen Stationen dieser SSID** deaktivieren. Dadurch unterbinden Sie die Kommunikation der einzelnen Public Spot-Benutzer untereinander.

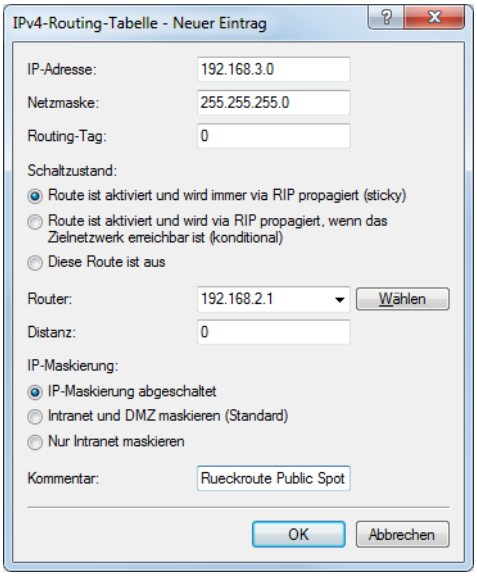
7. Weisen Sie dem Gerät die IP-Adresse und die Netzmaske zu, die Ihr Public Spot-Netzwerk spezifizieren soll.
   Das Public Spot-Modul enthält in Ihrem Netzwerk eine eigene IP-Adresse, die unabhängig von der Adresse ist, die Sie dem Gerät zugewiesen haben. Haben Sie z. B. ein 192.168.0.0/24-Netzwerk aufgespannt und Ihr Gerät besitzt darin die IP 192.168.2.1, können Sie dem Public Spot-Modul z. B. die IP `192.168.3.1` und die Subnetzmaske `255.255.255.0` vergeben, sofern diese IP nicht anderweitig belegt ist. Unter **Schnittstellen-Zuordnung** selektieren Sie die gewählte Schnittstelle, z. B. `WLAN-1`.

› LANconfig: **IPv4** > **Allgemein** > **IP-Netzwerke**



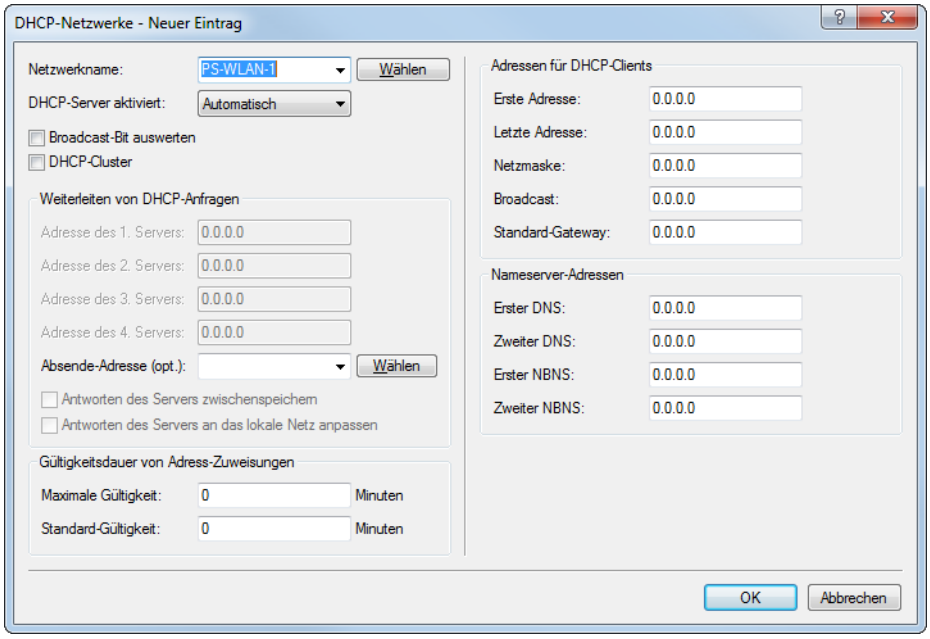
Sofern Ihr Gerät nicht direkt mit dem Internet verbunden ist und Sie für Ihr Public Spot-Netzwerk einen anderen Adresskreis aufgespannt haben, **müssen** Sie in Ihrem Internet-Gateway eine Rückroute in das Public Spot-Netzwerk einrichten. Ohne Rückroute erhalten Public Spot-Nutzer bei der Weiterleitung einen HTTP-Fehler, nachdem sie am Public Spot erfolgreich authentifiziert wurden.

Wie Sie eine Rückroute einrichten, entnehmen Sie bitte der Dokumentation Ihres Internet-Gateways. In LANconfig konfigurieren Sie diese unter **IP-Router** > **Routing** > **IPv4-Routing-Tabelle**. Legen Sie dazu einen neuen Eintrag an und tragen Sie unter **IP-Adresse** die Netzadresse Ihres Public Spot-Netzes ein sowie unter **Router** die Adresse, die der Public Spot in Ihrem lokalen Netz besitzt.



8. Konfigurieren Sie die DHCP-Server-Einstellungen für das Public Spot-Netzwerk.
   Da das Gerät ein IP-Netzwerk unabhängig von dem Netzwerk aufspannt, in dem es sich befindet, müssen Sie für dieses Netzwerk einen DHCP-Server konfigurieren. Setzen Sie dazu für das zuvor eingerichtete IP-Netzwerk (z. B. `PS-WLAN-1`) den Wert für **DHCP-Server aktiviert** auf `Ja`.

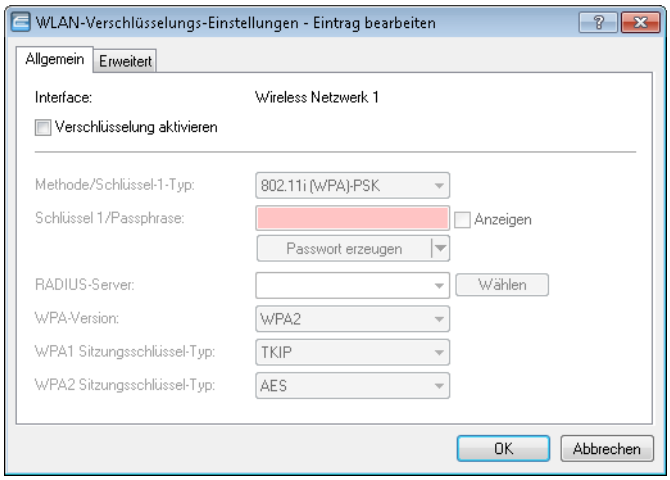
› LANconfig: **IPv4** > **DHCPv4** > **DHCP-Netzwerke**



9. Deaktivieren Sie die Verschlüsselung für das Interface, über das Sie den Public Spot anbieten.

Diese Einstellung betrifft nicht: Router, WLAN Controller, Central Site Gateways.

Standardmäßig ist für alle logischen WLANs eine Verschlüsselung aktiviert. In Public Spot-Anwendungen werden die Nutzdaten zwischen den WLAN-Clients und dem Access Point üblicherweise unverschlüsselt übertragen. Deaktivieren Sie daher unter **Wireless-LAN** > **Verschlüsselung** > **WLAN-Verschlüsselungs-Einstellungen** die Verschlüsselung für das logische WLAN, welches Sie zuvor für die Public Spot-Anmeldung freigegeben haben.

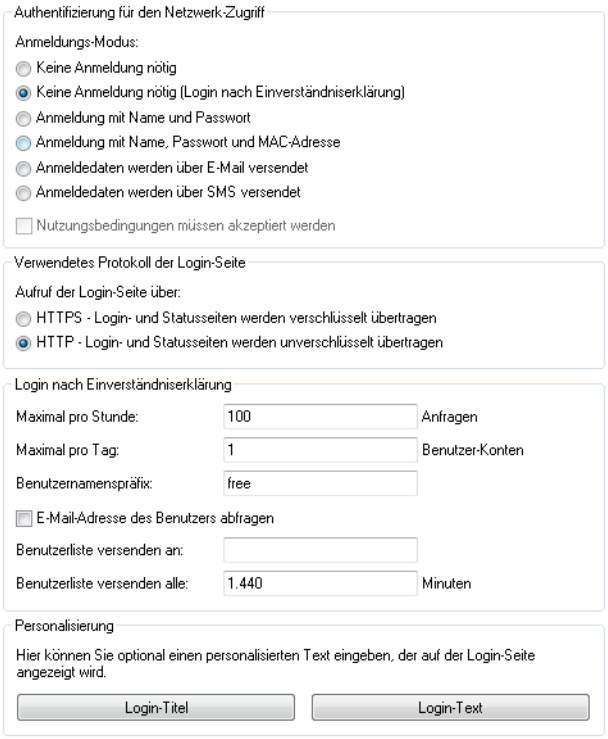


10. Wählen Sie den Anmeldungs-Modus und das verwendete Protokoll für die Benutzeranmeldung aus.

Über den Anmeldungs-Modus legen Sie fest, mit welchen Informationen sich die Benutzer des Public Spot-WLANs anmelden können. Wählen Sie **Anmeldung mit Name und Passwort**, um Ihren Nutzern z. B. die Anmeldung mit einem individuellen Benutzernamen und einem Passwort zu ermöglichen, das Sie diesen vorab zuweisen. Zusätzlich erlaubt Ihnen dieses Einstellung, über sogenannte Voucher (Tickets) kurzfristig Hotspot-Zugänge für Gäste bereitzustellen.

Verwenden Sie als Protokoll **HTTPS**, damit die Zugangsdaten Ihrer Nutzer bei der Anmeldung verschlüsselt übertragen werden.

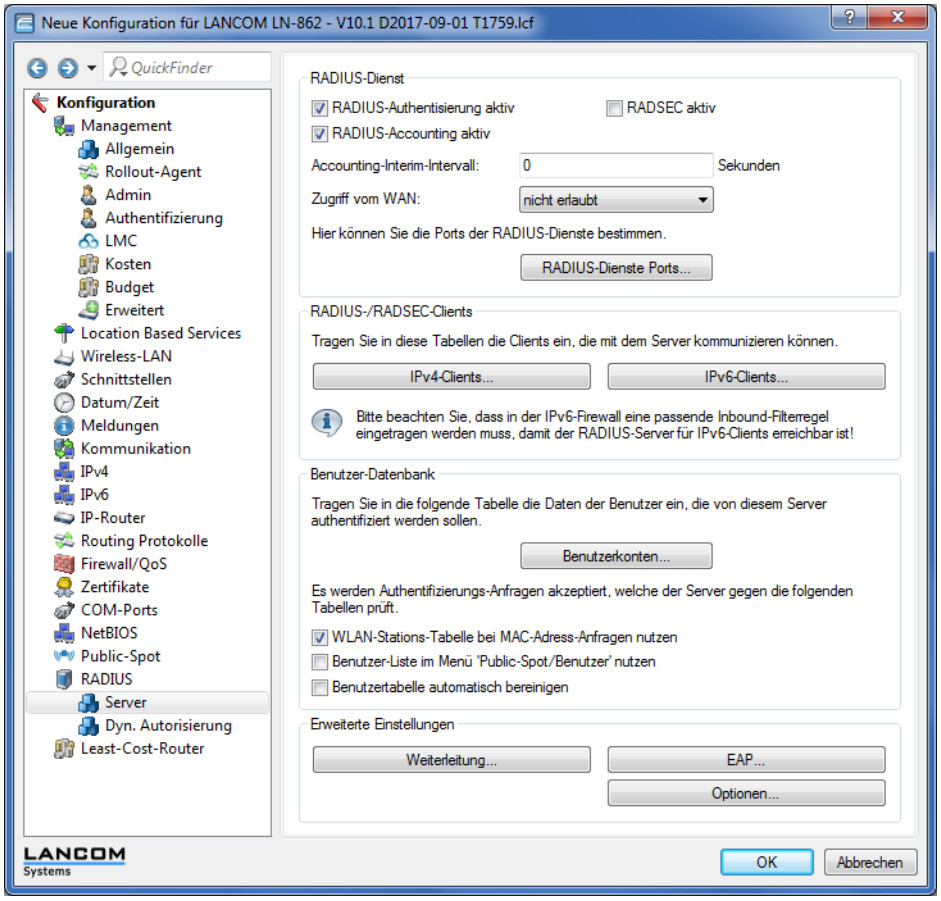
› LANconfig: **Public-Spot** > **Anmeldung** > **Anmeldungs-Modus**



Beachten Sie, dass – wenn Sie die Einstellungen **Keine Anmeldung nötig** wählen –, auch Unbefugte ungehinderten Zugriff auf Ihren Public Spot haben können!

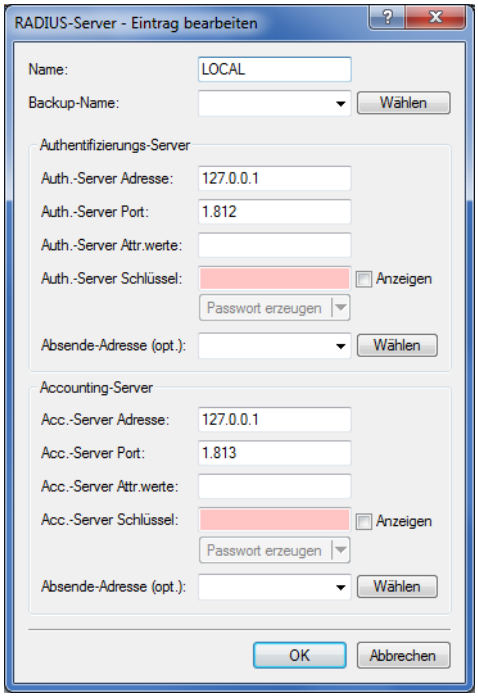
11. Schalten Sie den internen RADIUS-Server für die Benutzerverwaltung und das Accounting ein. Public-Spot-Zugänge speichern Sie in der Benutzer-Datenbank des geräteinternen RADIUS-Servers.

› LANconfig: **RADIUS** > **Server** > **Benutzer-Datenbank**



12. Standardmäßig ist der Public Spot bereits für die Benutzung des internen RADIUS-Servers vorkonfiguriert. Der Listeneintrag ist notwendig, damit der Public Spot die Adresse des RADIUS-Servers kennt und er die Public Spot-Zugänge am internen RADIUS-Server authentifizieren kann.

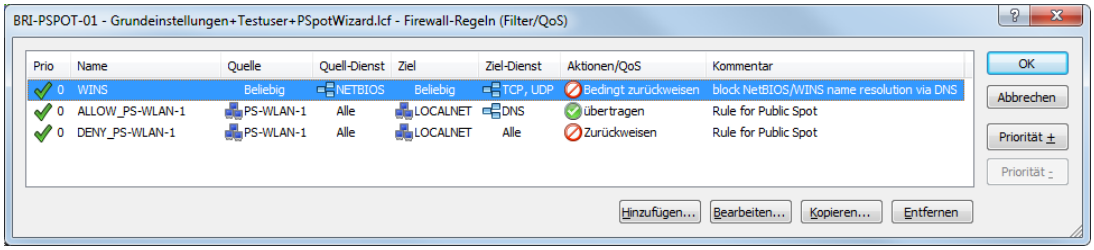
› LANconfig: **Public-Spot** > **Benutzer** > **Benutzer und RADIUS-Server** > **RADIUS-Server**

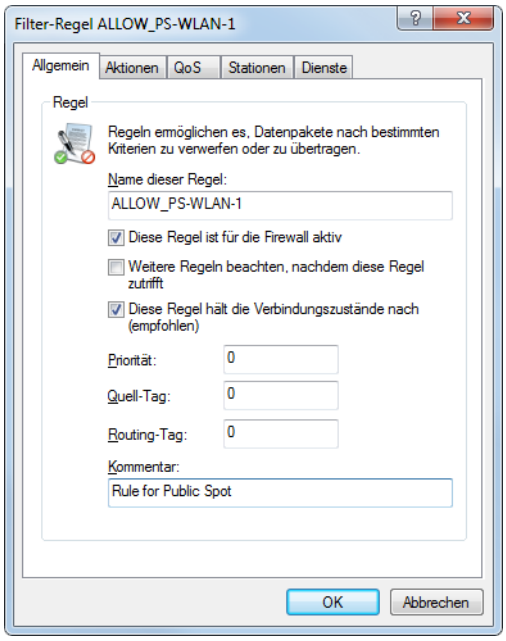


13. Richten Sie zur Absichererung Ihrer lokalen Netzwerke Filterregeln für den Public Spot in der Firewall ein. Erstellen dazu jeweils eine Erlaubnisregel (z. B. `ALLOW_PS-WLAN-1`) und eine Verbotsregel (z. B. `DENY_PS-WLAN-1`).

Über die Erlaubnisregel gestatten Sie Geräten aus dem Public Spot-Netzwerk explizit, DNS-Anfragen in alle lokalen Netzwerke – z. B. Ihr lokales Intranet – zu senden. Über die Verbotsregel hingegen schließen Sie alle übrigen Zugriffe bzw. Anfragen aus dem Public Spot-Netz in Ihre lokalen Netzwerke generell aus. Die Reihenfolge – Erlaubnis vor Verbot – ist dabei essentiell, da die Firewall Regeln nach Priorität von oben nach unten anwendet.

› LANconfig: **Firewall/QoS** > **IPv4-Regeln** > **Regeln…**





› **Einstellungen für die Erlaubnisregel:**

a) Tragen Sie unter **Allgemein** den Namen der Regel ein, z. B. `ALLOW_PS-WLAN-1`.

b) Entfernen Sie alle eventuell voreingestellten Aktions-Objekte aus der Liste und fügen Sie über **Aktionen** > **Hinzufügen…** ein Aktions-Objekt vom Typ **ACCEPT** hinzu.

c) Aktivieren Sie unter **Stationen** > **Verbindungs-Quelle** die Option **Verbindungen von folgenden Stationen** und wählen Sie **Hinzufügen…** > **Benutzerdefinierte Station hinzufügen**.

d) Wählen Sie im sich öffnenden Stations-Dialog die Option **Alle Stationen im lokalen Netzwerk** und wählen Sie unter **Netzwerk-Name** den Namen Ihres Public Spot-IP-Netzwerks, z. B. `PS-WLAN-1`. Schließen Sie den Stations-Dialog mit **OK**.

e) Aktivieren Sie unter **Stationen** > **Verbindungs-Ziel** die Option **Verbindungen an folgende Stationen** und wählen Sie **Hinzufügen…** den Eintrag **LOCALNET**.

f) Aktivieren Sie unter **Dienste** > **Protokolle/Ziel-Dienste** die Option **folgende Protokolle/Ziel-Dienste** und wählen Sie **Hinzufügen…** > **DNS**.

g) Beenden Sie den Filter-Regel-Dialog mit einem abschließenden Klick auf **OK**.
LANconfig trägt die Erlaubnisregel daraufhin in die Regel-Tabelle ein.

› **Einstellungen für die Verbotsregel:**

a) Tragen Sie unter **Allgemein** den Namen der Regel ein, z. B. `DENY_PS-WLAN-1`.

b) Entfernen Sie alle eventuell voreingestellten Aktions-Objekte aus der Liste und fügen Sie über **Aktionen** > **Hinzufügen…** ein Aktions-Objekt vom Typ **REJECT** hinzu.

c) Aktivieren Sie unter **Stationen** > **Verbindungs-Quelle** die Option **Verbindungen von folgenden Stationen** und wählen Sie **Hinzufügen…** > **Benutzerdefinierte Station hinzufügen**.

d) Wählen Sie im sich öffnenden Stations-Dialog die Option **Alle Stationen im lokalen Netzwerk** und wählen Sie unter **Netzwerk-Name** den Namen Ihres Public Spot-IP-Netzwerks, z. B. `PS-WLAN-1`. Schließen Sie den Stations-Dialog mit **OK**.

e) Aktivieren Sie unter **Stationen** > **Verbindungs-Ziel** die Option **Verbindungen an folgende Stationen** und wählen Sie **Hinzufügen…** den Eintrag **LOCALNET**.

f) Beenden Sie den Filter-Regel-Dialog mit einem abschließenden Klick auf **OK**.
LANconfig trägt die Verbotsregel daraufhin in die Regel-Tabelle ein.

14. Speichern Sie die Konfiguation auf Ihrem Gerät.

Fertig! Damit haben Sie Ihr Public Spot-Modul konfiguriert. Wenn Sie sich nun mit einem WLAN-fähigen Gerät in Reichweite des Public Spots begeben, kann das Gerät die eingerichtete SSID als öffentliches Netzwerk finden und sich an diesem anmelden.

15.2.1.2 Standardwerte für den Public Spot-Assistenten setzen

Der nachfolgende Abschnitt beschreibt, wie Sie die Standardwerte für den **Benutzer-Erstellungs-Assistenten** (Setup-Wizard **Public-Spot-Benutzer einrichten**) an Ihre Bedürfnisse anpassen. Die hier definierten Werte stehen einem Public Spot-Administrator beim Einrichten neuer Benutzer und Voucher-Druck anschließend als Auswahlwerte zur Verfügung (Laufzeiten, Bandbreitenprofile, etc.).

Ausgenommen davon sind die im untenstehenden Dialog abgebildeten Werte für Muster für Benutzernamen und Passwort-Länge, welche ausschließlich dem Gerät als Vorgabewerte dienen.

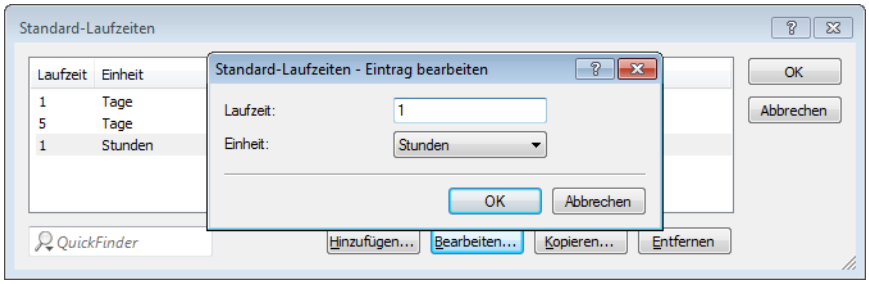
1. Starten Sie LANconfig und öffnen Sie den Konfigurationsdialog für das Gerät.

2. Wechseln Sie in die Ansicht **Public-Spot** > **Assistent**.

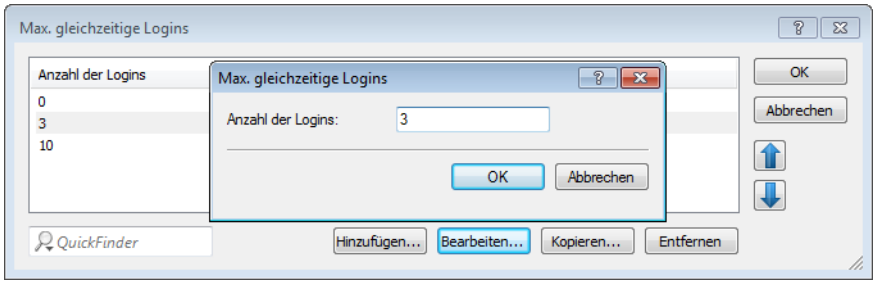


3. Definieren Sie unter **Standard-Laufzeiten**, welche auswählbaren Gültigkeiten von Benutzerkonten und Vouchern der Assistent standardmäßig anbietet.

Der Benutzer-Erstellungs-Assistent verwendet die kürzeste Laufzeit als Standardwert.



4. Definieren Sie unter **Max. gleichzeitige Logins** die für den jeweiligen Benutzer zutreffende Anzal von Geräten, die maximal gleichzeitig auf das Benutzerkonto zugreifen dürfen.
   Der Wert `0` steht dabei für 'Unbegrenzt'. Ob die mehrfache Anmeldung mit einem oder mehreren Geräten generell erlaubt ist, gibt der Public Spot-Administrator später beim Anlegen eines neues Benutzers über eine gesonderte Einstellung im Assistenten an.

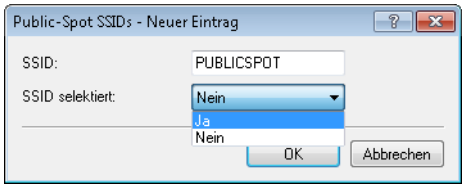


5. Legen Sie unter **Muster für Benutzernamen** fest, nach welchem Muster der Benutzer-Erstellungs-Assistent den Benutzernamen erzeugt.
   Sie können bis zu 19 Zeichen vergeben, wobei der Assistent für die Variable "`%n`" für jeden Benutzer eine eindeutige Nummer vergibt. Für die Standardbezeichnung `user%n` erscheint auf dem Voucher später z. B. `user12345`.

6. Bestimmen Sie unter **Passwort-Länge** die Länge des Passwortes, das der Benutzer-Erstellungs-Assistent für den Public Spot-Zugang generiert.
   Standardmäßig beträgt die Länge 6 Zeichen. Wenn Sie längere Passwörter vergeben möchten, sollten Sie bedenken, dass dem Gast bei deren Eingabe Fehler passieren können, was zu unnötigen Problemen und Rückfragen führt.

7. Optional: Legen Sie unter **Bandbreitenprofile** Grenzen für den Up- und Downlink eines jeden Public Spot-Benutzers fest.
   Mehr zu dieser Einstellung erfahren Sie unter *Bandbreitenprofile verwalten* auf Seite 1296.

8. Nur Public Spot über WLAN: Bestimmen Sie unter **Public-Spot SSIDs** die Namen der Public Spot-Netzwerke, für die Sie mit dem Benutzer-Erstellungs-Assistent Benutzerkonten standardmäßig anlegen.



Der Benutzer-Erstellungs-Assistent markiert die als **SSID selektiert** festgelegten Netzwerknamen bei der Einrichtung neuer Public Spot-Benutzer automatisch vor. Sofern Sie beispielsweise einen Access Point oder WLAN Controller einsetzen, können Sie mehrere Netzwerknamen als Vorgabewert auswählen, um den Benutzern standardmäßig den Zugang zu mehreren WLANs zu bereitzustellen. Beim Erstellen eines neuen Benutzers und dem anschließenden Voucher-Druck erscheinen diese SSIDs ebenfalls auf dem ausgedruckten Ticket.

Über die Pfeil-Schaltflächen ändern Sie die Reihenfolge der angezeigten SSIDs. Oft genutzte SSIDs können Sie damit z. B. an die oberen Positionen verschieben.

Fertig! Damit ist die Konfiguration der Standardwerte für den Public Spot-Assistenten abgeschlossen.

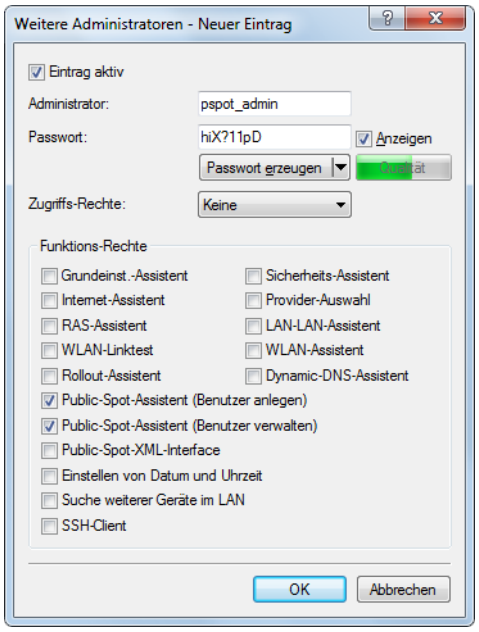
15.2.1.3 Beschränkten Administrator zur Public Spot-Verwaltung einrichten

Um Mitarbeitern auch ohne Zugriff auf die Gerätekonfiguration die Einrichtung und Verwaltung von Benutzern zu erlauben, haben Sie die Möglichkeit, einen beschränkten Administrator einzurichten, welcher ausschließlich über die Rechte zur Verwendung der *Public Spot-Assistenten* verfügt. Dieses Tutorial beschreibt die dafür erforderlichen Schritte sowie die notwendigen Zugriffs- und Funktionsrechte in LANconfig.

Da die Rechte zur Verwendung der Public Spot-Assistenten getrennt von einander konfigurierbar sind, lässt sich ein beschränkter Administrator auch auf einen einzelnen Assistenten einschränken. Im Falle des Benutzer-Erstellungs-Assistenten leitet das Gerät den beschränkten Administrator nach dem WEBconfig-Login dann automatisch an die entsprechende Eingabemaske weiter.

1. Öffnen Sie in LANconfig den Konfigurationsdialog des Gerätes, für das Sie einen Public Spot-Administrator hinzufügen wollen.
   In diesem Gerät muss das Public Spot-Modul aktiviert sein.
2. Wechseln Sie in die Ansicht **Management** > **Admin**. Klicken Sie im Abschnitt **Geräte-Konfiguration** auf **Weitere Administratoren** und klicken Sie anschließend **Hinzufügen**.

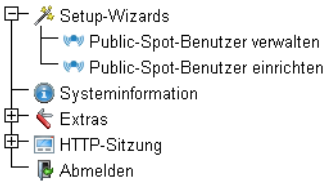
   Wenn Sie einem vorhandenen Administrator die Public Spot-Verwaltung zuweisen möchten, markieren Sie dessen Tabelleneintrag und klicken stattdessen **Bearbeiten**.



3. Aktivieren Sie das Profil, indem Sie die Option **Eintrag aktiv** markieren.
4. Vergeben Sie einen aussagekräftigen Namen im Feld **Administrator**.
5. Bestimmen Sie ein **Passwort** und wiederholen Sie es zur Kontrolle.
6. Setzen Sie die **Zugriffs-Rechte** auf **Keine**.
7. Aktivieren Sie im Abschnitt **Funktions-Rechte** die Optionen **Public-Spot-Assistent (Benutzer anlegen)** für den Benutzer-Erstellungs-Assistenten und **Public-Spot-Assistent (Benutzer verwalten)** für den Benutzer-Verwaltungs-Assistenten.

   Das Funktionsrecht **Public-Spot-XML-Interface** wird von einem Public Spot-Administrator nicht benötigt. Das Recht ist nur relevant, wenn Sie das XML-Interface verwenden und sollte auch dann aus Sicherheitsgründen nicht mit den oben beschriebenen Funktionsrechten kombiniert werden.
8. Speichern Sie das erstellte oder geänderte Administratorprofil mit einem Klick auf **OK**.

Sofern Sie die Funktions-Rechte für mehrere Assistenten gesetzt haben, kann der beschränkte Administrator in WEBconfig über die Navigationsleiste zwischen den Assistenten navigieren.



Sofern Sie ausschließlich das Funktionsrecht **Public-Spot-Assistent (Benutzer anlegen)** gesetzt haben, kann ein beschränkter Administrator lediglich innerhalb des Benutzer-Erstellungs-Assistenten navigieren; die Navigationsleiste bleibt verborgen. Ein manuelles Abmelden über WEBconfig ist in diesem Fall nicht mehr möglich. Aus Sicherheitsgründen ist die Lebensdauer der WEBconfig-Sitzung daher sehr kurz gehalten. Bei entsprechender Inaktivität loggt das Gerät den beschränkten Administrator automatisch aus.

Aus technischen Gründen kann sich der Benutzer-Erstellungs-Assistent nach Verwenden der Schaltfläche **User anlegen und CSV-Export** nicht automatisch aktualisieren. Möchte ein beschränkter Administrator weitere Benutzer einrichten und Voucher ausdrucken, muss er den Assistenten neu aufrufen (z. B. via URL oder Aktualisieren der Webseite, wenn die Navigationsleiste verborgen ist).

15.2.1.4 Public-Spot-Benutzer für einfache Szenarien einrichten und verwalten

Sie haben die Möglichkeit, Public Spot-Benutzer sowohl von Hand als auch mit Hilfe der Setup-Wizards einzurichten und zu verwalten. Die Einrichtung und Verwaltung von Hand bietet Ihnen umfassendere Konfigurationsmöglichkeiten und erlaubt Ihnen z. B. das Anlegen selbstdefinierter Benutzer von unbegrenzter Lebensdauer.

Über die Setup-Wizards hingegen erstellen Sie generische Public Spot-Benutzer mit automatisch generierten Zugangsdaten von beschränkter Lebensdauer. Der betreffende Setup-Wizard ist ausschließlich über WEBconfig zugänglich, was Ihnen das schnelle Anlegen von Nutzern erlaubt, ohne dass dafür allgemeine Administrationsrechte für das komplette Gerät erforderlich sind. Es wird lediglich ein Administrator mit beschränkten Rechten benötigt.

Es steht Ihnen natürlich auch frei, mit Hilfe des Setup-Wizards zunächst einen generischen Nutzer zu erzeugen und diesen dann manuell Ihren Bedürfnissen (z. B. Änderung des Benutzernamens) entsprechend anzupassen.

Einrichtung und Verwaltung über die Setup-Wizards (WEBconfig)

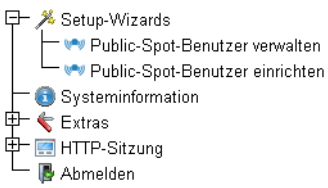
Die Setup-Wizards unterstützen Sie bei der einfachen Verwaltung von Public Spot-Benutzern.

Public-Spot-Benutzer mit einem Klick hinzufügen und Voucher-Druck

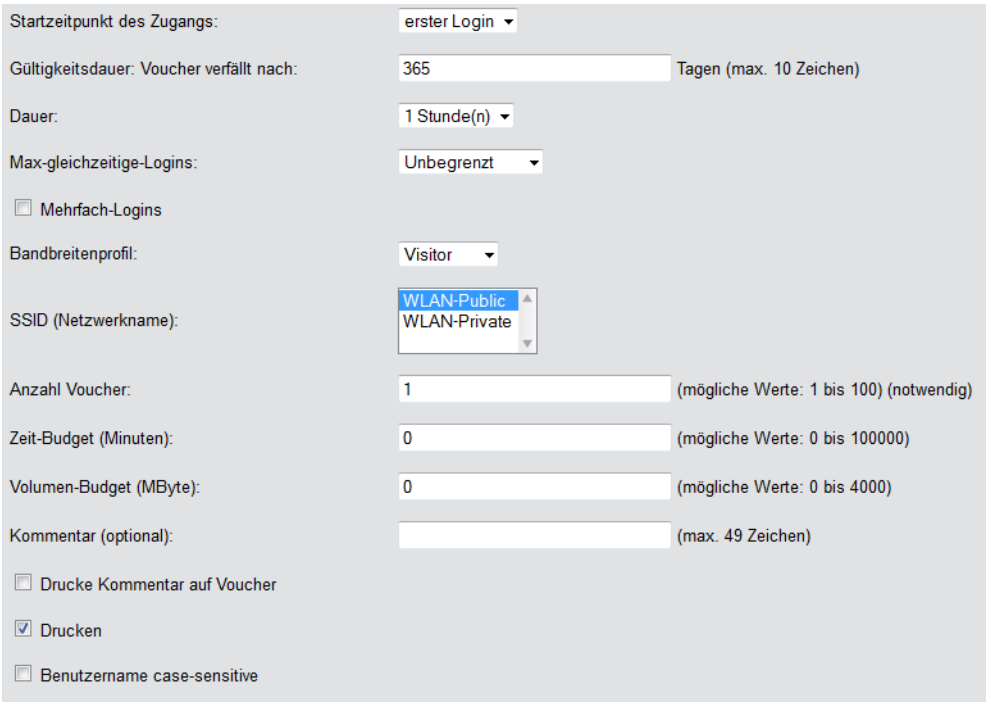
Der folgende Abschnitt beschreibt die Einrichtung eines Public Spot-Benutzers über WEBconfig und den anschließenden Ausdruck des Vouchers. Sie können Voucher dabei auch auf Vorrat anlegen.

Sie benötigen das Zugriffsrecht **Public-Spot-Assistent (Benutzer anlegen)**, um einen neuen Public Spot-Benutzer anzulegen.

1. Melden Sie sich auf der Startseite von WEBconfig als Public Spot-Administrator an.
2. Starten Sie den Setup-Assistenten mit einem Klick auf **Setup-Wizards** > **Public-Spot-Benutzer einrichten**.



3. Der Benutzer-Erstellungs-Assistent startet mit der Eingabemaske. Die Felder sind mit Standardwerten vorbelegt.



Der Assistent vergibt daraufhin automatisch einen Nutzernamen und ein Zugangs-Passwort. Im anschließenden Druck-Dialog können Sie den Voucher-Drucker auswählen und den Voucher ausdrucken.

4. Ändern Sie ggf. vor dem Druck die Standardwerte den Anforderungen entsprechend.

   Die folgenden Einträge beeinflussen sowohl Aussehen als auch Gültigkeit des Vouchers:

   - **Startzeitpunkt des Zugangs**: Legt fest, ab wann der Voucher gültig ist. In der Einstellung **erster Login** gilt der Zugang ab Erstanmeldung; in der Einstellung **sofort** ab Anlegen des Benutzers.

     Um mehrere Vouchers auf Vorrat anzulegen, wählen Sie hier als Gültigkeit des Vouchers `erster Login`. Somit stellen Sie sicher, dass die Vouchers auch nach längerer Vorhaltezeit ihre Gültigkeit behalten.
   - **Gültigkeitsdauer: Voucher verfällt nach**: Geben Sie die Dauer an, nach der der Voucher ungültig wird. Es ist nicht möglich, eine Gültigkeitsdauer einzutragen, wenn der Zugang ab sofort gültig ist.
   - **Dauer**: Wählen Sie die Dauer aus, für die dieser Zugang ab Erstanmeldung oder Anlegen des Benutzers gültig ist. Die hier aufgelisteten Einträge verwalten Sie in der **Default-Laufzeit**-Tabelle.
   - **Max-gleichzeitige-Logins**: Wählen Sie hier die für den jeweiligen Benutzer zutreffende Anzal von Geräten aus, die maximal gleichzeitig auf das Benutzerkonto zugreifen dürfen. Die hier aufgelisteten Einträge verwalten Sie in der **Max-gleichzeitige-Logins-Tabelle**.
   - **Mehrfach-Logins**: Aktivieren Sie diese Option, um dem Benutzer die Anmeldung mehrerer Geräte mit den selben Zugangsdaten generell zu erlauben. Die erlaubte Menge der gleichzeitig angemeldeten Geräte legen Sie über die Auswahlliste **Max-gleichzeitige-Logins** fest.
   - **Bandbreitenprofil**: Wählen Sie aus der Liste ein Bandbreitenprofil, um die dem Nutzer zur Verfügung gestellte Bandbreite (Uplink und Downlink) selektiv zu beschränken. Banbreitenprofile legen Sie in der **Bandbreitenprofile**-Tabelle an.
   - **SSID (Netzwerkname)**: Geben Sie an, für welches WLAN-Netz der Zugang gilt. Die hier aufgelisteten SSIDs verwalten Sie in der **SSID-Tabelle**. Durch drücken der "Strg"-Taste haben Sie die Möglichkeit, mehrere Einträge auszuwählen. Standardeinträge sind bereits vormarkiert.

     Sofern Sie in der Tabelle keinen Eintrag definiert haben, blendet der Assistent diese Einstellungsmöglichkeit aus.

- **Anzahl Voucher**: Geben Sie an, wie viele Vouchers Sie gleichzeitig erstellen möchten. Wenn Sie den ersten Login als Startzeitpunkt des Zugangs festgelegt haben, können Sie hierüber mehrere Vouchers "auf Vorrat" ausdrucken.
- **Zeit-Budget (Minuten)**: Geben Sie an, nach welcher Online-Zeit der Public Spot-Zugang schließt. Je nach gewählter Ablauf-Methode bestimmt entweder dieses Zeit-Budget (inkrementell) oder die eingestellte Voucher-Zugangsdauer (absolut) die Frist für den Zugang.
- **Volumen-Budget (MByte)**: Geben Sie an, nach welcher übertragenen Datenmenge der Zugang schließt.
- **Kommentar (optional)**: Fügen Sie einen Kommentar ein. Dieser Kommentar kann zum Beispiel weitere Hinweise zur Zugangsdauer oder die Telefonnummer der Rezeption bei Zugangsproblemen beinhalten.
- **Drucke Kommentar auf Voucher**: Aktivieren Sie diese Option, damit der Kommentar auf dem Voucher erscheint.
- **Drucken:** Aktivieren Sie diese Option, damit Sie beim Speichern gleichzeitig die registrierten Vouchers ausdrucken.
- **Benutzername case-sensitive**: Aktivieren Sie diese Option, wenn der Public Spot-Nutzer bei der Anmeldung auf die Groß- und Kleinschreibung seines Benutzernamens achten muss.

5. Wenn Sie die Default-Werte unverändert oder die neuen Werte übernehmen möchten, klicken Sie abschließend auf **Speichern und Drucken**.

   Wenn Sie die Option **Drucken** deaktiviert haben, zeigt Ihnen der Assistent nach der Registrierung eine Übersicht der neuen Public Spot-Benutzer. Sie erhalten dann noch einmal die Gelegenheit, die Vouchers auszudrucken.

   Über die Schaltfläche **Benutzerverwaltung aufrufen** gelangen Sie zum Setup-Wizard **Public-Spot-Benutzer verwalten**.



Diese Schaltfläche können Sie wahlweise anzeigen lassen oder ausblenden. Als Default ist sie eingeblendet.

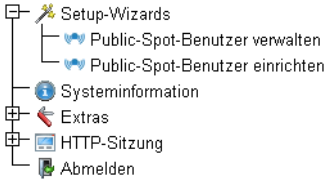
Assistent zum Verwalten von Public Spot-Benutzern

Der folgende Abschnitt beschreibt die Verwaltung von registrierten Public Spot-Benutzern über WEBconfig.

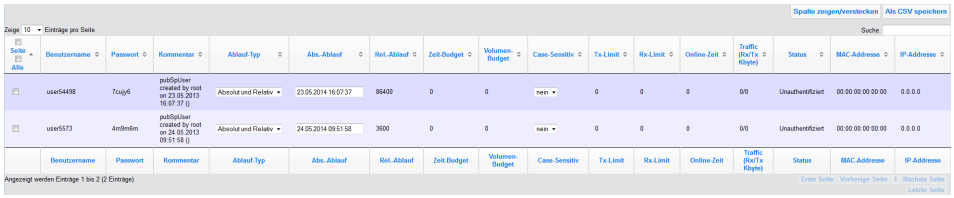
Sie benötigen das Zugriffsrecht **Public-Spot-Assistent (Benutzer verwalten)**, um Public Spot-Benutzer verwalten zu können.

Ungespeicherte Änderungen gehen verloren, sobald Sie diesen Assistenten beenden.

1. Melden Sie sich auf der Startseite von WEBconfig als Public Spot-Administrator an.
2. Starten Sie den Setup-Assistenten mit einem Klick auf **Setup-Wizards** > **Public-Spot-Benutzer verwalten**.



3. Der Public Spot-Assistent startet mit einer Liste der registrierten Public Spot-Benutzer.



In der Auswahlliste **Zeige ... Einträge pro Seite** stellen Sie die Anzahl angezeigter Einträge pro Seite ein. Die entsprechenden Seiten rufen Sie über die Seitennavigation rechts unten auf:

- **Erste Seite**: Zeigt die Seite mit den ersten Einträgen an.
- **Vorherige Seite**: Wechselt eine Seite zurück.
- **Seitennummern (1, 2, 3,...)**: Wechselt direkt zur gewählten Seite.
- **Nächste Seite**: Wechselt eine Seite weiter.
- **Letzte Seite**: Zeigt die Seite mit den letzten Einträgen an.

Über **Suche** filtern Sie die angezeigten Einträge. Der Filter führt eingegebene Zeichenfolgen sofort aus.

Markierte Einträge exportieren Sie über **Als CSV speichern**.

Die Tabellenspalten haben folgende Bedeutungen:

- **Seite/Alle**: In dieser Spalte markieren Sie den Benutzer für die gewünschte Aktion (Drucken, Löschen, Speichern). Um alle Einträge der aktuellen Seite auszuwählen, markieren Sie **Seite**. Um alle Einträge komplett auszuwählen, markieren Sie **Alle**.
- **Benutzername**: Zeigt den manuell oder automatisch vom System vergebenen Benutzernamen an.
- **Passwort**: Zeigt das manuell oder vom System vergebene Passwort an.
- **Kommentar**: Beinhaltet sowohl den bei der Registrierung angegebenen Kommentar (in Klammern) sowie Änderungen an den Benutzer-Daten (automatisch vom System dokumentiert).
- **Ablauf-Typ**: Zeigt an, ob die Gültigkeitsdauer dieses Benutzer-Accounts absolut (fester Zeitpunkt) oder relativ (Zeitspanne ab dem ersten erfolgreichen Login) festgelegt ist.
- **Abs.-Ablauf**: Wenn der Ablauf-Typ "Absolut" aktiviert ist, endet die Gültigkeit dieses Benutzer-Accounts zu dem in diesem Feld angegebenen Zeitpunkt.
- **Rel.-Ablauf**: Wenn der Ablauf-Typ "Relativ" aktiviert ist, endet die Gültigkeit dieses Benutzer-Accounts nach der in diesem Feld angegebenen Zeitspanne nach dem ersten erfolgreichen Login des Benutzers.
- **Zeit-Budget**: Gibt die maximale Nutzungsdauer für diesen Benutzer-Account an. Diese Nutzungsdauer kann der Benutzer bis zum Erreichen einer ggf. definierten relativen oder absoluten Ablaufzeit ausschöpfen.
- **Volumen-Budget**: Gibt das maximale Datenvolumen für diesen Benutzer-Account an. Dieses Datenvolumen kann der Benutzer bis zum Erreichen einer ggf. definierten relativen oder absoluten Ablaufzeit ausschöpfen.
- **Case-Sensitiv**: Gibt an, ob die Anmeldeseite die Groß- und Kleinschreibung des jeweiligen Benutzernamen berücksichtigt.
- **Tx-Limit**: Sofern beim Erstellen des Benutzers ein Bandbreitenprofil vergeben wurde, zeigt dieser Eintrag die maximale Sende-Bandbreite an, die dem Benutzer zur Verfügung steht.
- **Rx-Limit**: Sofern beim Erstellen des Benutzers ein Bandbreitenprofil vergeben wurde, zeigt dieser Eintrag die maximale Empfangs-Bandbreite an, die dem Benutzer zur Verfügung steht.
- **Traffic (Rx/Tx Kbyte)**: Zeigt die Datenmenge in Kilobyte an, die der betreffende Benutzer bisher empfangen (Rx) bzw. gesendet (Tx) hat.
- **Status**: Zeigt den Authentifizierungsstatus der einzelnen Benutzer an, also ob der Benutzer derzeit am Public Spot angemeldet ist (**Authentifiziert**) oder nicht (**Unauthentifiziert**).
- **MAC-Addresse**: Zeigt die physikalische Adresse der Netzwerkkarte des Benutzers, mit der Nutzer derzeit verbunden ist.
- **IP-Addresse**: Zeigt die IPv4-Adresse, die das System dem Benutzer derzeit zugewiesen hat.

Die Schaltflächen am unteren Fensterrand besitzen folgende Funktionen:

- **Drucken**: Drucken Sie die Vouchers der markierten Benutzer aus.
- **Löschen**: Löschen Sie die markierten Benutzer.
- **Speichern**: Speichern Sie die Änderungen.
- **Zurück zur Hauptseite**: Wechseln Sie zur Hauptseite zurück, wobei alle ungespeicherten Änderungen verloren gehen.

Folgende Angaben eines Benutzers passen Sie an, indem Sie die Inhalte der entsprechenden Felder ändern:

- **Ablauf-Typ**
- **Abs.-Ablauf**
- **Rel.-Ablauf**
- **Case-Sensitiv**

4. Markieren Sie den zu ändernden Benutzer in der ersten Spalte.
5. Ändern Sie die entsprechenden Feldinhalte, und klicken Sie auf **Speichern**, um diese Änderungen zu übernehmen. Ungespeicherte Änderungen gehen verloren, sobald Sie diesen Assistenten verlassen.
6. Wenn Sie einen Benutzer löschen möchten, markieren Sie den entsprechenden Eintrag in der ersten Spalte, und klicken Sie auf **Löschen**

Die Löschung eines Eintrags erfolgt ohne vorherige Rückfrage.

Felder mit WEBconfig ausblenden

Im Setup-Assistenten "Public-Spot-Benutzer verwalten" haben Sie über die Schaltfläche **Spalte zeigen/verstecken** die Möglichkeit, Tabellenspalten ein- oder auszublenden. Diese Änderungen sind jedoch nur temporär. Nach einem Seiten-Refresh oder bei einer neuen Sitzung werden die ausgeblendeten Spalten wieder angezeigt.

Um bestimmte Felder dauerhaft zu verbergen, wechseln Sie im LCOS-Menübaum zur Ansicht **Setup** > **Public-Spot-Modul** > **Verwalte-Benutzer-Assistent**. Standardmäßig werden alle Felder angezeigt. Blenden Sie bestimmte Felder aus, um z. B. das Zeit-Budget zu verbergen, bleiben diese Spalten sowohl im Assistenten selbst als auch im Dropdown-Menü unter der Schaltfläche **Spalte zeigen/verstecken** nach einem erneuten Aufrufen der Seite verborgen.

Um einen authentisierten Public Spot-Benutzer zu löschen, müssen die Spalten "Rufende-Station-Id-Maske" und "Gerufene-Station-Id-Maske" im Assistenten sichtbar sein. Nicht authentisierte Benutzer hingegen lassen sich auch löschen, wenn beide Spalten ausgeblendet sind.

Beachten Sie bitte, dass ausgeblendete Felder beim Betätigen der Schaltfläche **Drucken** nicht mit ausgegeben werden. Die Ausgabe als CSV-Datei beinhaltet dagegen alle Daten. Sie haben jedoch die Möglichkeit, die Schaltfläche **Als CSV speichern** zu verbergen. Wechseln Sie dazu im LCOS-Menübaum zur Ansicht **Setup** > **Public-Spot-Modul** > **Neuer-Benutzer-Assistent** > **CSV-Export-verstecken**. Wählen Sie "Ja" und speichern Sie Ihre Eingabe.

Manuelle Einrichtung und Verwaltung

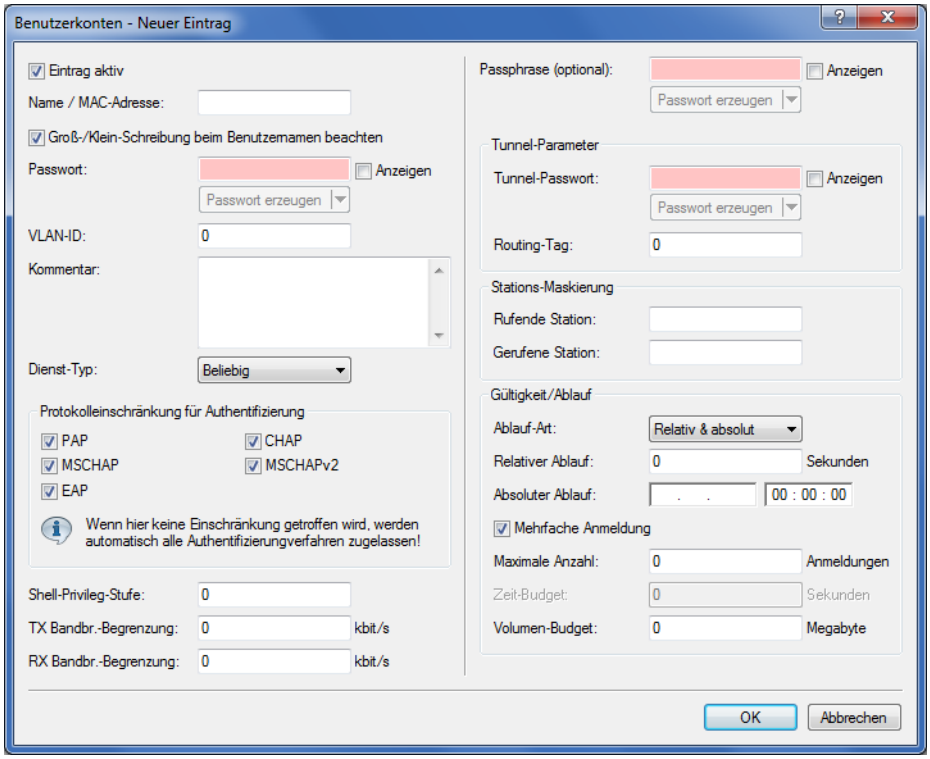
Die nachfolgenden Konfigurationsschritte zeigen Ihnen, wie Sie in LANconfig manuell einen Public Spot-Benutzer für einfache Einsatzszenarien einrichten. Public Spot-Nutzer erstellen und verwalten Sie über die **Benutzer-Datenbank** des geräteinternen RADIUS-Servers, erreichbar unter **RADIUS** > **Server** > **Benutzer-Datenbank**. Hier tragen Sie – aber auch die Setup-Wizards – alle Benutzer ein, die einen Zugang zum Public Spot erhalten sollen.

Das Public Spot-Modul verfügt für die Benutzerverwaltung noch über eine eigene, interne Liste (erreichbar unter **Public-Spot** > **Benutzer** > **Benutzer-Liste**). Im Zuge der technischen Entwicklung ist diese Liste seit LCOS 7.70 durch die Benutzerverwaltung via RADIUS ablöst. Aus Kompatibilitätsgründen wertet das Gerät die interne Benutzer-Liste des Public Spot-Moduls weiterhin aus, sofern Sie dies aktivieren. Für neue Installationen sollten Sie diese Liste jedoch nicht mehr verwenden, da Ihnen sonst zahlreiche Features nicht zur Verfügung stehen (Einrichtung und Verwaltung über die Assistenten, Bandbreiten-Begrenzung, Accounting via RADIUS, VLAN-IDs für Public Spot-Nutzer etc.).

1. Geben Sie unter **Name** den Benutzernamen des zukünftigen Nutzers oder die **MAC-Adresse** seines Endgerätes ein.

   Wenn Sie als Authentifizierungs-Modus **Anmeldung mit Name und Passwort** gewählt haben, tragen Sie hier die Kennung ein, mit welcher sich der Nutzer am Public Spot authentisiert. Die Vergabe eines **Passworts** ist optional, ist für den obigen Authentifizierungs-Modus jedoch zu empfehlen.

   › LANconfig: **RADIUS** > **Server** > **Benutzer-Datenbank** > **Benutzerkonten**



   Sofern die Authentifizierung zusätzlich über die MAC-Adresse erfolgt (Authentifizierungs-Modus **Anmeldung mit Name, Passwort und MAC-Adresse**), definieren Sie die MAC-Adresse über das Feld **Rufende Station** in der Form `12:34:56:78:90:AB`.

2. Setzten Sie den **Dienst-Typ** auf `Anmeldung`.

3. Heben Sie sämtliche Protokolleinschränkungen auf, indem Sie alle Auswahlkästchen deselektieren.
   In einem Public Spot-Szenario findet eine Phase-2-Authentifizierung nicht statt. Diese kann lediglich für direkte WLAN-Verbindungen abseits eines Public Spot-Betriebs und die dazugehörigen RADIUS-Benutzer sinnvoll sein.

   Wenn Sie die Protokolleinschränkungen nicht komplett aufheben, kann sich ein Nutzer nicht über die Login-Webseite Ihres Public Spots anmelden!

4. Optional: Auf Wunsch können Sie z. B. noch

   › im Abschnitt **Gültigkeit/Ablauf** ein relatives oder/und absolutes Ablaufdatum für die Gültigkeit des Benutzerkontos angeben (relativ = Gültigkeit in Sekunden nach erstem Login);
   › unter **TX/RX Bandbr.-Begrenzung Bandbreite** den Uplink/Downlink begrenzen;
   › die **Mehrfache Anmeldung** aktivieren und die **Maximale Anzahl** der Endgeräte angeben, die gleichzeitig über das Benutzerkonto angemeldet sein dürfen.

5. Speichern Sie die Konfiguation auf Ihrem Gerät.

Fertig! Ihre Public Spot-Nutzer können sich nun mit den von Ihnen festgelegten Zugangsdaten am Public Spot anmelden.

15.2.2 Sicherheitseinstellungen

Der Public Spot verfügt über zwei zusätzliche Schutzmechanismen, die ihn wirksam gegen Missbrauch absichern.

15.2.2.1 Traffic-Limit-Option

Um die Anmeldung am Public Spot über den Browser zu ermöglichen, ist es prinzipiell gestattet, dass auch unangemeldete Benutzer Datenpakete (z. B. DNS-Anfragen) an das Public Spot-Gerät senden. In der Standardeinstellung ist diese Datenmenge unbegrenzt. Daraus ergeben sich folgende Risiken:

- **Unberechtigte Nutzung des Public-Spots:** Mit geeigneten Tools könnte ein Benutzer alle Daten in ein DNS-Paket verpacken (also einen DNS-Tunnel aufbauen) und so einen Public Spot ohne Anmeldung nutzen.
- **Denial-of-Service:** Der Angreifer könnte erhebliche Datenmengen an das angegriffene Gerät senden und auf diese Weise versuchen, das Gerät bzw. den Public Spot zu blockieren.
- **Brute-Force:** Der Angreifer könnte versuchen, Zugang zur Basis-Station zu erhalten, indem er einfach so lange alle denkbaren Anmeldedaten durchprobiert, bis ihm der Zugang schließlich gelingt.

Die Traffic-Limit-Option ermöglicht, diese Risiken wirksam auszuschließen.

Sie aktivieren die Traffic-Limit-Option durch einen Wert ungleich "0". Der Wert bestimmt die maximale Datenmenge in Byte, die eine unangemeldetes Endgerät an den Public Spot senden und von ihm empfangen darf.

- LANconfig: **Public-Spot** > **Server** > **Zugriff ohne Anmeldung ermöglichen** > **Maximales Datenvolumen**

Sobald ein Endgerät dieses Transfervolumen überschreitet, sperrt der Public Sport dieses Gerät und verwirft fortan die von ihm empfangenen Daten ungeprüft. Diese Sperre erlischt erst wieder, wenn der zum Gerät gehörige Eintrag in der Stationstabelle verschwindet.

Bei WLAN-Geräten kann diese Löschung z. B. durch den Ablauf des allgemeinen Idle-Timeouts geschehen:

- WEBconfig: **Extras** > **LCOS-Menübaum** > **Setup** > **WLAN** > **Idle-Timeout**

Bitte beachten Sie, dass bei eingeschalteter Stationsüberwachung die Sperre möglicherweise auch schon früher entfernt wird. Ist eine Mobilstation 60 Sekunden lang unerreichbar, entfernt das Gerät dessen Eintrag aus der Stationstabelle und damit auch die Sperre.

Die Leerlaufzeitüberschreitung für das Public Spot-Modul erfüllt den gleichen Zweck wie der Idle-Timeout für WLAN, beschränkt sich allein auf Verbindungen über Public Spot. Ist die Leerlaufzeitüberschreitung gesetzt und kommen von einem Benutzer keine Datenpakete mehr, loggt das Gerät diesen nach Ablauf der eingetragenen Zeit automatisch aus.

- LANconfig: **Public-Spot** > **Server** > **Leerlaufzeitüberschreitung**

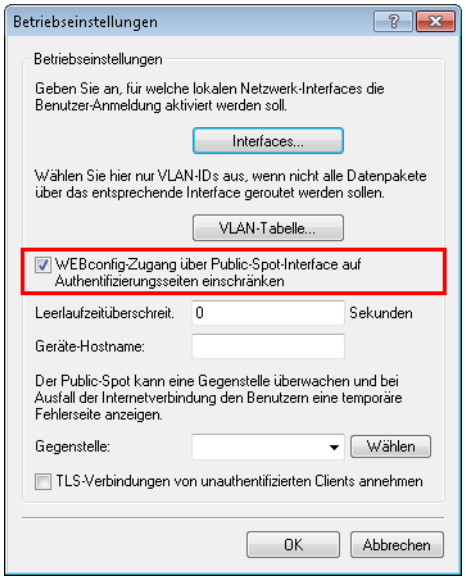
Der optimale Wert des Traffic-Limits hängt zum einen von der Datengröße der Anmeldeseite ab. Zum anderen wirkt sich dieser Wert maßgeblich auf die mögliche Anzahl erfolgloser Anmeldeversuche durch einen Benutzer aus. Im Regelfall bewirkt ein Traffic-Limit von 60.000 Bytes den wirksamen Schutz des Public-Spots, lässt aber gleichzeitig eine ausreichende Anzahl von Anmeldeversuchen zu. Bei Bedarf können Sie diesen Wert den individuellen Bedürfnissen anpassen. Der Default-Wert von "0" Bytes steht für ein unbegrenztes Datenvolumen.

Die Traffic-Limit-Option überwacht ausschließlich den Datenverkehr vor der Anmeldung. Sie berücksichtigt nicht den Datenverkehr von und zu einem ggf. eingerichteten, freien Web-Server. Dieser bleibt zu jeder Zeit unlimitiert.

15.2.2.2 Konfigurationszugriff einschränken

Der Zugriff aus einem Public Spot-Netzwerk auf die Konfiguration eines Public Spots (WEBconfig) sollte aus Sicherheitsgründen immer ausgeschlossen sein. Mit einem speziellen Schalter besteht die Möglichkeit, den Zugang über Public Spot-Interfaces auf die Public Spot-Authentisierungsseiten zu reduzieren und automatisch alle anderen Konfigurationsprotokolle zu sperren.

- LANconfig: **Public-Spot** > **Server** > **Betriebseinstellungen** > **WEBconfig-Zugang über Public Spot-Interface auf Authentifizierungsseiten einschränken**



Bitte beachten Sie, dass Sie über die Zugriffsrechte unter **Management** > **Admin** > **Konfigurations-Zugriffs-Wege** > **Zugriffs-Rechte** nicht generell den Zugriff über HTTP(S) auf das Gerät einschränken.

15.2.3 Erweiterte Funktionen und Einstellungen

Der Public Spot beinhaltet zahlreiche erweiterte Funktionen, Optionen und Parameter, mit denen Sie ihn individuell an die spezifischen Eigenarten seines Einsatzgebietes anpassen können.

In den folgenden Abschnitten finden Sie Informationen über:

- Multiple Anmeldungen

  Standardmäßig ist die Nutzung von Zugangsdaten auf die Anmeldung mit einem Gerät beschränkt. Erfahren Sie, wie Sie diese Limit heraufsetzen oder die Beschränkung für ein Benutzerkonto komplett aufheben.

- Anmeldungsfreie Netze

  Richten Sie zusätzliche Netze ein, die ein Public Spot-Benutzer auch ohne Anmeldung am Public Spot erreichen kann, um um ihn online mit zusätzlichen Informationen (z. B. Kundenwebseite in einem Unternehmen, Veranstaltungskalender in einem Hotel) zu versorgen.

- Benutzerverwaltung über das Web-API

  Nutzen Sie URLs, um Public Spot-Benutzer über Datei-Verknüpfungen oder Skripte zu anzulegen und zu verwalten.

- Individuelle Begrenzung der Bandbreite

  Begrenzen Sie für jeden Public Spot-Nutzer individuell den ihm zugewiesenen Up- und Downlink.

- Automatische Bereinigung von Benutzerkonten und Mobilstationen

  Nutzen Sie die geräteeigenen Funktionen, um abgelaufene Public Spot-Benutzerkonten und nicht ordnungsgemäß abgemeldetete Mobilstationen (nur WLAN) automatisch aus den geräteinternen Datenbanken zu entfernen.

- Übergabe von WLAN-Sitzungen zwischen Geräten

  Erfahren Sie mehr über die Roaming-Möglichkeiten von Mobilstationen zwischen einzelnen Access Points, und welche besonderen Konfigurationen notwendig sind, um Ihren Benutzern die unterbrechungsfreie Übergabe von WLAN-Sitzungen zu ermöglichen.

- Authentifizierung über RADIUS

Erfahren Sie, wie Sie ein mehrere RADIUS-Server für Authentifizierung und Accounting bereitstellen, und wie Sie Server sinnvoll miteinander verketten, um im Falle der Unerreichbarkeit einzelner Systeme die Nutzerdaten an entsprechende Backup-Systeme weiterzuleiten.

- Abrechnung von Public Spot-Verbindungen im kommerziellen Betrieb

  Erfahren Sie mehr über die Abrechnungsfunktionen, die Ihnen der Public Spot für den kommerziellen Betrieb bereitstellt. Diese Abrechnungsfunktionen lassen sich grob in zwei Modelle unterteilen:

  - Bezahlung tatsächlich genutzter Ressourcen im Nachhinein (Kredit-Abrechnung)
  - Benutzung des Services auf Guthabenbasis (Debit-Abrechnung, PrePaid)

- Verwenden mehrstufiger Zertifikate

  Erfahren Sie, wie Sie SSL-Zertifikatsketten in Ihr Gerät laden.

- Individuelle Zuweisung von VLAN-IDs

  Erfahren Sie, wie Sie einzelnen Public Spot-Nutzern individuelle VLAN-IDs zuweisen.

15.2.3.1 Mehrfach-Logins

Sie haben die Möglichkeit, Public Spot-Benutzern zu gestatten, sich mit mehreren Geräten gleichzeitig auf ein Benutzerkonto einzuloggen. Dies kann dann erforderlich sein, wenn eine Gruppe von zusammengehörigen Personen (z. B. eine Familie) mehrere Geräte besitzt und diese zur gleichen Zeit für den Zugang ins Netz nutzen möchte.

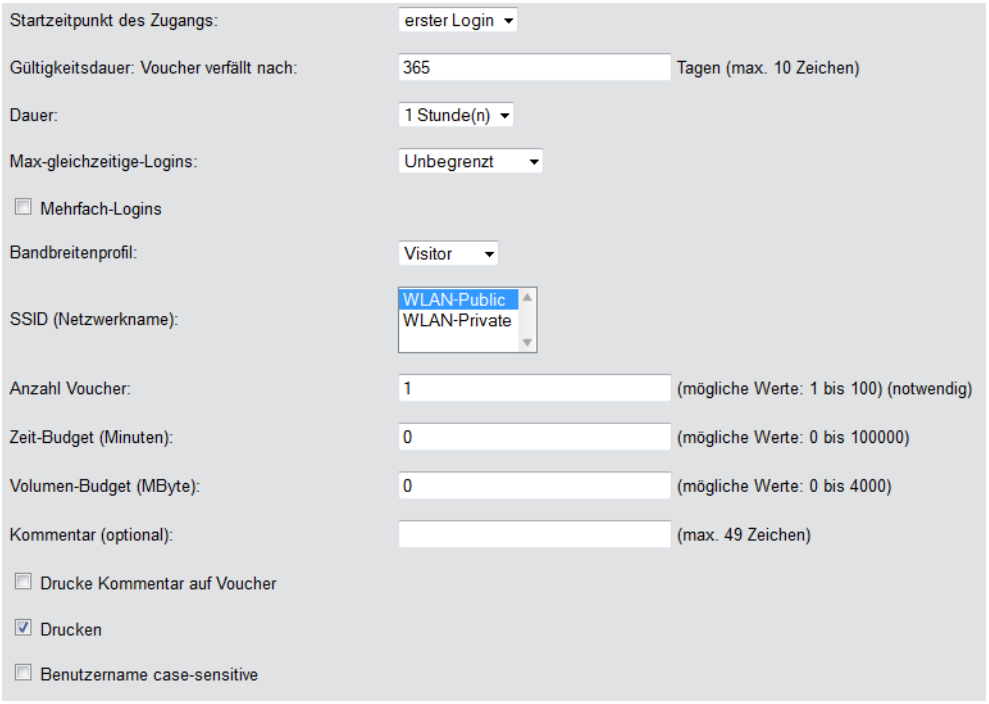
Standardwerte festlegen

Um diese Funktion zu verwenden, definieren Sie im ersten Schritt die mögliche Anzahl der gleichzeitig nutzbaren Geräte im Setup-Menü unter **Public-Spot-Modul** > **Neuer-Benutzer-Assistent** > **Max-gleichzeitige-Logins-Tabelle**. Hier tragen Sie jene Werte ein, die Sie im zweiten Schritt mit Hilfe des Assistenten **Public-Spot-Benutzer einrichten** zuweisen. Der Wert `0` steht dabei für "Unbegrenzt".

Auswahl der Mehrfach-Logins im Benutzer-Erstellungs-Assistenten

Wenn Sie den Assistenten **Public-Spot-Benutzer einrichten** aufrufen, finden Sie das Auswahlmenü **Max-gleichzeitige-Logins** vor. Die hier angezeigten Werte entsprechen den Zahlen, die Sie zuvor in der analog benannten Tabelle festgelegt haben. Die Zahlen werden innerhalb der Phrase "Nur...Gerät(e)" wiedergegeben.

Wählen Sie hier die für den jeweiligen Benutzer zutreffende Anzal von Geräten aus, die maximal gleichzeitig auf das Benutzerkonto zugreifen dürfen. Beachten Sie, dass für die Aktivierung der Funktion zusätzlich noch die Option **Mehrfach-Logins** ausgewählt sein muss.



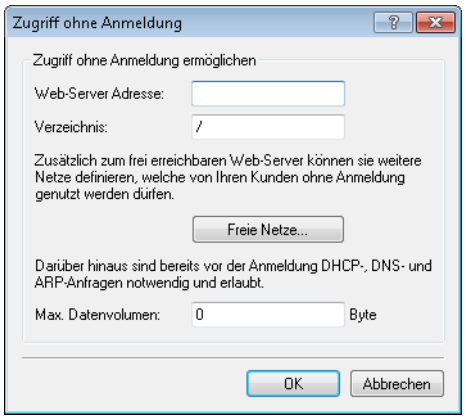
15.2.3.2 Anmeldungsfreie Netze

Um den Benutzern den Zugang zu wichtigen Informationen auch ohne Anmeldung zu ermöglichen (z. B. wichtige Kontaktinformationen), können Sie einen frei erreichbaren Web-Server definieren.

› LANconfig: **Public-Spot** > **Server** > **Zugriff ohne Anmeldung**

Falls Sie den hier definierten Server nicht vollständig freigegeben wollen, können Sie optional einen abweichenden Pfad auf dem Web-Server angeben:

› LANconfig: **Public-Spot** > **Server** > **Zugriff ohne Anmeldung** > **Verzeichnis**

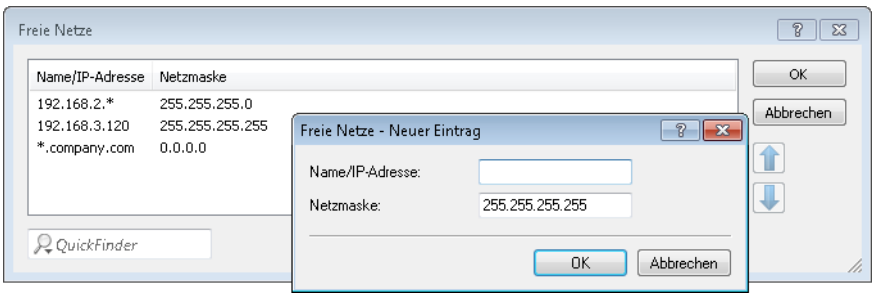


Zusätzlich zum frei erreichbaren Web-Server können Sie weitere Netze und Spezial-Seiten definieren, welche von Ihren Kunden ohne Anmeldung genutzt werden dürfen.

› **Public-Spot** > **Server** > **Zugriff ohne Anmeldung** > **Freie Netze**

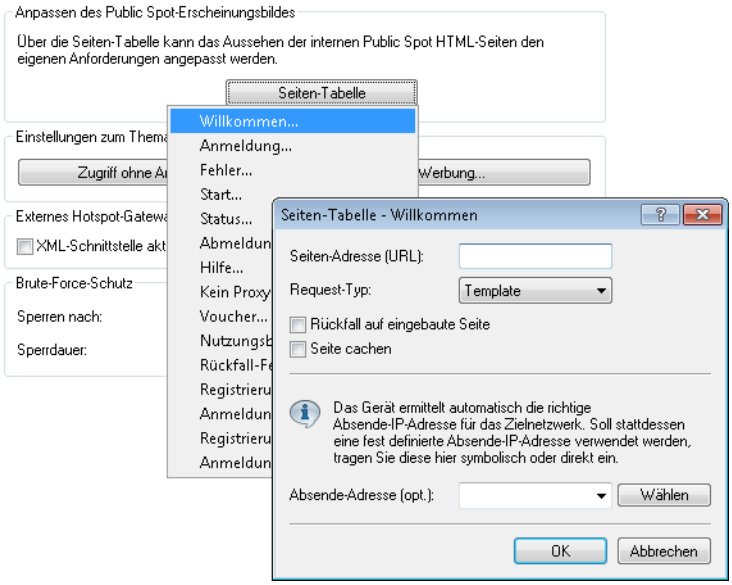
Tragen Sie die IP-Adresse des zusätzlichen Servers oder Netzwerks inklusive Netzmaske ein, auf welche die Public Spot-Benutzer zugreifen dürfen. Alternativ haben Sie auch die Möglichkeit, Domain-Namen (mit oder ohne Wildcard "*") einzutragen. Durch Wildcards können Sie z. B. auch den freien Zugriff auf alle Subdomains einer Domäne erlauben. Der Eintrag `*.company.com` gibt somit auch die Adressen `mail.company.com`, `service.company.com` etc. frei.

Wenn Sie nur eine einzelne Station mit der zuvor benannten Adresse oder eine Domain freischalten wollen, geben Sie als Netzmaske `255.255.255.255` ein. Wenn Sie ein ganzes IP-Netz freigeben wollen, geben Sie dafür die zugehörige Netzmaske an. Sofern Sie keine Netzmaske setzen (Wert `0.0.0.0`), ignoriert das Gerät den betreffenden Tabelleneintrag.



› **Public-Spot** > **Server** > **Seiten-Tabelle**

Tragen Sie die Adressen (URL) der Webseiten ein, die der Public Spot dem Benutzer für die Anmeldung, Fehlermeldungen, Status usw. anzeigen soll. Lesen Sie dazu auch das Kapitel über *geräteeigene und individuelle Authentifizierungsseiten*.



DNS-Snooping

Webdienste mit hohen Nutzerzahlen verteilen die Datenanfragen zur besseren Auslastung auf mehrere Server. So kommt es, dass zwei DNS-Anfragen für denselben Hostnamen (z. B. "www.google.de") zu zwei unterschiedlichen IP-Adressen führen können. Erhält der Public Spot für einen eingegebenen Hostnamen vom zuständigen DNS-Server nun mehrere gültige IP-Adressen, wählt er davon eine aus und speichert sie für zukünftige Anfragen von Public Spot-Benutzern. Bekommt der Benutzer jedoch bei einer weiteren Anfrage für denselben Hostnamen die IP-Adresse eines anderen Servers zugeteilt, sperrt der Public Spot diese Verbindung, weil er diese IP-Adresse nicht als zugangsberechtigt gespeichert hat.

Damit Public Spot-Benutzer sich trotz wechselnder IP-Adressen mit dem angefragten Host verbinden können, analysiert der Public Spot die DNS-Anfragen der Benutzer und speichert die jeweils zurückgegebene IP-Adresse zusammen mit dem Hostnamen, der Gültigkeitsdauer (TTL: "Time to Live"), dem Alter und der Datenquelle fortan als freie Zieladresse in der Tabelle **Status** > **Public-Spot** > **Freie-Hosts**.

Die Einträge in dieser Tabelle verfallen nach der in der DNS-Antwort übertragenen Gültigkeitsdauer (TTL). Um bei sehr niedrigen Werten (z. B. 5 Sekunden) den Public Spot-Benutzer nicht sofort nach einer Anfrage wieder auszusperren, können Sie unter **Setup** > **Public-Spot-Modul** > **Freie-Hosts-Minimal-TTL** eine Mindest-Gültigkeitsdauer festlegen.

15.2.3.3 Verwaltung von Public Spot-Nutzern über das Web-API

Über die Eingabe einer speziellen URL in der Adresszeile haben Sie die Möglichkeit, Public Spot-Benutzer direkt statt über den Setup-Assistenten anzuzeigen, neu anzulegen oder zu löschen.

URL-Aufbau

Die URL hat folgenden Aufbau:

```
http://<Geräte-URL>/cmdpbspotuser/?action=<action>&parameter1=value1&parameter2=value2
```

Die folgenden Aktionen stehen Ihnen zur Verfügung:

- **action=addpbspotuser**: legt einen oder mehrere neue Public Spot-Benutzer an und druckt anschließend Vouchers in der benötigten Anzahl.
- **action=delpbspotuser**: löscht den Public Spot-Benutzer mit der angegebenen Benutzer-ID.
- **action=editpbspotuser**: zeigt einen Public Spot-Benutzer an, dessen Benutzer-ID Sie mit übergeben haben. Anschließend können Sie den Voucher des Benutzers neu ausdrucken.

Die notwendigen Parameter und deren Werte sind abhängig von der angegebenen Aktion.

Der Assistent ignoriert falsche Parameter-Angaben und übernimmt ausschließlich die korrekten Parameter. Falls Sie einen erforderlichen Parameter falsch angegeben oder ausgelassen haben, zeigt der Assistent eine Eingabemaske. Tragen Sie in diese den korrekten Parameter-Wert ein.

Hinzufügen eines Public Spot-Benutzers

Über die folgende URL registrieren Sie einen neuen Public Spot-Benutzer:

```
http://<Geräte-URL>/cmdpbspotuser/
   ?action=addpbspotuser&parameter1=value1&parameter2=value2&...
```

Ihnen stehen folgende Parameter zur Verfügung:

`comment`

Kommentar zum registrierten Benutzer

Sind für einen Public Spot-Benutzer mehrere Kommentare möglich, geben Sie die Kommentare und die entsprechenden Kommentarfeld-Namen wie folgt an:

```
&comment=<Inhalt1>:<Feldname1>,<Inhalt2>:<Feldname2>,…,<Inhalt5>:<Feldname5>,
```

Existiert ausschließlich ein Kommentarfeld pro Benutzer, genügt die Angabe des Kommentars:

```
&comment=<Kommentar>
```

Deutsche Umlaute werden nicht unterstützt.

Die maximale Zeichenanzahl des Kommentar-Parameters beträgt 191 Zeichen.

`print`

Automatischer Ausdruck des Vouchers.

Fehlt dieser Parameter, zeigt der Assistent anschließend eine entsprechende Schaltfläche, über die Sie den Voucher ausdrucken können.

printcomment

Kommentar auf den Voucher drucken.

Fehlt dieser Parameter, erscheint der Kommentar nicht auf dem Voucher (Default-Einstellung).

nbGuests

Anzahl der anzulegenden Public Spot-Benutzer.

Fehlt dieser Parameter, legt der Assistent ausschließlich einen Benutzer an (Default-Einstellung).

defaults

Default-Werte verwenden

Der Assistent ersetzt fehlende oder falsche Parameter durch Default-Werte.

expirytype

Kombinierte Angabe von Ablauf-Typ und ggf. Verfallsdauer des Vouchers.

Geben Sie diesen Parameter wie folgt an:

```
&expirytype=<Wert1>+validper=<Wert2>
```

Die Parameter-Werte haben folgende Bedeutung:

- `Wert1`: Ablauf-Typ. Mögliche Werte sind `absolute`, `relative`, `both`und `none`.
- `Wert2`: Verfallsdauer des Vouchers, wenn `expirytype` den Wert `both` besitzt. In diesem Fall definieren Sie mittels `validper` die maximale Gültigkeit des Vouchers in Tagen für den absoluten Ablauf. Für alle anderen Ablauf-Typen wird der Parameter `validper` nicht gesetzt.

Fehlt ein Parameter oder geben Sie falsche Werte ein, setzt der Assistent die Default-Werte ein.

ssid

Netzwerk-Name

Fehlt dieser Parameter, verwendet der Assistent den Standard-Netzwerk-Namen (Default-Einstellung).

unit

Zugangsdauer

Geben Sie diesen Parameter wie folgt an:

```
&unit=<Wert1>+runtime=<Wert2>
```

Die Parameter-Werte haben folgende Bedeutung:

- `Wert1`: Einheit der Laufzeit. Mögliche Werte sind: Minute, Stunde, Tag
- `Wert2`: Laufzeit

timebudget

Zeit-Budget

Fehlt dieser Parameter, verwendet der Assistent den Default-Wert.

volumebudget

Volumen-Budget

Die folgenden Angaben sind möglich:

- `k` oder `K`: Angabe in Kilobytes (kB), z. B. `volumebudget=1000k`.
- `m` oder `M`: Angabe in Megabytes (MB), z. B. `volumebudget=100m`.
- `g` oder `G`: Angabe in Gigabytes (GB), z. B. `volumebudget=1g`.

Ohne Einheit entspricht die Angabe einem Wert in Byte (B).

Fehlt dieser Parameter komplett, verwendet der Assistent den Default-Wert.

`multilogin`

Mehrfach-Logins

Wenn Sie diesen Parameter angeben, kann sich der Benutzer mehrfach mit seinem Benutzer-Account anmelden. Fehlt dieser Parameter, sind Mehrfach-Logins standardmäßig deaktiviert.

`maxconclogin`

Anzahl der maximal gleichzeitigen Logins

Mit diesem Parameter legen Sie fest, mit wie vielen Endgeräten parallel sich ein Nutzer am Public Spot anmelden kann. Gültige Werte sind Ganzzahlen wie z. B. `0, 1, 2, ...`.

Fehlt dieser Parameter oder der Parameter hat den Wert `0`, ist dies gleichbedeutend mit einer unbegrenzten Anzahl von Endgeräten.

Dieser Parameter erfordert, dass Mehrfach-Logins erlaubt sind. Das Setzen dieses Parameters allein hat keine Auswirkungen.

`casesensitive`

Benutzername case-sensitive

Wenn Sie diesen Parameter angeben, muss der Public Spot-Nutzer bei der Anmeldung auf die Groß- und Kleinschreibung seines Benutzernamens achten. Gültige Werte sind:

- `0`: Benutzername case-sensitive ist deaktiviert
- `1`: Benutzername case-sensitive ist aktiviert

Fehlt dieser Parameter, verwendet der Assistent den Default-Wert.

`bandwidthprof`

Bandbreitenprofil

Mit diesem Parameter weisen Sie einem Public Spot-Nutzer ein existierendes Bandbreitenprofil zu. Als gültigen Wert für diesen Parameter geben Sie die Zeilennummer eines unter **Setup** > **Public-Spot-Modul** > **Neuer-Benutzer-Assistent** > **Bandbreitenprofile** angelegten Profilnamens an; z. B.

```
&bandwidthprof=1
```

für den ersten Eintrag in der Tabelle.

Fehlt dieser Parameter oder die Zeilennummer ist ungültig (die Tabelle ist z. B. leer), nimmt der Assistent kein Begrenzung der Bandbreite vor.

Sind für fehlende Parameter in der Public Spot-Verwaltung keine Default-Werte angegeben, öffnet Ihnen der Assistent einen entsprechenden Dialog. Tragen Sie in diesen die fehlenden Werte ein.

Bearbeiten eines Public Spot-Benutzers

Über die folgende URL bearbeiten Sie einen oder mehrere Public Spot-Benutzer:

```
http://<Geräte-URL>/cmdpbspotuser/
   ?action=editpbspotuser&parameter1=value1&parameter2=value2&...
```

Ihnen stehen folgende Parameter zur Verfügung:

`pbspotuser`

Name des Public Spot-Benutzers

Mehrere Benutzer geben Sie in der Form `&pbspotuser=<Benutzer1>+<Benutzer2>+...` an.

Findet der Assistent den angegebenen Benutzer nicht, haben Sie die Möglichkeit nach einem Benutzer suchen.

Nach der Änderung übernehmen Sie diese und drucken Sie diese ggf. zusätzlich aus.

`expirytype`

Kombinierte Angabe von Ablauf-Typ und ggf. Verfallsdauer des Vouchers.

Geben Sie diesen Parameter wie folgt an:

```
&expirytype=<Wert1>+validper=<Wert2>
```

Die Parameter-Werte haben folgende Bedeutung:

- `Wert1`: Ablauf-Typ. Mögliche Werte sind `absolute`, `relative`, `both` und `none`.
- `Wert2`: Verfallsdauer des Vouchers, wenn `expirytype` den Wert `both` besitzt. In diesem Fall definieren Sie mittels `validper` die maximale Gültigkeit des Vouchers in Tagen für den absoluten Ablauf. Für alle anderen Ablauf-Typen wird der Parameter `validper` nicht gesetzt.

Fehlt ein Parameter oder geben Sie falsche Werte ein, setzt der Assistent die Default-Werte ein.

`unit`

Zugangsdauer

Geben Sie diesen Parameter wie folgt an:

```
&unit=<Wert1>+runtime=<Wert2>
```

Die Parameter-Werte haben folgende Bedeutung:

- `Wert1`: Einheit der Laufzeit. Mögliche Werte sind: Minute, Stunde, Tag
- `Wert2`: Laufzeit

`timebudget`

Zeit-Budget

Fehlt dieser Parameter, verwendet der Assistent den Default-Wert.

`volumebudget`

Volumen-Budget

Fehlt dieser Parameter, verwendet der Assistent den Default-Wert.

`print`

Automatischer Ausdruck des Vouchers.

Fehlt dieser Parameter, zeigt der Assistent anschließend eine entsprechende Schaltfläche. Über diese haben Sie die Möglichkeit den Voucher auszudrucken.

bandwidthprof

Bandbreitenprofil

Mit diesem Parameter weisen Sie einem Public Spot-Nutzer ein existierendes Bandbreitenprofil zu. Als gültigen Wert für diesen Parameter geben Sie die Zeilennummer eines unter **Setup** > **Public-Spot-Modul** > **Neuer-Benutzer-Assistent** > **Bandbreitenprofile** angelegten Profilnamens an; z. B.

```
&bandwidthprof=1
```

für den ersten Eintrag in der Tabelle.

Fehlt dieser Parameter oder die Zeilennummer ist ungültig (die Tabelle ist z. B. leer), nimmt der Assistent kein Begrenzung der Bandbreite vor.

Sind für fehlende Parameter in der Public Spot-Verwaltung keine Default-Werte angegeben, öffnet Ihnen der Assistent einen entsprechenden Dialog. Tragen Sie in diesem die fehlenden Werte ein.

Löschen eines Public Spot-Benutzers

Über die folgende URL löschen Sie einen oder mehrere Public Spot-Benutzer:

```
http://<Geräte-URL>/cmdpbspotuser/
   ?action=delpbspotuser&pbSpotuser=<Benutzer1>+<Benutzer2>+...
```

Findet der Assistent den angegebenen Benutzer in der Benutzer-Liste, löscht er ihn und gibt eine entsprechende Meldung aus.

Findet der Assistent den angegebenen Benutzer nicht, zeigt er Ihnen eine Tabelle der registrierten Public Spot-Benutzer. Markieren Sie in dieser die zu löschenden Einträge.

15.2.3.4 Public Spot-Benutzer auf einem entfernten Public Spot-Gateway anlegen

Bei der Verwendung von Smart Ticket erhält der Benutzer im RADIUS-Server des lokalen Public Spot-Gateways einen entsprechenden Public Spot-Account.

Sind jedoch mehrere Public Spot-Gateways im Einsatz und soll nur ein Gateway die Benutzerkonten in seinem RADIUS-Server vorhalten, wird der Public Spot-Account bei der Verwendung von Smart Ticket auf dem zentralen RADIUS-Server angelegt. Dazu ist es notwendig, das entfernte Public Spot-Gateway im LCOS-Menübaum unter **Setup** > **Public-Spot-Modul** > **Authentifizierungs-Module** festzulegen.

Sofern kein entferntes Public Spot-Gateway definiert wird, werden Public Spot-Benutzerkonten auf dem lokalen Public Spot-Gateway angelegt.

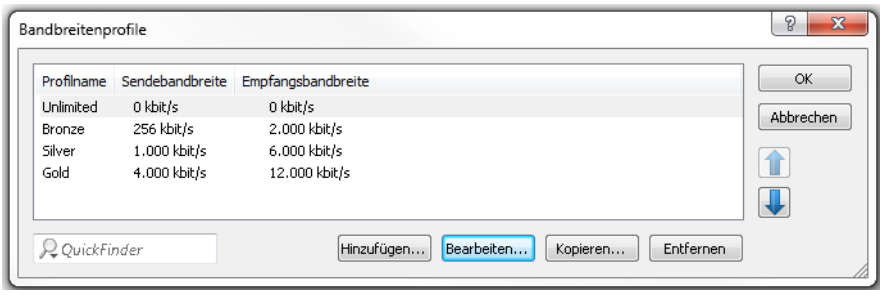
15.2.3.5 Bandbreitenprofile

Bandbreitenprofile verwalten

Über den Dialog **Public-Spot** > **Assistent** > **Bandbreitenprofile** haben Sie die Möglichkeit, Profile zur Beschränkung der Bandbreite (Uplink und Downlink) für Public Spot-Benutzer einzurichten. Wählen Sie je nach Bedarf zwischen vordefinierten Profilen oder erstellen Sie eigene Bandbreitenprofile. Diese Profile lassen sich neuen Benutzern beim Erstellen eines Zugangs für den Public Spot zuweisen, indem Sie im WEBconfig den Setup-Assistenten **Public-Spot-Benutzer einrichten** aufrufen.

Integration fertiger Bandbreitenprofile

Wählen Sie aus vier vordefinierten Profilen das Ihren Anforderungen entsprechende Bandbreitenprofil aus:



Unlimited

Keine Beschränkung in der Sende- und Empfangsbandbreite.

Diese Werte beziehen sich auf die Sendebandbreite (TX) und Empfangsbandbreite (RX) aus Sicht des Clients.

Bronze

Die Sendebandbreite (TX) beträgt 256 KBit/s, die Empfangsbandbreite (RX) 2 MBit/s.

Silver

Die Sendebandbreite (TX) beträgt 1 MBit/s, die Empfangsbandbreite (RX) 6 MBit/s.

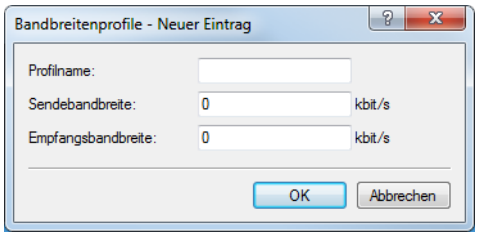
Gold

Die Sendebandbreite (TX) beträgt 4 MBit/s, die Empfangsbandbreite (RX) 12 MBit/s.

Sie haben die Möglichkeit, die fertigen Einträge Ihren Anforderungen entsprechend anzupassen. Markieren Sie dazu das zu bearbeitende Profil und klicken Sie auf die Schaltfläche **Bearbeiten**. Alternativ erstellen Sie eigene Profile.

Erstellen eigener Bandbreitenprofile

Um der Tabelle **Bandbreitenprofile** manuell Einträge hinzuzufügen, klicken Sie auf die Schaltfläche **Hinzufügen**.



Die Einträge im Bearbeitungsfenster haben folgende Bedeutung:

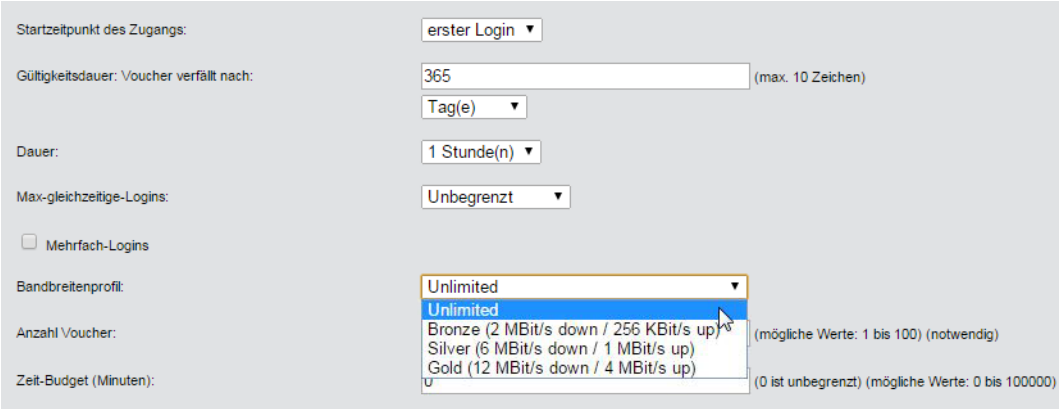
- **Profilname**: Geben Sie hier den Namen für das Bandbreitenprofil ein.
- **Sendebandbreite**: Geben Sie hier die maximale Bandbreite (in KBit/s) ein, die einem Public Spot-Benutzer im Uplink zur Verfügung stehen soll. Um die Bandbreite auf z. B. 1 MBit/s zu beschränken, tragen Sie den Wert `1024` ein.
- **Empfangsbandbreite**: Geben Sie hier die maximale Bandbreite (in KBit/s) ein, die einem Public Spot-Benutzer im Downlink zur Verfügung stehen soll. Um die Bandbreite auf z. B. 1 MBit/s zu beschränken, tragen Sie den Wert `1024` ein.

Bandbreitenprofile zuweisen

Die nachfolgenen Schritte erläutern, wie sie einem Public Spot-Nutzer eingerichtete Bandbreitenprofile zuweisen.

1. Öffnen Sie WEBconfig.

2. Starten Sie über **Setup-Wizards** > **Public Spot-Benutzer einrichten** den Benutzer-Erstellungs-Assistenten.
3. Weisen Sie dem neuen Benutzer aus der Auswahlliste **Bandbreitenprofil** ein entsprechendes Profil zu.



Beim Anlegen eines neuen Benutzers weist der RADIUS-Server dem dazugehörigen Konto automatisch die Ober- und Untergrenzen des betreffenden Bandbreitenprofils zu (nicht das Bandbreitenprofil an sich).

15.2.3.6 Benutzertabelle automatisch bereinigen

Das Gerät bietet Ihnen die Möglichkeit, abgelaufene Konten von Public Spot-Benutzern automatisch zu löschen.

Die Anwender des Public Spot-Assistenten haben als Administratoren in der Regel stark eingeschränkte Rechte und können Einträge in der Benutzertabelle daher nicht selbst löschen. Da die Benutzertabelle nur eine bestimmte Anzahl von Einträgen umfasst, können veraltete Einträge die Kapazität des Public Spot ggf. einschränken. Die Aktivierung dieser Option ist somit dringend zu empfehlen.

Sofern Sie den internen RADIUS-Server für die Verwaltung der Benutzerkonten verwenden, aktivieren Sie die automatische Bereinigung unter **RADIUS** > **Server** > **Benutzer-Datenbank** > **Benutzertabelle automatisch bereinigen**.

Diese Einstellung hat keine Auswirkungen auf die Benutzertabelle eines externen RADIUS-Servers!

Die nachfolgende Liste bietet Ihnen eine grobe Orientierung, welche Kapazitätsgrenzen für bestimmte Modellreihen gelten. Sollten Sie Ihr Gerät darin nicht wiederfinden, entnehmen Sie die genauen Angaben bitte der Produktbeschreibung.

Tabelle 33: Größe der Benutzertabelle bei ausgewählten LANCOM Modellen

LANCOM Modell	Größe der Benutzertabelle
mit Option **Public Spot**: › LANCOM LN-17xx-Serie › LANCOM L(N)-8xx › LANCOM LN-630acn › LANCOM L-3xx-Serie › LANCOM IAP-4G+ › LANCOM IAP-8xx-Serie › LANCOM IAP-5G › LANCOM OAP-8xx-Serie › LANCOM OAP-5G	64
› LANCOM vRouter 50 › LANCOM 178x-Serie › LANCOM 179x-Serie › LANCOM 18xx-Serie	128
› LANCOM 19xx-Serie	256

LANCOM Modell	Größe der Benutzertabelle
› LANCOM WLC-4006(+) › LANCOM vRouter 250 › LANCOM 2100 › LANCOM WLC-30 › LANCOM WLC-60	
› LANCOM vRouter 500 › LANCOM vRouter 1000 › LANCOM vRouter unlimited mit Option **Public Spot XL**: › LANCOM ISG-1000 › LANCOM ISG-4000 › LANCOM ISG-5000 › LANCOM ISG-8000 › LANCOM WLC-1000 › LANCOM WLC-2000	unbegrenzt*

*) Keine Limitierung der Tabelle, eine Obergrenze von max. 2.500 Benutzern ist jedoch empfehlenswert.

15.2.3.7 Stationsüberwachung

Bei eingeschalteter Stationsüberwachung überprüft der Public Spot regelmäßig alle angemeldeten Endgeräte daraufhin, ob sie auch tatsächlich erreichbar sind. Verschollene Endgeräte löscht er automatisch aus seiner lokalen Benutzertabelle. Bei ausgeschalteter Stationsüberwachung wird ein Benutzer erst dann abgemeldet, wenn die Gültigkeit seiner Authentifizierung abläuft.

Für kommerziell auf Zeitbasis betriebene Public-Spots ist die Stationsüberwachung außerordentlich wichtig. Bei solchen Installationen muss jederzeit gewährleistet sein, dass Benutzer nur für diejenigen Zeiten bezahlen, in denen sie die Dienste des Public-Spots auch tatsächlich in Anspruch genommen haben.

Konfiguration

Die Stationsüberwachung des Public Spot-Moduls ist standardmäßig deaktiviert. Sie aktivieren sie, indem Sie unter **Public-Spot** > **Server** > **Interface-Auswahl** > **Leerlaufzeitüberschreitung** einen Wert größer `0` – dieser Wert deaktiviert die Funktion – eintragen. Fortan werden alle Endgeräte nach einer bestimmten Zeit der Inaktivität automatisch vom Public Spot getrennt.

Sofern Ihr Public-Spot-Gerät über Wireless LAN verfügt, haben Sie zusätzlich die Möglichkeit, eine Stationsüberwachung global für alle WLAN-Schnittstellen zu aktivieren. Die dazugehörige Einstellung finden Sie unter **Wireless LAN** > **Security** > **Stationen überwachen, um inaktive Stationen zu erkennen**. Hierbei meldet das Gerät Mobilstationen nach spätestens 60 Sekunden ab (Vorgabewert); bei deaktivierter WLAN-Stationsüberwachung kann dies hingegen in der Standardeinstellung bis zu 15 Minuten dauern.

Sofern Sie Public-Spot über WLAN anbieten, beachten Sie bitte, dass die Stationsüberwachung für WLAN der für Public Spot übergeordnet ist, und eine Trennung früher erfolgen kann, wenn die Leerlaufzeitüberschreitung für WLAN (im Setup-Menü einstellbar unter **WLAN** > **Idle-Timeout**) geringer ist als die für Public Spot.

Überwachung

Im laufenden Betrieb können Sie den Public Spot via WEBconfig überwachen. Die Stations-Tabelle im Benutzer-Authentifizierungs-Menü gibt eine Aufstellung der

› aktuell am Public Spot angemeldeten Benutzer und der
› nicht angemeldeten Endgeräte im Netzwerk.

Sie erreichen die Stations-Tabelle im Status-Menü unter **Public-Spot** > **Stations-Tabelle**. Mit der Schaltfläche **Diese Tabelle beobachten** erneuern Sie die Ansicht der Tabelle automatisch und regelmäßig.

15.2.3.8 Übergabe von WLAN-Sitzungen zwischen Geräten

Wann immer der mit Hotspots zu versorgende Bereich größer wird, kann es erforderlich sein, mehr als nur einen Access Point einzusetzen. Eine mögliche Variante ist dann, ein zentrales Gerät für die Authentifizierung einzurichten, allein auf diesem Gerät das Public Spot-Modul zu aktivieren, und alle anderen Access Points dazu aufzufordern, die entsprechenden Anfragen an das zentrale Gerät weiterzuleiten. Damit fungieren alle übrigen Access Points als einfache, transparente Bridges, welche sich über das Ethernet-Backbone mit diesem zentralen Gateway verbinden. Das versetzt Benutzer in die Lage, sich mit Ihren Clients frei zwischen den Access Points zu bewegen, da alle Session-Informationen in dem zentralen Gateway gespeichert werden.

Diese Variante hat allerdings auch zwei Nachteile:

- Das zentrale Gateway ist ein "single point of failure" und skaliert zudem nicht mit den Anforderungen. Durch den Einsatz von VRRP zum Aufbau einer Redundanz-Lösung lässt sich das Ausfallrisiko minimieren.

  Da über VRRP keine Konfigurationen – wie z. B. die Benutzerdatenbank – abgeglichen werden, bedarf diese Lösung eines externen RADIUS-Servers. Dadurch stehen Ihnen jedoch auch bestimmte Funktionen (wie z. B. die Public Spot-Assistenten in WEBconfig) nicht mehr zur Verfügung.
- Roaming ist nur dann notwendig, wenn das Public Spot-Modul in den Access Points selbst eingerichtet ist. Wenn Sie einen WLAN-Controller verwenden, kann die Authentifizierung zum zentralen Gateway weitergeleitet werden. In diesem Fall ist das Roaming zwischen den Access Points für den WLAN-Controller transparent.

Eine Alternative zu diesem zentralisierten Aufbau ist das Aktivieren des Public Spot-Moduls in allen Access Points. Die Authentifizierung und Seiten-Ablaufsteuerung ist dadurch auf alle Geräte verteilt, und es existiert kein "single point of failure".

Inter Access Point Protocol (IAPP)

Da das Public Spot-Modul als eine "schaltbare" transparente Brigde implementiert ist, benötigen Clients keine neue IP-Adresse, wenn sie zu einem neuem Access Point roamen; offene Verbindungen werden daher auch nicht getrennt. Daraus ergibt sich allerdings die Anforderung, dass sich ein einmal authentifizierter Client nach dem Roamen zu einem anderen Access Point nicht erneut authentifizieren braucht. Die Authentifizierungsinformationen sollten also vom alten zum neuen Access Point mitgenommen werden.

Um Informationen über die roamenden Clients auszutauschen, verwenden Access Points deshalb das sogenannte Inter Access Point Protocol (IAPP): Wann immer ein WLAN-Client zu einem anderen Access Point wechselt, hat er die Möglichkeit, dem neuen Access Point mitzuteilen, mit welchem Access Point er vorher verbunden war. Diese Information erlauben – zusammen mit den regulären Hello-Paketen aus dem Ethernet-Backbone – dem neuen Access Point, den alten Access Point über den Wechsel zu informieren. Der alte Access Point kann daraufhin den Client aus seiner Stationstabelle austragen und die Übergabe bestätigen.

Sollte ein Client für die Verbindung zum neuen Access Point das entsprechende Reassociate-Paket nicht verwenden, sendet der neue Access Point eine Multicast-Übergabeanfrage über den Backbone, statt die Anfrage direkt an den alten Access Point zu richten. Daher funktioniert eine Übergabe auch für Clients, die das IAPP nicht unterstützen.

Die Hauptaufgabe des IAPPs in einem WLAN ist, den alten Access Point anzuweisen, keine Pakete mehr an den entsprechenden Client in seinem Funkbereich zu senden, weil dieser sie nicht mehr empfängt. Ein solches Verhalten könnte andernfalls (aufgrund der Beschaffenheit des 802.11-Frame-Austausch-Protokolls) zu Beeinträchtigungen der anderen mit ihm verbundenen Clients führen.

Wenn das Public Spot-Modul verwendet wird, dient der Kommunikationskanal, den das IAPP liefert, als Übertragungsmedium für Sitzungsinformationen über die WLAN-Clients. Immer dann, wenn ein Access Point eine Übergabeanfrage für einen seiner Clients erhält und für diesen Client über Sitzungsinformationen in seiner Stationstabelle verfügt, leitet er diese Informationen an den anfragenden Access Point weiter. Diese Information beinhalten:

- Den aktuellen Zustand des Clients (authentifiziert oder nicht authentifiziert)

  Für den Fall, dass der Client authentifiziert ist, zusätzlich noch:

- Den zur Authentifizierung verwendeten Benutzernamen
- Den bisher vom Client erzeugten Datenverkehr
- Die bisher verstrichene Sitzungsdauer
- Die IP-Adresse des Clients
- Mögliche Limits zu Sitzungsdauer und Datenvolumen
- Mögliche Angaben zur Leerlauf-Zeitüberschreitung

- Wenn RADIUS-Accounting für die Sitzung verwendet wurde:
  - Den für das RADIUS-Accounting verwendeten Eintrag in der Anmelde-Server-Liste, referenziert durch den Namen
  - Den für die Interim-Updates verwendeten Accounting-Zyklus

Nach erfolgreicher Übergabe beendet der alte Access Point die Sitzung; d. h. er sendet im Falle von RADIUS-Accounting eine Accounting-Stop-Anfrage an den RADIUS-Accounting-Server. Diese ist erforderlich, da ein RADIUS-Server die NAS-Identifizierung nutzen kann, um Anfragen bestimmten Sitzungen zuzuordnen, und er diese Anfragen nicht mehr der richtigen Sitzung zuordnen kann, sobald er die Datenpakete zu einer Sitzung von mehreren Geräten bekommt. Wenn ein Access Point diese Informationen in einer Übergabeantwort erhält, markiert er den Client sofort als authentifiziert und startet nach Möglichkeit eine neue RADIUS-Accounting-Session.

Beachten Sie, dass der neue Access Point einen entsprechenden Eintrag in seiner **Anmelde-Server**-Liste benötigt, um die hierfür benötigten Informationen zu erhalten. Der für das Public Spot-Modul spezifische Teil einer Übergabeantwort ist durch ein "shared secret" geschützt, welches im Setup-Menü unter **Public-Spot-Modul** > **Roaming-Schluessel**. Diese Sicherheitsmaßnahme soll das Fälschen von Übergabeantworten verhindern. Ohne ein konfiguriertes Passwort hängt ein Access Point die oben angeführten Informationen nicht an eine Übergabeantwort an, was den Client zwingt, sich erneut zu authentifizieren.

15.2.3.9 Authentifizierung über RADIUS

RADIUS ist ein weitläufig anerkanntes Protokoll, um auch größeren Benutzergruppen den Zugang zu einem Server bereitzustellen. Ursprünglich für den Dial-in-Serverzugang über Telefonleitungen entwickelt, eignet sich das Konzept ebenfalls für den Authentifizierungsprozess eines Hotspots. In einem komplexeren Provider-Netzwerk lässt sich dadurch z. B. dieselbe Benutzerbasis sowohl für Zugänge über Dial-in als auch via Hotspot verwenden. RADIUS-Server und ihre Zugangsparameter konfigurieren Sie im Dialog **Public-Spot** > **Benutzer** > **Benutzer und RADIUS-Server** unter **RADIUS-Server**.

In bestimmten Szenarien kann es sinnvoll sein, mehr als nur einen RADIUS-Server einzusetzen. Generell wird ein RADIUS-Server durch seine IP-Adresse, den UPD-Port (typischerweise Port 1645 oder 1812) und das sogenannte "shared secret" spezifiziert. Dies ist eine beliebige Zeichenfolge, welche als Passwort für den Zugang zum Server fungiert. Nur Clients, die das shared secret kennen, können mit dem RADIUS-Server interagieren, da das Passwort des Benutzerkontos mit dem shared secret gehashed wird, anstatt es im Klartext zu übermitteln.

Bei Verwendung eines eigenen externen Hotspot-Gateways ist es möglich, Public Spot-Sessions anzupassen, nachdem die Anmeldung des Benutzers bereits erfolgt ist. Dies ist durch die dynamische Autorisierung durch RADIUS CoA realisierbar (siehe *Dynamische Autorisierung durch RADIUS CoA (Change of Authorization)* auf Seite 1607 und *Annahme von RADIUS-CoA-Requests im Public Spot aktivieren* auf Seite 1301).

Die einfachste Transaktion zwischen einem RADIUS-Server und einem Client besteht aus dem Übermitteln der eingegebenen Benutzerdaten durch das Gerät und der Antwort des Server mit "ja" oder "nein". Das RADIUS-Protokoll erlaubt allerdings auch komplexere Antworten und Anfragen, bei denen die Kommunikationspartner für Anfragen und Anworten eine variable Liste von Werten – sogenannte "Attribute" – verwenden.

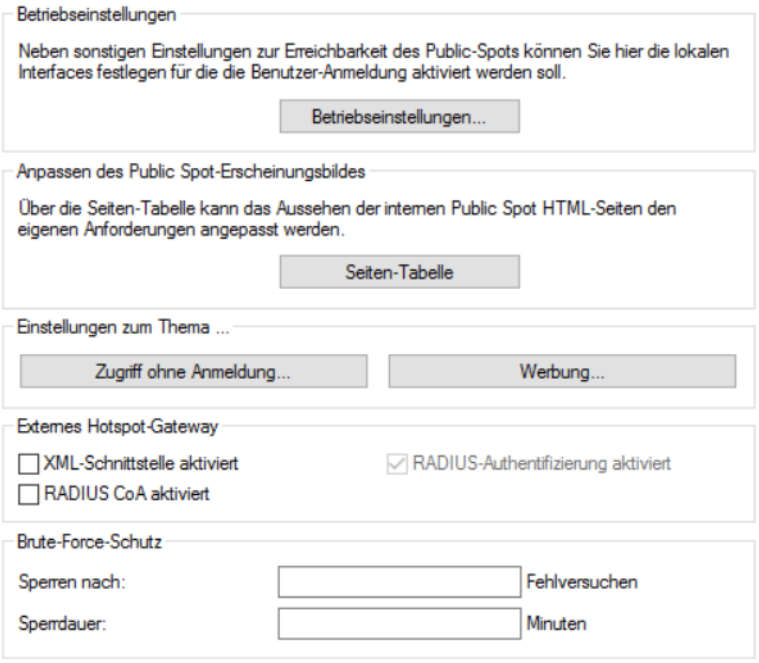
Annahme von RADIUS-CoA-Requests im Public Spot aktivieren

- Die nachfolgenden Handlungsschritte setzen einen funktionierenden Public Spot voraus, welcher an ein externes Hotspot-Gateway angebunden werden kann.
- Das externe Hotspot-Gateway befindet sich entweder in einem frei zugänglichen Netz des Public Spots oder seine Adresse gehört zur Liste der freien Hosts.

Alternativ zu einem XML-basierten `RADIUS_COA_REQUEST`s über das XML-Interface kann der Public Spot auch CoA-Requests über das RADIUS-Protokoll von einem externen Hotspot-Gateway oder einem externen RADIUS-Server entgegen nehmen. Sie haben jedoch auch die Möglichkeit, beide Formen der Befehlsübermittlung parallel zu nutzen.

Der folgende Abschnitt erläutert, wie Sie die RADIUS-CoA-Unterstützung nach RFC3576 im Public Spot aktivieren.

1. Öffnen Sie die Gerätekonfiguration in LANconfig und wechseln Sie in die Ansicht **Public-Spot** > **Server**.



2. Wählen Sie **RADIUS CoA aktiviert** an.
3. Schreiben Sie die Konfiguration zurück in das Gerät.

Der Public Spot verarbeitet fortan RADIUS-CoA-Requests, die von einem externen Hotspot-Gateway eingehen.

Multiple Anmelde-Server

Wie erwähnt, kann die Liste der Anmelde-Server mehr als nur einen Eintrag beinhalten. Es sind Szenarios denkbar, in denen ein Hotspot den Internetzugang für Kunden verschiedener Service-Provider (Anbieter) bereitstellt. Diese Anbieter haben möglicherweise getrennte Benutzerdatenbanken und eigene RADIUS-Server. Das Gerät muss dann anhand des Benutzernamens entscheiden, welcher Anbieter zum betreffenden Benutzer gehört.

Immer, wenn das Gerät für einen zu authentifizierenden Benutzer keinen Eintrag in eigenen, internen Benutzerliste vorfindet, geht es die Liste der Anmelde-Server durch und versucht den Anbieter zu finden, der zu dem betreffenden Benutzer gehört. Der Eintrag `Max.Mustermann@mydomain.de` enthält beispielsweise den Anmelde-Server-Eintrag `MYDOMAIN`. Scheitert diese erste Zuordnung, versucht das Gerät, dem Benutzer den Eintrag `DEFAULT` zuzuordnen.

Sofern auch dieser Eintrag nicht existiert, wählt das Gerät den Anmelde-Server, in der Liste an erster Stelle steht. Findet das Gerät auch hier keinen Eintrag (d. h. die Liste ist leer), schlägt die Benutzerauthentifizierung fehl.

Unabhängig von der Zuordnung eines Benutzers zum Anmeldeserver übermittelt Ihr Gerät stets den vollen Benutzername an den ausgewählten RADIUS-Server. Der ausgewählte RADIUS-Server wird als Anbieter für die anschließende Sitzung gespeichert und für das optionale RADIUS-Accounting verwendet.

Verkettung von Backup-Servern

Internetanbieter wünschen sich eine hohe Verfügbarkeit ihres Angebots und eine übliche Methode, dies zu erreichen, ist Redundanz. Diese Redundanz wird über Backup-Servers erreicht, welche immer dann angefragt werden, wenn die

Anfrage auf den primären Server eine Zeitüberschreitung erzeugt hat, z. B. weil der Server selbst oder andere Netzwerkkomponenten auf dem Weg dahin unerreichbar sind.

Der Bedarf an Backup-Servern variiert dabei stark zwischen den unterschiedlichen Anbietern, weshalb die Liste der Anmeldeserver keine fixe Anzahl von Eingabefeldern vorgibt. Stattdessen bietet Ihnen das Gerät eine Verkettung von Backup-Servern an (Backup-Chaining). Hierbei werden zwei oder mehr Einträge der Anmelde-Server-Liste miteinander verkettet, um eine Abfolge von RADIUS-Servern zu erstellen. Das Gerät arbeitet diese Liste Glied für Glied ab, bis es das Ende erreicht hat (Scheitern der Authentifizierung wegen Nicht-Erreichbarkeit des Servers) oder eine Antwort erhält (entweder Positiv oder Negativ).

Sie verketten Backup-Server über das Eingabefeld **Backup-Name** im Hinzufügen-/Bearbeiten-Dialog unter **Public-Spot** > **Server** > **Anmelde-Server**. Wann immer eine RADIUS-Anfrage scheitert (also eine Zeitüberschreitung erzeugt), prüft das Gerät das Backup-Feld und versucht, den darin referenzierten Server zu erreichen. Grundsätzlich lässt sich damit eine beliebige Anzahl von Servern miteinander verketten, wodurch auch die Möglichkeit besteht, mehreren Providern denselben Fallback-Server zuzuweisen. Die Kette von Backup-Servern wird dann abgebrochen, wenn eines der folgenden Ereignisse auftritt:

- Das Anfragen eines RADIUS-Servers ist fehlgeschlagen und der dazugehörige Eintrag der Anmelde-Server-Liste hat ein leeres Backup-Feld.
- Das Anfragen eines RADIUS-Servers ist fehlgeschlagen und der dazugehörige Eintrag der Anmelde-Server-Liste hat ein ungültiges Backup-Feld, der referenzierte Eintrag lässt sich also nicht in der Anmelde-Server-Liste finden.
- Das Anfragen eines RADIUS-Servers ist fehlgeschlagen und der dazugehörige Eintrag der Anmelde-Server-Liste referenziert einen Eintrag, den das Gerät bereits zu erreichen versucht hat. Dadurch werden endlose RADIUS-Anfragen durch Kreisverkettungen verhindert. Es ist möglich, dass zwei RADIUS-Server einander als Backup angeben, während der primäre Server durch den Benutzernamen gewählt wird.

Während das Gerät eine RADIUS-Anfrage sendet, bleibt die TCP/HTTP-Verbindung zum Client weiterhin bestehen. Überschreitet die Laufzeit der Verkettung irgendwann die Laufzeit der TCP/HTTP-Verbindung, bricht der Client den Anmeldeversuch ab. Es kann daher empfehlenswert sein, die Zahl der Anfrage-Wiederholungen an die einzelnen Backup-Server sowie die Zeitspanne zwischen Anfragen zu verringern. Sie tätigen diese Einstellungen im Dialog **RADIUS** > **Server** > **Erweiterte Einstellungen** > **Optionen**.

15.2.3.10 Abrechnung ohne RADIUS-Accounting-Server

Sofern die Benutzerverwaltung über die interne Benutzer-Liste des Public Spot-Moduls stattfindet und Sie keinen RADIUS-Accounting-Server einsetzen wollen, können Sie lediglich das Ablaufdatum der Benutzerkonten für Abrechnungszwecke verwenden.

Die Verwendung der internen Benutzer-Liste wird nicht mehr empfohlen. Verwenden Sie für neue Installationen stattdessen den internen RADIUS-Server zur Benutzerverwaltung und zum Accouting, um vom vollen Funktionsumfang des Public Spots zu profitieren.

Für Abrechnungsmodelle auf Kredit-Basis kann der Public Spot per SYSLOG detaillierte Verbindungsinformationen an beliebige Rechner im Netzwerk ausgeben. Bei Einsatz entsprechender Software auf dem Zielrechner können Sie die tatsächlich verwendeten Ressourcen (Verbindungszeiten oder Transfervolumen) exakt abrechnen.

15.2.3.11 Abrechnung über RADIUS-Accounting-Server

Bei Abrechnung über einen RADIUS-Server können Sie den Public Spot so einstellen, dass er regelmäßig aktuelle Verbindungsinformationen über jeden aktiven Benutzer an den angegebenen Accounting-Server ausgibt. Ein Accounting wird immer dann gestartet, wenn ein Client über RADIUS authentifiziert wurde und in der **Anmelde-Server**-Liste für den betreffenden **Authentifizierungs-Server** auch ein gültiger **Accounting-Server** konfiguriert ist. Es ist daher auch möglich, verschiedene RADIUS-Server für Accounting und Authentifizierung zu verwenden.

Jedes der regelmäßigen Meldepakete an den Accounting-Server enthält Angaben darüber, welche Ressourcen (Zeit, übertragene Datenmenge, etc.) der Benutzer seit der letzten Meldung verbraucht hat. So gehen bei einem Ausfall eines Public Spots (etwa durch Stromausfall o. ä.) auch im schlimmsten Fall nur wenige Abrechnungsinformationen verloren.

Die regelmäßige Meldung der Abrechnungsinformationen an den Accounting-Server (Interim-Updates) ist in der Voreinstellung ausgeschaltet. Die Aktivierung erfolgt, wenn Sie den Meldezyklus größer 0 festlegen.

› LANconfig: **Public-Spot** > **Benutzer** > **Update-Zyklus**

Der Meldezyklus wird in Sekunden angegeben. Er bestimmt den Zeitabstand, in dem Ihr Gerät regelmäßig Verbindungsinformationen an den Accounting-Server sendet. Ein Meldezyklus von `0` Sekunden deaktiviert die Funktion. In diesem Fall sendet Ihr Gerät nur zu Beginn und am Ende einer Sitzung Abrechnungsinformationen.

Bei Einsatz von Abrechnungsmodellen auf Guthabenbasis (PrePaid) übernimmt der RADIUS-Server die Überwachung der festgelegten Nutzungsbeschränkungen (Kontingente für Verbindungszeit oder Transfervolumen, Ablaufdatum). Sobald ein Benutzer sein Guthaben aufgebraucht hat, sperrt der RADIUS-Server das Benutzerkonto. Ihr Gerät weist künftige Anmeldeversuche des Benutzers daraufhin ab.

Zeitkontingente für PrePaid-Modelle kann der Public Spot auch während der aktiven Sitzungen überwachen. Wird ein Zeitguthaben vollständig aufgebraucht, so beendet der Public Spot automatisch die betreffende Sitzung. Die Guthabenüberwachung wird eingeschaltet, indem der RADIUS-Server zum Sitzungsbeginn eines Benutzers dessen Zeitguthaben als Attribut "Session Timeout" an den Public Spot übermittelt.

Anfragetypen

Ihr Gerät ist in der Lage, verschiedene Typen von RADIUS-Anfragen an einen Accounting-Server zu senden. Diese Anfragen unterscheiden sich nach je nach Sitzungsstatus eines Benutzers:

› Ein Accounting-Start wird nach einer erfolgreichen Authentifizierung gesendet.
› Ein Accounting-Stop wird nach Beenden einer Public Spot-Sitzung gesendet.
› Optional: Zwischenzeitliche Aktualisierungen (Interim-Updates) werden während der Sitzung gesendet.

Es gibt zwei Arten von Interim-Updates: Ein initiales Update wird im direkten Anschluss an die Start-Anfrage gesendet, da einige RADIUS-Server dieses benötigen, um eine Sitzung in ihrer Accounting-Datenbank anzulegen. Alle weiteren Updates sind davon abhängig, ob ein Accounting-Zyklus für die jeweilige Sitzung definiert wurde (unter **Public-Spot** > **Benutzer** > **Update-Zyklus**).

Alternativ kann dieser Wert auch Bestandteil einer RADIUS-Authentifizierungs-Antwort sein: Dabei bietet der RADIUS-Server einem RADIUS-Client (also z. B. Ihrem Public Spot) ein Accounting-Interim-Intervall an, welches der Client bei entsprechender Unterstützung übernimmt, sofern für ihn lokal kein eigenes Intervall definiert wurde.

Sofern ein lokaler Wert gesetzt wurde, wird dieser immer höher priorisiert als der von einem RADIUS-Server gelieferte Wert, welchen die RADIUS RFCs standardmäßig fordern!

Accounting-Backup

Die Backup-Lösung für das RADIUS-Accounting entspricht der für die RADIUS-Authentifizierung, d. h. Ihr Gerät arbeitet die in der Anmelde-Server-Liste angelegten Einträge nach und nach ab (siehe Kapitel *Verkettung von Backup-Servern*). Die Backup-Einträge für die Accouting-Server sollten dabei mit derselben Umsicht gewählt werden wie die für die Authentifizierungs-Server: Sofern Sie mehrere Backup-Server verwenden, müssen sie ggf. Werte für Wiederholung und Zeitüberschreitung der Anfragen anpassen, um eine gute Erreichbarkeit des Gesamtsystems zu erreichen.

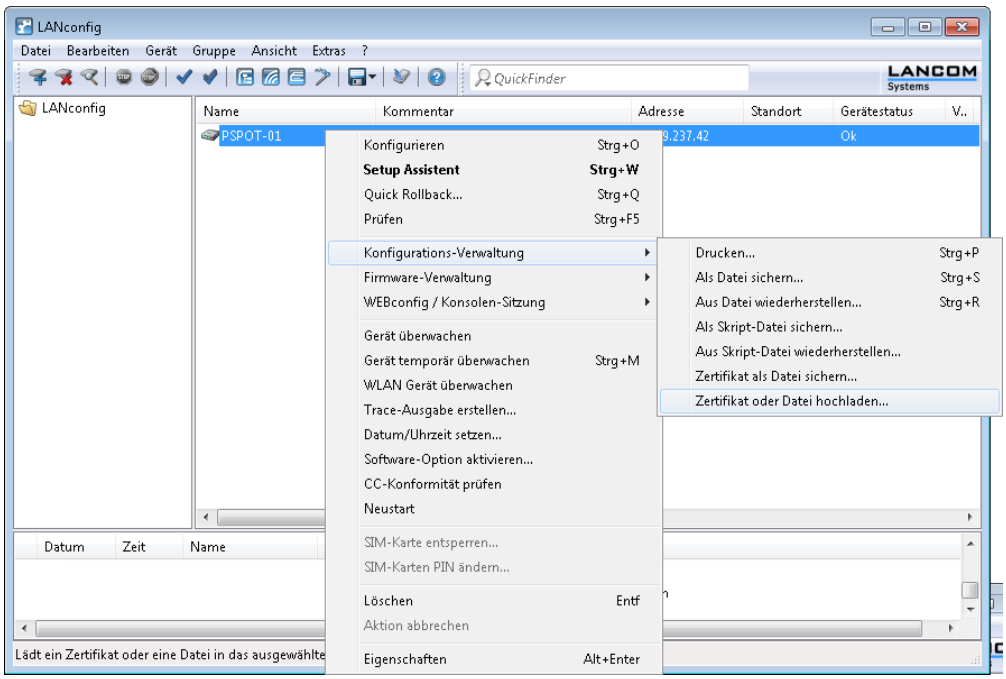
Während das Gerät Accounting-Anfragen sendet, werden laufende Benutzersitzungen nicht angehalten, was – im Gegensatz zur Authentifizierung – zusätzliche Ressourcen im Gerät verbraucht. Bitte achten Sie darauf, dass der Zeitbedarf für die Auswahl eines Accounting-Servers* geringer ausfällt als die Länge eines Accounting-Zyklusses bei Interim-Update-Anfragen. Somit vermeiden Sie einen Anfragestau und daraus resultierenden Stapelüberlauf.

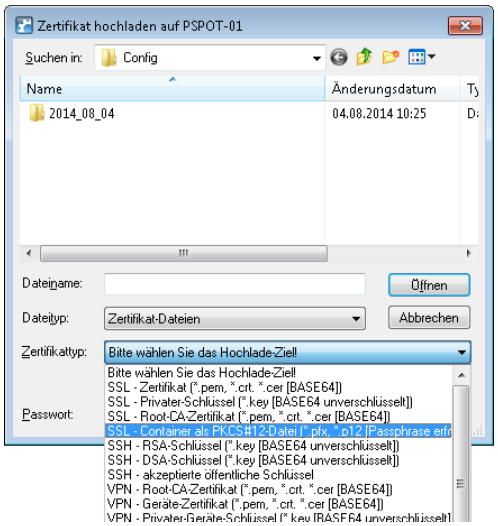
**Anzahl Backups x (Leerlaufzeit-Überschreitung + Anzahl Wiederholungen)*

15.2.3.12 Mehrstufige Zertifikate für Public Spots

SSL-Zertifikatsketten können in Form eines PKCS#12-Containers in das Gerät geladen werden. Diese Zertifikatsketten können für die Public Spot-Authentifizierungsseiten über den im Gerät implementierten HTTPS-Server verwendet werden. Zertifikate von allgemein anerkannten Trust-Centern sind üblicherweise mehrstufig. Offiziell signierte Zertifikate im Public Spot sind notwendig, um Zertifikatsfehlermeldungen des Browsers bei Public Spot-Authentifizierungen zu vermeiden.

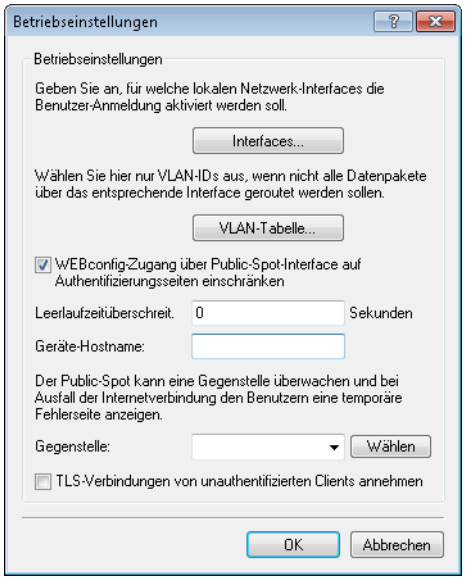
Das Zertifikat laden Sie über LANconfig im Dateimanagement mit den einzelnen Dateien des Root-CA-Zertifikats oder als PKCS#12-Container in das Gerät:





Da Zertifikate üblicherweise auf DNS-Namen ausgestellt werden, muss der Public Spot anstelle einer internen IP-Adresse den DNS-Namen des Zertifikats als Ziel angeben (einzugeben unter **Public-Spot** > **Server** > **Betriebseinstellungen**

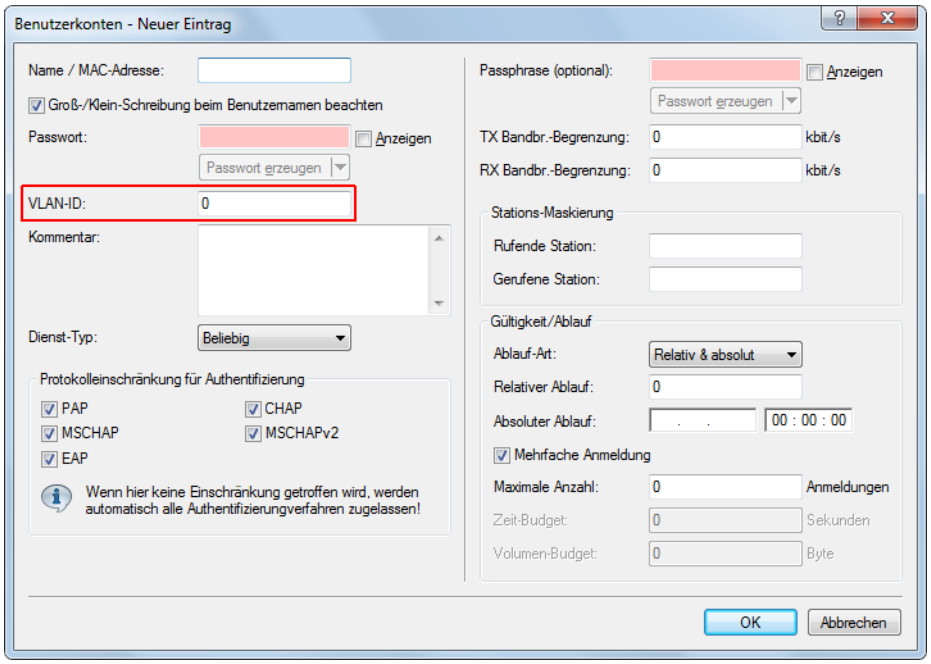
bei **Geräte-Hostname**). Dieser Name muss im DNS-Server auf die entsprechende IP-Adresse des Public Spots aufgelöst werden.



15.2.3.13 Benutzern individuelle VLANs zuweisen

Unabhängig von der Zuweisung einer VLAN-ID für das gesamte Public Spot-Modul bietet Ihnen das Gerät die Möglichkeit, individuelle VLAN-IDs für einzelne Public Spot-Benutzer zu vergeben. Diese ID wird Ihren Benutzern im Anschluss an eine erfolgreiche Authentifizierung automatisch vom RADIUS-Server zugewiesen. Auf diese Weise ist es z. B. möglich, unterschiedliche Public Spot-Nutzer in getrennte Netze mit verschiedenen Rechten und Zugriffsmöglichkeiten einzuordnen, ohne dass sich diese an getrennten SSIDs anmelden oder Sie die Verfügbarkeit verschiedener Netze öffentlich aussenden müssen (z. B. Netze für unterschiedliche Kunden-Typen). Die entsprechenden Regeln lassen sich über die Firewall realisieren, indem Sie als Quell-Tag die VLAN-ID des betreffenden Nutzers / der betreffenden Nutzergruppe angeben.

Vorraussetzung für die oben beschrieben Funktionen ist ein aktiviertes VLAN-Modul.



- Öffnen Sie die Tabelle **Benutzerkonten** im Dialog **RADIUS** > **Server** > **Benutzer-Datenbank** und klicken Sie auf **Hinzufügen...**, um einen neuen Benutzer zu erstellen.
- Weisen Sie dem neuen Benutzer eine individuelle VLAN-ID über das Eingabefeld **VLAN-ID** zu. Die individuelle VLAN-ID überschreibt nach der Authentifizierung durch den RADIUS-Server eine globale VLAN-ID, die ein Nutzer ansonsten über das Interface erhalten würde. Der Wert `0` deaktiviert die Zuweisung einer individuellen VLAN-ID.

Die Vergabe einer VLAN-ID erfordert technisch bedingt die erneute Adresszuweisung durch den DHCP-Server. Solange ein Client nach der erfolgreichen Authentifizierung noch keine neue Adresse zugewiesen bekommen hat, befindet sich er sich nachwievor in seinem bisherigen (z. B. ungetaggten) Netz. Damit der Client möglichst rasch in das neue Netz überführt wird, ist es notwendig, die Lease-Time des DHCP-Servers unter **IPv4** > **DHCPv4** möglichst gering einzustellen. Mögliche Werte (in Minuten) sind z. B.:

- **Maximale Gültigkeit:** `2`
- **Standard-Gültigkeit:** `1`

Berücksichtigen Sie dabei, dass eine derart starke Verkürzung der globalen Lease-Time Ihr Netz bedingt mit DHCP-Nachrichten flutet und bei größeren Nutzerzahlen zu einer gesteigerten Netzlast führt! Alternativ haben Sie die Möglichkeit, einen externen DHCP-Server einzusetzen oder Ihre Nutzer manuell – über ihren Client – eine neue Adresse anfordern zu lassen. In der Windows-Kommandozeile erfolgt dies z. B. über die Befehle `ipconfig /release` und `ipconfig /renew`.

Durch die Zuweisung einer VLAN-ID verliert ein Nutzer nach Ablauf des initialen DHCP-Leases seine Verbindung! Erst ab dem zweiten Lease – also nach erfolgter Zuweisung der VLAN-ID – bleibt die Verbindung konstant.

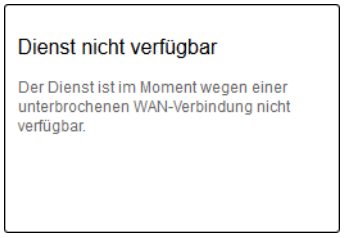
15.2.3.14 Fehlerseite bei Wegfall der WAN-Verbindung einrichten

Sie haben die Möglichkeit, das Public Spot-Modul gegenüber noch nicht authentifizierten Benutzern – zusätzlich zu den allgemeinen Anmeldefehlern – auch WAN-Verbindungsfehler ausgeben zu lassen. Dadurch werden mögliche Benutzer bereits vorab über die fehlende Verfügbarkeit des Netzwerks informiert. Die entsprechende Variante der **Fehler**-Seite erscheint immer dann, wenn das Public Spot-Modul einen Wegfall der WAN-Verbindung registriert.

Damit die Anzeige der Fehlerseite für diesen Fall korrekt funktioniert, **muss** eine entsprechende Gegenstelle benannt sein, deren Verbindungsstatus das Public Spot-Modul überwacht. Tragen Sie dazu im Dialog **Public-Spot** > **Server** eine entsprechende **Gegenstelle** ein. Über die Schaltfläche **Wählen** können Sie dem Auswahl-Eingabefeld bequem eine bereits eingerichtete oder neue Gegenstelle zuweisen.

Ohne Benennung einer zu überwachenden Gegenstelle deaktiviert das Public Spot-Modul die Ausgabe von Verbindungsfehlern auf der Fehlerseite. Ein Wegfall der WAN-Verbindung führt dann bei unauthentifizierten Benutzern stattdessen zu einem Verbindungs-Timeout in ihrem Browser.

Innerhalb einer individuellen Fehlerseite verwenden Sie den Bezeichner `LOGINERRORMSG`, um die Fehlermeldung des LCOS bei Wegfall der WAN-Verbindung einzufügen. Im Falle eines WAN-Verbindungsfehlers wird dann die folgende Fehlermeldung ausgegeben:



Bereits authentifizierte Benutzer hingegen erhalten unabhängig von der Fehlerseite immer eine entsprechende Fehlermeldung von ihrem Browser.

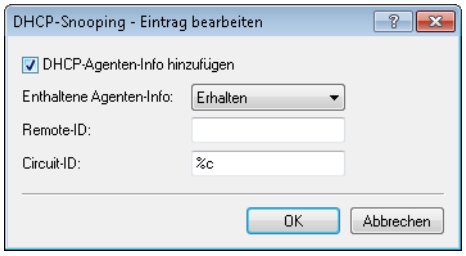
15.2.3.15 AP-spezifische Anmeldung an einem zentralen Public Spot

Ein zentraler WLC verwaltet in einer verteilten Infrastruktur einen Public Spot, dessen Konfiguration (Public Spot-SSID, Sicherheitsstandards) auf allen beteiligten APs entsprechend identisch ist. Auf diesem Weg kann ein Public Spot-Anbieter z. B. in allen seinen räumlich getrennten Filialen einen identischen Public Spot zur Verfügung stellen.

Die Kunden hätten also nach dem Erhalt eines Vouchers in jeder Filiale Zugriff auf diesen Public Spot. Um dennoch die Nutzung auf die Filiale zu beschränken, in der der Kunde den Voucher erhalten hat, überträgt der AP zusätzlich zu Username und Passwort auch seine Kennung. Diese Kennung ermöglicht die Zuordnung des Vouchers zu diesem AP. Der AP nutzt für die Übertragung der Kennung die Circuit-ID (DHCP-Option 82), die er den DHCP-Requests anhängt. Diese DHCP-Pakete durchlaufen den zentralen Public Spot, der die Kennung anhand der Einträge in der RADIUS-User-Tabelle überprüft.

Der Public Spot lässt diese Anfrage nur zu, wenn diesem Voucher in der RADIUS-User-Tabelle auch dieser AP zugeordnet ist. Kunden, die einen Voucher in Filiale A erhalten haben, können sich also nicht in der Filiale B am gleichen Public Spot anmelden, da beide Filial-APs unterschiedliche Kennungen übertragen.

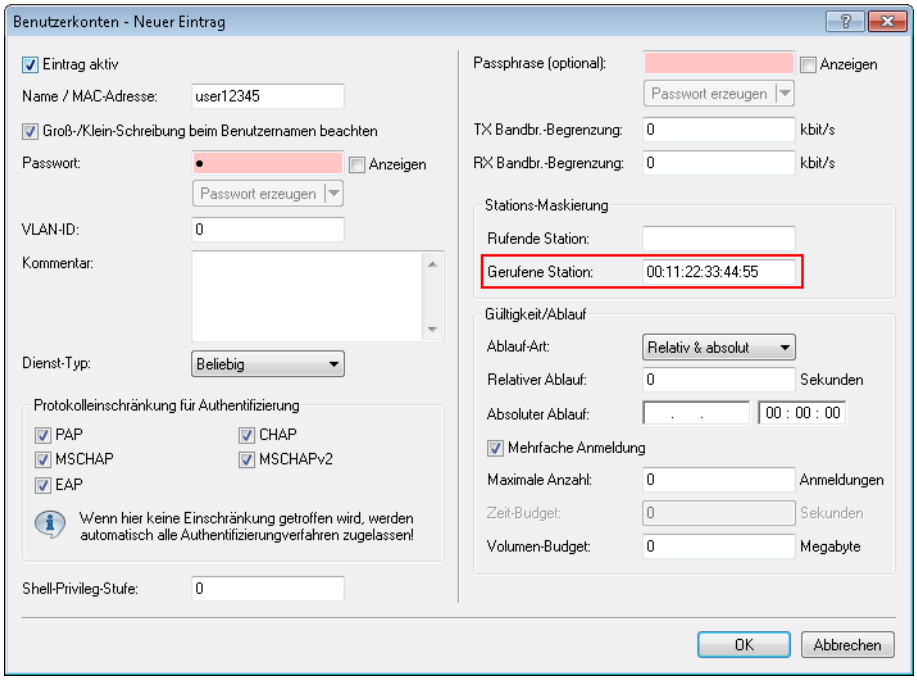
Die AP-Kennung konfigurieren Sie als Circuit-ID unter **Schnittstellen** > **Snooping** > **DHCP-Snooping** bei der entsprechenden Schnittstelle ein.



Sie können die folgenden Variablen verwenden:

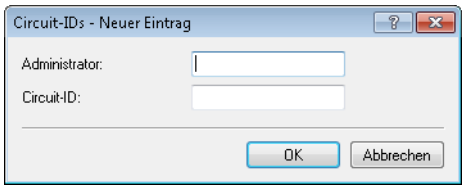
- **%%**: fügt ein Prozent-Zeichen ein.
- **%c**: fügt die MAC-Adresse der Schnittstelle ein, auf der sich der Public Spot-User anmeldet. Handelt es sich um eine WLAN-SSID, ist das die entsprechende BSSID.
- **%i**: fügt den Namen der Schnittstelle ein, auf der sich der Public Spot-User anmeldet.
- **%n**: fügt den Namen des APs ein, wie er z. B. unter **Management** > **Allgemein** festgelegt ist.
- **%v**: fügt die VLAN-ID des DHCP-Request-Paketes ein. Diese VLAN-ID stammt entweder direkt aus dem VLAN-Header des DHCP-Datenpakets oder aus der VLAN-ID-Zuordnung für diese Schnittstelle.
- **%p**: fügt den Namen der Ethernet-Schnittstelle ein, die das DHCP-Datenpaket empfangen hat. Diese Variable ist hilfreich bei Geräten mit eingebautem Ethernet-Switch oder Ethernet-Mapper, da diese mehr als eine physikalische Schnittstelle auf eine logische Schnittstelle mappen können. Bei anderen Geräten sind **%p** und **%i** identisch.
- **%s**: fügt die WLAN-SSID ein, wenn die Anmeldung über einen WLAN-Client erfolgt. Bei anderen Clients enthält diese Variable einen leeren String.
- **%e**: fügt die Seriennummer des APs ein, wie sie z. B. unter **Management** > **Allgemein** zu finden ist.

Im WLC konfigurieren Sie diese Kennung in der RADIUS-User-Tabelle unter **RADIUS** > **Server** > **Benutzer-Datenbank** > **Benutzerkonten**.



Als „Gerufene Station" fügen Sie die Kennung des APs ein, der den entsprechenden Voucher-Zugriff ermöglichen soll.

Der Public Spot-Setup-Assistent kann bei der Einrichtung neuer Public Spot-Nutzer automatisch die Kennung des Gerätes übernehmen, wenn diese unter **Public-Spot** > **Assistent** > **Circuit-IDs** konfiguriert ist.



Der Setup-Assistent prüft beim Anlegen eines neuen Public Spot-Nutzers, ob für den angemeldeten **Administrator** ein Eintrag in dieser Tabelle hinterlegt ist. Ist das der Fall, übernimmt der Setup-Assistent die entsprechende **Circuit-ID** als „gerufene Station" in die RADIUS-User-Tabelle.

15.2.3.16 Redirect für HTTPS-Verbindungen

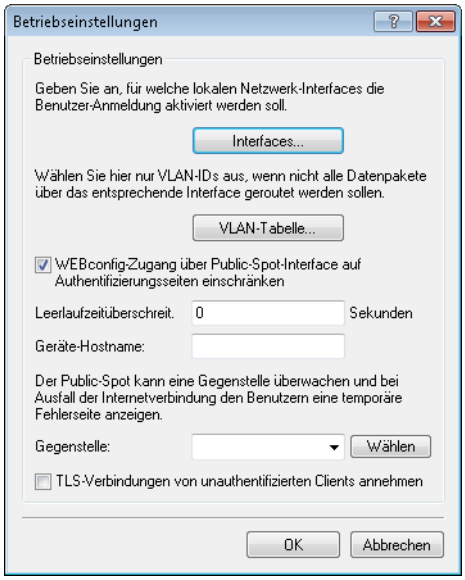
Versucht ein nicht angemeldeter Client über eine Schnittstelle, für die der Public Spot aktiv ist, via HTTPS auf eine Webseite zuzugreifen, wird diese Verbindungsanfrage an das Public Spot-Gateway selber umgeleitet, um dem Nutzer die Anmeldeseite zu präsentieren (ist bei HTTP auch der Fall). In diesem Fall wird dem Benutzer normalerweise eine Zertifikatswarnung seines Browsers präsentiert, da Name oder IP der ursprünglich angesurften Seite nicht dem Namen oder der IP des Public Spot entspricht. Um dies und die Erzeugung von erhöhter Last durch die aufgebauten HTTPS-/TLS-Verbindungen auf dem Public Spot Gateway zu verhindern, können Sie mit dieser Einstellung der Verbindungsaufbau über HTTPS für unangemeldete Clients verhindern.

Ist der Client einmal angemeldet, findet keinerlei Umleitung mehr statt und es können beliebig HTTP- und HTTPS-Verbindungen durch den Client aufgebaut werden.

Heutzutage übliche Clients führen eine "Captive Portal Detection" via HTTP durch. Dabei wird versucht, auf eine bestimmte URL via HTTP zuzugreifen, um das Vorhandensein einer Anmeldeseite (durch Public Spot oder andere Lösungen) zu überprüfen. Dieser Mechanismus wird durch das Ausschalten der HTTPS-Umleitung nicht beeinflusst, da die Erkennung normalerweise über HTTP stattfindet.

Ist es in einem Public Spot-Szenario jedoch nicht vorgesehen, dass unbekannte WLAN-Clients eine Verbindungsanfrage auch über HTTP ausführen sollen, würde dieser wirkungslose HTTPS-Redirect das Public Spot-Gateway unnötig belasten. Entsprechend ist es möglich, diesen HTTPS-Redirect prinzipiell zu deaktivieren. In diesem Fall würde der Benutzer vom Browser eine leere Seite erhalten.

Das Redirect für HTTPS-Verbindungen konfigurieren Sie im LANconfig unter **Public-Spot** > **Server** > **Betriebseinstellungen**.



Um das HTTPS-Redirect einzuschalten, aktivieren Sie die Option **TLS-Verbindungen von unauthentifizierten Clients annehmen**. In der Standardeinstellung ist diese Option deaktiviert.

15.2.3.17 Schutz vor Brute Force-Angriffen

Brute-Force-Angriffe sind die bekanntesten Angriffe auf ein Netzwerk. Diese Art von Angriff besteht darin, eine Menge an möglichen Passwörtern innerhalb kurzer Zeit auszuprobieren, bis das richtige Passwort gefunden wird. Ein möglicher Schutz vor Brute-Force-Angriffen besteht darin, nach einem oder mehreren aufeinander folgenden fehlgeschlagenen Eingabeversuchen die Zeit bis zur nächsten möglichen Eingabe zu verzögern.

Den Schutz vor Brute-Force-Angriffen konfigurieren Sie mit LANconfig unter **Public-Spot** > **Server** im Abschnitt **Brute-Force-Schutz**.



Sperren nach

Bestimmen Sie, nach wie vielen Fehlversuchen die Eingabesperre für weitere Versuche eingreifen soll.

Sperrdauer

Bestimmen Sie, für wie lange die Eingabesperre gelten soll.

Über die Konsole zeigt der Befehl `show pbbruteprotector` den aktuellen Status des Brute-Force-Schutzes:

`show pbbruteprotector`

Zeigt eine Übersicht über alle am Public Spot angemeldeten MAC-Adressen.

`show pbbruteprotector [MAC-Adresse[ MAC-Adresse[ ...]]]`

Die Angabe einer oder mehrerer durch Leerzeichen getrennter MAC-Adressen zeigt den Status der jeweiligen MAC-Adressen an.

Die Angabe von MAC-Adressen erfolgt in den Formaten `11:22:33:44:55:66`, `11-22-33-44-55-66` oder `112233445566`.

15.2.4 Alternative Anmeldeformen

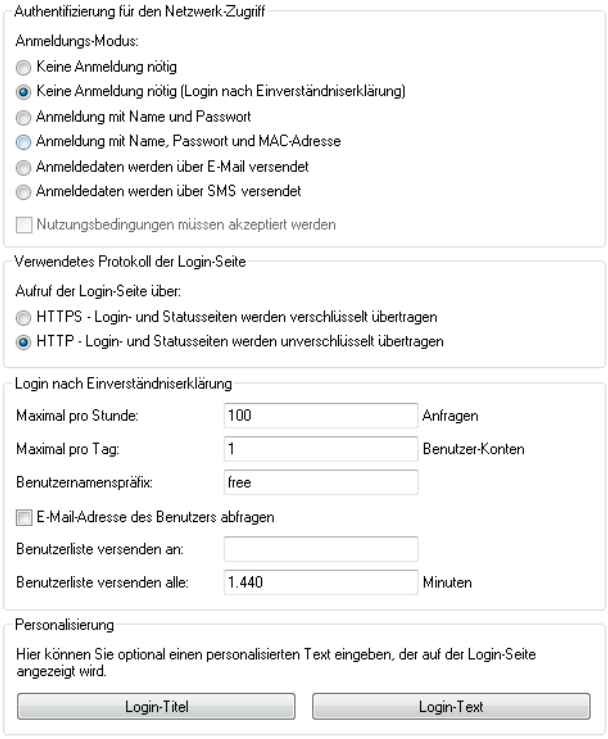
Neben der Anmeldung über vorab mitgeteilte Zugangsdaten können Ihre Nutzer die Zugangsdaten auch selbstständig per E-Mail oder SMS anfordern, oder den schnellen Public Spot-Zugang durch Akzeptieren einer Einverständniserklärung erlangen. Alternativ können Sie über die XML- oder die PMS-Schnitstelle (Modul als Option erhältlich) Ihren Public Spot auch mit anderen Software-Systemen verknüpfen, um so umfassendere oder mehrstufige Anmeldeszenarien zu realisieren.

Ebenso können Sie Ihren Nutzern einen zusätzlichen Komfort bieten, indem Sie z. B. automatisierte Anmeldeverfahren erlauben (Automatische Anmeldung sowie Re-Login über die MAC-Adresse, Anmeldung über WISPr, Hotspot 2.0) und Ihren Nutzern – darauf aufbauend – entsprechende Roaming-Dienste anbieten.

Die Hotspot-2.0- und Roaming-Funktionalitäten sind nur im Zusammenhang mit WLAN verfügbar.

15.2.4.1 Übersicht der Anmeldemodi

Die Anmeldung am Public Spot kann auf verschiedenen Wegen erfolgen. Diese Einstellungen für die Authentifizierung am Netzwerk legen Sie im Dialog **Public-Spot** > **Anmeldung** fest.



Folgende Anmeldungsmodi stehen Ihnen zur Auswahl:

- **Keine Anmeldung nötig**

  Nutzer erhalten freien Zugang zum Public Spot, eine Anmeldung ist nicht erforderlich.

Verwenden Sie diese Einstellung nicht, wenn Ihr Gerät uneingeschränkten Zugriff auf das Internet bietet!

- **Keine Anmeldung nötig (Login nach Einverständniserklärung)**

  Nutzer erhalten freien Zugang zum Public Spot, nachdem sie die Einverständniserklärung des Betreibers akzeptiert haben. Die Anmeldung erfolgt dabei für die Nutzer völlig transparent über einen RADIUS-Server. Voraussetzung dafür ist, dass Sie eine individuelle Seitenvorlage (Willkommensseite mit Einverständniserklärung) eingerichtet haben: In diesem Fall leitet der Public Spot einen neuen Nutzer zunächst auf die Willkommensseite weiter. Nach Zustimmung der Einverständniserklärung legt das Gerät entsprechend der unter **Public-Spot** > **Assistent** gesetzten Standardwerte automatisch ein Benutzerkonto an und gibt den Zugriff auf das angeschlossene Netzwerk frei.

  Darüber hinaus ist bei Anwählen dieses Anmeldungsmodus der Dialog-Abschnitt **Login nach Einverständniserklärung** verfügbar, in dem Sie zusätzliche Rahmenbedingungen für das Erstellen von freien Benutzerkonten durch den RADIUS-Server festlegen:

  - **Maximal pro Stunde**: Geben Sie an, wie viele Benutzer sich pro Stunde am Gerät automatisch ein Konto erstellen können. Verringern Sie diesen Wert, um Leistungseinbußen durch übermäßig viele Nutzer zu reduzieren.
  - **Maximal pro Tag**: Geben Sie an, wie viele Konten ein Nutzer pro Tag anlegen darf. Ist dieser Wert erreicht und die Nutzer-Sitzung abgelaufen, kann sich ein Benutzer für den Rest des Tages nicht mehr automatisch am Public Spot anmelden und authentifizieren lassen.
  - **Benutzernamenspräfix**: Geben Sie hier einen Präfix an, anhand dessen Sie Benutzer in der RADIUS-Benutzertabelle erkennen, die das Gerät automatisch nach Bestätigen der Nutzungsbedinungen angelegt hat. Dieser Präfix wird dem unter **Public-Spot** > **Assistent** spezifizierten **Muster für den Benutzernamen** unmittelbar vorangestellt.
  - **E-Mail-Adresse des Benutzers abfragen**: Aktivieren Sie diese Checkbox, um die E-Mail-Adresse des Nutzers für die Verwendung des Public Spot abzufragen. Die hier angegebene E-Mail-Adresse trägt das Gerät automatisch im Kommentarfeld des neu angelegten RADIUS-Benutzers ein. Eine Liste aller vorhandenen Adressen wird täglich einmal im Flash-Speicher des Gerätes abgelegt und bleibt auch im Falle eines Neustartes bestehen.
  - **Benutzerliste versenden an**: Geben Sie hier die E-Mail-Adresse an, an die die Adressliste gesendet werden soll. Es werden nur Informationen gesendet, die seit der letzten Übermittlung neu hinzugekommen sind. Die Übermittlung der Adressliste erfolgt als CSV-Datei.
  - **Benutzerliste versenden alle**: Legen Sie fest, in welchem Intervall die aktualisierte Adressliste an die angegebene E-Mail-Adresse übermittelt werden soll. Der Wert wird in Minuten angegeben.

  Die in der Willkommensseite hinterlegten Einverständniserklärung ist nicht mit der Nutzungsbedingungsseite zu verwechseln. Die Seite **Nutzungsbedingungen** ist eine Sonderseite, die nach gesonderter Aktivierung bei anderen Anmeldungsmodi zur Verfügung steht (siehe *Mögliche Authentifizierungsseiten* auf Seite 1347). Sofern Sie keine Willkommensseite einrichten (siehe *Konfiguration benutzerdefinierter Seiten* auf Seite 1353), zeigt das Gerät beim Zugriff auf den Public Spot eine Fehlermeldung an.

- **Anmeldung mit Name und Passwort**

  Nutzer melden sich am Public Spot mit ihrem Namen und ihrem Passwort an. Die Login-Daten erhalten Nutzer von einem Netzwerk-Administrator über einen Voucher.

- **Anmeldung mit Name, Passwort und MAC-Adresse**

  Nutzer melden sich am Public Spot mit ihrem Namen und ihrem Passwort an. Die Login-Daten erhalten Nutzer von einem Netzwerk-Administrator über einen Voucher. Zusätzlich muss bei diesem Anmeldungs-Modus die MAC-Adresse des Client mit der in der Benutzer-Liste vom Administrator hinterlegten Adresse übereinstimmen.

- **Anmeldedaten werden über E-Mail versendet**

  Nutzer melden sich am Public Spot mit ihrem Namen und ihrem Passwort an. Die Login-Daten generieren sich die Nutzer selbst; zugestellt werden die Daten per E-Mail. Die Aktivität eines Administrators ist nicht erforderlich. Mehr zu diesem Anmeldungsmodus erfahren Sie unter *Selbständige Benutzeranmeldung (Smart Ticket)* auf Seite 1313.

- **Anmeldedaten werden über SMS versendet**

Nutzer melden sich am Public Spot mit ihrem Namen und ihrem Passwort an. Die Login-Daten generieren sich die Nutzer selbst; zugestellt werden die Daten per SMS. Die Aktivität eines Administrators ist nicht erforderlich. Mehr zu diesem Anmeldungsmodus erfahren Sie unter *Selbständige Benutzeranmeldung (Smart Ticket)* auf Seite 1313.

Durch aktivieren der Option **Nutzungsbedingungen müssen akzeptiert werden** haben Sie in bestimmten Anmeldungsmodi außerdem die Möglichkeit, die Anmeldung an die Anerkennung von Nutzungsbedingungen zu koppeln. In diesem Fall zeigt der Public Spot auf der Anmeldeseite ein zusätzliches Optionsfeld an, welches die Benutzer vor Registrierung bzw. Anmeldung zum Akzeptieren der Nutzungsbedingungen auffordert. Stimmt ein Nutzer diesen Nutzungsbedingungen nicht explizit zu, bleibt ihm eine Anmeldung am Public Spot verwehrt.

Denken Sie daran, vorab eine Seite mit Nutzungsbedingungen in das Gerät zu laden, bevor Sie diese Option aktivieren. Andernfalls zeigt das Gerät dem Benutzer lediglich einen Platzhalter an Stelle der Nutzungsbedingungen an.

15.2.4.2 Selbständige Benutzeranmeldung (Smart Ticket)

Geräte mit Public Spot bieten Anwendern einen zeitlich begrenzten Zugang zu bestimmten Netzwerken, klassischerweise dem Internet. In vielen Szenarien wird für das Anlegen eines Zugangs ein beschränkter Administrations-Account eingesetzt: Ein Mitarbeiter an einer Hotel-Rezeption z. B. erhält hierbei einen Account, der ausschließlich über die Funktionsrechte zum Anlegen und ggf. Verwalten von Public Spot-Benutzern verfügt. Mit wenigen Mausklicks kann der Mitarbeiter dann den Hotelgästen einen Voucher für den Netzzugang ausdrucken.

Da allerdings auch die komfortable Lösung mit Vouchern immer die Aktivität eines Administrators erfordert, können Sie Ihren Nutzern alternativ die Möglichkeit einräumen, die Zugangsdaten zum drahtlosen Netzwerk eigenständig zu generieren und sich die Zugangsdaten per E-Mail oder SMS zusenden zu lassen (Anmeldung über "Smart Ticket").

Login nach Einverständniserklärung

Alternativ bietet das Gerät Ihnen die Möglichkeit, die Anmeldung für Public Spot-Nutzer völlig transparent über einen RADIUS-Server abzuwickeln. Der Benutzeranmeldung ist in diesem Fall eine Abfrage vorangestellt, bei der ein Nutzer zunächst der im Gerät hinterlegten Einverständniserklärung zustimmen muss, bevor er automatisch Zugang zum Public Spot erhalten. Ein nutzerseitiges Erstellen eigener Zugangsdaten via E-Mail oder SMS entfällt bei dieser Authentifizierungsmethode. Mehr hierzu erfahren Sie im betreffenden Abschnitt unter *Übersicht der Anmeldemodi* auf Seite 1311, da der "Login nach Einverständniserklärung" kein Bestandteil der Smart-Ticket-Funktion ist.

E-Mail-Anmeldung konfigurieren

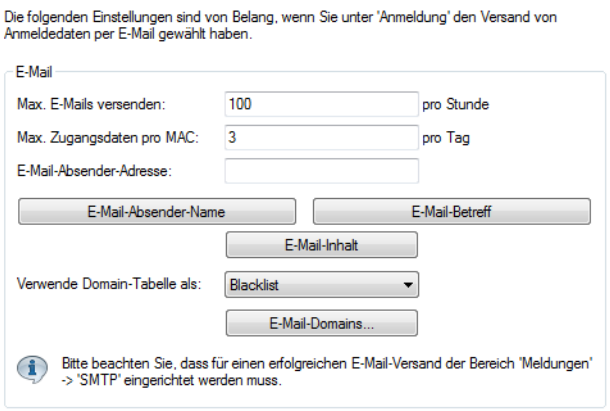
Die Einstellungen für den Versand der Anmeldedaten an das vom Benutzer angegebene E-Mail-Konto nehmen Sie im Dialog **Public-Spot** > **E-Mail** vor. Die nachfolgenden Schritte zeigen Ihnen, wie Sie die E-Mail-Anmeldung korrekt konfigurieren.

Für den erfolgreichen Versand der Anmeldedaten als E-Mail muss unter **Meldungen** > **SMTP-Konto** sowie **Meldungen** > **SMTP-Optionen** ein gültiges SMTP-Konto eingerichtet sein.

Darüber hinaus haben Sie in dem Dialog auch die Möglichkeit, individuelle Texte festzulegen, die das Gerät für den Versand der Anmeldedaten nutzt; siehe *Nachrichtentexte anpassen* auf Seite 1317. Standardmäßig setzt das Gerät vordefinierte Textbausteine ein; eine Übersicht dieser Standardtexte finden Sie unter *Standardtexte für E-Mail-Absender, -Betreff und -Inhalt* auf Seite 1318.

1. Starten Sie LANconfig und öffnen Sie den Konfigurationsdialog für das Gerät.
2. Wechseln Sie in die Ansicht **Public-Spot** > **Anmeldung**.
3. Ändern Sie den Anmeldungsmodus auf **Anmeldedaten werden über E-Mail versendet**.

4. Wechseln Sie in die Ansicht **Public-Spot** > **E-Mail**.



5. Tragen Sie im Eingabefeld **Max. E-Mails versenden** die maximale Anzahl an E-Mails ein, die das Public Spot-Modul innerhalb einer Stunde an Benutzer für die E-Mail-Anmeldung verschicken darf. Reduzieren Sie den Wert, um die Anzahl der neuen Benutzer pro Stunde zu verringen.
6. Geben Sie im Eingabefeld **Max. Zugangsdaten pro MAC** an, wie viele verschiedene Zugangsdaten das Gerät für eine MAC-Adresse innerhalb eines Tages bereitstellen darf.
7. Geben Sie im Eingabefeld **E-Mail-Absender-Adresse** die E-Mail-Adresse an, die dem zukünftigen Public Spot-Benutzer bei der Zustellung der E-Mail als Absenderadresse angezeigt wird, z. B. `support@providerX.org`.
8. Geben Sie über das Auswahlmenü **Verwende Domain-Tabelle als** an, ob das Gerät die Tabelle **E-Mail-Domains** als Blacklist oder Whitelist verwendet.

   Diese Definition bestimmt, welche E-Mail-Adressen bzw. Domains Ihre Public Spot-Benutzer zur Registrierung angeben dürfen.

   - **Blacklist**: Die Registrierung ist über alle E-Mail-Domains erlaubt bis auf diejenigen, die in dieser Tabelle stehen.
   - **Whitelist**: Die Registrierung ist ausschließlich über die E-Mail-Domains möglich, die in dieser Tabelle stehen.

   Bitte beachten Sie, dass der Public Spot bei einer leeren Domain-List als Whitelist alle Domains ablehnt.

9. Definieren Sie über die Tabelle **E-Mail-Domains** alle E-Mail-Domains, die Sie im Falle einer Anmeldung Ihrer Public Spot-Benutzer via E-Mail erlauben bzw. verbieten wollen. Geben Sie die Domains im Format `web-domain.de` an.
10. Schreiben Sie die Konfiguration zurück auf das Gerät.

SMS-Anmeldung konfigurieren

Die Einstellungen für den Versand der Anmeldedaten als Kurznachricht (SMS) an die vom Benutzer angegebene Rufnummer nehmen Sie im Dialog **Public-Spot** > **SMS** vor. Dabei können Sie – je nach Gerätetyp – zwischen mehreren Varianten wählen:

- Versand der Anmeldedaten als SMS über das geräteeigene 3G/4G WWAN-Modul;
- Versand der Anmeldedaten als SMS über das 3G/4G WWAN-Modul eines anderen Gerätes;
- Versand der Anmeldedaten als E-Mail an ein externes E-Mail2SMS-Gateway, welches die Umwandlung der E-Mail in eine SMS übernimmt.

LCOS überprüft die eingegebene Rufnummer auf ungültige Zeichen. Erlaubt sind ausschließlich Zahlen zwischen 0 und 9. Der Nutzer muss 5 bis 15 Zahlen (exklusive Landesvorwahl) eingeben.

Die nachfolgenden Schritte zeigen Ihnen, wie Sie die einzelnen Varianten der SMS-Anmeldung korrekt konfigurieren.

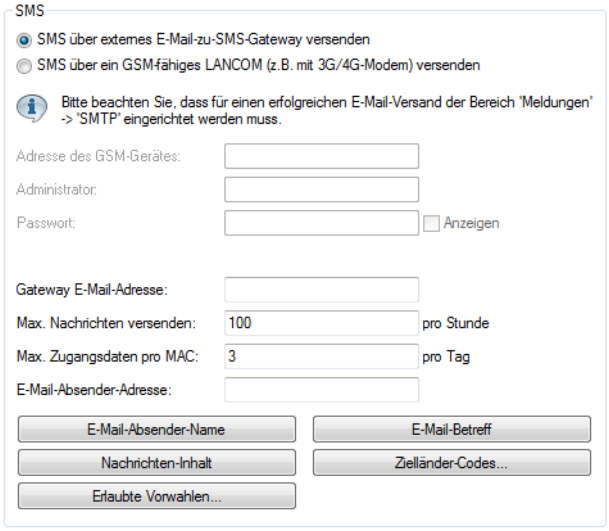
Für den erfolgreichen Versand der Anmeldedaten als Kurznachricht durch ein 3G/4G WWAN-fähiges Gerät muss unter **Meldungen** > **SMS-Nachrichten** dessen internes SMS-Modul eingerichtet sein, siehe *Basiskonfiguration des SMS-Moduls* auf Seite 1724.

Der SMS-Versand eignet sich für Installationen mit einem maximalen Durchsatz von 10 SMS pro Minute.

Für den erfolgreichen Versand der Anmeldedaten als E-Mail muss unter **Meldungen** > **SMTP-Konto** sowie **Meldungen** > **SMTP-Optionen** ein gültiges SMTP-Konto eingerichtet sein.

Darüber hinaus haben Sie in dem Dialog auch die Möglichkeit, individuelle Texte festzulegen, die das Gerät für den Versand der Anmeldedaten nutzt; siehe *Nachrichtentexte anpassen* auf Seite 1317. Standardmäßig setzt das Gerät vordefinierte Textbausteine ein; eine Übersicht dieser Standardtexte finden Sie unter *Standardtexte für E-Mail-Absender, -Betreff und -Inhalt* auf Seite 1318.

1. Starten Sie LANconfig und öffnen Sie den Konfigurationsdialog für das Gerät.
2. Wechseln Sie in die Ansicht **Public-Spot** > **Anmeldung**.
3. Ändern Sie den Anmeldungsmodus auf **Anmeldedaten werden über SMS versendet**.
4. Wechseln Sie in die Ansicht **Public-Spot** > **SMS**.



5. Legen Sie fest, auf welche Art und Weise der SMS-Versand erfolgt:

   - Für den Versand der Anmeldedaten als SMS über das geräteeigene 3G/4G WWAN-Modul, wählen Sie die Einstellung **SMS über internes GSM-Modem versenden** und fahren anschließend mit dem nächsten Konfigurations-Hauptschritt fort.
   - Für den Versand der Anmeldedaten als SMS über das 3G/4G WWAN-Modul eines anderen Gerätes, führen Sie zunächst die Schritte im Abschnitt *Geräte mit 3G/4G WWAN-Modul als SMS-Gateway einsetzen* auf Seite 1316 aus und fahren anschließend mit dem nächsten Konfigurations-Hauptschritt fort.
   - Für Versand der Anmeldedaten als E-Mail an ein externes E-Mail2SMS-Gateway, wählen Sie die Einstellung **SMS über externes E-Mail-zu-SMS-Gateway versenden** und fahren im Anschluss an die nachstehenden Unterschritte mit dem nächsten Konfigurations-Hauptschritt fort.

   a) Tragen Sie im Eingabefeld **Gateway E-Mail-Adresse** die IP-Adresse oder den Host-Namen des Gateway-Servers ein, der die E-Mail in eine SMS umwandelt. Erwartet der Provider die Mobilfunknummer im lokalen Teil der E-Mail, können Sie dafür die Variable `$PSpotUserMobileNr` verwenden.

   b) Geben Sie im Eingabefeld **E-Mail-Absender-Adresse** die E-Mail-Adresse an, die dem zukünftigen Public Spot-Benutzer bei der Zustellung der SMS als Absenderadresse angezeigt wird, z. B. `support@providerX.org`.

6. Tragen Sie im Eingabefeld **Max. Nachrichten versenden** die maximale Anzahl an Kurznachrichten ein, die das Public Spot-Modul innerhalb einer Stunde an Benutzer für die SMS-Anmeldung verschicken darf. Reduzieren Sie den Wert, um die Anzahl der neuen Benutzer pro Stunde zu verringen.
7. Geben Sie im Eingabefeld **Max. Zugangsdaten pro MAC** an, wie viele verschiedene Zugangsdaten das Gerät für eine MAC-Adresse innerhalb eines Tages bereitstellen darf.
8. Tragen Sie in die Tabelle **Zielländer-Codes** sämtliche Rufnummern ein, die der Public Spot für den Versand der Anmeldedaten über SMS akzeptiert.
   Die Eingabe eines Länder-Codes kann direkt oder mit vorangestellter Doppel-Null erfolgen, zum Beispiel für Deutschland `49` oder `0049`.

   Diese Tabelle agiert als Whitelist. Sie müssen Länder-Codes definieren, damit ein Versand der Login-Daten erfolgt.
9. Um den SMS-Versand auf bestimmte landesspezifische Vorwahlen zu beschränken, geben Sie die zulässigen Vorwahlen gefolgt von einem '*' in einer kommaseparierten Liste ein. Ein Beispiel für deutsche Mobilfunkanbieter: `15*, 16*, 17*`.

   Wenn Sie für ein Land hier keine Eintragung vornehmen, so werden alle landesspezifischen Vorwahlen zugelassen. Zu dem jeweiligen Land muss zuvor ein Eintrag in der Tabelle Erlaubte-Landesvorwahlen angelegt worden sein.
10. Schreiben Sie die Konfiguration zurück auf das Gerät.

Geräte mit 3G/4G WWAN-Modul als SMS-Gateway einsetzen

Sie haben bei der Public Spot-Anmeldung via SMS (Smart Ticket) die Möglichkeit, den Versand der Zugangsdaten über das 3G/4G WWAN-Modul eines anderen Gerätes anstelle eines externen E-Mail2SMS-Gateways abzuwickeln. Dazu hinterlegen Sie im Gerät, das den Public Spot bereitstellt, die Adresse und die Zugangsdaten des betreffenden 3G/4G-Gerätes. Für den Versand der SMS schickt das Public Spot-Modul dann via URL-Aufruf die Anmeldedaten und die Kurznachricht an das fremde 3G/4G-Gerät.

Die Option steht Ihnen sowohl auf Geräten ohne als auch mit eigenem 3G/4G WWAN-Modul zur Verfügung. Auf diese Weisen haben Sie z. B. die Möglichkeit, mehrere Geräte miteinander zu verketten und eine eigene Versandeinheit einzurichten, falls Sie Public Spot auf einem Gerät ohne 3G/4G WWAN-Modul und / oder mehrere Public Spots betreiben.

1. Starten Sie LANconfig und richten Sie auf dem 3G/4G-Gerät, das als SMS-Gateway fungieren soll, dass SMS-Modul ein (siehe *Basiskonfiguration des SMS-Moduls* auf Seite 1724). Darüber hinaus empfiehlt es sich, für den Zugang einen separaten Administrator ohne Zugriffsrechte (Auswahl **Keine**) mit dem alleinigen Funktionsrecht **Senden von SMS** anzulegen.
2. Öffnen Sie den Konfigurationsdialog für das Gerät, das den Public Spot bereitstellt.

3. Wechseln Sie in die Ansicht **Public-Spot** > **SMS**.



4. Wählen Sie die Einstellung **SMS über ein GSM-fähiges Gerät (z. B. mit 3G/4G-Modem) versenden**.
5. Geben Sie in den Eingabefeldern **Administrator** und **Passwort** den Namen und das Passwort für den Administrator auf dem anderen 3G/4G-Gerät ein.
6. Geben Sie im Eingabefeld **Adresse des GSM-Gerätes** die IP-Adresse ein, unter der das andere 3G/4G-Gerät für den Public Spot erreichbar ist.

Nachrichtentexte anpassen

Standardmäßig setzt das Gerät für den Inhalt der versendeten E-Mails oder Kurznachrichten vordefinierte Textbausteine ein; eine Übersicht dieser Standardtexte finden Sie unter *Standardtexte für E-Mail-Absender, -Betreff und -Inhalt* auf Seite 1318. Sie haben aber auch die Möglichkeit, eigene Texte zu definieren.

Sofern Sie für eine Sprache keinen individuellen Text spezifizieren, trägt das Gerät automatisch den geräteinternen Standardtext ein.

1. Starten Sie LANconfig und öffnen Sie den Konfigurationsdialog für das Gerät.
2. Wechseln Sie – je nach gewähltem Anmeldungsmodus – in die Ansicht **Public-Spot** > **E-Mail** bzw. **SMS**.
3. Geben über die Schaltfläche **E-Mail-Absender-Name** zu den verfügbaren Sprachen einen individuellen Absendernamen an, den die vom Public Spot zugestellten E-Mails bzw. Kurznachrichten tragen, z. B. `Provider X`.
4. Geben über die Schaltfläche **E-Mail-Betreff** zu den verfügbaren Sprachen eine individuelle Betreffzeile an, die das Public Spot-Modul für seine E-Mails bzw. Kurznachrichten verwendet. Die dabei zur Verfügungen stehenden Steuerzeichen entnehmen Sie dem Abschnitt *Verfügbare Variablen und Steuerzeichen* auf Seite 1317.
5. Geben über die Schaltfläche **E-Mail-Inhalt** bzw. **Nachrichteninhalt** zu den verfügbaren Sprachen einen individuellen Text an, den das Public Spot-Modul für seine E-Mails bzw. Kurznachrichten verwendet. Die dabei zur Verfügungen stehenden Variablen und Steuerzeichen entnehmen Sie dem Abschnitt *Verfügbare Variablen und Steuerzeichen* auf Seite 1317.
6. Schreiben Sie die Konfiguration zurück in das Gerät.

Verfügbare Variablen und Steuerzeichen

Für die Individualisierung der Standardtexte von Smart Ticket stehen Ihnen verschiedene Variablen und Steuerzeichen zur Verfügung. Die Variablen werden vom Public Spot-Modul beim Versand der E-Mail an den Benutzer bzw. das SMS-Gateway automatisch mit Werten gefüllt.

Variablen

Folgende Variablen stehen Ihnen im Eingabefeld **E-Mail-Inhalt** zur Verfügung:

`$PSpotPasswd`

Platzhalter für das nutzerspezifische Passwort des Public Spot-Zugangs.

`$PSpotLogoutLink`

Platzhalter für die Abmelde-URL des Public Spots in der Form `http://<IP-Adresse des Public Spots>/authen/logout`. Über diese URL hat ein Public Spot-Benutzer die Möglichkeit, sich vom Public Spot abzumelden, falls nach einem erfolgreichen Login das Sitzungsfenster – welches diesen Link ebenfalls enthält – z. B. vom Browser geblockt oder vom Benutzer geschlossen wird.

Steuerzeichen

Der Text in den Eingabefeldern **E-Mail-Betreff** und **E-Mail-Inhalt** darf auch folgende Steuerzeichen enthalten:

`\n`

CRLF (Carriage Return, Line Feed)

`\t`

Tabulator

`\<ASCII>`

ASCII-Code des entsprechenden Zeichens

Verlangt der E-Mail2SMS-Provider eine Variable, in der ein Backslash ("\") vorkommt, müssen Sie diesem ein weiteres "\" voranstellen. Dies unterbindet die Umwandlung des "\" durch LCOS.

Standardtexte für E-Mail-Absender, -Betreff und -Inhalt

Wenn Sie im Dialog **Public-Spot** > **E-Mail** oder. **SMS** zu einer Sprache für das jeweilige Eingabefeld keinen individuellen Text angeben, greift das Gerät beim Generieren der E-Mail automatisch auf die im LCOS hinterlegten Standardtexte zurück. Die verwendete Sprache ist dabei abhängig von der Spracheinstellung des Browsers, den der Benutzer für die Registrierung verwendet hat. Sofern zu einer Sprache keine geräteinternen Standardtexte vorliegen, setzt das Gerät die englischen Texte ein.

Tabelle 34: Übersicht der geräteinternen Standardtexte für die Anmeldung über E-Mail/SMS

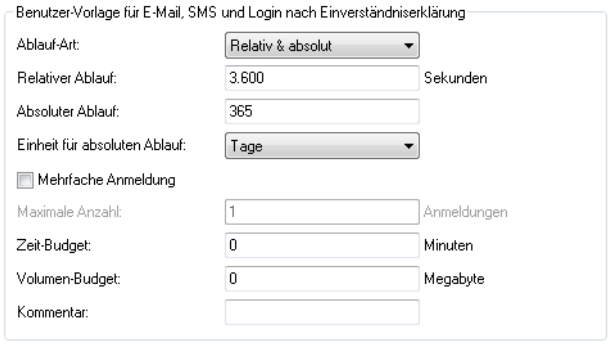
	E-Mail-Absender-Name	E-Mail-Betreff	E-Mail-Inhalt
Deutsch	Public Spot	Ihre Anmeldedaten für den Public Spot	Ihr Passwort für den Public Spot: $PSpotPasswd $PSpotLogoutLink
Englisch	Public Spot	Your Public Spot account	Your password for the Public Spot: $PSpotPasswd $PSpotLogoutLink

Standardwerte für die Benutzer-Vorlage setzen

Der nachfolgende Abschnitt beschreibt, wie Sie die Standardwerte für die **Benutzer-Vorlage** an Ihre Bedürfnisse anpassen. Das Gerät verwendet die hier definierten Werte als Vorgabewerte beim Anlegen neuer Benutzer über Smart-Ticket und dem Login nach Einverständniserklärung. Sofern Sie also den Versand der Anmeldedaten über E-Mail/SMS oder den Login nach Einverständniserklärung als Anmeldungsmodus gewählt haben, enthält jeder neue Benutzer-Account die von der Benutzer-Vorlage vorgegebenen Befugnisse und Einschränkungen.

1. Starten Sie LANconfig und öffnen Sie den Konfigurationsdialog für das Gerät.

2. Wechseln Sie in die Ansicht **Public-Spot** > **Assistent**.



3. Füllen Sie die Eingabefelder im Abschnitt **Benutzer-Vorlage** entsprechend Ihren Vorstellungen aus:

Ablauf-Art

Über diesen Eintrag definieren Sie, auf welche Art ein automatisch angelegtes Public Spot-Benutzerkonto abläuft. Sie können festlegen, ob die Gültigkeitsdauer eines Benutzer-Accounts absolut (fester Zeitpunkt) und / oder relativ (Zeitspanne ab dem ersten erfolgreichen Login) ist. Wenn Sie beide Werte auswählen, hängt der Ablaufzeitpunkt davon ab, welcher Fall als Erstes eintritt.

Relativer Ablauf

Über diesen Eintrag definieren Sie die relative Ablaufzeit eines automatisch angelegten Benutzerkontos (in Sekunden). Der von Ihnen gewählte **Ablauf-Typ** muss ein `relativ` beinhalten, damit diese Einstellung greift. Die Gültigkeit des Kontos endet nach der in diesem Feld angegebenen Zeitspanne nach dem ersten erfolgreichen Login des Benutzers.

Absoluter Ablauf

Über diesen Eintrag definieren Sie die absolute Ablaufzeit eines automatisch angelegten Benutzerkontos (in Tagen). Die von Ihnen gewählte **Ablauf-Art** muss ein `absolut` beinhalten, damit diese Einstellung greift.

Die Gültigkeit des Kontos endet zu dem in diesem Feld angegebenen Zeitpunkt, hochgerechnet vom Tag der Kontoerstellung.

Einheit für absoluten Ablauf

Um kürzere Ablaufzeiten zu konfigurieren, wählen Sie im Dropdown-Menü die Einheit für den absoluten Ablauf aus. Passen Sie ggf. den Wert des absoluten Ablaufes an.

Mehrfache Anmeldung

Über diesen Eintrag erlauben bzw. verbieten Sie ganz allgemein, ob Nutzer eines automatisch erstellten Accounts mehrere Geräte gleichzeitig mit den selben Zugangsdaten am Public Spot anmelden dürfen. Die erlaubte Menge der gleichzeitig angemeldeten Geräte legen Sie über das Eingabefeld **Maximale Anzahl** fest.

Maximale Anzahl

Über diesen Eintrag legen Sie die maximale Anzahl der Geräte fest, die gleichzeitig unter einem automatisch erstellten Account angemeldet sein dürfen. Der Wert `0` steht dabei für 'unbegrenzt'. Damit diese Einstellung greift, muss gleichzeitig der Parameter **Mehrfache Anmeldung** aktiviert sein.

Zeit-Budget

Über diesen Eintrag definieren Sie das Zeit-Budget, welches automatisch angelegte Benutzer erhalten. Der Wert `0` deaktiviert die Funktion.

Volumen-Budget

Über diesen Eintrag definieren Sie das Volumen-Budget, welches automatisch angelegte Benutzer erhalten. Der Wert `0` deaktiviert die Funktion.

Kommentar

Über diesen Eintrag vergeben Sie einen Kommentar oder Infotext, mit dem der RADIUS-Server ein automatisch erstelltes Benutzerkonto versieht.

4. Optional: Verändern Sie bei Bedarf das **Muster für Benutzernamen** sowie die **Passwort-Länge**. Das Gerät benutzt in den o. g. Anmeldungsmodi die betreffenden *Vorgabewerte des Benutzer-Erstellungs-Assistenten*, um automatisch einen Benutzernamen und ein Passwort zu generieren.
5. Schreiben Sie die Konfiguration zurück auf das Gerät.

15.2.4.3 Automatisches Re-Login

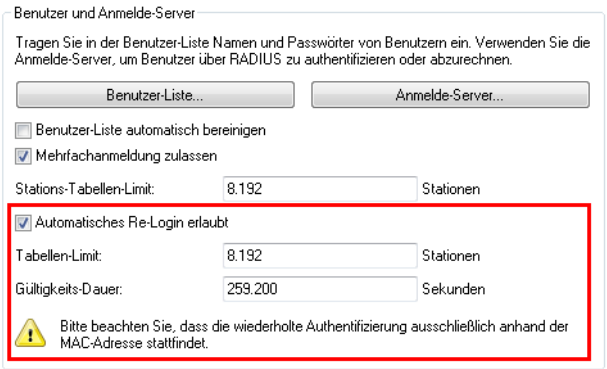
Mobile WLAN-Clients (z. B. Smartphones und Tablett-PCs) buchen sich automatisch in bekannte WLAN-Netze (SSID) ein, wenn sie erneut deren Funkzelle erreichen. Viele Apps greifen in diesem Fall automatisch ohne Umweg über den Webbrowser auf Webinhalte zu, um aktuelle Daten abzufragen (z. B. E-Mails, Soziale Netzwerke, Wetterbericht, etc.). Ähnliches gilt für mobile LAN-Clients (z. B. Notebooks), welche für einen Ortswechsel (z. B. in einer Hochschule dem Wechsel zwischen Hörsaal und Bibliothek) kurzzeitig vom Netz getrennt werden müssen. In allen Fällen ist es unpraktisch, wenn der Benutzer sich zunächst erneut im Browser manuell an einem Public Spot autorisieren muss.

Mit dem automatischen Re-Login genügt es, wenn der Benutzer sich einmalig am Public Spot identifiziert. Nach einer temporären Abwesenheit kann der Benutzer anschließend nahtlos weiter den Public Spot nutzen.

Der Public Spot protokolliert sowohl die manuelle An- und Abmeldung sowie einen Re-Login im SYSLOG. Dabei speichert er für einen Re-Login dieselben Anmeldedaten, die der Benutzer für die erstmalige Authentifizierung verwendet hat.

Die Authentifizierung erfolgt ausschließlich über die MAC-Adresse des Clients, wenn Re-Login aktiviert ist. Da das zu Sicherheitsproblemen führen kann, ist Re-Login standardmäßig deaktiviert.

Die Einstellungen für das automatische Re-Login finden sich bei LANconfig in der Geräte-Konfiguration unter **Public-Spot** > **Benutzer** im Abschnitt **Benutzer und Anmelde-Server**.



Das Auswahlkästchen **Automatische Wiederanmeldung (Auto-Re-Login) erlaubt** aktiviert diese Funktion.

Im Feld **Auto-Re-Login-Tabellen-Limit** bestimmen Sie die Anzahl der Clients (maximal 65536), die die Funktion Re-Login nutzen dürfen.

Im Feld **Auto-Re-Login-Gültigkeitsdauer** bestimmen Sie, wie lange der Public Spot die Anmeldedaten eines Clients für ein Re-Login in der Tabelle speichert. Nach Ablauf dieser Frist muss sich der Public Spot-Benutzer erneut über den Browser auf der Anmeldeseite des Public Spots anmelden.

15.2.4.4 Automatische Authentifizierung mit der MAC-Adresse

Ein Public Spot gewährt einem Benutzer nach erfolgreicher Authentifizierung den Zugang zu bestimmten Diensten. Zur Authentifizierung zeigt der Public Spot dem Benutzer nach dem Öffnen des Browsers üblicherweise eine Webseite. Der Benutzer gibt in dieser Anmeldeseite seine Benutzerdaten ein, der Public Spot leitet den Benutzer dann auf die erlaubten Webseiten weiter.

In manchen Anwendungsfällen ist die Authentifizierung über eine Webseite nicht erwünscht oder nicht möglich, wie die folgenden Beispiele zeigen:

- Das Endgerät verfügt nicht über einen Browser und kann daher die Anmeldeseite nicht öffnen.
- Der manuelle Aufruf der Anmeldeseite ist z. B. für einen Performance-Test zu langwierig.

Die automatische Authentifizierung am Public Spot mit der MAC-Adresse erlaubt die Nutzung des Public Spot ohne den vorherigen Aufruf der Anmeldeseite. Dazu trägt der Administrator alle MAC-Adressen der entsprechenden Endgeräte in die Tabelle der erlaubten MAC-Adressen unter **Public-Spot** > **Benutzer** > **MAC-authentifizierte Benutzer** ein.

Ablauf der MAC-Adress-Prüfung

Wenn das Gerät die Anfrage eines Clients empfängt, vollzieht der Public Spot bei der automatischen Authentifizierung mit der MAC-Adresse folgende Schritte:

- Wenn der Public Spot die MAC-Adresse der empfangenen Datenpakete bereits authentifiziert hat, leitet das Gerät die zugehörigen Datenpakete weiter.
- Wenn die MAC-Adresse in der Liste der erlaubten Clients enthalten ist, startet der Public Spot eine neue Sitzung für diesen Benutzer und leitet die zugehörigen Datenpakete weiter.
- Wenn ein Provider für die Prüfung der MAC-Adressen über RADIUS definiert und eine positive, noch gültige Authentifizierung für die MAC-Adresse im Public Spot-Cache gespeichert ist, startet der Public Spot eine neue Sitzung für diesen Benutzer und leitet die zugehörigen Datenpakete weiter.
- Wenn ein Provider für die Prüfung der MAC-Adressen über RADIUS definiert, jedoch keine gültige Authentifizierung für die MAC-Adresse im Cache des Public Spot gespeichert ist, leitet der Public Spot die Authentifizierung der MAC-Adresse bei dem entsprechenden RADIUS-Server ein. Nach einer positiven Antwort startet der Public Spot eine neue Sitzung für diesen Benutzer und leitet die zugehörigen Pakete weiter.
- Sind alle zuvor beschriebenen Prüfungen erfolglos, leitet der Public Spot den Benutzer an die Anmeldeseite weiter.

Authentifizierung der MAC-Adresse über RADIUS

Wenn die MAC-Adresse eines anfragenden WLAN-Clients nicht in der Liste der erlaubten Adressen enthalten ist, kann der Public Spot die Adresse alternativ über einen RADIUS-Server authentifizieren.

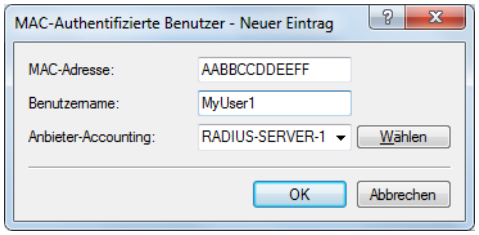
Zur Aktivierung dieser RADIUS-Authentifizierung wählt der Administrator einen der im Gerät definierten RADIUS-Server aus der Anbieter-Liste aus.

Zusätzlich definiert der Administrator eine Lebensdauer für die abgelehnten MAC-Adressen. Mit dieser Lebensdauer verhindert der Public Spot das Fluten des RADIUS-Servers mit wiederholten Anfragen nach MAC-Adressen, die weder über die MAC-Adress-Tabelle noch über den RADIUS-Server ohne Anmeldung authentifiziert werden können.

Wenn eine MAC-Adresse bei einer Anfrage zur Authentifizierung über den RADIUS-Server abgelehnt wird, speichert der Public Spot diese Ablehnung für die definierte Lebensdauer. Weitere Anfragen für die gleiche MAC-Adresse beantwortet der Public Spot innerhalb der Lebensdauer direkt ohne Weiterleitung an den RADIUS-Server.

Konfiguration in LANconfig

Bei der Konfiguration mit LANconfig finden Sie die Parameter für die Authentifizierung der Clients über die MAC-Adresse im Dialog **Public-Spot** > **Benutzer** > **MAC-Authentifizierte Benutzer**.



15.2.4.5 Automatische Anmeldung über WISPr

Ihr Gerät stellt eine Schnittstelle für die Anmeldung über WISPr bereit. Der **WISPr**-Standard ist der technologische Vorläufer der 802.11u- und Hotspot-2.0-Spezifikation. Die Abkürzung steht für **Wireless Internet Service Provider Roaming** und bezeichnet sowohl ein Verfahren als auch Protokoll, welches Nutzern von WLAN-fähigen Endgeräten dazu ermöglicht, zwischen den WLANs unterschiedlicher Betreiber – respektive deren Internet-Service-Provider – unterbrechungsfrei zu roamen. Die Idee dahinter ähnelt somit der von 802.11u und Hotspot 2.0, erfordert allerdings eine umfassendere Betreuung durch den jeweiligen Nutzer.

Über das WISPr-Protokoll können Sie Endgeräten, für die herstellerseitig keine Unterstützung für Hotspot 2.0 mehr angeboten wird, eine Hotspot-2.0-ähnliche Anmeldung und Netzwerknutzung über Ihren Hotspot ermöglichen. Voraussetzung ist, dass Ihr Service-Provider die dazugehörige Infrastruktur bereitstellt. Nutzerseitig erfolgt die Unterstützung entweder über das verwendete Betriebssystem oder eine geeignete App (Smart-Client). Dieser Client übernimmt für den Nutzer die Authentifizierung am Hotspot; liegen für das betreffende Netzwerk keine Authentifizierungsdaten vor, fragt der Client den Nutzer auf Systemebene nach gültigen Zugangsdaten. Für den Nutzer entfällt somit in jedem Fall die Anmeldung über eine Login-Seite in seinem Browser.

Aufgrund seines Alters unterstützen fast alle aktuelle Endgeräte mit iOS, Android und Windows 8 das WISPr-Protokoll. Darüber hinaus bieten größere WLAN-Internet-Service-Provider häufig auch eigene Apps an, um Ihren Kunden die Anmeldung zu erleichtern: Diese Apps beeinhalten eine vorkonfigurierte Datenbank der Provider-eigenen Hotspots und – optional – der Hotspots seiner Roaming-Partner. Der Ablauf der Authenifizierung entspricht dann dem folgenden Schema:

1. Ein Kunde installiert als Client die Hotspot-App seines Providers, welche in einer Datenbank vorkonfigurierte Hotspot-SSIDs bereitstellt.
2. Der Client verbindet sich automatisch mit einem dieser Hotspots und sendet einen HTTP-GET-Request an eine beliebige URL, um zu testen, ob ein direkter Internetzugriff besteht oder der Public Spot eine Authentifizierung anfordert.
3. Der Hotspot sendet im HTTP-Redirect ein WISPr-XML-Tag mit der Login-URL.
4. Der Client sendet in einem HTTP-Post seine Anmeldedaten an die Login-URL.

Beispiel für XML-Tag im Redirect:

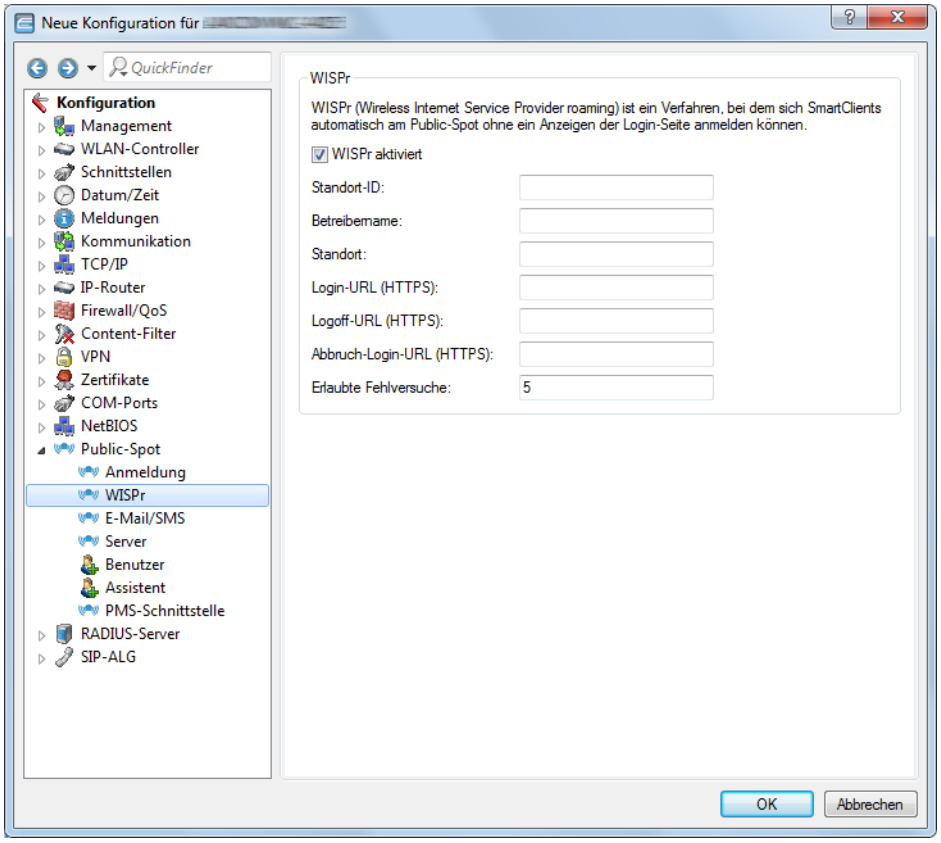
```
<HTML>
<?xml version="1.0" encoding="UTF-8"?>
  <WISPAccessGatewayParam xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xsi:noNamespaceSchemaLocation="http://www.acmewisp.com/WISPAccess GatewayParam.xsd">
    <Redirect>
      <AccessProcedure>1.0</AccessProcedure>
      <AccessLocation>Hotel Contoso Guest Network</AccessLocation>
      <LocationName>Hotel Contoso</LocationName>
      <LoginURL>https://captiveportal.com/login</LoginURL>
      <MessageType>100</MessageType>
      <ResponseCode>0</ResponseCode>
    </Redirect>
   </WISPAccessGatewayParam>
</HTML>
```

Für die Nutzung von WISPr sind zwingend ein SSL-Zertifikat und ein Private-Key im Gerät erforderlich. Das Zertifikat muss entweder von einer vertrauenswürdigen Stelle signiert oder – sofern Sie ein selbst-signiertes

Zertifikat verwenden – im Client als vertrauenswürdig importiert sein. Ansonsten verweigert ein Client das Login via WISPr. Weitere Informationen zum Laden dieser Objekte in Ihr Gerät finden Sie im LANCOM Techpaper "Zertifikatsmanagement im Public Spot", erhältlich unter *www.lancom-systems.de*.

WISPr konfigurieren

Die WISPr-Funktion Ihres Gerätes konfigurieren Sie über den Dialog **Public-Spot** > **WISPr**.



In diesem Dialog haben Sie folgende Einstellungsmöglichkeiten:

- **WISPr aktiviert**: Aktivieren oder deaktivieren Sie die WISPr-Funktion für das Gerät.
- **Standort-ID**: Vergeben Sie hierüber eine eindeutige Standort-Nummer oder -Kennung für Ihr Gerät, z. B. in der Form `isocc=<ISO_Country_Code>,cc=<E.164_Country_Code>,ac=<E.164_Area_Code>,network=<SSID/ZONE>`.
- **Betreibername**: Geben Sie hier den Namen des Hotspot-Betreibers ein, z. B. `providerX`. Diese Angabe hilft dem Nutzer bei der manuellen Auswahl eines Internet-Service-Providers.
- **Standort**: Beschreiben Sie den Standort Ihres Gerätes, z. B. `CafeX_Markt3`. Diese Angabe dient einem Nutzer zur besseren Identifizierung Ihres Hotspots.
- **Login-URL (HTTPS)**: Geben Sie die HTTPS-Adresse ein, an die die WISPr-Client die Zugangsdaten für Ihren Internet-Service-Provider übermittelt. Es kann hier eine beliebige externe URL angegeben werden oder der Public Spot selbst. Falls der Public Spot selbst Benutzer über WISPr authentifizieren soll geben Sie die URL an in der Form `https://<Device-FQDN>/wisprlogin`. Für "wisprlogin" im Beispiel kann eine beliebige, frei definierbare Sub-URL verwendet werden.
- **Logoff-URL (HTTPS)**: Geben Sie die HTTPS-Adresse ein, über die sich ein WISPr-Client von Ihrem Internet-Service-Provider abmeldet. Es gelten die gleichen Regeln wie bei der Login-URL.

- **Abbruch-Login-URL (HTTPS)**: Geben Sie die HTTPS-Adresse ein, an die das Gerät einen WISPr-Client weiterleitet, wenn die Authentifizierung fehlschlägt. Es gelten die gleichen Regeln wie bei der Login-URL.

  Die drei URLs müssen unterschiedlich sein, falls der Public Spot im Gerät verwendet wird, z. B.:

  - Login-URL: https://<Device-FQDN>/wisprlogin
  - Logoff-URL: https://<Device-FQDN>/wisprlogoff
  - Abbruch-Login-URL: https://<Device-FQDN>/wisprabort

  Ausschließlich zu Testzwecken können Sie auch eine URL mit IP-Adressen konfigurieren. In einem Produktiv-System wird ein Client den FQDN des Zertifikates prüfen!

- **Erlaubte Fehlversuche**: Geben Sie hier die Anzahl der Fehlversuche ein, welche die Login-Seite Ihres Internet-Service-Providers maximal erlaubt. Wenn der Public Spot verwendet wird, verweigert der Public Spot nach dieser Anzahl der Fehlversuche weitere Logins vom betreffenden Client.

15.2.4.6 IEEE 802.11u und Hotspot 2.0

Ihr Gerät unterstützt WLAN-Verbindungen nach dem IEEE-Standard 802.11u und – darauf aufbauend – die Hotspot-2.0-Spezifikation. Über 802.11u haben Sie die Möglichkeit, in einem lokalen WLAN-Netzwerk (z. B. innerhalb Ihrer Firma) oder einem Public Spot-Netzwerk die automatische Authentisierung und Authentifizierung Ihrer Nutzer zu realisieren. Voraussetzung dafür ist, dass die betreffenden Stationen (Smartphones, Tablet-PCs, Notebooks, usw.) Verbindungen nach 802.11u und Hotspot 2.0 auch unterstützen. Folgende Funktionen bieten sich Ihnen im Detail:

- **Automatische Netzwerkwahl**

  In einer 802.11u-fähigen Umgebung entfällt für einen Benutzer die manuelle Suche und Auswahl einer SSID. Stattdessen übernehmen die Stationen eigenständig die Suche und Auswahl eines geeigneten Wi-Fi-Netzwerks, indem sie selbstständig die Betreiber- und Netzwerkdaten aller 802.11u-fähigen Access Points in Reichweite erfragen und auswerten. Eine vorangehende Anmeldung am Access Point ist dabei nicht erforderlich.

  Mit Hotspot 2.0 erhalten Stationen überdies die Möglichkeit, Informationen über die in einem Wi-Fi-Netzwerk verfügbaren Dienste abzurufen. Sind spezifische, für einen Benutzer aber relevante Dienste (z. B. Verbindungen via HTTP, VPN oder VoIP) für ein Wi-Fi-Netzwerk nicht verfügbar, werden alle Netzwerke, die die Kriterien nicht erfüllen, von der weiteren Suche ausgeschlossen. Somit ist sichergestellt, dass Nutzer immer das für sie optimale Netzwerk erhalten.

- **Automatische Authentisierung und Authentifizierung**

  In einer 802.11u-fähigen Umgebung übernimmt die Station automatisch die Anmeldung des Benutzers, sofern die notwendigen Zugangsdaten vorliegen. Die Authentifizierung kann z. B. anhand einer SIM-Karte, eines Benutzernamens und Passworts, oder eines digitalen Zertifikats erfolgen. Ein manuelles und wiederholtes Eingeben der Zugangsdaten in eine Anmeldemaske durch den Benutzer entfällt. Nach erfolgreicher Authentifizierung kann der Nutzer die benötigten Dienste unmittelbar nutzen.

- **Unterbrechungsfreie Verbindungsübergabe (Seamless Handover)**

  Verbindungen nach 802.11u ermöglichen im Zusammenspiel mit 802.21 die unterbrechungsfreie Übergabe von Datenverbindungen über verschiedene Netzwerktypen hinweg. Dies erlaubt es Nutzern, mit ihren Stationen aus dem Mobilfunknetz unterbrechungsfrei in ein WLAN-Netz zu wechseln, sobald sie in den Empfangsbereich einer entsprechenden Hotspot-2.0-Zone kommen – und umgekehrt. Gleiches gilt für den Wechsel zwischen verschiedenen Betreibern, wenn Nutzer z. B. während einer Busfahrt von einem homogenen Netzwerk in ein anderes wechseln.

- **Automatisches Roaming**

  Verbindungen nach 802.11u ermöglichen das Roaming über unterschiedliche Betreibernetzwerke hinweg. Gelangt ein Benutzer in die Hotspot-2.0-Zone eines Betreibers, für den er keine Authentifizierungsdaten besitzt, besteht für seine Station dennoch die Option, in das Heimnetzwerk zu roamen. Die Authentifizierung an der fremden Hotspot-2.0-Zone erfolgt dann durch den Roaming-Partner des Betreibers, was den Nutzer schließlich zur Nutzung des fremden Wi-Fi-Netzwerks berechtigt. Neben Gebieten, in denen nur einzelne Netzwerkbetreiber mit Acess Points präsent sind, gewinnt diese Möglichkeit vor allem auch für Auslandsreisende an Attraktivität.

Beispiel: Angenommen, ein Nutzer ist mit seinem 802.11u-fähigen Smartphone (seiner Station) in der Stadt unterwegs und aktiviert die WLAN-Funktion, um im Internet zu surfen. Die Station beginnt daraufhin damit, alle verfügbaren Wi-Fi-Netzwerke in der Umgebung zu suchen. Bietet ein Teil der dazugehörigen Access Points 802.11u an, wählt die Station anhand der vorab erhaltenen Betreiber- und Netzinformationen dasjenige Netzwerk aus, welches am besten zum benötigten Dienst passt – z. B. einen Hotspot der eigenen Mobilfunkgesellschaft mit Internetfreigabe. Die anschließende Authentifizierung kann in diesem Fall automatisch über die SIM-Karte erfolgen, sodass der Benutzer während des gesamten Vorgangs nicht mehr einzugreifen braucht. Die für die Verbindung gewählte Verschlüsselungsmethode – z. B. WPA2 – bleibt davon unberührt.

Zusammengefasst verknüpfen Datenverbindungen nach 802.11u und mit aktiviertem Hotspot 2.0 die Sicherheitsmerkmale und Leistungsfähigkeit klassischer Wi-Fi-Hot-Spots mit der Flexibilität und Einfachheit von Datenverbindungen über Mobilfunk. Zeitgleich entlasten sie die Mobilfunknetzwerke, indem sie den Datenverkehr (und ggf. auch die Telefonie) auf die Netzstrecken und Frequenzbänder der Access Points umverteilen.

Passpoint® Release 2

Ab LCOS 10.40 ist die erweiterte Hotspot 2.0-Funktionalität Ihres WLAN-Gerätes nach dem von der Wi-Fi Alliance spezifizierten Passpoint® Release 2 konfigurierbar. Der im LCOS integrierte RADIUS-Server beinhaltet ab Version 10.32 RU4 die benötigten Features.

Passpoint® Release 2 vereinfacht das Onboarding von Geräten in ein Netz mit der Verschlüsselungsmethode WPA2-Enterprise (802.1X). Mittels eigener Onboarding-SSID kann ein Benutzer sich ein Profil auf Passpoint® Release 2-fähige Endgeräte installieren und dann automatisch mit den hinterlegten Anmeldedaten ins verschlüsselte Netz wechseln. Somit lassen sich Hotspots realisieren, die verschlüsselte drahtlose Kommunikation ermöglichen. Hierbei können die Gäste über eine offene Onboarding-SSID mit zeitlich begrenzten Zugangsdaten ausgestattet werden.

Ebenso kann ein Mobilfunkanbieter sein Mobilfunknetz entlasten, indem er Wi-Fi Offloading einführt und mobile Endgeräte, die mit einer SIM-Karte ausgestattet sind, automatisch in sein WLAN-Netz einbuchen lässt. Die Endgeräte der Kunden finden das WLAN-Netz des Mobilfunkanbieters automatisch und buchen sich mit den hinterlegten Benutzerdaten der SIM-Karte automatisch in das WLAN-Netz des Betreibers ein.

Mit Passpoint® Release 2 wird die Hotspot 2.0-Funktionalität um die folgenden Features erweitert:

- Online Sign-Up (OSU) – Mit Passpoint® Release 2 bekommen Unternehmen und Netzbetreiber die Möglichkeit, Benutzerprofile über einen so genannten „Online Sign-Up"-Server (OSU-Server) zur Verfügung zu stellen. Über eine offene OSU-SSID hat der Benutzer die Möglichkeit, verschiedene OSU-Server anhand von hinterlegten Icons zu identifizieren und somit den für ihn passenden auszuwählen. Der OSU-Server kann ggf. Benutzerdaten abfragen, bevor er ein passendes Profil für das Endgerät des Benutzers bereitstellt. Neben der offenen OSU-SSID kann auch eine verschlüsselte SSID genutzt werden, welche mittels „anonymous EAP-TLS" die Benutzerdaten verschlüsselt abfragt und bereitstellt. Hierfür wird ein entsprechender RADIUS-Server mit „anonymous EAP-TLS" Unterstützung benötigt.

  Ein OSU-Server ist kein Bestandteil des LCOS. Es gibt allerdings Lösungen von LANCOM Partnern.

- OSU-Icons – Für die unterstützten OSU-Server können im LCOS über die WEBconfig im Bereich **Dateimanagement** entsprechende Icons als Datei hochgeladen werden. Als Dateiformat empfehlen wir PNG.
- Benachrichtigungsmöglichkeit – Auf Netzseite gibt es die Möglichkeit, den Benutzer zu benachrichtigen, wenn eine Abmeldung seitens RADIUS-Server kurz bevor steht. Dies kann z. B. der Fall sein, wenn die Benutzerdaten nicht mehr länger gültig sind oder die festgelegte Verbindungsdauer erreicht wurde.
- QoS Map – Ein Access Point kann über die Funktion „QoS Map Set" seine Clients anweisen, eine bestimmte QoS Map zu verwenden. Hierbei werden die Werte für das Contention Window (Medienzugriff via EDCA) der verschiedenen Access Categories für Voice, Video, Best Effort und Background-Datenpakete und deren zugehörige DSCP-Werte definiert. Gleichzeitig nutzt auch der Access Points die in der QoS Map hinterlegten Werte.

  Aktuell stehen neben den zwei durch die Wi-Fi Alliance vorgegebenen QoS Maps nur die Standard-QoS-Map des LCOS zur Verfügung.

Hotspot-Betreiber und -Service-Provider

Die Hotspot-2.0-Spezifikation der Wi-Fi Alliance unterscheidet zwischen Hotspot-Betreibern und Hotspot-Service-Providern: Ein **Hotspot-Betreiber** unterhält lediglich ein Wi-Fi-Netzwerk, während ein **Hotspot-Service-Provider** (SP) die Verbindung der Nutzer ins Internet oder Mobilfunknetz realisiert. Natürlich ist es möglich, dass ein Betreiber gleichzeitig ein SP ist. In allen anderen Fällen jedoch benötigt ein Hotspot-Betreiber entsprechende Roaming-Vereinbarungen mit einem SP oder einem Zusammenschluss mehrerer SP (Roaming-Konsortium genannt). Erst wenn ein Betreiber diese Vereinbarungen getroffen hat, sind Kunden der entsprechenden Roaming-Partner dazu in der Lage, sich am Hotspot des Betreibers zu authentifizieren. Jeder Service-Provider betreibt dazu seine eigene AAA-Infrastruktur. Die Liste der möglichen Roaming-Partner und der Name des Hotspot-Betreibers teilt ein Hotspot den Stationen über ANQP mit (siehe Funktionsbeschreibung).

Funktionsbeschreibung

Bei 802.11u handelt es sich um den Basis-Standard der IEEE. Dieser Standard erweitert Access Points bzw. Hotspots im Wesentlichen um die Fähigkeit, sogenannte „ANQP-Datenpakete" (Advanced Message Queuing Protocol) in seinen Funksignalen auszustrahlen. ANQP ist ein Query / Response-Protokoll, mit dem ein Gerät eine Reihe von Informationen über den Hotspot abfragen kann. Hierzu gehören sowohl Metadaten, wie z. B. Angaben zum Betreiber und dem Standort, als auch Angaben zum dahinterliegenden Netzwerk, wie z. B. Angaben zu Betreiber-Domänen, Roaming-Partnern, den Authentifizierungsmethoden, Weiterleitungsadressen, usw. Alle 802.11u-fähigen Geräte in Reichweite haben die Möglichkeit, diese Datenpakete ohne vorangehende Anmeldung am Access Point abzufragen, um anhand ihrer die Netzwerkwahl und den -beitritt zu entscheiden.

Die Wi-Fi Alliance hat dem Standard weitere ANQP-Elemente hinzugefügt und vermarktet diese Spezifikation als **Hotspot 2.0**. Die Hotspot-2.0-Funktion ist somit lediglich eine Erweiterung des Standards um zusätzliche Elemente, die Geräte bei ihrer Netzwerkwahl als Kriterien heranziehen können. Hierzu gehören z. B. Angaben zu den am Hotspot verfügbaren Diensten und WAN-Metriken. Das dazugehörige Zertifizierungsprogramm heisst Passpoint®, welches in verschiedenen Ausbaustufen gibt. Bestimmte LANCOM Access Points sind von der Wi-Fi Alliance Passpoint® CERTIFIED (Release 1 und / oder 2).

ANQP-Datenpakete stellen also das zentrale Informationselement des 802.11u-Standards dar. Um die Unterstützung für 802.11u zu signalisieren und die Datenpakete zu übertragen, bedarf es allerdings noch weiterer Elemente, die für den Betrieb von 802.11u essentiell sind:

- Die Signalisierung der 802.11u-Unterstützung in den Beacons und Probes eines Hotspots erfolgt durch das sogenannte „Interworking-Element". In ihm sind bereits erste grundlegende Netzwerkinformationen – wie z. B. die Netzklassifikation, die Internetverfügbarkeit (Internet-Bit) und die OI des Roaming-Konsortiums und / oder des Betreibers – enthalten. Zugleich dient es 802.11u-fähigen Geräten als erstes Filterkriterium bei der Netzsuche.
- Die Übertragung der ANQP-Datenpakete erfolgt innerhalb der sogenannten GAS-Container. GAS steht für Generic Advertisement Service und bezeichnet generische Container, welche einem Gerät erlauben, vom Hotspot – ergänzend zu den Informationen in den Beacons – erweiterte interne und externe Informationen für die Netzwahl abzufragen. Die GAS-Container werden ihrerseits durch sogenannte Public Action Frames auf Layer 2 übermittelt.

Anmeldung eines 802.11u-fähigen Clients an einem Hotspot 2.0

Diese Funktionsbeschreibung erläutert schematisch Auswahl und Anmeldevorgang eines 802.11u-fähigen Geräts an einem Hotspot 2.0.

Anmeldung via Benutzername / Passwort oder digitalem Zertifikat

1. Die Hotspots antworten daraufhin mit einem ANQP-Response, der u. a. jeweils den Namen des Hotspot-Betreibers sowie eine Liste der NAI-Realms enthält, welche alle verfügbaren Roaming-Partner (Service-Provider, kurz SP) auflistet.
2. Das Gerät lädt die auf ihm lokal abgespeicherten Zugangsdaten aus den vom Benutzer eingerichten WLAN-Profilen oder installierten Zertifikaten, und gleicht die dortigen Realms mit den unter (2) erhaltenen NAI-Realm-Listen ab.
   a. Erzielt das Gerät hierbei einen Treffer, weiß es, dass es sich bei betreffenden Wi-Fi-Netzwerk erfolgreich authentisieren kann.

b. Erzielt das Gerät mehrere Treffer, erfolgt die Auswahl eines Wi-Fi-Netzwerks anhand einer vom Benutzer eingerichteten Präferenzliste. Diese Liste legt die Reihenfolge der bevorzugten Betreiber im Zusammenhang mit den möglichen Roaming-Partnern fest. Das Gerät vergleicht hierbei die unter (2) erhaltenen Betreiber-Namen mit der Liste und wählt jenen Betreiber aus, der die höchste Priorität besitzt.

3. Das Gerät authentisiert sich mit seinen lokalen Zugangsdaten am Hotspot des bevorzugten Betreibers für den passenden SP. Der Access Point übermittelt diese Daten seinerseits über die SSPN-Schnittstelle (Subscription Service Provider Network) an ein für die Authentifizierung zuständiges AAA-System. Die Authentisierung erfolgt dabei über die vom SP festgelegte Authentifizierungsmethode; bei der Authentisierung via Benutzername / Passwort umfasst dies EAP-TTLS, bei der Authentisierung via digitalem Zertifikat EAP-TLS.

Anmeldung via (U)SIM

1. Im Unterschied zur Anmeldung via Benutzername / Passwort oder digitalem Zertifikat fragt ein Gerät bei vorliegen einer (U)SIM in seinen ANQP-Requests nicht nach der Liste der NAI-Realms, sondern der 3GPP Cellular Network Information. In den ANQP-Responses beinhaltet diese Cellular-Netzwerk-Informations-Liste alle Mobilfunkanbieter, für die der Access Point eine Authentisierung ermöglicht.

2. Das Gerät lädt aus seiner lokalen (U)SIM-Karte die Kennwerte für das Mobilfunknetzwerk und gleicht diese Daten mit den erhaltenen Cellular-Netzwerk-Informations-Listen ab. Der Listenabgleich sowie die Auswahl eines bevorzugten Betreibernetzwerkes erfolgen synonym zur Anmeldung via Benutzername/Passwort oder digitalem Zertifikat.

3. Das Gerät authentisiert sich mit seinen lokalen Zugangsdaten am Hotspot des bevorzugten Betreibers für die passende Mobilfunkgesellschaft. Der Hotspot übermittelt diese Daten seinerseits über die SSPN-Schnittstelle (Subscription Service Provider Network) an ein für die Authentifizierung zuständiges AAA-System. Durch das Vorhandensein einer (U)SIM-Karte ändert sich die mögliche Authentifizierungsmethode für das Gerät zu EAP-SIM oder EAP-AKA.

4. Das AAA-System erkundigt sich für die Authentifizierung über die MAP-Schnittstelle (Mobile Application Part) beim HLR-Server (Home Location Register) der Mobilfunkgesellschaft, um die Zugangsdaten zu verifizieren.

Im Falle einer erfolgreichen Authentisierung erhält das Gerät den Zugriff auf das WLAN-Netzwerk entweder via Hotspot (Zugangsdaten für das Betreiber-Netzwerk liegen vor) oder automatischem Roaming (Zugangsdaten für das Betreiber-Netzwerk liegen nicht vor).

Stehen dem Gerät mehrere Authentifizierungsmöglichkeiten zur Auswahl (z. B. SIM-Karte und Benutzername / Passwort), hat es die Möglichkeit, anhand der NAI-Realm- bzw. Cellular-Netzwerk-Informations-Liste die bevorzugte EAP-Authentifizierungsmethode und damit die bevorzugten Zugangsdaten auszuwählen.

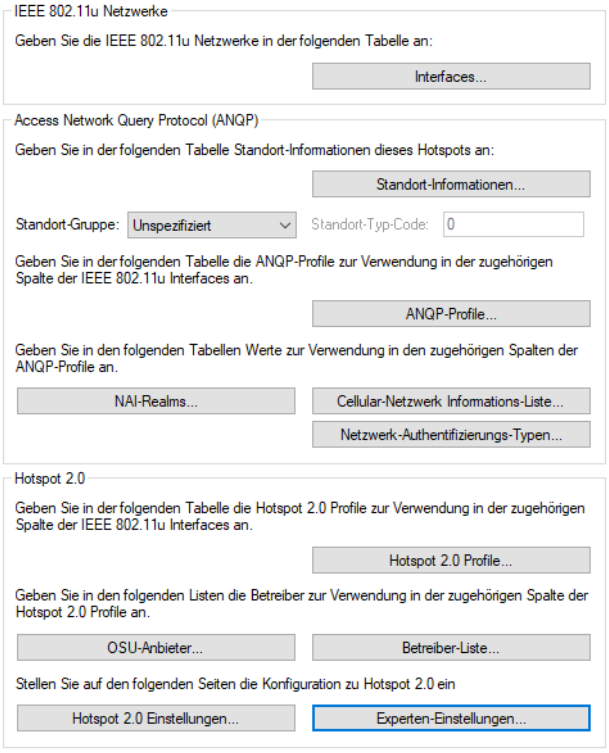
Empfohlene allgemeine Einstellungen

Die Hotspot-2.0-Spezifikation empfiehlt für den 802.11u-Betrieb folgende allgemeine Einstellungen:

- Aktivierte WPA2-Enterprise Sicherheit (802.1X)
- Authentifizierung via EAP mit der entsprechenden Variante:
  - EAP-SIM/EAP-AKA bei Authentifizierung mit SIM/USIM-Karte
  - EAP-TLS bei Authentifizierung mit digitalem Zertifikat
  - EAP-TTLS bei Authentifizierung mit Benutzername und Passwort
- Aktiviertes und eingerichtetes Proxy-ARP
- Deaktivierte Multicast- und Broadcasts in Funkzellen
- Nicht-zugelassener Datenverkehr zwischen den einzelnen mobilen Endgeräten (Layer-2 Traffic-Inspection & Filtering). Die dazugehörigen Schalter finden Sie im LANconfig unter **Wireless-LAN** > **Securtity** > **Datenverkehr zwischen SSIDs**.
- Aktivierte und eingerichtete Firewall auf dem Access-Router, welcher den Internetzugang zur Verfügung stellt

Konfigurationsmenü für IEEE 802.11u / Hotspot 2.0

Das Konfigurationsmenü für IEEE 802.11u und Hotspot 2.0 finden Sie unter **Wireless-LAN** > **IEEE 802.11u**.



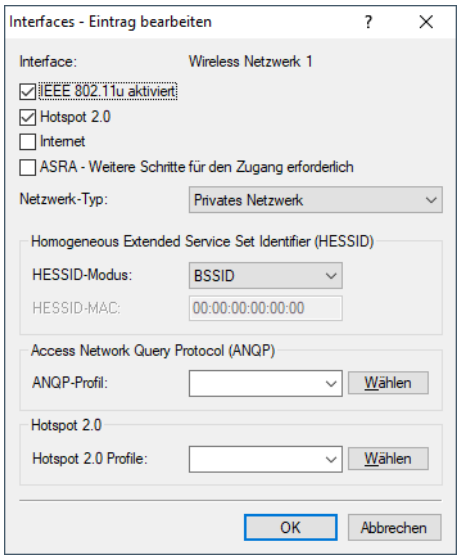
Das Gerät bietet Ihnen über die Schaltfläche **Interfaces** die Möglichkeit, die Unterstützung für den IEEE-802.11u-Standard sowie die Hotspot-2.0-Funktionalität für jede logische WLAN-Schnittstelle separat zu aktivieren bzw. zu deaktivieren sowie zu konfigurieren.

Ein Teil der zu konfigurierenden Parameter ist in sogenannte „Profile" ausgelagert. Über Profile gruppieren Sie Reihen unterschiedlicher Parameter in Listen, auf die Sie aus den einzelnen Dialogen lediglich referenzieren. Im Wesentlichen handelt es sich dabei um Profile für ANQP-Datenpakete sowie Hotspot 2.0. Die Beziehungen zwischen den Profillisten untereinander stellen sich wie folgt dar:

```
|-- Interfaces
  |-- ANQP-Profile
    |-- NAI-Realms
    |-- Cellular-Netzwerk Informations-Liste
    |-- Netzwerk-Authentifizierungs-Typen
  |-- Hotspot 2.0 Profile
    |-- Betreiber-Liste
    |-- OSU-Anbieter
```

Aktivierung für Interfaces

Die Tabelle **Interfaces** ist die höchste Verwaltungsebene für IEEE 802.11u und Hotspot 2.0. Hier haben Sie die Möglichkeit, die Funktionen für jede Schnittstelle ein- oder auszuschalten, ihnen unterschiedliche Profile zuzuweisen oder allgemeine Einstellungen vorzunehmen.



Interface

Name der logischen WLAN-Schnittstelle, die Sie gerade bearbeiten.

IEEE 802.11u aktiviert

Aktivieren oder deaktivieren Sie an der betreffenden Schnittstelle die Unterstützung für Verbindungen nach IEEE 802.11u. Wenn Sie die Unterstüzung aktivieren, sendet das Gerät für die Schnittstelle – bzw. für die dazugehörige SSID – das Interworking-Element in den Beacons / Probes. Dieses Element dient als Erkennungsmerkmal für IEEE-802.11u-fähige Verbindungen: Es enthält z. B. das Internet-Bit, das ASRA-Bit, die HESSID sowie den Standort-Gruppen-Code und den Standort-Typ-Code. Diese Einzelelemente nutzen 802.11u-fähige Geräte als erste Filterkriterien bei der Netzsuche.

Hotspot 2.0

Aktivieren oder deaktivieren Sie an der betreffenden Schnittstelle die Unterstützung für Hotspot 2.0 der Wi-Fi Alliance®. Hotspot 2.0 erweitert den IEEE-802.11u-Standard um zusätzliche Netzwerkinformationen, welche Stationen über einen ANQP-Request abfragen können. Dazu gehören z. B. der betreiberfreundliche Name, die Verbindungs-Fähigkeiten, die Betriebsklasse und die WAN-Metriken. Über diese zusätzlichen Informationen sind Stationen dazu in der Lage, die Wahl eines Wi-Fi-Netzwerkes noch selektiver vorzunehmen.

Internet

Wählen Sie aus, ob das Internet-Bit gesetzt wird. Über das Internet-Bit informieren Sie alle Stationen explizit darüber, dass das Wi-Fi-Netzwerk den Internetzugang erlaubt. Aktivieren Sie diese Einstellung, sofern über Ihr Gerät nicht nur interne Dienste erreichbar sind.

Über diese Funktion teilen Sie lediglich die Verfügbarkeit einer Internetverbindung mit. Die entsprechenden Regularien konfigurieren Sie unabhängig von dieser Option über die Firewall!

ASRA – Weitere Schritte für den Zugang erforderlich

Wählen Sie aus, ob das ASRA-Bit (Additional Step Required for Access) gesetzt wird. Über das ASRA-Bit informieren Sie alle Stationen explizit darüber, dass für den Zugriff auf das Wi-Fi-Netzwerk noch weitere Authentifizierungsschritte notwendig sind. Aktivieren Sie diese Einstellung, wenn Sie z. B. eine Online-Registrierung, eine zusätzliche Web-Authentifikation oder eine Zustimmungswebseite für Ihre Nutzungsbedingungen eingerichtet haben.

Denken Sie daran, in der Tabelle **Netzwerk-Authentifizierungs-Typen** eine Weiterleitungsadresse für die zusätzliche Authentifizierung anzugeben und / oder **WISPr** für das Public Spot-Modul zu konfigurieren, wenn Sie das ASRA-Bit setzen.

Netzwerk-Typ

Wählen Sie aus der vorgegebenen Liste einen Netzwerk-Typ aus, der das Wi-Fi-Netzwerk hinter der ausgewählten Schnittstelle am ehesten charakterisiert. Anhand der hier getroffenen Einstellung haben Nutzer die Wahl, die Netzsuche ihrer Geräte auf bestimmte Netzwerk-Typen zu beschränken. Mögliche Werte sind:

Privates Netzwerk

Beschreibt Netzwerke, in denen unauthorisierte Benutzer nicht erlaubt sind. Wählen Sie diesen Typ z. B. für Heimnetzwerke oder Firmennetzwerke, bei denen der Zugang auf die Mitarbeiter beschränkt ist.

Privat mit Gast-Zugang

Wie **Privates Netzwerk**, doch mit Gast-Zugang für unauthorisierte Benutzer. Wählen Sie diesen Typ z. B. für Firmennetzwerke, bei denen neben den Mitarbeitern auch Besucher das Wi-Fi-Netzwerk nutzen dürfen.

Kostenpflichtiges Öffentliches Netzwerk

Beschreibt öffentliche Netzwerke, die für jedermann zugänglich sind und deren Nutzung gegen Entgelt möglich ist. Informationen zu den Gebühren sind evtl. auf anderen Wegen abrufbar (z. B: IEEE 802.21, HTTP/HTTPS- oder DNS-Weiterleitung). Wählen Sie diesen Typ z. B. für Hotspots in Geschäften oder Hotels, die einen kostenpflichtigen Internetzugang anbieten.

Kostenloses öffentliches Netzwerk

Beschreibt öffentliche Netzwerke, die für jedermann zugänglich sind und für deren Nutzung kein Entgelt anfällt. Wählen Sie diesen Typ z. B. für Hotspots im öffentlichen Nah- und Fernverkehr oder für kommunale Netzwerke, bei denen der Wi-Fi-Zugang eine inbegriffene Leistung ist.

Persönliches Geräte-Netzwerk

Beschreibt Netzwerke, die drahtlose Geräte im Allgemeinen verbinden. Wählen Sie diesen Typ z. B. bei angeschlossenen Digital-Kameras, die via WLAN mit einem Drucker verbunden sind.

Netzwerk für Notdienste

Beschreibt Netzwerke, die für Notdienste bestimmt und auf diese beschränkt sind. Wählen Sie diesen Typ z. B. bei angeschlossenen ESS- oder EBR-Systemen.

Test oder experimentell

Beschreibt Netzwerke, die zu Testzwecken eingerichtet sind oder sich noch im Aufbaustadium befinden.

Wildcard

Platzhalter für bislang undefinierte Netzwerk-Typen.

HESSID-Modus

Geben Sie an, woher das Gerät seine HESSID für das homogene ESS bezieht. Als homogenes ESS bezeichnet man den Verbund einer bestimmten Anzahl von Access Points, die alle dem selben Netzwerk angehören. Als weltweit eindeutige Kennung (HESSID) dient die MAC-Adresse eines angeschlossenen Access Points. Die SSID taugt in diesem Fall nicht als Kennung, da in einer Hotspot-Zone unterschiedliche Netwerkbetreiber die gleiche SSID vergeben haben können, z. B. durch Trivialnamen wie „HOTSPOT". Mögliche Werte für den HESSID-Modus sind:

BSSID

Wählen Sie diesen Eintrag, um die BSSID des Gerätes als HESSID für Ihr homogenes ESS festzulegen.

Benutzer

Wählen Sie diesen Eintrag, um eine HESSID manuell zu vergeben.

Keiner

Wählen Sie diesen Eintrag, um die Schnittstelle keinem homogenen ESS zuzuordnen und aus dem Geräteverbund zu isolieren.

HESSID-MAC

Sofern Sie als **HESSID-Modus** die Einstellung `Benutzer` gewählt haben, tragen Sie hier die HESSID Ihres homogenen ESS in Form einer 6-oktettigen MAC-Adresse ein. Wählen Sie für die HESSID die BSSID eines beliebigen Access Apoints in Ihrem homogenen ESS in Großbuchstaben und ohne Trennzeichen, z. B. „008041AEFD7E“ für die MAC-Adresse 00:80:41:ae:fd:7e.

Sofern Ihr Gerät nicht in mehreren homogenen ESS vertreten ist, ist die HESSID für alle Schnittstellen identisch!

ANQP-Profil

Wählen Sie aus der Liste ein ANQP-Profil aus. ANQP-Profile legen Sie im Konfigurationsmenü über die gleichnamige Schaltfläche an.

Hotspot 2.0 Profile

Wählen Sie aus der Liste ein Hotspot-2.0-Profil aus. Hotspot-2.0-Profile legen Sie im Konfigurationsmenü über die gleichnamige Schaltfläche an.

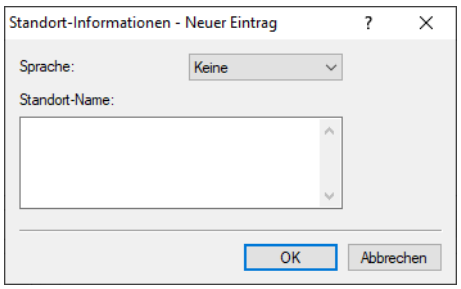
ANQP-Datenpakete konfigurieren

Standort-Informationen und -Gruppe

Über die Tabelle **Standort-Informationen** sowie den nachgelagerten Dialogabschnitt zur **Standort-Gruppe** und zum **Standort-Typ-Code** verwalten Sie die Angaben zum Standort des Access Points.

Mit Angaben zu den **Standort-Informationen** unterstützen Sie einen Nutzer bei der Auswahl des richtigen Hotspots im Falle einer manuellen Suche. Verwenden in einer Hotspot-Zone mehrere Betreiber (z. B. mehrere Cafés) die gleiche SSID, kann der Nutzer mit Hilfe der Standort-Informationen die passende Lokalität eindeutig identifizieren.

Über die **Standort-Gruppe** und den **Standort-Typ-Code** ordnen Sie dagegen Ihr Gerät – im Gegensatz zu den frei definierbaren Standort-Informationen – in eine vorgegebene Kategorie ein.



Sprache

Sie haben die Möglichkeit, für jede Sprache individuelle Informationen zum Standort des Access Points anzugeben. Ihre Nutzer bekommen dann die zur ihrer Sprache passenden Standort-Namen angezeigt. Ist eine Sprache für einen Nutzer nicht vorhanden, entscheidet seine Station, z. B. anhand der Default-Sprache.

Standort-Name

Tragen Sie hier für die ausgewählte Sprache eine kurze Beschreibung zum Standort des Gerätes ein, z. B.

```
Eiscafé Valenzia
Am Markt 3
12345 Musterstadt
```

Die **Standort-Gruppe** beschreibt das Umfeld, in dem Sie den Access Point einsetzen. Sie definieren sie global für alle Sprachen. Die möglichen Werte, festgelegt durch den „Venue Group Code", werden durch den 802.11u-Standard vorgegeben.

Über den **Standort-Typ-Code** haben Sie die Möglichkeit, die Standort-Gruppe weiter zu spezifizieren. Auch hier sind die Werte durch den Standard spezifiziert. Die möglichen Typ-Codes entnehmen Sie bitte der nachfolgenden Tabelle.

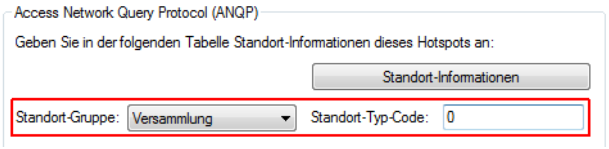


Tabelle 35: Übersicht möglicher Werte für Standort-Gruppen und -Typen

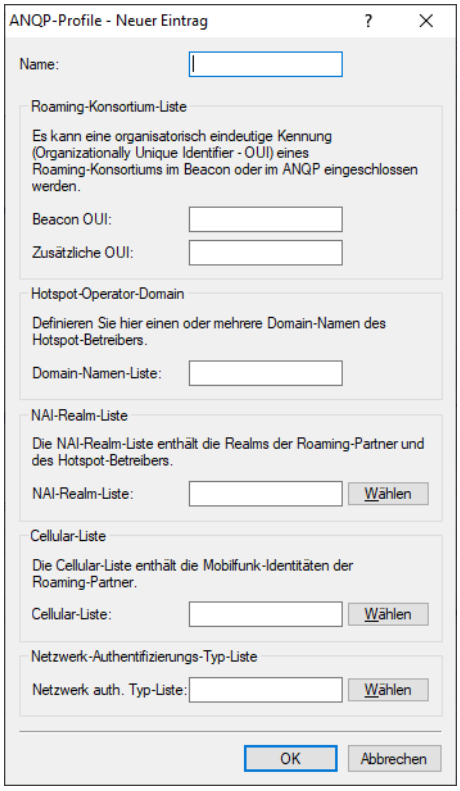
Standort-Gruppe	Standort-Typ-Code
Unspezifiziert	
Versammlung	0 = Unspezifizierte Versammlung 1 = Bühne 2 = Stadion 3 = Passagier-Terminal (z. B. Flughafen, Busbahnhof, Fähranleger, Bahnhof) 4 = Amphitheater 5 = Vergnügungspark 6 = Andachtsstätte 7 = Kongresszentrum 8 = Bücherei 9 = Museum 10 = Restaurant 11 = Schauspielhaus 12 = Bar 13 = Café 14 = Zoo, Aquarium 15 = Notfallleitstelle
Geschäft	0 = Unspezifiziertes Geschäft 1 = Arztpraxis 2 = Bank 3 = Feuerwache 4 = Polizeiwache 6 = Post 7 = Büro 8 = Forschungseinrichtung 9 = Anwaltskanzlei
Ausbildung	0 = Unspezifizierte Ausbildung 1 = Grundschule 2 = Weiterführende Schule 3 = Hochschule

Standort-Gruppe	Standort-Typ-Code
Fabrik und Industrie	› 0 = Unspezifizierte Fabrik und Industrie › 1 = Fabrik
Institutional	› 0 = Unspezifizierte Institution › 1 = Krankenhaus › 2 = Langzeit-Pflegeeinrichtung (z. B. Seniorenheim, Hospiz) › 3 = Entzugsklinik › 4 = Einrichtungsverbund › 5 = Gefängnis
Handel	› 0 = Unspezifizierter Handel › 1 = Ladengeschäft › 2 = Lebensmittelmarkt › 3 = KFZ-Werkstatt › 4 = Einkaufszentrum › 5 = Tankstelle
Wohnheim	› 0 = Unspezifiziertes Wohnheim › 1 = Privatwohnsitz › 2 = Hotel oder Motel › 3 = Studentenwohnheim › 4 = Pension
Lager	› 0 = Unspezifiziertes Lager
Dienste und sonstiges	› 0 = Unspezifizierter Dienst und sonstiges
Fahrzeug	› 0 = Unspezifiziertes Fahrzeug › 1 = Personen- oder Lastkraftwagen › 2 = Flugzeug › 3 = Bus › 4 = Fähre › 5 = Schiff oder Boot › 6 = Zug › 7 = Motorrad
Außen	› 0 = Unspezifizierter Außenbereich › 1 = Städtisches Wi-Fi-Netzwerk (Muni-Mesh-Netzwerk) › 2 = Stadtpark › 3 = Rastplatz › 4 = Verkehrsregelung › 5 = Bushaltestelle › 6 = Kiosk

ANQP-Profile

Über diese Tabelle verwalten Sie die Profillisten für ANQP. **ANQP-Profile** bieten Ihnen die Möglichkeit, bestimmte ANQP-Elemente zu gruppieren und sie in der Tabelle **Interfaces** unabhängig voneinander logischen WLAN-Schnittstellen

zuzuweisen. Zu diesen Elementen gehören z. B. Angaben zu Ihren OIs, Domains, Roaming-Partnern und deren Authentifizierungsmethoden. Ein Teil der Elemente ist in weitere Profillisten ausgelagert.



Name

Vergeben Sie hierüber einen Namen für das ANQP-Profil. Dieser Name erscheint später innerhalb der Interfaces-Tabelle in der Auswahlliste für die ANQP-Profile.

Beacon OUI

Organizationally Unique Identifier, abgekürzt OUI, vereinfacht OI. Als Hotspot-Betreiber tragen Sie hier die OI des Roaming-Partners ein, mit dem Sie einen Vertrag abgeschlossen haben. Sind Sie als Hotspot-Betreiber gleichzeitig der Service-Provider, tragen Sie hier die OI Ihres Roaming-Konsortiums oder Ihre eigene OI ein. Ein Roaming-Konsortium besteht aus einer Gruppe von Service-Providern, die untereinander Vereinbarungen zum gegenseitigen Roaming getroffen haben. Um eine OI zu erhalten, muss sich ein solches Konsortium – ebenso wie ein einzelner Service-Provider – bei der IEEE registrieren lassen.

Es besteht die Möglichkeit, bis zu 3 OIs parallel anzugeben, z. B. für den Fall, dass Sie als Betreiber Verträge mit mehreren Roaming-Partnern haben. Mehrere OIs trennen Sie durch eine kommaseparierte Liste, z. B. `00105E,00017D,00501A`.

Das Gerät strahlt die eingegebene(n) OI(s) in seinen Beacons aus. Soll das Gerät mehr als 3 OIs übertragen, lassen sich diese unter **Zusätzliche OUI** konfigurieren. Zusätzliche OIs werden allerdings erst nach dem GAS-Request einer Station übertragen; sie sind für die Stationen also nicht unmittelbar sichtbar!

Zusätzliche OUI

Tragen Sie hier die OI(s) ein, die das Gerät nach dem GAS-Request einer Station zusätzlich aussendet. Mehrere OIs trennen Sie durch eine kommaseparierte Liste, z. B. `00105E,00017D,00501A`.

Domain-Namen-Liste

Tragen Sie hier eine oder mehrere Domains ein, über die Sie als Hotspot-Betreiber verfügen. Mehrere Domain-Namen trennen Sie durch eine kommaseparierte Liste, z. B. `providerX.org,provx-mobile.com,wifi.mnc410.provX.com`. Für Subdomains reicht es aus, lediglich den obersten gültigen Domain-Namen anzugeben. Hat ein Nutzer z. B. providerX.org als Heimat-Provider in seinem Gerät konfiguriert, werden dieser Domain auch Access Points mit dem Domain-Namen wi-fi.providerX.org zugerechnet. Bei der Suche nach passenden Hotspots bevorzugt eine Station immer den Hotspot seines Heimat-Providers, um mögliche Roaming-Kosten über den Access Point eines Roaming-Partners zu vermeiden.

NAI-Realm-Liste

Wählen Sie aus der Liste ein NAI-Realm-Profil aus. Profile für NAI-Realms legen Sie im Konfigurationsmenü über die Schaltfläche **NAI-Realms** an.

Cellular-Liste

Wählen Sie aus der Liste eine Mobilfunk-Identität aus. Identitäten für Mobilfunknetzwerke legen Sie – wie bei einem Profil – im Konfigurationsmenü über die Schaltfläche **Cellular-Netzwerk Informations-Liste** an.

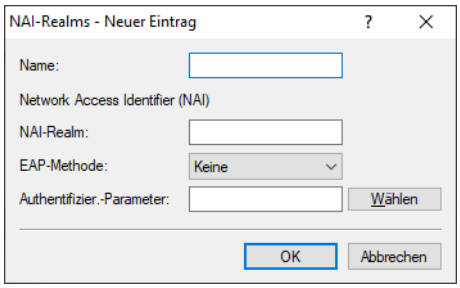
Netzwerk auth. Typ-Liste

Wählen Sie aus der Liste einen Authentifizierungs-Profil aus. Profile zur Netzwerk-Authentifizierung legen Sie im Konfigurationsmenü über die Schaltfläche **Netzwerk-Authentifizierungs-Typen** an.

Zusätzlich haben Sie über die Konsole die Möglichkeit, Ihren Nutzern auch den Typ der verfügbaren IP-Adresse anzuzeigen, den diese nach einer erfolgreichen Authentifizierung vom Netzwerk erhalten können. Sie erreichen die betreffenden Parameter **IPv4-Addr-Type** und **IPv6-Addr-Type** über den Pfad **Setup** > **IEEE802.11u** > **ANQP-General**.

NAI-Realms

Über diese Tabelle verwalten Sie die Profillisten für die NAI-Realms. Mit diesen Listen haben Sie die Möglichkeit, bestimmte ANQP-Elemente zu gruppieren. Hierzu gehören die Realms des Hotspot-Betreibers und seiner Roaming-Partner mitsamt der zugehörigen Authentifizierungs-Methoden und -Parameter. Stationen nutzen diese Liste, um anhand der hier hinterlegten Angaben festzustellen, ob sie für den Hotspot-Betreiber oder einen seiner Roaming-Partner über gültige Anmeldedaten verfügen.



Name

Vergeben Sie hierüber einen Namen für das NAI-Realm-Profil, z. B. den Namen des Service-Providers oder Dienstes, zu dem der NAI-Realm gehört. Dieser Name erscheint später im ANQP-Profil in der Auswahl für die **NAI-Realm-Liste**.

NAI-Realm

Geben Sie hier den Realm für das Wi-Fi-Netzwerk an. Der NAI-Realm selbst ist ein Identifikationspaar aus einem Benutzernamen und einer Domäne, welches durch reguläre Ausdrücke erweitert werden kann. Die Syntax für einen NAI-Realm wird in *RFC 2486* definiert und entspricht im einfachsten Fall

`<username>@<realm>`; für `user746@providerX.org` lautet der entsprechende Realm also `providerX.org`.

EAP-Methode

Wählen Sie aus der Liste eine Authentifizierungsmethode für den NAI-Realm aus. EAP steht dabei für das Authentifizierungs-Protokoll (Extensible Authentication Protocol), gefolgt vom jeweiligen Authentisierungsverfahren. Mögliche Werte sind:

EAP-TLS

Authentifizierung via Transport Layer Security (TLS). Wählen Sie diese Einstellung, wenn die Authentifizierung über den betreffenden NAI-Realm durch ein digitales Zertifikat erfolgt, das der Nutzer installiert.

EAP-SIM

Authentifizierung via Subscriber Identity Module (SIM). Wählen Sie diese Einstellung, wenn die Authentifizierung über den betreffenden NAI-Realm durch das GSM Subscriber Identity Module (die SIM-Karte) der Station erfolgt.

EAP-TTLS

Authentifizierung via Tunneled Transport Layer Security (TTLS). Wählen Sie diese Einstellung, wenn die Authentifizierung über den betreffenden NAI-Realm durch einen Benutzernamen und ein Passwort erfolgt. Zur Sicherheit wird die Verbindung bei diesem Verfahren getunnelt.

EAP-AKA

Authentifizierung via Authentication and Key Agreement (AKA). Wählen Sie diese Einstellung, wenn die Authentifizierung über den betreffenden NAI-Realm durch das UTMS Subscriber Identity Module (die USIM-Karte) der Station erfolgt.

Keine

Wählen Sie diese Einstellung, wenn der betreffende NAI-Realm keine Authentifizierung erfordert.

Authentifizierungs-Parameter

Klicken Sie die zur EAP-Methode passenden Authentifizierungs-Parameter, z. B. für EAP-TTLS

`NonEAPAuth.MSCHAPV2,Credential.UserPass`

oder für EAP-TLS `Credentials.Certificate`.

Mögliche Werte sind:

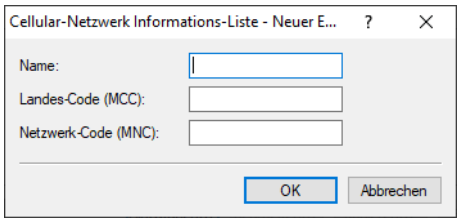
Tabelle 36: Übersicht der möglichen Authentifizierungs-Parameter

Parameter	Sub-Parameter	Erläuterung
NonEAPAuth.		Bezeichnet das Protokoll, welches der Realm für die Phase-2-Authentifizierung erfordert:
	PAP	Password Authentication Protocol
	CHAP	Challenge Handshake Authentication Protocol, ursprüngliche CHAP-Implementierung, spezifiziert im *RFC 1994*
	MSCHAP	CHAP-Implementierung von Microsoft v1, spezifiziert im *RFC 2433*
	MSCHAPV2	CHAP-Implementierung von Microsoft v2, spezifiziert im *RFC 2759*
Credentials.		Beschreibt die Art der Authentifizierung, die der Realm akzeptiert:

Parameter	Sub-Parameter	Erläuterung
	SIM	SIM-Karte
	USIM	USIM-Karte
	NFCSecure	NFC-Chip
	HWToken*	Hardware-Token
	SoftToken*	Software-Token
	Certificate	Digitales Zertifikat
	UserPass	Benutzername und Passwort
	None	Keine Zugangsdaten erforderlich
TunnelEAPCredentials.*		
	SIM*	SIM-Karte
	USIM*	USIM-Karte
	NFCSecure*	NFC-Chip
	HWToken*	Hardware-Token
	SoftToken*	Software-Token
	Certificate*	Digitales Zertifikat
	UserPass*	Benutzername und Passwort
	Anonymous*	Anonyme Anmeldung

Cellular-Netzwerk Informations-Liste

Über diese Tabelle verwalten Sie die Identitätslisten für die Mobilfunknetze. Mit diesen Listen haben Sie die Möglichkeit, bestimmte ANQP-Elemente zu gruppieren. Hierzu gehören die Netzwerk- und Landes-Codes des Hotspot-Betreibers und seiner Roaming-Partner. Stationen mit SIM- oder USIM-Karte nutzen diese Liste, um anhand der hier hinterlegten Angaben festzustellen, ob der Hotspot-Betreiber zu ihrer Mobilfunkgesellschaft gehört oder einen Roaming-Vertrag mit ihrer Mobilfunkgesellschaft hat.



Name

Vergeben Sie hierüber einen Namen für die Mobilfunk-Identität, z. B. ein Kürzel des Netzanbieters in Kombination mit dem verwendeten Mobilfunkstandard. Dieser Name erscheint später im ANQP-Profil in der Auswahl für die **Cellular-Liste**.

Landes-Code (MCC)

Geben Sie hier den Mobile Country Code (MCC) des Hotspot-Betreibers oder seiner Roaming-Partner ein, bestehend aus 2 oder 3 Zeichen, z. B. `262` für Deutschland.

* Der betreffende Parameter oder Sub-Parameter ist im Rahmen der Passpoint™-Zertifizierung für zukünftige Einsatzzwecke reserviert worden, findet gegenwärtig jedoch keine Verwendung.

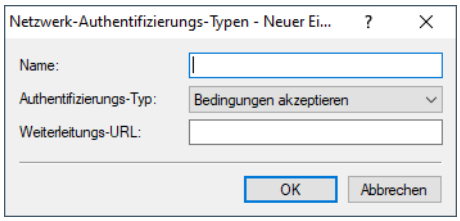
Netzwerk-Code (MNC)

Geben Sie hier den Mobile Network Code (MNC) des Hotspot-Betreibers oder seiner Roaming-Partner ein, bestehend aus 2 oder 3 Zeichen.

Netzwerk-Authentifizierungs-Typen

Über diese Tabelle verwalten Sie Adressen, an die das Gerät Stationen für einen zusätzlichen Authentifizierungsschritt weiterleitet, nachdem sich die Station bereits beim Hotspot-Betreiber oder einem seiner Roaming-Partner erfolgreich authentisiert hat. Pro Authentifizierungs-Typ ist nur eine Weiterleitungsangabe erlaubt.

Denken Sie daran, das ASRA-Bit in der Tabelle **Interfaces** zu setzen, wenn Sie einen zusätzlichen Authentifizierungsschritt einrichten!



Name

Vergeben Sie hierüber einen Namen für den Listeneintrag, z. B. `AGB akzeptieren`. Dieser Name erscheint später im ANQP-Profil in der Auswahl für die **Netzwerk auth. Typ-Liste**.

Authentifizierungs-Typ

Wählen Sie aus der Auswahlliste den Kontext, vor dem die Weiterleitung gilt. Mögliche Werte sind:

Bedingungen akzeptieren

Es ist ein zusätzlicher Authentifizierungsschritt eingerichtet, bei dem ein Benutzer die Nutzungsbedingungen des Betreibers akzeptieren muss.

Online Registrierung

Es ist ein zusätzlicher Authentifizierungsschritt eingerichtet, bei dem sich ein Benutzer erst online registrieren muss.

HTTP-Weiterleitung

Es ist ein zusätzlicher Authentifizierungsschritt eingerichtet, zu dem ein Benutzer via HTTP weitergeleitet wird.

DNS-Weiterleitung

Es ist ein zusätzlicher Authentifizierungsschritt eingerichtet, zu dem ein Benutzer via DNS weitergeleitet wird.

Weiterleitungs-URL

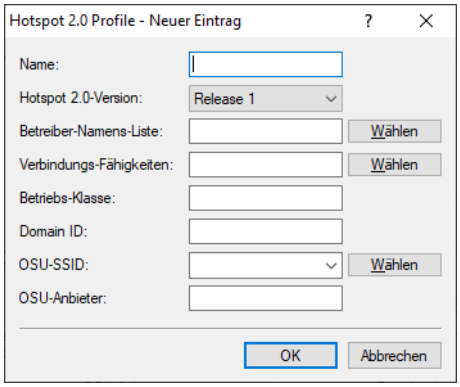
Geben Sie die Adresse an, an die das Gerät Stationen für den zusätzlichen Authentifizierungsschritt weiterleitet.

Hotspot 2.0 konfigurieren

Hotspot 2.0 Profile

Über diese Tabelle verwalten Sie die Profillisten für Hotspot 2.0. **Hotspot 2.0 Profile** bieten Ihnen die Möglichkeit, bestimmte ANQP-Elemente (die der Hotspot-2.0-Spezifikation) zu gruppieren und sie in der Tabelle **Interfaces** unabhängig voneinander logischen WLAN-Schnittstellen zuzuweisen. Zu diesen Elementen gehören z. B. der betreiberfreundliche

Name, die Verbindungs-Fähigkeiten, die Betriebsklasse und die WAN-Metriken. Ein Teil der Elemente ist in weitere Profillisten ausgelagert.



Name

Vergeben Sie hierüber einen Namen für das Hotspot-2.0-Profil. Dieser Name erscheint später innerhalb der Interfaces-Tabelle in der Auswahlliste für die Hotspot-2.0-Profile.

Hotspot 2.0 Version

Stellen Sie das in diesem Profil unterstützte Release von Hotspot 2.0 ein.

Ein Client muss das entsprechende Release beherrschen, um sich verbinden zu können.

Betreiber-Namens-Liste

Wählen Sie aus der Liste das Profil eines Hotspot-Betreibers aus. Profile für Hotspot-Betreiber legen Sie im Konfigurationsmenü über die Schaltfläche **Betreiber-Liste** an.

Verbindungs-Fähigkeiten

Wählen Sie für jeden Dienst die Verbindungs-Fähigkeit aus. Stationen nutzen diese Liste, um anhand der hier hinterlegten Angaben vor einem Netzbeitritt festzustellen, ob Ihr Hotspot die benötigten Dienste (z. B. Internetzugang, SSH, VPN) überhaupt erlaubt. Aus diesem Grund sollten so wenig Einträge wie möglich den Status „unbekannt" tragen. Mögliche Statuswerte für die einzelnen Dienste sind „closed" (`-C`), „open" (`-O`) oder „unknown" (`-U`):

- `ICMP`: Geben Sie an, ob Sie den Austausch von Informations- und Fehlermeldungen via ICMP erlauben.
- `TCP-FTP`: Geben Sie an, ob Sie Dateiübertragungen via FTP erlauben.
- `TCP-SSH`: Geben Sie an, ob Sie verschlüsselte Verbindungen via SSH erlauben.
- `TCP-HTTP`: Geben Sie an, ob Sie Internetverbindungen via HTTP/HTTPS erlauben.
- `TCP-TLS`: Geben Sie an, ob Sie verschlüsselte Verbindungen via TLS erlauben.
- `TCP-PPTP`: Geben Sie an, ob Sie das Tunneln von VPN-Verbindungen via PPTP erlauben.
- `TCP-VOIP`: Geben Sie an, ob Sie Internettelefonie via VoIP (TCP) erlauben.
- `UDP-IPSEC-500`: Geben Sie an, ob Sie IPsec via UDP und Port 500 erlauben.
- `UDP-VOIP`: Geben Sie an, ob Sie Internettelefonie via VoIP (UDP) erlauben.
- `UDP-IPSEC-4500`: Geben Sie an, ob Sie IPsec via UDP und Port 4500 erlauben.
- `ESP`: Geben Sie an, ob Sie ESP (Encapsulating Security Payload) für IPsec erlauben.

Wenn Sie nicht wissen, ob in Ihrem Netzwerk ein Dienst verfügbar und seine Ports offen oder geschlossen sind, oder Sie gegenüber einer Station bewusst keine Angabe zum Status machen wollen, wählen Sie eine `-U`-Einstellung.

Über diesen Dialog legen Sie keine Berechtigungen fest! Die Angaben dienen den Stationen lediglich dazu, den Netzbeitritt über Ihr Gerät zu entscheiden. Spezifische Zugangsberechtigungen für Ihr Netzwerk konfigurieren Sie über andere Gerätefunktionen, wie z. B. die Firewall / QoS.

Betriebs-Klasse

Geben Sie hier den Code für die globale Betriebsklasse des Access Points an. Über die Betriebs-Klasse teilen Sie einer Station mit, auf welchen Frequenzbändern und Kanälen Ihr Access-Point verfügbar ist. Beispiel:

- `81`: Betrieb bei 2,4 GHz mit Kanälen 1–13
- `116`: Betrieb bei 40 MHz mit Kanälen 36 und 44

Die für Ihr Gerät passende Betriebsklasse entnehmen Sie bitte dem IEEE Standard 802.11-2012, Anhang E, Tabelle E-4: Global operating classes; erhältlich unter *standards.ieee.org*.

Domain ID

Die Domain-ID gibt an, welcher ANQP-Server verwendet wird. Alle Access Points bzw. SSIDs mit gleicher Nummer / Domain-ID (16-Bit-Wert) verwenden den gleichen ANQP-Server.

Ein Client würde somit auf eine ANQP-Anfrage auf Access Points / SSIDs mit identischer Domain-ID immer die gleiche Antwort erhalten. Um unterschiedliche Antworten zu erhalten, müsste der Client nach unterschiedlichen Domain-IDs Ausschau halten.

OSU-SSID

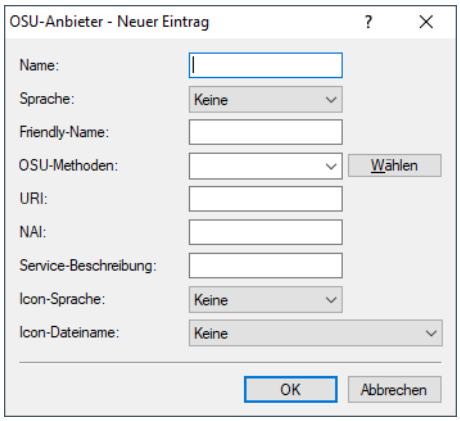
Name der SSID, die Zugang zum OSU-Server bietet.

OSU-Anbieter

Liste der OSU-Providernamen aus *OSU-Anbieter* auf Seite 1101, die im Profil unterstützt werden.

OSU-Anbieter

In dieser Tabelle konfigurieren Sie die OSU-Provider für Online Sign-Up bei Passpoint® Release 2.



Name

Geben Sie diesem OSU-Provider einen Namen, über den Sie ihn später referenzieren können. Wenn der gleiche Name erneut verwendet wird, dann kann dieser Provider z. B. für mehrere Spachen verwendet werden.

Sprache

Stellen Sie die von diesem OSU-Provider unterstützte Sprache ein.

Friendly-Name

Geben Sie diesem OSU-Provider einen sprechenden Namen.

OSU-Methoden

Stellen Sie hier die von diesem OSU-Provider verwendeten OSU-Methoden ein. Möglich sind „OMA-DM“ oder „SOAP-XML-SPP“.

Mögliche Methoden innerhalb des Online Sign-Up-Servers bei Passpoint® Release 2:

- OMA – Open Mobile Alliance
- DM – Device Management
- SOAP – Simple Object Access Protocol
- XML – eXtended Markup Language
- SPP – Subscription Provisioning Protocol

URI

Geben Sie eine URI ein, unter der ein Client den OSU-Server erreicht.

NAI

Geben Sie den Network Access Identifier (NAI) für diesen OSU-Provider ein.

Service-Beschreibung

Geben Sie hier einen Beschreibungstext für diesen Dienst ein.

Icon-Sprache

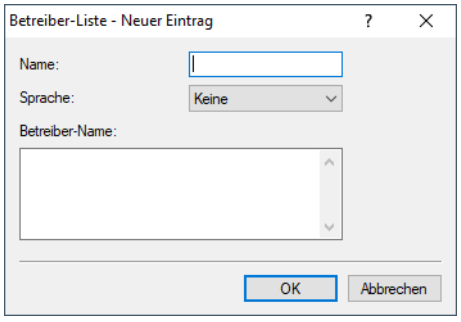
Stellen Sie hier die Sprache des ausgewählten Icons ein.

Icon-Dateiname

Wählen Sie ein Icon für diesen OSU-Provider aus. Die Icons können über die WEBconfig im Bereich ***Dateimanagement*** als Datei hochgeladen werden. Als Dateiformat empfehlen wir PNG.

Betreiber-Liste

Über diese Tabelle verwalten Sie die Klartext-Namen der Hotspot-Betreiber. Ein Eintrag in dieser Tabelle bietet Ihnen die Möglichkeit, einen benutzerfreundlichen Betreiber-Namen an die Stationen zu senden, den diese dann anstelle der Realms anzeigen können. Ob sie das allerdings tatsächlich tun, ist abhängig von der Implementierung.



Name

Vergeben Sie hierüber einen Namen für den Eintrag, z. B. eine Indexnummer oder Kombination aus Betreiber-Name und Sprache.

Sprache

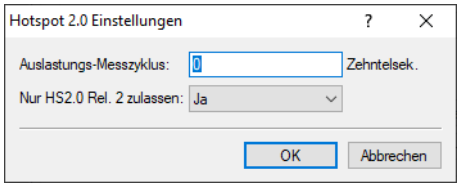
Wählen Sie aus der Liste eine Sprache für den Hotspot-Betreiber aus.

Betreiber-Name

Geben Sie hier den Klartext-Namen des Hotspot-Betreibers ein.

Hotspot 2.0 Einstellungen

In dieser Tabelle konfigurieren Sie spezielle Einstellungen für Hotspot 2.0.



Auslastungs-Messzyklus

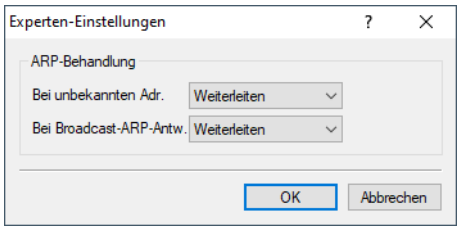
Messzyklus der WAN-Down- / Uplink-Geschwindigkeiten in Zehntelsekunden.

Nur Hotspot 2.0 Release 2 zulassen

Für HotSpot 2.0 Release 2 wird gefordert, nur Release 2-Clients zuzulassen. Dies kann durch diesen Schalter ausgeschaltet werden.

Experten-Einstellungen

In dieser Tabelle konfigurieren Sie Experten-Einstellungen für Hotspot 2.0. Die Einstellungen in diesem Menü dienen der Unterdrückung von ARP (IPv4) bzw. Neighbor Solicitation (IPv6) innerhalb der SSID zwischen den Clients. Alternativ kann dies i.d.R. auch durch die Unterdrückung von Broad- / Multicasts via **Nur Unicasts übertragen, Broad- und Multicasts unterdrücken** in den logischen WLAN-Netzwerkeinstellungen gelöst werden.



Bei unbekannten Adressen

Bei unbekannten Adressen wird das Paket entweder weitergeleitet oder verworfen.

Bei Broadcast-ARP-Antworten

Bei Broadcasts wird das Paket entweder weitergeleitet oder verworfen.

15.2.4.7 Schnittstelle für Property-Management-Systeme

Sofern Sie ein Property Management System (PMS) einsetzen, bieten Ihnen bestimmte Gerätetypen und -serien die Möglichkeit, das Public Spot-Modul über die PMS-Schnittstelle mit Ihrer PMS-Datenbank zu verknüpfen. Als Hotelbetreiber erhalten Sie so z. B. die Möglichkeit, einem Gast bereits bei der Registrierung automatisch einen Zugang zu Ihrem Public Spot bereitzustellen. Dieser Zugang kann wahlweise kostenlos oder kostenpflichtig (über Prepaid erworbenes Zeitguthaben) erfolgen, wobei anfallende Gebühren auf die Zimmerrechnung des Gastes gebucht werden. Als Zugangsdaten dienen

ihm dabei sein Nachname, seine Zimmernummer sowie optional eine weitere Sicherheitskennung (z. B. seine Registrierungsnummer oder das Abreisedatum).

Gegenüber einer Voucher-Lösung bietet Ihnen die aktivierte PMS-Schnittstelle den Vorteil, dass keine weiteren administrativen Schritte für die Einrichtung und Verwaltung eines Public Spot-Benutzerkontos mehr notwendig sind: Das Gerät legt für einen Gast selbstständig ein Benutzerkonto an, sobald dieser Ihren Public Spot aufruft und sich mit seinen Registrierungsdaten authentifiziert. Registrierungsänderungen, die diesen Gast zukünftig betreffen (Zimmerwechsel, Änderung des Abreisedatums, Check-out, etc.), übernimmt das Gerät eigenständig von Ihrem PMS.

Folgende Anmeldemethoden werden derzeit unterstützt:

1. Voucher
2. PMS-Anmeldung
3. PMS-Anmeldung und Voucher
4. E-Mail
5. SMS

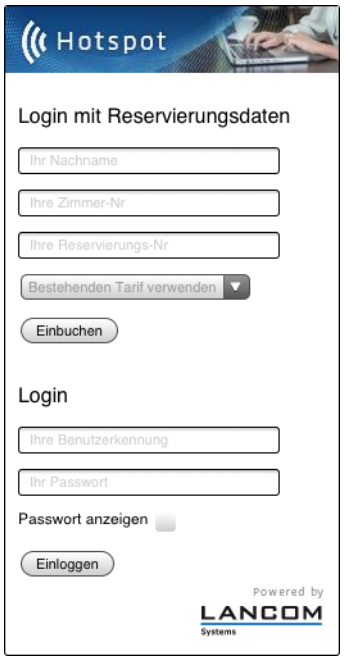
Mit Anmeldemethode (2) kann z. B. für Hotelgäste die Anmeldung anhand der Zimmernummer und des Nachnamen erfolgen, während Sie für Gäste im Restaurant Voucher verkaufen (1). Natürlich haben Sie trotz aktivierter PMS-Schnittstelle auch weiterhin die Möglichkeit, Voucher – z. B. für Tagungsgäste oder Besucher – auszugeben (3).

Die Anmeldemethode konfigurieren Sie global pro Gerät; sie ist somit für alle SSIDs bzw. Netze gleich.

Die PMS-Schnittstelle beinhaltet zur Zeit zur Zeit ausschließlich die Unterstützung für das Hotel-Property-Management-System von Micros Fidelio über TCP/IP.

Funktionsbeschreibung

Wenn Sie die PMS-Schnittstelle aktivieren und eine kostenlose oder kostenpflichtige Login-Seite einstellen, erscheinen auf der Public Spot-Portalseite neue Eingabefelder, über die sich der Gast mit seinem Nachnamen, seiner Zimmernummer und ggf. einer weiteren Sicherheitskennung authentisiert. Die Art dieser Kennung legen Sie über das Setup-Menü fest; möglich sind z. B. die Registrierungsnummer oder das An-/Abreisedatum des Gastes. Sofern Sie den Zugang zu Ihrem Hotspot als kostenpflichtig markiert haben, erscheint überdies ein Auswahlmenü, über welches der Gast das Zeitkontingent bzw. den Tarif auswählt, den er via Prepaid erwerben will (z. B. 1 min für 0,20 EUR oder 1 h für 1 EUR). Die dabei entstehenden Kosten bucht das im Hintergrund arbeitende PMS automatisch auf die Zimmerrechnung.



Bei jeder Anmeldung eines Hotelgastes am Public Spot führt das Gerät einen Abgleich der eingegebenen Registrierungsdaten mit den im PMS hinterlegten Registrierungsdaten durch. Erkennt das PMS in den übermittelten Daten eine gültige Übereinstimmung, meldet es diese Information an das Gerät zurück. Das Gerät legt daraufhin eine neue Sitzung für den Hotelgast an und trägt die dazugehörigen Daten die dazugehörige Accounting-Tabelle (WEBconfig: **Status** > **PMS-Interface** > **Accounting**) ein. In dieser Tabelle erfasst das Gerät – neben den Tarifen – sämtliche Hotelgäste, die sich über die PMS-Schnittstelle eingeloggt haben; ganz egal, ob sie dabei eine kostenlose oder kostenpflichtige Verbindung verwenden. Anschließend gibt das Gerät dem Benutzer den Zugang ins Internet frei.

Hat ein Benutzer für einen kostenpflichtigen Zugang ein Zeitkontingent erworben, kann er dieses verlängern, indem er im angemeldeten Zustand weitere Kontingente erwirbt. Meldet sich vor Ablauf seines Kontingents vom Public Spot ab, kann er seine Sitzung zu einem späteren Zeitpunkt wieder aufnehmen, indem er auf der Login-Seite das entsprechende Feld auswählt. Das Gerät speichert seine Sitzung solange zwischen, bis diese ungültig wird; d. h. das Zeitkontingent aufgebraucht ist oder das PMS dem Gerät die Ausbuchung des Hotelgastes meldet. Bei einem erneuten Login und Abgleich mit dem PMS erkennt das Gerät das immer noch gültige Benutzerkonto und führt dieses fort, anstatt ein neues anzulegen.

Ändern sich zwischenzeitlich die Registrierungsinformationen (z. B. die Zimmernummer), bleibt eine bestehende Sitzung davon zunächst unbeeinflusst. Erst, wenn der Hotelgast seine aktuelle Sitzung beendet und sich erneut am Public Spot anmeldet, muss er sich mit seinen geänderten Zugangsdaten authentisieren. Eine Ausnahme bildet die Ausbuchung eines Gastes aus Ihrem PMS (Check-out): Hierbei beendet das Gerät eine bestehende Sitzung sofort.

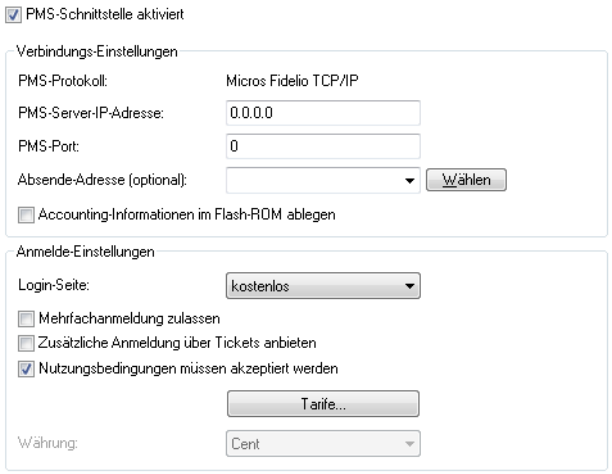
Ihre Nutzer sollten darauf achten, sich ordnungsgemäß vom Public Spot abzumelden. Ohne ordnungsgemäße Abmeldung (hervorgerufen durch einfaches Schließen des Browsers, Trennen der Netzwerkverbindung, Ausschalten des Gerätes, usw.) gilt ein Benutzer als nach wie vor eingeloggt. Dies kann für die Nutzer zu Problemen bei der Wiederanmeldung führen, wenn Sie als Public Spot-Betreiber z. B. keine Mehrfach-Logins erlauben.

Durch die *Stationsüberwachung* haben Sie die Möglichkeit, solche Benutzer nach einer festgelegten Leerlaufzeit automatisch auszuloggen. Dieses Feature ist standardmäßig ausgeschaltet. Für einen kostenpflichtigen Zugang sollten Sie es jedoch unbedingt aktivieren. Andernfalls erfolgt der automatische, geräteinterne Logout erst nach ablaufen des Benutzerkontos, d. h wenn das eingekaufte Zeitkontingent vollständig aufgebraucht ist.

Eine temporäre Abmeldung vom Public Spot verschiebt nicht den Ablaufzeitpunkt eines eingekauften Zeitkontingents! Es nicht möglich, ein bereits gekauftes Zeitguthaben zu "pausieren", um es zu einem späteren Zeitpunkt erneut aufzunehmen. Die Herunterzählung der Zeit beginnt unabhängig vom Anmeldestatus ab Kauf des Kontingents.

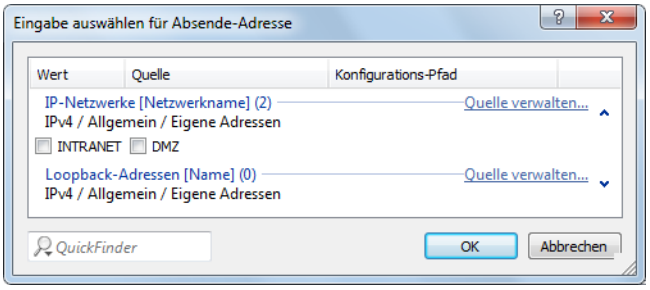
PMS-Schnittstelle konfigurieren

Die PMS-Schnittstelle Ihres Gerätes konfigurieren Sie über den Dialog **Public-Spot** > **PMS-Schnittstelle**.



In diesem Dialog haben Sie folgende Einstellungsmöglichkeiten:

- **PMS-Schnittstelle aktiviert**: Aktivieren oder deaktivieren Sie die PMS-Schnittstelle für das Gerät.
- **PMS-Protokoll**: Bezeichnet das von Ihrem Property-Management-System verwendete Protokoll. Zur Zeit besteht ausschließlich Unterstützung für das Hotel-Property-Management-System von Micros Fidelio über TCP/IP.
- **PMS-Server-IP-Adresse**: Geben Sie hier die IPv4-Adresse Ihres PMS-Servers ein.
- **PMS-Port**: Geben Sie hier den TCP-Port ein, über den Ihr PMS-Server erreichbar ist.
- **Absende-Adresse**: Klicken Sie auf die Schaltfläche **Wählen**, um optional eine andere Adresse zu konfigurieren, an die der PMS-Server seine Antwort-Nachrichten schickt. Standardmäßig schickt der PMS-Server seine Antworten zurück an die IP-Adresse Ihres Gerätes, ohne dass Sie diese hier angeben müssen.



  Mögliche Eingabeformen einer Adresse sind:

  - Name des IP-Netzwerks (ARF-Netz), dessen Adresse eingesetzt werden soll
  - `INT` für die Adresse des ersten Intranets
  - `DMZ` für die Adresse der ersten DMZ

    Wenn eine Schnittstelle namens "DMZ" existiert, wählt das Gerät stattdessen deren Adresse!

  - `LB0`...`LBF` für eine der 16 Loopback-Adressen oder deren Name

    Das Gerät verwendet Loopback-Adressen auch auf maskiert arbeitenden Gegenstellen stets **unmaskiert**!

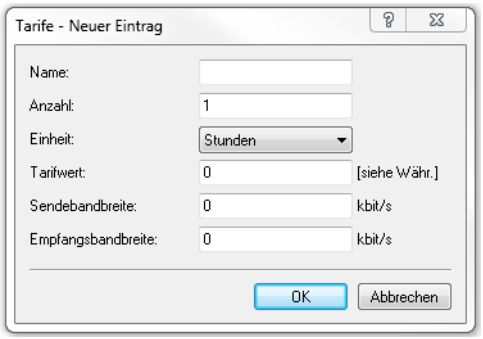
  - Beliebige IPv4-Adresse

- **Accounting-Informationen im Flash-ROM ablegen**: Aktivieren oder deaktivieren Sie, ob Ihr Gerät die Abrechnungsinformationen in regelmäßigen Abständen im internen Flash-ROM speichert. Dies geschieht standardmäßig stündlich, Sie können das betreffende Intervall aber über das Setup-Menü verändern. Aktivieren Sie diese Option, um bei einem Stromausfall den Komplettverlust von Accounting-Informationen zu vermeiden.

  Beachten Sie, dass ein häufiges Beschreiben dieses Speichers die Lebendauer Ihres Gerätes reduziert!

- **Login-Seite**: Wählen Sie aus der Liste, welche Anmeldemaske die Portalseite für Ihre PMS-Schnittstelle anzeigt. Mögliche Werte sind:
  - `kostenlos`: Wählen Sie diese Einstellung, wenn Sie Ihren Hotelgästen einen kostenlosen Internetzugang anbieten. Ihre Hotelgäste werden auf der Portalseite dennoch dazu aufgefordert, sich mit ihrem Benutzernamen, ihrer Zimmernummer und ggf. einer weiteren Kennung am Hotspot zu authentisieren, um eine Internetnutzung durch Unbefugte zu erschweren.
  - `kostenpflichtig`: Wählen Sie diese Einstellung, wenn Sie Ihren Hotelgästen einen kostenpflichtig Internetzugang anbieten. Ihre Hotelgäste werden auf der Portalseite dazu aufgefordert, sich mit ihrem Benutzernamen, ihrer Zimmernummer und ggf. einer weiteren Kennung am Hotspot zu authentisieren und einen Tarif auszuwählen.
- **Mehrfachanmeldung zulassen**: Aktivieren oder deaktivieren Sie, ob Sie einem Hotelgast erlauben, mehrere WLAN-Geräte mit den selben Zugangsdaten am Hotspot anzumelden.

- **Zusätzliche Anmeldung über Tickets anbieten**: Aktivieren oder deaktivieren Sie, ob Sie zusätzlich zur Anmeldung über die Kombination Benutzername/Zimmernummer auch die Anmeldung über Voucher erlauben.
- **Nutzungsbedingungen müssen akzeptiert werden**: Aktivieren Sie diese Checkbox, um Hotelgäste die Nutzungsbedingungen zur Verwendung Ihres Hotspots bestätigen zu lassen.
- **Tarife**: Sofern Sie einen kostenpflichtigen Internetzugang anbieten, verwalten Sie über diese Tabelle die Tarife für das Accounting.



  - **Name**: Legen Sie hier einen aussagekräftigen Tarifnamen fest.
  - **Anzahl**: Geben Sie hier die Höhe des Zeitkontingents ein, z. B. `1`. In Kombination mit der Einheit entspricht dies im oben gezeigten Screenshot z. B. 1 Stunde.
  - **Einheit**: Wählen Sie aus der Liste eine Einheit für das Zeitkontingent aus. Mögliche Werte sind: `Minuten`, `Stunden`, `Tage`
  - **Tarifwert**: Geben Sie hier die Höhe des Betrags ein, mit dem Sie die Zeitkontingente vergelten. In Kombination mit der in den Anmelde-Einstellungen gewählten Währung entspricht dies z. B. 50 Cent.
  - **Sendebandbreite**: Definieren Sie hier die maximal zulässige Sendebandbreite für diesen Tarif.
  - **Empfangsbandbreite**: Definieren Sie hier die maximal zulässige Empfangsbandbreite für diesen Tarif.

  Eine temporäre Abmeldung vom Public Spot verschiebt nicht den Ablaufzeitpunkt eines eingekauften Zeitkontingents! Es nicht möglich, ein bereits gekauftes Zeitguthaben zu "pausieren", um es zu einem späteren Zeitpunkt erneut aufzunehmen. Die Herunterzählung der Zeit beginnt unabhängig vom Anmeldestatus ab Kauf des Kontingents.

- **Währung**: Sofern Sie einen kostenpflichtigen Internetzugang anbieten, wählen Sie hier die Währungseinheit aus, mit der Sie die angebotenen Zeitkontingente (einstellbar über die Tarif-Tabelle) abrechnen. Diese Einheit erscheint ebenfalls auf der Portalseite. Achten Sie darauf, dass sie mit der Währung des PMS-Servers übereinstimmt. Mögliche Werte sind:
  - `Cent`
  - `Penny`

Erweiterte Einstellungsmöglichkeiten

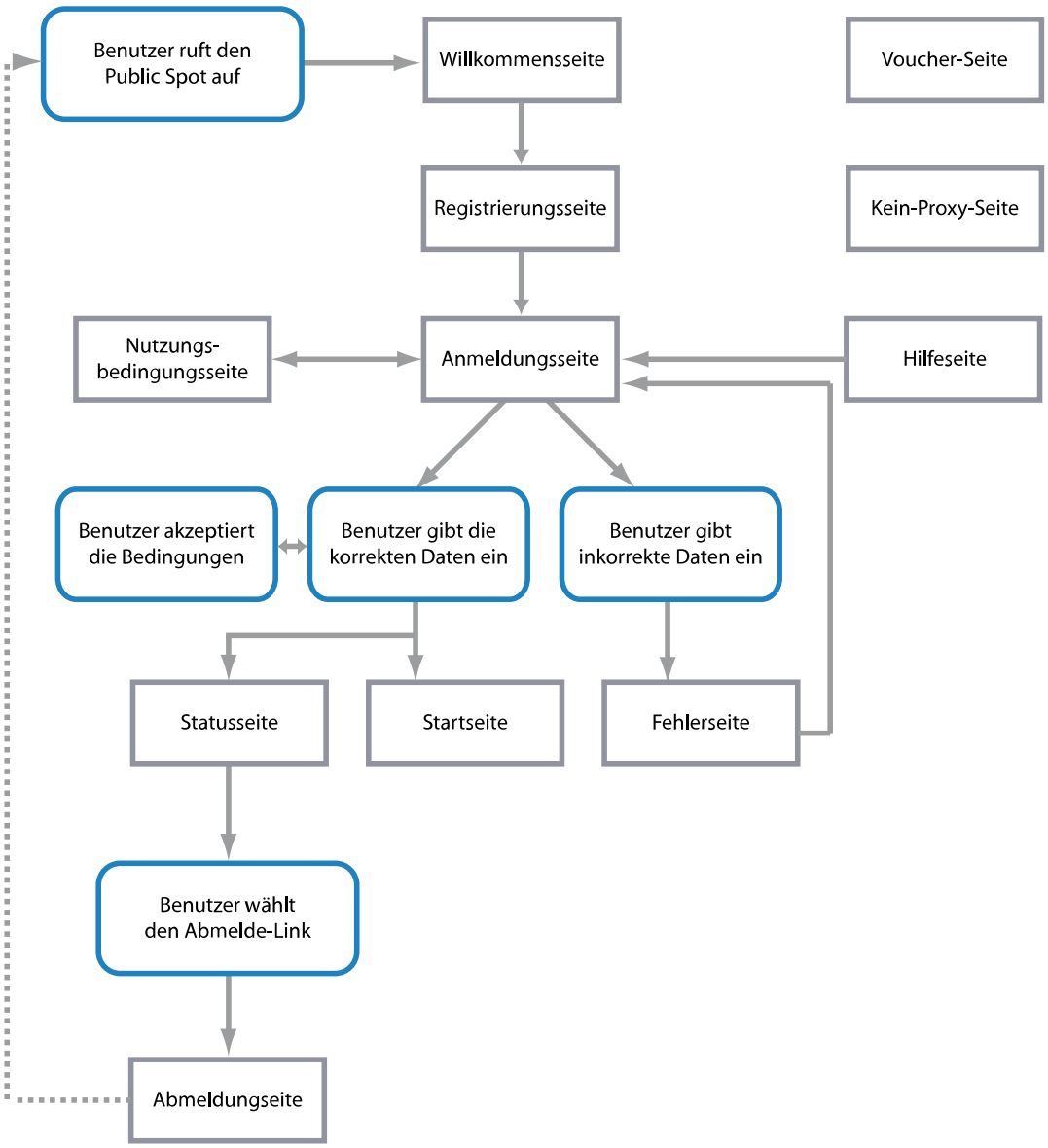
Erweiterte Einstellungen der PMS-Schnittstelle nehmen Sie auf der Konsole bzw. im Setup-Menü vor. Eine Übersicht aller zusätzlichen Parameter finden Sie im *Anhang*.

15.2.5 Geräteeigene und individuelle Voucher- und Authentifizierungsseiten (Templates)

Standardmäßig greift Ihr Gerät für die Anmeldeseite und alle übrigen Authentifizierungsseiten, die Ihre Benutzer vor, während und nach einer Public Spot-Sitzung angezeigt bekommen, auf geräteintern vorinstallierte Standardseiten (Templates) zurück. Sie haben jedoch auch die Möglichkeit, die einzelnen Webseiten Ihren Bedürfnissen entsprechend anzupassen und individuell zu gestalten. Sie benötigen dazu grundlegende HTML-Kenntnisse im Umgang mit DIV-Containern und Cascading Style Sheets (CSS), um die Struktur und das Layout der einzelnen Seiten gezielt zu verändern.

15.2.5.1 Mögliche Authentifizierungsseiten

Das nachfolgende Flussdiagramm zeigt Ihnen eine Übersicht und das Zusammenspiel aller vorhandenen Authentifizierungsseiten des Public Spot-Moduls. Die Abbildung orientiert sich dabei am Beispiel der Authentisierung mittels Zugangsdaten. Je nach Anmeldungsmodus und eventuell auftretender Fehler kann das Zusammenspiel von dem nachfolgend Gezeigten jedoch leicht abweichen:



Die Seiten **Willkommen** bzw. **Anmeldung** sind jene Seiten, die ein Benutzer angezeigt bekommt, wenn er erstmalig auf das Internet bzw. den Public Spot zugreift.

› Die Seite **Willkommen** ist dabei der Anmeldungsseite vorangestellt und in fast allen Anmeldungsmodi optional: Sie können diese Seite z. B. dafür verwenden, um einen Benutzer zu begrüßen, auf Informationen zum lokalen Angebot zu verweisen oder ihm eine Kurzanleitung zur Verwendung des Public Spot bereitzustellen, bevor er auf die Startseite mit dem Anmeldeformular gelangt. Nur wenn Sie den "Login nach Einverständniserklärung" als Anmeldungsmodus gewählt haben, ist eine individuelle Willkommensseite – welche die Einverständniserklärung beinhaltet – Pflicht, da sie an die Stelle des Anmeldeformulars auf der Anmeldungsseite tritt.

Die Standardseiten, die in Ihrem Gerät vorinstalliert sind, umfassen keine Willkommensseite. Wenn Sie eine solche Seite einrichten, ohne zuvor eine entsprechende Vorlage ins Gerät oder auf einen externen Server zu

laden, gelangt der Benutzer entweder direkt auf die Anmeldungsseite oder erhält eine Fehlermeldung (je nach Anmeldungsmodus).

- Die **Anmeldung** beinhaltet das Anmeldeformular, sofern für die Anmeldung am Public Spot die Authentisierung mittels Zugangsdaten und ggf. Anforderung der selben erforderlich ist.
- Die Seite mit den **Nutzungsbedingungen** ist nur dann zugänglich, wenn Sie die Bestätigung Ihrer Nutzungsbedingungen für den ausgewählten Anmeldungsmodus erforderlich gemacht haben. In diesem Fall erscheint unterhalb des Anmeldeformulars eine Checkbox mit einem zusätzlichen Link, der die Nutzungsbedingungen in einem Pop-Up öffnet.

Die Standardseiten, die in Ihrem Gerät vorinstalliert sind, umfassen für die Nutzungsbedingungs-Seite lediglich einen Platzhalter und keine generischen Nutzungsbedingungen.

Nachdem sich der Benutzer mit seinen Zugangsdaten (sofern erforderlich) autorisiert hat, überprüft das Gerät die Korrektheit der Angaben und stellt daraufhin entweder eine **Fehler**-Seite, die den Benutzer wieder auf die Anmeldeseite zurückführt, oder die **Start**-Seite dar.

- Die **Fehler**-Seite wird dabei lediglich gegenüber unauthentifizierten Public Spot-Benutzern ausgegeben und ist damit mehr oder weniger direkt mit dem Anmeldevorgang verknüpft. Typische Situationen, in denen ein Benutzer die Fehlerseite erhält, sind z. B. der unauthorisierte Zugriff auf den Public Spot, ein erreichtes Benutzerlimit sowie die fehlgeschlagene Authentifizierung durch Eingabe falscher Zugangsdaten oder Fehler beim Authentifizierungsserver. Sofern Sie eine zu überwachende Gegenstelle eingerichtet haben, erscheint die Seite außerdem immer dann, wenn das Public Spot-Modul einen Wegfall der WAN-Verbindung registriert, um einen mögliche Benutzer über die fehlende Verfügbarkeit des Netzwerks vorab zu informieren (siehe *Fehlerseite bei Wegfall der WAN-Verbindung einrichten* auf Seite 1307).

  Bereits authentifizierte Benutzer hingegen erhalten unabhängig von der Fehlerseite immer eine entsprechende Fehlermeldung von ihrem Browser.
- Sofern bei der Anmeldung keine Fehler auftraten, verifiziert die **Start**-Seite die erfolgreiche Anmeldung und leitet den Benutzer nach einigen Sekunden Wartezeit auf diejenige Internetseite weiter, die er ursprünglich erreichen wollte.

Zusätzlich öffnet sich nach einer erfolgreichen Anmeldung ein kleines Pop-Up, die **Status**-Seite:

- Die **Status**-Seite zeigt dem Benutzer aktuelle Informationen zu seiner Sitzung an (z. B. die bisherige Nutzungszeit, die gesendeten und empfangenen Datenmenge sowie Gültigkeitsdauer seines Kontos). Sie beinhaltet auch einen Link zum Schließen der aktuellen Sitzung und Beenden des Accountings. Klickt ein Benutzer auf diesen Link, gelangt er auf die Seite **Abmeldung**.
- Die Seite **Abmeldung** bestätigt einem Benutzer die erfolgreiche Abmeldung vom Public Spot.

Die verbleibenden Seiten **Rückfall-Fehler**, **Kein Proxy** und **Hilfe** sind isoliert und nicht unmittelbar mit dem Anmeldevorgang verknüpft.

- Die **Rückfall-Fehler**-Seite erscheint immer dann, wenn das Gerät eine benutzerdefinierte Template-Seite nicht ausliefern kann und der Rückfall auf die LCOS-interne Standardseite fehlt. Die Auslieferung scheitert z. B., wenn Sie innerhalb der Seiten-Tabelle einen falschen Datei-Pfad angegeben haben oder die Template-Seite noch nicht im Gerät vorhanden ist.
- Die **Kein-Proxy**-Seite erscheint immer dann, wenn ein Benutzer versucht, eine HTTP-Verbindung über den Port 8080 an Stelle des normalen HTTP-Ports 80 aufzubauen. Der Port 8080 wird in Intranets typischerweise für HTTP-Proxies verwendet. Da Proxies aber als statische IP-Adresse in den Browsereinstellungen hinterlegt werden, diese sich jedoch nicht über DHCP konfigurieren lassen, liesse sich der Proxy nicht erreichen. Die Seite hat daher nur den Zweck, dem Benutzer eine Anleitung zum Deaktivieren seiner Proxy-Einstellungen zu bieten, bevor er fortfahren kann.
- Die **Hilfe**-Seite ist lediglich ein Platzhalter, um bestimmte Informationen (z. B. Details zur Anmeldung oder Erhaltbarkeit von Vouchern) in die übrigen Authentifizierungsseiten (z. B. die Willkommensseite) einzubetten. Die vorinstallierten Seiten beinhalten keine Hilfe-Seite und auch keinen Link, der auf diese Seite verweist. Um die Hilfe-Seite zu nutzen, müssen Sie demnach eine individuelle Vorlagenseite einrichten.

Keine Authentifizierungsseite stellt die Seite **Voucher** dar: Hierbei handelt es sich um die grafische Vorlage für den Voucher-Druck. Indem Sie dafür eine eigene Vorlage hochladen, können Sie Tickets z. B. im Corporate Design Ihres Unternehmens ausgeben.

15.2.5.2 Vorinstallierte Standardseiten

Ihr Gerät enthält im Lieferzustand bereits einen Satz vorinstallierter Seiten, mit denen sich ein funktionsfähiger Public Spot-Betrieb bereitstellen lässt.

Die nachfolgende Tabelle gibt Ihnen eine schnellen Überblick über die im LCOS enthaltenen Standardseiten:

Tabelle 37: Übersicht aller vorinstallierten Standardseiten

Seitenbezeichnung	Vorinstalliert?
Willkommen…	nein
Anmeldung…	ja
Fehler…	ja
Start…	ja
Status…	ja
Abmeldung…	ja
Hilfe…	nein
Kein Proxy…	nein
Voucher…	ja
Nutzungsbedingungen…	nein
Rückfall-Fehler…	ja
Anmeldung(E-Mail)…	ja
Registrierung(E-Mail)…	ja
Anmeldung(E-Mail zu SMS)…	ja
Registrierung(E-Mail zu SMS)…	ja

Die Seiten wurden mit der Absicht entwickelt, so simpel wie möglich zu sein, und verwenden daher keine komplexen Techniken wie z. B. Java Skript oder dynamisches HTML. Durch die Verwendung von schlichtem XHTML und CSS für allein die notwendigen Elemente ist sichergestellt, dass sie auf einer Vielzahl von Browsern und Bildschirmgrößen korrekt angezeigt werden.

Als Betreiber eines Hotspots möchten Sie ggf. aber etwas anspruchsvollere Seiten darstellen oder eine möglichst neutrale Seite ohne Herstellerbezug anzeigen. Das Public Spot-Modul bietet Ihnen daher die Möglichkeit, einzelne Standardseiten wahlweise zu Personalisieren oder durch selbstgestaltete Seiten zu ersetzen. Letzteres erreichen Sie entweder mittels HTTP-Umleitungen oder Vorlagen, die Sie in das Gerät laden, und welche das Gerät dann wie ein intelligenter HTML-Preprozessor bearbeitet. Diese Seitenvorlagen lassen sich direkt in den Flash-Speicher laden, wodurch Sie auf einen externen HTTP-Server verzichten können.

Zusätzliche Sprachen für die Authentifizierungsseiten

LCOS 8.84 erweitert die vom Public Spot-Modul ausgegeben Authentifizierungsseiten (d. h. alle vorinstallierten Standardseiten bis auf die Voucher-Seite) um die Sprachunterstützung für Französisch, Spanisch, Italienisch und Niederländisch. Somit haben Sie die Möglichkeit, einem breiteteren internationalen Nutzerspektrum einen Public Spot-Zugang in der jeweiligen Landessprache anzubieten. Die Ausgabe der entsprechenden Sprache erfolgt wie bisher über die Spracheinstellungen des Webbrowsers, mit denen der Nutzer den Public Spot aufruft.

Die Mehrsprachigkeit bezieht sich ausschließlich auf die 8.84-internen Standardseiten. Mehrsprachige inidividuelle Vorlagenseiten lassen sich jedoch unter Zuhilfenahme eines externen Servers realisieren.

15.2.5.3 Personalisierung der Standardseiten

Als Alternative zu den benutzerdefinierten Seiten bietet Ihnen das Gerät die Möglichkeit, die vorinstallierten Standardseiten in begrenztem Umfang zu personalisieren. Hierzu gehören z. B. die Eingabe eines Login-Textes, welcher Ihren Benutzern innerhalb des Anmeldeformulars angezeigt wird, oder das Austauschen der Header-Grafik (dem sogenannten Kopfbild). Auf diese Weise können Sie schnell einen individuellen Public Spot-Betrieb bereitstellen, ohne sich eingehend mit dem Thema der Webseitenerstellung zu beschäftigen.

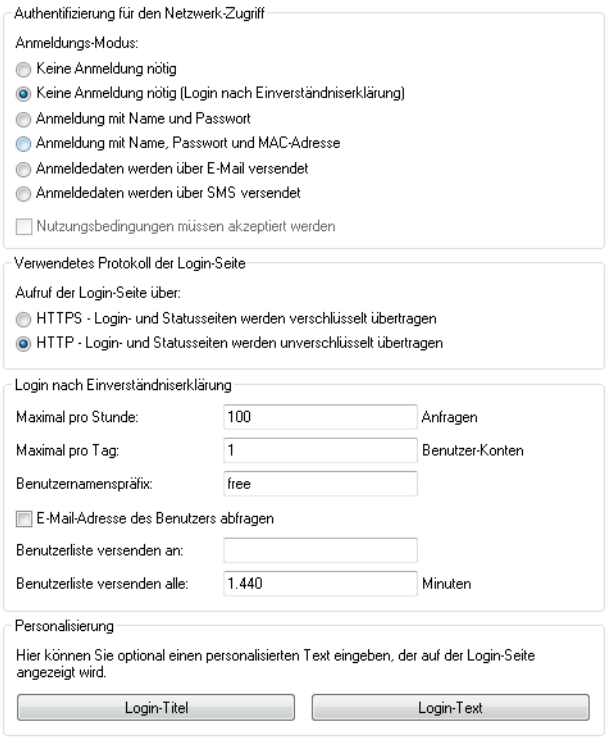
Individueller Text oder Login-Titel auf der Anmeldeseite

Sie haben innerhalb des Public Spot-Moduls die Möglichkeit, einen individuellen **Login-Text** und einen **Login-Titel** anzugeben, welche auf der Anmeldeseite innerhalb der Box des Anmeldeformulars eingeblendet wird. Sowohl Text als auch Titel sind in mehreren Sprachen definierbar (Deutsch, Englisch, Französisch, Italienisch, Spanisch und Niederländisch). Welche Sprache das Gerät letztlich ausgibt, hängt von den Spracheinstellungen des vom Benutzer verwendeten Webbrowsers ab. Wenn Sie für eine Sprache keinen individuellen Login-Text oder Titel spezifizieren, greift das Gerät auf den englischen Login-Text zurück (sofern vorhanden).

Bitte beachten Sie, dass es sich bei Login-Text und Login-Titel um unterschiedliche Elemente handelt!

Um einen individuellen Text oder einen Login-Titel auf der Anmeldeseite einzurichten, führen Sie die nachfolgenden Schritte aus.

1. Öffnen Sie in LANconfig den Konfigurationsdialog für das betreffende Gerät.
2. Wechseln Sie in den Dialog **Public Spot** > **Anmeldung**, klicken Sie auf die Schaltfläche **Login-Text** (alternativ **Login-Titel)** und wählen Sie eine Sprache aus.



3. Tragen Sie in dem sich öffnenden Dialog den Text ein, den Sie Ihren Public Spot-Nutzern anzeigen möchten. Erlaubt ist ein HTML-String mit max. 254 Zeichen, bestehend aus:

```
[Leerzeichen][0-9][A-Z[a-z] @{|}~!$%&amp;'()+-,/:;&lt;=>?[\]^_.#*
```

LANconfig transformiert eingegebene Umlaute automatisch in ihre entsprechenden Umschreibungen (`ü` zu `ue`; `ß` zu `ss`; usw.). Um Umlaute einzugeben, müssen Sie deren HTML-Äquivalente verwenden (z. B. `ü` für `ü`), da

der Text unmittelbar in die Webseite eingebunden wird. Über HTML-Tags haben Sie außerdem die Möglichkeit, den Text zusätzlich zu strukturieren und zu formatieren. Beispiel:

```
Herzlich Willkommen!<br/><i>Bitte f&uuml;llen Sie das Formular aus.</i>
```

4. Klicken Sie **OK**, um die Eingabe abzuschließen, und laden Sie die Konfiguration zurück in das Gerät.

Nach dem erfolgreichen Schreiben der Konfiguration erscheinen Login-Text und Login-Titel beim nächsten Aufruf der Public Spot-Seite.



Individuelle Kopfbilder für variable Bildschirmbreiten

Bestandteil der im Gerät vorinstallierten Seiten ist eine Header-Grafik (Kopfbild genannt), die Ihren Benutzern beim Aufruf des Public Spots oberhalb des Anmelde-Formulars anzeigt wird. Sie können dieses Kopfbild nach Belieben ändern, um z. B. eine dem Einsatzumfeld oder Ihrem Corporate Design angemessene Grafik einzubinden. Sie benötigen dafür keine externen Webserver, sondern können über das Dateimanagement in WEBconfig bzw. die Konfigurationsverwaltung in LANconfig die Grafik direkt ins Gerät laden.

Eine Besonderheit des Kopfbildes ist dabei, dass es im Gerät in zwei unterschiedlichen Varianten vorliegt: Einmal als Großbild für Bildschirme bzw. Browser-Fenster mit einer horizontalen Auflösung >800 px (normale Monitore, Laptops, Tablet-PCs usw.) und einmal als Kleinbild für Bildschirme mit einer geringeren horizontalen Auflösung (PDAs, Mobiltelefone

usw.). Auf diese Weise haben Sie die Möglichkeit, Kopfbilder für unterschiedliche Zielgruppen bereitzustellen und diesen stets ein für Ihr Gerät geeignetes Anmelde-Formular anzubieten.

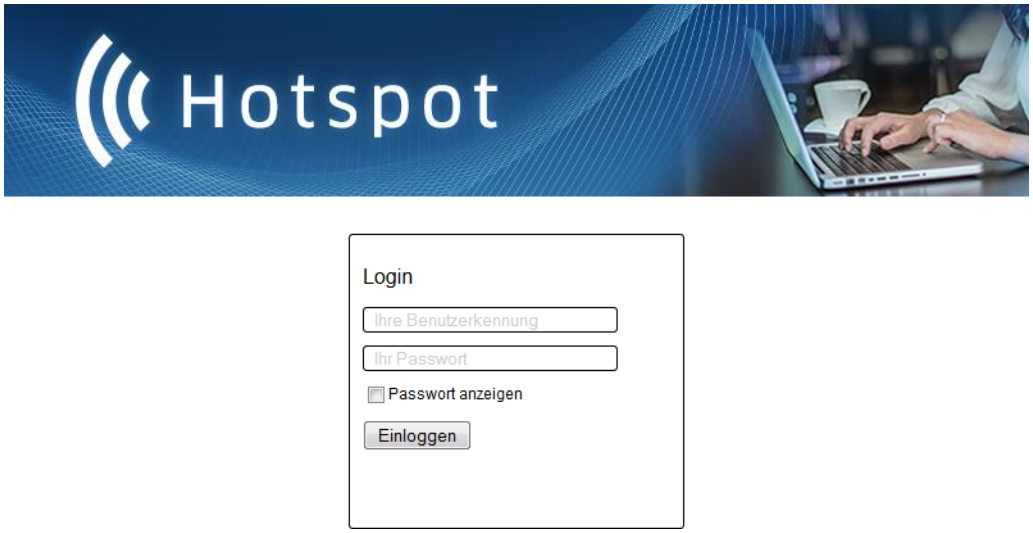


Abbildung 30: Anmeldeseite für breite Bildschirme



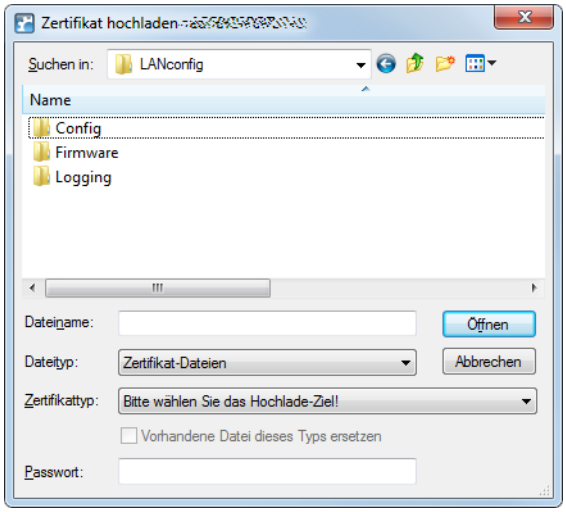
Abbildung 31: Anmeldeseite für schmale Bildschirme

Die möglichen Auflösungen werden durch die CSS-Datei des Gerätes vorgegeben. Für die vorinstallierten Standardgrafiken betragen sie 800x150 px für das Großbild und 258x52 px für das Kleinbild. Der Dateityp muss entweder JPG, GIF oder PNG sein.

Um ein neues Kopfbild als Groß- oder Kleinvariante ins Gerät zu laden, führen Sie die nachfolgenden Schritte aus.

1. Starten Sie LANconfig und markieren Sie das betreffende Gerät.

2. Klicken in der Menüleiste auf **Gerät** > **Konfigurations-Verwaltung** > **Zertifikat oder Datei hochladen**. Der Dialog **Zertifikat hochladen** öffnet sich.



3. Stellen Sie den **Dateityp** auf **Alle Dateien** und wählen Sie den **Zertifikattyp**, den Sie hochladen möchten.
   - **Public Spot – Kopfbild Seiten**: Zertifikattyp für das Großbild
   - **Public Spot – Kopfbild Box**: Zertifikattyp für das Kleinbild

4. Wählen Sie Ihr individuelles Kopfbild aus und klicken Sie auf **Öffnen**. LANconfig beginnt daraufhin mit dem Dateiupload.

Nach dem erfolgreichen Upload erscheint das neue Kopfbild beim nächsten Aufruf der Public Spot-Seite.

Sie können das Zusammenspiel von großem und kleinen Kopfbild überprüfen, indem Sie den Public Spot mit einem Browserfenster >800 px aufrufen und dann die Fensterbreite verkleinern. Durch die eingesetzten CSS-Techniken schaltet die Webseite automatisch zwischen Groß- und Kleinbild um.

Hersteller-Logo und -Kopfbild im Voucher ein-/ausblenden

Ein vom Gerät ausgegebener Voucher enthält standardmäßig das von der Public Spot-Startseite bekannte Kopfbild und Logo. Sie haben die Möglichkeit, die Einbindung dieser Grafiken über die Option **Public-Spot** > **Assistent** > **Kopfbild und Logo mitdrucken** direkt im Gerät zu deaktivieren, ohne dafür ein individuell angepasstes Vouchers-Template einzusetzen, welches diese Grafiken entfernt. In dem Fall gibt das Gerät lediglich einen textneutralen Voucher aus.

15.2.5.4 Konfiguration benutzerdefinierter Seiten

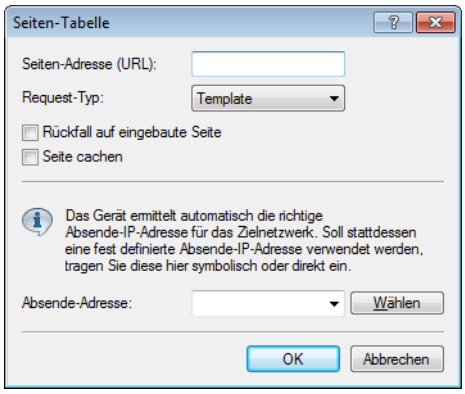
Sofern Sie die vorinstallierten Seiten durch selbstgestaltete Webseiten ersetzen möchten, können Sie diese entweder direkt im Gerät oder auf einem externen HTTP-Server ablegen. Anspruchsvollere HTML-Seiten benötigen ggf. mehr Speicherplatz, als im Gerät zur Verfügung steht. Darüber hinaus bietet Ihnen die Bereitstellung der Webseiten durch einen externen Server noch weitere Vorteile:

- Änderungen lassen sich zentral durchführen. Dadurch reduziert sich der Aufwand, die Anmeldeseiten bei Einsatz mehrerer Geräte in jedem Gerät ändern zu müssen.
- Der Server kann dynamische Seiten bereitstellen, deren Erscheinungsbild davon beeinflusst wird, welche Informationen ihm das Gerät liefert. Auf diese Informationen wird in den folgenden Kapiteln noch näher eingegangen.

Der Speicherort der Vorlagenseiten geben Sie im LANconfig unter **Public-Spot** > **Server** > **Seiten-Tabelle** > **<Name der Vorlagenseite>** > **Seiten-Adresse (URL)** ein. Es stehen Ihnen drei Protokolle für die URL zur Auswahl:

- `http://`...: Lädt die Seite über HTTP von einem externen Server herunter. Das Überschreiben des Standard-TCP-Ports sowie das Angeben von Benutzerdaten ist möglich
- `https://`...: Verhält sich genau wie HTTP, aber verwendet SSL um die Verbindung zu verschlüsseln.

› `file://...`: Verwendet eine Vorlage aus dem lokalen Speicher des Geräts.



Sie können beliebige Dateinamen verwenden. Sofern Sie sich für die Ablage der Templateseiten im lokalen Speicher des Geräts entscheiden, verwendeten Sie die speziell für den jeweiligen Zweck reservierten URLs. Durch Angabe der lokalen URL als **Seiten-Adresse (URL)** z. B. wird eine geräteeigene Standardseite durch eine ins Gerät geladene Seite ersetzt.

Tabelle 38: Übersicht der reservierten Dateinamen für Vorlagenseiten

Lokale URL im Gerät	Seitenbezeichnung
file://pbspot_template_welcome	Willkommen…
file://pbspot_template_login	Anmeldung…
file://pbspot_template_error	Fehler…
file://pbspot_template_start	Start…
file://pbspot_template_status	Status…
file://pbspot_template_logoff	Abmeldung…
file://pbspot_template_help	Hilfe…
file://pbspot_template_noproxy	Kein Proxy…
file://pbspot_template_voucher	Voucher…*
file://pbspot_template_agb	Nutzungsbedingungen…
file://pbspot_template_fallback	Rückfall-Fehler…
file://pbspot_template_reg_email	Registrierung(E-Mail)…
file://pbspot_template_login_email	Anmeldung(E-Mail)…
file://pbspot_template_reg_sms	Registrierung(E-Mail zu SMS)…
file://pbspot_template_login_sms	Anmeldung(E-Mail zu SMS)…

*) Vorlagenseite für den Voucher-Druck, keine Authentifizierungsseite

Durch das Hochladen benutzerdefinierter Webseiten werden die im Geräte vorinstallierten Webseiten nur ersetzt, nicht jedoch überschrieben. Sie können durch Löschen der lokalen URL jederzeit wieder zu den geräteeigenen Standardseiten zurückkehren.

Um eine Möglichst hohe Kompatibilität mit den verschienenen Anzeigegeräten und Web-Browsern zu erreichen, sollten Sie nach Möglichkeit auf den Einsatz von Frames verzichten. Auch spezielle Inhalte (JavaScript, Plug-In-Elemente) können zu einer fehlerhaften Anzeige führen.

Login-Seiten in Abhängigkeit vom Anmeldungsmodus

Die nachfolgende Tabelle liefert Ihnen darüber hinaus eine Übersicht, welche Login-Seite das Gerät in welchem Anmeldungsmodus ausgibt. Sofern für einen Anmeldungsmodus keine individuelle Seitenvorlage eingerichtet ist; verwendet das Public Spot-Modul dafür die 8.84-interne Standardseite:

Tabelle 39: Übersicht der Login-Seiten der einzelnen Anmeldungsmodi

Anmeldungsmodus	Seitenbezeichnung
Keine Anmeldung nötig	–
Keine Anmeldung nötig (Login nach Einverständniserklärung)	Willkommen…
Anmeldung mit Name und Passwort	Anmeldung…
Anmeldung mit Name, Passwort und MAC-Adresse	Anmeldung…
Anmeldedaten werden über E-Mail versendet	› Registrierung(E-Mail)… › Anmeldung(E-Mail)…
Anmeldedaten werden über SMS versendet	› Registrierung(E-Mail zu SMS)… › Anmeldung(E-Mail zu SMS)…

Besondere Template-Seiten für Smart Ticket

Während das Public Spot-Modul in LCOS-Versionen vor 8.84 noch eine zentrale Login-Seite für sämtliche Anmeldemodi verwendet, haben Sie ab LCOS 8.84 die Möglichkeit, für die Smart-Ticket-Funktion (die selbstständige Benutzeranmeldung via E-Mail/SMS) gesonderte Template-Seiten ins Gerät zu laden. Dazu konfigurieren Sie für die Anmeldung über E-Mail/SMS je zwei Seiten: **Registrierung(…)** und **Anmeldung(…)**.

- Auf der Registrierungsseite geben Benutzer zunächst ihre persönlichen Daten (E-Mail-Adresse oder Mobilfunknummer) ein, um sich beim Public Spot zu registrieren und dessen Zugangsdaten anzufordern.
- Auf der Anmeldungsseite geben Benutzer die ihnen zugesendeten Zugangsdaten ein, um sich schlussendlich am Public Spot zu authentisieren.

Die nachfolgende Tabelle liefert Ihnen eine Übersicht aller damit in Verbindung stehenden Abhängigkeiten, die Sie für das erstellen eigener Seitenvorlagen (Templates) benötigen:

Tabelle 40: Übersicht der Abhängigkeiten der SmartTicket-Anmeldeseiten

Anmeldungsmodus	Seitenbezeichnung	Lokale URL im Gerät	Seitenvorlagen-Bezeichner
Anmeldedaten werden über E-Mail versendet	Registrierung(E-Mail)…	file://pbspot_template_reg_email	<regemailform>
	Anmeldung(E-Mail)…	file://pbspot_template_login_email	<loginemailform>
Anmeldedaten werden über SMS versendet	Registrierung(E-Mail zu SMS)…	file://pbspot_template_reg_sms	<regsmsform>
	Anmeldung(E-Mail zu SMS)…	file://pbspot_template_login_sms	<loginsmsform>

15.2.5.5 Einrichten einer individuellen Vorlagenseite

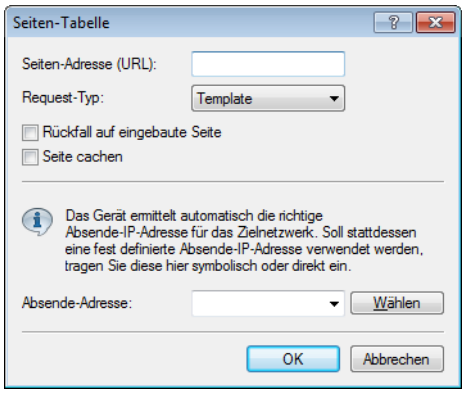
Über eine individuelle Vorlagenseite (auch Template-Seite genannt) haben Sie Möglichkeit, die LCOS-eigenen Vorlagenseiten durch eigene Webseiten zu ersetzen. Die LCOS-eigenen Vorlagenseiten werden dabei nicht überschrieben, sondern lediglich gegen Ihre eigene Seite ausgetauscht, sodass Sie bei Bedarf auf diese standardmäßig installierten Seiten zurückgreifen können.

Die nachfolgenden Schritte zeigen Ihnen am Beispiel einer **Login**-Seite, wie Sie mit Hilfe von LANconfig eine individuelle Vorlagenseite korrekt einrichten.

1. Laden Sie Ihre individuell erstellte Fehlerseite wahlweise auf einen externen HTTP(S)-Server oder als **Public Spot – Login-Seite (*.html, *.htm)** in den Speicher des Gerätes.

Weitere Informationen zum Hochladen eigener Templates sowie entsprechende Beispieldateien finden Sie im Internet in der *LANCOM Support Knowledgebase* unter *Implementierung eigener Webseiten für die LANCOM Public Spot Option*.

2. Öffnen Sie den Konfigurationsdialog des Gerätes in LANconfig, wechseln Sie in den Dialog **Public-Spot** > **Server** und wählen Sie **Seiten-Tabelle** > **Anmeldung**.



3. Tragen Sie unter **Seiten-Adresse (URL)** wahlweise die URL der Anmeldungsseite auf dem externen Server oder den gerätelokalen Dateiverweis ein (`file://pbspot_template_login`).

4. Nehmen Sie bei Bedarf weitere optionale Einstellungen vor.

   - **Request-Typ**: Sofern Sie einen externen Server einsetzen, haben Sie die Möglichkeit die Art des Seitenaufrufs verändern. Standardmäßig (in der Einstellung **Template)** lädt das Gerät eine extern gespeicherte HTM(L)-Seite von der angegebenen URL zur weiteren Verarbeitung durch den internen HTTP-Server. Wenn Sie die Einstellung zu **Redirect** ändern, lagert das Gerät die Seiten-Erzeugung an den externen Server aus (siehe auch *Benutzerdefinierte Seiten via HTTP Redirect* auf Seite 1358).
   - **Rückfall auf eingebaute Seite**: Sofern Sie einen externen Server einsetzen und als Template-Typ **Request** gewählt haben, besteht die Möglichkeit, dass das Public Spot-Modul im Falle von HTTP(S)-Fehlern (z. B. Unerreichbarkeit des Servers) die LCOS-eigene Vorlagenseite benutzt, um ggf. einen Weiterbetrieb des Public Spots zu ermöglichen (siehe auch *Auto-Fallback* auf Seite 1358. Wenn Sie diese Einstellung nicht aktivieren, zeigt der Public Spot stattdessen die Rückfall-Fehler-Seite an.
   - **Seite cachen**: Auf einigen Geräten haben Sie die Möglichkeit, lokale und externe Templates zu cachen. Mehr dazu erfahren Sie unter *Template Caching* auf Seite 1357.
   - **Absende-Adresse**: Über diese Einstellung definieren Sie optional die Loopback-Adresse, die das Gerät benutzt, um sich mit dem externen HTTP(S)-Server zu verbinden. Standardmäßig schickt der Server seine Antworten zurück an die IP-Adresse Ihres Gerätes, ohne dass Sie diese hier angeben müssen. Durch Angabe einer optionalen Loopback-Adresse verändern Sie die Quelladresse bzw. Route, mit der das Gerät den Server anspricht. Dies kann z. B. dann sinnvoll sein, wenn der Server über verschiedene Wege erreichbar ist und dieser einen bestimmten Weg für seine Antwort-Nachrichten wählen soll.

5. Schließen Sie den Dialog sowie den allgemeinen Konfigurationsdialog mit jeweils einem Klick auf **OK**. LANconfig schreibt die getätigten Einstellungen daraufhin zurück in das Gerät.

Fertig!

Grafiken in benutzererstellte Vorlagenseiten einbinden

Für Ihre Seiten stehen Ihnen weitere fünf Bilder-Slots (Voucher-Bild 1 bis Voucher-Bild 5) zur Verfügung, mit denen Sie Bilder für Ihre Voucher ins Gerät laden können. Diese werden im Flash-Speicher abgelegt und verleiben im Gerät.

Übertragen Sie dazu die gewünschten Bilder in das Gerät wie im Abschnitt *Individuelle Kopfbilder für variable Bildschirmbreiten* beschrieben. Wählen Sie beim Upload als **Zertifikattyp** "Public Spot – Voucher-Bild 1" bis "Public Spot – Voucher-Bild 5".

Modifizieren Sie das jeweilige HTML-Template des betreffenden Vouchers (z. B. mit einem Texteditor wie Notepad++) und referenzieren Sie die hochgeladenen Bilder, indem Sie diese als `<img src="/images/voucherimg1">` bis `<img src="/images/voucherimg5">` in die Vorlage einbauen. Wie Sie eine individuelle Vorlagenseite einrichten, lesen Sie im Abschnitt *Einrichten einer individuellen Vorlagenseite*.

15.2.5.6 Template Caching

Bei der Konfiguration benutzerdefinierter Template-Seiten haben Sie auf Geräten mit hinreichend großem Arbeitsspeicher (z. B. Public Spot-Gateways) die Möglichkeit, Templates im Gerät zu cachen. Das Caching verbessert die Performance des Public Spot-Moduls insbesondere in größeren Szenarien, indem das Gerät einmal geladene Templates und daraus erzeugte HTML-Seiten intern zwischenspeichert.

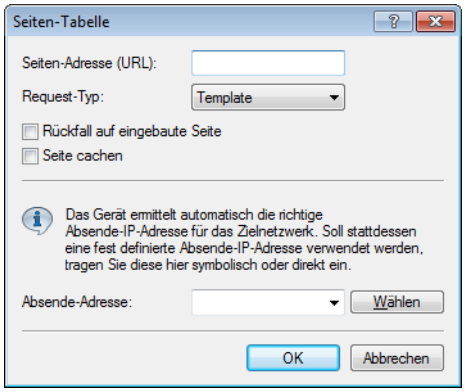
Das Caching ist möglich für:

- Templates abgelegt im lokalen Dateisystem
- Templates abgelegt auf externen HTTP(S)-Servern über statische URLs

Templates auf externen Servern, die mittels Template-Variablen referenziert werden, werden vom Gerät nicht gecached.

Template Caching aktivieren

Um das Caching für eine Seitenvorlage zu aktivieren, setzen Sie in LANconfig unter **Public-Spot** > **Server** > **Seiten-Tabelle** > **<Name der Vorlagenseite>** die Einstellung **Seite cachen**.



Im Setup-Menü finden Sie den dazugehörigen Paramter unter **Public-Spot-Modul** > **Seitentabelle** > **Template-Cache** .

Template Cache löschen

Das Gerät löscht bzw. aktualisiert im Cache gespeicherte Templates automatisch, sobald Sie eine neue Template-Datei in das Dateisystem Ihres Gerätes laden (bei lokaler Speicherung) bzw. die Cache-Zeit für ein HTTP(S)-Template abläuft (bei Speicherung auf externem einem Server). Hierzu wertet das Gerät den `Cache-Control`-Header eines HTTP(S)-Templates aus, um die maximale Cache-Zeit zu erfahren.

Sofern kein `Cache-Control`-Header gesetzt ist, wird die Webseite nicht gecached und direkt wieder verworfen.

Achten Sie beim Einrichten eines individuellen Templates somit darauf, das entsprechende META-Tag in Verbindung mit einer sinnvollen Cache-Zeit (in Sekunden) zu setzen, z. B. `<meta http-equiv="cache-control" content="max-age=60">`. Die Dauer der Cache-Zeit ist dabei vom Szenario abhängig; es gibt keine konkreten Empfehlungen.

Sie haben aber auch die Möglichkeit, den Template Cache über eine Aktion manuell zu löschen. Starten Sie dazu im Status-Menü unter **Public-Spot** die Aktion **Flush-Template-Cache**.

15.2.5.7 Benutzerdefinierte Seiten via HTTP Redirect

Sofern Sie benutzerdefinierte Seiten als Umleitung realisieren (Request-Typ: Redirect), setzt Ihr Gerät diese wie folgt um: Immer, wenn Ihr Gerät eine betreffende Seite an einen Client liefern muss, erweitert es die URL gemäß der im vorangegangenen Kapitel vorgestellten Platzhalter und sendet eine HTTP-Antwort 307 (temporäre Umleitung) mit dieser URL an den Client.

Umleitungen sind besonders dann sinnvoll, wenn Sie eine Willkommensseite verwenden und alle Authentifizierungen auf einem externen Gateway erfolgen sollen. In diesem Fall können die Clients sofort zu diesem Gateway umgeleitet werden. Dieses Feature wird oft gemeinsam mit der externen Gerätekontroller verwendet.

15.2.5.8 Benutzerdefinierte Seiten über Seitenvorlagen

Alternativ kann das Gerät auch selbst als Client auftreten und die erweiterte URL verwenden um, um über eine HTTP-Verbindung die benutzerdefinierte Seite herunterzuladen. Der interne Preprozessor übernimmt die Bearbeitung der Seite und sendet das Ergebnis anschließend an den Public Spot-Nutzer. Diese Vorverarbeitung erlaubt es, Session-spezifische Daten zu verarbeiten, obwohl der Server eine statische Seite bereithält. Das Gerät verwendet Syntax-Befehle, wie sie bei Web-Browsern bekannt sind. Allerdings beherrscht es allerdings nur eine Teilmenge der möglichen Befehle:

- Die Benutzer-Authentifizierung erfolgt über die Form `user:password@host/...`
- Das Gerät kann nicht-fatale HTTP-Fehler, wie z. B. Redirects, nicht automatisch bereinigen. Stellen Sie also sicher, dass der Zugriff auf die Seite diese Seite auch direkt ausgibt.

Sie können symbolische Namen anstatt IP-Adressen für die Server-Hosts verwenden, solange der DNS korrekt konfiguriert ist. Dieser Mechanismus lässt sich daher in vielerlei Hinsicht als ein Proxy begreifen, der HTML-Seiten einholt und dann an die Clients weiterreicht. Der größte Unterschied ist dabei, dass die URL der Seiten im Gerät und nicht vom Client des Public Spot-Benutzers festgelegt werden.

Auto-Fallback

Für jeden Eintrag in der Seiten-Tabelle lässt sich individuell festlegen, ob eine Fallback-Funktion benutzt werden soll oder nicht. Diese Fallback-Funktion hat nur dann eine Bedeutung, wenn eine Seite als Vorlage (Request-Typ: Template) und nicht als Umleitung (Request-Typ: Redirect) definiert ist. Beim Herunterladen einer Seite über HTTP können eine Reihe von Fehlern auftreten:

- Das Nachschlagen eines Hosts beim DNS kann fehlschlagen.
- Die TCP/HTTP-Verbindung zum Server kann fehlschlagen.
- Der HTTP-Server kann eine Fehlermeldung ausgeben (wie z. B. 404, wenn eine ungültige URL angefragt wurde).

Standardmäßig gibt das Gerät solche Fehler an den Benutzer weiter, damit dieser eine erneute Anfrage starten oder den Betreiber des Public Spots davon in Kenntnis setzen kann. Alternativ kann das Konfigurieren einer Fallback-Funktion sicherstellen, dass der Hotspot weiter funktioniert, indem das Gerät stattdessen die standardmäßig installierten Seiten verwendet. Sie aktivieren die Fallback-Funktion im LANconfig über die Einstellung **Rückfall auf eingebaute Seite**.

Weitergegebene HTTP-Attribute

Wie bereits erwähnt kann das Gerät in einige Punkten als eine Art HTTP-Proxy gesehen werden, dass die Anmelde- und Status-Seite einholt. HTTP-Proxies sollten bestimmte Attribute intakt lassen, wenn Sie Anfragen des Clients weiterleiten:

- Das Gerät leitet Cookies zwischem dem Client und dem Server weiter. Cookie-Werte des Clients können also den Server transparent erreichen, und der Server kann Cookies auf dem Client setzen. Der Einsatz von Cookies ist notwendig, wenn die vom Server gesendeten Dateien aus ASP-Skripten stammen, da ASP die Session-ID in einem Cookie hinterlegt.
- Das Gerät wird den `User-Agent`-Wert des Clients unverändert weiterleiten. Dadurch kann der Server verschiedene Seiten je nach Browser und Betriebssystem ausgeben. PDAs und Mobiltelephone erwarten für kleine Bildschirme optimierte Seiten.
- Das Gerät wird eine `X-Forwarded-For`-Zeile in die HTTP-Anfrage anfügen um die IP-Adresse des Clients zu übermitteln..

› WEBconfig versucht die eigene Sprache anhand der durch `Accept-Languages` gelieferten Sprachpräferenz auszurichten und dann anhand der internen Datenbank auszugeben (momentan nur Englisch und Deutsch). Die gewählte Sprache wird dem Server durch ein weiteres `Accept-Languages`-Tag gemeldet, damit dieser eine Seite in der korrekten Sprache anbieten kann. Beim Übertragen der Seite prüft das Gerät, ob die Seite ein Language-Tag enthält. Wird es nicht gefunden, ersetzt das Gerät die Spracheinstellungen in der Vorlage mit der tatsächlich genutzten Sprache.

15.2.5.9 URL-Platzhalter (Template-Variablen)

Die URLs in der Seiten-Tabelle brauchen keine konstante Adresse darstellen. Sie haben die Möglichkeit, bestimmte Platzhalter – auch Template-Variablen genannt – in die Adresse zu integrieren, die dann mit den Parametern einer Public Spot-Sitzung gefüllt werden, wenn das Gerät die Seiten vom Server anfordert. Die Platzhalter haben dabei ein ähnliches Format wie in der Programmiersprache C; also ein Prozentzeichen, welchem unmittelbar ein einzelner, kleingeschriebener Buchstabe folgt. Folgende Platzhalter sind definiert:

%a

Fügt die IP-Adresse des Geräts ein. Dieser Platzhalter liefert nur dann einen Wert, wenn der **Request-Typ** in der **Seiten-Tabelle** auf `Template` gesetzt ist.



Bitte beachten Sie, dass dieser Platzhalter keine erreichbare Adresse erzeugt, wenn das Gerät sich hinter einem Router mit aktiviertem NAT befindet.

%c

Fügt die LAN-MAC-Adresse des Public Spot-Gerätes als 12-stelligen Hexadezimal-String ein. Die Ausgabe erfolgt im Format 'aa:bb:cc:dd:ee:ff'.

%d

Geben Sie den URL-Parameter "%d" als Circuit-ID an, z. B. `http://ipaddress/?circuit=%d&nas=%i`. Diese Variable ersetzt das Public Spot Modul mit der Circuit-ID, die im DHCP-Request des Clients erkannt wurde.

Dafür ist es erforderlich, dass auf dem AP "DHCP Snooping" so konfiguriert ist, dass der AP die Circuit-ID in der Public Spot-Stationstabelle des WLCs abfragen kann.

Somit ist es möglich, die Public Spot-Willkommensseite auf den angemeldeten Clients je nach Standort zu verändern.

%e

Fügt die Seriennummer des Geräts ein.

%i

Fügt die NAS-Port-Id ein. 'NAS' steht in diesem Zusammenhang für 'Network Access Server'. Diese Variable überträgt das Interface des Gerätes, über das sich ein Client anmeldet. Bei einem WLC oder Router ohne WLAN entspräche dies einer physischen Schnittstelle wie z. B. `LAN-1`, bei einem Standalone-Access-Point hingegen der SSID.

%l

Fügt den Hostnamen des Geräts ein.

%m

Fügt die MAC-Adresse des Clients als 12-stelligen Hexadezimal-String ein. Die individuellen Bytes werden durch zwei Doppelpunkte getrennt.

%n

Fügt den Namen des Geräts ein, wie er im Setup-Menü unter **Name** konfiguriert ist.

%o

Fügt die URL der Internetseite ein, die der Benutzer ursprünglich angefordert hat. Nach erfolgreicher Authentifizierung leitet das Gerät den Benutzer an diese URL weiter.

%p

Fügt die IP-Adresse des Public Spot-Gerätes in dem ARF-Kontext des jeweiligen Clients ein.

Sofern Ihr Gerät also in verschiedenen IP-Netzwerken aktiv ist, können Sie über diese Variable die IP-Adresse angeben, welche das Gerät in dem Netz benutzt, in dem auch der Client anzutreffen ist.

%r

Fügt die IP-Adresse des Clients ein (aus Sicht des Public Spot-Gerätes in dem jeweiligen ARF-Kontext).

%s

Fügt die WLAN SSID des Netzwerks ein, über das sich der Client verbunden hat. Diese Funktion ist besonders dann interessant, wenn sie MultiSSID verwenden, da der Server hierüber die Möglichkeit erhält, in Abhängigkeit von der SSID verschiedene Seiten auszugeben. Sollte der Client über einen anderen Access Point, welcher sich mit dem Gerät über ein Punkt-zu-Punkt-WLAN verbindet, verbunden sein, fügt dieser Platzhalter die SSID des ersten WLANs ein. Wenn der Client über Ethernet verbunden ist, produziert dieser Platzhalter einen leeren Wert.

%t

Fügt das Routing-Tag ein, mit dem die Datenpakete des Clients versehen werden.

%v

Sofern dem anfragenden Client eine individuelle VLAN-ID zugewiesen wurde, überträgt diese Variable die Quell-VLAN-ID.

%0-9

Fügt eine einzelne Zahl im Bereich von 0 bis 9 ein.

%%

Fügt ein einzelnes Prozentzeichen ein.

Um die Variablen für ein Template zu verwenden, ergänzen Sie in der Seiten-Tabelle die angegebene **Seiten-Adresse (URL)** um die betreffemden Parameter. In den nachfolgenden URLs würde `%i` gemäß dem o. g. Beispielwert durch `LAN-1` ersetzt werden:

Beispiel: `http://192.168.1.1/willkommen.php?nas=%i`

Beispiel: `http://192.168.1.1/%i_willkommen.html`

15.2.5.10 Seitenvorlagen-Tags und Syntax

Nachdem das Gerät die Seite vom Server empfangen hat, führt es einige Transformationen an den Seitenvorlagen durch, bevor es die Seite an den Client weitergibt. Diese Transformationen ersetzen die vordefinierten HTML-Tag-Platzhalter mit Daten der aktuellen Session (z. B. der aktuelle Ressourcenverbrauch in der Status-Seite). Eine vom Server bereitgestellte Seite sollte daher eher als eine Vorlage für eine HTML-Seite betrachtet werden. Die HTML-Syntax wurde deshalb für die Platzhalter gewählt, weil dadurch das Erstellen der Seiten mit Hilfe handelsüblicher HTML-Editoren möglich ist, ohne die Syntax zu verletzen.

Insgesamt sind drei Platzhalter-Tags definiert:

› `<pblink **identifier**>**text**</pblink>`

Markiert **text** als einen klickbaren Link zu **identifier**, typischerweise um eine andere Seite zu verknüpfen. Bitte beachten Sie, dass `</pblink>` nur ein Alias für `</a>` ist, da eine solch symetrische Definition zu weniger Probleme mit den gängigen HTML-Editoren führt. Das folgende Fragment definiert z. B. einen Link zur Hilfe-Seite:

```
Bitte klicken Sie <pblink helplink>hier</pblink> um weitere Hilfe aufzurufen.
```

› `<pbelem **identifier**>`

Fügt den unter **identifier** als Bezeichner angegebenen Wert an diesem Ort ein. Zum Beispiel fügt die folgende Zeile das Zeitguthaben des Benutzers ein:

```
Session wird in <pbelem sesstimeout> Sekunden beendet.
```

› `<pbcond **identifier(s)**>**code**</pbcond>`

Fügt nur dann **code** in die Seite ein, wenn alle Bezeichner TRUE sind, dass heisst numerische Werte sind nicht Null und Zeichenfolgen sind nicht leer. Bitte beachten Sie, dass sich diese Abhängigkeiten nicht ineinander verschachteln lassen. Vom vorherigen Beispiel ausgehend, zeigt die folgende Zeile nur dann an, wieviel Zeit einem Benutzer noch bleibt, wenn dieser ein Limit hat:

```
<pbcond sesstimeout>Session wird in <pbelem sesstimeout> Sekunden beendet.</pbcond>
```

Ein Satz von Beispiel-Seitenvorlagen ist bei LANCOM Systems verfügbar. Diese Beispiele sollen als reine Illustration und Anregung zum Erstellen eigener Seiten dienen.

15.2.5.11 Seitenvorlagen-Bezeichner

Für die Gestaltung benutzerdefinierter Template-Seiten stehen Ihnen die nachfolgenden Bezeichner zur Verfügung. Das Gerät unterscheidet dabei nicht zwischen Groß- und Kleinschreibung.

Bitte beachten Sie, dass nicht alle Bezeichner für alle Ausdrücke verfügbar sind. Nicht alle Bezeichner stehen auf allen Seiten zur Verfügung.

ACCOUNTEND

Gültig für: `<pbelem>`

Dieser Bezeichner fügt auf einem Voucher Informationen zur Gültigkeit des Vouchers ein, d. h. ab wann und bis wann der erstellte Zugang gültig ist.

APADDR

Gültig für: `<pbelem>`

Dieser Bezeichner beinhaltet die IP-Adresse des Public Spots aus Sicht des Clients. Kann für benutzerdefinierte Anmeldeseiten verwendet werden, wenn das `LOGINFORM`-Element nicht benutzt wird.

AUTOPRINT

Gültig für: `<pbelem>`

Dieser Bezeichner fügt ein Java-Skript in die Seite ein mit der Anweisung, den Druck-Dialog zu öffnen, um die angezeigte Seite auszudrucken. Beachten Sie, dass Sie den `pbelem`-Tag in diesem Fall mit einem separaten `script` abschließen **müssen**, also `<pbelem autoprint></script>`.

BANDWIDTHPROFNAME

Gültig für: `<pbelem>`

Dieser Bezeichner beinhaltet das Bandbreiten-Profil, mit dem der Benutzer verknüpft ist.

Dieser Bezeichner ist ab LCOS-Version 9.18 RU1 verfügbar. Templates mit diesem Bezeichner sind für LCOS-Versionen vor 9.18 RU1 nicht geeignet.

COMMENT

Gültig für: `<pbelem>`

Dieser Bezeichner beinhaltet auf einem Voucher den optionalen Kommentar, sofern Sie im Setup-Wizard dafür einen entsprechenden Text eingetragen haben.

HELPLINK

Gültig für: `<pblink>`

Dieser Bezeichner beinhaltet die URL der Hilfeseite.

LOGINEMAILFORM

Gültig für: `<pbelem>`

Dieser Bezeichner beinhaltet für die Anmeldung über Smart-Ticket das HTML-Formular zur Authentisierung am Public Spot mit den via E-Mail erhaltenenen Zugangsdaten.

LOGINERRORMSG

Gültig für: `<pbelem>`

Dieser Bezeichner liefert die Fehlermeldung des LCOS im Falle einer gescheiterten Anmeldung sowie bei Wegfall der WAN-Verbindung. Dieser Bezeichner steht nur auf der allgemeinen Fehlerseite und der Rückfall-Fehlerseite zur Verfügung.

Um die Fehlermeldung des RADIUS-Servers im Falle einer gescheiterten Anmeldung abzurufen, verwenden Sie den Bezeichner **SERVERMSG**.

LOGINFORM

Gültig für: `<pbelem>`

Dieser Bezeichner beinhaltet für die Anmeldung über Benutzername und Passwort (und ggf. MAC-Adresse) das HTML-Formular zur Authentisierung am Public Spot.

LOGINLINK

Gültig für: `<pblink>`

Dieser Bezeichner beinhaltet die URL der Anmeldungsseite.

LOGINSMSFORM

Gültig für: `<pbelem>`

Dieser Bezeichner beinhaltet für die Anmeldung über Smart-Ticket das HTML-Formular zur Authentisierung am Public Spot mit den via SMS erhaltenenen Zugangsdaten.

LOGOFFLINK

Gültig für: `<pblink>`

Dieser Bezeichner beinhaltet die URL der Abmeldungsseite.

ORIGLINK

Gültig für: `<pbelem>` `<pblink>` `<pbcond>`

Dieser Bezeichner beinhaltet die URL, die vom Benutzer angefordert wurde, bevor der Authentifizierungsprozess begonnen wurde. Ist diese Adresse nicht bekannt, ist der Bezeichner leer.

PASSWORD

Gültig für: `<pbelem>`

Dieser Bezeichner beinhaltet auf einem Voucher das Password für den Public Spot-Zugang.

REDIRURL

Gültig für: `<pbelem>` `<pblink>` `<pbcond>`

Dieser Bezeichner hält eine mögliche Umleitungs-URL aus der Authentifizierungsantwort des RADIUS-Servers bereit (sofern es diese gab). Lässt sich nur auf Fehler- und Startseite verwenden.

REGEMAILFORM

Gültig für: `<pbelem>`

Dieser Bezeichner beinhaltet für die Anmeldung über Smart-Ticket das HTML-Formular zum Anfordern der Zugangsdaten via E-Mail (Registrierung).

REGSMSFORM

Gültig für: `<pbelem>`

Dieser Bezeichner beinhaltet für die Anmeldung über Smart-Ticket das HTML-Formular zum Anfordern der Zugangsdaten via SMS (Registrierung).

RXBANDWIDTH

Gültig für: `<pbelem>`

Dieser Bezeichner beinhaltet die maximale Empfangsbandbreite des Bandbreitenprofils.

Dieser Bezeichner ist ab LCOS-Version 9.18 RU1 verfügbar. Templates mit diesem Bezeichner sind für LCOS-Versionen vor 9.18 RU1 nicht geeignet.

RXBYTES

Gültig für: `<pbelem>`

Dieser Bezeichner gibt an, wieviele Daten in Bytes das Gerät in dieser Session vom Client empfangen hat.

RXTXBYTES

Gültig für: `<pbelem>`

Dieser Bezeichner gibt an, wieviele Daten in Bytes das Gerät in dieser Session vom Client empfangen und wieviele Daten es an den Client gesendet hat. Er gibt somit die Summe aus TXBYTES und RXBYTES aus.

SERVERMSG

Gültig für: `<pbelem>` `<pbcond>`

Dieser Bezeichner hält die Authentifizierungsantwort des RADIUS-Servers bereit (sofern es diese gab). Lässt sich nur auf der Fehler- und der Startseite verwenden. Im Falle einer gescheiterten Anmeldung enthält dieser Bezeichner die Fehlermeldung des RADIUS-Servers.

Um die Fehlermeldung des LCOS-Servers im Falle einer gescheiterten Anmeldung abzurufen, verwenden Sie den Bezeichner **LOGINERRORMSG**.

SESSIONSTATUS

Gültig für: `<pbelem>`

Dieser Bezeicher gibt eine Text-Repräsentation über das aktuelle Verhältnis des Clients zum Gerät aus (ob authentifiziert oder nicht).

SESSIONTIME

Gültig für: `<pbelem>`

Dieser Bezeichner gibt die Zeit in Sekunden an, die seit der Anmeldung am Public Spot verstrichen ist.

SESSTIMEOUT

Gültig für: `<pbelem>` `<pbcond>`

Dieser Bezeichner gibt die noch verbleibende Zeit der aktuellen Sitzung an. Nach Ablauf dieser Zeit beendet das Gerät die aktuelle Sitzung automatisch. Für eine Sitzung ohne Zeitlimit ist dieser Bezeichner gleich Null.

SSID

Gültig für: `<pbelem>` `<pbcond>`

Dieser Bezeichner enthält auf einem Voucher die SSID, für die der Public Spot-Zugang erstellt wurde.

STATUSLINK

Gültig für: `<pbelem>` `<pblink>`

Dieser Bezeichner beinhaltet die URL der Abmeldeseite. Innerhalb des `<pblink>`-Elements wird automatisch eine Referenz generiert, die ein neues Browser-Fenster öffnet.

TXBANDWIDTH

Gültig für: `<pbelem>`

Dieser Bezeichner beinhaltet die maximale Sendebandbreite des Bandbreitenprofils.

Dieser Bezeichner ist ab LCOS-Version 9.18 RU1 verfügbar. Templates mit diesem Bezeichner sind für LCOS-Versionen vor 9.18 RU1 nicht geeignet.

TXBYTES

Gültig für: `<pbelem>`

Dieser Bezeichner gibt an, wieviele Daten in Bytes das Gerät während der aktuellen Sitzung zum Client gesendet hat.

USER NAME

Gültig für: `<pbcond>`

Über diesen Bezeichner haben Sie die Möglichkeit, auf der Voucher-Seite konditionalen HTML-Code einzufügen, den das Gerät nur bei bestimmten Benutzern bzw. Administratoren ausgibt. `USER` gilt dabei als Präfix und **muss** dem Benutzernamen (`NAME`) mit einem Leerzeichen vorangestellt werden. Um also bei Aufruf der Voucher-Seite eine HTML-Ausgabe speziell für den Benutzer 'root' zu erzeugen, verwenden Sie die folgende Syntax:

```
<pbcond USER root>Conditional HTML Code</pbcond>
```

In größeren Public Spot-Szenarien mit zentraler Verwaltung – z. B. auf einem WLAN-Controller – lässt sich diese Abhängigkeit auch zur Standortlokalisierung einsetzen: Dazu erstellen Sie für jeden der betreffenden Access Points einen eigenen Public Spot-Admin und spezifizieren für die einzelnen Administratoren einen konditionalen Voucher-Text.

USERID

Gültig für: `<pbelem>`

Dieser Bezeichner beinhaltet die User-ID (in Form des Benutzernamens), mit der die aktuelle Sitzung gestartet wurde. Der Bezeichner ist undefiniert, wenn der Client (noch) nicht eingeloggt ist.

VOLLIMIT

Gültig für: `<pbelem>` `<pbcond>`

Dieser Bezeichner gibt die verbleibende Datenmenge an, die dem Benutzer noch zur Verfügung steht, bevor das Gerät die aktuelle Sitzung automatisch beendet. Für eine Sitzung ohne Datenlimit ist dieser Bezeichner gleich Null.

VOUCHERIMG

Gültig für: `<pbelem>`

Dieser Bezeichner fügt das Seitenbanner Bild (in Groß) in die Seite ein.

Neue Platzhalter ab LCOS-Version 9.20:

Mit diesen Platzhaltern ist eine detailliertere Anpassung der Seitenvorlagen möglich. Im Unterschied zu den oben genannten Platzhaltern wird bei Nutzung dieser Platzhalter kein zusätzlicher beschreibender Text ausgegeben, sondern nur die reinen Werte.

${SSID}

Gibt den Netzwerknamen / die SSID aus.

${USERID}

Gibt den Benutzernamen aus.

${PASSWORD}

Gibt das Benutzerpasswort aus.

${COMMENT}

Gibt den Kommentar aus.

${BandwidthProfName}

Gibt den Namen des Bandbreitenprofils aus.

${TxBandwidth}

Gibt die vorgegebene Maximalbandbreite (Senderichtung) aus.

${RxBandwidth}

Gibt die vorgegebene Maximalbandbreite (Empfangsrichtung) aus.

${ACCOUNTEND}

Dieser Bezeichner gibt das Ticket-Ende (Datum und Uhrzeit) aus.

Zur Verwendung dieser Platzhalter ist es erforderlich, in der Vorlage die jquery-Bibliothek einzubinden. Dazu fügen Sie in der Vorlage folgendes ein:

```
<script src="/jquery/jquery.js" type="text/javascript"></script>

<script src="/jquery/jquery.tmpl.min.js" type="text/javascript"></script>
```

Verwenden Sie außerdem die neuen Platzhalter innerhalb eines <script>-Blocks:

```
<script id="voucherTemplate" type="text/x-jquery-tmpl">

[... Inhalt ...]

</script>
```

15.2.5.12 Grafiken in benutzererstellten Seiten

Beinahe alle Webseiten beinhalten Bilder, die vom Browser des Clients unabhängig von der eigentlichen HTML-Seite heruntergeladen werden. Bei den vorinstallierten Seiten sind auch die dazugehörigen Grafikdateien im Gerät gespeichert. Das Gerät passt dabei automatisch die notwendigen Rechte an, damit auch nicht-authentifizierte Clients problemlos auf die Bilder zugreifen können. Bei benutzerdefinierten Seiten wird jedoch jeder Zugriff auf die referenzierten (geräteexternen) Bilder wie ein normaler Internetzugriff behandelt, und würde Benutzer daher automatisch wieder auf die Willkommens- oder Startseite führen.

Um dieses Verhalten zu verhindern, sollten Sie darauf achten, dass die Server, die die Grafikdateien bereithalten, zu den **Freien Servern** gehören. Freie Server sind Adressen, deren Zugang nicht beschränkt ist; die also auch von nicht-authentifizierten Clients aufrufbar sind und die von der Accounting-Funktion nicht mit dem übrigen Datenverkehr verrechnet werden.

Das Kapitel *Anmeldungsfreie Netze* auf Seite 1290 erhält weitere Informationen, wie Sie einen freien Server konfigurieren. Bitte beachten Sie, dass, wenn eine benutzererstellte Seite als eine Umleitung definiert ist, das Ziel dieser Umleitung ebenfalls zu den Freien Servern gehören sollte.

15.2.5.13 Template-Vorschau über WEBconfig

Um Änderungen an den Public Spot-Vorlagen verfolgen zu können, wechseln Sie in WEBconfig zur Ansicht **Extras** > **Public-Spot Template-Vorschau**.

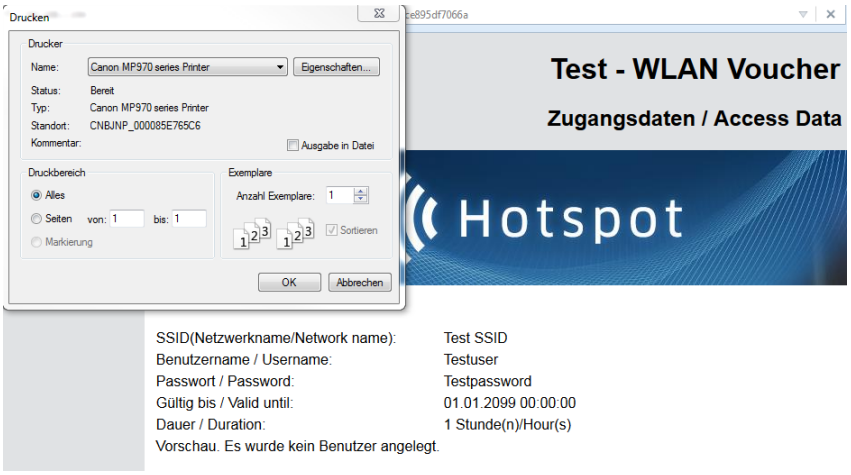


Wählen Sie ein Template zum Anzeigen aus der Liste aus.

Das ausgewählte Template wird im gleichen Browserfenster angezeigt. Über die "Zurück"-Funktion Ihres Browsers gelangen Sie zum WEBconfig zurück.

Einige Templates beinhalten einen Javascript-Code. Dieser Code wird beim Aufrufen des jeweiligen Templates ausgeführt. So enthält das Template "Voucher-Seite" z. B. den Code zum Ausdrucken, sobald die Seite angezeigt wird.

Auf dieser Seite sind Testdaten hinterlegt. Es wird jedoch kein entsprechender Benutzer angelegt. Sie haben also die Möglichkeit, das Template zu testen und auszudrucken.



Sofern kein Template vorliegt oder gefunden werden kann, erscheint eine Fehlermeldung im WEBconfig.

15.2.5.14 Public Spot Captive Portal API

Der Public Spot unterstützt den neuen Standard der Captive Portal API nach *RFC 8908*. Der Standard erlaubt es WLAN-Clients in einem Hotspot ein Captive Portal bzw. eine Login-Seite automatisch zu finden.

Der Client erhält per DHCP die URL der Portal-Seite und kann dann per API-Anfrage an den Hotspot prüfen, ob ein Login erforderlich ist oder der Zugriff für den Client schon erlaubt ist. Das beschleunigt die Benutzererfahrung in einem Hotspot deutlich und stellt durch die Definition eines Standards nun eine bessere Herstellerinteroperabilität zwischen Hotspot und Clients her.

Folgende Schritt sind dazu erforderlich:

1. Die Verwendung von TLS-Zertifikaten im Public Spot ist zwingend erforderlich. Ohne HTTPS-Login stellt der Client an das Portal keine Anfrage.
2. Der DHCP-Server muss die Captive Portal DHCP-Option an den Client ausliefern.

Die Konfiguration finden sie in LANconfig unter **Public-Spot** > **Server** > **Captive Portal API (RFC 8908)**.



Captive Portal API aktiviert

Aktiviert bzw. deaktiviert die Funktion der Captive Portal API im Public Spot.

Benutzerportal-URL

(Optional) Die Captive Portal API unterstützt laut Standard nur die Betriebsart über TLS. Deshalb muss das Gerät über ein vertrauenswürdiges Zertifikat sowie einen DNS-Namen verfügen. Im Default kann der Parameter leer gelassen werden und wird automatisch vom System eingefügt. Dazu muss der Gerätename in den Public Spot Betriebseinstellungen konfiguriert werden und mit dem TLS-Zertifikat übereinstimmen. Wird ein externer Hotspot-Server verwendet, kann auch eine URL des externen Servers eingetragen werden. Als weitere Voraussetzung gilt, dass die Clients im Hotspot das Captive Portal per DHCP-Option finden müssen. Dazu muss die entsprechende DHCP-Option nach *RFC 8910* für das Hotspot-Netzwerk konfiguriert werden.

Venue-URL

(Optional) URL (TLS), über die der Betreiber dem Benutzer zusätzliche Informationen über die Lokation des Hotspots bereitstellen kann, z. B. die Webseite des Hotels des Hotspots.

DHCPv4-Option konfigurieren(laut RFC 8910)

Legen Sie in LANconfig einen neuen Tabelleneintrag unter **IPv4** > **DHCPv4** > **DHCP-Optionen** an.

Options-Nummer

Nummer der Option, die an die DHCP-Clients übermittelt werden soll. Hier 114.

Netzwerkname

Name des Public Spot-Netzwerks (siehe IPv4-Netzwerke)

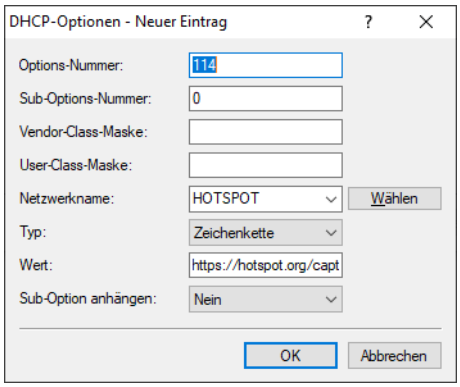
Typ

Typ des Eintrags. Hier Zeichenkette.

Wert

HTTPS-URL des LANCOM Routers im Hotspot, z. B. „https://hotspot.org/captive-portal-api“. Der DNS-Name, z. B. „hotspot.org“, ist der Gerätename des Routers im TLS-Zertifikat ergänzt um den internen Pfad der Public Spot Login-Seite „captive-portal-api“. Der DNS-Name muss durch den Hotspot-Clients auflösbar sein. Ebenso

muss der Gerätename in den Public Spot-Betriebseinstellungen konfiguriert werden und mit dem TLS-Zertifikat übereinstimmen.



DHCPv6-Option konfigurieren (laut RFC8910)

Legen Sie in LANconfig einen neuen Tabelleneintrag unter **IPv6** > **DHCPv6** > **DHCPv6-Server** > **Weitere Optionen** an.

Interface-Name / Relay-IP

Name des Public Spot Netzwerks (siehe IPv6-Netzwerke)

Optionscode

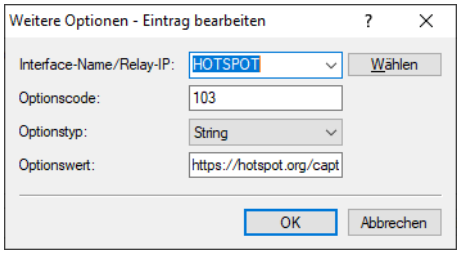
103

Optionstyp

String

Optionswert

HTTPS-URL des LANCOM Routers im Hotspot, z. B. „https://hotspot.org/captive-portal-api". Der DNS-Name, z. B. „hotspot.org", ist der Gerätename des Routers im TLS-Zertifikat ergänzt um den internen Pfad der Public Spot Login-Seite „captive-portal-api". Der DNS-Name muss durch den Hotspot-Clients auflösbar sein. Ebenso muss der Gerätename in den Public Spot-Betriebseinstellungen konfiguriert werden und mit dem TLS-Zertifikat übereinstimmen.

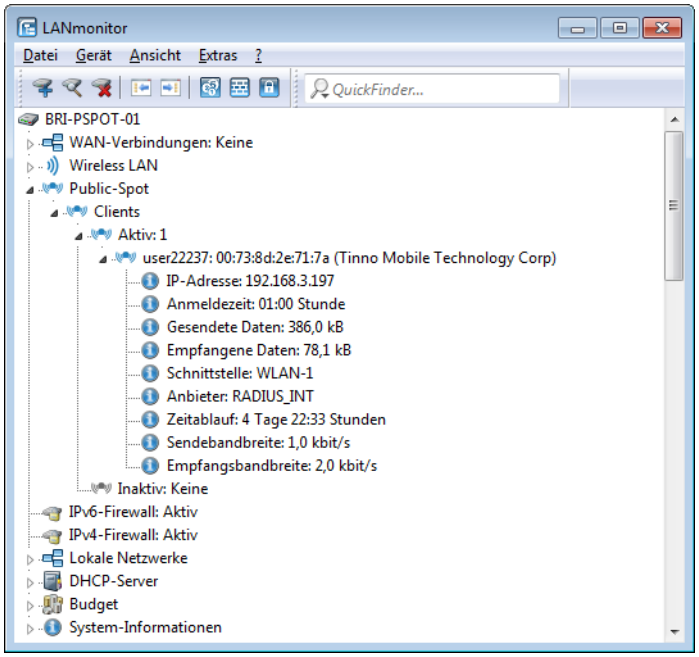


15.2.6 Public Spot-Clients anzeigen

Sie haben die Möglichkeit, sich im LANmonitor detaillierte Informationen zu Public Spot-Clients anzeigen zu lassen.

1. Öffnen Sie den Menüzweig **Public-Spot** > **Clients**.
2. Doppelklicken Sie auf **Aktiv**, um aktive Clients anzuzeigen, oder auf **Inaktiv**, um inaktive Clients anzuzeigen.

3. Doppelklicken Sie auf einen Client, um detaillierte Informationen zu diesem abzurufen.



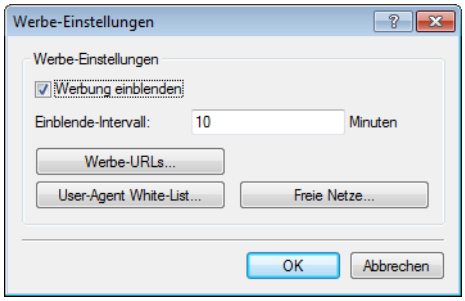
15.2.7 Public Spot-Benutzern Werbung einblenden

Sie haben die Möglichkeit, Public Spot-Benutzern in konfigurierbaren Zeitabständen Werbung einzublenden. Der Public Spot zeigt die Werbung im normalen Browser-Fenster des Benutzers an und nicht über Pop-ups, da alle modernen Browser Pop-ups in der Regel blocken. In der Public Spot-Stationstabelle gibt es somit drei Zustände für einen Client:

- Authentifiziert: Der Client ist angemeldet und darf surfen.
- Unauthentifiziert: Der Client ist nicht angemeldet und darf nicht surfen.
- Werbung: Der Client wird beim nächsten Aufruf einer URL auf eine Werbeseite umgeleitet.

Dabei haben Sie die Möglichkeit, über eine Whitelist bestimmte Netze und User-Agents von den Werbe-Einblendungen auszunehmen.

1. Wählen Sie in der Geräte-Konfiguration den Menüzweig **Public-Spot** > **Server** aus und klicken Sie dort auf **Werbe-Einstellungen**.
2. Aktivieren Sie das Kontrollkästchen **Werbung einblenden**.



Sie haben jetzt die Möglichkeit, den Einblende-Intervall zu verändern und weitere Einstellungen vorzunehmen.

3. Geben Sie unter **Einblende-Intervall** ein Intervall in Minuten, nach dem der Public Spot einen Benutzer auf eine Werbe-URL umleitet. Bei einem Intervall von 0 erfolgt die Umleitung direkt nach der Anmeldung.
4. Klicken Sie auf **Werbe-URLs**, um eine Werbe-URL hinzuzufügen. Wenn Sie mehrere Werbe-URLs hinzufügen, blendet der Public Spot diese im festgelegten Intervall nacheinander ein.

5. Optional: Klicken Sie auf **User-Agent White-List**, um User-Agents hinzuzufügen, die der Public Spot von Werbe-Einblendungen ausnimmt.
6. Optional: Klicken Sie auf **Freie Netze**, um Netze hinzuzufügen, die der Public Spot von Werbe-Einblendungen ausnimmt. Hier besteht beispielsweise die Möglichkeit, die automatischen Such-URLs der Browser eingeben, z. B. `*.google.com`. Normalerweise sendet ein Browser jede Tastatureingabe in der Adressleiste an eine Suchmaschine; durch das Setzen der Ausnahme reagiert die Werbeseite aber nicht auf diesen Zugriff.

   Anmeldungsfreie Netze sind generell werbefrei. Eine explizite Aufnahme derartiger Netze in die Whitelist ist somit nicht erforderlich.
7. Schließen Sie alle Dialoge durch einen Klick auf **OK**.

Public Spot-Benutzer werden nach Ablauf des Einblende-Intervalls auf eine Werbe-URL umgeleitet, sofern ihr User-Agent nicht auf der White-List steht oder sie sich innerhalb eines Freien Netzes bewegen.

Der Zeitpunkt der Werbe-Einblendungen bezieht sich auf die Session-Zeit eines aktiven Public Spot-Clients. Sendet ein Client eine bestimmte Zeit keine Daten, so verschiebt sich auch der Zeitpunkt, zu dem der Public Spot das nächste Mal Werbung einblendet.

15.3 Zugriff auf den Public Spot

15.3.1 Voraussetzungen für die Anmeldung

- Gerät mit Netzwerkadapter
- Betriebssystem mit TCP/IP-Protokoll (automatischer Bezug der IP-Adresse per DHCP ist eingeschaltet)
- Web-Browser (Unterstützung von JavaScript und Frames)
- Direkter Internetzugriff (Proxy-Verwendung ausgeschaltet)
- Notwendige Informationen zum Zugriff auf das WLAN (Netzwerkname, Verschlüsselungs-Informationen)
- Gültige Benutzerdaten (Kennung und Passwort)

Informationen für den WLAN-Zugang

Für den Zugang zum WLAN sind maximal zwei Angaben erforderlich:

- **Netzwerkname des WLAN (SSID)**

  Wenn die Basis-Stationen des Public-Spots für den Betrieb als Closed-Network konfiguriert sind, muss ein Benutzer den exakten Netzwerknamen des WLANs (die SSID) kennen.
- **WLAN-Verschlüsselung**

  Obwohl Gastzugänge auch mit aktivierter WLAN-Verschlüsselung wie z. B. WPA denkbar sind, werden Public-Spots in der Regel ohne WLAN-Verschlüsselung betrieben. Für den Zugriffsschutz sorgt dabei die Benutzeranmeldung mit Username und Passwort. Die Datensicherheit bei der Übertragung über den Public Spot muss vom Endanwender selbst bereitgestellt werden (z. B. über einen VPN-Client).

Informationen für den LAN-Zugang

Sofern Sie die IP-Adressen in Ihrem Netzwerk automatisch (z. B. via DHCP) vergeben, benötigen Benutzer lediglich:

- eine Anschlussdose, auf welcher der Public Spot aufgelegt ist.
- ein LAN-Kabel, um Ihren LAN-Adapter mit der Anschlussdose zu verbinden.

Informationen für die Authentifizierung

Folgende Daten müssen dem Benutzer für die Anmeldung vorliegen:

- Benutzerkennung
- Passwort
- MAC-Adresse

Wenn Sie an den Basis-Stationen des Public-Spots den Authentifizierungs-Modus "MAC+Benutzer+Passwort" gewählt haben, müssen Sie als Betreiber zusätzlich die MAC-Adressen der Endgeräte Ihrer Benutzer kennen. Ein Endgerät übermittelt seine eigene MAC-Adresse automatisch während der gesamten Kommunikation mit dem Public Spot. Der Benutzer muss sie daher nicht bei jeder Anmeldung manuell eingeben, sondern dem Betreiber nur einmal vor der Benutzung mitteilen.

15.3.2 Anmelden am Public Spot

1. Wählen Sie sich in das WLAN des Public-Spots ein (für WLAN-Verbindungen) oder verbinden Sie sich über das Ethernet-Kabel mit dem Netzwerk (für LAN-Verbindungen).
   Die notwendigen Einstellungen für diese Einwahl erfolgen je nach Mobilgerät bzw. WLAN-Adapter auf mehr oder weniger komfortable Art und Weise. Bei vielen Geräten wird der Netzwerkname (SSID) des gewünschten WLANs in einem Konfigurationsprogramm des WLAN-Adapters angegeben. Bei einigen Produkten ist auch die Ansicht aller Access Points in Funkreichweite möglich, aus denen Sie einfach die gewünschte auswählen können.

   Die notwendigen Einstellungen für die Verbindung über einen LAN-Adapter erhält ein Nutzer – je nach Konfiguration – automatisch durch das Netzwerk bzw. einen angeschlossenen DHCP-Server oder vom Netzwerk-Administrator.

2. Starten Sie Ihren Web-Browser.

   Sobald der Web-Browser auf eine beliebige Internet-Seite zugreift, schaltet sich automatisch der Public Spot dazwischen und präsentiert seine Anmeldeseite. Je nachdem, welche Firmware-Version Sie verwenden und welchen Anmeldemodus Sie gewählt haben, besitzt die Anmeldeseite bzw. das darin angezeigte Anmeldeformular ein unterschiedliches Erscheinungsbild. Im Nachfolgenden wird die Anmeldung über einen Vouchers (bzw. mittels Benutzername und Passwort) angenommen.

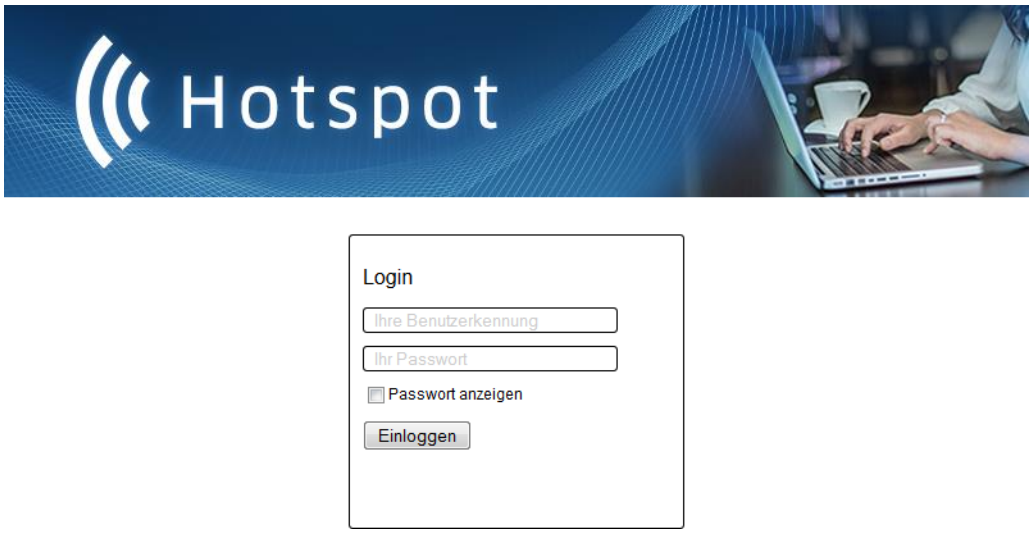


Abbildung 32: Anmeldeseite für breite Bildschirme

3. Geben Sie die vollständige **Benutzerkennung** und das **Passwort** in die entsprechenden Felder ein und bestätigen Sie Ihre Eingabe mit **Einloggen**.

   Für die Anmeldung sollten Sie einen Web-Browser mit aktivierter JavaScript-Unterstützung verwenden, damit das Popup-Fenster mit den Statusmeldungen über die Sitzung geöffnet werden kann.

   Bei erfolgreicher Anmeldung am Public Spot öffnet sich ein zusätzliches Fenster, das die wichtigsten Informationen der aktuellen Sitzung anzeigt. Auch die Abmeldung erfolgt über dieses Fenster. Daher sollte es während der gesamten Sitzung nach Möglichkeit geöffnet bleiben (z. B. in minimierter Darstellung).

Schlägt die Anmeldung fehl, öffnet sich eine Fehlerseite mit der Aufforderung, zur Anmeldeseite zurückzukehren und die Authentisierung zu wiederholen. Das Eingabeformular übernimmt dabei einen Teil der zuvor eingegebenen Daten, um dem Benutzer z. B. im Falle von Tippfehlern die Eingabe zu erleichtern.

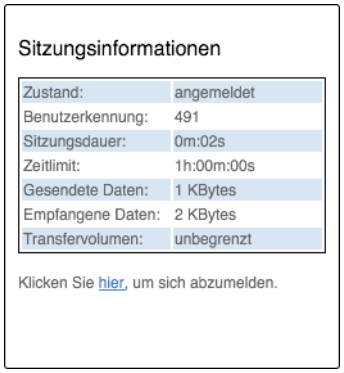
15.3.3 Informationen zur Sitzung

Das Fenster mit den Sitzungsinformationen aktualisiert sich automatisch regelmäßig. Neben Zustand und verwendeter Benutzerkennung sind vor allem die angebotenen Informationen über Verbindungszeit und übertragenes Datenvolumen von Interesse.

Falls das Sitzungsinformations-Fenster nicht geöffnet ist, können Sie es durch Eingabe folgender Adresszeile im Web-Browser öffnen:

```
http://<IP-Adresse des Public Spots>/authen/status
```

Alternativ können Sie auch über die Kurz-URL `http://logout` die Sitzungsseite öffnen.



15.3.4 Abmelden vom Public Spot

Im Sitzungsinformations-Fenster können Sie sich vom Public Spot abmelden. Klicken Sie dazu auf **hier** in der unteren Textzeile des Fensters.

Falls das Sitzungsinformations-Fenster nicht geöffnet ist, können Sie sich auch durch Eingabe folgender Adresszeile im Web-Browser abmelden:

```
http://<IP-Adresse des Public Spots>/authen/logout
```

Alternativ können Sie auch über die Kurz-URL `http://logout` die Sitzungsseite öffnen und sich darüber vom Public Spot abmelden.

Der Betreiber kann seinen Public Spot so einstellen, dass dieser einen Benutzer nach 60 Sekunden Unerreichbarkeit automatisch abmeldet. Fragen Sie im Zweifel beim Betreiber des Public-Spots nach, ob er die automatische Abmeldung (*Stationsüberwachung*) aktiviert hat.

15.3.5 Rat und Hilfe

Im folgenden Abschnitt finden Sie Lösungen für die häufigsten Probleme, die bei der Benutzung eines Public Spots auftreten können.

15.3.5.1 Die Anmeldeseite des Public Spots erscheint nicht

› Der Internet-Zugang muss so eingestellt sein, dass er direkt über den Netzwerkadapter und nicht über eine DFÜ-Einwahlverbindung erfolgt. Prüfen Sie daher die Verbindungseinstellungen in Ihrem Web-Browser. Wenn Sie den Microsoft Internet Explorer verwenden, so müssen unter **Extras** > **Internetoptionen** > **Verbindungen** die eingetragenen DFÜ-Konfigurationen deaktiviert sein.

- Der Internet-Zugang muss direkt erfolgen, also ohne Umweg über einen Proxy-Server. Beim Microsoft Internet Explorer schalten Sie dazu die Verwendung des Proxy-Servers im Menü **Extras** > **Internetoptionen** > **Verbindungen** > **LAN-Einstellungen…** aus.
- Sofern Sie die Verbindung über einen WLAN-Adapter herstellen: Prüfen Sie, ob Ihr Netzwerkadapter den Public Spot überhaupt finden kann. Für die Suche nach einem Access Point bietet Ihr WLAN-Adapter geeignete Hilfsmittel an.
- Sofern Sie die Verbindung über einen WLAN-Adapter herstellen: Prüfen Sie, ob Sie Ihren Netzwerkadapter ausreichend für den Zugang zum Public Spot-Netz konfiguriert haben.
  - Vermutlich müssen Sie den Netzwerknamen des WLAN angeben.
  - Bei Einsatz eines verschlüsselten Public Spots ist zusätzlich auch die Eingabe des passenden WPA- oder WEP-Schlüssels erforderlich.
- Prüfen Sie, ob Ihr Netzwerkadapter auf den automatischen Bezug einer IP-Adresse (DHCP) eingeschaltet ist. Ihm darf keine feste IP-Adresse zugewiesen sein.



Wenn Ihr Netzwerkadapter auf eine feste IP-Adresse konfiguriert ist, dann kann durch die Umstellung auf den automatischen Adressbezug per DHCP der Verlust wichtiger Konfigurationswerte ausgelöst werden. Notieren Sie sich vor der Umstellung alle Werte, die in den Netzwerkeinstellungen aufgeführt sind (IP-Adresse, Standard-Gateway, DNS-Server usw.).

15.3.5.2 Die Anmeldung funktioniert nicht

- Achten Sie auf die vollständige und richtige Eingabe der Benutzerdaten. Bei allen Eingaben ist auf korrekte Groß- und Kleinschreibung zu achten.
- Ist die Feststelltaste (CAPS-LOCK) an Ihrem Gerät aktiviert? Dadurch wird die Groß- und Kleinschreibung vertauscht. Deaktivieren Sie die Feststelltaste und wiederholen Sie die Eingabe Ihrer Anmeldedaten.
- Möglicherweise überprüft der Betreiber des Public Spots nicht nur Benutzername und Kennung, sondern auch die sogenannte MAC-Adresse (physikalische Adresse) Ihres Netzwerkadapters. Vergewissern Sie sich in diesem Fall beim Public Spot-Betreiber, dass er Ihre korrekte MAC-Adresse kennt.

15.3.5.3 Es sind keine weiteren Anmeldeversuche mehr möglich

Wenn der Public Spot nach einer Reihe von erfolglosen Anmeldeversuchen die Kommunikation mit Ihnen abbricht, so deaktivieren Sie für mindestens 60 Sekunden den WLAN-Adapter (oder Ihr komplettes Gerät) bzw. trennen den LAN-Adapter vom Netz, und versuchen Sie es danach erneut.

15.3.5.4 Das Sitzungsinformations-Fenster wird nicht angezeigt

Zur Anzeige des Sitzungsinformations-Fensters geben Sie in der Adresszeile Ihres Web-Browsers folgende Zeile ein:

```
http://<IP-Adresse des Public Spots>/authen/status
```

Der Public Spot-Betreiber gibt Ihnen die `<IP-Adresse des Public Spots>` auf Nachfrage an.

15.3.5.5 Der Public Spot fordert ohne Grund die Neuanmeldung (WLAN)

Beim Wechsel in den Funkbereich eines anderen Access Points (Roaming) wird die erneute Anmeldung erforderlich. Wenn Sie sich im Überschneidungsbereich zweier Access Points befinden, kann es sogar zu einem regelmäßigen Verbindungswechsel zwischen beiden Access Points kommen. Die Angabe des Roaming Secret ermöglicht die Übergabe einer Public Spot-Sitzung an anderen Access Point ohne Neuanmeldung.

- LANconfig: **Public-Spot** > **Benutzer** > **Roaming Secret**

15.4 Tutorials zur Einrichtung und Verwendung des Public Spots

Die folgenden Tutorials beschreiben beispielhaft, wie Sie das Public Spot-Modul sinnvoll einsetzen können.

15.4.1 Virtualisierung und Gastzugang über WLAN Controller mit VLAN

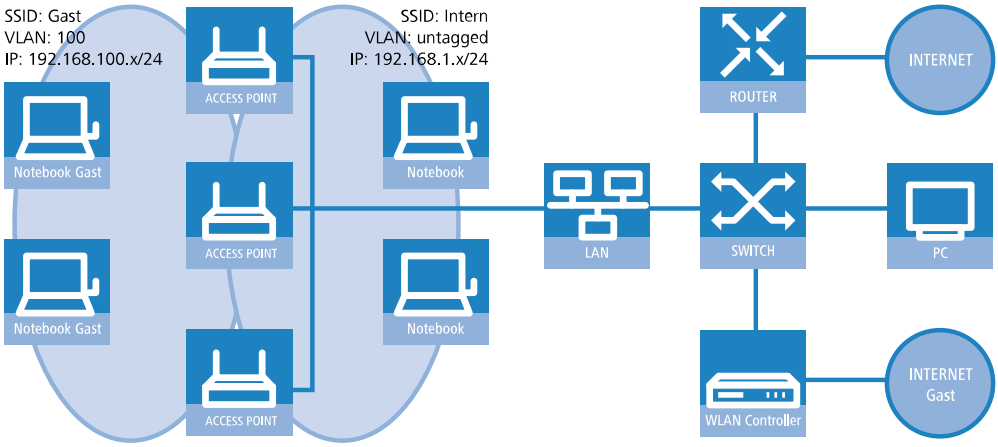
In vielen Unternehmen ist es erwünscht, den Besuchern für die mitgebrachten Notebooks o. ä. einen Internetzugang über WLAN anzubieten. In einem größeren Netzwerk mit mehreren Access Points kann die Konfiguration der nötigen Einstellungen zentral im WLAN Controller erfolgen.

15.4.1.1 Ziele

- Nutzung der WLAN-Infrastruktur für interne Mitarbeiter und Gäste
- Nutzung der gleichen physikalischen Komponenten (Kabel, Switche, Access Points)
- Trennung der Netzwerke über VLAN und ARF
- Auskopplung der Datenströme zu bestimmten Zielnetzwerken:
  - Gäste: nur Internet
  - Interne Mitarbeiter: Internet sowie alle lokalen Geräte und Dienste
- Gäste melden sich über ein Webformular am WLAN an.
- Interne Mitarbeiter nutzen die WLAN-Verschlüsselung zur Authentifizierung.

15.4.1.2 Aufbau

- Die Verwaltung der Access Points erfolgt zentral über den WLC.
- Der WLC dient als DHCP-Server für die WLAN-Clients des Gastnetzes.
- Für das Gastnetz wird der Internetzugang vom WLC (z. B. separater DSL Zugang oder Internetzugang über Firmen-DMZ) bereitgestellt.
- Die kabelgebundene Infrastruktur basiert auf gemanagten VLAN-fähigen Switches:
  - Das VLAN-Management der Access Points erfolgt über den WLC.
  - Das VLAN-Management der Switches erfolgt separat über die Switch-Konfiguration.
- Die Access Points werden innerhalb des internen VLANs betrieben.

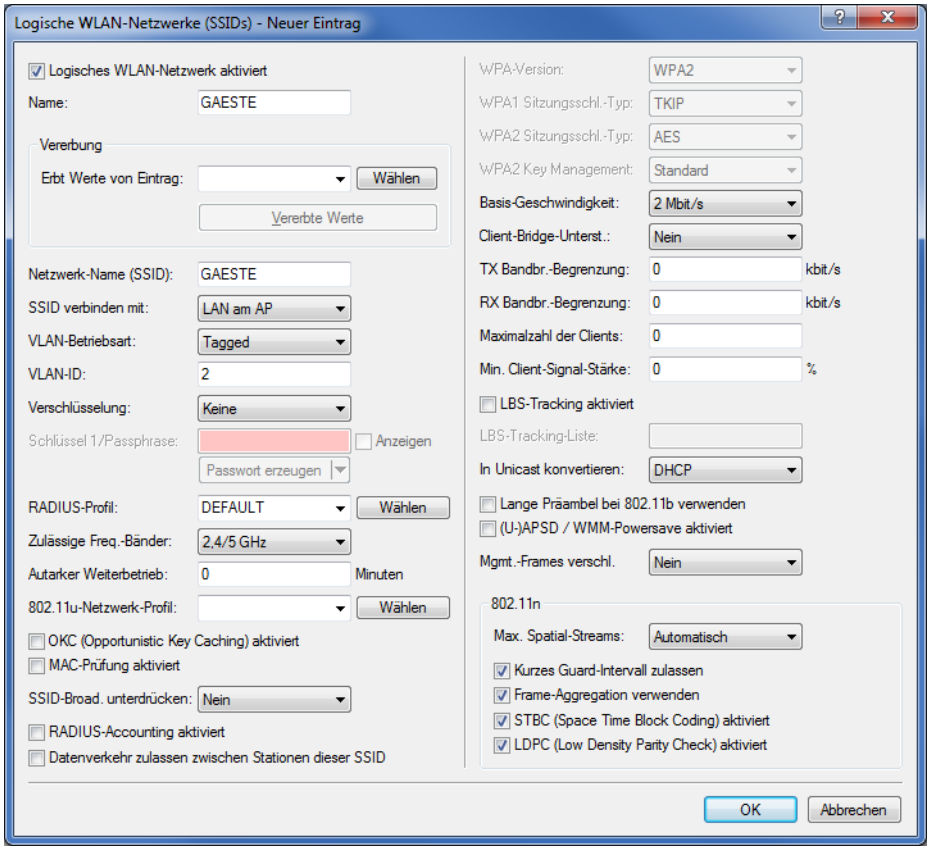


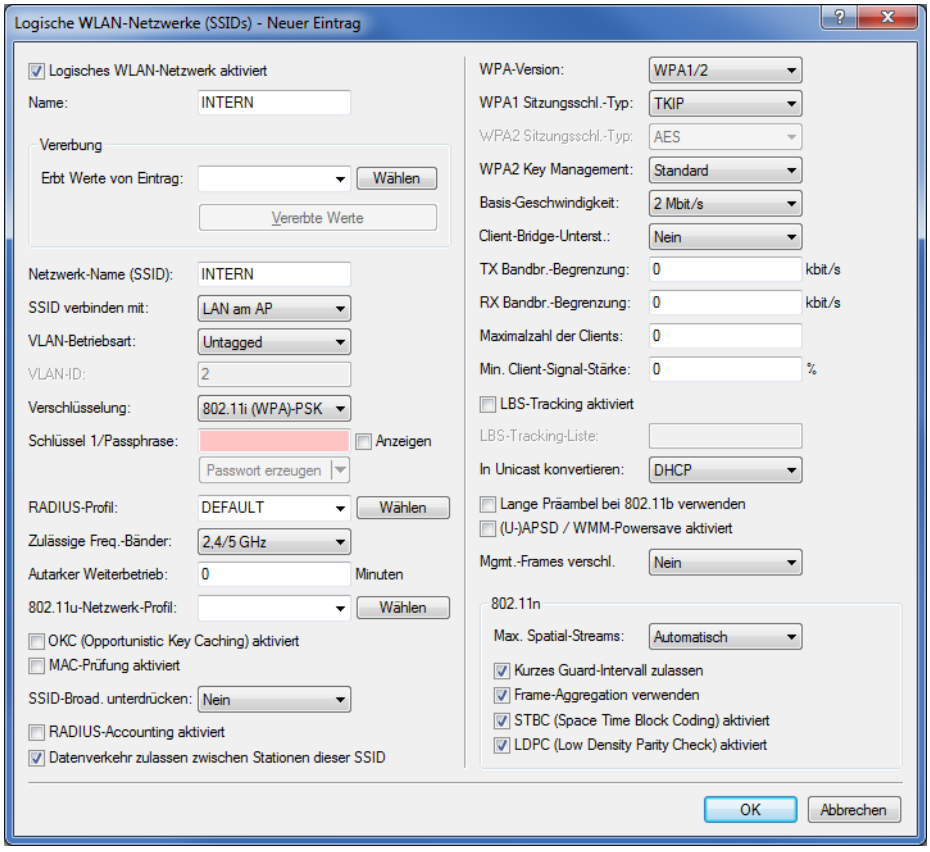
15.4.1.3 WLAN-Konfiguration des WLAN Controllers

Bei der WLAN-Konfiguration definieren Sie die benötigten WLAN-Netzwerke und weisen sie zusammen mit den physikalischen WLAN-Einstellungen den vom Controller verwalteten Access Points zu.

1. Erstellen Sie ein logisches WLAN für die Gäste und eines für die internen Mitarbeiter.
   - Das WLAN mit der SSID `GAESTE` erhält die VLAN-ID `100` (VLAN-Betriebsart **Tagged**) und verwendet **Keine** Verschlüsselung.
   - Das WLAN mit der SSID `INTERN` erhält keine VLAN-ID (VLAN-Betriebsart **Untagged**, d. h. Datenpakete werden ohne VLAN-Tag in das Ethernet übertragen) und verwendet eine Verschlüsselung nach WPA, z. B. **802.11i (WPA)-PSK**.

› LANconfig: **WLAN-Controller** > **Profile** > **Logische WLAN-Netzwerke (SSIDs)**

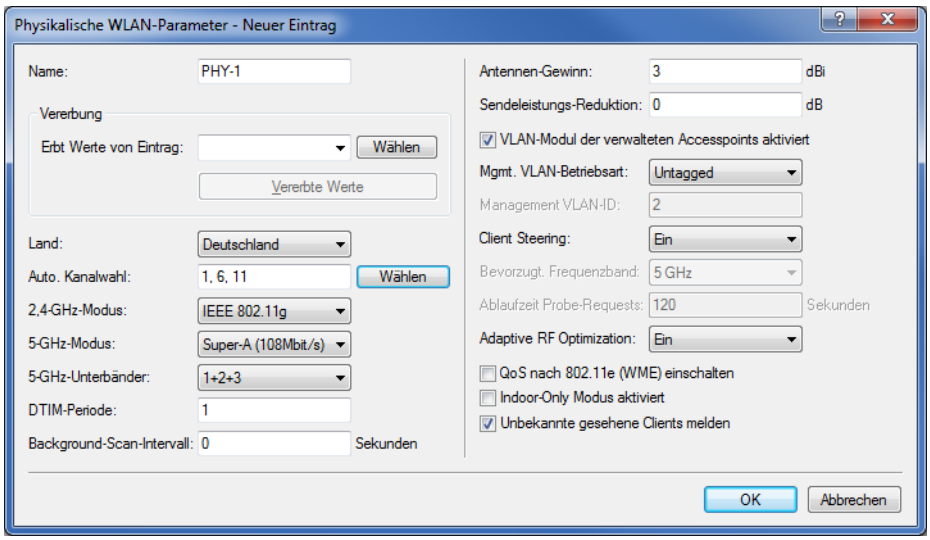




Wenn Sie die **VLAN-Betriebsart** auf **Untagged** stellen, graut LANconfig das Eingabefeld **VLAN-ID** im oben gezeigten Hinzufügen-/Bearbeiten-Dialog aus. Die dazugehörige Tabelle **Logische WLAN-Netzwerke (SSIDs)** zeigt als zugewiesene VLAN aber trotzdem den im ausgegrauten Feld ausgewiesenen Wert an. Dieser Eintrag ist lediglich programmintern, da der zulässige Wertebereich zwischen 2 und 4094 liegt. Letztlich entscheidend ist die VLAN-Betriebsart: Wenn diese auf **Untagged** steht, wird in keinem Fall eine VLAN-ID übertragen.

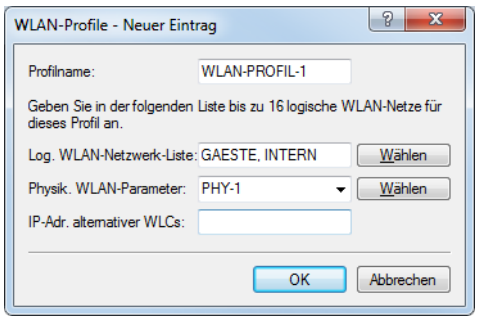
2. Erstellen Sie einen Satz von physikalischen Parametern für die verwendeten Access Points.
Dabei wird die Management-VLAN-ID auf `1` gesetzt, um die VLAN-Nutzung generell zu aktivieren (jedoch ohne separates Management-VLAN für das Gerät; der Management-Datenverkehr wird ungetagged übertragen).

   › LANconfig: **WLAN-Controller** > **Profile** > **Physikalische WLAN-Parameter**



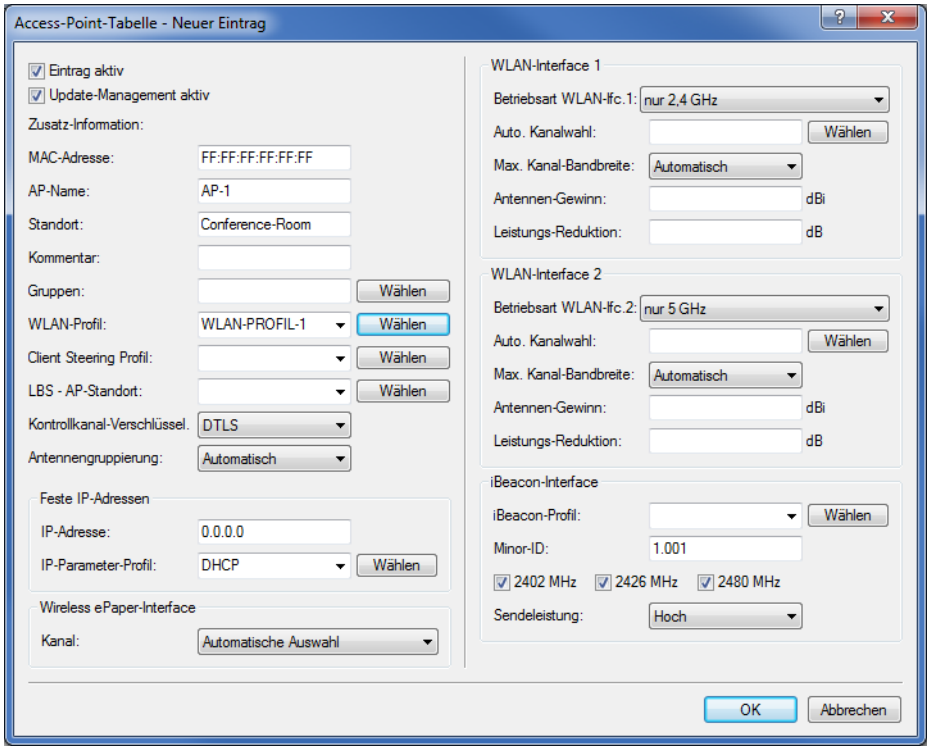
3. Erstellen Sie ein WLAN-Profil, welches Sie den Access Points zuweisen.
   Unter diesem WLAN-Profil vereinen Sie die beiden zuvor erstellten logischen WLAN-Netzwerke und den zuvor erstellten Satz von physikalischen Parametern.

   › LANconfig: **WLAN-Controller** > **Profile** > **WLAN-Profile**



4. Ordnen Sie das WLAN-Profil den vom Controller verwalteten Access Points zu.
   Tragen Sie dazu die einzelnen Access Points mit der MAC-Adresse in die Access-Point-Tabelle ein. Alternativ können Sie über die Schaltfläche **Default** auch ein Standardprofil anlegen, das für alle Access Points gilt.

   › LANconfig: **WLAN-Controller** > **AP-Konfig.** > **Access-Point-Tabelle**



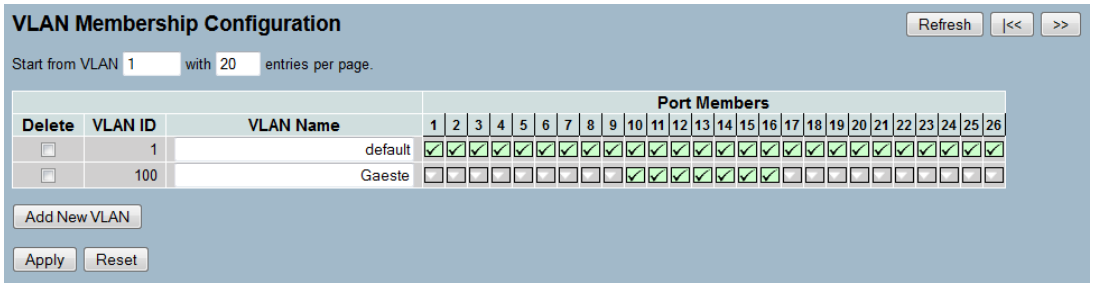
15.4.1.4 Konfiguration des Switches (LANCOM GS-2326P)

In diesem Kapitel beschreiben die Konfiguration des Switches am Beispiel eines LANCOM GS-2326P.

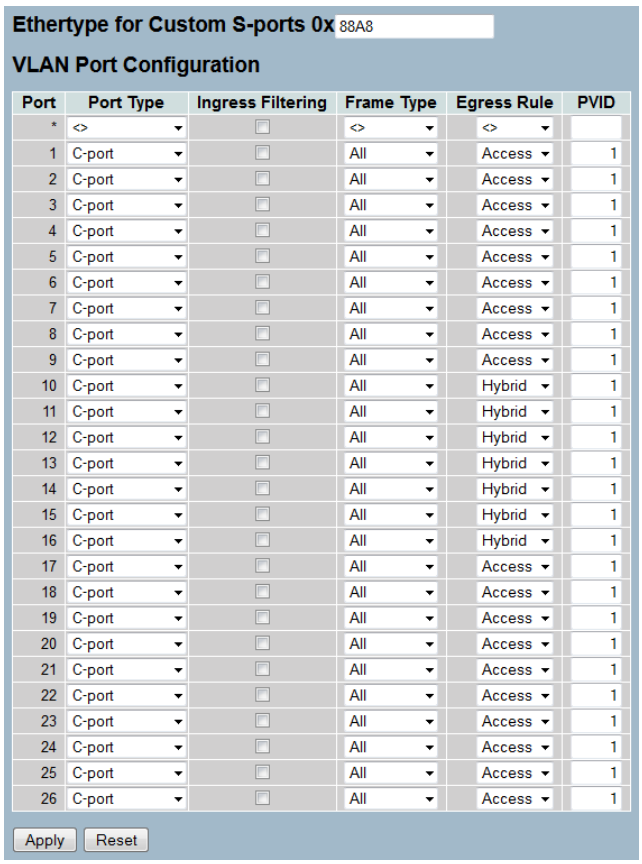
1. Legen Sie unter **Configuration** > **VLAN** > **VLAN-Membership** für das eingerichtete Gäste-Netz eine weitere VLAN-Gruppe an.

   Zur Unterscheidung der VLANs im Switch werden zwei Gruppen verwendet. Das interne Netz für die Mitarbeiter wird in der Gruppe `default` abgebildet, das der Gäste in der Gruppe `Gaeste`.

- Die VLAN-Gruppe für die internen Mitarbeiter verwendet die Default-VLAN-ID `1`. Diese zur internen Verwaltung eingesetzte VLAN-ID gilt auf allen Ports und wird ungetagged betrieben; d. h. alle ungetaggt eingehenden Datenpakete erhalten für das interne Routing die VLAN-ID 1, welche bei ausgehenden Datenpaketen wieder entfernt wird (siehe auch "PVID" im nächsten Schritt).
- Die VLAN-Gruppe für die Gäste verwendet die VLAN-ID `100`, die Sie bereits bei der Konfiguration der WLANs im Controller eingetragen haben. Sie gilt nur auf den Ports, an denen der WLAN-Controller und die Access Points angeschlossen sind (in diesem Beispiel: Port 10 bis 16, grüner Haken unter **Port Members**). Bei ausgehenden Datenpaketen entfernt der Switch die Tags nicht; d. h. alle getaggt eingehenden Datenpakete mit der VLAN-ID 100 behalten diesen Tag und werden nur an die Ports geroutet, die Mitglied der entsprechenden Gruppe sind.



2. Stellen Sie unter **Configuration** > **VLAN** > **Ports** den **Port Type** alle Ports auf **C-port**. Details zu dieser Einstellung finden Sie in der Switch-Dokumentation.
3. Konfigurieren Sie die **Egress Rule** für die einzelnen Ports.
   - Alle Ports außer Port 10 bis 16 erhalten die Regel **Access**. Dadurch leiten diese Ports nur ungetaggte Datenpakete weiter, alle anderen werden verworfen.
   - Die Ports 10 bis 16 erhalten die Regel **Hybrid**. Dadurch leiten diese Ports sowohl ungetaggte als auch getaggte Datenpakete weiter.



Achten Sie darauf, dass die **PVID** (Port-VLAN-ID) für jeden Port den Wert `1` besitzt. Die PVID ist die VLAN-ID, die ein Port eingehenden Datenpaketen ohne VLAN-Tag zuweist; daher entspricht die PVID der VLAN-ID der `default`-Gruppe.

4. OPTIONAL: Sofern Sie den Zugang zum Gäste-Netz auch über Ethernet erlauben möchten, stellen Sie unter **Configuration** > **VLAN** > **Ports** z. B. für die Ports 17 bis 20 die **PVID** auf `100`, und weisen unter **Configuration** > **VLAN** > **VLAN-Membership** diese Ports der Gruppe `Gaeste` zu. Dadurch erhalten alle über diese Ports ungetaggt eingehenden Datenpakete die VLAN-ID 100.

Beachten Sie, dass die betreffenden Datenpakete den Switch dann lediglich über die Ports des Gäste-Netzes wieder verlassen können!

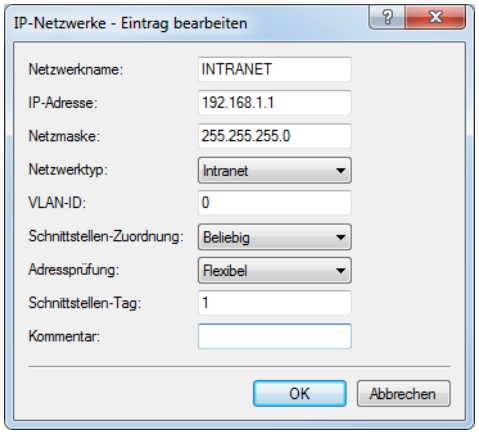
15.4.1.5 Konfiguration der IP-Netzwerke im WLAN Controller

Für die Trennung der Datenströme auf Layer 3 werden zwei verschiedene IP-Netzwerke verwendet (ARF – Advanced Routing and Forwarding).

1. Stellen Sie für das interne Netzwerk das **INTRANET** auf die Adresse `192.168.1.1` ein.

   Dieses IP-Netzwerk verwendet die **VLAN-ID** `0`. Damit werden alle ungetaggten Datenpakete diesem Netzwerk zugeordnet (das VLAN-Modul des Controllers selbst muss dazu deaktiviert sein). Das **Schnittstellen-Tag** `1` wird für die spätere Auskopplung der Daten im virtuellen Router verwendet.

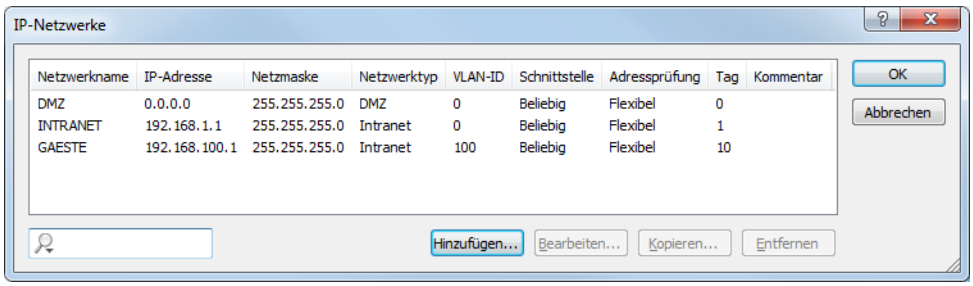
   › LANconfig: **TCP/IP** > **Allgemein** > **IP-Netzwerke**



2. Legen Sie für die Gäste ein neues IP-Netzwerk mit der Adresse `192.168.100.1` an.

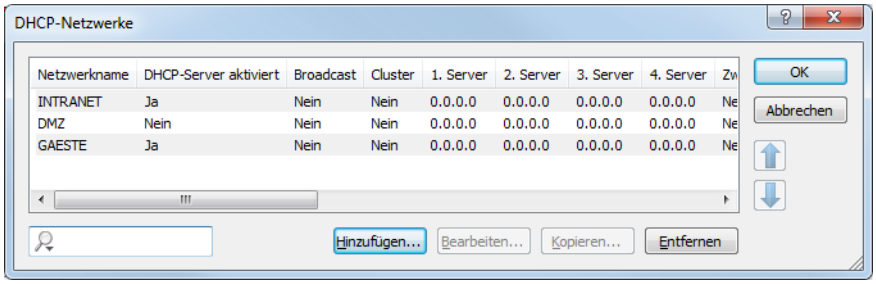
   Dieses Netzwerk verwendet die **VLAN-ID** `100`. Damit werden alle Datenpakete mit dieser ID dem Gäste-Netzwerk zugeordnet. Auch hier dient das **Schnittstellen-Tag** `10` der späteren Verwendung im virtuellen Router.

   › LANconfig: **TCP/IP** > **Allgemein** > **IP-Netzwerke**

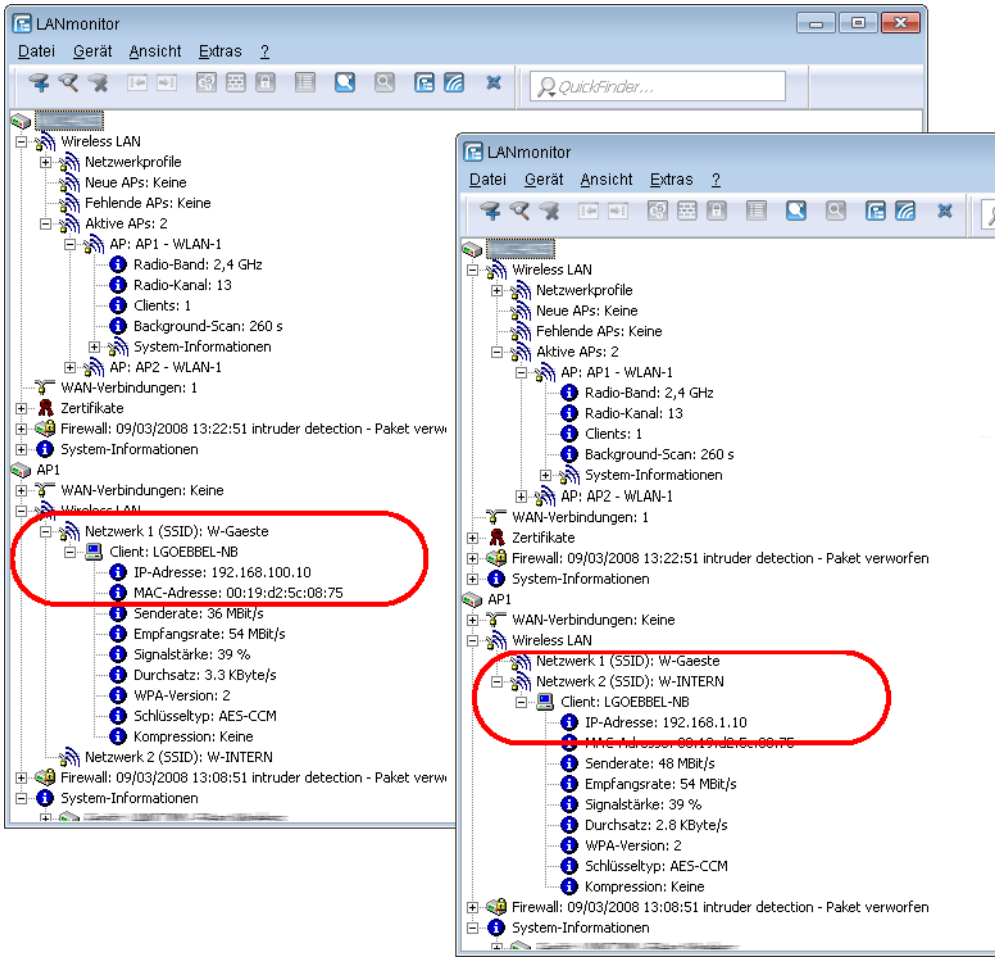


3. Aktivieren Sie für die beiden IP-Netzwerke den DHCP-Server.

› LANconfig: **TCP/IP** > **Allgemein** > **IP-Netzwerke**



Mit diesen Einstellungen können die WLAN-Clients der internen Mitarbeiter und der Gäste gezielt den jeweiligen Netzwerken zugeordnet werden.

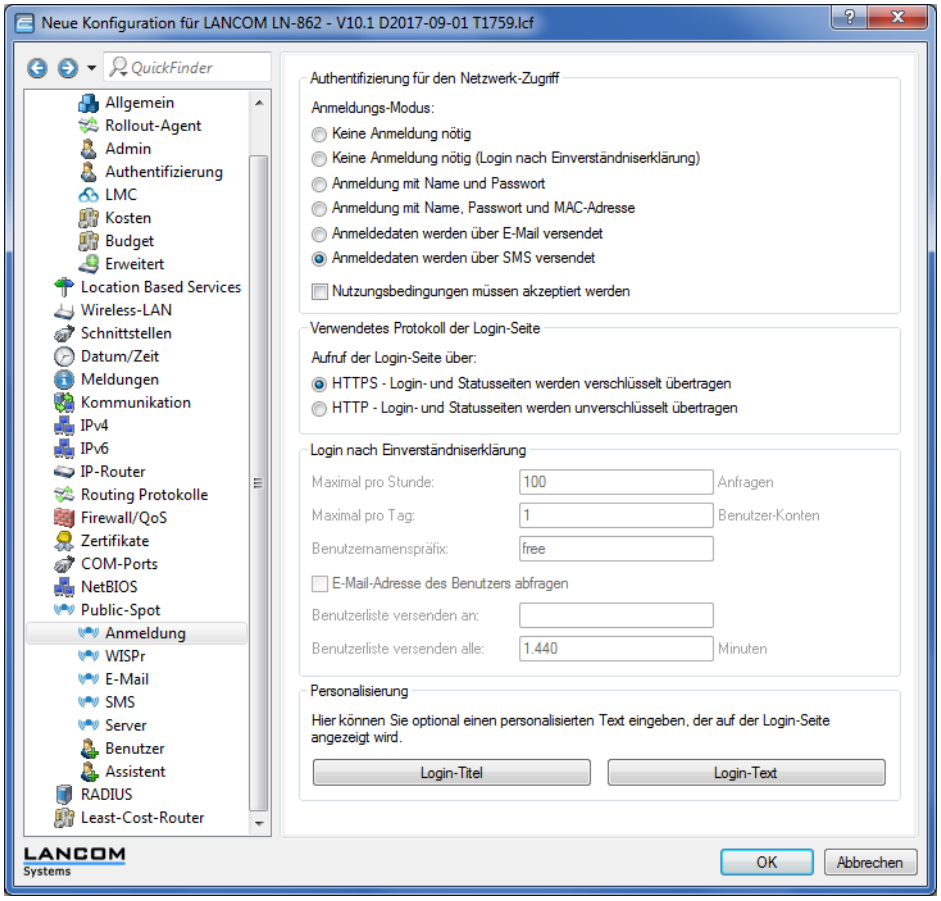


15.4.1.6 Konfiguration der Public Spot-Zugänge

Mit dem Public Spot bieten Sie einen kontrollierten Zugriffspunkt auf Ihr WLAN. Die Authentifizierung erfolgt durch Benutzerabfrage über ein Webinterface. Bei Bedarf können Sie den Zugang zeitlich begrenzen.

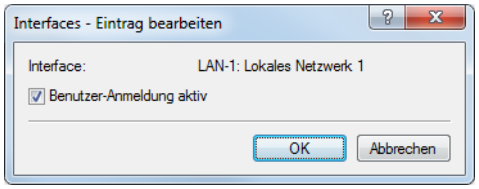
1. Aktivieren Sie die Authentifizierung für den Netzwerk-Zugriff mit Benutzername und Passwort.

› LANconfig: **Public-Spot** > **Anmeldung** > **Authentifizierung für den Netzwerk-Zugriff**



2. Aktivieren Sie die Benutzeranmeldung für das Controller-Interface, über das er mit dem Switch verbunden ist.

   › LANconfig: **Public-Spot** > **Server** > **Betriebseinstellungen** > **Interfaces**

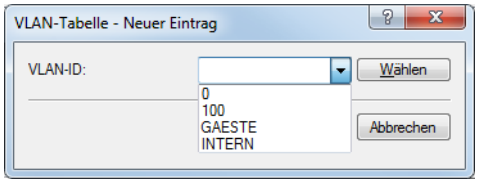


3. Regulieren Sie den Zugang zum Public Spot.

   Mit dem Eintrag der VLAN-ID "100" für das Gäste-Netzwerk in der VLAN-Tabelle beschränken Sie die Public Spot-Verwendung auf Datenpakete aus diesem virtuellen LAN. Alle Datenpakete aus anderen VLANs werden ohne Anmeldung am Public Spot weitergeleitet. Achten Sie dabei auch darauf, dass der WEBconfig-Zugang über das Public Spot-Interface auf die Authentifizierungsseiten beschränkt ist (siehe *Konfigurationszugriff einschränken*).

   Ohne die Einschränkung des Interfaces auf die VLAN-ID ist der Controller auf dem angegebenen physikalischen Ethernet-Port nicht mehr erreichbar!

› LANconfig: **Public-Spot** > **Server** > **VLAN-Tabelle**



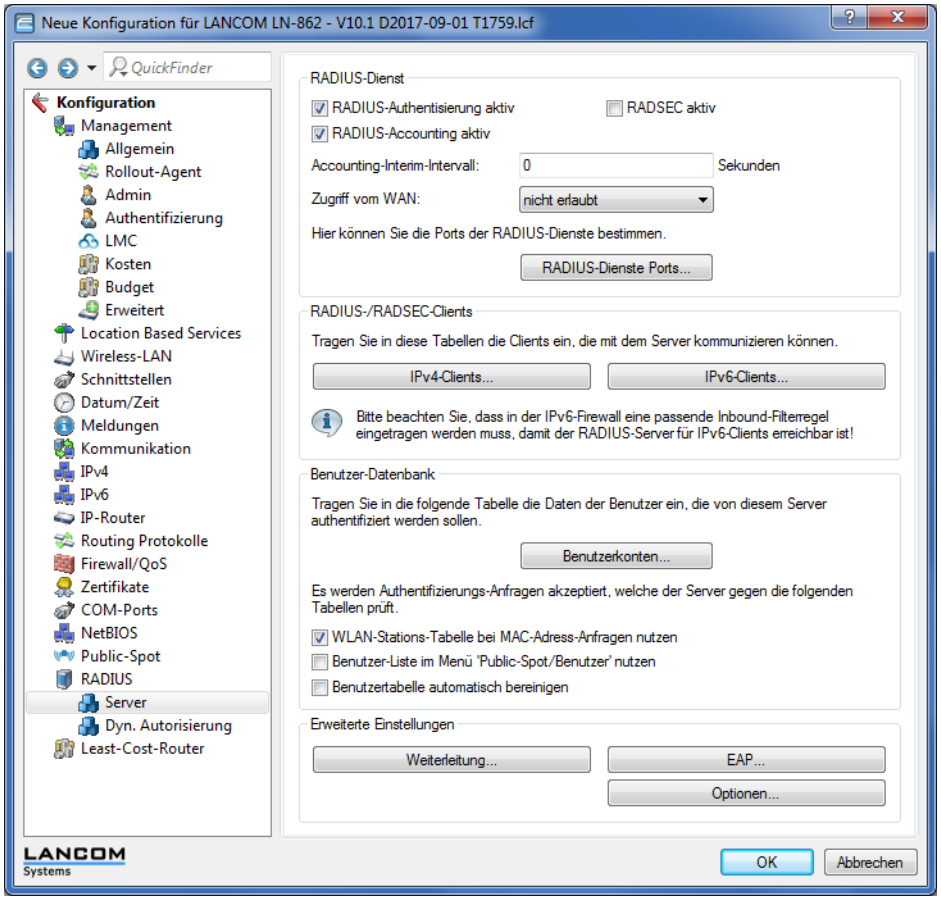
4. Aktivieren Sie die Option zum Bereinigen der Benutzertabelle, damit das Gerät nicht mehr benötigte Einträge automatisch löscht.

   › LANconfig: **RADIUS** > **Server** > **Benutzer-Datenbank** > **Benutzertabelle automatisch bereinigen**

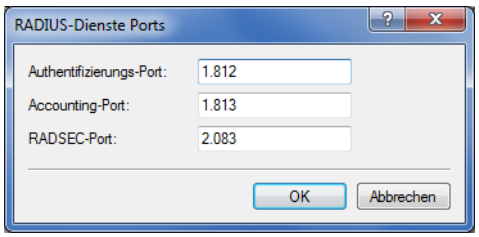
15.4.1.7 Internen RADIUS-Server für Public Spot-Nutzung konfigurieren

Der Assistent speichert die Public Spot-Zugänge in der Benutzerdatenbank des internen RADIUS-Servers. Damit Sie diese Public Spot-Zugänge nutzen können, wurde der interne RADIUS-Server standardmäßig vorkonfiguriert. Dies können Sie in **LANconfig** wie folgt einsehen:

1. Navigieren Sie zu **RADIUS** > **Server** > **RADIUS-Dienst**.
2. Stellen Sie sicher, dass die Häkchen für **RADIUS-Authentisierung aktiv** und **RADIUS-Accounting aktiv** gesetzt sind.



3. Klicken Sie die Schaltfläche **RADIUS-Dienste Ports**.

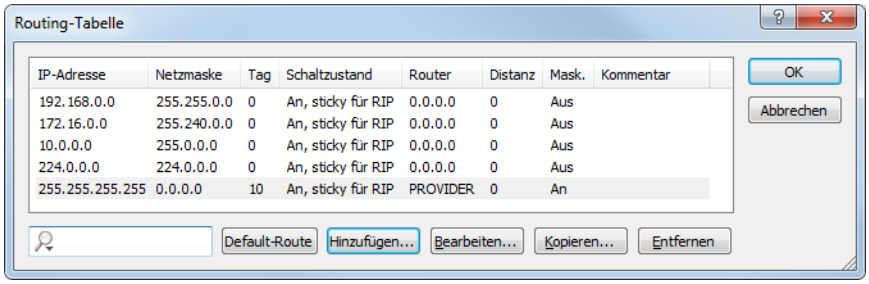


Hier sehen Sie die Default-Einstellungen.

15.4.1.8 Konfiguration des Internetzugangs für das Gästenetzwerk

1. Um den Benutzern des Gast-Netzes einen Internetzugang bereitzustellen, nutzen Sie z. B. den Assistenten für die Einrichtung eines Zugangs zum Providernetz.
2. Beschränken Sie den Zugang zum Providernetz.
   Damit dieser Zugang nur für die Benutzer im Gästenetzwerk zur Verfügung steht, vergeben Sie der entsprechenden Route das Routing-Tag "10". Damit können nur Datenpakete aus dem IP-Netzwerk "GAESTE" mit dem Schnittstellen-Tag "10" in das Netz des Providers übertragen werden. Das Routing zwischen dem Gäste-Netzwerk und dem internen Netzwerk ist aufgrund der unterschiedlichen Routing-Tags ausgeschlossen.

   › LANconfig: **IP-Router** > **Routing** > **Routing-Tabelle**



3. Optional: Laden Sie im LANconfig ggf. über **Gerät** > **Konfigurations-Verwaltung** > **Zertifikat oder Datei hochladen** eine HTML-Vorlage und ein Bild als Vorlage für die Ausgabe der Vouchers in das Gerät.
   Das Bild kann als GIF, JPEG oder PNG vorliegen und darf maximal 64 KB groß sein.

15.4.2 Virtualisierung und Gastzugang über WLAN Controller ohne VLAN

15.4.2.1 "Overlay Netzwerk": Netzwerke für Access Points trennen ohne VLAN

Die Trennung von Netzwerken in einer gemeinsam genutzten physikalischen Infrastruktur basiert in vielen Fällen auf dem Einsatz von VLANs. Dieses Verfahren setzt allerdings voraus, dass die eingesetzten Switches VLAN-fähig sind und dass in allen Switches die entsprechenden VLAN-Konfigurationen durchgeführt werden. Der Administrator rollt die VLAN-Konfiguration in diesem Beispiel also über das gesamte Netzwerk aus.

Mit einem WLC können Sie die Netze auch mit minimalem Einsatz von VLANs trennen. Über einen CAPWAP-Datentunnel leiten die APs die Nutzdaten der angeschlossenen WLAN-Clients direkt zum WLC, der die Daten den entsprechenden VLANs zuordnet. Die VLAN-Konfiguration beschränkt sich dabei auf den WLC und einen einzigen zentralen Switch. Alle anderen Switches arbeiten in diesem Beispiel ohne VLAN-Konfiguration.

Mit dieser Konfiguration reduzieren Sie das VLAN auf den Kern der Netzstruktur (in der Grafik blau hinterlegt dargestellt). Darüber hinaus erfordern lediglich 3 der genutzten Switch-Ports eine VLAN-Konfiguration.

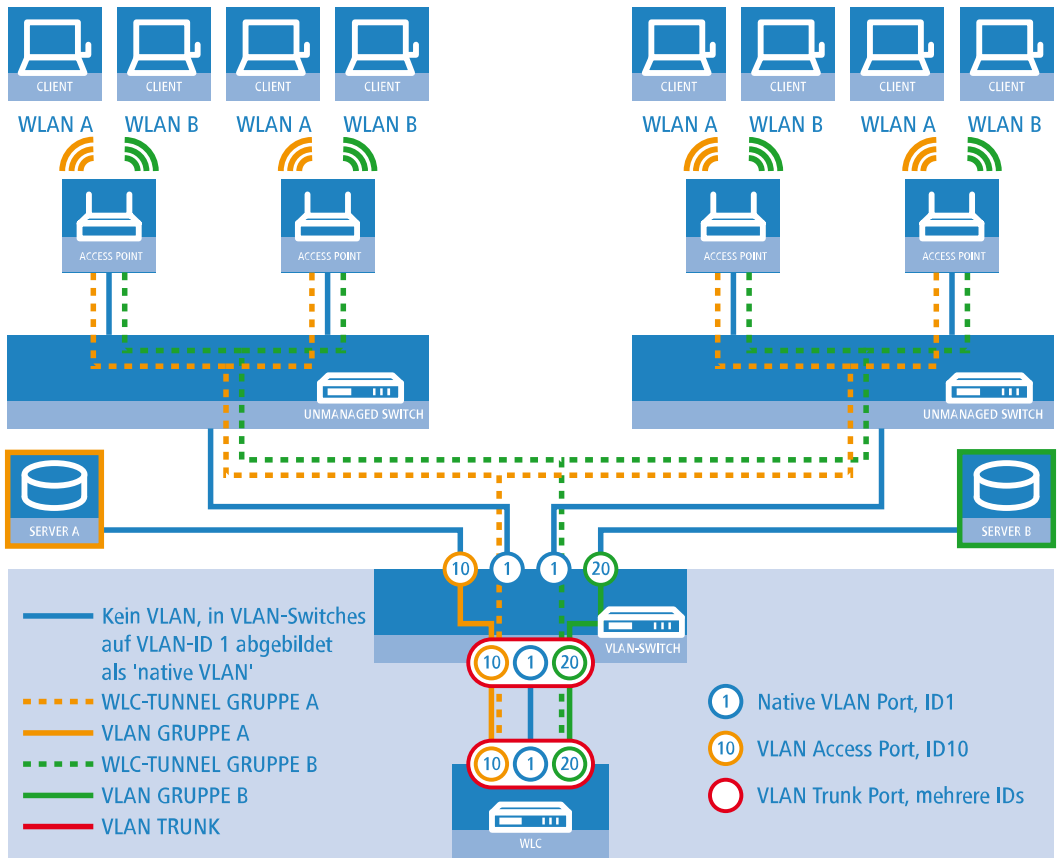


Abbildung 33: Anwendungsbeispiel Overlay-Netz

Die Grafik zeigt ein Anwendungsbeispiel mit den folgenden Komponenten:

- Das Netz besteht aus zwei Segmenten mit jeweils einem eigenen (nicht unbedingt VLAN-fähigen) Switch.
- In jedem Segment stehen mehrere APs, angeschlossen an den jeweiligen Switch.
- Jeder AP bietet zwei SSIDs für die WLAN-Clients aus verschiedenen Benutzergruppen an, in der Grafik dargestellt in Grün und Orange.
- Jede der Benutzergruppen hat Zugang zu einem eigenen Server, der vor dem Zugriff aus anderen Benutzergruppen getrennt ist. Die Server sind nur durch die auf dem Switch konfigurierten Access-Ports über die entsprechenden VLANs erreichbar.
- Ein WLC verwaltet alle APs in Netz.
- Ein zentraler, VLAN-fähiger Switch verbindet die Switches der Segmente, die gruppenbezogenen Server und den WLC.

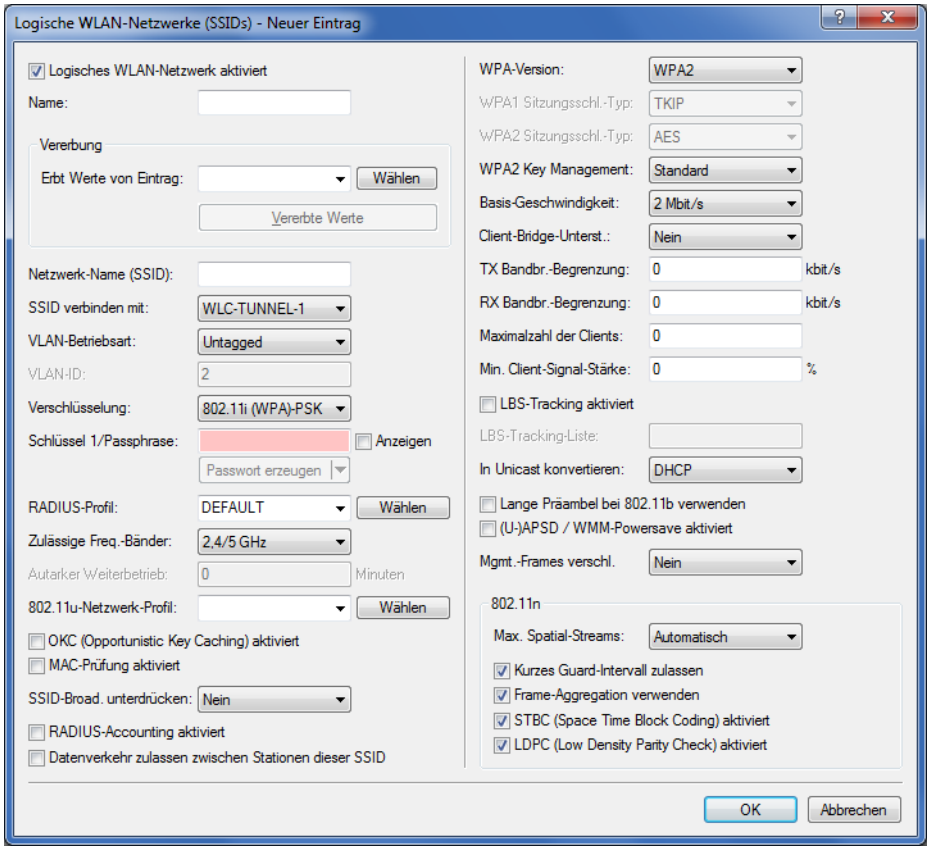
Das Ziel der Konfiguration: Ein WLAN-Client, der sich an einer bestimmten SSID anmeldet, soll Zugang zu "seinem" Server haben – unabhängig vom verwendeten AP und unabhängig vom Segment, in dem er sich gerade befindet.

Die folgende Beschreibung basiert auf einer funktionsfähigen Grundkonfiguration des WLCs. Die Konfiguration des VLAN-Switches ist nicht Bestandteil dieser Beschreibung.

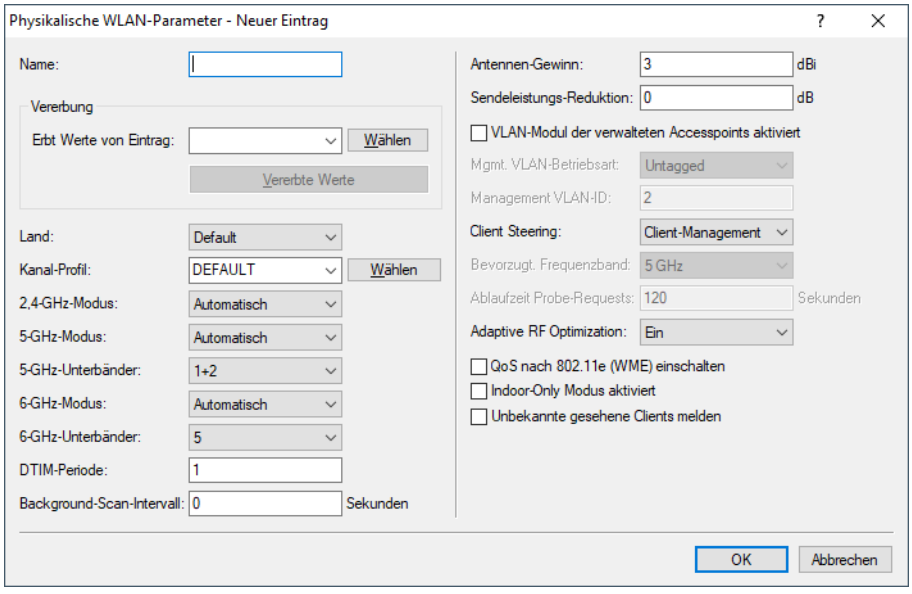
Konfiguration der WLAN-Einstellungen

1. Erstellen Sie für jede SSID einen Eintrag in der Liste der logischen Netzwerke mit einem passenden Namen und der zugehörigen SSID. Verbinden Sie diese SSID mit einem WLC-Tunnel, die erste SSID z. B. mit 'WLC-TUNNEL-1' und die zweite mit 'WLC-TUNNEL-2'. Stellen Sie die VLAN-Betriebsart jeweils auf 'Tagged' mit der VLAN-ID '10' für das

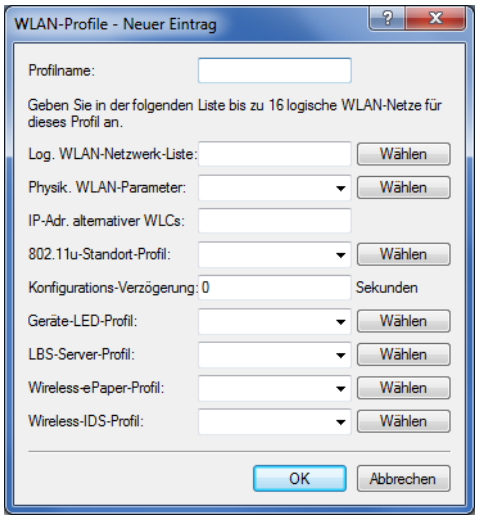
erste logischen Netz und der VLAN-ID '20' für das zweite logischen Netz. In LANconfig finden Sie diese Einstellungen unter **Konfiguration** > **WLAN-Controller** > **Profile** > **Logische WLAN-Netzwerke (SSIDs)**.



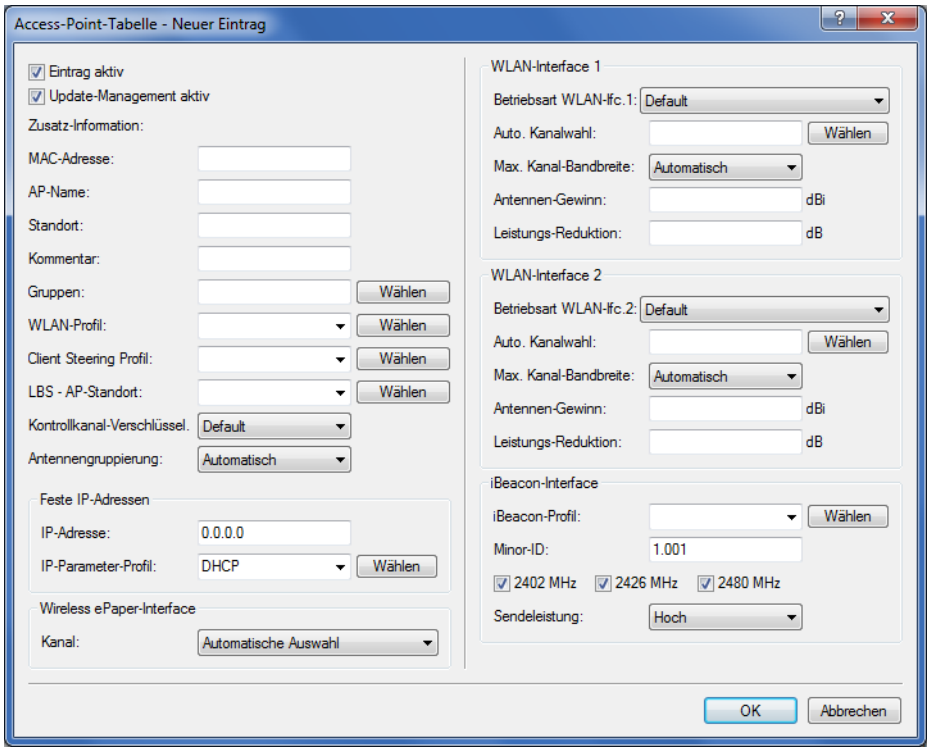
2. Erstellen Sie einen Eintrag in der Liste der physikalischen WLAN-Parameter mit den passenden Einstellungen für Ihre APs, z. B. für das Land 'Europa' mit den Kanälen 1, 6 und 11 im 802.11g/b/n und 802.11a/n gemischten Modus. Aktivieren Sie für dieses Profil der physikalischen WLAN-Parameter die Option, das VLAN-Modul auf den APs einzuschalten. Stellen Sie die Betriebsart für das Management-VLAN in den APs auf 'Ungetagged' ein. In LANconfig finden Sie diese Einstellungen unter **Konfiguration** > **WLAN-Controller** > **Profile** > **Physikalische WLAN-Parameter**.



3. Erstellen Sie ein WLAN-Profil mit einem passenden Namen und ordnen Sie diesem WLAN-Profil die zuvor erstellten logischen WLAN-Netzwerke und die physikalischen WLAN-Parameter zu. In LANconfig finden Sie diese Einstellungen unter **Konfiguration** > **WLAN-Controller** > **Profile** > **WLAN-Profile**.

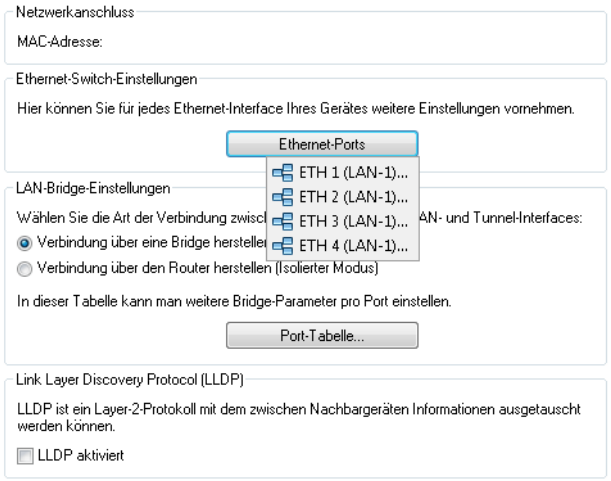


4. Erstellen Sie für jeden verwalteten AP einen Eintrag in der AP-Tabelle mit einem passenden Namen und der zugehörigen MAC-Adresse. Ordnen Sie diesem AP das zuvor erstellte WLAN-Profil zu. In LANconfig finden Sie diese Einstellungen unter **Konfiguration** > **WLAN-Controller** > **AP-Konfig.** > **Access-Point-Tabelle**.

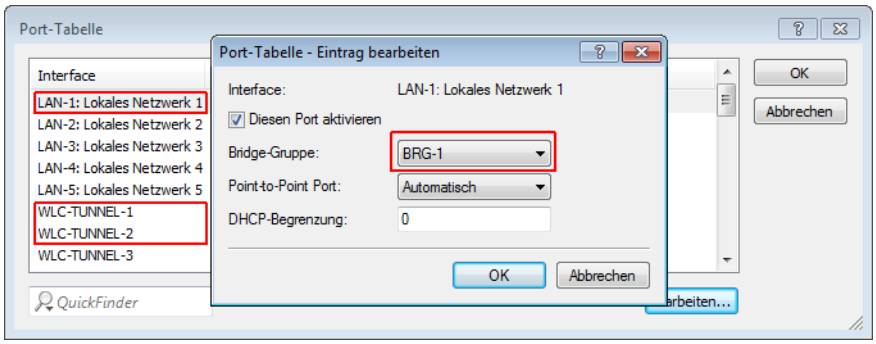


Konfiguration der Schnittstellen am WLC

5. Ordnen Sie jedem physikalischen Ethernet-Port eine separate logische LAN-Schnittstelle zu, z. B. 'LAN-1'. Stellen Sie sicher, dass die anderen Ethernet-Ports nicht der gleichen LAN-Schnittstelle zugeordnet sind. In LANconfig finden Sie diese Einstellungen unter **Konfiguration** > **Schnittstellen** > **LAN** > **Ethernet-Ports**.

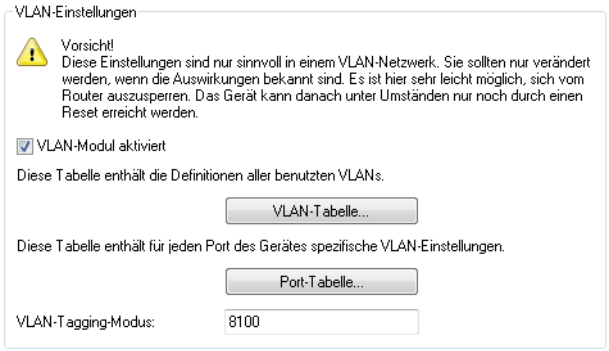


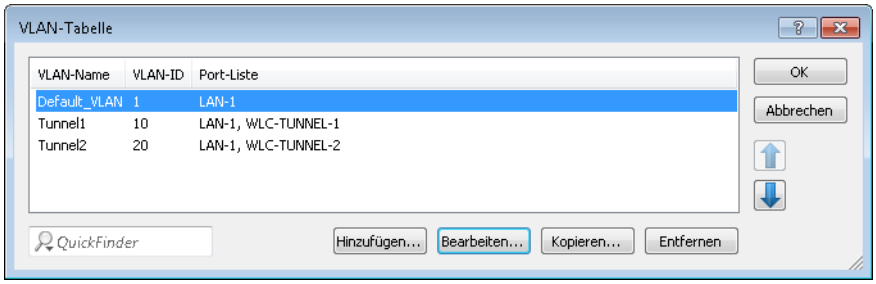
6. Ordnen Sie die logische LAN-Schnittstelle 'LAN-1' und die WLC-Tunnel 'WLC-Tunnel-1' und 'WLC-Tunnel-2' der Bridge-Gruppe 'BRG-1' zu. Stellen Sie sicher, dass die anderen LAN-Schnittstellen nicht der gleichen Bridge-Gruppe zugeordnet sind. In LANconfig finden Sie diese Einstellungen unter **Konfiguration** > **Schnittstellen** > **LAN** > **Port-Tabelle**.



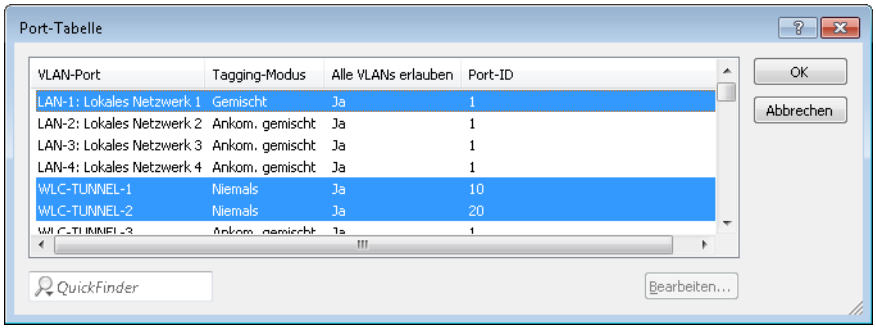
Die LAN-Schnittstellen und WLC-Tunnel gehören standardmäßig keiner Bridge-Gruppe an. Indem Sie die LAN-Schnittstelle 'LAN-1' sowie die beiden WLC-Tunnel 'WLC-Tunnel-1' und 'WLC-Tunnel-2' der Bridge-Gruppe 'BRG-1' zuordnen, leitet das Gerät alle Datenpakete zwischen LAN-1 und den WLC-Tunneln über die Bridge weiter.

7. Aktivieren Sie unter **Schnittstellen** > **VLAN** das VLAN-Modul des WLC und ordnen Sie unter **VLAN-Tabelle** dem gewünschten VLAN den oben gewählten LAN-Port (LAN-1) sowie den passenden WLC-Tunnel zu.





8. Stellen Sie unter **Schnittstellen** > **VLAN** > **Port-Tabelle** den Tagging-Modus der Tunnel-Interfaces sowie des LAN-Interfaces korrekt ein und setzen Sie die passende Port-VLAN-ID.



Je nach Schaltung des Switches konfigurieren Sie den Tagging-Modus des LAN-Interfaces auf 'Gemischt' oder 'Immer'.

Im Normalfall betreibt man die Tunnel-Interfaces im Modus 'Niemals', da Pakete hier (aus dem WLAN) immer ungetaggt ankommen und der WLC sie mit der Port-VLAN-ID versieht.

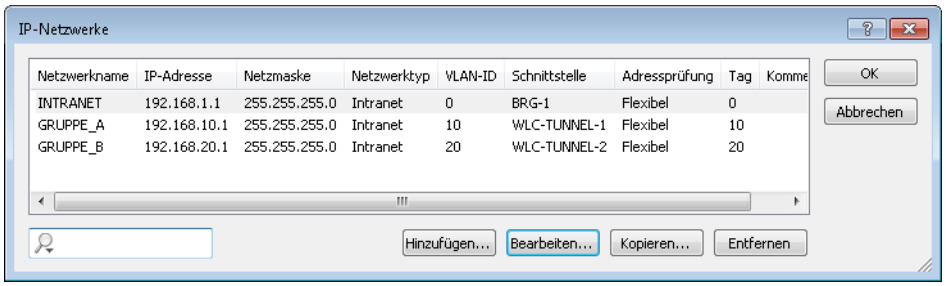
Bitte beachten Sie, dass bei Aktivierung des VLAN-Moduls die auf dem WLC angelegten ARF-Netze eine VLAN-ID erhalten müssen. Soll der WLC das Netz ohne VLAN-Tag erreichen, setzen Sie bei oben stehender VLAN-Konfiguration die '1' als VLAN-ID für das IP-Netz.

Eine ähnliche Konfiguration ist möglich, indem Sie schon am Access Point ein VLAN-Tag für die durch den Tunnel zu leitenden Pakete setzen und das VLAN-Modul des WLC nicht nutzen.

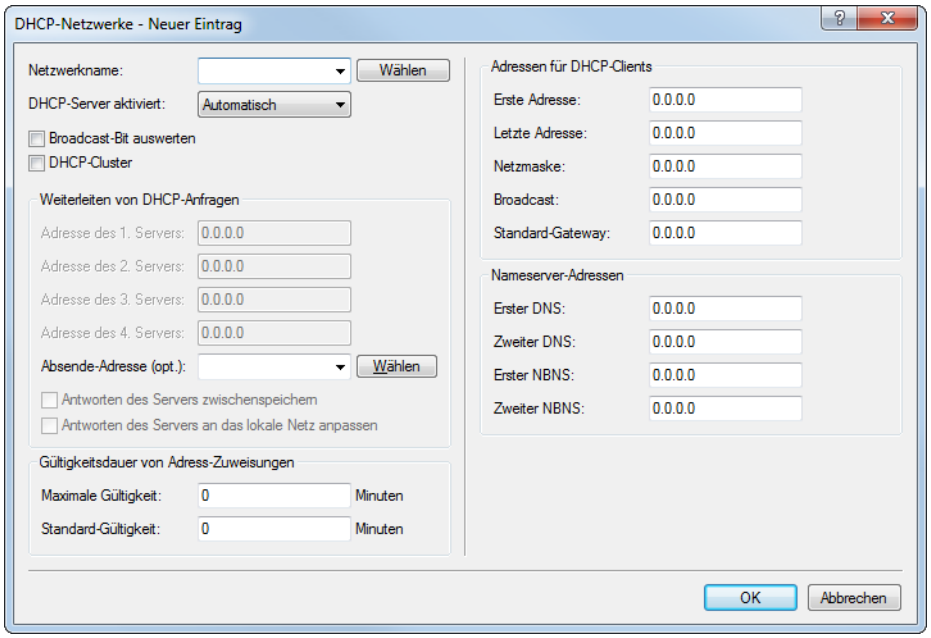
Dabei würde der WLC allerdings durch das Bridgen der verschiedenen WLC-Tunnel untereinander auch Broadcasts in alle Tunnel weiterleiten, was ab einer bestimmten Menge von Tunneln/SSIDs und APs zu Lastproblemen im Netz und auf dem WLC führen kann. Die vorliegende Konfiguration des VLAN-Moduls verhindert das.

9. Ergänzend konfigurieren Sie unter **IPv4** > **Allgemein** > **IP-Netzwerke** für die auf Layer 2 getrennten Netzwerke die IP-Einstellungen.

   Damit das Gerät die Netzwerke nicht wieder auf Layer 3 verbindet, ist auch eine Trennung auf Layer 3 erforderlich, z. B. durch ein Schnittstellen-Tag oder durch die Firewall.



10. Der WLC kann optional als DHCP-Server für die APs fungieren. Aktivieren Sie dazu den DHCP-Server für das 'INTRANET'. In LANconfig finden Sie diese Einstellungen unter **IPv4** > **DHCPv4** > **DHCP-Netzwerke**.



15.4.2.2 WLAN-Controller mit Public Spot

Dieses Szenario basiert auf dem ersten Szenario (Overlay-Netzwerk) und erweitert es um spezifische Einstellungen für eine Benutzer-Authentifizierung.

Die Durchleitung der Nutzdaten aus den WLANs über WLC-Tunnel bis zum WLC ermöglicht eine besonders einfache Konfiguration von Public Spots z. B. für Gäste parallel zu einem intern genutzten WLAN.

In diesem Beispiel haben die Mitarbeiter einer Firma Zugang zu einem eigenen WLAN (SSID), die Gäste erhalten über einen Public Spot ebenfalls Zugang zum Internet. Die APs in allen Bereichen des Gebäudes bieten die beiden SSIDs 'FIRMA' und 'GAESTE' an.

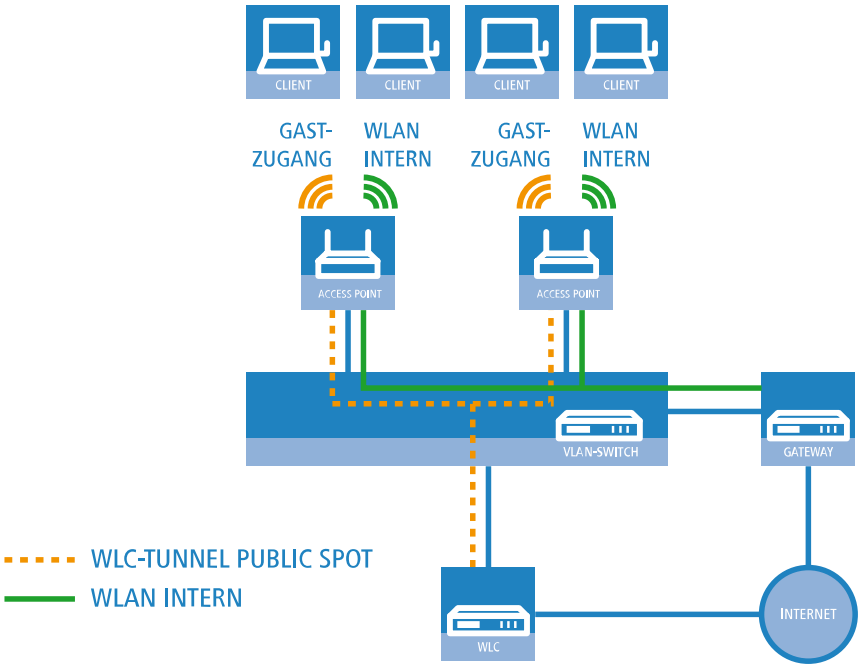
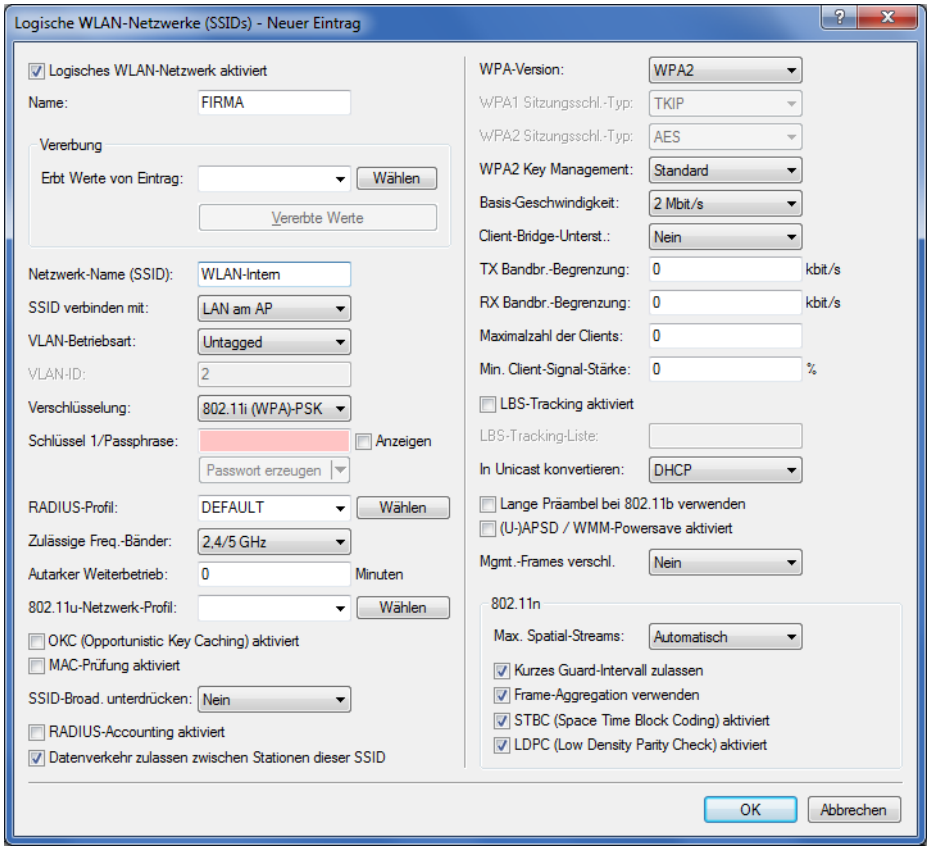


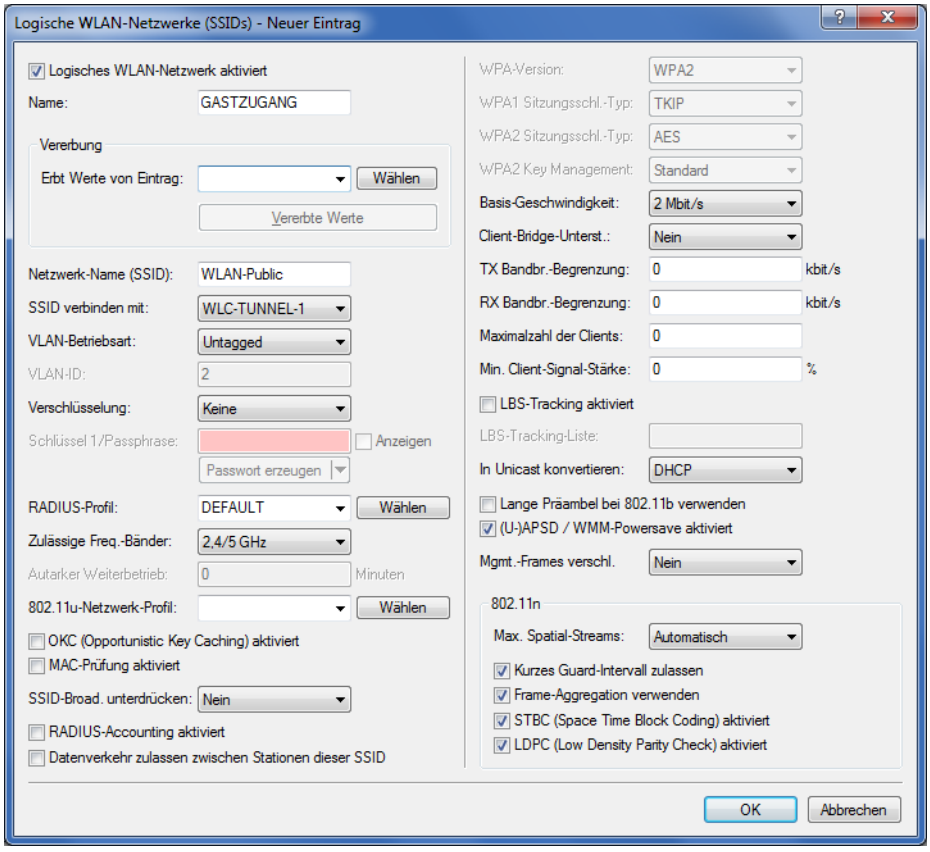
Abbildung 34: Anwendungsbeispiel WLAN-Controller mit Public Spot

Das Ziel der Konfiguration: Ein WLAN-Client, der sich an der internen SSID anmeldet, soll Zugang zu allen internen Ressourcen und zum Internet über das zentrale Gateway erhalten. Die APs koppeln die Nutzdaten der internen Clients lokal aus und leiten sie direkt in das LAN weiter. Die WLAN-Clients der Gäste melden sich am Public Spot an. Die APs leiten die Nutzdaten der Gäste-Clients über einen WLC-Tunnel direkt zum WLC, der über eine separate WAN-Schnittstelle Zugang zum Internet ermöglicht.

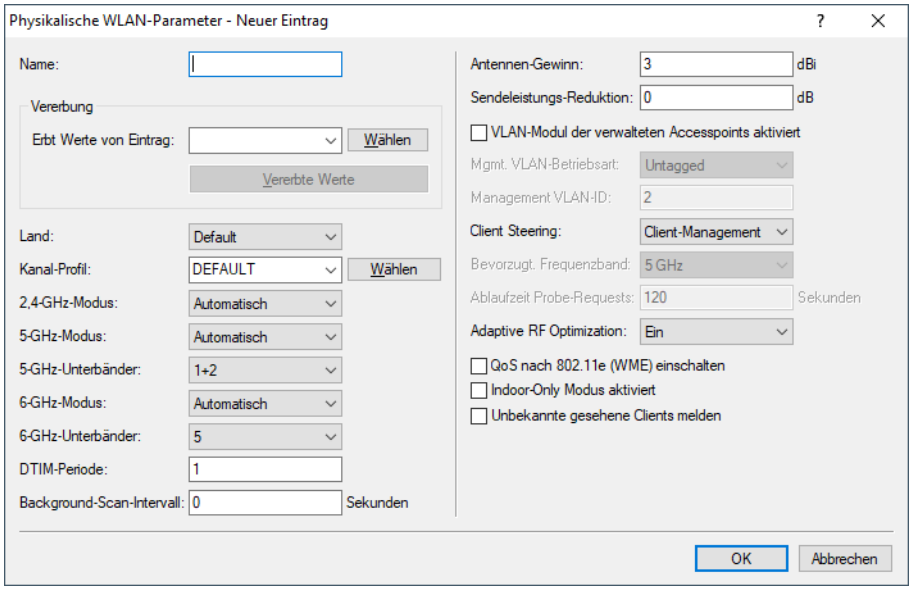
1. Erstellen Sie für das interne WLAN und das Gäste-WLAN jeweils einen Eintrag in der Liste der logischen Netzwerke mit einem passenden Namen und der zugehörigen SSID. Verbinden Sie die SSID für die interne Nutzung mit dem 'LAN am AP', die SSID für die Gäste z. B. mit 'WLC-TUNNEL-1'. Deaktivieren Sie bei der SSID für das Gästenetzwerk die Verschlüsselung, damit sich die WLAN-Clients der Gäste beim Public Spot anmelden können. Unterbinden Sie

für diese SSID außerdem den Datenverkehr der Stationen untereinander (Interstation-Traffic). In LANconfig finden Sie diese Einstellung unter **Konfiguration** > **WLAN-Controller** > **Profile** > **Logische WLAN-Netzwerke (SSIDs)**.

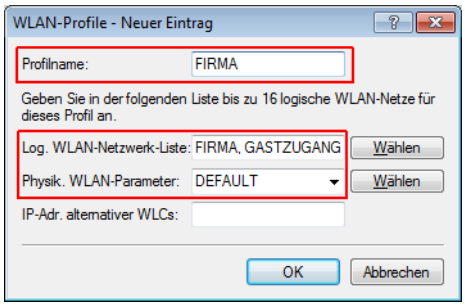




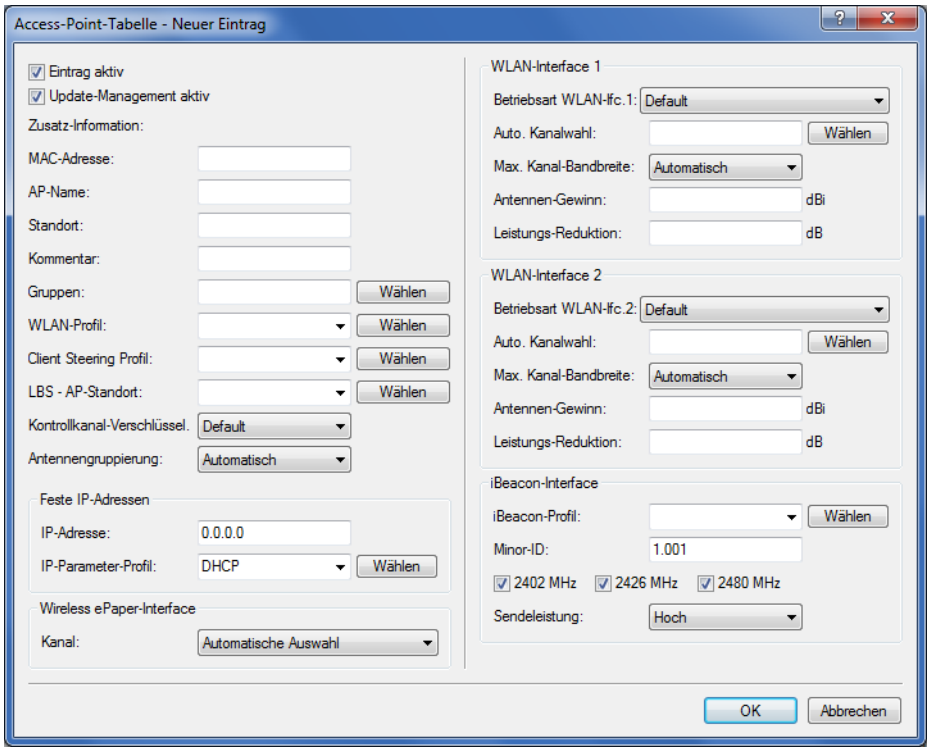
2. Erstellen Sie einen Eintrag in der Liste der physikalischen WLAN-Parameter mit den passenden Einstellungen für Ihre APs, z. B. für das Land 'Europa' mit den Kanälen 1, 6 und 11 im 802.11g/b/n und 802.11a/n gemischten Modus. In LANconfig finden Sie diese Einstellung unter **Konfiguration** > **WLAN-Controller** > **Profile** > **Physikalische WLAN-Parameter**.



3. Erstellen Sie ein WLAN-Profil mit einem passenden Namen und ordnen Sie diesem WLAN-Profil die zuvor erstellten logischen WLAN-Netzwerke und die physikalischen WLAN-Parameter zu. In LANconfig finden Sie diese Einstellung unter **Konfiguration** > **WLAN-Controller** > **Profile** > **WLAN-Profile**.

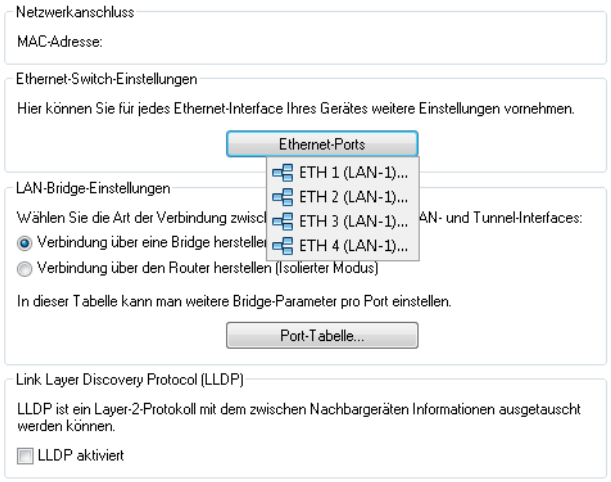


4. Erstellen Sie für jeden verwalteten AP einen Eintrag in der AP-Tabelle mit einem passenden Namen und der zugehörigen MAC-Adresse. Ordnen Sie diesem AP das zuvor erstellte WLAN-Profil zu. In LANconfig finden Sie diese Einstellung unter **Konfiguration** > **WLAN-Controller** > **AP-Konfig** > **Access-Point-Tabelle**.

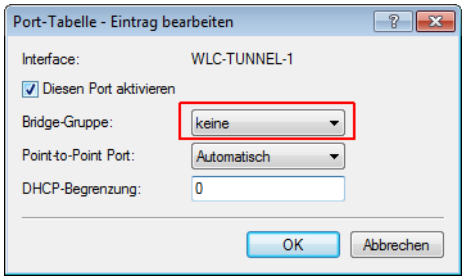


5. Ordnen Sie jedem physikalischen Ethernet-Port eine separate logische LAN-Schnittstelle zu, z. B. 'LAN-1'. Stellen Sie den 4. Ethernet-Port auf die logische LAN-Schnittstelle 'DSL-1' ein. Der WLC verwendet diese LAN-Schnittstelle später

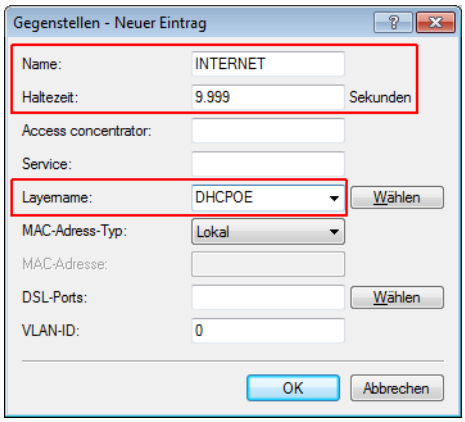
für den Internetzugang des Gästenetzes. In LANconfig finden Sie diese Einstellung unter **Konfiguration** > **Schnittstellen** > **LAN** > **Ethernet-Ports**.



6. Überprüfen Sie, dass die logische LAN-Schnittstelle 'WLC-Tunnel 1' keiner Bridge-Gruppe zugeordnet ist. So stellen Sie sicher, dass die anderen LAN-Schnittstellen keine Daten zum Public Spot-Netzwerk übertragen. In LANconfig finden Sie diese Einstellung unter **Konfiguration** > **Schnittstellen** > **LAN** > **Port-Tabelle**.

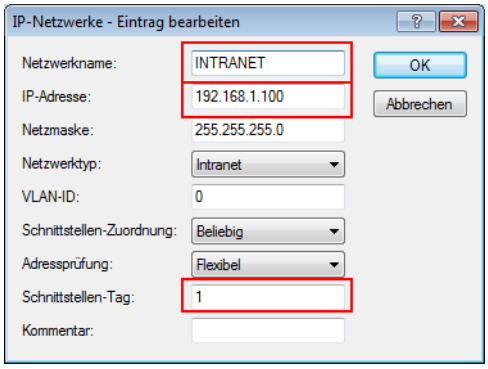


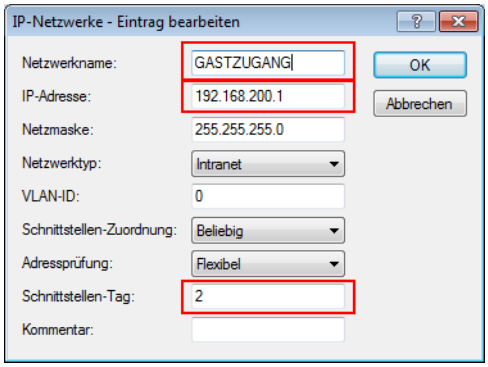
7. Erstellen Sie für den Internetzugang der Gäste einen Eintrag in der Liste der DSL-Gegenstellen mit der Haltezeit '9999' und dem vordefinierten Layer 'DHCPOE'. Dieses Beispiel setzt voraus, dass ein Router mit aktiviertem DHCP-Server den Internetzugang bereitstellt. In LANconfig finden Sie diese Einstellung unter **Konfiguration** > **Kommunikation** > **Gegenstellen** > **Gegenstellen**.



8. Erstellen Sie für die interne Nutzung das IP-Netzwerk 'INTRANET' z. B. mit der IP-Adresse '192.168.1.100' und mit dem Schnittstellen-Tag '1', für die Gäste das IP-Netzwerk 'GASTZUGANG' z. B. mit der IP-Adresse '192.168.200.1' und mit dem Schnittstellen-Tag '2'. Der virtuelle Router im WLC nutzt die Schnittstellen-Tags, um die Routen für die

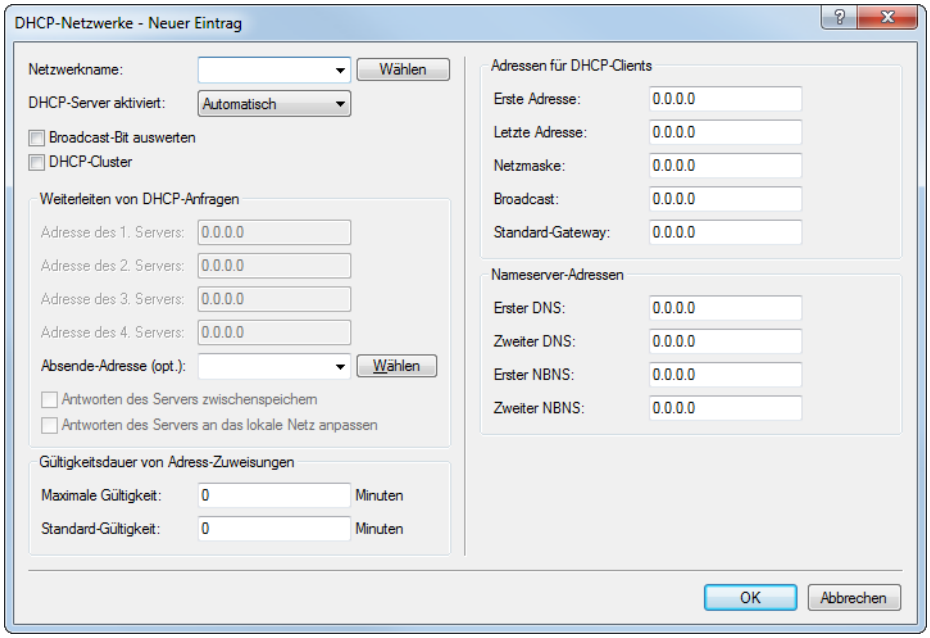
beiden Netzwerke zu trennen. In LANconfig finden Sie diese Einstellung unter **Konfiguration** > **TCP/IP** > **Allgemein** > **IP-Netzwerke**.



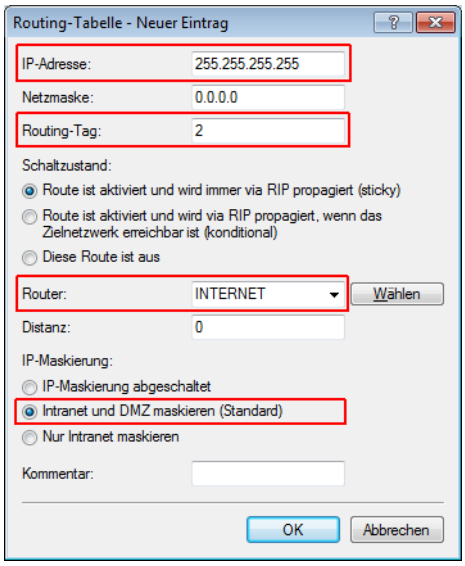


9. Der WLC kann als DHCP-Server für die APs und die angemeldeten WLAN-Clients fungieren. Aktivieren Sie dazu den DHCP-Server für das 'INTRANET' und den 'GASTZUGANG. In LANconfig finden Sie diese Einstellung unter **Konfiguration** > **TCP/IP** > **DHCP** > **DHCP-Netzwerke**.

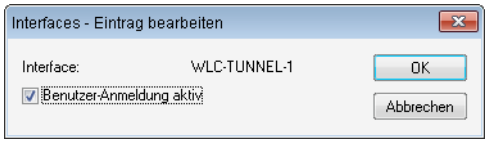
Die Aktivierung des DHCP-Servers ist für das Gästenetz zwingend, für das interne Netz optional. Für das interne Netz können Sie den DHCP Server auch anders realisieren.



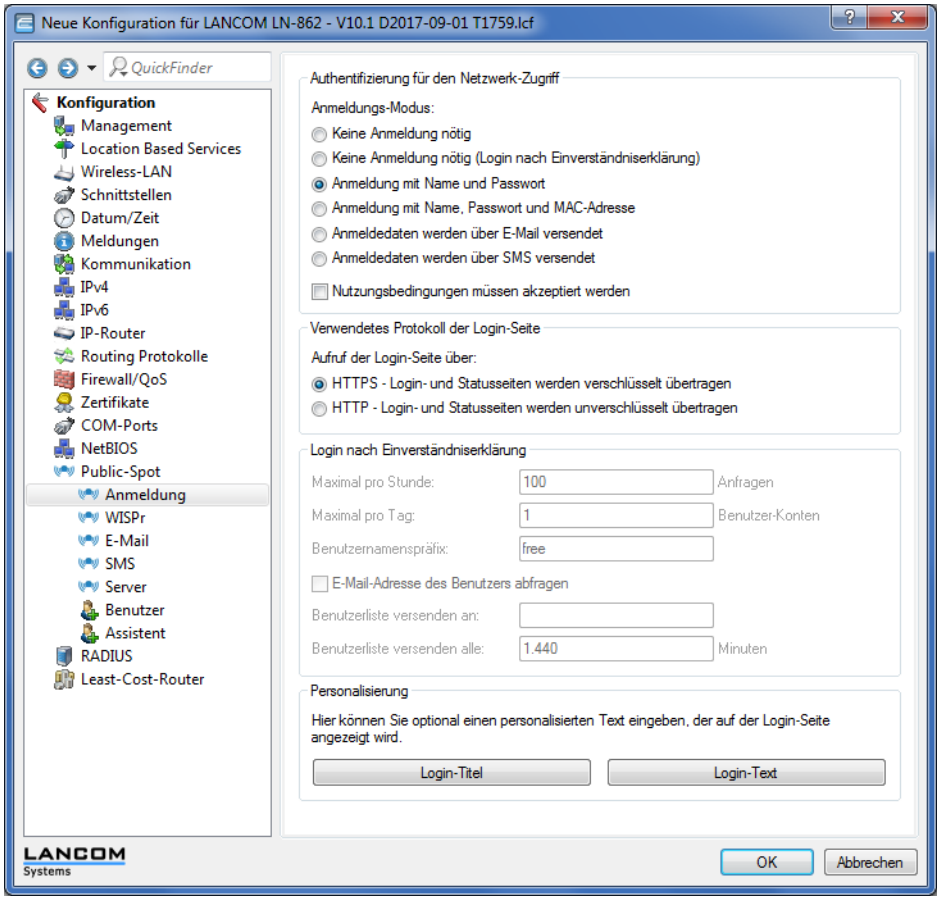
10. Erstellen Sie eine neue Standard-Route in der Routing-Tabelle, welche die Daten aus dem Gästenetzwerk auf den Internet-Zugang des WLCs leitet. Wählen Sie dazu das Routing-Tag '2' und den Router 'Internet'. Aktivieren Sie außerdem die Option 'Intranet und DMZ maskieren (Standard)'. In LANconfig finden Sie diese Einstellung unter **Konfiguration** > **IP-Router** > **Routing** > **Routing-Tabelle**.



11. Aktivieren Sie die Public Spot-Anmeldung für die logische LAN-Schnittstelle 'WLC-Tunnel 1'. In LANconfig finden Sie diese Einstellung unter **Konfiguration** > **Public-Spot** > **Server** > **Betriebseinstellungen** > **Interfaces**.



12. Aktivieren Sie im letzten Schritt die Anmeldung über den Public-Spot für den WLC. In LANconfig finden Sie diese Einstellung unter **Konfiguration** > **Public-Spot** > **Anmeldung**.



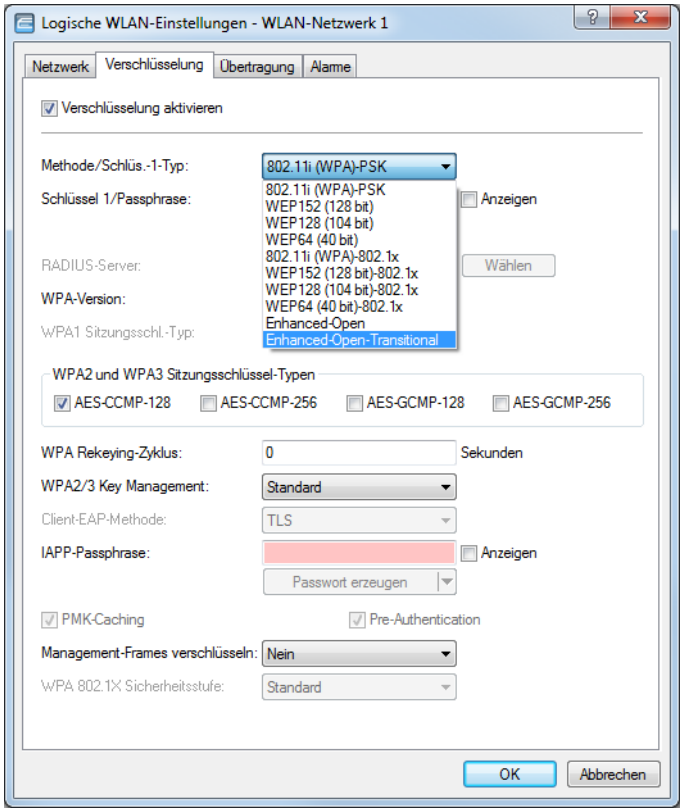
Neben der Konfiguration des WLCs konfigurieren Sie den Public Spot nach Ihren Wünschen entweder für die interne Benutzerliste oder für die Verwendung eines RADIUS-Servers.

15.4.3 Einrichtung eines sicheren Hotspots mit Enhanced Open

Mit Enhanced Open bietet sich erstmals die Möglichkeit, einen sicheren und trotzdem einfach bedienbaren Hotspot anzubieten.

Hierzu wird Enhanced Open mit der LANCOM Public Spot Option kombiniert.

Richten Sie hierzu das für den Hotspot zu nutzende WLAN wie gewohnt ein – wählen Sie allerdings als Verschlüsselungsmethode **Enhanced Open-Transitional**:



Die Eingabe eines Schlüssels ist nicht erforderlich und auch nicht möglich: Ein Enhanced Open-fähiger Client baut ohne Angabe eines Schlüssels eine verschlüsselte Verbindung zum Access Point auf. Die Benutzererfahrung ist damit identisch zu der bei Verwendung eines unverschlüsselten WLANs: Das Eingeben eines vorher erhaltenen Schlüssels wie bei WPA2-PSK entfällt.

Die Nutzung des Transitional-Modus bewirkt, dass die selbe SSID gleichzeitig von Clients verwendet werden kann, die Enhanced Open unterstützen, sowie von Clients, die noch kein Enhanced Open unterstützen. Im letztgenannten Fall kommt allerdings keine Verschlüsselung zum Einsatz, so dass die SSID wie eine ohne Verschlüsselung betriebene SSID funktioniert. Sobald Enhanced Open in der Zukunft eine hohe Marktdurchdringung erreicht hat, kann vom Transitional-Modus in den regulären Enhanced Open-Modus gewechselt werden.

Anschließend kann wie gewohnt mit der Konfiguration des Public Spot-Moduls fortgefahren werden. Da das Public Spot-Modul unabhängig von den Verschlüsselungseinstellungen der WLAN-Schnittstellen ist, können alle Funktionen des Public Spot-Moduls in Zusammenhang mit Enhanced Open ohne Einschränkung verwendet werden.

Zusammenfassend eignet sich Enhanced Open ideal für den Betrieb von Hotspots, da es ein höheres Sicherheitsniveau als die bisher verwendeten, unverschlüsselten Hotspots bietet. Durch den optionalen Transitional-Modus ist sichergestellt, dass auch Clients, welche Enhanced Open noch nicht unterstützen, transparent angebunden werden können.

15.4.4 Einrichtung eines externen RADIUS-Servers für die Benutzerverwaltung

In manchen Anwendungen sollen die Benutzerdaten nicht im Gerät gespeichert werden, sondern in einem externen, zentralen RADIUS-Server. In diesem Fall muss der Public Spot zur Überprüfung der Benutzerdaten mit diesem externen RADIUS-Server kommunizieren.

Beachten Sie, dass Ihnen bestimmte Funktionen (wie z. B. die Public Spot-Assistenten in WEBconfig) nicht zur Verfügung stehen, wenn Sie einen externen RADIUS-Server zur Benutzerverwaltung einsetzen!

Die folgende Anleitung setzt voraus, dass Ihnen die IP-Adresse eines funktionsfähigen RADIUS-Servers im Netzwerk bekannt ist.

Mit den folgenden Konfigurationsschritten richten Sie einen Public Spot für die Nutzung eines externen RADIUS-Servers ein:

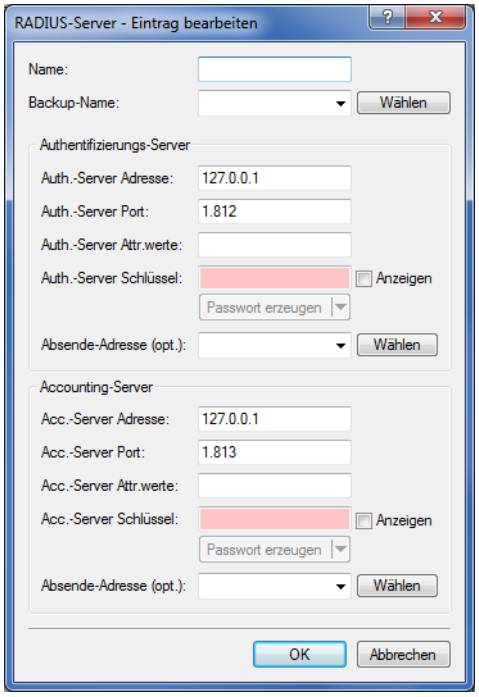
1. Führen Sie die Schritte aus dem Abschnitt *Manuelle Installation* aus.

   Die exakte Uhrzeit im Gerät ist hier u. a. für die korrekte Steuerung von zeitlich begrenzten Zugängen notwendig.

   Wenn die Authentifizierung mit zusätzlicher Prüfung der physikalischen Adresse (MAC-Adresse) eingestellt ist, übermittelt der Public Spot bei der Anmeldung eines Benutzers die MAC-Adresse des Endgerätes an den RADIUS-Server. Dabei bleibt dem Public Spot verborgen, ob der Server die MAC-Adresse auch tatsächlich prüft oder nicht. Die korrekte Überprüfung der MAC-Adresse muss durch entsprechende Konfiguration des RADIUS-Servers gewährleistet sein.

2. Tragen Sie die Angaben zum RADIUS-Server ein.

   Bei der Konfiguration eines Public Spots können die Benutzer-Anmeldedaten an einen oder mehrere RADIUS-Server weitergeleitet werden. Diese Server konfigurieren Sie in LANconfig unter **Public-Spot** > **Benutzer** > **Benutzer und RADIUS-Server** > **RADIUS-Server**. Welche Anmeldedaten die einzelnen RADIUS-Server von den Benutzern benötigen, ist für das den Public Spot bereitstellende Gerät nicht wichtig, da dieses die Daten transparent an den RADIUS-Server weiterreicht.



   Die angegebenen IP-Adressen müssen statisch sein. Außerdem muss der Public Spot die angegebenen Ziel-Adressen erreichen können. Für IP-Adressen außerhalb des eigenen Netzwerkes ist es daher erforderlich, einen Router mit Kontakt zum Ziel-Netzwerk als Gateway in den DHCP-Einstellungen des Public Spots einzutragen. Dieses Gateway müssen Sie als Default-Route in die Routing-Tabelle eintragen.

   Zur Verbuchung der Verbindungsdaten durch den RADIUS-Server ist es erforderlich, die Angaben zum Accounting-Server vollständig einzutragen. Alternativ zur Verwendung eines RADIUS-Accounting-Servers können Sie sich die Verbindungsinformationen vom Public Spot auch per SYSLOG-Funktion ausgeben lassen.

3. Fertig!

   Damit ist Ihr Public Spot betriebsbereit. Alle Benutzer, die über ein gültiges Konto am RADIUS-Server verfügen, können sich über das Web-Interface am Public Spot anmelden.

15.4.5 Interner und externer RADIUS-Server kombiniert

Für die Authentifizierung von Benutzern mit IEEE 802.1X wird in manchen Unternehmen ein externer RADIUS-Server eingesetzt. In einer Anwendung mit einem WLAN Controller und mehreren Access Points fungiert zunächst der WLAN Controller als RADIUS-Server für alle Access Points. Im WLAN Controller definieren Sie dazu die entsprechende Weiterleitung der RADIUS-Anfragen an den externen RADIUS-Server.

Die im folgenden beschriebenen Einstellungen sind nur dann notwendig, wenn Sie in Ihrem Gerät neben dem Public Spot einen externen RADIUS-Server nutzen.

Im Zusammenhang mit einem Public Spot für Gast-Zugänge sind weitere Einstellungen notwendig:

- Die Authentifizierungsanfragen der internen Mitarbeiter sollen an den externen RADIUS-Server weitergeleitet werden.
- Die Authentifizierungsanfragen der Public Spot-Zugänge sollen vom internen RADIUS-Server geprüft werden.

15.4.5.1 Realm-Tagging für das RADIUS-Forwarding

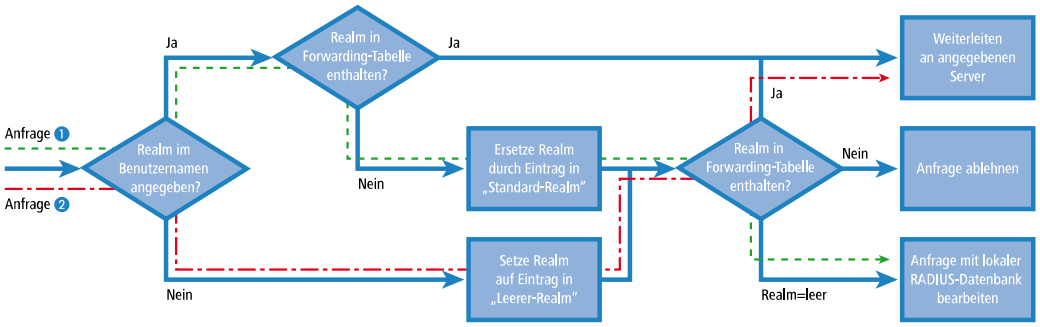
Die Authentifizierungsanfragen der beiden Benutzergruppen müssen separat behandelt werden. Damit der WLAN Controller diese beiden Gruppen unterscheiden kann, nutzt er sogenannte "Realms". Realms dienen der Adressierung von Domänen, innerhalb derer Benutzeraccounts gültig sind. Der WLAN Controller kann die Realms mit der Authentifizierungsanfrage an den internen RADIUS-Server übermitteln. Alternativ kann der RADIUS-Server nach folgenden Regeln die Realms der Benutzernamen verändern, um das RADIUS-Forwarding zu steuern:

- Der als "Standard-Realm" definierte Wert ersetzt einen vorhandenen Realm einer eingehenden Anfrage, wenn für diesen Realm keine Weiterleitung definiert ist.
- Der RADIUS-Server verwendet den unter "Leerer-Realm" definierten Wert **nur dann**, wenn der eingehende Benutzername **noch keinen** Realm enthält.

Über einen Eintrag in der Weiterleitungstabelle leitet der WLAN Controller alle Authentifizierungsanfragen mit einem bestimmten Realm an einen RADIUS-Server weiter. Wenn in der Weiterleitungstabelle kein passender Eintrag vorhanden ist, lehnt er die Anfrage ab.

Stellt der WLAN Controller nach der Ermittlung eines Realms einen leeren Realm fest, so prüft er die Authentifizierungsanfrage **immer** mit der internen RADIUS-Datenbank.

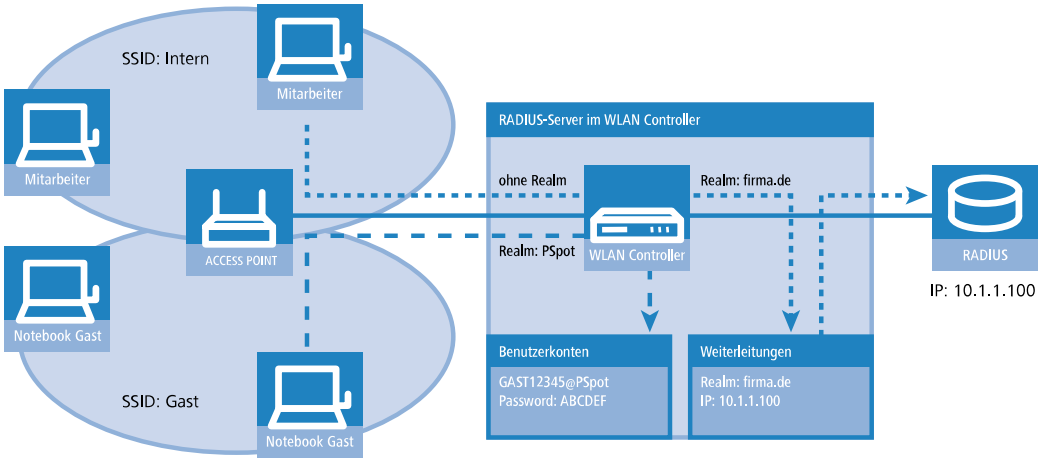
Das folgende Flussdiagramm zeigt schematisch die Arbeitsweise des RADIUS-Server bei der Verarbeitung von Realms:



Durch ein unterschiedliches Realm-Tagging können somit verschiedene RADIUS-Server angesprochen werden. Den Entscheidungsweg im RADIUS-Server des Gerätes können Sie im Diagramm für die beiden Anfragen verfolgen:

1. Da die Benutzernamen für die Gastzugänge automatisch erzeugt werden, wird für diese Benutzernamen der Realm "PSpot" verwendet. Da in der Weiterleitungstabelle kein entsprechender Eintrag vorhanden ist und der Standard-Realm leer ist, leitet der WLAN Controller alle Authentifizierungsanfragen mit diesem Realm an den internen RADIUS-Server weiter.
2. Um den Konfigurationsaufwand zu begrenzen, werden die internen Benutzer weiterhin ohne Realm geführt. Der RADIUS-Server im Gerät kann einen leeren Realm automatisch durch einen anderen Realm ersetzen, mit dem er die internen Benutzer identifiziert. In diesem Beispiel ersetzt er den leeren Realm durch die Domäne der Firma "firma.de".

Mit den Angaben in der Weiterleitungstabelle können alle Authentifizierungsanfragen mit diesem Realm an den externen RADIUS-Server weitergeleitet werden.

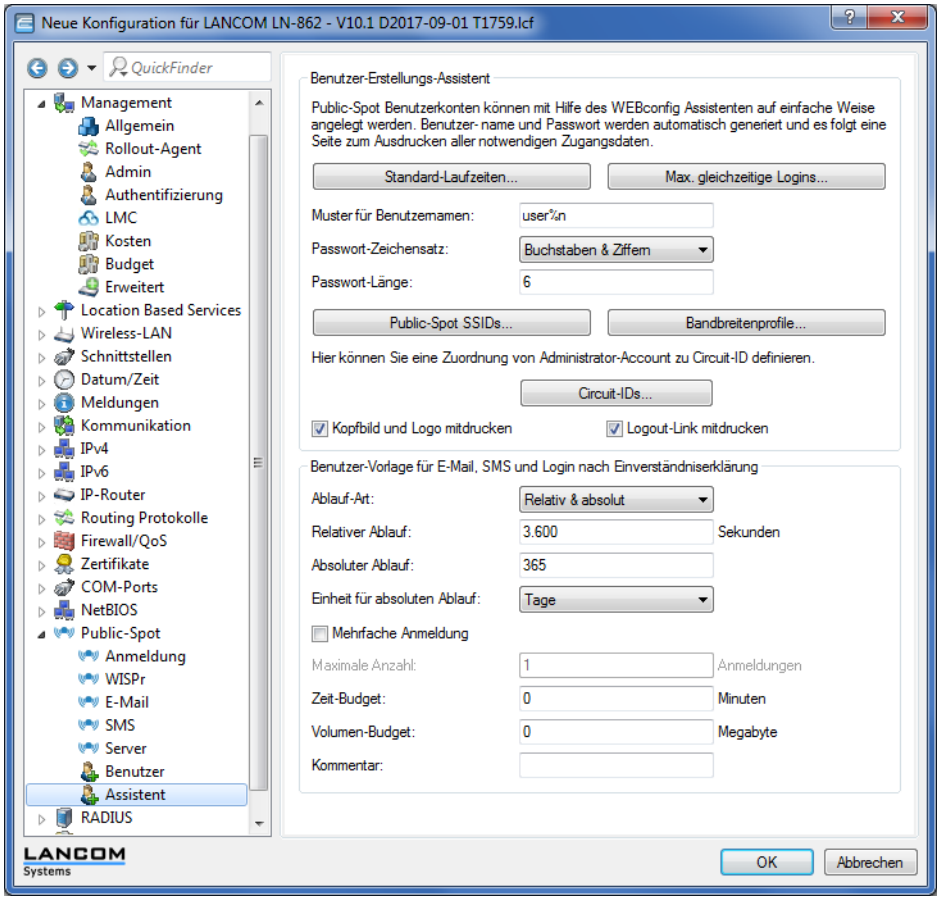


15.4.5.2 Konfiguration für das RADIUS-Forwarding

Mit den folgenden Konfigurationsschritten können Sie die separate Behandlung der internen Benutzer und der Gastzugänge definieren.

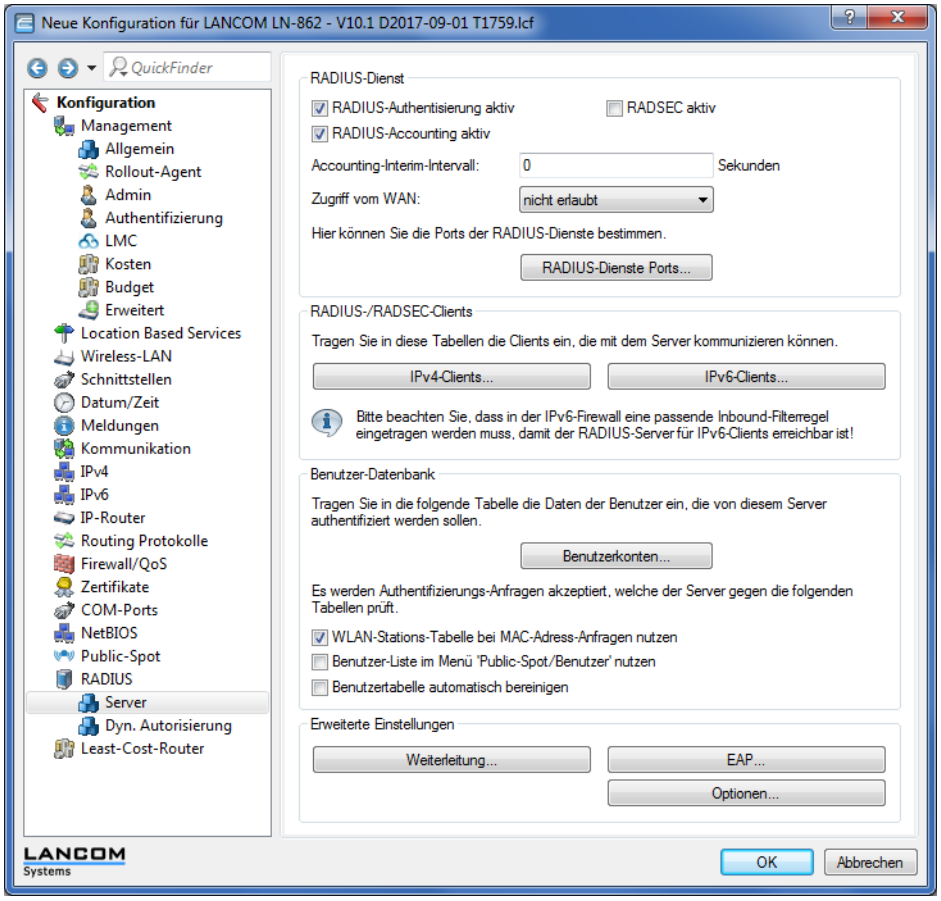
1. Passen Sie im Public Spot das Muster für die Benutzernamen so an, dass ein eindeutiger Realm verwendet wird. Mit dem Muster "user%n@PSpot" generiert der Public-Spot z. B. Benutzernamen der Form "user12345@PSpot".

   › **LANconfig: Public-Spot** > **Assistent** > **Benutzer-Erstellungs-Assistent**



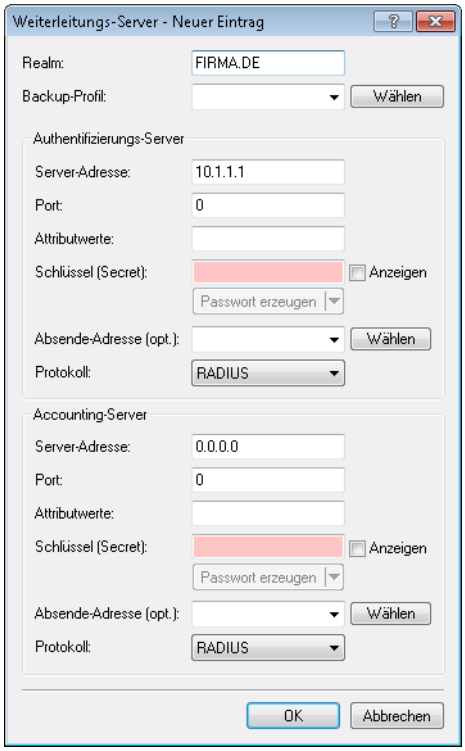
2. Tragen Sie im RADIUS-Server des WLAN Controllers einen "leeren Realm" ein (z. B. "FIRMA.DE").
   Dieser Realm wird für alle Benutzernamen verwendet, die ohne Realm eine Authentifizierungsanfrage bei dem WLAN Controller stellen. Das sind in dieser Anwendung die internen Benutzer, für die kein Realm definiert ist. Damit der RADIUS-Server des WLAN Controllers für diese Benutzernamen auch keinen Realm einsetzt, müssen Sie den "Standard-Realm" unbedingt leer lassen.

   › **LANconfig: RADIUS > Server > Erweiterte Einstellungen > Weiterleitung > RADIUS-Weiterleitungs-Server > Weiterleitungs-Server**



3. Damit der WLAN Controller die Authentifizierungsanfragen der internen Benutzer an den externen RADIUS-Server weiterleiten kann, legen Sie einen passenden Eintrag bei den Weiterleitungen an.

Mit dem Realm "FIRMA.DE" werden alle eingehenden RADIUS-Anfragen an die angegebene IP-Adresse weitergeleitet, die über diesen Realm verfügen.



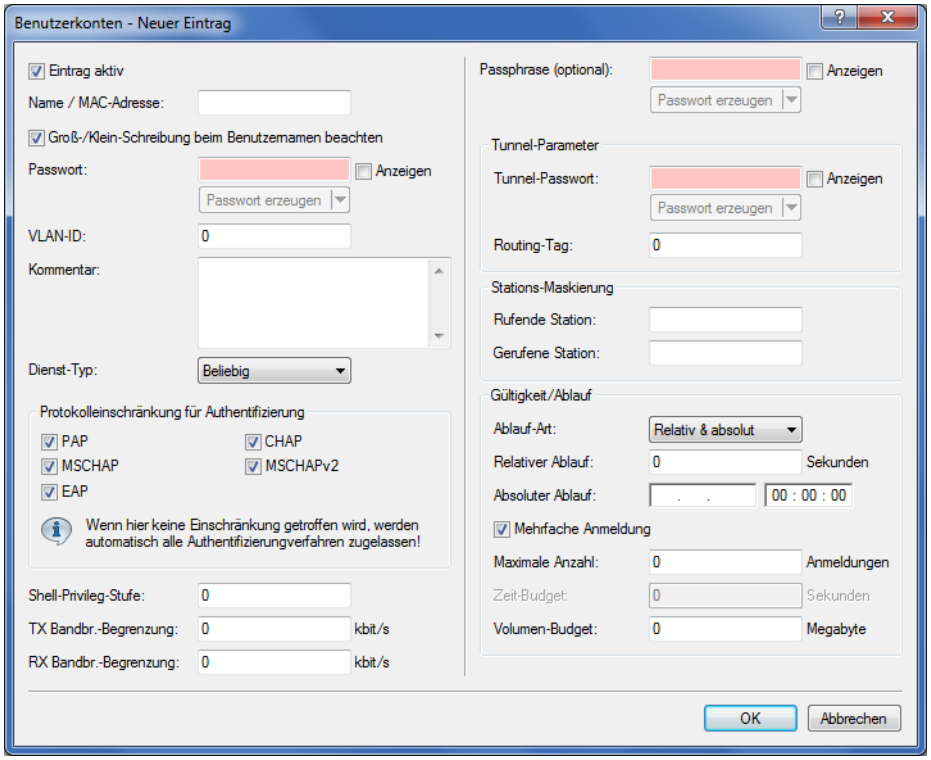
4. Die Authentifizierungsanfragen der Public Spot-Benutzer gehen mit dem Realm "@PSpot" beim WLAN Controller ein. Da für diesen Realm keine Weiterleitung definiert ist, werden die Benutzernamen automatisch in der internen RADIUS-Datenbank geprüft. Da die über den Assistenten angelegten Public Spot-Zugänge in dieser Datenbank gespeichert werden, können diese Anfragen wie gewünscht authentifiziert werden.

15.4.6 Prüfung von WLAN-Clients über RADIUS (MAC-Filter)

Bei der Nutzung von RADIUS zur Authentifizierung von WLAN-Clients können Sie neben einem externen RADIUS-Server auch die interne RADIUS-Benutzerdatenbank eines WLAN Controllers nutzen, um nur bestimmten WLAN-Clients anhand ihrer MAC-Adresse den Zugang zum WLAN zu erlauben.

Tragen Sie die zugelassenen MAC-Adressen über LANconfig in die RADIUS-Datenbank ein und aktivieren Sie alle Authentifizierungsmethoden. Wählen Sie als **Name / MAC-Adresse** und **Passwort** jeweils die MAC-Adresse in der Schreibweise 'AABBCC-DDEEFF'.

› LANconfig: **RADIUS** > **Server** > **Benutzer-Datenbank** > **Benutzerkonten**



15.4.7 Einrichtung eines externen SYSLOG-Servers

Je nach Anwendungsfall, ist für den Betrieb eines Public Spots das Speichern der Nutzungsdaten erforderlich. Diese Daten lassen sich z. B. in einem SYSLOG-Server speichern. SYSLOG-Server sind teilweise als freie Software verfügbar.

Zum Speichern der Nutzungsdaten aus einem Public Spot über SYSLOG wird der externe SYSLOG-Server in dem jeweiligen Public Spot konfiguriert. Daraufhin wird das Anlegen bzw. Löschen von Public Spot-Benutzern sowie der Anfang und das Ende von Public Spot-Sitzungen mit einer Nachricht an den SYSLOG-Server protokolliert. Beim Ende der Sitzung wird in dieser Nachricht – mit der Quelle "Login" und der Priorität "Information" – neben dem übertragenen Datenvolumen auch die verwendete IP-Adresse gemeldet.

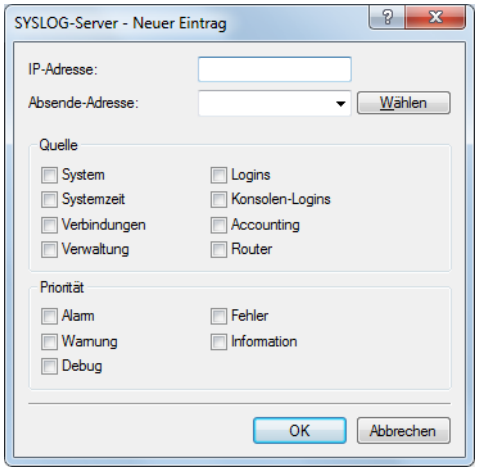
Weitere Informationen über die Konfiguration von SYSLOG entnehmen Sie bitte dem Kapitel *Das SYSLOG-Modul*. Informationen über die rechtlichen Regelungen finden Sie im LANCOM Techpaper "Public Spot", erhältlich unter *www.lancom-systems.de*.

15.4.7.1 Externen SYSLOG-Server konfigurieren

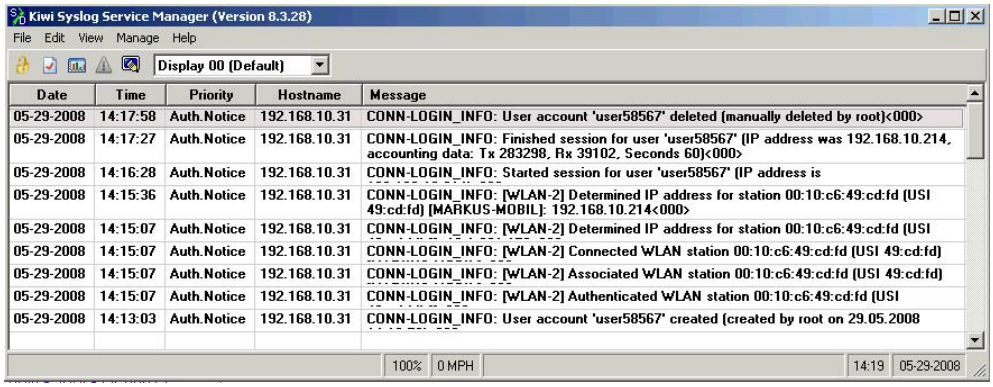
Ihr Gerät ist dazu in der Lage, das Anlegen und Löschen von neuen Public Spot-Benutzern sowie deren An- und Abmeldevorgänge zu protokollieren. Diese intern gespeicherten Informationen können Sie aber auch an einen externen SYSLOG-Server weiterleiten. Die nachfolgenden Schritte zeigen Ihnen, wie Sie die Protokollierung mit einem auf einem externen SYSLOG-Server installierten Programm vornehmen (in diesem Beispiel "Kiwi").

1. Starten Sie LANconfig und öffnen Sie den Konfigurationsdialog Ihres Gerätes.
2. Wechseln Sie in den Dialog **Meldungen** > **Allgemein** und öffnen Sie die Tabelle **SYSLOG-Server**.

3. Fügen Sie einen neuen Eintrag hinzu. Definieren Sie dazu die **IP-Adresse** des Rechners, auf dem der SYSLOG-Client installiert ist (z. B. `192.168.10.237`), und geben Sie die **Quelle** (`Logins`, `Accounting`) sowie die **Priorität** (`Information`) an.



4. Schließen Sie die Dialoge und schreiben Sie die Konfiguration zurück auf Ihr Gerät.
5. Starten Sie das Auswertungsprogramm auf Ihrem SYSLOG Server (z. B. "Kiwi"). Sobald das Programm gestartet ist, zeichnet es das Anlegen und Löschen von neuen Public Spot-Benutzern sowie die An- und Abmeldungen von Public Spot-Benutzers auf.



15.5 XML-Interface

Um eine Vielzahl von Public Spot-Szenarios abdecken zu können, ist die Standard-Authentifizierungsmethode des Public Spots alleine über Name und Passwort nicht ausreichend. Zugriffs- und Abrechnungsmodelle über Social Media, Kreditkarten und weitere Methoden erfordern oft zusätzliche Zugriffsdaten, die der Public Spot in dieser Form nicht verwalten kann.

Die implementierte XML-Schnittstelle verbindet den Public Spot und ein externes Gateway. Sie leitet dabei die Daten des Benutzers nur an das Gateway weiter, das anschließend die Authentifizierung und Abrechnung übernimmt und dem Public Spot nur Informationen über Dauer und Limitierungen des Benutzerzugangs mitteilt.

Der Public Spot übernimmt also dabei nur die folgenden Aufgaben:

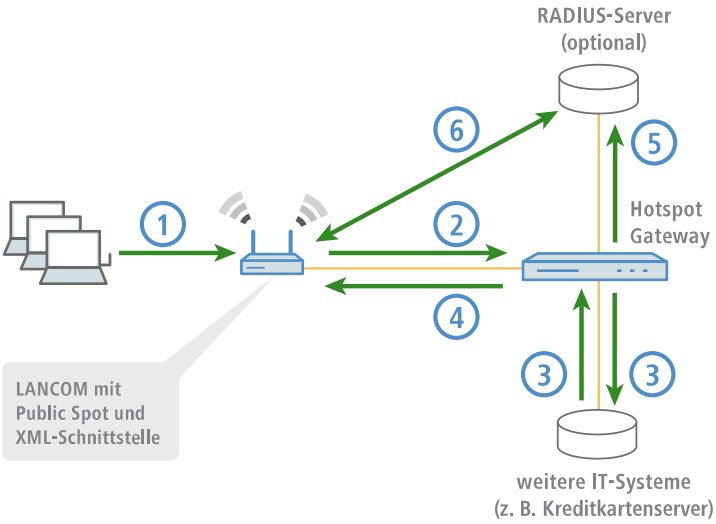
- Weiterleiten der Benutzeranfragen
- Einschränken von unerlaubten Zugangsversuchen
- Annahme der Gateway-Kommandos zum Starten und Beenden einer Sitzung

› ggf. Abrechnen der Sitzungen

Da es nicht sinnvoll ist, alle vorhandenen, teilweise sehr speziellen Szenarios mit den zugehörigen Gateway-Befehlen im Public Spot zu implementieren, ist die XML-Schnittstelle universal und flexibel aufgebaut.

15.5.1 Funktion

Die Kommunikation zwischen XML-Interface und externem Gateway läuft ab wie folgt:



1. Der Benutzer verbindet sich mit dem WLAN auf dem Public Spot und sendet eine HTTP-Anfrage an den Public Spot.
2. Der Public Spot leitet die HTTP-Anfrage für den Login-Vorgang weiter an das externe Hotspot-Gateway. Dazu befindet sich das externe Hotspot-Gateway entweder in einem frei zugänglichen Netz des Public Spots oder seine Adresse gehört zur Liste der freien Hosts.

   Das externe Gateway erhält die MAC-Adresse des anfragenden Public Spot-Clients dabei in der Weiterleitung durch den Public Spot. Unter **Public-Spot-Modul** > **Seitentabelle** wählen Sie dazu bei der entsprechenden Seite den **Typ** "Redirect" aus und ergänzen die **URL** um den Parameter `?myvar=%m`.

   Beispiel: `http://192.168.1.1/?myvar=%m`

   Hierbei ist `myvar` eine beliebig wählbare Variable. Entscheidend ist die Variable `%m`, die der Public Spot beim Weiterleiten der Anfrage durch die MAC-Adresse des Public Spot-Clients ersetzt.

Tabelle 41: Variblen

Variable	Bedeutung
%s	SSID-Name
%v	Quell-VLAN
%i	Interface (gilt für LAN, WLAN, WLC-Tunnel)
%t	Routing-Tag
%m	MAC-Adresse des Clients
%c	MAC-Adresse des Public Spot Gateways
%r	Remote-IP (Client)
%p	lokale IP (Public Spot Gateway)
%o	original durch den Client aufgerufene URL
%n	Gerätename des Public Spot Gateways

Variable	Bedeutung
%e	Seriennummer des Public Spot Gateways
%l	Hostname des Public Spot Gateways
%0-9	Fügt eine einzelne Zahl im Bereich von 0 bis 9 ein
%%	Fügt ein einzelnes Prozentzeichen ein

3. Das Hotspot-Gateway prüft die Anmeldedaten des Benutzers und kontaktiert ggf. weitere IT-Systeme zur Kreditkartenabrechnung o. ä.
4. Das Hotspot-Gateway sendet eine XML-Datei mit den Benutzerdaten an die XML-Schnittstelle des Public Spots. Das externe Hotspot-Gateway kontaktiert das Gerät mit Public Spot-XML-Schnittstelle über die URL `http://<Geräte-URL>/xmlauth`.

   Die XML-Schnittstelle im Public Spot analysiert diese Datei und veranlasst die entsprechenden Aktionen. Bei einer Login-Anfrage übernimmt die XML-Schnittstelle den Benutzer mit seiner MAC-Adresse in die Liste der angemeldeten Public Spot-Benutzer. Bei einer Logout-Anfrage entfernt die XML-Schnittstelle den Benutzer wieder aus dieser Liste. Gleichzeitig bestätigt die XML-Schnittstelle die jeweilige Anfrage, indem sie eine entsprechende XML-Datei an das Hotspot-Gateway sendet.

   Damit der Public Spot die Anweisungen der XML-Datei verarbeiten kann, muss im Gerät ein spezieller Administrator eingerichtet sein, der das Funktionsrecht "Public Spot-XML-Schnittstelle" besitzt. Über dieses Admin-Konto meldet sich das Hotspot-Gateway am Public Spot an.

   Während der Benutzer am Public Spot angemeldet ist, können XML-Schnittstelle und Hotspot-Gateway Statusinformationen in Form von XML-Dateien über die aktuelle Session austauschen.

   Hat der Benutzer sein Online-Kontingent ausgeschöpft, sendet das Hotspot-Gateway einen Stop-Befehl an die XML-Schnittstelle, woraufhin der Public Spot dem Benutzer den weiteren Zugang sperrt. Auch die Sperrung des Zugangs bestätigt das XML-Interface wieder mit einer entsprechenden XML-Datei an das Hotspot-Gateway.
5. Sofern die zusätzliche Nutzung eines RADIUS-Servers aktiviert ist, meldet das Hotspot-Gateway einen Benutzer an einem RADIUS-Server an.
6. Der Public Spot übermittelt während der Sitzung die relevanten Daten an den RADIUS-Server, z. B. für eine spätere Abrechnung der Public Spot-Nutzung (Accounting). Standardmäßig verwendet der Public Spot dazu seinen internen RADIUS-Server. Bei Bedarf konfigurieren Sie auf dem Gerät mit Public Spot die Nutzung eines externen RADIUS-Servers.



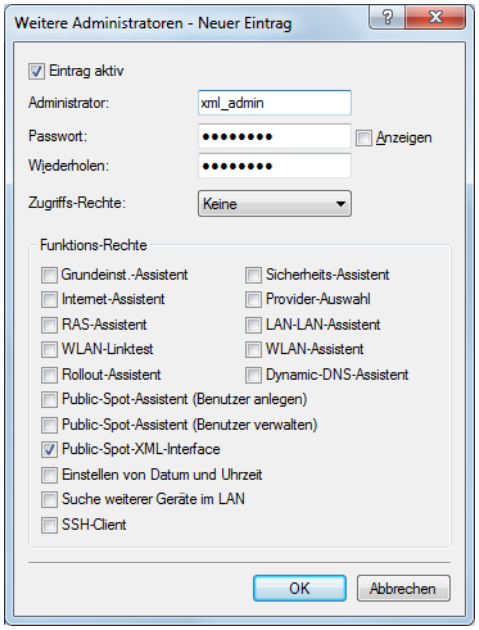
Die Kommunikation zwischen dem Public Spot und einem Hotspot-Gateway über XML ist nicht genormt. Konfigurieren Sie das Hotspot-Gateway entsprechend den Vorgaben im Abschnitt *Befehle*, so dass Public Spot und Hotspot-Gateway die verwendeten XML-Nachrichten in der erforderlichen Form austauschen. Der Austausch der XML-Nachrichten läuft unsichtbar ohne grafische Oberfläche ab. Testen Sie diesen Nachrichtenaustausch z. B. über Tools wie *cURL*.

15.5.2 Einrichtung des XML-Interfaces

Der folgende Abschnitt beschreibt die Einrichtung des XML-Interfaces.

1. Erstellen Sie unter **Management** > **Admin** > **Weitere Administratoren** einen neuen Administrator mit dem Funktionsrecht **Public-Spot-XML-Schnittstelle**.

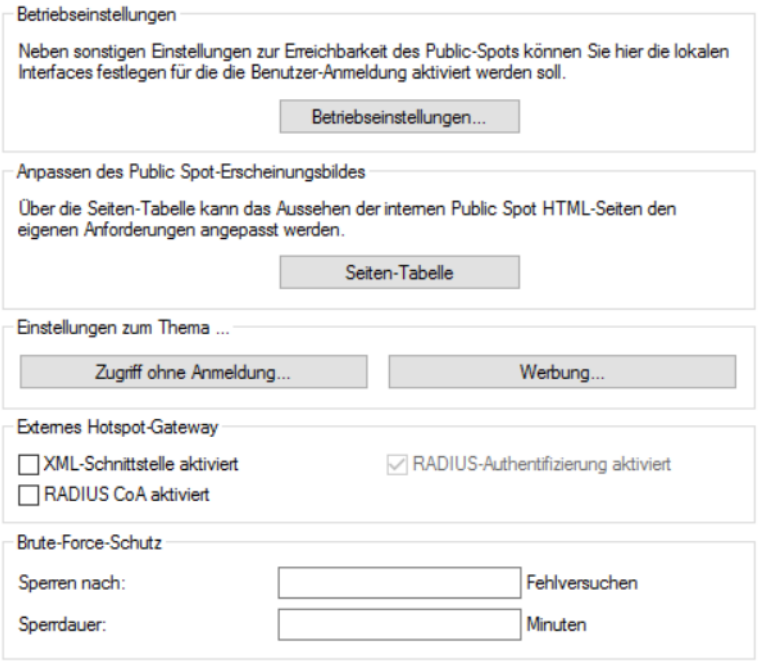
Über dieses Administrator-Konto sendet das (externe) Gateway später seine XML-Anfragen an die XML-Schnittstelle des Public Spots.



Der angelegte Administrator sollte über keine weiteren Public Spot-Funktionsrechte verfügen, da sie das Konto mit bestimmten Konfigurationsrechten ausstatten und dies in Kombination mit dem XML-Interface ein potentielles Sicherheitsrisiko darstellt (z. B. wenn die Kommunikation zwischen XML-Sender und Gerät unverschlüsselt erfolgt).

2. Aktivieren Sie unter **Public-Spot** > **Server** im Abschnitt **Externes Hotspot-Gateway** die XML-Schnittstelle und die RADIUS-Authentifizierung.

   Ankommende XML-Anfragen übergibt das Public Spot-Modul entweder an den internen RADIUS-Server oder – bei Nutzung eines externen RADIUS-Servers über einen Realm – an den externen RADIUS-Server.



3. Klicken Sie im Rahmen **Zugriff ohne Anmeldung ermöglichen** auf die Schaltfläche **Freie Netze** und fügen Sie ein neues Netz hinzu. Für **Name/IP-Adresse** geben Sie den Host-Namen bzw. die IP-Adresse der Anmeldeseite des Gateways ein, dessen Dienste die Public Spot-Benutzer nutzen dürfen. Als **Netzmaske** geben Sie `255.255.255.255` ein.

   Durch die Speicherung als freies Netz können die Benutzer ohne Anmeldung am Public Spot direkt auf die Anmeldeseite des Gateways zugreifen.

4. Konfigurieren Sie das Gateway so, dass es die Sitzungsdaten des Benutzers als XML-Datei an die XML-Schnittstelle des Public Spots sendet.
   Bei Fragen zur Konfiguration des Gateways wenden Sie sich an den zuständigen Service-Provider.

15.5.3 Analyse des XML-Interfaces mit cURL

Der folgende Abschnitt beschreibt die Analyse des XML-Interfaces mit der Open-Source-Software cURL.

cURL (Client for URL) ist eine Kommandozeilen-Anwendung, mit der man Dateien ohne den Einsatz von Web-Browsern oder FTP-Clients in einem Netzwerk übertragen kann. cURL ist Bestandteil von vielen Linux-Distributionen und steht auch für weitere Betriebssysteme zur Verfügung.

Um das XML-Interface mit cURL analysieren zu können, benötigen Sie im Public Spot einen Administrator mit dem Funktionsrecht "Public Spot-XML-Schnittstelle".

1. Laden Sie zunächst cURL herunter und installieren bzw. entpacken Sie es.
2. Starten Sie cURL mit der Befehlszeile `curl -X POST -H "Content-Type:text/xml" -d @filename http://user:pass@myhost/xmlauth/`.

   Die Parameter haben folgende Bedeutung:

   filename

   Pfad und Name der lokalen XML-Datei, z. B. der Login-Request aus den *Beispielen*.

   user

   Benutzername mit Funktionsrecht "Public Spot-XML-Schnittstelle". Ohne diese Authentifizierung funktioniert das XML-Feature nicht.

   pass

   Passwort des Benutzers

   myhost

   IP-Adresse bzw. DNS-Name des Gerätes mit Public Spot-XML-Schnittstelle

3. Über Telnet können Sie mit dem Befehl `trace # XML-Interface-PbSpot` einen Trace aktivieren, um zu überprüfen, ob XML-Anfragen erfolgreich waren bzw. Fehlermeldungen erhalten.

15.5.4 Befehle

Das XML-Interface kann je drei Arten von Anfragen und Antworten verarbeiten:

- Login
- Logout
- Status

Dabei kann eine XML-Datei auch mehrere Anfragen bzw. Antworten enthalten.

15.5.4.1 Login

Sendet das externe Gateway in einer XML-Datei einen "Login"-Request, schaltet der Public Spot den Online-Zugriff für den entsprechenden Benutzer frei. Ein "Login"-Request enthält das Attribut `COMMAND="RADIUS_LOGIN"`.

Verwendet der Public Spot keinen RADIUS-Server, speichert er bei einem "Login"-Request den Benutzer inkl. seiner MAC-Adresse direkt in der internen Statustabelle. Dadurch kann er den Benutzer zukünftig sofort authentifizieren und muss ihm nicht erst eine Login-Seite anzeigen, auf der er Benutzername und Passwort eingeben muss.

Bei Verwendung eines RADIUS-Servers ist eine erfolgreiche Ausführung des "Login"-Request nur dann möglich, wenn die Anmeldedaten des entsprechende Benutzers schon im RADIUS-Server vorliegen.

Über das Web-API des Public Spots können Sie komfortabel neue Public Spot-Benutzer im internen RADIUS-Server des Gerätes anlegen.

Das XML-Interface kann die folgenden XML-Elemente im **Login-Request** verarbeiten:

`SUB_USER_NAME`

Benutzername

`SUB_PASSWORD`

Benutzerpasswort

`SUB_MAC_ADDR`

MAC-Adresse des Benutzer-Gerätes. Mögliche Formate sind:

- 00164115208c
- 00:16:41:15:20:8c
- 00-16-41-15-20-8c

`VLAN_ID` (optional)

Individuelle VLAN-ID, die das Gerät dem Public Spot-Benutzer beim Login zuweist. Die individuelle VLAN-ID überschreibt nach der Authentifizierung durch den RADIUS-Server eine globale VLAN-ID, die ein Nutzer ansonsten über das XML-Interface erhalten würde.

Der Wert `0` deaktiviert die Verwendung eines VLANs.

`SOURCE_VLAN` (optional, nur in Verbindung mit der Authentifizierung über einen RADIUS-Server)

Die VLAN-ID des Netzes, aus dem sich ein Public Spot-Benutzer anzumelden versucht (Quell-VLAN). Der Public Spot leitet die Quell-VLAN in seinem Access-Request an den internen oder einen externen RADIUS-Server weiter. Dazu verwendet der Public Spot das RADIUS-Attribut 81 (**Tunnel-Private-Group-Id**) im Zusammenspiel mit den RADIUS-Attributen 64 (**Tunnel-Type**) und 65 (**Tunnel-Medium-Type**). Der RADIUS-Server kann auf Basis der Quell-VLAN dann z. B. entscheiden, ob er den Access-Request des Public Spots akzeptiert oder ablehnt.

Hat der RADIUS-Server die Anfrage akzeptiert, überträgt er in seinem Access-Accept die o. g. RADIUS-Attribute zurück an den Public Spot. Anschließend hinterlegt der Public Spot das Quell-VLAN für den jeweiligen Client und dessen Stationsliste und gibt dem Benutzer den Zugriff auf das Public Spot-Netz frei.

Nutzen Sie Quell-VLAN in Verbindung mit dem Setup-Parameter *2.24.47*. Dadurch verhindern Sie, dass sich ein Public Spot-Benutzer in VLAN-getrennten Public Spot-Netzen/SSIDs nach einmaliger Authentisierung durch den RADIUS-Server an sämtlichen verwalteten Public Spot-Netzen/SSIDs anmelden kann.

Die SOURCE_VLAN ist nicht mit der VLAN_ID zu verwechseln. Die VLAN_ID wird nicht an den RADIUS-Server übermittelt, sondern vom Public Spot dazu genutzt, einem Benutzer nach erfolgreicher Authentifizierung eine vom Gateway vorgegebene VLAN-ID zuzuweisen.

PROVIDER (teilweise erforderlich)

Name des RADIUS-Servers, den der Public Spot für den Benutzer verwendet (Authentifizierung und Accounting). Wenn Sie keinen RADIUS-Server angeben, verwendet der Public Spot den für das Modul global konfigurierten Server.

Dieses XML-Element ist zwingend erforderlich, wenn Sie

- für das Public Spot-Modul mehrere RADIUS-Server konfiguriert haben.
- die XML-Schnittstelle ohne RADIUS-Authentifizierung, aber mit RADIUS-Accounting verwenden wollen.

In den übrigen Fällen ist die Angabe dieses XML-Elements optional.

Der referenzierte RADIUS-Server muss in der Konfiguration vorhanden sein.

TXRATELIMIT (optional)

Maximale Bandbreite (in KBit/s), die dem Public Spot-Benutzer im Uplink zur Verfügung steht.

RXRATELIMIT (optional)

Maximale Bandbreite (in KBit/s), die dem Public Spot-Benutzer im Downlink zur Verfügung steht.

SECONDSEXPIRE (optional)

Nutzungsdauer (die maximale Online-Zeit) für einen Benutzer-Account in Sekunden. Diese Nutzungsdauer kann der Benutzer bis zum Erreichen einer ggf. definierten relativen oder absoluten Ablaufzeit ausschöpfen.

Der Wert 0 schaltet die Überwachung der Nutzungsdauer aus.

TRAFFICEXPIRE (optional)

Maximales Datenvolumen für einen Benutzer-Account. Dieses Datenvolumen kann der Benutzer bis zum Erreichen einer ggf. definierten relativen oder absoluten Ablaufzeit ausschöpfen.

Die folgenden Angaben sind möglich:

- k oder K: Angabe in Kilobytes (kB), z. B. <TRAFFICEXPIRE>1000k</TRAFFICEXPIRE>.
- m oder M: Angabe in Megabytes (MB), z. B. <TRAFFICEXPIRE>100m</TRAFFICEXPIRE>.
- g oder G: Angabe in Gigabytes (GB), z. B. <TRAFFICEXPIRE>1g</TRAFFICEXPIRE>.

Ohne Einheit entspricht die Angabe einem Wert in Byte (B).

Der Wert 0 schaltet die Überwachung des Datenvolumens aus.

Das XML-Interface sendet dem Gateway daraufhin eine "Login"-Response, die die folgenden XML-Elemente enthalten kann:

SUB_USER_NAME

Benutzername

SUB_STATUS

Der aktuelle Benutzerstatus. Folgende Werte sind möglich:

- `RADIUS_LOGIN_ACCEPT`: Login erfolgreich
- `RADIUS_LOGIN_REJECT`: Login wird zurückgewiesen

`SUB_MAC_ADDR`

MAC-Adresse des Benutzer-Gerätes. Mögliche Formate sind:

- 00164115208c
- 00:16:41:15:20:8c
- 00-16-41-15-20-8c

`PROVIDER`

Name des RADIUS-Servers der für diesen Benutzer verwendet werden soll.

Im Folgenden finden Sie einige Beispiele für XML-Dateien:

Login-Request

Das externe Gateway sendet die Daten für den Start einer Sitzung an den Public Spot:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<PUBLICSPOTXMLINTERFACE>
  <ACCESS_CUBE COMMAND="RADIUS_LOGIN">
    <SUB_USER_NAME>user2350</SUB_USER_NAME>
    <SUB_PASSWORD>5juchb</SUB_PASSWORD>
    <SUB_MAC_ADDR>00164115208c</SUB_MAC_ADDR>
    <PROVIDER>DEFAULT</PROVIDER>
  </ACCESS_CUBE>
</PUBLICSPOTXMLINTERFACE>
```

Der Public Spot aktiviert den Benutzer 'user2350' in der internen Status-Tabelle.

Login-Response:

Das XML-Interface sendet eine Bestätigung über den Start einer Sitzung an das externe Gateway:

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
<PUBLICSPOTXMLINTERFACE>
 <ACCESS_CUBE ID="WLC_PM" IP="192.168.100.2" COMMAND="USER_STATUS">
    <SUB_STATUS>RADIUS_LOGIN_ACCEPT</SUB_STATUS>
    <SUB_MAC_ADDR>00:16:41:15:20:8b</SUB_MAC_ADDR>
    <SUB_USER_NAME>user2350</SUB_USER_NAME>
    <TXRATELIMIT>0</TXRATELIMIT>
    <RXRATELIMIT>0</RXRATELIMIT>
    <SECONDSEXPIRE>0</SECONDSEXPIRE>
    <TRAFFICEXPIRE>0</TRAFFICEXPIRE>
    <ACCOUNTCYCLE>0</ACCOUNTCYCLE>
    <IDLETIMEOUT>0</IDLETIMEOUT>
    </ACCESS_CUBE>
</PUBLICSPOTXMLINTERFACE>
```

15.5.4.2 CoA

Für die Anmeldung eines Public Spot-Benutzers ohne Änderungen während des Anmeldezeitraums genügt der Parameter `RADIUS_LOGIN`. Mittels `RADIUS_CoA` hingegen haben Sie die Möglichkeit, die für einen Public Spot-Benutzer geltenden Rahmenbedingungen auch während einer laufenden Sitzung zu verändern. Dazu sendet Ihr externes Hotspot-Gateway einen `RADIUS-CoA-Request` an den Public Spot, welcher die darin enthaltenen Änderungen direkt auf die **Stations-Tabelle** unter **Status** > **Public-Spot** überträgt.

Ein möglicher Anwendungsfall für CoA-Nachrichten ist z. B. die automatische Drosselung der Bandbreite: Hat ein Public Spot-Benutzer sein Volumenbudget verbraucht, kann ein externe Hotspot-Gateway diesen Benutzer drosseln, indem das Hotspot-Gateway nach Auswerten der Accounting-Daten eine entsprechende CoA-Nachricht an den Public Spot schickt

Die XML-Nachrichten für die Verhandlung zwischen Hotspot-Gateway und Public Spot sehen wie folgt aus:

RADIUS-CoA-Request

Das externe Gateway sendet die Daten für die Änderung einer Sitzung an den Public Spot. Der Public Spot ändert daraufhin die Sitzungsdaten des angemeldeten Benutzers 'user2350' in der Stations-Tabelle:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<PUBLICSPOTXMLINTERFACE>
  <ACCESS_CUBE COMMAND="RADIUS_COA_REQUEST">
    <SUB_USER_NAME>user2350</SUB_USER_NAME>
    <SUB_PASSWORD>5juchb</SUB_PASSWORD>
    <SUB_MAC_ADDR>00164115208c</SUB_MAC_ADDR>
    <TXRATELIMIT>100</TXRATELIMIT>
    <RXRATELIMIT>100</RXRATELIMIT>
    <SECONDSEXPIRE>3600</SECONDSEXPIRE>
    <TRAFFICEXPIRE>10000000</TRAFFICEXPIRE>
  </ACCESS_CUBE>
</PUBLICSPOTXMLINTERFACE>
```

Im obigen Beispiel werden dem Benutzer eine Sitzungsdauer von 3.600 Sekunden sowie ein übertragbares Datenvolumen von 10.000.000 Byte bei einer Sende- und Empfangsbandbreite von 100 kBit/s zugewiesen.

RADIUS-CoA-Response:

Das XML-Interface sendet eine Bestätigung über die Änderung der Sitzungsdaten an das externe Hotspot-Gateway:

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
<PUBLICSPOTXMLINTERFACE>
 <ACCESS_CUBE ID="WLC_PM" IP="192.168.100.2" COMMAND="USER_STATUS">
    <SUB_STATUS>RADIUS_COA_ACCEPT</SUB_STATUS>
    <SUB_MAC_ADDR>00:16:41:15:20:8b</SUB_MAC_ADDR>
    <SUB_USER_NAME>user2350</SUB_USER_NAME>
    <TXRATELIMIT>100</TXRATELIMIT>
    <RXRATELIMIT>100</RXRATELIMIT>
    <SECONDSEXPIRE>3600</SECONDSEXPIRE>
    <TRAFFICEXPIRE>10000000</TRAFFICEXPIRE>
    <ACCOUNTCYCLE>0</ACCOUNTCYCLE>
    <IDLETIMEOUT>0</IDLETIMEOUT>
    </ACCESS_CUBE>
</PUBLICSPOTXMLINTERFACE>
```

Im Falle des Drosselungsbeispiels betrifft die Änderung der Benutzersitzung immer das Kontingent, das dem Benutzer ab Änderungszeitpunkt noch zusteht. War der Benutzer z. B. bereits eine Stunde angemeldet, stehen ihm nach der Änderung des Zeitkontingents auf sechs Stunden anschließend noch fünf Stunden zur Verfügung. Fällt das zugewiesene Zeitkontingent dagegen geringer aus als der Benutzer bereits angemeldet ist, loggt der Public Spot den betreffenden Nutzer aus und sendet eine Logout-Nachricht an das Hotspot-Gateway.

15.5.4.3 Logout

Sendet das externe Gateway in einer XML-Datei einen "Logout"-Request, sperrt der Public Spot den Online-Zugriff für den entsprechenden Benutzer. Ein "Logout"-Request enthält das Attribut `COMMAND="RADIUS_LOGOUT"`.

Das XML-Interface kann die folgenden XML-Elemente einer Anfrage verarbeiten:

`SUB_USER_NAME`

Benutzername

Bekommt das Gerät diesen Request und stellt das Public Spot-Modul fest, dass dieser User mit den passenden MAC online ist, loggt der Public Spot diesen aus.

`SUB_MAC_ADDR`

MAC-Adresse des Benutzer-Gerätes. Mögliche Formate sind:

- 00164115208c
- 00:16:41:15:20:8c

- 00-16-41-15-20-8c

TERMINATION_CAUSE

Grund für das Abmelden des Benutzers

Das XML-Interface sendet dem Gateway daraufhin eine "Logout"-Response, die die folgenden XML-Elemente enthalten kann:

SUB_USER_NAME

Benutzername

SUB_STATUS

Der aktuelle Benutzerstatus. Folgende Werte sind möglich:

- `RADIUS_LOGOUT_DONE`: Logout erfolgreich
- `RADIUS_LOGOUT_REJECT`: Logout wird zurückgewiesen

SUB_MAC_ADDR

MAC-Adresse des Benutzer-Gerätes. Mögliche Formate sind:

- 00164115208c
- 00:16:41:15:20:8c
- 00-16-41-15-20-8c

TERMINATION_CAUSE

Grund für die Sperrung des Zugangs

Im Folgenden finden Sie einige Beispiele für XML-Dateien:

Logout-Request

Das externe Gateway sendet den Befehl für die Beendigung einer Sitzung an den Public Spot:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<PUBLICSPOTXMLINTERFACE>
  <ACCESS_CUBE COMMAND="RADIUS_LOGOUT">
    <SUB_USER_NAME>user2350</SUB_USER_NAME>
    <SUB_MAC_ADDR>00164115208c</SUB_MAC_ADDR>
    <TERMINATION_CAUSE>Check-Out</TERMINATION_CAUSE>
  </ACCESS_CUBE>
</PUBLICSPOTXMLINTERFACE>
```

Logout-Response:

Das XML-Interface sendet eine Bestätigung über den Stopp einer Sitzung an das externe Gateway:

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
<PUBLICSPOTXMLINTERFACE>
   <ACCESS_CUBE ID="WLC_PM" IP="192.168.100.2" COMMAND="USER_STATUS">
     <SUB_STATUS>RADIUS_LOGOUT_DONE</SUB_STATUS>
     <SUB_MAC_ADDR>00:16:41:15:20:8b</SUB_MAC_ADDR>
     <SUB_USER_NAME>user2350</SUB_USER_NAME>
     <TERMINATION_CAUSE>User logout request</TERMINATION_CAUSE>
    </ACCESS_CUBE>
</PUBLICSPOTXMLINTERFACE>
```

15.5.4.4 Status

Mit einem "Status"-Request erfragt das externe Gateway beim Public Spot den aktuellen Status eines Benutzers. Ein "Status"-Request enthält das Attribut `COMMAND="RADIUS_Status"`.

Das XML-Interface kann die folgenden XML-Elemente einer Anfrage verarbeiten:

`SUB_USER_NAME`

Benutzername

`SUB_MAC_ADDR`

MAC-Adresse des Benutzer-Gerätes. Mögliche Formate sind:

- 00164115208c
- 00:16:41:15:20:8c
- 00-16-41-15-20-8c

Das XML-Interface sendet dem Gateway daraufhin eine "Status"-Response, die die folgenden XML-Elemente enthalten kann:

`SUB_USER_NAME`

Benutzername

`SUB_MAC_ADDR`

MAC-Adresse des Benutzer-Gerätes. Mögliche Formate sind:

- 00164115208c
- 00:16:41:15:20:8c
- 00-16-41-15-20-8c

`SUB_STATUS`

Der aktuelle Benutzerstatus. Folgende Werte sind möglich:

- `RADIUS_STATUS_DONE`: Status Anfrage erfolgreich
- `RADIUS_STATUS_REJECT`: Status Anfrage zurückgewiesen, z. B. unbekannter User oder MAC Adresse

`SESSION_TXBYTES`

Aktuell gesendete Datenmenge

`SESSION_RXBYTES`

Aktuell empfangene Datenmenge

`SESSION_TXPACKETS`

Anzahl der bisher gesendeten Datenpakete

`SESSION_RXPACKETS`

Anzahl der bisher empfangenen Datenpakete

`SESSION_STATE`

Aktueller Status der Sitzung

SESSION_ACTUAL_TIME

Aktuelle Uhrzeit

Im Folgenden finden Sie einige Beispiele für XML-Dateien:

Status-Request

Das externe Gateway sendet den Befehl für die Statusabfrage an den Public Spot:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<PUBLICSPOTXMLINTERFACE>
  <ACCESS_CUBE COMMAND="RADIUS_STATUS">
    <SUB_USER_NAME>user2350</SUB_USER_NAME>
    <SUB_MAC_ADDR>00164115208c</SUB_MAC_ADDR>
  </ACCESS_CUBE>
</PUBLICSPOTXMLINTERFACE>
```

Status-Response:

Das XML-Interface sendet eine Statusmeldung an das externe Gateway:

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
<PUBLICSPOTXMLINTERFACE>
   <ACCESS_CUBE ID="WLC_PM" IP="192.168.100.2" COMMAND="USER_STATUS">
     <SUB_STATUS>RADIUS_STATUS_DONE</SUB_STATUS>
     <SUB_MAC_ADDR>00:16:41:15:20:8b</SUB_MAC_ADDR>
     <SUB_USER_NAME>user2350</SUB_USER_NAME>
     <SESSION_ID>2</SESSION_ID>
     <SESSION_TXBYTES>0</SESSION_TXBYTES>
     <SESSION_RXBYTES>0</SESSION_RXBYTES>
     <SESSION_TXPACKETS>0</SESSION_TXPACKETS>
     <SESSION_RXPACKETS>0</SESSION_RXPACKETS>
     <SESSION_STATE>Authenticated</SESSION_STATE>
     <SESSION_ACTUAL_TIME>0</SESSION_ACTUAL_TIME>
   </ACCESS_CUBE>
</PUBLICSPOTXMLINTERFACE>
```

15.6 Anhang

15.6.1 Allgemein übermittelte RADIUS-Attribute

Das RADIUS-Client-Modul wurde auf Basis der RFCs Nr. 2865 und Nr. 2866 implementiert.

Diese Spezifikationen definieren sogenannte Attribute, die teilweise zwingend implementiert werden müssen, teilweise aber auch optional sind. Die folgenden Übersichtsseiten zeigt, welche Attribute bei welchen Meldungen zwischen RADIUS-Server und Ihrem Gerät übertragen bzw. ausgewertet werden.

15.6.1.1 Meldungen an den und vom Authentifizierungs-Server

Übertragene Attribute

Wie bereits erwähnt, übermittelt Ihr Gerät in einer RADIUS-Anfrage weit mehr als ausschließlich Benutzername und -kennwort. RADIUS-Server können diese zusätzlichen Informationen komplett ignorieren oder lediglich eine Teilmenge davon verarbeiten. Viele dieser Attribute werden auch für den Serverzugang über Dial-in verwendet und sind in den RADIUS RFCs als Standard-Attribute definiert. Einige für den Hotspot-Betrieb wichtige Informationen lassen sich jedoch

nicht mit den Standard-Attributen abbilden. Diese zusätzlichen Attribute werden als herstellerspezifisch mit der Herstellerkennung 2356 (LANCOM Systems GmbH) verwendet.

Tabelle 42: Übersicht der vom Gerät an den Authentifizierungs-Server übertragenen RADIUS-Attribute

ID	Bezeichnung	Bedeutung	Mögliche Werte in LCOS
1	User-Name	Der vom Benutzer eingegebene Name.	
2	User-Password	Das vom Benutzer eingegebene Passwort.	
4	NAS-IP-Address	IP-Adresse Ihres Gerätes.	<IPv4-Adresse des Gerätes>
6	Service-Type	Art des Dienstes, den der Benutzer angefragt hat. Der Wert „1“ steht dabei für Login.	
8	Framed-IP-Address	Gibt die dem Client zugewiesene IP-Adresse an.	<IP-Adresse des Clients>
30	Called-Station-Id	MAC-Adresse Ihres Gerätes.	<nn:nn:nn:nn:nn:nn>
31	Calling-Station-Id	MAC-Adresse des Clients. Die Ausgabe erfolgt byte-weise in hexadezimaler Schreibweise mit Trennzeichen.	<nn:nn:nn:nn:nn:nn>
32	NAS-Identifier	Name Ihres Gerätes, sofern konfiguriert.	<Geräte-Name>
61	NAS-Port-Type	Art des physikalischen Ports, über den ein Benutzer eine Authentifizierung angefragt hat.	› **Id 19** kennzeichnet Clients aus dem WLAN. › **Id 15** kennzeichnet Clients aus dem Ethernet.
87	NAS-Port-Id	Bezeichnung des Interfaces, über welches ein Client mit Ihrem Gerät verbunden ist. Dies kann sowohl eine physische als auch logische Schnittstelle sein. Bedenken Sie, dass mehr als nur ein Client über ein Interface verbunden sein kann; die Port-Nummer verweist also im Gegensatz zu Dial-in-Servern nicht eindeutig auf einen Client.	z. B. › LAN-1 › WLAN-1-5 › WLC-TUNNEL-27

Ausgewertete Attribute

Ihr Gerät untersucht die Authentifizierungs-Antwort eines RADIUS-Servers auf Attribute, die es eventuell weiterverarbeiten kann. Die meisten Attribute haben allerdings nur dann eine Bedeutung, wenn die Antwort positiv war, sodass sie die anschließende Sitzung beeinflussen.

Tabelle 43: Übersicht aller unterstützten RADIUS-Attribute

ID	Bezeichnung	Bedeutung	Mögliche Werte in LCOS
18	Reply-Message	Eine beliebige Zeichenfolge des RADIUS-Servers, die entweder ein gescheitertes Anmelden oder eine Willkommensnachricht beinhaltet. Diese Nachricht lässt sich über das `SERVERMSG`-Element in eine benutzerdefinierte Start- oder Fehlerseite integrieren.	
25	Class	Ein beliebiges Oktett oder Achtbitzeichen, das die Daten vom Authentifizerungs- / Accounting-Backend enthält. Jedes Mal, wenn das Gerät eine RADIUS-Accounting-Anfrage stellt, wird dieses Attribut unverändert gesendet. Innerhalb einer Authentifizierungs-Antwort kann dieses Attribut mehrmals vorkommen, um z. B. eine Zeichenfolge zu übertragen, die länger als 255 Bytes ist. Das Gerät behandelt alle Vorkommen dieses Attributes in Accounting-Anfragen in der Reihenfolge, in der sie in der Authentifizierungs-Antwort aufgetreten sind.	

ID	Bezeichnung	Bedeutung	Mögliche Werte in LCOS
26	Vendor 2356, Id 1 LCS-Traffic-Limit	Definiert eine Datenmenge in Bytes, nach der das Gerät die Sitzung automatisch beendet. Dieser Wert ist nützlich, um Volumen-limitierte Benutzerkonten zu erstellen. Wenn dieses Attribut in der Authentifizierungs-Antwort fehlt, wird kein Volumen-Limit angenommen. Ein Datenlimit von 0 wird als ein Benutzerkonto interpretiert, das zwar grundsätzlich gültig ist, aber sein Datenvolumen aufgebraucht hat. In diesem Fall startet das Gerät keine Sitzung.	
26	Vendor 2356, Id 3 LCS-Redirection-URL	Kann eine beliebige URL enthalten, die als zusätzlicher Link auf der Startseite angeboten wird. Dies kann die Startseite des Benutzers sein oder eine Seite mit zusätzlichen Informationen zum Benutzerkonto.	
26	Vendor 2356, Id 5 LCS-Account-End	Definiert einen absoluten Zeitpunkt (gemessen in Sekunden seit dem 1. Januar 1970 0:00:00), nach dem der Account ungültig wird. Wenn dieses Attribut in der Authentifizierungs-Antwort fehlt, wird kein Datumslimit angenommen. Das Gerät startet keine Sitzung, wenn die interne Systemuhr nicht eingestellt ist oder der angegebene Zeitpunkt in der Vergangenheit liegt.	
26	Vendor 2356, Id 7 LCS-Public-Spot-Username	Enthält den Namen eines Public Spot-Benutzers für den Auto-Login. Der Auto-Login bezieht sich dabei auf die Tabelle der MAC-authentifizierten Benutzer, denen der Server automatisch einen Benutzernamen zuweist.	
26	Vendor 2356, Id 8 LCS-TxRateLimit	Definiert eine maximale Downstream-Rate in kbps. Diese Beschränkung lässt sich mit der dazugehörigen Public Spot-Funktion kombinieren.	
26	Vendor 2356, Id 9 LCS-RxRateLimit	Definiert eine maximale Upstream-Rate in kbps. Diese Beschränkung lässt sich mit der dazugehörigen Public Spot-Funktion kombinieren.	
26	Vendor 2356, Id 13 LCS-Advertisement-URL	Definiert eine kommaseparierte Liste von Werbe-URLs.	
26	Vendor 2356, Id 14 LCS-Advertisement-Interval	Definiert das Intervall in Minuten, nach dem der Public Spot einen Benutzer an eine Werbe-URL umleitet. Bei einem Intervall von 0 erfolgt die Umleitung direkt nach der Anmeldung.	
27	Session-Timeout	Definiert eine optionale Maximal-Dauer für die Sitzung in Sekunden. Wenn dieses Attribut in der Authentifizierungs-Antwort fehlt, wird kein Zeitlimit angenommen. Ein Zeitlimit von 0 wird als ein Benutzerkonto interpretiert, das zwar grundsätzlich gültig ist, aber seine verfügbare Zeit aufgebraucht hat. In diesem Fall startet das Gerät keine Sitzung.	
28	Idle-Timeout	Definiert einen Zeitraum in Sekunden, nach dem das Gerät die Sitzung beendet, wenn es keine Pakete vom Client mehr empfängt. Dieser Wert überschreibt möglichweise eine unter **Public-Spot** > **Server** > **Leerlaufzeitüberschreitung** lokal definierte Leerlauf-Zeitüberschreitung.	
64	Tunnel-Type	Definiert das Tunneling-Protokoll, welches für die Sitzung verwendet wird.	
65	Tunnel-Medium-Type	Definiert das Transportmedium, über das eine getunnelte Sitzung hergestellt wird.	
81	Tunnel-Private-Group-ID	Definiert die Gruppen-ID, falls die Sitzung getunnelt ist.	

ID	Bezeichnung	Bedeutung	Mögliche Werte in LCOS
85	Acct-Interim-Interval	Definiert die Zeit zwischen aufeinander folgenden RADIUS-Accounting-Aktualisierungen. Dieser Wert wird nur dann ausgewertet, wenn auf dem RADIUS-Client lokal kein eigenes Accounting-Intervall festgelegt ist, Sie für das Public Spot-Modul also keinen **Update-Zyklus** festgelegt haben.	

Beachten Sie, dass sich die Attribute für LCS-Account-Ende und Session-Zeitüberschreitung gegenseitig ausschließen und daher beide Attribute nicht in einer Antwort auftreten sollten. Sollten dennoch beide Attribute auftreten, wertet das Gerät das zuletzt auftretende Attribut aus.

15.6.1.2 Meldungen an/vom Accounting-Server

Übertragene Attribute

Der Satz von RADIUS-Attributen der einem RADIUS-Server in einer Accounting-Anfrage übergeben wird ähnelt einer Authentifizierungs-Anfrage. Dennoch werden einige spezifische Accounting-Attribute hinzugefügt. Die folgenden Attribute sind in allen RADIUS-Accounting-Anfragen vorhanden:

Übersicht der vom Gerät an den Accounting-Server übertragenen RADIUS-Attribute

1

User-Name

Name des Benutzerkontos, dass zur Authentifizierung verwendet wurde.

4

NAS-IP-Address

IP-Adresse Ihres Gerätes.

8

Framed-IP-Address

IP-Adresse, die dem Client zugewiesen wurde.

25

Class

Alle Class-Attribut-Werte, die der RADIUS-Authentifizierungs-Server in seiner Antwort geliefert hat.

30

Called-Station-Id

MAC-Adresse Ihres Gerätes

31

Calling-Station-Id

MAC-Adresse des Clients. Die Ausgabe erfolgt byte-weise in hexadezimaler Schreibweise mit Trennzeichen (nn:nn:nn:nn:nn:nn).

32

NAS-Identifier

Name Ihres Gerätes, sofern konfiguriert.

40

Acct-Status-Type

Anfragetyp, welcher den Start oder den Stop des Accountings, oder ein Interim-Update signalisiert. Weitere Erläuterungen finden Sie im Kapitel *Anfragetypen*.

44

Acct-Session-Id

Eine Zeichenfolge, die den Client eindeutig identifiziert. Sie besteht aus der MAC-Adresse des Netzwerkadapters, dem Zeitpunkt der Anmeldung (gemessen in Sekunden seit dem 1. Januar 1970 0:00:00) und der Sitzungszähler, den Ihr Gerät lokal verwaltet.

61

NAS-Port-Type

Art des physikalischen Ports, über den ein Benutzer eine Authentifizierung angefragt hat.

- **Id 19** kennzeichnet Clients aus dem WLAN
- **Id 15** kennzeichnet Clients aus dem Ethernet

87

NAS-Port-Id

Bezeichnung des Interfaces, über welches ein Client mit Ihrem Gerät verbunden ist. Dies kann sowohl eine physische als auch logische Schnittstelle sein, wie z. B. `LAN-1`, `WLAN-1-5` oder `WLC-TUNNEL-27`.

Bedenken Sie, dass mehr als nur ein Client über ein Interface verbunden sein kann; die Port-Nummer also im Gegensatz zu Dial-in-Servern nicht eindeutig auf einen Client verweist.

Im Falle einer Accounting-Stop-Anfrage oder eines Interim-Updates beinhaltet die Anfrage zusätzlich folgendes Attribute:

42

Acct-Input-Octets

Die Summe aller vom Client empfangenen Daten-Bytes in dieser Sitzung, Modulo 2^{32}.

43

Acct-Output-Octets

Die Summe aller zum Client gesendeten Daten-Bytes in dieser Sitzung, Modulo 2^{32}.

46

Acct-Session-Time

Die Gesamtdauer der Sitzung des Clients in Sekunden.

Wurde die Sitzung wegen einer Leerlauf-Zeitüberschreitung beendet, reduziert sich dieser Wert um die Leerlaufzeit.

47

Acct-Input-Packets

Die Anzahl der Datenpakete, die Ihr Gerät während der Sitzung vom Client empfangen hat.

48

Acct-Output-Packets

Die Anzahl der Datenpakete, die Ihr Gerät während der Sitzung zum Client gesendet hat.

49

Acct-Terminate-Cause

Der Grund für den Abbruch oder das Ende der Accounting-Sitzung. Wird gesendet, wenn das der **Acct-Status-Type** den Wert `Start` oder `Stop` besitzt.

52

Acct-Input-Gigawords

Die oberen 32 Bits der Summe aller vom Client empfangenen Daten-Bytes während dieser Sitzung.

53

Acct-Output-Gigawords

Die oberen 32 Bits der Summe aller zum Client gesendeten Daten-Bytes während dieser Sitzung.

55

Event-Timestamp

Der Zeitpunkt, an dem diese Accounting-Anfrage gestartet wurde (gemessen in Sekunden seit dem 1. Januar 1970 0:00:00). Dieses Attribut ist nur dann vorhanden, wenn die Systemuhr Ihres Gerätes eine gültige Zeit aufweist.

Beachten Sie, dass das RADIUS-Accounting erst nach der erfolgreichen Anmeldung eines Clients mit der Abrechnung beginnt; also die für die Authentifizierung benötigte Zeit nicht aufgezeichnet wird. Über die *Traffic-Limit-Option* können Sie den Datenverkehr während der Authentifizierungsphase einschränken. Die finale Accounting-Stop-Anfrage enthält natürlich ebenso das Termination-Cause-Attribute (49). Eine Übersicht der dieser Attribute finden Sie im LANCOM "Public Spot: Implementation Guide", erhältlich unter *www.lancom-systems.de*.

Ausgewertete Attribute

Ihr Gerät wertet die Antworten von RADIUS-Accounting-Servern derzeit nicht aus.

15.6.2 Durch WISPr übermittelte RADIUS-Attribute

Wenn Sie WISPr aktivieren und einen externen RADIUS-Server verwenden, übermittelt der Public Spot die Attribute (Access-Request):

- **Location-ID**
- **Location-Name**
- **Logoff-URL**

Bei diesen Attributen handelt es sich um einen Auszug der vorangegangenen Abschnitt konfigurierten Werte. Über sie kann ein Provider oder Roaming-Broker den Ort des Clients zu Abrechnungszwecken identifizieren. Es werden Vendor Specific Attributes (VSA) mit der IANA Private Enterprise Number (PEN) 14122 verwendet.

Von einem externen RADIUS-Server verarbeitet der Public Spot die Attribute (Access-Accept):

- **Redirection-URL**: URL, zu der ein Client nach der Anmeldung weitergeleitet werden soll. Diese Funktion wird nicht von allen Smart-Clients unterstützt.
- **Bandwidth-Max-Up**: Maximale Bandbreite der Upload-Geschwindigkeit, die der Client erhalten soll.
- **Bandwidth-Max-Down**: Maximale Bandbreite der Download-Geschwindigkeit die der Client erhalten soll.
- **Session-Terminate-Time**: Zeitpunkt, zu dem der Client automatisch de-authentifiziert werden soll. Dieses Attribut besitzt nach ISO 8601 das Format `YYYY-MM-DDThh:mm:ssTZD`. Falls TZD nicht angegeben wird, wird der Client nach Ortszeit des Public Spots de-authentifiziert.
- **Session-Terminate-End-Of-Day**: Der Wert dieses Attributs kann entweder 0 oder 1 sein. Er gibt an, ob der Client am Ende des Abrechnungstages vom Public Spot de-authentifiziert werden soll.

Für das Accounting verwendet der Public Spot die Attribute:

- **Location-ID**
- **Location-Name**

16 Voice over IP – VoIP

16.1 Einleitung

Voice-over-IP (VoIP) steht für Sprachkommunikation in Computernetzwerken auf Basis des Internet Protokolls (IP). Die Kernidee ist, Funktionen der klassischen Telefonie über kostengünstige und weit verbreitete Netzwerkstrukturen wie z. B. das Internet bereit zu stellen. VoIP selbst ist dabei kein Standard, sondern nur ein Sammelbegriff für verschiedene Technologien (Endgeräte, Protokolle, Sprachkodierung usw.), die Sprachkommunikation in IP-Netzwerken ermöglichen.

Im allgemeinen Sprachgebrauch verwendet man für das Telefonieren über ein Netzwerk (LAN oder Internet) verschiedene Begriffe. Die Begriffe "Voice over IP" oder "IP-Telefonie" werden gleichwertig verwendet, obwohl sie im eigentlichen Sinn unterschiedliche Bedeutungen haben.

- Genauer betrachtet ist "Voice over IP" lediglich ein Begriff für die Technologie der Echtzeit-Gesprächsübertragung über Datennetze unter Verwendung des IP-Protokolls (Internet-Protokoll). Der Begriff wird auch verwendet, wenn die Technik nur in den Kernnetzen der Provider – im sogenannten Backbone – eingesetzt wird.
- Der Begriff "IP-Telefonie" wird verwendet, wenn die VoIP-Technik auch im Endgerät eingesetzt wird, so dass der Gesprächsteilnehmer selbst das IP-Netz zum Telefonieren nutzt.
- Unter "Internet-Telefonie" wird allgemein das Telefonieren mittels VoIP über das Internet bezeichnet.

Im Folgenden wird dem allgemeinen Sprachgebrauch folgend meistens von "Voice over IP" gesprochen, auch wenn IP-Telefonie gemeint ist.

Es gibt vier grundsätzliche Arten von Endgeräten, mit denen man die VoIP-Telefonie nutzen kann:

- Mit einer auf dem PC laufenden Software, einem sogenannten "Softphone".
- Mit einem direkt an das lokale Netz angeschlossenen IP- bzw. VoIP-Telefon.
- Mit einem herkömmlichen Telefon, das über ein Adaptergerät (analoger Telefon-Adapter, ATA) an das lokale Netz angeschlossen wird.
- Über ein VoIP-Gateway, das Telefongespräche von Telefonen (analog und ISDN) auf VoIP umsetzt und dann zwischen den beiden "Telefonwelten" wie eine TK-Anlage vermitteln kann.

Grundsätzlich unterschiedet man dabei, ob eine VoIP-Verbindung zwischen zwei direkt über das Datennetz verbundenen Endgeräten (also PC oder ein IP-Telefon) aufgebaut wird, oder ob ein Teilnehmer im Fest- oder Mobilfunknetz eine Umsetzung der Signalisierung, der Rufnummern und der Sprachdaten erfordert. Zur Unterscheidung der verschiedenen Verbindungsvarianten haben sich die Begriffe "PC" für ein Gerät im LAN und "Phone" für ein Gerät im Festnetz eingebürgert.

PC-to-PC Kommunikation

Bei dieser Anwendung muss das Endgerät direkt in das LAN des Benutzers integriert werden. Beispiele sind ein PC, ein IP-Telefon oder ein Telefon, dass über ein ATA an das LAN angeschlossen ist.

Für den PC stehen verschiedene Softwarelösungen zur Verfügung, die als „Softphone“ bezeichnet werden. Dabei ist zu beachten, dass einige dieser Programme nur mit Anwendern der gleichen Software kommunizieren können und nicht mit Softphones von anderen Herstellern. Die Kommunikation ist meist kostenlos innerhalb des Internets. Ein gängiges Beispiel ist Skype, das ein eigenes Protokoll verwendet.

PC-to-Phone und Phone-to-PC Kommunikation

In diesem Fall müssen die Gesprächsdaten vom Internet auf das Festnetz übertragen werden, in der Regel mit Hilfe so genannter VoIP-Gateways. Diese Gateways werden im Allgemeinen von Providern zur Verfügung gestellt und sind gebührenpflichtig.

Um selbst an einem PC angerufen werden zu können, benötigt der Teilnehmer eine VoIP-Telefonnummer, die in der Regel ebenfalls von einem Provider bereitgestellt wird.

VoIP-Provider stellen üblicherweise nur einzelne Rufnummern bereit und keine kompletten Rufnummernkreise mit Stammnummer und Durchwahlen. Daher sind die von öffentlichen Providern bereitgestellten Rufnummern für viele Business-Kunden nicht attraktiv. Beim Einsatz der LANCOM VoIP Router mit SIP-Gateway können die bisher verwendeten Rufnummern weiter verwendet werden, die Funktionen der VoIP-Telefonie können zusätzlich genutzt werden.

16.2 VoIP-Implementation im LANCOM VoIP Router

Kernfunktion der VoIP-Implementierung im LANCOM VoIP Router ist die Vermittlung von Telefongesprächen von verschiedenen lokalen Schnittstellen (LAN, WLAN, ISDN) auf die von dem Router erreichbaren WAN Verbindungen. Dabei wird sowohl die Vermittlung zwischen den lokalen Schnittstellen untereinander (lokales Gespräch) ermöglicht, als auch die Vermittlung zwischen WAN Schnittstellen.

Grundlage für die Implementierung und Vermittlung ist dabei das SIP-Protokoll. Die Gespräche aller Schnittstellen werden über Interface-Umsetzer auf SIP umgewandelt (im Wesentlichen betrifft das die ISDN-Schnittstellen).

Darüber hinaus wird die bittransparente Verbindung grundsätzlich bei Gesprächen zwischen mehreren lokalen ISDN Schnittstellen verwendet, um höchstmögliche Kompatibilität und Qualität zu erreichen.

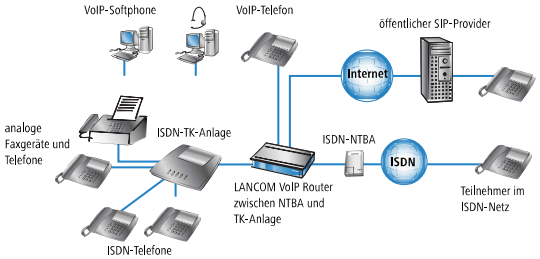
16.2.1 Anwendungsbeispiele

Voice-over-IP-Lösungen bringen ihre Vorteile in einem sehr breiten Anwendungsspektrum ein, angefangen von kleinen Unternehmen bis hin zu großen Konzernen mit ausgedehntem Filialbetrieb. In diesem Abschnitt stellen wir einige Beispiele vor.

Konkrete Hinweise zur Konfiguration finden Sie im Kapitel 'Konfiguration der VoIP-Funktionen'.

16.2.1.1 Ergänzung bestehender ISDN-TK-Anlagen

Bestehende Telefonstrukturen können durch den Einsatz eines LANCOM VoIP Router sehr komfortabel um VoIP-Funktionen erweitert werden. Der LANCOM VoIP Router wird dabei einfach zwischen den öffentlichen ISDN-Anschluss (z. B. ISDN-NTBA) und die ISDN-TK-Anlage geschaltet.



Über die TK-Anlage und die angeschlossenen ISDN-Telefone sind weiterhin alle Gespräche wie zuvor möglich, auch die Erreichbarkeit unter den bekannten Telefonnummern bleibt erhalten. Zusätzlich bietet diese Anwendung folgende Möglichkeiten:

- Zu den bisher verwendeten ISDN-Telefonen können auch VoIP-Telefone oder VoIP-Softphones in die Telefonstruktur aufgenommen werden. Die VoIP-Teilnehmer im eigenen LAN können auch die externen Teilnehmer im ISDN-Netz erreichen.

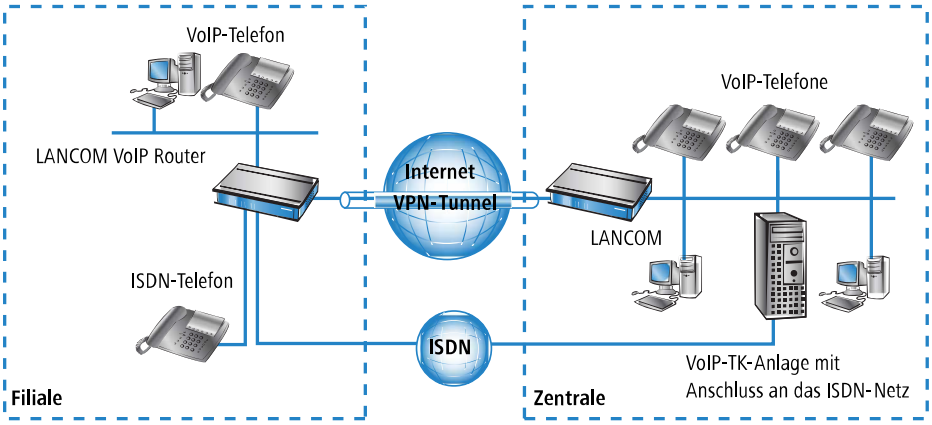
- Die ISDN-Telefone lassen sich weiterhin verwenden, können aber zusätzlich die internen VoIP-Telefone sowie VoIP-Softphones im LAN erreichen.
- Gespräche mit externen SIP-Teilnehmern im Netz des eigenen Internetproviders können bei vielen Anbietern kostenlos geführt werden.
- Mit der Verbindung zu einem öffentlichen SIP-Provider können auch alle anderen SIP-Teilnehmer weltweit in anderen Provider-Netzen erreicht werden. Alternativ zur direkten ISDN-Verbindung lassen sich Teilnehmer im ISDN-Netz auch über den Umweg eines SIP-Providers erreichen. Die Gebühren richten sich nach den Tarifen der jeweiligen Anbieter. Für Fern- und Auslandsgespräche ist in vielen Fällen die Nutzung des SIP-Providers deutlich günstiger als die klassische Telefonverbindung.

Der LANCOM VoIP Router übernimmt in diesem Aufbau die Vermittlung der Gespräche. Aufgrund der individuellen Konfiguration des Gerätes kann z. B. anhand bestimmter Vorwahlbereiche entschieden werden, ob ein Telefonanruf über die ISDN-Schnittstelle oder als VoIP-Gespräch über das Internet erfolgen soll.

16.2.1.2 Anbindung von Filialen oder Heimarbeitsplätzen an die Zentrale

Viele Filialen oder Heimarbeitsplätze sind schon über VPN an das Netz der Zentrale angebunden. Allerdings beschränkt sich die Anbindung in vielen Fällen nur auf die Datenübertragung. Mit dem Einsatz von VoIP können die firmeninternen Gespräche über die ohnehin vorhandene VPN-Verbindung kostenlos und – dank der VPN-Verschlüsselung – abhörsicher geführt werden.

Mit dem Einsatz eines LANCOM VoIP Router in der Filiale bzw. am Heimarbeitsplatz erschließen sich die klassische Telefonwelt über ISDN und VoIP-Telefonie mit nur einem einzigen Telefon: als Endgerät kann ein vorhandenes ISDN-Telefon oder ein VoIP-Telefon verwendet werden, um eine gebührenfreie Telefon-Verbindung per VPN zur Zentrale oder auch eine gewöhnliche Verbindung per ISDN aufzunehmen.



Die Vorteile der Telefon-Anbindung an die Zentrale:

- Die komplette Konfiguration der Telefonfunktionen kann an einer Stelle in der VoIP-TK-Anlage der Zentrale vorgenommen werden.
- Die Teilnehmer aus den Heimbüros oder den Filialen melden sich an der zentralen TK-Anlage an.
- Gespräche innerhalb des Firmennetzwerks werden kostenlos geführt.
- Bei den ausgehenden Gesprächen kann je nach Verbindungs- oder Kostensituation automatisch entschieden werden, welche Leitung genutzt werden soll.

16.2.1.3 VoIP für Unternehmen mit SIP-Trunking

Eine der größten Hürden für einen vollständigen Umstieg von Unternehmen auf VoIP-Lösungen stellt die Beibehaltung der verwendeten Rufnummern dar. Die üblichen SIP-Accounts bei den entsprechenden Providern bieten zwar teilweise Rufnummern für den Übergang in das Telefon-Festnetz an, dabei handelt es sich in der Regel aber um einzelne Rufnummern aus einem "Pool" des Providers. Für Unternehmen mit einer größeren Anzahl an Telefonteilnehmern und Rufnummern ist aber die Übernahme der bisherigen Rufnummern und die "Durchwahlfähigkeit" ein entscheidendes Kriterium bei der Migration zu VoIP.

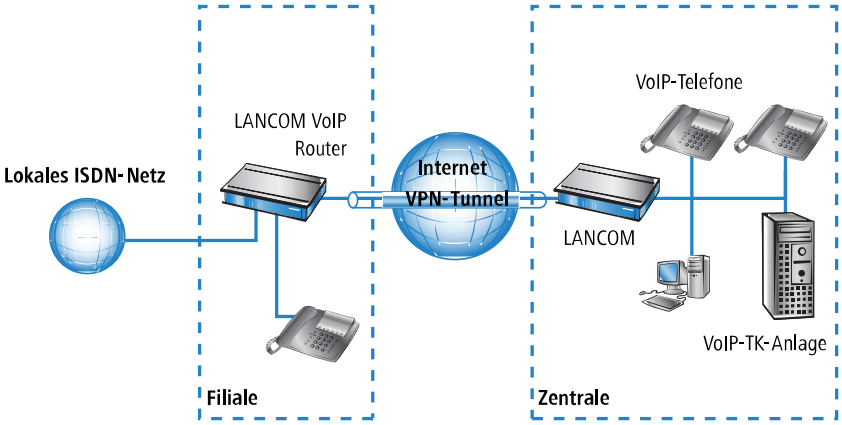
Mit der Funktion SIP-Trunking können LANCOM VoIP Router komplette Rufnummernbereiche aus Stammnummern und zugehörigen Durchwahlen auf eine einzige Verbindung zu einem SIP-Provider abbilden, wenn dieser ebenfalls das Direct Dialing In (DDI) unterstützt und mehrere gleichzeitige Verbindungen anbietet. Die SIP-Provider bieten mit dem SIP-Trunking üblicherweise auch die Übernahme der verwendeten Rufnummern vom bisherigen Telefonanbieter an.

16.2.1.4 Einbindung lokaler ISDN-Anschlüsse mit Remote-SIP-Gateway

Die Netzwerke an national oder international verteilten Unternehmens-Standorten sind oft schon über VPN verbunden. Mit einem LANCOM VoIP Router können nicht nur die SIP- und ISDN-Telefone einer Filiale an die SIP-TK-Anlage der Zentrale angebunden werden, der Übergang zum lokalen ISDN-Netz kann mit der Funktion "SIP-Gateway" in die Unternehmenskommunikation eingebunden werden.

Das SIP-Gateway ist für abgehende und ankommende Rufe aktiv:

- Eine Zentrale in Hamburg kann z. B. einen LANCOM VoIP Router mit SIP-Gateway in der Filiale in München nutzen, um Gespräche mit den Kunden und Lieferanten im Ortsbereich München zu den Gebühren für Ortsgespräche zu führen ("local break out").
- Um für die Kunden in einem anderen Land besser erreichbar zu sein, kann die Zentrale in Hamburg z. B. einen LANCOM VoIP Router mit SIP-Gateway am Vertriebsstandort in Italien nutzen. Die Kunden können den Support oder Service dann über eine entsprechende nationale Service-Rufnummer erreichen. Die Rufe werden aus dem lokalen ISDN-Netz angenommen und im Netz des Unternehmens an einen freien oder zuständigen Mitarbeiter zugestellt. Über das Call-Routing können dabei z. B. anhand der Rufnummer des Kunden bestimmte Anschlüsse für die Weiterleitung ausgewählt werden.

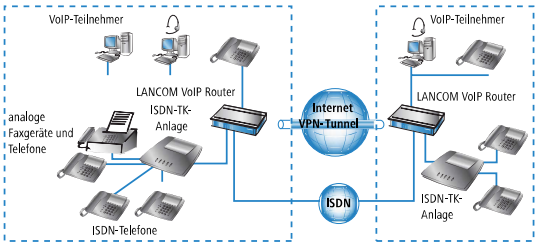


Die Vorteile des SIP-Gateways:

- Der lokale ISDN-Anschluss an einem bestimmten Standort steht allen Standorten im gesamten Unternehmen zur Verfügung.
- Nationale und internationale Ferngespräche können auf Ortsgespräche oder regionale Gespräche abgebildet werden und so Kosten einsparen.
- Automatisches Routing von eingehenden Rufen zu zuständigen Mitarbeitern.

16.2.1.5 Verbindung von Standorten ohne SIP-TK-Anlage

Auch verteilte Unternehmen ohne eigene SIP-TK-Anlage können die Vorteile der VoIP-Standortverbindung nutzen. In diesem "Peer-to-Peer"-Szenario werden an beiden Standorten LANCOM VoIP Router eingesetzt.



Neben der Datenübertragung über VPN können auch die VoIP-Funktionen zwischen den beiden Standorten genutzt werden.

Die Vorteile der Peer-to-Peer-Standortverbindung:

- ISDN-TK-Anlagen an verschiedenen Standorten lassen sich zu einem gemeinsamen internen Telefonnetz zusammenschalten.
- Keine SIP-TK-Anlage erforderlich.
- Gespräche innerhalb des Firmennetzwerks werden gebührenfrei geführt.
- Bei den ausgehenden Gesprächen kann je nach Verbindungs- oder Kostensituation automatisch entschieden werden, welche Leitung genutzt werden soll.
- Eingehende Gespräche können direkt an die entsprechenden Mitarbeiter eines anderen Standorts vermittelt werden.

16.2.2 Die zentrale Position der LANCOM VoIP Router

LANCOM VoIP Router nehmen eine zentrale Position bei der Vermittlung von Telefongesprächen zwischen internen und externen Gesprächsteilnehmern über verschiedene Kommunikationswege ein. Je nach Modell und Ausstattung verbinden die Geräte die folgenden Kommunikationsteilnehmer und -wege zu einer gemeinsamen Telefonstruktur:

1. die intern an LAN, WLAN und DMZ angeschlossenen VoIP-Endgeräte wie SIP-Telefone und SIP-Softphones
2. die interne ISDN-Infrastruktur mit ISDN-TK-Anlage und ISDN-Telefonen
3. die analogen Endgeräte, intern eingebunden entweder über eine TK-Anlage mit a/b-Ports in das ISDN-Netz oder alternativ über einen ATA (Analog-Telefon-Adapter) in das VoIP-Netz
4. externe SIP-Provider mit allen über den jeweiligen Provider erreichbaren, externen Gesprächsteilnehmern
5. übergeordnete SIP-TK-Anlagen mit allen über diese Anlage erreichbaren, internen und externen Gesprächsteilnehmern

6. die externe ISDN-Welt über einen ISDN-NTBA oder eine übergeordnete ISDN-TK-Anlage mit allen über das Festnetz erreichbaren, externen Gesprächsteilnehmern



16.2.2.1 Benutzer und Leitungen

Telefonie-Teilnehmer in internen Bereichen können in der Sprachkommunikation aktiv werden und werden in der LANCOM VoIP-Umgebung als "Benutzer" bezeichnet. Das LANCOM unterscheidet dabei:

ISDN-Benutzer

Maximal 40 über das ISDN-Netz angeschlossene Endgeräte, inkl. der an einer übergeordneten ISDN-TK-Anlage angeschlossenen ISDN- und Analog- Endgeräte.

Bei der Anbindung von untergeordneten TK-Anlagen an Anlagenanschlüsse wird die Anzahl der möglichen ISDN-Teilnehmer durch die Länge der Durchwahl (DDI) festgelegt. In diesem Fall können alle an der TK-Anlage angeschlossenen Endgeräte mit einem einzigen ISDN-Benutzer-Eintrag abgebildet werden.

SIP-Benutzer

Maximal 40 (mit LANCOM VoIP +10 Option) über LAN und WLAN angeschlossene SIP-Endgeräte sowie die über ATA angeschlossenen analogen Endgeräte.

Die externen Kommunikationswege für die Benutzer werden als "Leitungen" bezeichnet. Das LANCOM kennt die folgenden Leitungen:

ISDN

Ein Anschluss an einen ISDN-NTBA über die TE-Schnittstelle. Zusätzlich können an die NT-Schnittstelle ISDN-Endgeräte direkt oder über eine untergeordnete ISDN-TK-Anlage angeschlossen werden.

SIP-Leitungen

Es sind maximal 55 Leitungen (mit VoIP +10 Option) möglich. Für die SIP-Leitungen werden drei Varianten unterschieden:

- Als "Einzel-Account"-Leitung verhält sich die Leitung wie ein üblicher SIP-Account mit einer einzigen Rufnummer. Die internen Benutzer können diesen Account gemeinsam für SIP-Telefonate nutzen, dabei ist immer nur ein Gespräch zur gegebenen Zeit möglich.

Je nach Angebot des Providers können über diese Leitungen die Teilnehmer im Netz des Providers, die Teilnehmer in anderen SIP-Netzen (Partner-Netze) oder auch die Teilnehmer im Festnetz erreicht werden. Auch die eigene Erreichbarkeit über eine Rufnummer aus dem Festnetz oder nur über SIP-Namen aus dem Internet ist je nach Anbieter verschieden.

- Als "Trunk"-Leitung verhält sich die Leitung wie ein erweiterter SIP-Account mit einer Stamm- und mehreren Durchwahlnummern. Die internen Benutzer nutzen diesen Account parallel, es sind mehrere Gespräche gleichzeitig möglich (bis zur maximalen Ausnutzung der verfügbaren Bandbreite).
- Als "SIP-Gateway"-Leitung stellt der LANCOM VoIP Router für eine entfernte SIP-TK-Anlage einen Übergang in ein lokales ISDN-Netz her. Das SIP-Gateway wird mit einer einzigen Nummer bei der SIP-TK-Anlage registriert, es sind allerdings mehrere Gespräche gleichzeitig möglich (bis zur maximalen Ausnutzung der verfügbaren Bandbreite). Die Verbindung zwischen der SIP-TK-Anlage und dem LANCOM VoIP Router wird üblicherweise über eine VPN-Verbindung hergestellt.

SIP-TK-Anlagen

Maximal 4 Verbindungen zu übergeordneten SIP-TK-Anlagen. Bei diesen Leitungen handelt es sich in der Regel um Verbindungen zu großen TK-Anlagen, die im Netzwerk der Zentrale stehen und die über eine VPN-Verbindung erreicht werden können.

Die genaue Anzahl der möglichen Benutzer und Leitungen kann je nach Modell bzw. Software-Option variieren.

16.3 Die Gesprächsvermittlung: Call-Routing

Alle Gespräche zwischen den internen Teilnehmern und den über die externen Leitungen erreichbaren Teilnehmer werden im LANCOM wie SIP-Gespräche behandelt – auch wenn die Verbindung zwischen zwei ISDN-Teilnehmern aufgebaut wird.

Der Call-Router im LANCOM VoIP Router übernimmt die Vermittlung der Gespräche. Die Vermittlung stützt sich dabei im Wesentlichen auf die Informationen aus zwei Tabellen:

- Die Regeln in der Call-Routing-Tabelle können die beim Call-Router eingehenden Rufnummern bei Bedarf verändern und flexibel entscheiden, über welche Leitung ein Gespräch geführt werden soll.
- Die Tabelle der lokal angemeldeten Benutzer gibt Aufschluss darüber, welches Endgerät über welche interne Rufnummer erreichbar ist.

Die Bandbreitenreservierung sowie QoS- und Firewall-Einstellungen, die für die zuverlässige Übertragung der Voice-Daten notwendig sind, werden vom LANCOM automatisch vorgenommen.

- Beim Verbindungsaufbau prüft das LANCOM, welche Bandbreite (unter Beachtung der erlaubten Codecs) für diese Verbindung **maximal** benötigt werden könnte.
  - Diese Bandbreite wird dann automatisch beim Verbindungsbeginn im QoS-Modul reserviert.
  - Steht diese maximale Bandbreite bei der Verhandlung nicht zur Verfügung, kommt die Verbindung nicht zustande.
  - Sofern sich die beteiligten Endgeräte während der Verhandlung auf einen Codec mit geringeren Bandbreitenbedarf einigen, wird die reservierte Bandbreite entsprechend herabgesetzt.

- Alle Pakete von ISDN-Benutzern werden im LANCOM mit einer DiffServ-Markierung versehen (bei SIP-Benutzern kommen die QoS-Markierungen üblicherweise aus den Telefonen bzw. Soft-Phones):
  - SIP-Pakete zur Signalisierung werden als CS1 markiert.
  - RTP-Pakete werden als EF markiert.
- Die für die Übertragung notwendigen Ports werden automatisch freigeschaltet.

16.3.1 SIP-Proxy und SIP-Gateway

Die Aufgaben der Gesprächsvermittlung zwischen den SIP- und ISDN-Teilnehmern auf den verschiedenen Leitungen werden durch zwei Funktionen im LANCOM VoIP Router realisiert:

SIP-Proxy

Ein SIP-Proxy übernimmt die Aufgaben einer reinen Vermittlung zwischen den Gesprächsteilnehmern.

SIP-Gateway

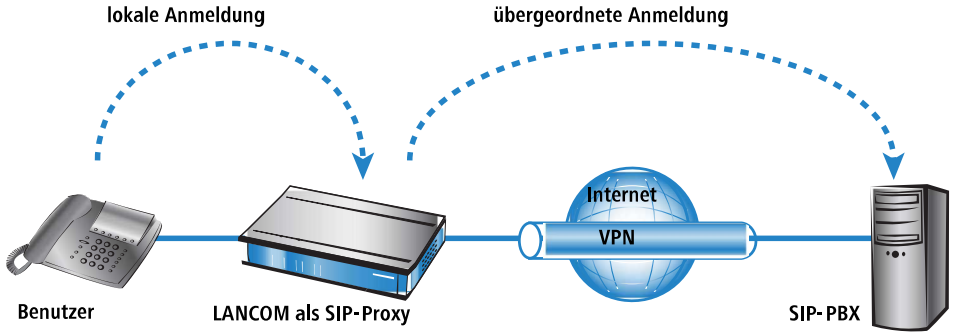
Das SIP-Gateway übernimmt die Funktion des Umsetzers zwischen IP-basierender Telefonie auf Basis des SIP-Protokolls und anderen (Fernmelde-) Netzwerken, z. B. dem ISDN-Netz.

16.3.2 Die Anmeldung von Benutzern am SIP-Proxy

Ein LANCOM VoIP Router bildet die zentrale Vermittlungsstelle für SIP-Gespräche zwischen verschiedenen Teilnehmern, die über unterschiedliche Leitungen miteinander kommunizieren wollen. Die Aufgaben der Vermittlung werden im LANCOM vom SIP-Proxy übernommen. Die Telefon-Endgeräte teilen dem SIP-Proxy ihre Wünsche nach Verbindungsaufbau mit, der SIP-Proxy entscheidet anhand bestimmter Regeln, über welche Leitung die Verbindung aufgebaut werden soll. Umgekehrt kann der SIP-Proxy die eingehenden Gespräche anhand seiner Regeln einem bestimmten Endgerät zuordnen.

Damit die Endgeräte diese Vermittlung nutzen können, müssen sie am SIP-Proxy angemeldet (registriert) sein. Sofern die Anmeldung auf die Vermittlung der Rufe im LANCOM beschränkt ist, spricht man von "lokaler Anmeldung".

Werden weitere Vermittlungsstellen – wie z. B. eine SIP-TK-Anlage an einem anderen Standort – in die Vermittlung der Gespräche mit einbezogen, spricht man von einer übergeordneten Anmeldung. In diesem Fall nimmt das LANCOM zunächst den Anmeldewunsch entgegen und leitet ihn bei Bedarf an die übergeordnete Instanz weiter. In diesem Zusammenhang bezeichnen wir das LANCOM als "transparenten Proxy".



Der große Vorteil dieser zweistufigen Anmeldung kommt im Backup-Fall zum Tragen: Falls die Verbindung zu einer übergeordneten SIP-PBX einmal nicht zur Verfügung steht, kann der SIP-Proxy auch die übergeordnet angemeldeten Benutzer als lokale Benutzer verwalten und die Gespräche über die definierten Alternativ-Leitungen führen.

16.3.2.1 Anmeldung am LANCOM VoIP-Router (lokale Anmeldung)

Für die lokale Anmeldung am LANCOM reicht es zunächst aus, wenn der Benutzer eine gültige VoIP-Domäne an den SIP-Proxy übermittelt und als SIP-Benutzer eingetragen ist. Gültig sind die interne VoIP-Domäne des LANCOM VoIP Router und alle Domänen, die in einer SIP-Leitung eingetragen sind.

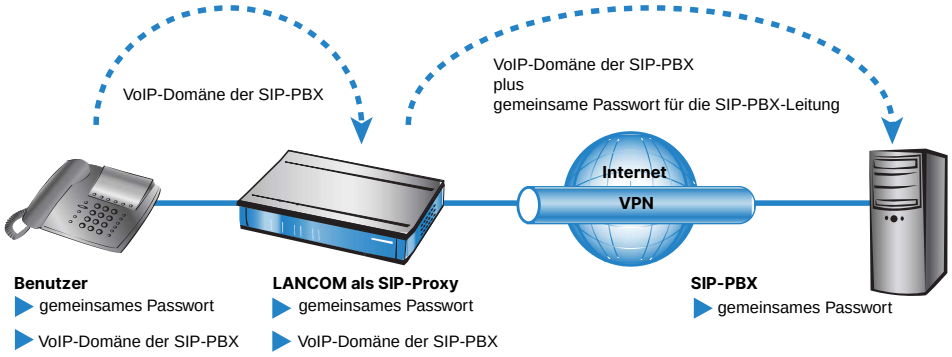
- Die Domäne wird bei SIP-Endgeräten im LAN (SIP-Telefon oder SIP-Softphone) in der Konfiguration eingetragen.
- Bei ISDN-Endgeräten kann die Domäne nicht im Telefon eingetragen werden, daher ist für die Anmeldung von ISDN-Benutzern immer ein entsprechender Eintrag als ISDN-Benutzer in der Konfiguration des LANCOM erforderlich.
- Um Anmeldungen von unbekannten Teilnehmern zu verhindern, kann für die lokale Anmeldung eine Authentifizierung am SIP-Proxy vorgeschrieben werden (lokale Authentifizierung). In diesem Fall muss für den SIP- oder ISDN-Benutzer in der Konfiguration des LANCOM VoIP-Routers auch ein Passwort eingetragen sein.

Die automatische Anmeldung ohne Eintrag eines Passworts ist auf die SIP-Benutzer im LAN beschränkt. SIP-Benutzer aus dem WAN müssen immer über einen entsprechenden Benutzer-Eintrag mit Passwort authentifiziert werden.

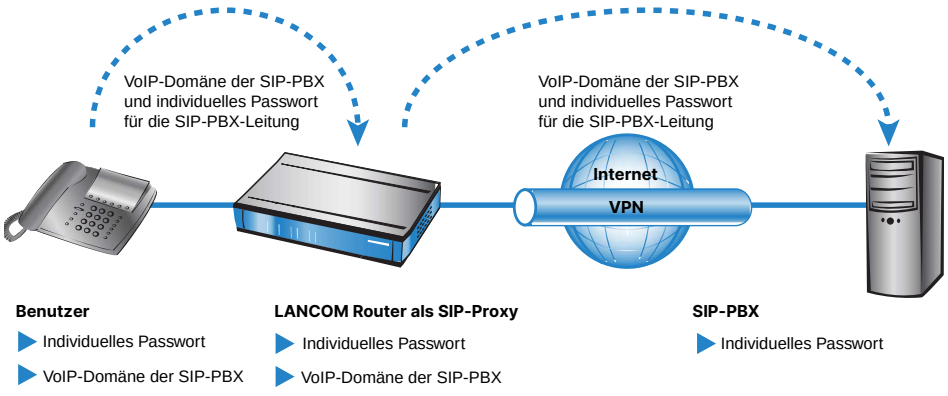
16.3.2.2 Anmeldung an übergeordnete SIP-PBX (übergeordnete Anmeldung)

Für die Anmeldung an einer SIP-PBX ist in der Regel immer eine Authentifizierung mit Benutzer und Passwort erforderlich. Hier gibt es zwei Möglichkeiten zur Übertragung der Authentifizierungsdaten an die SIP-PBX:

- Alle SIP- und ISDN-Benutzer auf Seite des LANCOM VoIP Router verwenden die gleichen, gemeinsamen Zugangsdaten. In diesem Fall wird nur die VoIP-Domäne der SIP-PBX und die entsprechende Benutzer-ID im SIP-Endgerät eingetragen. Für die ISDN-Benutzer wird die VoIP-Domäne der SIP-PBX im LANCOM als ISDN-Benutzer eingetragen. Der SIP-Proxy erkennt den Anmeldewunsch an einer übergeordneten SIP-PBX daran, dass die vom Client übermittelte Domäne mit einer eingetragenen Domäne einer SIP-PBX-Leitung übereinstimmt. Er ergänzt die Anmeldedaten mit dem gemeinsamen Passwort und leitet die Anmeldung weiter an die SIP-PBX.



- Falls in der SIP-PBX die SIP- oder ISDN-Benutzer am LANCOM VoIP Router mit unterschiedlichen Passwörtern eingetragen sind, müssen die Benutzer bei der Anmeldung ihr individuelles Passwort übermitteln. Für jeden SIP- oder ISDN-Benutzer wird daher im LANCOM ein Benutzereintrag mit dem individuellen Passwort angelegt, dass auch bei den SIP-Endgeräten so eingetragen wird. Benutzer mit gemeinsamen und individuellen Passwörtern können parallel verwaltet werden.



16.3.2.3 Besondere Aspekte für ISDN-Benutzer

Die Integration von ISDN-Endgeräten in die VoIP-Umgebung des LANCOM und die erforderlichen Konfigurationsschritte sind abhängig vom jeweiligen Anwendungsbeispiel und von den Möglichkeiten einer evtl. eingesetzten ISDN-TK-Anlage. Wichtig für die Anwender sind vor allem die folgenden Fragen:

- Können die ISDN-Endgeräte intern mit SIP-Benutzern telefonieren?
- Sind die ISDN-Endgeräte von extern über SIP-Leitungen erreichbar?
- Können die ISDN-Endgeräte extern über SIP-Leitungen telefonieren?

Wenn die ISDN-Endgeräte über eine ISDN-TE-Schnittstelle des LANCOM erreichbar sind, bezeichnen wir sie als "übergeordnet". Aus Sicht des LANCOM befinden sich die ISDN-Endgeräte dann an einer externen Leitung. Die ISDN-Endgeräte werden normalerweise nicht als lokale Benutzer geführt, daher sind auch keine Einträge für ISDN-Benutzer erforderlich.

ISDN-Endgeräte an einer übergeordneten ISDN-TK-Anlage ...

- können interne Rufe zu den SIP-Benutzern aufbauen, wenn die entsprechenden Rufnummern als interne MSNs in der ISDN-TK-Anlage konfiguriert sind.
- können interne Rufe der SIP-Benutzer empfangen, wenn die Call-Routing-Tabelle die internen MSNs der ISDN-Endgeräte z. B. über eine Standard-Route auf der ISDN-Leitung ausgeben.
- können nur dann über SIP-Leitungen Gespräche aufbauen, wenn die TK-Anlage bestimmte Rufnummern über ihren internen ISDN-Bus ausgeben kann. Ansonsten wird die ISDN-TK-Anlage alle Rufe, die nicht zu ihren internen MSNs passen, über ihre externe ISDN-Schnittstelle an das öffentliche Telefonnetz ausgeben.
- können nur dann von einer übergeordneten SIP-PBX Gespräche empfangen, wenn Sie als ISDN-Benutzer im LANCOM eingerichtet sind und so an der SIP-PBX angemeldet werden.

Wenn die ISDN-Endgeräte über eine ISDN-NT-Schnittstelle des LANCOM erreichbar sind, bezeichnen wir sie als "untergeordnet". Für das LANCOM handelt es sich dann um lokale Teilnehmer, die über die Liste der angemeldeten Benutzer aufgelöst werden können. Da die ISDN-Endgeräte selbst keine Domäne zur Anmeldung am LANCOM übermitteln können, müssen sie mit einem entsprechenden Eintrag als ISDN-Benutzer eingetragen und so dem VoIP-System bekannt gemacht werden.

ISDN-Endgeräte an einer untergeordneten ISDN-TK-Anlage ...

- können interne Rufe zu den SIP-Benutzern aufbauen, indem sie das für die TK-Anlage notwendige Amtsholungszeichen vor die interne Rufnummer der SIP-Benutzer stellen. Die TK-Anlage gibt den Anruf dann mit der internen Rufnummer des SIP-Benutzers – ohne das Amtsholungszeichen – auf ihrem externen ISDN-Bus an das LANCOM weiter.
- können interne Rufe der SIP-Benutzer empfangen, wenn im Eintrag für den ISDN-Benutzer die richtige Zuordnung von interner Rufnummer zur entsprechenden MSN eingetragen ist. Das LANCOM setzt einen Ruf an die interne Nummer des ISDN-Benutzers auf die MSN und gibt diese auf dem zugewiesenen ISDN-Bus aus. Die TK-Anlage empfängt die MSN wie einen externen Anruf und leitet ihn an das entsprechende ISDN-Endgerät weiter.
- können eingehende und abgehende Gespräche über SIP- und ISDN-Leitungen führen wie die SIP-Benutzer. Bei den abgehenden Rufen ist wieder das ggf. notwendige Zeichen für die Amtsholung an der TK-Anlage erforderlich.

Dynamische ISDN-Benutzer an Anlagenanschlüssen

Beim Anschluss von untergeordneten TK-Anlagen an einem Punkt-zu-Punkt-Interface des LANCOM VoIP Router (Anlagenanschluss) wird die Anzahl der möglichen ISDN-Endgeräte nur durch die Länge der Durchwahl begrenzt. Schon bei dreistelligen Durchwahlnummern können fast 1000 Endgeräte angeschlossen werden, die alle als ISDN-Benutzer im LANCOM VoIP Router verwaltet werden. Durch einen ISDN-Benutzer-Eintrag mit einem #-Zeichen als Platzhalter für die Rufnummern können alle ISDN-Endgeräte mit den jeweiligen Durchwahlen als dynamische ISDN-Benutzer angelegt werden.



Benutzereinträge mit #-Zeichen zur Abbildung von Benutzergruppen können nicht für eine Anmeldung an einer übergeordneten TK-Anlage verwendet werden. Für diese Anmeldung ist immer ein spezifischer Eintrag für den einzelnen ISDN-Benutzer notwendig.

16.3.3 Rufnummernumsetzung an Netz-Übergängen

LANCOM VoIP Router vermitteln Gespräche zwischen verschiedenen Telefonnetzen, z. B. dem ISDN-Netz, den Netzen verschiedener SIP-Provider und dem internen Telefonnetz. In jedem dieser Netze werden üblicherweise andere Rufnummernbereiche oder sogar unterschiedliche Konventionen zur Adressierung der Gesprächsteilnehmer verwendet. Während das klassische Festnetz die aus numerischen Zeichen bestehenden Rufnummern mit Landes- und Ortsnetzvorwahlen verwendet, erlaubt die SIP-Welt auch alphanumerische Namen mit Domänen-Angaben.

Beim Übergang von Anrufen zwischen diesen Bereichen müssen die "Rufnummern" jeweils so umgesetzt werden, dass die gewünschten Gesprächsteilnehmer erreicht werden können.

Sowohl gerufene als auch rufende Nummer müssen je nach Anwendungsfall so modifiziert werden, dass auch der Rückruf zur Quelle des Anrufs möglich ist.

Die Rufnummernumsetzung an den Amtsübergängen wird in erster Linie realisiert durch entsprechende Mapping-Einträge bei den ISDN- und SIP-Leitungen sowie durch die Regeln der Call-Routing-Tabelle.

16.3.4 Der Call-Manager

Der Call-Manager hat die zentrale Aufgabe, einen zur Vermittlung anliegenden Ruf einer bestimmten Leitung oder einem bestimmten Benutzer zuzuordnen. Für diese Zuordnung nutzt der Call-Manager die Call-Routing-Tabelle und die Liste der angemeldeten Benutzer. Die Vermittlung der Anrufe läuft in folgenden Schritten ab:

- Bearbeitung der gerufenen Nummer (Called Party ID)

  Zunächst wird überprüft, ob eine numerische oder alphanumerische Nummer vorliegt. Dazu werden typische Wahltrennzeichen wie „()-/" und <Blank> entfernt. Ein „+" an erster Stelle bleibt erhalten. In diesem Fall gilt die Nummer weiter als numerische Nummer. Wird bei der Prüfung ein anderes alphanumerisches Zeichen entdeckt, wird die Rufnummer als alphanumerisch betrachtet und bleibt unverändert.

- Auflösung des Rufes in der Call-Routing-Tabelle

  Nach der Bearbeitung der Called Party ID wird der Ruf an die Call-Routing-Tabelle übergeben. Die Einträge in der Call-Routing-Tabelle bestehen aus Sätzen von Bedingungen und Anweisungen. Die Einträge – mit Ausnahme der Default-Routen – werden der Reihe nach durchsucht, der erste Eintrag wird ausgeführt, bei dem **alle** angegebenen Bedingungen erfüllt sind.

- Auflösung des Rufes über die Tabellen der lokalen Teilnehmer

  Wird in der Call-Routing-Tabelle kein Eintrag gefunden, der mit dem anliegenden Ruf übereinstimmt, sucht der Call-Manager in den Listen der lokalen Teilnehmer. Für das Call-Routing werden alle dem Call-Router bekannten Benutzer verwendet (angemeldete SIP-Benutzer und konfigurierte ISDN-Benutzer). Wird dort ein Eintrag gefunden, dessen Nummer mit der gerufenen Nummer übereinstimmt und der auch über die passende Ziel-Domäne verfügt, dann wird dieser Ruf an den entsprechenden Teilnehmer zugestellt.

  Wird kein lokaler Teilnehmer gefunden, für den Nummer und Ziel-Domäne übereinstimmen, reicht in einem weiteren Durchlauf auch die Übereinstimmung der Rufnummer des lokalen Teilnehmers mit der gerufenen Nummer, die Ziel-Domäne bleibt ohne Berücksichtigung.

- Auflösung des Rufes über die Default-Einträge in der Call-Routing-Tabelle

  Falls die vorangehenden Durchläufe durch die Call-Routing-Tabelle und die Listen mit den lokalen Teilnehmern keinen Erfolg hatten, wird der anliegende Ruf erneut in der Call-Routing-Tabelle geprüft. In diesem Durchlauf werden dann allerdings nur die Default-Routen berücksichtigt. Dabei werden die in den Default-Routen eingetragenen Nummern und Ziel-Domänen nicht berücksichtigt. Nur die Quell-Filter werden ausgewertet, sofern die Default-Route über solche Filter verfügt.

Konkrete Beispiele für den Ablauf des Call-Routing finden Sie bei der Beschreibung der Konfigurationsbeispiele.

16.3.5 Telefonieren mit dem LANCOM VoIP Router

Mit dem Einsatz der LANCOM VoIP Router eröffnen sich zahlreiche neue Möglichkeiten zum Aufbau von Telefongesprächen. Je nach Konstellation der eingesetzten Endgeräte (z. B. SIP- oder ISDN-Telefone, SIP- oder ISDN-TK-Anlagen) und abhängig von der Konfiguration des Call-Routings im LANCOM VoIP Router sind einige Hinweise für das Verständnis des Verbindungsaufbaus wichtig.

16.3.5.1 Automatische Amtsholung

Der Einsatz der LANCOM VoIP Router und die Ergänzung um VoIP-Funktionen in Ihrer Telefonstruktur soll das Telefonverhalten der Anwender möglichst komfortabel unterstützen. Einer der zentralen Aspekte dabei ist die Verwendung einer „spontanen" oder „automatischen" Amtsholung, wie sie auch von üblichen TK-Anlagen bekannt ist.

- Die meisten TK-Anlagen sind so eingestellt, dass die Telefonteilnehmer der gewünschten Rufnummer eine "0" voranstellen müssen, um eine Amtsleitung zu bekommen – um also ein Gespräch über ein öffentliches Telefonnetz führen zu können.

  Ohne die vorangestellte "0" wird die gewählte Rufnummer als interne Rufnummer eines anderen Nebenstellenanschlusses an der eigenen TK-Anlage gewertet.

- Ist für die TK-Anlage die „automatische Amtsholung" eingerichtet, werden alle gewählten Rufnummern direkt über das öffentliche Telefonnetz geführt. Internes Telefonieren zu anderen Nebenstellen ist in diesem Fall nicht oder nur durch die Wahl eines besonderen Zeichens vor der Rufnummer möglich.

Mit der Erweiterung der Telefonstruktur um einen LANCOM VoIP Router eröffnen sich zahlreiche neue Möglichkeiten zum Anschluss von verschiedenen Telefon-Endgeräten. Dazu gehören die evtl. schon vorhandenen analogen oder ISDN-Telefone (ggf. angeschlossen an eine entsprechende TK-Anlage) oder auch VoIP-Endgeräte wie SIP-Telefone oder PCs mit VoIP-Software.

Ein LANCOM VoIP Router als neuer und zentraler Baustein der Telefonstruktur übernimmt für die angeschlossenen Endgeräte einige Aufgaben einer TK-Anlage. Daher können Sie auch die automatische Amtsholung für die am LANCOM VoIP Router angeschlossenen Endgeräte gezielt für die Gruppen der ISDN- oder SIP-Teilnehmer einstellen und so an das bisherige Telefonverhalten anpassen.

- Wenn die automatische Amtsholung ausgeschaltet ist, müssen die Teilnehmer der gewünschten Rufnummer jeweils eine "0" voranstellen, um ein Gespräch über ein öffentliches Telefonnetz zu führen.

  Alle Anrufe ohne eine vorangestellte "0" werden als Rufe zu internen Nebenstellen im eigenen Telefonnetz behandelt.

- Wenn die automatische Amtsholung eingeschaltet ist, werden alle Rufe zunächst als Gespräch über ein öffentliches Telefonnetz geführt.

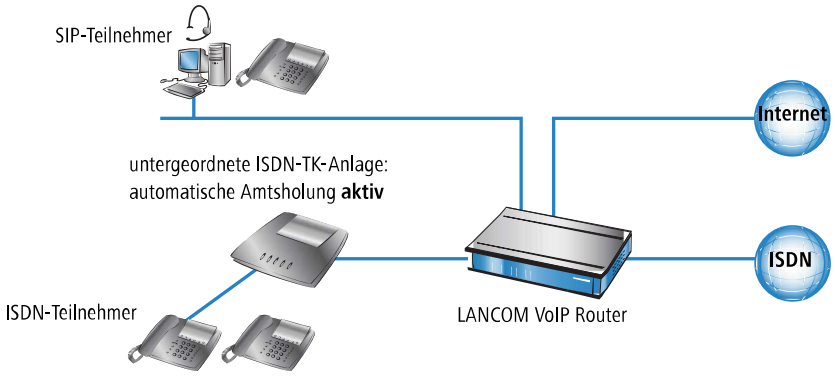
  Für Anrufe zu internen Gegenstellen wird der Rufnummer in diesem Fall ein spezielles Zeichen oder eine bestimmte Nummernkombination vorangestellt. In der Standardeinstellung wird mit dem Aktivieren der automatischen Amtsholung ein Stern * als Erkennungszeichen für eine interne Rufnummer aktiviert. Diese Einstellung können Sie nach Bedarf an die ggf. bisher verwendeten Erkennungszeichen anpassen.

  Wenn Sie den LANCOM VoIP Router am Nebenstellenanschluss einer TK-Anlage betreiben, empfiehlt es sich, die Amtsholung des Routers der TK-Anlage entsprechend einzustellen, damit das Verhalten aus Benutzersicht gleich ist.

Beispiel untergeordnete TK-Anlage

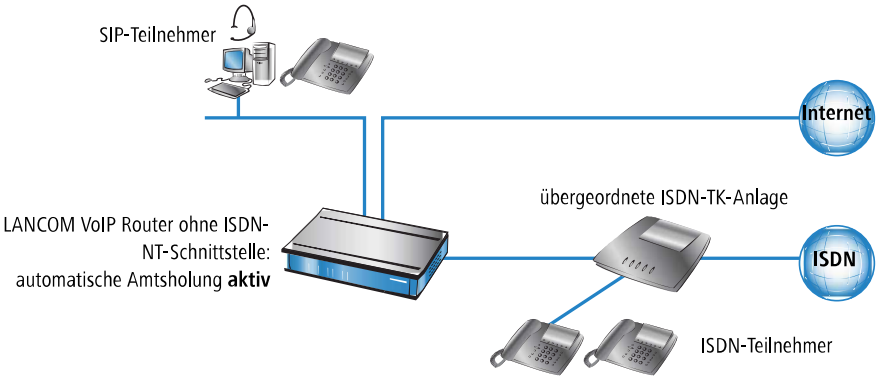
Ein LANCOM VoIP Router wird zwischen dem ISDN-Amtsanschluss und die vorhandene ISDN-TK-Anlage geschaltet. In der TK-Anlage wird die automatische Amtsholung aktiviert, die Einstellungen im Call-Router des LANCOM VoIP Router

entscheiden darüber, ob bei den angeschlossenen ISDN- und SIP-Teilnehmern eine "0" für die Amtsholung vorgewählt werden muss.



Beispiel übergeordnete TK-Anlage

Ein LANCOM VoIP Router wird an den Nebenstellenanschluss einer ISDN-TK-Anlage angeschlossen. Im LANCOM VoIP Router wird die automatische Amtsholung aktiviert, die Einstellungen in der übergeordneten TK-Anlage entscheiden darüber, ob bei den angeschlossenen ISDN- und SIP-Teilnehmern eine "0" für die Amtsholung vorgewählt werden muss.



16.3.5.2 Anwahl von verschiedenen Rufnummernbereichen

Für die Anwahl von Gesprächspartnern stehen Ihnen die folgenden Rufnummernbereiche zur Verfügung:

- Interne Rufnummern sind vergleichbar mit den Nebenstellenrufnummern herkömmlicher TK-Anlagen („Durchwahl"). Über diese interne Rufnummer können sich die Teilnehmer direkt ohne den Umweg über ein öffentliches Telefonnetz erreichen.

  Die internen Rufnummern müssen über alle im eigenen Telefonnetz verbundenen Teilnehmer eindeutig sein, d. h. auch über alle evtl. angeschlossenen TK-Anlagen hinweg!

  Die internen Teilnehmer erreichen Sie über die einfache Anwahl der internen Rufnummer, ohne vorangestellte "0".

  Je nach Einstellung der automatischen Amtsholung muss ggf. ein besonderes Wahlzeichen vorangestellt werden.

- Über die **örtlichen Rufnummern** erreichen Sie alle nicht internen Teilnehmer, die sich im gleichen Telefonortsnetz wie der LANCOM VoIP Router befinden, die also die gleiche öffentliche Ortsnetzvorwahl haben wie der Amtsanschluss für den LANCOM VoIP Router.

  Dabei ist in verteilten Standorten über Städte- oder Ländergrenzen hinweg der physikalische Standort des Gerätes maßgeblich, auch wenn z. B. eine zentrale TK-Anlage an einem anderen Standort vorhanden ist. Für einen LANCOM

VoIP Router in München sind also alle Telefonteilnehmer im Ortsnetz München über örtliche Rufnummern zu erreichen, selbst wenn eine über VPN angebundene SIP-TK-Anlage in Hamburg erreichbar ist.

Je nach Einstellung der automatischen Amtsholung muss ggf. eine "0" vorangestellt werden.

- Die **nationalen und internationalen Rufnummern** verhalten sich analog zu den örtlichen, auch hier ist der physikalische Standort der Geräte ausschlaggebend für die Zuordnung zu den entsprechenden Vorwahlbereichen. Ein LANCOM VoIP Router in Österreich gehört also zum nationalen Telefonnetz in Österreich, auch wenn eine VPN-Anbindung an die SIP-TK-Anlage der Zentrale in Deutschland eingerichtet ist.

Je nach Einstellung der automatischen Amtsholung muss ggf. eine "0" vorangestellt werden.

16.3.5.3 Sonderrufnummern

Bestimmte Sonderrufnummern (Notfallrufnummern, kostenfreie oder besonders kostenintensive Servicerufnummern) können im Call-Router einer speziellen Behandlung unterworfen werden.

- So ist z. B. die Erreichbarkeit von Notfallrufnummern der Polizei oder Feuerwehr immer sicher zu stellen, auch wenn die Telefonteilnehmer einmal nicht das richtige Wählzeichen zur Amtsholung voranstellen.

  In der Standardeinstellung sind die Notfallrufnummern „110“ und „112“ daher so eingerichtet, dass sie mit oder ohne vorangestellte „0“ immer korrekt ausgegeben werden.
- Für kostenfreie Rufnummernbereiche wie die „0800“ wird üblicherweise eine Verbindung direkt über ISDN gewählt, weil so die kostenfreie Festnetz-zu-Festnetz-Verbindung genutzt wird.

16.3.5.4 Wählen über bestimmte Leitungen

Mit dem Einsatz der LANCOM VoIP Router können neben der vorher vorhandenen ISDN-Amtsleitung weitere Leitungen zum Aufbau von Telefongesprächen definiert werden, z. B. zu einer über VPN angebundenen SIP-TK-Anlage oder zu einem öffentlichen SIP-Provider über das Internet. Für jeden Verbindungsaufbau entscheidet der Call-Router anhand der festgelegten Regeln, welche der vorhandenen Leitungen für den Anruf genutzt werden soll.

Alternativ zur automatischen Auswahl durch den Call-Router können Sie einzelne Anrufe gezielt über eine bestimmte Leitung führen, weil Sie z. B. einen Gesprächspartner bewusst über ISDN und nicht über die SIP-TK-Anlage in der Zentrale anrufen wollen. Zu diesem Zweck werden den vorhandenen Leitungen im Call-Router spezielle Kennziffern zugeordnet, z. B. die „98“ für ISDN oder die „97“ für einen SIP-Provider. Der gezielte Anruf über diese Leitung wird dann mit der entsprechenden Kennung eingeleitet:

- Der Anruf mit „089 123456“ wird über den Call-Router einer entsprechenden Leitung zugeordnet, z. B. über die SIP-TK-Anlage der Zentrale.
- Der Anruf mit „98 089 123456“ wird dagegen vom Call-Router direkt über den ISDN-Anschluss ausgeführt.

16.3.6 Halten, Makeln, Verbinden

LANCOM VoIP Router unterstützen verschiedene Dienstmerkmale, wie sie aus dem ISDN-Netz bekannt sind:

- Bei **Halten** versetzt der Benutzer eine aktive Gesprächsverbindung in einen Wartezustand. In diesem Zustand kann der Benutzer mit seinem Endgerät z. B. eine weitere Verbindung zu einem anderen Gesprächspartner aufbauen.
- Beim **Makeln** schaltet der Benutzer zwischen zwei Gesprächsverbindungen hin und her. Der Benutzer kann dabei jeweils nur mit einem Gesprächspartner sprechen, der andere Gesprächspartner wird im Wartezustand gehalten.
- Beim **Verbinden** schaltet der Benutzer die aktive Gesprächsverbindung und eine im Wartezustand zusammen. Anschließend sind die beiden Gesprächspartner untereinander verbunden, der Benutzer selbst ist nicht mehr Teilnehmer der Gesprächsverbindung.

Die Dienstmerkmale Halten, Makeln und Verbinden stehen zwischen allen lokalen SIP-, ISDN- und Analog-Benutzern und den Teilnehmern an einer übergeordneten SIP-PBX zur Verfügung, können aber immer nur von einem SIP-Teilnehmer eingeleitet werden.

16.3.7 Übertragung von DTMF-Tönen

Aus dem ISDN-Telefonnetz ist die Möglichkeit bekannt, mit Hilfe der DTMF-Töne (Dual Tone Multiple Frequency) die Information zu übertragen, welche Taste am Telefon gedrückt wurde. Mit Hilfe der DTMF-Töne kann der Benutzer des Telefons z. B. mit Sprachmailboxen und Computer-Telefonie-Systemen kommunizieren.

In VoIP-Anwendungen müssen spezielle Mechanismen die Funktion der DTMF-Töne übernehmen. Wird z. B. während eines Anrufes eine Taste an einem VoIP-Telefon oder einem VoIP-Softphone gedrückt, soll die gleiche Aktion ausgelöst werden wie bei einem Anruf mit einem ISDN-Telefon.

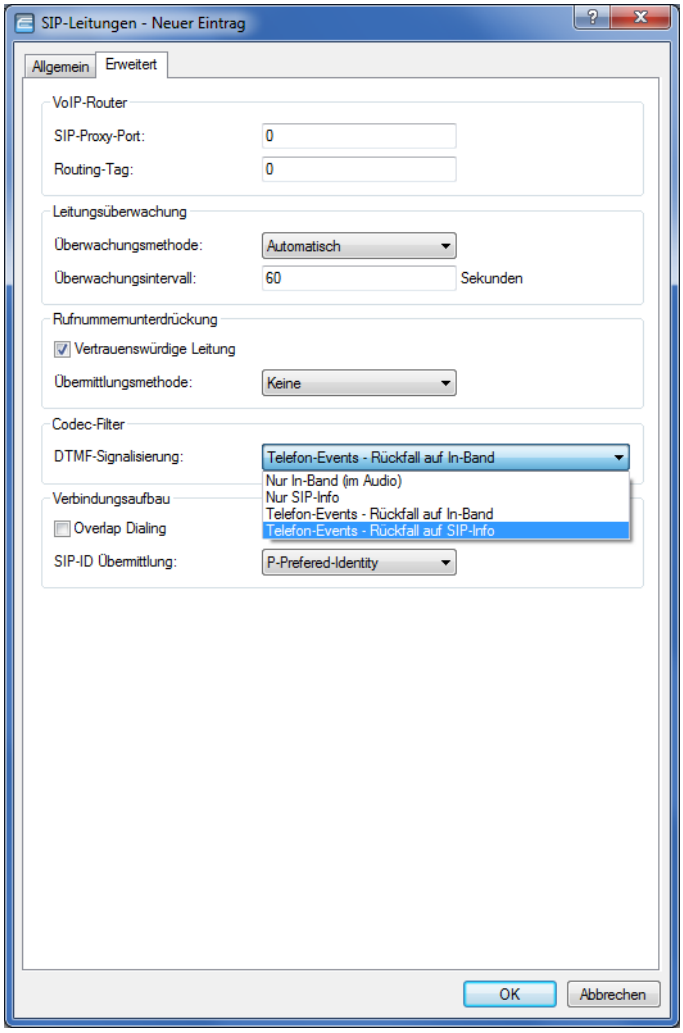
Grundsätzlich können die DTMF-Töne bei VoIP-Anwendungen auf zwei Arten übertragen werden:

- In-band bezeichnet die Übertragung der DTMF-Töne im gleichen Datenstrom, in dem auch die Sprachdaten übertragen werden. Dieses Verfahren gilt jedoch als relativ unzuverlässig, da die DTMF-Töne im Audio-Datenstrom leicht mit den Sprachdaten verwechselt werden können, insbesondere bei komprimierenden Codecs.
- Out-of-band bezeichnet die Übertragung der DTMF-Töne parallel zu den eigentlichen Sprachdaten. Zwei Normen werden üblicherweise für die out-of-band-Übertragung verwendet:
  - SIP INFO (RFC 2976)
  - RFC 2833 (RTP Payload for DTMF Digits)

  Beide Varianten können Informationen z. B. über die gedrückten Tasten, deren Tonfrequenz und die Dauer des Tastendrucks in den Signalisierungsdatenstrom verpacken. Darüber hinaus können die Ereignisse, die mit den DTMF-Tönen übertragen werden sollten, auch im Klartext in die SIP-Daten eingetragen werden.

16.3.7.1 Konfiguration der DTMF-Signalisierung

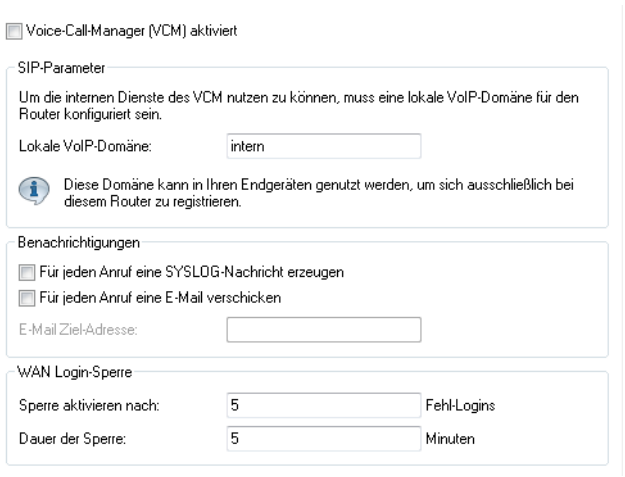
Bei der Konfiguration der DTMF-Signalisierung konfigurieren Sie unter **Voice Call Manager** > **Leitungen** > **SIP-Leitungen**, welche Variante das Gerät zur Übertragung der DTMF-Töne verwenden soll:



16.4 Konfiguration der VoIP-Parameter

16.4.1 Allgemeine Einstellungen

Die allgemeinen Einstellungen der VoIP-Parameter konfigurieren Sie unter **Voice Call Manager** > **Allgemein**.



Voice-Call-Manager (VCM) aktiviert

Aktiviert bzw. deaktiviert den Voice-Call-Manager.

Lokale VoIP-Domäne

Name der Domain, in der die angeschlossenen Telefone und der LANCOM Wireless Router betrieben werden.

- Endgeräte, die mit der gleichen Domain arbeiten, melden sich als lokale Teilnehmer am LANCOM Wireless Router an und nutzen so den SIP-Proxy.
- Endgeräte, die mit der anderen Domain einer aktiven SIP-PBX-Leitung arbeiten, melden sich als Teilnehmer an einer übergeordneten TK-Anlage an.

Für jeden Anruf eine SYSLOG-Nachricht erzeugen

Erzeugt bei jedem Anruf über den LANCOM VoIP Router eine SYSLOG-Nachricht.

Bitte beachten Sie, dass die Nutzung dieser Funktion nur mit den entsprechenden SYSLOG-Einstellungen möglich ist.

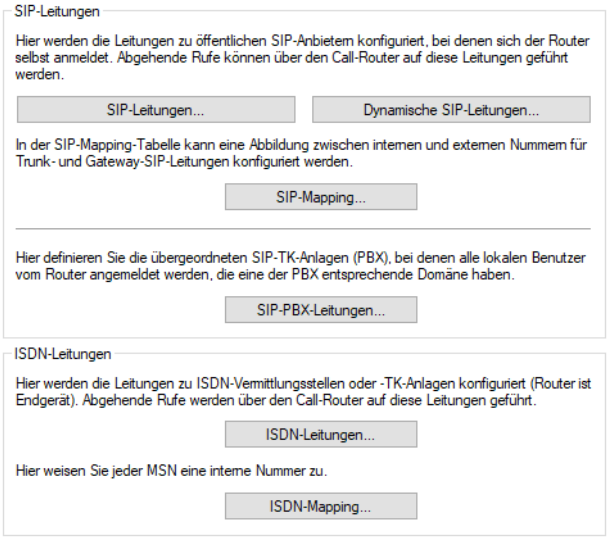
Für jeden Anruf eine E-Mail verschicken

Verschickt bei jedem Anruf über den LANCOM VoIP Router eine E-Mail an die angegebene Mail-Adresse.

Bitte beachten Sie, dass die Nutzung dieser Funktion nur mit einem entsprechend eingerichteten SMTP-Konto möglich ist.

16.4.2 Konfiguration der Leitungen

Die Konfiguration der Leitungsparameter erfolgt unter **Voice Call Manager** > **Leitungen**.

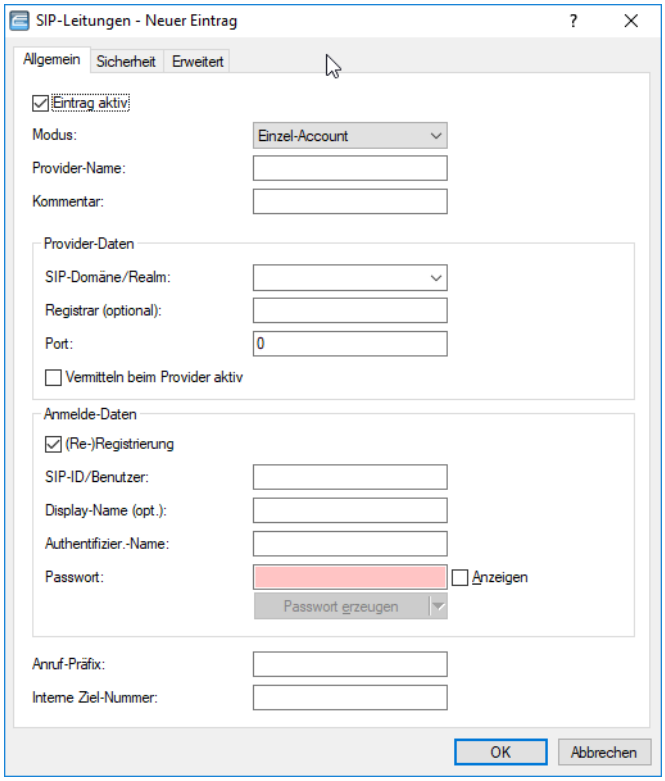


16.4.2.1 SIP-Leitungen

Über diese Leitungen meldet das Gerät sich bei anderen SIP-Gegenstellen (in der Regel SIP-Provider oder als Remote Gateway bei SIP-TK-Anlagen) an. Die Verbindung erfolgt entweder über das Internet oder einen VPN-Tunnel.

Die Konfiguration erfolgt über **Voice Call Manager** > **Leitungen** mit einem Klick auf die Schaltfläche **SIP-Leitungen**.

Auf dem Reiter **Allgemein** haben Sie die folgenden Konfigurationsmöglichkeiten:



Eintrag aktiv

Aktiviert bzw. deaktiviert diesen Eintrag.

Modus

Mit dieser Auswahl bestimmen Sie die Betriebsart der SIP-Leitung. Mögliche Werte sind:

Einzel-Account

Verhält sich nach außen wie ein üblicher SIP-Account mit einer einzigen öffentlichen Nummer. Die Nummer wird beim Serviceprovider registriert und die Registrierung regelmäßig aufgefrischt (wenn eine (Re-)Registrierung für diese SIP-Provider-Line aktiviert ist). Bei ausgehenden Rufen wird die Nummer des Rufenden (Absender) durch die registrierte Nummer ersetzt (maskiert). Eingehende Rufe werden der konfigurierten internen Ziel-Nummer zugestellt. Die maximale Anzahl von gleichzeitigen Verbindungen wird entweder vom Provider vorgegeben oder von der vorhandenen Bandbreite und den verwendeten Codecs bestimmt.

Trunk

Verhält sich nach außen wie ein erweiterter SIP-Account mit einer Stamm- und mehreren Durchwahlnummern. Die SIP-ID wird als Stammnummer beim Serviceprovider registriert und die Registrierung regelmäßig aufgefrischt (wenn eine (Re-)Registrierung für diese SIP-Provider-Line aktiviert ist). Bei ausgehenden Rufen fungiert die Stammnummer als Präfix, das jeder rufenden Nummer (Absender; SIP: "From:") vorangestellt wird. Bei eingehenden Rufen wird das Präfix aus der Ziel-Nummer entfernt (SIP: "To:"). Die verbleibende Nummer wird als interne Durchwahl verwendet. Im Fehlerfall (Präfix nicht auffindbar, Ziel gleich Präfix) wird der Ruf an die konfigurierte interne Ziel-Nummer geleitet. Die maximale Anzahl der Verbindungen zu einem bestimmten Zeitpunkt ist durch die zur Verfügung stehende Bandbreite und möglicherweise durch den Provider begrenzt.

Gateway

Sie verhält sich nach außen wie ein üblicher SIP-Account mit einer einzigen öffentlichen Nummer, der SIP-ID. Die Nummer (SIP-ID) wird beim Serviceprovider registriert und die Registrierung regelmäßig aufgefrischt (wenn eine (Re-)Registrierung für diese SIP-Provider-Line aktiviert ist). Bei ausgehenden Rufen wird die Nummer des Rufenden (Absender) durch die registrierte Nummer (SIP-ID in SIP: "From:") ersetzt (maskiert) und in einem separaten Feld (SIP: "Contact:") übertragen. Bei eingehenden Rufen wird die gerufene Nummer (Ziel) nicht modifiziert. Die maximale Anzahl der Verbindungen zu einem bestimmten Zeitpunkt ist durch die zur Verfügung stehende Bandbreite und möglicherweise durch den Provider begrenzt.

Link

Verhält sich nach außen wie ein üblicher SIP-Account mit einer einzigen öffentlichen Nummer (SIP-ID). Die Nummer wird beim Serviceprovider registriert und die Registrierung regelmäßig aufgefrischt (wenn eine (Re-)Registrierung für diese SIP-Provider-Line aktiviert ist). Bei ausgehenden Rufen wird die Nummer des Rufenden (Absender; SIP: "From:") nicht modifiziert. Bei eingehenden Rufen wird die gerufene Nummer (Ziel; SIP: "To:") nicht modifiziert. Die maximale Anzahl der Verbindungen zu einem bestimmten Zeitpunkt ist durch die zur Verfügung stehende Bandbreite und möglicherweise durch den Provider begrenzt.

Flex

- Sie verhält sich nach außen wie ein handelsüblicher SIP-Account mit einer einzigen öffentlichen Nummer.
- Die Nummer wird beim Serviceprovider registriert und die Registrierung regelmäßig aufgefrischt.
- Bei ausgehenden Rufen wird die Nummer des Rufenden (Absender) nicht modifiziert.
- Bei eingehenden Rufen wird die gerufene Nummer (Ziel) nicht modifiziert.
- Die maximale Anzahl der Verbindungen zu einem bestimmten Zeitpunkt ist nur durch die zur Verfügung stehende Bandbreite begrenzt.

Tabellen für die Rufnummernumsetzungen:

Einzel-Account	An der Leitung anliegende SIP-Nummer	Von der Leitung abgesetzte SIP-Nummer
Ausgehender Ruf	“From:”	Beim Provider registrierte Nummer (User-ID)

Einzel-Account	An der Leitung anliegende SIP-Nummer	Von der Leitung abgesetzte SIP-Nummer
Eingehender Ruf	"To:"	User-ID

Trunk	An der Leitung anliegende SIP-Nummer	Von der Leitung abgesetzte SIP-Nummer
Ausgehender Ruf	"From:"	Stammnummer (User-ID) + "From:"
Eingehender Ruf	Stammnummer (User-ID) + "To:"	"To:" als interne Durchwahl

Gateway	An der Leitung anliegende SIP-Nummer	Von der Leitung abgesetzte SIP-Nummer
Ausgehender Ruf	"From:"	Beim Provider registrierte Nummer (User-ID)
	"From:"	"Contact:"
Eingehender Ruf	"To:"	"To:"

Link	An der Leitung anliegende SIP-Nummer	Von der Leitung abgesetzte SIP-Nummer
Ausgehender Ruf	"From:"	"From:"
Eingehender Ruf	"To:"	"To:"

Name

Der Name der Leitung. Er darf nicht identisch sein mit einer anderen in dem Gerät konfigurierten Leitung (SIP-Provider, ISDN oder SIP-PBX).

Kommentar

Kommentar zu diesem Eintrag.

SIP-Domäne/Realm

SIP-Domäne/Realm der übergeordneten Gegenstelle. Sofern die Gegenstelle DNS-Service Records für SIP unterstützt, genügt diese Angabe, um Proxy, Outbound-Proxy, Port, Registrar automatisch zu ermitteln – das ist bei typischen SIP-Provider-Angeboten i.d.R. der Fall.

Registrar

Der SIP-Registrar ist die Stelle, welche die Anmeldung mit den konfigurierten Authentifizierungsdaten für diesen Account beim SIP-Provider entgegen nimmt.

Dieses Feld kann frei bleiben, sofern der SIP-Provider keine speziellen Angaben macht. Der Registrar wird dann über DNS-SRV-Anfragen zur konfigurierten SIP-Domäne/Realm ermittelt (bei SIP-Services im Firmennetz/VPN ist dies oftmals nicht der Fall, d. h., der Wert muss explizit gesetzt werden).

Um eine Registrierung über IPv4 oder IPv6 zu erzwingen, kann die SIP-Domäne gefolgt von dem Suffix **?4** bzw. **?6** im Feld **Registrar** eingetragen werden (z.B. **SIP-Domain.de?4**). Siehe hierzu *Konfigurationsmöglichkeit für IPv4/IPv6-Auflösung bei DNS-Auflösungen* auf Seite 172.

Outbound-Proxy

Der Outbound-Proxy des SIP-Providers nimmt alle vom Gerät ausgehenden SIP-Anrufsignalisierungen einer Verbindung zu diesem Provider für die Dauer der Verbindung entgegen.

Dieses Feld kann frei bleiben, sofern der SIP-Provider keine speziellen Angaben macht. Der Outbound-Proxy ist in dem Fall identisch mit dem Registrar. Dies entspricht einer typischen Konfiguration für SIP-Provider-Angebote.

Port

Dies ist der entfernte Port zur Kommunikation mit dem Provider.

Vermitteln beim Provider aktiv

Bei der Rufvermittlung (Verbindung) von zwei entfernten Gesprächsteilnehmern kann die Vermittlung im Gerät selbst gehalten (Media-Proxy) oder an die Vermittlungsstelle beim Provider übergeben werden, wenn beide zu verbindende Gesprächsteilnehmer über diese SIP-Provider-Leitung erreicht werden. Dies hat den Vorteil, dass im LANCOM VoIP Router keine Bandbreite mehr benötigt wird. Andernfalls übernimmt der Media-Proxy im Gerät die Vermittlung der Medienströme, z. B. beim Verbinden zwischen zwei SIP-Provider-Leitungen.

Voraussetzung für die Vermittlung beim Provider ist, dass beide Verbindungen über die gleiche Providerleitung aufgebaut wurden.

Eine Übersicht über die wichtigsten SIP-Provider, die diese Funktion unterstützen, finden Sie im Support-Bereich auf der Internet-Seite.

(Re-)Registrierung

Hiermit aktivieren Sie die (wiederholte) Registrierung der SIP-Provider-Leitung. Die Registrierung kann auch zur Leitungsüberwachung herangezogen werden.

Für die Nutzung der (Re-)Registrierung stellen Sie die Methode der Leitungsüberwachung in der Ansicht **Erweitert** entsprechend auf "Register" oder "Automatisch". Das Gerät wiederholt die Registrierung jeweils nach Ablauf des Überwachungsintervalls. Wenn der SIP-Registrar des Providers ein anderes Intervall vorschlägt, übernimmt das Gerät dieses automatisch.

SIP-ID/Benutzer

Telefonnummer des SIP-Accounts oder Name des Benutzers (SIP-URI).

Bei einem SIP-Trunking-Account wird hier die Stammnummer eingetragen. Bei ankommenden Rufen werden alle über diese Stammnummer hinausgehenden Zeichen als Durchwahl (DDI) erkannt und nur diese an den Call Router übergeben. Bei abgehenden Rufen wird die vom Call Router empfangene DDI um die Stammnummer ergänzt. Mit den Zugangsdaten wird die Leitung (Einzel-Account, Trunk, Link, Gateway) angemeldet, nicht jedoch einzelne lokale Benutzer mit ihren individuellen Anmeldedaten. Wenn einzelne Benutzer (SIP, ISDN, Analog) mit den dort bzw. auf dem Endgerät hinterlegten Daten bei einer übergeordneten Instanz registriert werden sollen, muss eine SIP-PBX-Leitung eingerichtet werden.

Display-Name

Name, der auf dem angerufenen Telefondisplay erscheinen soll.

Dieser Wert sollte im Normalfall nicht gesetzt werden, da bei eingehenden Rufen der SIP-Provider den Display-Namen setzt und bei ausgehenden Rufen der lokale Client bzw. die Rufquelle (ggf. überschrieben mit den Einstellungen zum Display-Namen des jeweiligen Benutzers). Oftmals werden hier zusätzliche Informationen übermittelt (z. B. Originalrufnummer bei einer Umleitung etc.), die für den Angerufenen hilfreich sein können. Im Fall von SIP-Einzel-Accounts verlangen manche Provider allerdings auch den in den Anmeldedaten vorgegebenen Display-Namen bzw. einen zur SIP-ID identischen Eintrag (z. B. T-Online). Mit den Zugangsdaten wird die Leitung (Einzel-Account, Trunk, Link, Gateway) angemeldet, nicht jedoch einzelne lokale Benutzer mit ihren individuellen Anmeldedaten. Wenn einzelne Benutzer (SIP, ISDN, Analog) mit den dort oder auf dem Endgerät hinterlegten Daten bei einer übergeordneten Instanz registriert werden sollen, muss eine SIP-PBX-Leitung eingerichtet werden.

Authentifizier.-Name

Name zur Authentifizierung an der übergeordneten SIP-Gegenstelle (Provider/SIP-TK-Anlage).

Mit den Zugangsdaten wird die Leitung (Einzel-Account, Trunk, Link, Gateway) angemeldet, nicht jedoch einzelne lokale Benutzer mit ihren individuellen Anmeldedaten. Wenn einzelne Benutzer (SIP,

ISDN, Analog) mit den dort bzw. auf dem Endgerät hinterlegten Daten bei einer übergeordneten Instanz registriert werden sollen, muss eine SIP-PBX-Leitung eingerichtet werden.

Passwort

Das Passwort zur Authentifizierung beim SIP-Registrar und SIP-Proxy des Providers. Bei Leitungen ohne (Re-)Registrierung kann das Passwort unter Umständen entfallen.

Mit den Zugangsdaten wird die Leitung (Einzel-Account, Trunk, Link, Gateway) angemeldet, nicht jedoch einzelne lokale Benutzer mit ihren individuellen Anmeldedaten. Wenn einzelne Benutzer (SIP, ISDN, Analog) mit den dort oder auf dem Endgerät hinterlegten Daten bei einer übergeordneten Instanz registriert werden sollen, muss eine SIP-PBX-Leitung eingerichtet werden.

Anruf-Präfix

Das Anruf-Präfix ist eine Nummer, die das Gerät den Anrufer-Nummern (CLI; SIP "From:") allen ankommenden Anrufern auf dieser SIP-Leitung voranstellt, um eindeutige Rückruf-Nummern zu erzeugen.

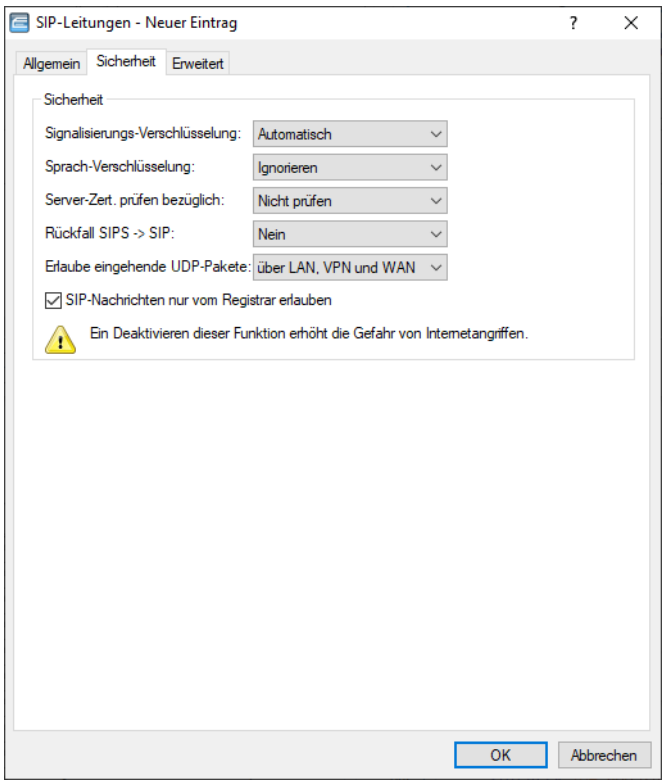
Beispielsweise ergänzen Sie hier eine Nummer, die der Call-Router bei abgehenden Rufen (dem Rückruf) zur Leitungsauswahl auswertet und anschließend wieder entfernt.

Interne Ziel-Nummer

Die Wirkung dieses Feldes hängt von der Einstellung des Modus der Leitung ab:

- Wenn der Modus der Leitung "Einzel-Account" ist, werden alle über die Leitung eingehenden Rufe mit dieser Nummer als Ruf-Ziel (SIP: "To:") an den Call-Router übergeben.
- Wenn der Modus "Trunk" ist, wird die Ziel-Nummer durch Entfernen der für den Trunk definierten Stammnummer ermittelt – falls dabei ein Fehler auftritt, wird der Ruf mit der in diesem Feld eingetragenen Nummer versehen (SIP: "To:") an den Call-Router übergeben.
- Wenn der Modus auf "Gateway" oder "Link" eingestellt ist, hat der Eintrag in diesem Feld keine Wirkung.

Auf dem Reiter **Sicherheit** haben Sie die folgenden Konfigurationsmöglichkeiten:



Signalisierungs-Verschlüsselung

Diese Einstellung legt das Protokoll zur Signalisierungs-Verschlüsselung (SIP/SIPS) bei der Kommunikation mit dem Provider fest.

Automatisch

Zur DNS-Auflösung werden NAPTR (Naming Adress Pointer)-Records verwendet. Der Provider gibt in den DNS-Daten die Verwendung des Transportprotokolls wie UDP, TCP oder TLS vor. Ebenso können Gewichte bzw. Prioritäten durch den Provider vorgegeben werden.

Wenn TLS als Transportprotokoll zur Signalisierungsverschlüsselung durch NAPTR vorgegeben wird, wird automatisch auch Sprachverschlüsselung verwendet, unabhängig von der expliziten Konfigurationseinstellung der Sprachverschlüsselung.

Keine (UDP)

Alle SIP Pakete werden verbindungslos übertragen. Die meisten Anbieter unterstützen diese Einstellung.

Keine (TCP)

Alle SIP Pakete werden verbindungsorientiert übertragen. Das Gerät baut eine TCP Verbindung zum Provider auf und erhält diese für die Dauer der Registrierung aufrecht. Spezielle Anbieter, wie z. B. Anbieter von Trunk Anschlüssen, unterstützen oder erzwingen diese Einstellung.

TLS

Gleiche Übertragungsweise wie bei TCP, allerdings werden alle SIP Pakete zusätzlich durch eine Verschlüsselung bis zum Provider geheim gehalten. Die jeweils in der Konfiguration ausgewählte TLS-Version wird als minimale Anforderung für die TLS-Verschlüsselung verwendet.

Sprach-Verschlüsselung

Diese Einstellung legt fest, ob und wie Sprachdaten (RTP/SRTP) bei der Kommunikation mit dem Provider verschlüsselt werden.

Sprach-Verschlüsselung

Ablehnen	Eine Verschlüsselung wird bei ausgehenden Gesprächen nicht angeboten. Eingehende Gespräche mit einem Verschlüsselungsvorschlag werden abgelehnt. Der Sprachkanal ist nicht verschlüsselt.
Ignorieren	Eine Verschlüsselung wird bei ausgehenden Gesprächen nicht angeboten. Eingehende Gespräche mit einem Verschlüsselungsvorschlag werden akzeptiert. Der Sprachkanal ist nicht verschlüsselt.
Bevorzugt	Eine Verschlüsselung wird bei ausgehenden Gesprächen angeboten. Eingehende Gespräche ohne einen Verschlüsselungsvorschlag werden akzeptiert. Der Sprachkanal ist nur dann verschlüsselt, wenn auch die Gegenstelle eine Verschlüsselung unterstützt.
Erzwingen	Eine Verschlüsselung wird bei ausgehenden Gesprächen angeboten. Eingehende Gespräche ohne Verschlüsselungsvorschlag werden abgelehnt. Der Sprachkanal ist entweder verschlüsselt oder wird nicht aufgebaut.

Sollen Sprachdaten verschlüsselt übertragen werden, ist es erforderlich, dass auch die Signalisierung über einen verschlüsselten Kanal erfolgt. Beachten Sie aber bitte, dass die Nutzung von SRTP keine Ende-zu-Ende Verschlüsselung garantiert.

Server-Zert. prüfen bezüglich:

Mit dieser Einstellung legen Sie fest, ob das Zertifikat des SIP-Servers auf bestimmte Certificate Authorites (CAs) überprüft werden soll. Die CA Zertifikate von global bekannten Zertifikatsketten werden durch LCOS Updates aktualisiert und können zusätzlich durch Truststore Updates manuell auf einen aktuellen Stand gebracht werden.

Server Zertifikat

Nicht prüfen	Das Serverzertifikat wird nicht überprüft. Alle gültigen Serverzertifikate werden akzeptiert, egal von welcher CA sie unterzeichnet wurden. Insbesondere werden somit selbst-signierte Zertifikate akzeptiert.
Allen vertrauten CAs	Das Serverzertifikat wird gegen alle dem Gerät bekannten CAs geprüft. Dazu zählen alle im LCOS als vertrauenswürdig bekannte CAs und jene aus den VoIP Server Zertifikats Slots 1 bis 3. Nur wenn die Verbindung mit einem dieser Zertifikate erfolgreich überprüft wurde, wird die verschlüsselte Verbindung aufgebaut.
VoIP Zert.-Slot 1	Es wird überprüft, ob das Serverzertifikat von einer CA unterzeichnet wurde, deren Zertifikat in Slot 1 der VoIP Zertifikate hochgeladen wurde.
VoIP Zert.-Slot 2	Es wird überprüft, ob das Serverzertifikat von einer CA unterzeichnet wurde, deren Zertifikat in Slot 2 der VoIP Zertifikate hochgeladen wurde.
VoIP Zert.-Slot 3	Es wird überprüft, ob das Serverzertifikat von einer CA unterzeichnet wurde, deren Zertifikat in Slot 3 der VoIP Zertifikate hochgeladen wurde.
Telekom-Shared-Business-CA4	Mit dieser Einstellung akzeptiert das Gerät nur Serverzertifikate, die von der Telekom Shared Business CA4 CA unterzeichnet wurden. Verwenden Sie diese Einstellung für Telekom SIP-Trunk Anschlüsse.

Rückfall SIPS > SIP

Nein

Es wird kein Rückfall auf eine unverschlüsselte Verbindung durchgeführt. Kann eine verschlüsselte Verbindung zum VoIP-Provider nicht aufgebaut werden, so bleibt die Leitung unregistriert.

UDP

In der Regel werden verschlüsselte SIP-Verbindungen über das TCP-Protokoll und unverschlüsselte Verbindungen über das UDP-Protokoll hergestellt. Mit dieser Einstellung wird direkt auf eine unverschlüsselte UDP-Verbindung gewechselt, wenn die verschlüsselte TCP-Verbindung nicht aufgebaut werden kann.

Komplett

Wird eine verschlüsselte TCP-Verbindung mit der konfigurierten TLS-Version nicht aufgebaut, dann wird zunächst versucht, eine unverschlüsselte TCP- und zuletzt eine UDP-Verbindung aufzubauen, um die VoIP-Leitung zu registrieren.



Diese Einstellung bietet die beste Kompatibilität, führt aber unter Umständen zu einer längeren Registrierungszeit.

Erlaube eingehende UDP-Pakete

Wenn die Providerleitung UDP zur Kommunikation mit dem Registrar verwendet, empfängt Sie UDP-Pakete auf dem gewünschten lokalen Port. Mit dieser Einstellung definieren Sie, in welchen Netzwerk-Kontext ein UDP-Paket akzeptiert wird. Ein Paket aus dem WAN / VPN / LAN akzeptiert das Gerät nur, wenn Sie die entsprechende Einstellung aktiviert haben. Andernfalls wird das Paket verworfen.

SIP-Nachrichten nur vom Registrar erlauben (Strikt-Modus)

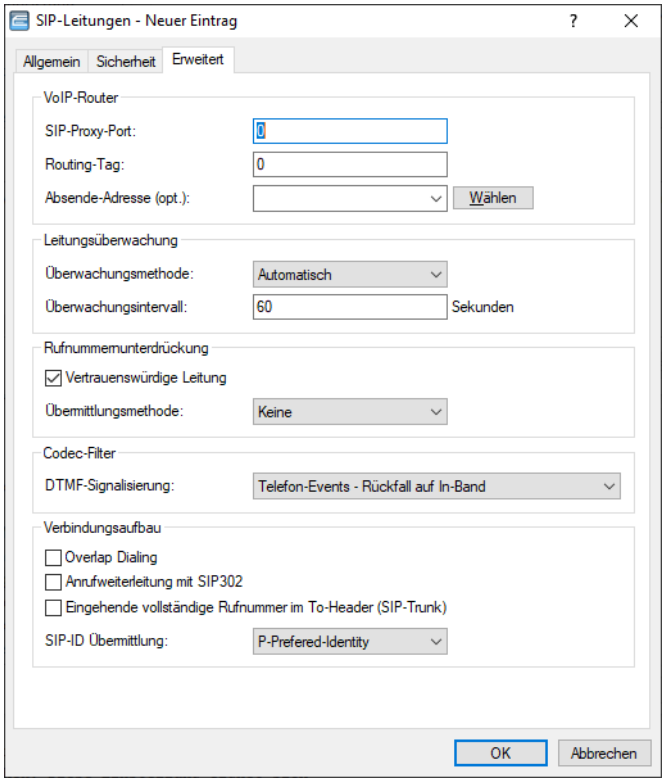
Wird dieser Modus aktiviert, werden eingehende SIP-Nachrichten nur von den IP-Adressen akzeptiert, die bei DNS-Auflösung der / des Domain / Registrars vom Provider gemeldet wurden.

Sollte der VoIP-Provider Rufe von IP-Adressen signalisieren, die nicht in der DNS-Auflösung der / des Domain / Registrars enthalten waren, werden eingehende Rufe nicht an den internen Teilnehmer signalisiert.



Ein Deaktivieren dieser Funktion erhöht die Gefahr von Internetangriffen. Von einem Angreifer gesendete SIP-Messages können zu Rufaufbauten und damit zu ungewollten Kosten führen. SIP-Messages, die so zu internen Clients weitergeleitet werden, können unter Umständen Sicherheitslücken bei den Endgeräten ausnutzen.

Auf dem Reiter **Erweitert** konfigurieren Sie den SIP-Proxy, die Leitungsüberwachung sowie die Rufnummernunterdrückung.



SIP-Proxy-Port

Dies ist der lokale Port des Geräte-SIP-Proxys zur Kommunikation mit der Gegenstelle.

Standardmäßig ist hier „0“ eingestellt. Dadurch wird der Port dynamisch aus dem Pool der freien Portnummern gewählt. Die Angabe eines Ports im Bereich von „1“ bis „65535“ ist ebenfalls möglich.

Routing-Tag

Dieses Routing-Tag dient zur Auswahl einer bestimmten Route über die Routing-Tabelle für Verbindungen zu diesem SIP-Server.

Absende-Adresse

Das Gerät ermittelt automatisch die richtige Absende-IP-Adresse für das Zielnetzwerk. Wollen Sie stattdessen eine fest definierte Absende-IP-Adresse verwenden, tragen Sie diese symbolisch oder direkt hier ein.

Überwachungsmethode

Spezifiziert die Methode der Leitungsüberwachung. Die Leitungsüberwachung prüft die Verfügbarkeit einer SIP-Provider-Leitung. Der Status der Überwachung kann im Call Router zum Wechsel auf eine Backup-Leitung herangezogen werden. Die Überwachungsmethode legt fest, wie der Status geprüft wird. Mögliche Werte sind:

Automatisch

Die Methode wird automatisch ermittelt (Default).

Deaktiviert

Keine Überwachung. Die Leitung wird stets als verfügbar gemeldet, wenn die Option (Re-)Registrierung deaktiviert ist. Andernfalls gilt sie erst nach erfolgreicher Registrierung als verfügbar. In dieser Einstellung kann die tatsächliche Verfügbarkeit der Leitung nicht überwacht werden.

Register

Überwachung mittels Register-Requests während des Registrierungsvorgangs. Für die Nutzung dieser Einstellung muss für diese Leitung ebenfalls die **(Re-)Registrierung** aktiviert sein.

Options

Überwachung mittels Options-Requests. Dabei wird wie bei einem Polling regelmäßig eine Anfrage an die Gegenstelle verschickt, je nach Antwort wird die Leitung als verfügbar oder nicht verfügbar angesehen. Diese Einstellung eignet sich z. B. für registrierungslose Leitungen.

Überwachungsintervall

Das Intervall der Leitungsüberwachung in Sekunden. Dieser Wert wirkt sich auf die Leitungsüberwachung mit Option-Request aus. Das Überwachungsintervall muss mindestens 60 Sekunden betragen und legt fest, nach welcher Zeit die Überwachungsmethode erneut angewendet wird.

Vertrauenswürdige Leitung

Spezifiziert die Zugehörigkeit der Gegenstelle dieser Leitung (Provider) zur "Trusted-Area". In dieser vertrauenswürdigen Zone wird die Caller ID als Information über den Gesprächsteilnehmer nicht entfernt, selbst wenn das durch Einstellungen in der Leitung (CLIR) oder durch das Endgerät gewünscht ist. Bei einer Verbindung über eine vertrauenswürdige Leitung wird die Caller ID entsprechend der ausgewählten Privacy-Methode übertragen und erst in der letzten Vermittlungsstelle vor dem entfernten Gesprächsteilnehmer entfernt. Innerhalb der vertrauenswürdigen Zone kann so z. B. die Caller ID für Abrechnungszwecke ausgewertet werden. Diese Funktion ist u. a. für Provider interessant, die mit einem VoIP-Router direkt beim Kunden das von ihnen selbst verwaltete Netzwerk bis zum Anschluss der VoIP-Endgeräte ausdehnen.

Bitte beachten Sie, dass diese Funktion nicht von allen Providern unterstützt wird.

Übermittlungsmethode

Spezifiziert die verwendete Methode zur Übermittlung der Caller ID im separaten SIP-Header-Feld. Mögliche Werte sind:

Keine

Ist standardmäßig eingestellt und bedeutet, dass keine Übertragung stattfindet.

RFC3325

Bedeutet Übermittlung mittels "P-Preferred-Id/P-Asserted-Id".

IETF-Draft-Sip-Privacy-04

Bedeutet Übermittlung konform zu "IETF-Draft-Sip-Privacy-04" mittels RPID (Remote Party ID).

DTMF-Signalisierung

Je nach Anforderung genügt es ggf. nicht, DTMF-Töne „inband" zu übertragen, wenn ein SIP-Empfänger diese Töne nicht erkennt. In diesem Fall ist die Konfiguration einer anderen DTMF-Übertragungsart für All-IP-Verbindungen möglich.

Nur In-Band (im Audio)

Die Übertragung erfolgt in Form von DTMF-Tönen (G.711) innerhalb des RTP-(Sprach-)Streams.

Nur SIP-Info

Die Übertragung der DTMF-Töne erfolgt „out-of-band" als SIP-Info-Nachricht mit den Parametern `Signal` und `Duration` (gem. RFC 2976). Eine parallele Übertragung als G.711-Töne erfolgt nicht.

Telefon-Events – Rückfall auf In-Band (Default)

Die Übertragung der DTMF-Töne erfolgt als speziell markierte Events innerhalb des RTP-Streams (gem. RFC 4733). Eine parallele Übertragung als G.711-Töne erfolgt nicht.

Falls die Verhandlung beim Call-Aufbau mit dem Kommunikationspartner im SDP keine `telephone-event`-Signalisierung enthält, erfolgt ein Rückfall auf Inband-Übertragung nach G.711.

Telefon-Events – Rückfall auf SIP-Info

Die Übertragung der DTMF-Töne erfolgt als speziell markierte Events innerhalb des RTP-Streams (gem. RFC 4733). Eine parallele Übertragung als G.711-Töne erfolgt nicht.

Falls die Verhandlung beim Call-Aufbau mit dem Kommunikationspartner im SDP keine `telephone-event`-Signalisierung enthält, erfolgt ein Rückfall auf eine Übertragung als SIP-Info-Nachricht.

Overlap Dialing

Mittels Overlap Dialing können Sie die Wartezeit zwischen gewählter Rufnummer und Rufaufbau deutlich verkürzen.

Ihr LANCOM Gerät verwendet bei deaktiviertem Overlap Dialing einen Overlap-Timer. Werksseitig ist er fest auf 6 Sekunden eingestellt. Falls Sie nach Ablaufen des Timers keine weitere Ziffer gewählt haben, so wird die bis dahin eingegebene Rufnummer als vollständig angesehen und der Ruf aufgebaut.

Ist Overlap Dialing für die Leitung aktiviert, werden schon vorab Teile der gewählten Rufnummer zum All-IP Provider geschickt.

Antwortet der All-IP Provider auf eine unvollständige Rufnummer mit einem "484 number incomplete", so sammelt der Voice Call Manager weiter gewählte Ziffern auf und schickt diese erneut zur Vermittlungsstelle.

Auf diese Weise kann ohne den 6 Sekunden Timer schnellstmöglich ein Ruf aufgebaut werden, wie Sie es von Ihrem ISDN-Anschluss gewohnt sind.

Da diese Funktionalität jedoch nicht von allen SIP-Providern unterstützt wird, ist das Overlap Dialing für jede einzelne SIP-Leitung zu konfigurieren.

Anrufweiterleitung mit SIP 302

Aktiviert die Rufumleitung beim SIP-Provider über SIP 302. Siehe auch *Rufumleitung (Call Deflection / Partial Rerouting) am SIP-Trunk (SIP 302)* auf Seite 1491.

SIP-ID Übermittlung

In diesem Feld kann eingestellt werden, wie die SIP-ID bei einem ausgehenden Telefonat bei Verwendung eines SIP-Trunks übertragen wird. Je nach Provider kann es erforderlich sein die SIP-ID über ein anderes Feld zu übertragen, da der Anruf ansonsten vom Provider abgelehnt wird.

Es können folgende Werte ausgewählt werden:

- P-Preferred-Identity (Standard-Wert)
- FROM
- Keine
- P-Preferred-Identity ohne DDI
- PPI-PPI
- Keine – PPI (P-Preferred-Identity)
- Keine – PAI (P-Asserted-Identity)

Bei Auswahl der Option **P-Preferred-Identity** (PAI-PPI)) wird die SIP-ID inklusive DDI über die PPI / PAI übertragen. Die Quellrufnummer wird über das FROM-Feld übertragen.

Bei Auswahl der Option **FROM** wird die SIP-ID über das FROM-Feld übertragen. Die Quellrufnummer wird über die PPI / PAI übertragen.

Mit der Einstellung **Keine** wird die SIP-ID nicht übermittelt. Die erste Calling Number wird im FROM, die Zweite im PPI / PAI übertragen.

Mit der Einstellung **P-Preferred-Identity ohne DDI** wird im Gegensatz zur P-Preferred-Identity eine eventuell vorhandene Durchwahl (DDI) nicht in der SIP-ID über die PPI übertragen.

Bei Auswahl der Option **PPI-PPI** (PPI) wird die SIP-ID inklusive DDI über die PPI übertragen. Die Quellrufnummer wird über das FROM-Feld übertragen.

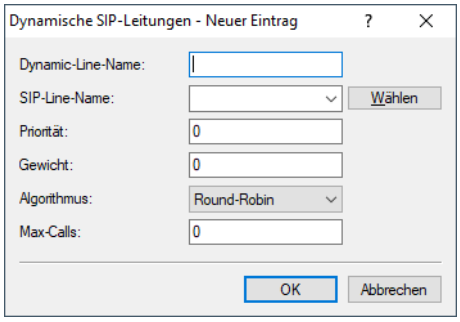
Mit der Einstellung **Keine – PPI (P-Preferred-Identity)** wird die SIP-ID nicht übermittelt. Die erste Calling Number wird im FROM, die Zweite im PPI übertragen.

Mit der Einstellung **Keine – PAI (P-Asserted-Identity)** wird die SIP-ID nicht übermittelt. Die erste Calling Number wird im FROM, die Zweite im PAI übertragen.

Bei einem Einzel-Account wird die SIP-ID bei einem ausgehenden Anruf immer über das **FROM**-Feld signalisiert.

16.4.2.2 Dynamische SIP-Leitungen

Die Konfiguration erfolgt über **Voice Call Manager** > **Leitungen** mit einem Klick auf die Schaltfläche **Dynamische SIP-Leitungen**.



Dynamic-Line-Name

Geben Sie hier den Namen der dynamischen Leitung an. Besteht die dynamische Leitung aus mehreren physikalischen Leitungen, verwenden Sie diesen dynamischen Leitungsnamen ebenfalls bei weiteren Tabelleneinträgen.Dieser dynamische Leitungsname kann später in der Callrouting Tabelle als Ziel-Leitung verwendet werden.

SIP-Line-Name

Wählen Sie hier eine der bereits konfigurierten physikalischen SIP-Verbindungen aus.

Priorität

Geben Sie hier die Priorität der physikalischen Leitung an, mit der die Leitung in der Verteilung ausgehender Rufe berücksichtigt werden soll.

Gewicht

Geben Sie hier die Gewichtung der physikalischen Leitung an, mit der die Leitung in der Verteilung ausgehender Rufe berücksichtigt werden soll.

Algorithmus

Der Algorithmus muss für alle Einträge, die zu einer dynamischen Leitung gehören, identisch konfiguriert werden. Dabei können folgende Algorithmen verwendet werden:

Gewicht

Mit diesem Algorithmus kann eine prozentuale Verteilung der Rufe auf verschiedene physikalische Leitungen bestimmt werden.

Round-Robin

Bei diesem Algorithmus werden ausgehende Rufe der Reihe nach auf die physikalischen Leitungen verteilt.

Priorität

Die physikalische Leitung mit der höchsten Priorität wird zunächst vollständig ausgelastet, bevor die physikalische Leitung mit der nächst niedrigeren Priorität verwendet wird.

Max-Calls

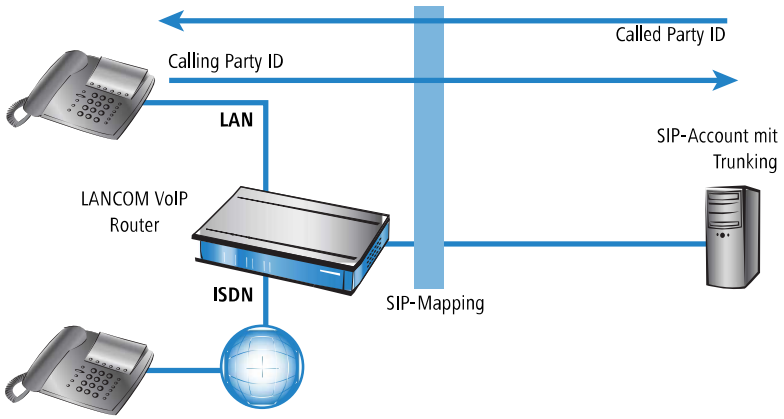
Geben Sie hier an, wie viele gleichzeitige Sprachkanäle auf der physikalischen SIP-Leitung möglich sind. Ist keine Beschränkung der Sprachkanäle notwendig, tragen Sie hier eine 0 ein.

16.4.2.3 SIP-Mapping

Mit den Einträgen für das SIP-Mapping wird in Form von Regeln eine Rufnummernumsetzung auf SIP-Leitungen im Trunk- oder Gateway-Modus eingerichtet.

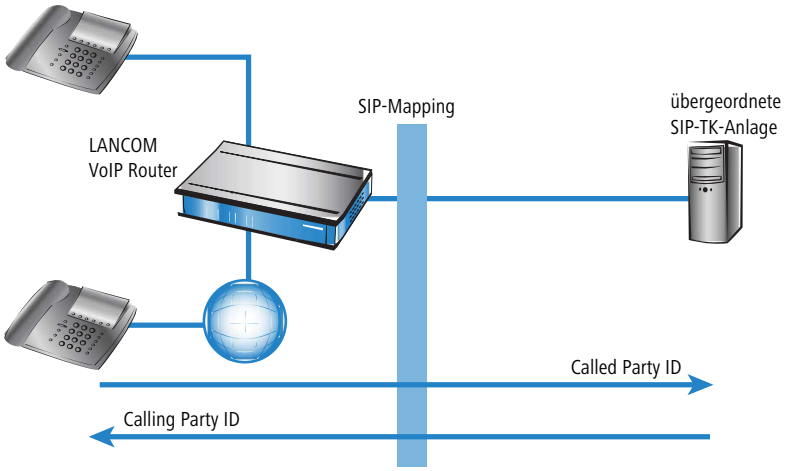
- Bei einer SIP-Leitung im Trunk-Modus wird eine Anpassung der intern verwendeten Rufnummern an den Rufnummernkreis des SIP-Accounts vorgenommen.
  - Bei ankommenden Rufen wird die Zielrufnummer (Called Party ID) verändert. Die interne Nummer wird eingesetzt, wenn die Called Party ID mit der externen Nummer übereinstimmt.
  - Bei abgehenden Rufen wird die Absenderrufnummer (Calling Party ID) verändert. Die externe Nummer wird eingesetzt, wenn die Calling Party ID mit der internen Nummer übereinstimmt.

Beim SIP-Mapping auf Trunk-Leitungen wird nur die Durchwahl (DDI) umgesetzt. Als Durchwahl werden alle über die Stammnummer (SIP-ID der SIP-Leitung) hinausgehenden Ziffern gewertet.

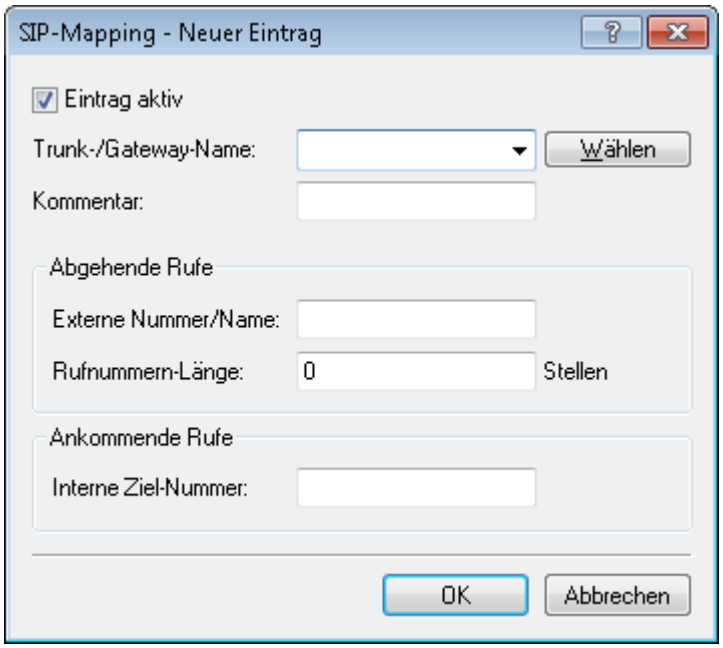


- Bei einer SIP-Leitung im Gateway-Modus wird eine Anpassung des Rufnummernplans der übergeordneten SIP-TK-Anlage an die internen Nummern des Call-Routers vorgenommen.
  - Bei ankommenden Rufen (von der SIP-Leitung) wird die Absenderrufnummer (Calling Party ID) verändert. Die interne Nummer wird eingesetzt, wenn die Calling Party ID mit der externen Nummer übereinstimmt.
  - Bei abgehenden Rufen (zur übergeordeten TK-Anlage) wird die Zielrufnummer (Called Party ID) verändert. Die externe Nummer wird eingesetzt, wenn die Called Party ID mit der internen Nummer übereinstimmt.

Beim SIP-Mapping auf Gateway-Leitungen wird die vollständige Rufnummer umgesetzt. Die Rufnummer an der ISDN-Schnittstelle kann je nach Konfiguration einer weiteren Umsetzung (ISDN-Mapping) unterworfen sein.



Das SIP-Mapping konfigurieren Sie unter **Voice Call Manager** > **Leitungen** mit einem Klick auf die Schaltfläche **SIP-Mapping**.



Eintrag aktiv

Aktiviert bzw. deaktiviert diesen Eintrag.

Trunk-/Gateway-Name

Name der Leitung, für welche die Rufnummernumsetzung gilt.

Kommentar

Kommentar zu dieser Regel.

Externe Nummer/Name

Rufnummer im Bereich des SIP-Trunk-Accounts bzw. im Bereich der übergeordneten SIP-TK-Anlage.

Rufnummern-Länge

Dieser Wert gibt an, nach wievielen Stellen eine gerufene Nummer als komplet angesehen wird. Er ist nur auf SIP-Gateway-Leitungen bei solchen Einträgen von Bedeutung, die mit einem #-Zeichen enden.

Bei einem abgehenden Ruf wird die von diesem Eintrag erzeugte externe Rufnummer automatisch nach der angegebenen Anzahl von Stellen als komplett betrachtet und weitergeleitet. Durch diesen Vorgang wird die Anwahl beschleunigt. Alternativ wird die Rufnummer als komplett betrachtet, wenn:

- der Benutzer ein #-Zeichen als Abschluss der Rufnummer wählt oder
- ein exakt passender Eintrag in der SIP-Mapping-Tabelle ohne #-Zeichen gefunden wurde oder
- die eingestellte Wartezeit abgelaufen ist.

Eine Rufnummern-Länge von '0' deaktiviert die vorzeitige Anwahl über die Rufnummernlänge.

Interne Ziel-Nummer

Rufnummer im Bereich des VoIP-Routers.

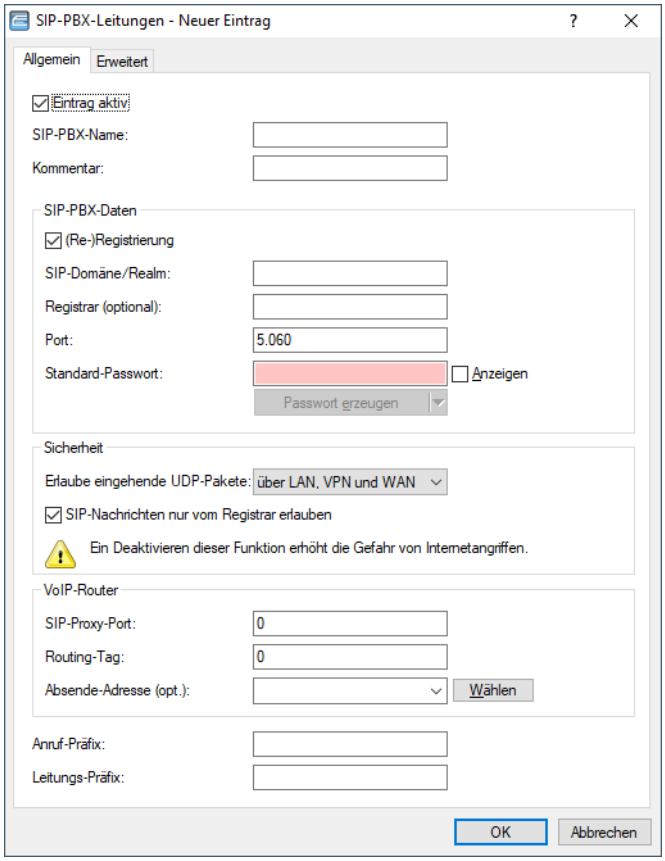
Mit dem #-Zeichen als Platzhalter können ganze Rufnummernblöcke in einer Regel erfasst werden.

16.4.2.4 SIP-PBX-Leitungen

Über diese Leitungen verbindet sich das Gerät mit übergeordneten SIP-TK-Anlagen. In der Regel erfolgt die Verbindung über VPN.

Die Konfiguration erfolgt über **Voice Call Manager** > **Leitungen** mit einem Klick auf die Schaltfläche **SIP-PBX-Leitungen**.

Auf dem Reiter **Allgemein** haben Sie die folgenden Konfigurationsmöglichkeiten:



Eintrag aktiv

Aktiviert bzw. deaktiviert diesen Eintrag.

SIP/PBX-Name

Name der Leitung. Darf nicht identisch sein mit einer anderen in dem Gerät konfigurierten Leitung (ISDN oder SIP-Provider oder SIP-PBX).

Kommentar

Kommentar zu diesem Eintrag.

(Re-)Registrierung

Hiermit aktivieren Sie die (wiederholte) Registrierung der SIP-PBX-Leitung. Mit einer aktivierten (Re-)Registrierung ist auch eine Leitungsüberwachung möglich.

Für die Nutzung der (Re-)Registrierung stellen Sie die Methode der Leitungsüberwachung in der Ansicht **Erweitert** entsprechend auf "Register". Das Gerät wiederholt die Registrierung jeweils nach Ablauf des Überwachungsintervalls. Wenn der SIP-Registrar der SIP-TK-Anlage ein anderes Intervall vorschlägt, übernimmt das Gerät dieses automatisch.

SIP-Domäne/Realm

SIP-Domäne/Realm der übergeordneten SIP-TK-Anlage.

Registrar (optional)

Der SIP-Registrar ist die Stelle, welche die Anmeldung mit den konfigurierten Authentifizierungsdaten für diesen Account in der SIP-TK-Anlage entgegen nimmt.

Outbound-Proxy (opt.)

Port

Port der übergeordneten SIP-TK-Anlage, an den das Gerät die SIP-Pakete sendet.

Achten Sie darauf, diesen Port in der Firewall freizuschalten, damit die Verbindung funktionieren kann.

Standard-Passwort

Gemeinsames Passwort zum Anmelden an der SIP-TK-Anlage. Dieses Passwort ist notwendig unter den folgenden Bedingungen:

- wenn sich SIP-Teilnehmer ohne eigene SIP-Zugangsdaten in der SIP-Benutzertabelle des Gerätes an der TK-Anlage anmelden sollen;
- wenn sich SIP-Benutzer ohne Passwort am Gerät anmelden können (keine lokale Authentifizierung), aber mit dem gemeinsamen Passwort Zugriff auf die übergeordnete SIP-TK-Anlage erhalten. Die Domäne der SIP-Benutzer muss in diesem Fall der Domäne der SIP-PBX-Line entsprechen.

Erlaube eingehende UDP-Pakete

Wenn die Providerleitung UDP zur Kommunikation mit dem Registrar verwendet, empfängt Sie UDP-Pakete auf dem gewünschten lokalen Port. Mit dieser Einstellung definieren Sie, in welchen Netzwerk-Kontext ein UDP-Paket akzeptiert wird. Ein Paket aus dem WAN / VPN / LAN akzeptiert das Gerät nur, wenn Sie die entsprechende Einstellung aktiviert haben. Andernfalls wird das Paket verworfen.

SIP-Nachrichten nur vom Registrar erlauben

Aktivieren Sie diese Checkbox, wenn Sie nur SIP-Nachrichten durch den Registrar zulassen wollen.

SIP-Proxy-Port

Dies ist der lokale Port des Geräte-Proxies zur Kommunikation mit der übergeordneten SIP-TK-Anlage. Ist diese Einstellung "0", erwartet das Gerät die Pakete der SIP-TK-Anlage am lokalen SIP-UDP-Server-Port (5060).

Zur beschleunigten Paketzuordnung konfigurieren Sie einen festen, eindeutigen, lokalen Port und tragen diesen als Zielport auch in der SIP-TK-Anlage ein.

Routing-Tag

Routing-Tag zur Auswahl einer bestimmten Route über die Routing-Tabelle für Verbindungen zu dieser SIP-TK-Anlage.

Absende-Adresse

Das Gerät ermittelt automatisch die richtige Absende-IP-Adresse für das Zielnetzwerk. Wollen Sie stattdessen eine fest definierte Absende-IP-Adresse verwenden, tragen Sie diese symbolisch oder direkt hier ein.

Anruf-Präfix

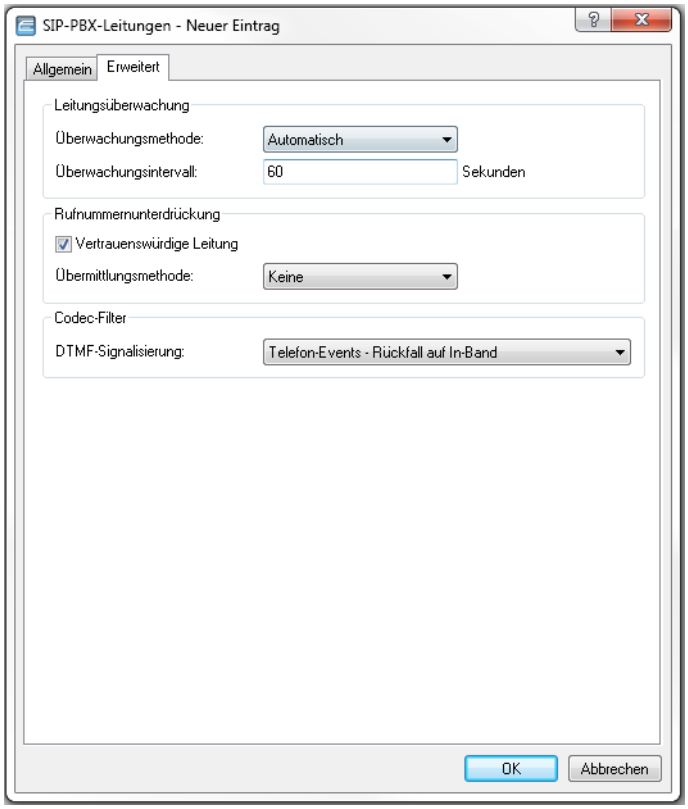
Das Anruf-Präfix ist eine Nummer, die das Gerät den Anrufer-Nummern (CLI; SIP "From:") allen ankommenden Anrufern auf dieser SIP-PBX-Leitung voranstellt, um eindeutige Rückruf-Nummern zu erzeugen.

Beispielsweise ergänzen Sie hier eine Nummer, die der Call-Router bei abgehenden Rufen (dem Rückruf) zur Leitungsauswahl auswertet und anschließend wieder entfernt.

Leitungs-Präfix

Bei ausgehenden Anrufen über diese Leitung stellt das Gerät der angerufenen Rufnummer dieses Präfix voran, um eine vollständige für diese Leitung gültige Rufnummer zu erzeugen. Bei ankommenden Rufen entfernt das Gerät dieses Präfix, falls vorhanden.

Auf dem Reiter **Erweitert** konfigurieren Sie die Leitungsüberwachung sowie die Rufnummernunterdrückung.



Überwachungsmethode

Spezifiziert die Methode der Leitungsüberwachung. Die Leitungsüberwachung prüft die Verfügbarkeit einer SIP-PBX-Leitung. Der Status der Überwachung kann im Call Router zum Wechsel auf eine Backup-Leitung herangezogen werden. Die Überwachungsmethode legt fest, wie der Status geprüft wird. Mögliche Werte sind:

Automatisch

Die Methode wird automatisch ermittelt.

Deaktiviert

Keine Überwachung. Die Leitung wird stets als verfügbar gemeldet. In dieser Einstellung kann die tatsächliche Verfügbarkeit der Leitung nicht überwacht werden.

Register

Überwachung mittels Register-Requests während des Registrierungsvorgangs. Für die Nutzung dieser Einstellung muss für diese Leitung ebenfalls die **(Re-)Registrierung** aktiviert sein.

Options

Überwachung mittels Options-Requests. Dabei wird wie bei einem Polling regelmäßig eine Anfrage an die Gegenstelle verschickt, je nach Antwort wird die Leitung als verfügbar oder nicht verfügbar angesehen. Diese Einstellung eignet sich z. B. für registrierungslose Leitungen.

Überwachungsintervall

Das Intervall der Leitungsüberwachung in Sekunden. Dieser Wert wirkt sich auf die Leitungsüberwachung mit Option-Request aus. Das Überwachungsintervall muss mindestens 60 Sekunden betragen und legt fest, nach welcher Zeit die Überwachungsmethode erneut angewendet wird.

Vertrauenswürdige Leitung

Spezifiziert die Zugehörigkeit der Gegenstelle dieser Leitung (Provider) zur "Trusted-Area". In dieser vertrauenswürdigen Zone wird die Caller ID als Information über den Gesprächsteilnehmer nicht entfernt, selbst wenn das durch Einstellungen in der Leitung (CLIR) oder durch das Endgerät gewünscht ist. Bei einer Verbindung über eine vertrauenswürdige Leitung wird die Caller ID entsprechend der ausgewählten Privacy-Methode übertragen und erst in der letzten Vermittlungsstelle vor dem entfernten Gesprächsteilnehmer entfernt. Innerhalb der vertrauenswürdigen Zone kann so z. B. die Caller ID für Abrechnungszwecke ausgewertet werden. Diese Funktion ist u. a. für Provider interessant, die mit einem VoIP-Router direkt beim Kunden das von ihnen selbst verwaltete Netzwerk bis zum Anschluss der VoIP-Endgeräte ausdehnen.

Bitte beachten Sie, dass diese Funktion nicht von allen Providern unterstützt wird.

Übermittlungsmethode

Spezifiziert die verwendete Methode zur Übermittlung der Caller ID im separaten SIP-Header-Feld. Mögliche Werte sind:

Keine

Ist standardmäßig eingestellt und bedeutet, dass keine Übertragung stattfindet.

RFC3325

Bedeutet Übermittlung mittels "P-Preferred-Id/P-Asserted-Id".

IETF-Draft-Sip-Privacy-04

Bedeutet Übermittlung konform zu "IETF-Draft-Sip-Privacy-04" mittels RPID (Remote Party ID).

DTMF-Signalisierung

Je nach Anforderung genügt es ggf. nicht, DTMF-Töne „inband" zu übertragen, wenn ein SIP-Empfänger diese Töne nicht erkennt. In diesem Fall ist die Konfiguration einer anderen DTMF-Übertragungsart für All-IP-Verbindungen möglich.

Nur In-Band (im Audio)

Die Übertragung erfolgt in Form von DTMF-Tönen (G.711) innerhalb des RTP-(Sprach-)Streams.

Nur SIP-Info

Die Übertragung der DTMF-Töne erfolgt „out-of-band" als SIP-Info-Nachricht mit den Parametern `Signal` und `Duration` (gem. RFC 2976). Eine parallele Übertragung als G.711-Töne erfolgt nicht.

Telefon-Events – Rückfall auf In-Band (Default)

Die Übertragung der DTMF-Töne erfolgt als speziell markierte Events innerhalb des RTP-Streams (gem. RFC 4733). Eine parallele Übertragung als G.711-Töne erfolgt nicht.

Falls die Verhandlung beim Call-Aufbau mit dem Kommunikationspartner im SDP keine `telephone-event`-Signalisierung enthält, erfolgt ein Rückfall auf Inband-Übertragung nach G.711.

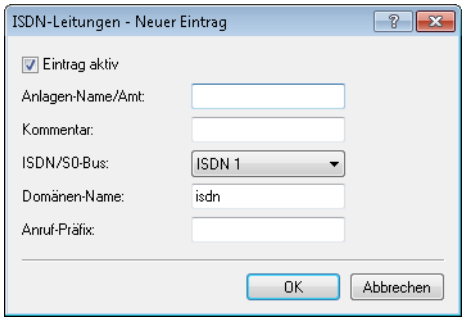
Telefon-Events – Rückfall auf SIP-Info

Die Übertragung der DTMF-Töne erfolgt als speziell markierte Events innerhalb des RTP-Streams (gem. RFC 4733). Eine parallele Übertragung als G.711-Töne erfolgt nicht.

Falls die Verhandlung beim Call-Aufbau mit dem Kommunikationspartner im SDP keine `telephone-event`-Signalisierung enthält, erfolgt ein Rückfall auf eine Übertragung als SIP-Info-Nachricht.

16.4.2.5 ISDN-Leitungen

Die ISDN-Leitungen konfigurieren Sie über **Voice Call Manager** > **Leitungen** mit einem Klick auf die Schaltfläche **ISDN-Leitungen**:



Eintrag aktiv

Aktiviert bzw. deaktiviert die ISDN-Leitung.

Anlagen-Name/Amt

Name der Leitung. Darf nicht identisch sein mit einer anderen im Gerät konfigurierten Leitung.

Kommentar

Kommentar zur Leitung

ISDN/S0-Bus

ISDN-Schnittstelle(n), über die das Gerät an das ISDN-Netz angeschlossen ist. Die eingetragenen Leitungen sind normalerweise als ISDN-TE konfiguriert.

Domänen-Name

Domäne, unter der das Gerät die Anrufe von der bzw. zur ISDN-Leitung in der SIP-Welt verwaltet.

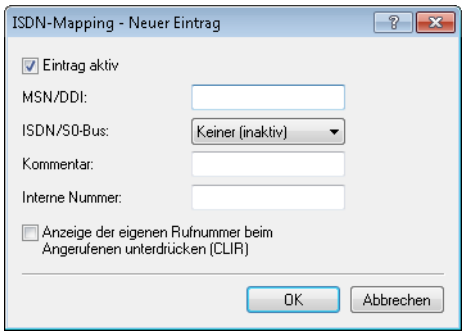
Anruf-Präfix

Das Anruf-Präfix ist eine Nummer, die das Gerät den Anrufer-Nummern (CLI; SIP "From:") allen ankommenden Anrufern auf dieser ISDN-Leitung voranstellt, um eindeutige Rückruf-Nummern zu erzeugen.

Beispielsweise ergänzen Sie hier eine Nummer, die der Call-Router bei abgehenden Rufen (dem Rückruf) zur Leitungsauswahl auswertet und anschließend wieder entfernt.

16.4.2.6 ISDN-Mapping

Mit dem ISDN-Mapping konfigurieren Sie eine Zuordnung von externen ISDN-Rufnummern (MSN oder DDI) zu den intern verwendeten Rufnummern. Klicken Sie dazu unter unter **Voice Call Manager** > **Leitungen** auf die Schaltfläche **ISDN-Mapping**.



Eintrag aktiv

Aktiviert bzw. deaktiviert die externe Telefonnummer.

MSN/DDI

Externe Telefonnummer des Anschlusses im ISDN-Netz.

Ankommende Anrufe von dieser MSN leitet das Gerät an die unten konfigurierte interne Nummer weiter. Bei ausgehenden Rufen ersetzt das Gerät die eigene Nummer durch die hier konfigurierte MSN.

- MSN: Nummer des Telefonanschlusses
- DDI (Direct Dialing in): Durchwahlnummer des Telefons, wenn der Anschluss als Anlagenanschluss konfiguriert ist.

Mit dem #-Zeichen als Platzhalter können Sie ganze Gruppen von Rufnummern erfassen, z. B. bei der Verwendung von Durchwahlnummern in einem einzigen Eintrag

ISDN/S0-Bus

ISDN-Schnittstelle(n), über die Endgeräte an das Gerät angeschlossen sind. Diese Leitungen müssen Sie als ISDN-NT konfigurieren.

Kommentar

Kommentar zur externen Telefonnummer

Interne Nummer

Interne Telefonnummer des ISDN-Telefons oder Name des Benutzers (SIP-URL).

Für ankommende Rufe ist das der SIP-Name oder interne Telefonnummer des Telefons, an das der Ruf von diesem Interface mit der zugehörigen MSN/DDI vermittelt wird. Für ausgehende Rufe wird der SIP-Name durch die MSN/DDI des zugehörigen Eintrages ersetzt.

Mit dem #-Zeichen als Platzhalter können Sie ganze Gruppen von Rufnummern erfassen, z. B. bei der Verwendung von Durchwahlnummern in einem einzigen Eintrag.

Anzeige der eigenen Rufnummer beim Angerufenen unterdrücken (CLIR)

Bei aktivierter Option unterdrückt das Gerät die eigene Rufnummer beim angerufenen Teilnehmer.

16.4.3 Konfiguration der Benutzer

Lokale Benutzer sind die am VoIP-Gerät angeschlossenen Endgeräte. Die Benutzer lassen sich in folgende Kategorien einteilen:

SIP-Benutzer

Benutzer, die über SIP an das LAN angeschlossen sind. Für die Konfiguration des Benutzers ist dabei unerheblich, ob das LAN lokal oder via VPN (über das Internet) erreichbar ist. Neben SIP-Telefonen haben Sie auch die Möglichkeit, eine SIP-TK-Anlage als Benutzer einzurichten (interne SIP-Trunk-Verbindung).

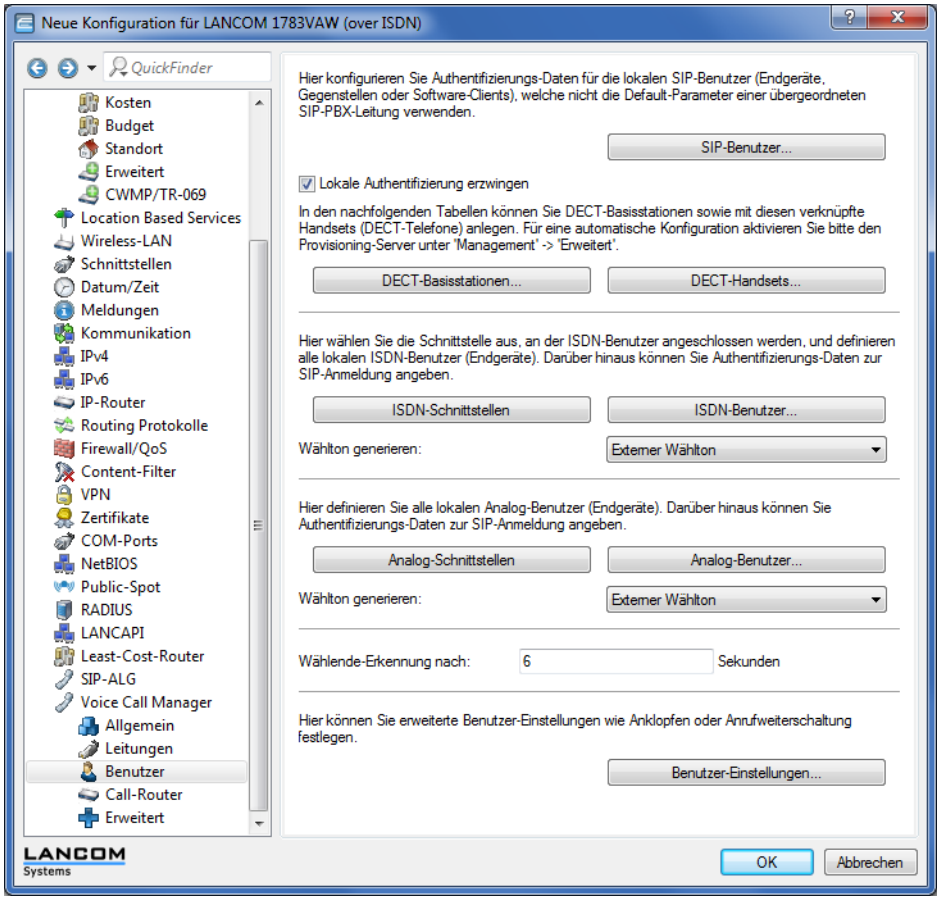
ISDN-Benutzer

Benutzer, die über ISDN angeschlossen sind. Diese Benutzer verwenden das SIP-Gateway, um über die VoIP-Funktion zu telefonieren.

Analog-Benutzer

Benutzer, die an die analogen Schnittstellen angeschlossen sind. Diese Benutzer verwenden das SIP-Gateway, um über die VoIP-Funktion zu telefonieren.

Die Benutzer konfigurieren Sie im LANconfig unter **Voice Call Manager** > **Benutzer**.



16.4.3.1 SIP-Benutzer

Normalerweise akzeptiert der SIP-Proxy Anmeldung von allen SIP-Benutzern, die sich mit einer gültigen Domain anmelden und als SIP-Benutzer im System bekannt sind. Wenn Sie unter **Voice Call Manager** > **Benutzer** im Abschnitt **SIP-Benutzer** die Option **Lokale Authentifizierung erzwingen** aktivieren, dann muss auch ein Passwort für den SIP-Benutzer eingetragen sein, das dann bei der Anmeldung überprüft wird.

Die Anmeldung ohne Eintrag eines Passworts ist auf die SIP-Benutzer im LAN beschränkt. SIP-Benutzer aus dem WAN und ISDN- sowie Analog-Benutzer müssen sich immer über das Passwort im entsprechenden Benutzer-Eintrag authentifizieren.

Über die Schaltfläche **SIP-Benutzer** konfigurieren Sie Authentifizierungsdaten der SIP-Benutzer (Endgeräte, Gegenstellen oder Software-Clients), die nicht die Default-Parameter einer übergeordneten SIP-PBX-Leitung verwenden.

Je nach Gerätemodell können Sie unterschiedlich viele SIP-Benutzer anlegen, wobei gleiche Namen oder gleiche Rufnummern nicht zugelassen sind.

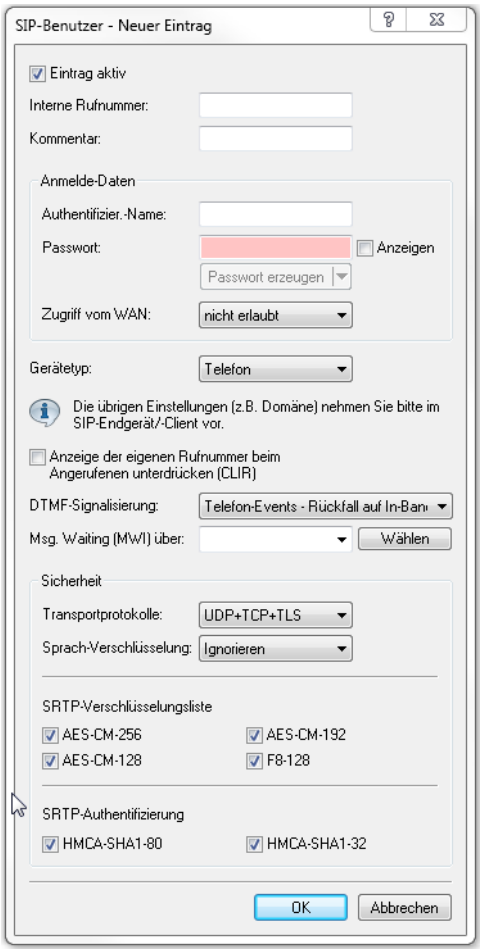


Abbildung 35: Neuen Eintrag in der SIP-Benutzer-Tabelle hinzufügen

Die vom SIP-Teilnehmer verwendete Domäne wird üblicherweise im Endgerät selbst eingestellt.

Eintrag aktiv

Aktiviert bzw. deaktiviert diesen Eintrag.

Interne Rufnummer

- Telefonnummer des SIP-Telefons
- Name des Benutzers (SIP-URI)
- Stammnummer der SIP-TK-Anlage, gefolgt von einem #. Ihre SIP-TK-Anlage muss sich dazu im selben Netz wie ihr Gerät befinden, wahlweise lokal oder via VPN (interne SIP-Trunk-Verbindung).

Kommentar

Kommentar zu diesem SIP-Benutzer.

Authentifizier.-Name

Name zur Authentifizierung am SIP-Proxy, ggf. auch an einer übergeordneten SIP-TK-Anlage, wenn die Domäne des Benutzers mit der Domäne einer SIP-PBX-Line übereinstimmt. Der Name wird benötigt, wenn eine

Anmeldung erforderlich ist (z. B. bei übergeordneter Anmeldung an einer SIP-TK-Anlage oder Setzen von **Lokale Authentifizierung erzwingen** für die SIP-Benutzer).

Passwort

Passwort zum Anmelden des SIP-Benutzers, ggf. auch an einer übergeordneten SIP-TK-Anlage, wenn die Domäne des Benutzers mit der Domäne einer SIP-PBX-Line übereinstimmt. Es ist möglich, dass sich Benutzer lokal am SIP-Proxy ohne Authentifizierung anmelden (**Lokale Authentifizierung erzwingen** für SIP-Benutzer ist deaktiviert) und ggf. an einer übergeordneten SIP-TK-Anlage mit einem gemeinsamen Passwort (**Standard-Passwort** an der SIP-PBX-Leitung) anmelden.

Zugriff vom WAN

Zugriffsrecht für die Anmeldung von SIP-Benutzern über eine WAN-Verbindung. Mögliche Werte sind:

- nicht erlaubt (Default)
- nur über VPN

Gerätetyp

Bestimmen Sie, welchen Gerätetyp SIP-Benutzer verwendet.

Anzeige der eigenen Rufnummer beim Angerufenen unterdrücken

Schaltet die Übermittlung der Absenderinformationen ein oder aus.

DTMF-Signalisierung

Je nach Anforderung genügt es ggf. nicht, DTMF-Töne „inband" zu übertragen, wenn ein SIP-Empfänger diese Töne nicht erkennt. In diesem Fall ist die Konfiguration einer anderen DTMF-Übertragungsart für All-IP-Verbindungen möglich.

Nur In-Band (im Audio)

Die Übertragung erfolgt in Form von DTMF-Tönen (G.711) innerhalb des RTP-(Sprach-)Streams.

Nur SIP-Info

Die Übertragung der DTMF-Töne erfolgt „out-of-band" als SIP-Info-Nachricht mit den Parametern `Signal` und `Duration` (gem. RFC 2976). Eine parallele Übertragung als G.711-Töne erfolgt nicht.

Telefon-Events – Rückfall auf In-Band (Default)

Die Übertragung der DTMF-Töne erfolgt als speziell markierte Events innerhalb des RTP-Streams (gem. RFC 4733). Eine parallele Übertragung als G.711-Töne erfolgt nicht.

Falls die Verhandlung beim Call-Aufbau mit dem Kommunikationspartner im SDP keine `telephone-event`-Signalisierung enthält, erfolgt ein Rückfall auf Inband-Übertragung nach G.711.

Telefon-Events – Rückfall auf SIP-Info

Die Übertragung der DTMF-Töne erfolgt als speziell markierte Events innerhalb des RTP-Streams (gem. RFC 4733). Eine parallele Übertragung als G.711-Töne erfolgt nicht.

Falls die Verhandlung beim Call-Aufbau mit dem Kommunikationspartner im SDP keine `telephone-event`-Signalisierung enthält, erfolgt ein Rückfall auf eine Übertragung als SIP-Info-Nachricht.

Msg. Waiting (MWI) über

Die Benachrichtigung über hinterlassene Sprachnachrichten auf Ihrer Provider-Mailbox im Netz erfolgt über eine Signalisierung am Endgerät. Je nach Endgerät erfolgt die Signalisierung auf unterschiedliche Weise. Wählen Sie unter **Voice Call Manager** > **Leitungen** > **SIP-Benutzer** aus den konfigurierten SIP-Leitungen die entsprechende Leitung aus, für die diese Funktion aktiviert werden soll.

Eine Benachrichtigung erfolgt nur, sofern diese Funktion vom Provider unterstützt wird.

Transportprotokolle

Wählen Sie ein Protokoll, mit dem dieser Benutzer mit dem lokalen SIP-Server kommunizieren darf. SIP-Anforderungen von diesem Benutzer werden mit einer SIP-Fehlerantwort (SIP/406) abgelehnt, sofern das entsprechende Protokoll nicht ausgewählt ist. Hierdurch wird sichergestellt, dass sich kein Benutzer über ein hier nicht erlaubtes Protokoll registrieren kann.

UDP

Alle SIP-Pakete an diesen SIP-Benutzer werden über das verbindungslose UDP übertragen. Die meisten SIP-Benutzer unterstützen diese Einstellung.

TCP

Alle SIP-Pakete an diesen SIP-Benutzer werden über das verbindungsorientierte TCP übertragen. Die TCP-Verbindung bleibt für die Dauer der Registrierung bestehen.

TLS

Alle SIP-Pakete an diesen SIP-Benutzer werden verbindungsorientiert übertragen. Zusätzlich werden alle SIP-Pakete verschlüsselt.

Sprach-Verschlüsselung

Legen Sie mit diesem Eintrag fest, über welches Protokoll die Sprachdaten eines Anrufes (RTP/SRTP) an den lokalen SIP-Server übermittelt werden.

Ablehnen

Es erfolgt kein Verschlüsselungsvorschlag bei Gesprächen für diesen Benutzer. Gespräche von diesem Benutzer mit Verschlüsselungsvorschlag werden abgelehnt. Der Sprachkanal ist niemals verschlüsselt.

Ignorieren

Es erfolgt kein Verschlüsselungsvorschlag bei Gesprächen für diesen Benutzer. Allerdings werden Gespräche von diesem Benutzer auch mit Verschlüsselungsvorschlag akzeptiert. Der Sprachkanal ist jedoch niemals verschlüsselt.

Bevorzugt

Es erfolgt ein Verschlüsselungsvorschlag bei Gesprächen für diesen Benutzer. Es werden auch Gespräche ohne Verschlüsselungsvorschlag von diesem Benutzer akzeptiert. Der Sprachkanal ist nur dann verschlüsselt, wenn der Benutzer Verschlüsselung unterstützt.

Erzwingen

Es erfolgt ein Verschlüsselungsvorschlag bei Gesprächen für diesen Benutzer. Gespräche von diesem Benutzer ohne entsprechenden Verschlüsselungsvorschlag werden ignoriert. Der Sprachkanal ist entweder verschlüsselt oder wird nicht aufgebaut.

Wenn Sie Sprachdaten sicher verschlüsselt übertragen möchten, ist es erforderlich, auch die Signalisierung über einen verschlüsselten Kanal zu übertragen. Andernfalls ist es u.U. möglich, dass die Schlüssel für die Sprachdaten im Falle eines Angriffes aus der ungesicherten Signalisierung ausgelesen werden. Beachten Sie, dass Ihr Provider möglicherweise Ihre Sprachdaten entschlüsselt und neu verschlüsselt oder unverschlüsselt weitervermittelt. Die Nutzung von SRTP garantiert keine Ende-zu-Ende-Verschlüsselung!

SRTP-Verschlüsselungsliste

Geben Sie hier an, mit welchem Verschlüsselungsverfahren die Kommunikation mit dem Benutzer verschlüsselt werden soll. Wählen Sie dazu eine oder mehrere der folgenden Methoden aus:

AES-CM-256

Die Verschlüsselung erfolgt mittels AES256. Die Schlüssellänge beträgt 256 Bit.

AES-CM-128

Die Verschlüsselung erfolgt mittels AES128. Die Schlüssellänge beträgt 128 Bit.

AES-CM-192

Die Verschlüsselung erfolgt mittels AES192. Die Schlüssellänge beträgt 192 Bit.

F8-128

Die Verschlüsselung erfolgt mittels F8-128. Die Schlüssellänge beträgt 128 Bit.

SRTP-Authentifizierung

Mit dieser Einstellung schränken Sie die verhandelte Menge der (vorgeschlagenen oder akzeptierten) SRTP Suites mit dem entsprechenden Benutzer ein. Sollten Sie eine oder mehrere der folgenden Cipher zur Verschlüsselung von SRTP Paketen nicht ausgewählt haben, schlägt das Gerät die entsprechenden SRTP Suites niemals vor und werden niemals ausgewählt. So erzwingen Sie die bestmögliche Verschlüsselung.

HMAC-SHA1-80

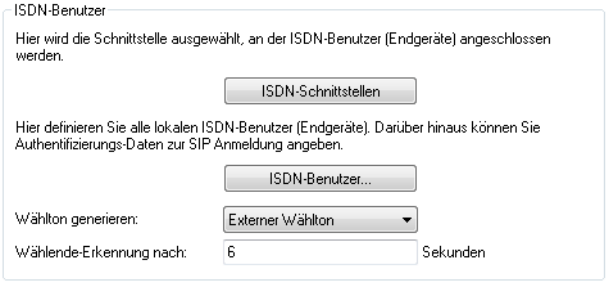
Die Authentifizierung des SIP-Benutzers erfolgt mit dem Hash-Algorithmus HMAC-SHA1-80. Die Hash-Länge beträgt 80 Bit.

HMAC-SHA1-32

Die Authentifizierung des SIP-Benutzers erfolgt mit dem Hash-Algorithmus HMAC-SHA1-32. Die Hash-Länge beträgt 32 Bit.

16.4.3.2 Allgemeine Einstellungen für alle ISDN-Benutzer

Unter **Voice Call Manager** > **Benutzer** konfigurieren Sie im Abschnitt **ISDN-Benutzer** allgemeine Einstellungen für alle ISDN-Benutzer.



Wählton generieren

Der Wählton bestimmt, welchen Ton ein ISDN-Benutzer nach dem Abheben des Hörers hört. Der "interne Wählton" gleicht dem Ton, den ein Benutzer an einer TK-Anlage ohne spontane Amtsholung hört (drei kurze Töne gefolgt von einer Pause). Der "externe Wählton" gleicht folglich dem Ton, der nach dem Abheben ein Amt anzeigt (anhaltender Ton ohne Unterbrechungen). Passen Sie den Wählton nach Bedarf an die Verwendung der spontanen Amtsholung für die entsprechenden Benutzer an, um ein ähnliches Verhalten wie an einem externen Anschluss zu simulieren.

Wählende-Erkennung nach

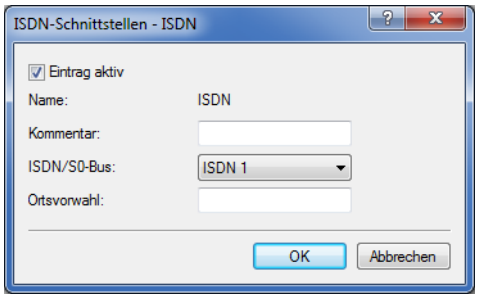
Für diese Dauer in Sekunden wartet das Gerät bei der Wahl von einem ISDN-Telefon auf weitere Ziffern, bevor es eine Nummer als vollständig annimmt und in Richtung SIP absendet.

Beim Eintrag '0' muss der ISDN-Benutzer jede Nummer mit dem '#'-Zeichen abschließen.

Das '#'-Zeichen dient auch dazu, die hier konfigurierte Wartezeit zu verkürzen.

16.4.3.3 ISDN-Schnittstellen

Konfigurieren Sie mit einem Klick auf die Schaltfläche **ISDN-Schnittstellen** global die zu verwendenden Schnittstellen für die ISDN-Benutzer. Es kann ein ISDN-NT-Interface (extern) oder auch ein ISDN-TE-Interface (intern) konfiguriert werden. Letzteres ist der Fall, wenn Benutzer einer übergeordneten TK-Anlage als lokale Benutzer verwaltet werden sollen.



Eintrag aktiv

Aktiviert bzw. deaktiviert diesen Eintrag.

Name

Interface, an das die ISDN-Teilnehmer angeschlossen sind.

Kommentar

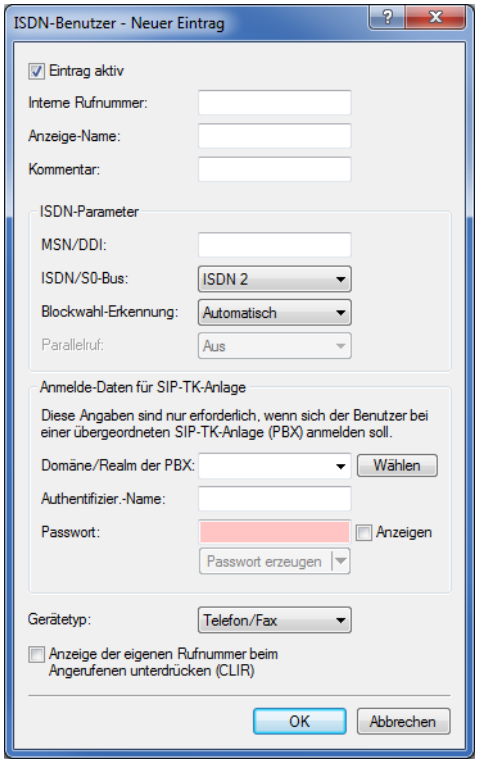
Kommentar zu diesem Eintrag.

ISDN/S0-Bus

Schnittstellen, die die ISDN-Benutzer für einen Verbindungsaufbau verwenden sollen.

16.4.3.4 ISDN-Benutzer

Die Konfiguration der entsprechenden ISDN-Benutzer erfolgt mit einem Klick auf die Schaltfläche **ISDN-Benutzer**.



Eintrag aktiv

Aktiviert bzw. deaktiviert diesen Eintrag.

Interne Rufnummer

Interne Rufnummer des ISDN-Telefons oder Name des Benutzers (SIP-URI).

Mit dem #-Zeichen als Platzhalter können Sie ganze Gruppen von Rufnummern z. B. bei der Verwendung von Durchwahlnummern an einem Anlagenanschluss in einem einzigen Eintrag erfassen.

Sie können Benutzereinträge mit #-Zeichen zur Abbildung von Benutzergruppen nicht für eine Anmeldung an einer übergeordneten TK-Anlage verwenden. Für diese Anmeldung ist immer ein spezifischer Eintrag für den einzelnen ISDN-Benutzer notwendig.

Anzeige-Name

Name, der auf dem angerufenen Telefondisplay erscheinen soll.

Kommentar

Kommentar zu diesem Eintrag.

MSN/DDI

Interne MSN, die für diesen Benutzer auf dem internen ISDN-Bus verwendet wird.

- MSN: Nummer des Telefonanschlusses, wenn es sich um einen Mehrgeräteanschluss handelt.
- DDI (Direct Dialing in): Durchwahlnummer des Telefons, wenn der Anschluss als Anlagenanschluss konfiguriert ist.

Mit dem #-Zeichen als Platzhalter können Sie ganze Gruppen von Rufnummern erfassen, z. B. bei der Verwendung von Durchwahlnummern an einem Anlagenanschluss in einem einzigen Eintrag.

Sie können Benutzereinträge mit #-Zeichen zur Abbildung von Benutzergruppen nicht für eine Anmeldung an einer übergeordneten TK-Anlage verwenden. Für diese Anmeldung ist immer ein spezifischer Eintrag für den einzelnen ISDN-Benutzer notwendig.

ISDN/S0-Bus

ISDN-Interface, das die Benutzer für den Verbindungsaufbau verwenden sollen.

Blockwahl-Erkennung

Bei Blockwahl kann das Gerät die gewählte Nummer automatisch als vollständig markieren. Dies hat zur Folge, dass das Gerät einen Anruf schneller aufbaut, wenn es eine beliebige Zifferngruppe als einen zusammenhängenden Block erkennt (z. B. bei Zielwahl). Sie haben dann allerdings nicht mehr die Möglichkeit nachzuwählen.

Parallelruf

Wenn Sie diese Funktion verwenden, erfolgt eine Signalisierung auf allen ausgewählten ISDN-Leitungen. Das Gespräch wird dort geführt, wo zuerst abgehoben wird.

Domäne/Realm der PBX

Domäne einer übergeordneten SIP-TK-Anlage, wenn der ISDN-Benutzer als SIP-Benutzer angemeldet werden soll. Die Domäne muss bei einer SIP-PBX-Line konfiguriert sein, damit eine übergeordnete Anmeldung erfolgt.

Authentifizier.-Name

Name zur Authentifizierung an einer übergeordneten SIP-TK-Anlage, wenn die Domäne des Benutzers mit der Domäne einer SIP-PBX-Line übereinstimmt.

Passwort

Passwort zum Anmelden als SIP-Benutzer an einer übergeordneten SIP-TK-Anlage, wenn die Domäne des ISDN-Benutzers mit der Domäne einer SIP-PBX-Line übereinstimmt. Es ist möglich, dass sich ISDN-Benutzer an einer übergeordneten SIP-TK-Anlage mit einem gemeinsamen Passwort (**Standard-Passwort** an der SIP-PBX-Line) anmelden.

Gerätetyp

Typ des angeschlossenen Gerätes.

Anzeige der eigenen Rufnummer beim Angerufenen unterdrücken (CLIR)

Schaltet die Übermittlung der Absenderinformationen ein oder aus.

16.4.3.5 Allgemeine Einstellungen für alle Analog-Benutzer

LANconfig: **Voice Call Manager** > **Benutzer**

Wählton generieren

Der Wählton bestimmt, welchen Ton ein Analog-Benutzer nach dem Abheben des Hörers hört. Der "interne Wählton" gleicht dem Ton, den ein Benutzer an einer TK-Anlage ohne spontane Amtsholung hört (drei kurze Töne gefolgt von einer Pause). Der "externe Wählton" gleicht folglich dem Ton, dass nach dem Abheben ein Amt anzeigt (anhaltender Ton ohne Unterbrechungen). Passen Sie den Wählton nach Bedarf an die Verwendung der spontanen Amtsholung für die entsprechenden Benutzer an, um ein ähnliches Verhalten wie an einem externen Anschluss zu simulieren.

Analog-Schnittstellen

Die internen Analog-Schnittstellen (a/b-Ports) müssen für die Verwendung durch lokale Benutzer (Anschluss von Endgeräten) konfiguriert werden.

LANconfig: **Voice Call Manager** > **Benutzer** > **Analog-Schnittstellen**

Interface

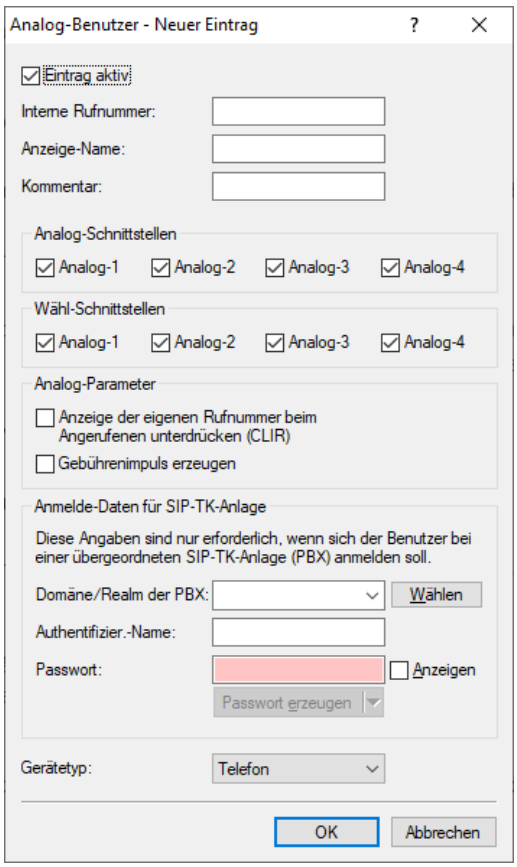
Ein internes Interface, an das Analog-Teilnehmer angeschlossen sind.

Eintrag aktiv

Interface ist aktiv / nicht aktiv.

Analog-Benutzer

LANconfig: **Voice Call Manager** > **Benutzer** > **Analog-Benutzer**



Eintrag aktiv

Aktiviert oder deaktiviert den Eintrag.

Interne Rufnummer

Interne Rufnummer des Analog-Telefons oder Name des Benutzers (SIP-URI).

Anzeige-Name

Name, der auf dem angerufenen Telefondisplay erscheinen soll.

Kommentar

Kommentar zu diesem Eintrag.

Analog-Schnittstellen

Wählen Sie die Analog-Schnittstellen aus, die bei einem Anruf an die **Interne Rufnummer** klingeln sollen.

Wähl-Schnittstellen

Wählen Sie eine Analog-Schnittstelle aus. Ein an dieser Schnittstelle angeschlossenes Analog-Telefon verwendet bei einem Telefonat die **Interne Rufnummer** als Quell-Rufnummer.

Anzeige der eigenen Rugnummer beim Angerufenen unterdrücken (CLIR)

Schaltet die Übermittlung der Absenderinformationen ein oder aus.

Gebührenimpuls erzeugen

Mit dem Gebührenimpuls (GBI) werden in analogen Telefonnetzen Informationen über die während einer Verbindung anfallenden Kosten zum Anrufer übermittelt. In dessen Endgerät (Telefon mit Gebührenanzeige, Gebührenanzeiger) wird der Gebührenimpuls aus dem übertragenen Gesamtsignal heraus gefiltert und in eine entsprechende Gebührenanzeige umgewandelt.

Mit dieser Option wird die Übertragung des Gebührenimpulses an den analogen Benutzer/das Endgerät ermöglicht. Dabei kann eine Gebühreninformation beispielsweise aus dem ISDN-Telefonnetz an eine ISDN-Leitung übermittelt und in einen analogen Gebührenimpuls umgesetzt werden.

Domäne/Realm der PBX

Domäne einer übergeordneten SIP-TK-Anlage, wenn der Analog-Benutzer als SIP-Benutzer angemeldet werden soll. Die Domäne muss bei einer SIP-PBX-Line konfiguriert sein, damit eine übergeordnete Anmeldung erfolgt.

Authentifizier.-Name

Name zur Authentifizierung an einer übergeordneten SIP-TK-Anlage, wenn die Domäne des Benutzers mit der Domäne einer SIP-PBX-Line übereinstimmt.

Secret

Passwort zum Anmelden als SIP-Benutzer an einer übergeordneten SIP-TK-Anlage, wenn die Domäne des Analog-Benutzers mit der Domäne einer SIP-PBX-Line übereinstimmt. Es ist möglich, dass sich ISDN-Benutzer an einer übergeordneten SIP-TK-Anlage mit einem gemeinsamen Passwort ("Standard-Passwort" an der SIP-PBX-Line) anmelden.

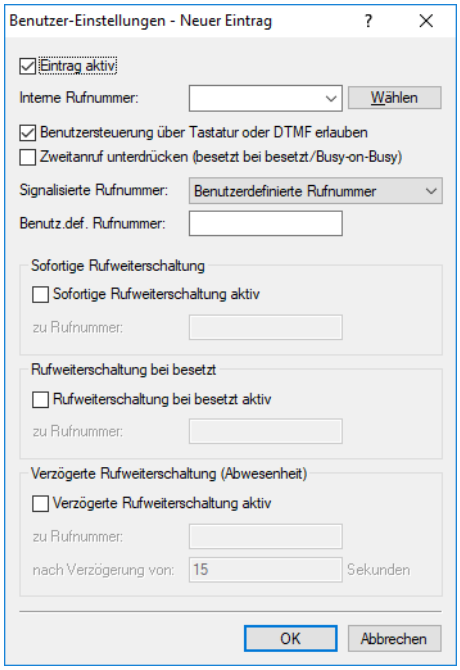
Gerätetyp

Typ des angeschlossenen Geräts.

Der Typ entscheidet, ob ggf. eine Umwandlung einer analogen Fax-Verbindung in SIP T.38 erfolgt. Bei Auswahl des Typs "Fax" oder "Telefon/Fax" wird eine Erkennung von Fax-Signalen aktiviert, die u. U. bei einem Telefon zu Beeinträchtigungen der Verbindungsqualität führen kann. Bitte wählen Sie daher den Typ entsprechend des angeschlossenen Gerätes, um die optimale Qualität zu erzielen.

16.4.3.6 Erweiterte Benutzer-Einstellungen

Die Konfiguration der erweiterten Benutzer-Einstellungen wie Anklopfen oder Anrufweiterschaltung erfolgt mit einem Klick auf die Schaltfläche **Benutzer-Einstellungen**.



Eintrag aktiv

Aktiviert bzw. deaktiviert diesen Eintrag.

Interne Rufnummer

Für diese Rufnummer bzw. diese SIP-ID gilt die Anrufweiterschaltung.

Anrufweiterschaltungen können für alle lokalen Benutzer (SIP, ISDN oder Analog) eingerichtet werden.

Benutzersteuerung über Tastatur oder DTMF erlauben

Aktiviert oder deaktiviert die Möglichkeit, die Benutzer-Einstellungen auch über das Telefon zu konfigurieren.

Zweitanruf unterdrücken (Busy on Busy)

Verhindert das Zustellen eines zweiten Anrufs zu einem Endgerät, unabhängig davon, ob "Anklopfen" (CW, Call Waiting Indication) auf dem Endgerät erlaubt oder unterbunden ist, d. h., diese Option verhindert auch das "Anklopfen". Zudem erhält der zweite Anrufende einen Besetzt-Ton. Dies gilt auch, wenn sich bei der internen Rufnummer um eine Mehrfachanmeldung handelt und nur mit einem der möglichen Endgeräte telefoniert wird.

Signalisierte Rufnummer

Einstellung der signalisierten Rufnummer. Mögliche Werte:

Weiterleitende Nummer

Signalisiert die Rufnummer, die den Anruf weiterleitet.

Anrufer

Signalisiert die eingehende Rufnummer. Bei der Weiterleitung an ein Handy kann ein Teilnehmer so die Original-Rufnummer des anrufenden Teilnehmers erkennen.

Benutzerdefinierte Rufnummer

Signalisiert die im Feld **Benutzerdefinierte Rufnummer** eingetragene Rufnummer.

Sofortige Rufweiterschaltung (CFU)

Aktiviert bzw. deaktiviert die sofortige Rufweiterschaltung (CFU) ohne Bedingung.

zu Rufnummer

Ziel für die sofortige Rufweiterschaltung ohne Bedingung.

Rufweiterschaltung bei besetzt (CFB)

Aktiviert bzw. deaktiviert die Rufweiterschaltung bei "besetzt".

zu Rufnummer

Ziel für die Rufweiterschaltung bei "besetzt".

Verzögerte Rufweiterschaltung (CFNR)

Aktiviert oder deaktiviert die verzögerte Rufweiterschaltung (bei Abwesenheit; CFNR).

zu Rufnummer

Ziel für die verzögerte Rufweiterschaltung.

nach Verzögerung von

Wartezeit für die verzögerte Rufweiterschaltung. Nach Ablauf dieser Zeit leitet das Gerät den Anruf an das Rufziel weiter, wenn der Teilnehmer den Anruf nicht annimmt.

16.5 Konfiguration des Call-Managers

Der Call-Manager verwaltet und verbindet die verschiedenen oben beschriebenen Teilnehmer und Leitungen miteinander. Die Kernaufgabe des Call-Managers besteht darin, für jeden anliegenden Anruf den richtigen Ziel-Teilnehmer zu ermitteln und eine passende Leitung zu diesem Teilnehmer auszuwählen. Um diese Aufgabe erfüllen zu können, verwendet der Call-Manager im Wesentlichen zwei Tabellenbereiche:

- Die Call-Routing-Tabelle
- Die Tabellen mit den lokalen Teilnehmern

Da der Call-Manager üblicherweise zwischen internen und externen Telefonnetzen mit unterschiedlichen Nummernbereichen vermittelt, muss der Call-Manager in einigen Fällen die gerufenen Nummern verändern, man spricht von der Rufnummernumsetzung.

In der Welt der VoIP-Telefonie können sowohl Rufnummern als auch Rufnamen (z. B. "mustermann@company.com") verwendet werden. Auch wenn in der folgenden Beschreibung meistens von Rufnummern die Rede ist, sind damit auch die Rufnamen gemeint, sofern nicht explizit anders angegeben.

Dabei wird das von Nebenstellen bekannte Verfahren mit internen Rufnummern verwendet, wobei Verbindungen zu nicht internen Teilnehmern mit einer vorangestellten '0' beginnen. Der Call-Manager verarbeitet Rufe von und zu allen angemeldeten Teilnehmern bzw. Leitungen.

16.5.1 Ablauf des Call-Routings

Die Vermittlung der Anrufe läuft in folgenden Schritten ab:

- Bearbeitung der rufenden Nummer (Called Party ID)

Zunächst wird überprüft, ob eine numerische oder alphanumerische Nummer vorliegt. Dazu werden typische Wahltrennzeichen wie "()-/" und <Blank> entfernt. Ein "+" an erster Stelle bleibt erhalten. In diesem Fall gilt die Nummer weiter als numerische Nummer. Wird bei der Prüfung ein anderes alphanumerisches Zeichen entdeckt, wird die Rufnummer als alphanumerisch betrachtet und bleibt unverändert.

- Auflösung des Rufes in der Call-Routing-Tabelle

  Nach der Bearbeitung der Called Party ID wird der Ruf an die Call-Routing-Tabelle übergeben. Die Einträge in der Call-Routing-Tabelle bestehen aus Sätzen von Bedingungen und Anweisungen. Die Einträge werden der Reihe nach durchsucht, der erste Eintrag wird ausgeführt, bei dem **alle** angegebenen Bedingungen erfüllt sind.

- Auflösung des Rufes über die Tabellen der lokalen Teilnehmer

  Wird in der Call-Routing-Tabelle kein Eintrag gefunden, der mit dem anliegenden Ruf übereinstimmt, sucht der Call-Manager in den Listen der lokalen Teilnehmer. Wird dort ein Eintrag gefunden, dessen Nummer mit der gerufenen Nummer übereinstimmt und der auch über die passende Zieldomain verfügt, dann wird dieser Ruf an den entsprechenden Teilnehmer zugestellt.

  Wird kein lokaler Teilnehmer gefunden, für den Nummer und Zieldomain übereinstimmen, reicht in einem weiteren Durchlauf auch die Übereinstimmung der Rufnummer des lokalen Teilnehmers mit der gerufenen Nummer, die Zieldomain bleibt ohne Berücksichtigung.

- Auflösung des Rufes über die Default-Einträge in der Call-Routing-Tabelle

  Falls die vorangehenden Durchläufe durch die Call-Routing-Tabelle und die Listen mit den lokalen Teilnehmern keinen Erfolg haben, wird der anliegende Ruf erneut in der Call-Routing-Tabelle geprüft. In diesem Durchlauf werden dann allerdings nur die Default-Routen berücksichtigt. Dabei werden die in den Default-Routen eingetragenen Nummern und Zieldomains nicht berücksichtigt. Nur die Quell-Filter werden ausgewertet, sofern die Default-Route über solche Filter verfügt.



Der hier vorgestellte Ablauf berücksichtigt nur die Rufnummern, wie sie vom Call-Router verarbeitet werden. Ein Mapping auf der ISDN- oder SIP-Leitung kann die Rufnummern ggf. zusätzlich verändern.

16.5.2 Behandlung der Calling Party ID

Die Konfigurationsmöglichkeiten des Call-Routers bieten zahlreiche Möglichkeiten, die für den Verbindungsaufbau verwendeten Rufnummern zu manipulieren. Darüber hinaus verbindet der Call-Router in der Regel verschiedene "Telefonwelten" (interne und externe, SIP und ISDN), die ganz unterschiedliche Rufnummernbereiche einsetzen. Zur erfolgreichen Kommunikation der Teilnehmer untereinander müssen die Rufnummern an den Schnittstellen der Vermittlung so umgesetzt werden, dass zum einen der gewünschte Teilnehmer über die richtige Leitung erreicht wird und zum anderen auch ein Rückruf (ggf. automatisch bei "besetzt") erfolgreich aufgebaut werden kann. Um diesen Rückruf zu ermöglichen, muss die rufende Nummer (Calling Party ID) **nach** der Bearbeitung durch den Call-Manager, direkt vor der Zustellung an den jeweiligen Teilnehmer angepasst werden.

16.5.2.1 Behandlung von abgehenden Rufen

Die Rufnummern von abgehenden Rufen werden je nach verwendeter Leitung umgesetzt:

SIP-Leitungen

Die Behandlung der Calling Party ID auf SIP-Leitungen ist abhängig vom Betriebs-Modus der Leitung:

- Einzel-Account: Bei einem abgehenden Ruf über eine SIP-Leitung wird die Calling Party ID auf die bei der SIP-Leitung eingetragene Nummer (SIP-ID) umgesetzt.
- Trunk und Gateway: Bitte beachten Sie die Informationen im Abschnitt SIP-Mapping.

SIP-PBX-Leitungen

Bei einem abgehenden Ruf über eine SIP-PBX-Leitung ist der Teilnehmer an der übergeordneten SIP-TK-Anlage angemeldet und Teil des dortigen Rufnummernbereiches. Daher wird die Calling Party ID – die in diesem Fall die interne Rufnummer oder "Durchwahl" des Teilnehmers darstellt – unverändert an die SIP-PBX-Leitung weitergegeben.

ISDN-Leitungen

Bei einem abgehenden Ruf über einen ISDN-Mehrgeräteanschluss wird die Calling Party ID auf die MSN umgesetzt, die für den Teilnehmer (bzw. die interne Rufnummer) in der ISDN-Mapping-Tabelle eingetragen ist.

Gibt es dort zu der aktuell rufenden Nummer keinen Eintrag, wird keine Calling Party ID gesendet. Bei aktiviertem CLIR (Calling Line Identifier Restriction) wird ebenfalls keine Calling Party ID gesendet.

16.5.2.2 Behandlung von eingehenden Rufen

Die Rufnummern von eingehenden Rufen werden nach den Kriterien SIP- oder ISDN-Teilnehmer sowie automatische Amtsholung aktiv oder nicht unterschiedlich umgesetzt.

Die Veränderung der Calling Party ID erfolgt abhängig von folgenden Parametern:

- Das bei der jeweiligen **Leitung** hinterlegte Präfix ("Anrufpräfix" oder "Cln-Prefix" – Default: <Leer>).
- Das Präfix für interne Verbindungen mit Ziel ISDN-User ("internes ISDN-Präfix" oder "Intern-Cln-Prefix" – Default: '99').
- Das Präfix für interne Verbindungen mit Ziel SIP-User ("internes SIP-Präfix" oder "Intern-Cln-Prefix" – Default: '99').
- Das Präfix für externe Verbindungen mit Ziel ISDN-User ("externes ISDN-Präfix" oder "Extern-Cln-Prefix" – Default: <leer>).
- Das Präfix für externe Verbindungen mit Ziel SIP-User ("externes SIP-Präfix" oder "Extern-Cln-Prefix" – Default: <leer>).

Die Aktivierung der automatischen Amtsholung wird durch eine geeignete Konfiguration der Präfixe berücksichtigt:

- Bei aktivierter automatischer Amtsholung werden die internen Präfixe typischerweise auf das Wählzeichen gesetzt, das zum Erreichen der internen Teilnehmer verwendet wird, also in der Regel '99' oder '*'.
- Ohne automatische Amtsholung werden die externen Präfixe typischerweise auf '0' gesetzt.

Die Erweiterung der Calling Party ID wird nur durchgeführt, wenn der eingehende Ruf über eine Calling Party ID verfügt. Ist die Calling Party ID leer, wird kein Präfix vorangestellt.

Die Veränderung läuft wie folgt ab:

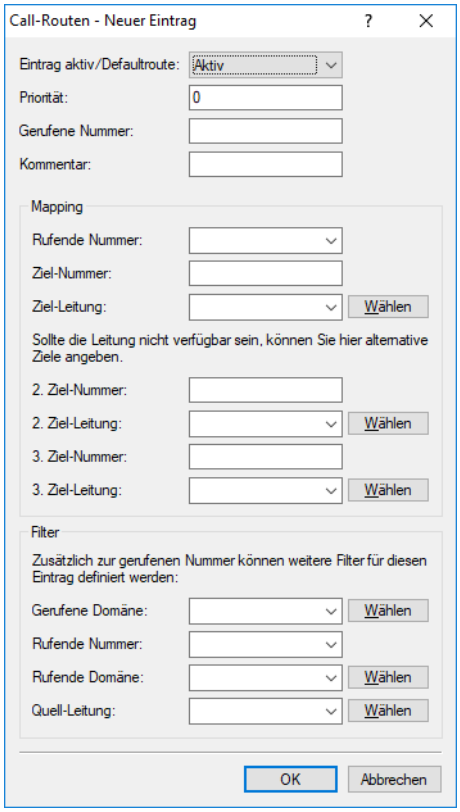
- Bei internen Verbindungen wird das interne Teilnehmer-Präfix (SIP oder ISDN) der Calling Party ID vorangestellt.
- Bei externen Verbindungen wird abhängig vom (Leitungs-)Anrufpräfix entschieden:
  - (Leitungs-)Anrufpräfix leer: es wird das externe Teilnehmer-Präfix (SIP oder ISDN) der Calling Party ID vorangestellt.
  - (Leitungs-)Anrufpräfix nicht leer: es werden das interne Teilnehmer-Präfix (SIP oder ISDN) **und** das (Leitungs-)Anrufpräfix der Calling Party ID vorangestellt.



Ein Ruf gilt dann als extern, wenn er von einer "Leitung" kommt. Wenn diese Leitung eine SIP-PBX Leitung ist, dann ist der Ruf nur dann extern, wenn die kommende Calling Party ID eine führende '0' hat.

16.5.3 Die Parameter der Call-Routing-Tabelle

Die Einträge der Call-Routing-Tabelle konfigurieren Sie im LANconfig unter **Voice-Call-Manager** > **Call-Router** mit einem Klick auf die Schaltfläche **Call-Routen**.



Ein Eintrag in der Call-Routing-Tabelle besteht aus:

- Bedingungen, die erfüllt sein müssen, damit der Eintrag als zutreffend "betrachtet" wird. Dazu gehören:
  - Die Information, welcher Teilnehmer angerufen werden soll – gerufene Nummer/Name (Called Party ID), ggf. gerufene Domain.
  - Informationen über den anrufenden Teilnehmer – rufende Nummer/Name, rufende Domain, Quell-Leitung, über die der Ruf in den LANCOM VoIP Router eingeht.
- Anweisungen, wie mit dem Ruf zu Verfahren ist:
  - Wie wird die Rufnummer umgesetzt und für die weitere Verarbeitung verändert?
  - Auf welcher Leitung soll der Ruf ausgegeben werden (Ziel-Leitung)?
  - Welche Backup-Leitungen sollen verwendet werden, wenn die Ziel-Leitung nicht verfügbar ist?

Die Einträge werden der Reihe nach durchsucht, der erste passende Eintrag wird ausgeführt. Daher sollten zuerst die speziellen Einträge konfiguriert werden, die allgemeinen Einträge dahinter.

Wird ein Eintrag in der Call Routing Tabelle gefunden mit der Ziel-Leitung "RESTART", dann beginnt mit der neuen, umgesetzten Called Party ID wieder der komplette Durchlauf. Dabei wird die Angabe der Quell-Leitung (Calling Line) für den nächsten Durchlauf gelöscht.

Sowohl die Call Routing Tabelle als auch die lokale Teilnehmertabelle können dabei soweit sinnvoll auch alphanumerische Namen enthalten und verarbeiten.

Eintrag aktiv/Defaultroute

Der Routingeintrag kann aktiviert, deaktiviert oder aber als Default-Eintrag gekennzeichnet werden. Alle über die ersten Durchläufe nicht über die Call-Routing-Tabelle bzw. lokale Teilnehmertabelle auflösbaren Anrufe werden dann automatisch über diese Default-Einträge aufgelöst. Zielname und Zieldomain sind dann beliebig, nur die ggf. gesetzten Quellfilter werden berücksichtigt.

Priorität

Der Call-Manager sortiert alle Einträge mit gleicher Priorität automatisch so, dass die Tabelle sinnvoll von oben nach unten durchlaufen werden kann. Bei einigen Einträgen muss jedoch (z. B. zur Rufnummernumsetzung) die Reihenfolge der Einträge vorgegeben werden. Die Einträge mit der höchsten Priorität werden automatisch nach oben sortiert.

Gerufene Nummer

Der gewählte Called Party Name bzw. die Ziel-Rufnummer (ohne Domänen-Angabe).

Das #-Zeichen wird als Platzhalter für beliebige Zeichenfolgen verwendet. Alle Zeichen vor dem '#' werden entfernt, die restlichen Zeichen werden im Feld "Nummer/Name" anstelle des #-Zeichens für den weiteren Verbindungsaufbau verwendet.

Beispiel: In der Call-Routing-Tabelle enthält ein Eintrag die '00049#' als gerufene Nummer/Name und die '00#' als Nummer/Name. Bei allen Rufen mit einer führenden Null für die Amtsholung und der kompletten Vorwahl für Deutschland wird als Nummer/Name nur die führende Null für die Amtsholung und die führende Null für die Ortsnetzvorwahl beibehalten, die Landeskennung wird entfernt. Aus '00049 2405 123456' wird also die '0 02405 123456'.

Unabhängig davon kann auch ein alphanumerischer Name angegeben werden.

Kommentar

Kommentar zum aktuellen Routing-Eintrag

Rufende Nummer

Wenn in der Call-Route die rufende Nummer gegen eine andere Rufnummer ersetzt werden soll, muss die gewünschte Rufnummer in diesem Feld eingetragen werden. Bei Auswahl des speziellen Wertes „EMPTY“ und gleichzeitigem ausfüllen des Filter-Feldes **Rufende Nummer** mit einem beliebigen Zeichen (z. B. der Wildcard #) kann für die Call-Route eine Rufnummernunterdrückung für abgehende Aurufe konfiguriert werden.

Ziel-Nummer

Diese Rufnummer wird für den weiteren Verbindungsaufbau verwendet. Kann über diese Rufnummer und die zugehörige Leitung keine Verbindung hergestellt werden, werden die Backup-Rufnummern mit den zugehörigen Leitungen verwendet.

Mindestens eines der Felder **Ziel/Nummer**, **2. Ziel-Nummer** oder **3. Ziel-Nummer** muss einen Inhalt haben. Die Auswertung erfolgt in dieser Reihenfolge. Ein leeres Feld wird übersprungen.

Ziel-Leitung

Über die Zielleitung wird die Verbindung aufgebaut. Normale Zielleitungen können sein:

- ISDN
- Alle definierten SIP Leitungen.

Folgende Sonderfunktionen können als Ziel-Leitung eingetragen werden:

- REJECT markiert eine gesperrte Rufnummer.

  Über diesen Wert können Sie auch *Steuerzeichen auf SIP-Leitungen verbieten*.

- USER leitet den Ruf an lokale SIP- bzw. ISDN-Teilnehmer weiter.

- RESTART beginnt mit der zuvor gebildeten **Ziel-Nummer** einen neuen Durchlauf in der Call-Routing-Tabelle. Dabei wird zuvor **Quell-Leitung** gelöscht.



Dieses Feld muss ausgefüllt werden, sonst wird der Eintrag nicht verwendet!

2. Ziel-Nummer, 3. Ziel-Nummer

Diese Rufnummer wird für den weiteren Verbindungsaufbau verwendet, wenn unter **Ziel-Nummer** nichts eingetragen ist oder die zugehörige "Leitung" nicht erreichbar ist. Kann über die 2. Ziel-Nummer und die zugehörige 2. Ziel-Leitung keine Verbindung hergestellt werden, werden die 3. Ziel-Nummer und die 3. Ziel-Leitung verwendet.

Gerufene Domäne

Dieser Eintrag filtert auf die gerufene Domäne, die "Called Party Domain". Der Call-Router-Eintrag wird nur dann als übereinstimmend gewertet, wenn die Called Party Domain des anliegenden Rufes mit der hier eingetragenen Domain übereinstimmt. Wird hier nichts angegeben, wird jede Zieldomäne akzeptiert.

Als gerufene Domäne können eingetragen werden:

- ISDN
- Die interne VoIP-Domäne des LANCOM VoIP Router.
- Alle bei den SIP- und SIP-PBX-Leitungen eingetragenen Domänen.

Rufende Nummer

Dieser Eintrag filtert auf die rufende Nummer/Name, die "Calling Party ID". Die Angabe erfolgt entweder als interne Nummer, nationale oder internationale Rufnummer. Die Domäne wird nicht mit angegeben. Es wird keine '0' oder anderes Zeichen für eine Leitungskennung vorangestellt, die ID wird wie von der Leitung bzw. wie von internen Rufen kommend verwendet.

Der Call-Router-Eintrag wird nur dann als übereinstimmend gewertet, wenn die Calling Party ID des anliegenden Rufes mit der hier eingetragenen Nummer übereinstimmt. Ab einem '#' können beliebige Ziffern akzeptiert werden. Wird hier nichts angegeben, wird jede Calling Party ID akzeptiert.



Die folgende Sonderfunktion kann als rufende Nummer eingetragen werden:

- EMPTY kann für nicht angegebene Calling Party IDs verwendet werden.

Rufende Domäne

Dieser Eintrag filtert auf die rufende Domäne, die "Calling Domain". Der Call-Router-Eintrag wird nur dann als übereinstimmend gewertet, wenn die Calling Domain des anliegenden Rufes mit der hier eingetragenen Domain übereinstimmt. Wird hier nichts angegeben, wird jede rufende Domäne akzeptiert.

Als rufende Domäne können eingetragen werden:

- ISDN
- Die interne VoIP-Domäne des LANCOM VoIP Router.
- Alle bei den SIP- und SIP-PBX-Leitungen eingetragenen Domänen.

SIP-Telefone verfügen üblicherweise über mehrere Leitungstasten, für die verschiedene Domänen konfiguriert werden können. Mit diesem Filter kann der Auswahl entsprechend eine bestimmte Behandlung der Rufe über unterschiedliche Leitungstasten vorgenommen werden.

Quell-Leitung

Dieser Eintrag filtert auf die Quell-Leitung. Der Call-Router-Eintrag wird nur dann als übereinstimmend gewertet, wenn die Quell-Leitung des anliegenden Rufes mit der hier eingetragenen Leitung übereinstimmt. Wird hier nichts angegeben, wird jede rufende Leitung akzeptiert.

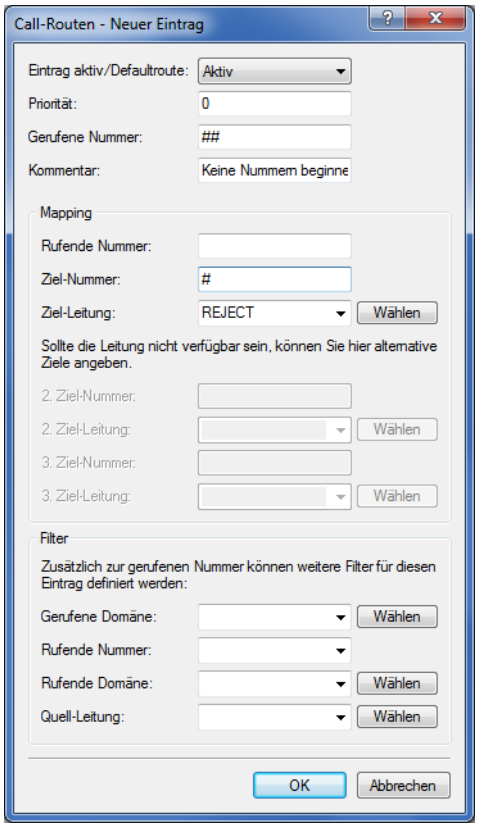
Als Quell-Leitung können eingetragen werden:

- USER.ISDN für Rufe eines lokalen ISDN-Teilnehmers
- USER.SIP für Rufe eines lokalen SIP-Teilnehmers
- USER.# für Rufe eines lokalen Teilnehmers allgemein
- Alle eingetragenen ISDN-, SIP- und SIP-PBX-Leitungen.

16.5.3.1 Steuercodes auf SIP-Leitungen verbieten

Hier verhindern Sie, dass Steuercodes gewählt werden können. Über Steuercodes können z. B. Rufumleitungen konfiguriert werden. Dies können Sie für beliebige Leitungen bzw. Mitarbeiter unterbinden. Um beispielsweise das Zeichen '#' abzuweisen, gehen Sie wie folgt vor:

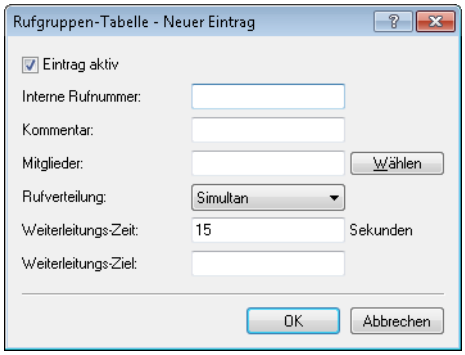
1. Tragen Sie in **Gerufene Nummer:** ## ein.
2. Tragen Sie in **Ziel-Nummer:** # ein.
3. Wählen Sie für **Ziel-Leitung** REJECT.
4. Machen Sie in **Kommentar:** z. B. den Eintrag "Keine Nummern beginnend mit #".



5. Übernehmen Sie Ihre Einstellungen durch einen Klick auf die Schaltfläche **OK**.

16.5.3.2 Gruppenruf-Funktionen

Die Einträge der Rufgruppen-Tabelle konfigurieren Sie im LANconfig unter **Voice-Call-Manager** > **Call-Router** mit einem Klick auf die Schaltfläche **Rufgruppen-Tabelle**.



Eintrag aktiv

Aktiviert bzw. deaktiviert den Eintrag.

Interne Rufnummer

Unter dieser Rufnummer bzw. dieser SIP-ID ist die Rufgruppe erreichbar (max. 64 alphanumerische Zeichen).

Namen für Rufgruppen dürfen nicht mit Namen von Benutzern (SIP, ISDN oder Analog) übereinstimmen.

Kommentar

Kommentar zu diesem Eintrag (max. 64 Zeichen).

Mitglieder

Komma-separierte Liste der Mitglieder dieser Rufgruppe. Als Mitglieder können Benutzer, Rufgruppen oder auch externe Rufnummern eingetragen werden, so dass eine unbegrenzte Skalierung möglich ist.

- Mögliche Mitglieder: Benutzer, Rufgruppen, externe Rufnummern
- Mögliche Werte: Maximal 128 alphanumerische Zeichen.

Rufgruppen können sich nicht selbst oder einen Vorgänger in der hierarchischen Struktur enthalten – es sind also keine Rekursionen durch den Eintrag der Mitglieder möglich! Schleifen zu einem Vorgänger in der Struktur sind jedoch über das Weiterleitungs-Ziel möglich.

Rufverteilung

Bestimmt die Art der Ruf-Verteilung:

- Simultan: Der Anruf wird aufgeteilt und an alle Gruppenmitglieder gleichzeitig weitergeleitet. Wenn ein Mitglied den Anruf innerhalb der Weiterleitungs-Zeit annimmt, wird die Anrufsignalisierung für die anderen Mitglieder beendet. Wenn kein Mitglied den Anruf innerhalb der Weiterleitungs-Zeit annimmt, wird der Anruf zum Weiterleitungs-Ziel weitergeleitet.
- Sequentiell: Der Anruf wird der Reihe nach an die Gruppenmitglieder weitergeleitet. Wenn ein Mitglied den Anruf innerhalb der Weiterleitungs-Zeit nicht annimmt, wird der Anruf an das jeweils folgende Mitglied weitergeleitet. Wenn auch das letzte Gruppenmitglied den Anruf innerhalb der Weiterleitungs-Zeit nicht annimmt, wird der Anruf zum Weiterleitungs-Ziel weitergeleitet.

Weiterleitungs-Zeit

Wenn ein anliegender Ruf von einem Gruppenmitglied nicht innerhalb der Weiterleitungs-Zeit angenommen wird, wird der Ruf je nach Art der Ruf-Verteilung weitergeleitet:

- Bei simultaner Ruf-Verteilung wird der Anruf zum Weiterleitungs-Ziel weitergeleitet.

- Bei sequentieller Ruf-Verteilung wird der Anruf an das nächste Gruppenmitglied in der gültigen Reihenfolge weitergeleitet. Wenn das Gruppenmitglied das letzte Mitglied der Reihenfolge ist, wird der Anruf an das Weiterleitungs-Ziel weitergeleitet.
- Mögliche Werte: Maximal 255 Sekunden.
- Default: 0 Sekunden
- Werte mit besonderer Bedeutung: 0 Sekunden. Der Ruf wird sofort zum Weiterleitungs-Ziel geleitet (temporäres Überspringen einer Rufgruppe in einer Hierarchie).

Sind alle Mitglieder der Gruppe besetzt oder aus anderen Gründen nicht erreichbar, wird der Anruf an das Weiterleitungs-Ziel weitergeleitet, ohne die Weiterleitungs-Zeit abzuwarten.

Weiterleitungs-Ziel

Wenn keines der Gruppenmitglieder den Anruf innerhalb der Weiterleitungs-Zeit annimmt, wird der Anruf an das hier eingetragene Weiterleitungs-Ziel weitergeleitet. Sowohl Benutzer, Rufgruppen als auch externe Rufnummern können als Weiterleitungs-Ziel eingetragen werden. Es kann dabei nur genau ein Weiterleitungs-Ziel angegeben werden.

- Mögliche Ziele: Benutzer, Rufgruppen, externe Rufnummern
- Mögliche Werte: Maximal 64 alphanumerische Zeichen.

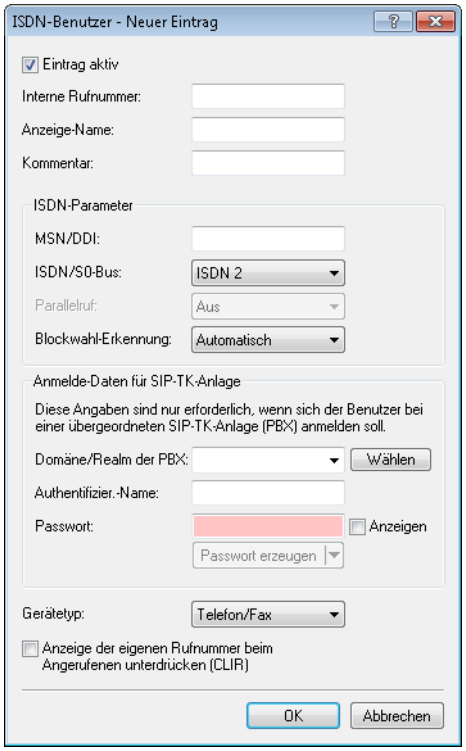
Wenn kein Weiterleitungs-Ziel angegeben wird, wird der Anruf zurückgewiesen, sobald die Liste der Mitglieder abgearbeitet ist bzw. wenn alle Mitglieder besetzt oder nicht erreichbar sind.

Das Weiterleitungs-Ziel wird erst aktiv, wenn die Weiterleitungs-Zeit der Gruppe vollständig abgelaufen ist bzw. kein Mitglied erreichbar ist. Aus diesem Grund sind hier auch Verweise auf eine höhere Stelle einer Rufgruppenstruktur möglich, anders als beim Eintrag der Mitglieder.

16.5.4 Parallelruf im ISDN signalisieren

Auf LANCOM Business VoIP Routern kann ein Parallelruf aktiviert werden. Wenn Sie diese Funktion verwenden, erfolgt eine Signalisierung auf beiden ISDN-Leitungen (ISDN 1 & ISDN 2). Das Gespräch wird dort geführt, wo zuerst abgehoben wird.

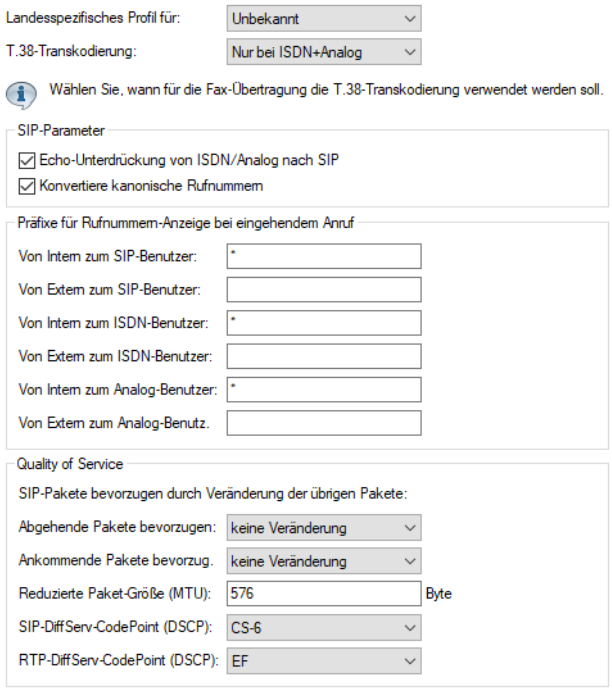
Aktivieren Sie den Parallelruf über **Voice Call Manager** > **Benutzer** > **ISDN-Benutzer**.



Wählen Sie im Abschnitt **ISDN-Parameter** unter **ISDN/S0-Bus** die Option „ISDN 1 & ISDN 2" und aktivieren Sie anschließend den **Parallelruf** mit der Einstellung „Ein".

16.5.5 Erweiterte Einstellungen

Die erweiterten Einstellungen für den Voice-Call-Manager konfigurieren Sie unter **Voice-Call-Manager** > **Erweitert**.



Landesspezifisches Profil für

Ermöglicht die Auswahl eines landesspezifischen Profils zur Voreinstellung der Eingabewerte.

Echo-Unterdrückung von SIP nach ISDN

Aktiviert die Echounterdrückung des fernen Echos. Bei einem zu starken Echo hört der Teilnehmer sich selber mit kurzer Verzögerung wieder. Mit der Aktivierung dieser Option wird das ISDN-Echo am SIP-ISDN-Gateway reduziert.

Präfix intern zu SIP-Benutzer

Dieses Präfix wird bei einem eingehenden, **internen** Anruf der vorhandenen Calling Party ID vorangestellt, wenn der Anruf an einen SIP-Benutzer gerichtet ist.

Ein Ruf gilt dann als extern, wenn er von einer "Leitung" kommt. Wenn diese Leitung eine SIP-PBX-Leitung ist, dann ist der Ruf nur dann extern, wenn die kommende Calling Party ID eine führende '0' hat. Alle anderen Anruf gelten als intern.

Präfix extern zu SIP-Benutzer

Dieses Präfix wird bei einem eingehenden, **externen** Anruf der vorhandenen Calling Party ID vorangestellt, wenn der Anruf an einen SIP-Benutzer gerichtet ist.

Präfix intern zu ISDN-Benutzer

Dieses Präfix wird bei einem eingehenden, **internen** Anruf der vorhandenen Calling Party ID vorangestellt, wenn der Anruf an einen ISDN-Benutzer gerichtet ist. Sofern ein Leitungspräfix definiert ist, wird dieses der gesamten Rufnummer vorangestellt.

Präfix extern zu ISDN-Benutzer

Dieses Präfix wird bei einem eingehenden, **externen** Anruf der vorhandenen Calling Party ID vorangestellt, wenn der Anruf an einen ISDN-Benutzer gerichtet ist. Sofern ein Leitungspräfix definiert ist, wird dieses der gesamten Rufnummer vorangestellt.

Präfix intern zu Analog-Benutzer

Dieses Präfix wird bei einem eingehenden, **internen** Anruf der vorhandenen Calling Party ID vorangestellt, wenn der Anruf an einen Analog-Benutzer gerichtet ist. Sofern ein Leitungspräfix definiert ist, wird dieses der gesamten Rufnummer vorangestellt.

Präfix extern zu Analog-Benutzer

Dieses Präfix wird bei einem eingehenden, **externen** Anruf der vorhandenen Calling Party ID vorangestellt, wenn der Anruf an einen Analog-Benutzer gerichtet ist. Sofern ein Leitungspräfix definiert ist, wird dieses der gesamten Rufnummer vorangestellt.

Abgehende Pakete bevorzugen

Für alle SIP-Gespräche wird abhängig vom verwendeten Audio-Codec eine ausreichende Bandbreite über die Firewall reserviert (soweit die verfügbare Bandbreite ausreicht). Zur Steuerung der Firewall kann hier die Behandlung der restlichen Datenpakete eingestellt werden, die nicht zu den SIP-Datenströmen gehören. Folgende Werte sind möglich:

- Reduktion der PMTU

  Die Teilnehmer der Datenverbindung werden informiert, dass sie nur Datenpakete bis zu einer bestimmen Länge versenden sollen (Path Maximum Transmission Unit, PMTU).

- Fragmentierung

  Der LANCOM Wireless Router reduziert selbst die Datenpakete durch Fragmentierung auf die gewünschte Länge.

- keine Veränderung (Default)

Die Länge der Datenpakete wird durch den VoIP-Betrieb nicht verändert.

Weitere Informationen finden Sie bei der Beschreibung von PMTU und Fragmentierung im Zusammenhang mit Quality-of-Service.

Ankommende Pakete bevorzugen

Analog zu den abgehenden Datenpakete wird hier die Behandlung der Nicht-VoIP-Datenpakete bei Bandbreitenreservierung für SIP-Daten eingestellt. Folgende Werte sind möglich:

- Reduktion der PMTU

  Die Teilnehmer der Datenverbindung werden informiert, dass sie nur Datenpakete bis zu einer bestimmen Länge versenden sollen (Path Maximum Transmission Unit, PMTU).

- keine Veränderung

  Die Länge der Datenpakete wird durch den VoIP-Betrieb nicht verändert.

Reduzierte Paket-Größe

Dieser Parameter gibt die Paketgröße an, die für die PMTU-Anpassung bzw. die Fragmentierung bei Bevorzugung der SIP-Daten verwendet werden soll.

SIP-DiffServ-CodePoint (DSCP), RTP-DiffServ-CodePoint (DSCP)

Der Voice-Call-Manager markiert SIP- und RTP-Pakete mit sogenannten DiffServ-CodePoints (DSCP), um es nachgeschalteter Hardware zu ermöglichen, diese Pakete zu erkennen und richtig zu priorisieren.

Standardmäßig werden SIP-Pakete (Anruf-Signalisierung) mit 'CS-1' und RTP-Pakete (Voice-Datenstrom) mit 'EF' markiert. Sie haben hier die Möglichkeit, dieses Verhalten zu ändern. Bei der Einstellung 'DSCP BE' bzw. 'CS-0' werden die Pakete ohne Markierung versendet Weitere Informationen zu den DiffServ-CodePoints finden Sie im Kapitel *Quality of Service*.

Die Verwendung von 'CS-1' für SIP-DSCP ist heute überholt und zur Erhaltung der Abwärts-Kompatibilität als Default gesetzt. Typische Werte für aktuellen VoIP-Installationen sind 'CS-3', 'AF-31' oder 'AF-41'. Wegen der großen Verbreitung im Markt empfehlen wir bei SIP-DSCP den Einsatz von 'CS-3'.

16.6 Telefoniefunktionen für LANCOM VoIP Router (PBX-Funktionen)

Ein LANCOM VoIP Router bietet Telefoniefunktionen für kleine Firmen oder verteilte Standorte von Filial-Unternehmen:

- Telefonfunktionen wie Halten, Makeln, Verbinden oder Anrufweiterschaltung ("Rufumleitung")
- Gruppenruf-Funktion mit flexibler Ruf-Verteilung und Kaskadierung von Rufgruppen
- Mehrfachanmeldung für die Nutzung verschiedener Telefone für eine Rufnummer

Bitte beachten Sie, dass der Umfang der Unterstützung von SIP inbesondere im Hinblick auf Verbinden und automatische Anrufweiterschaltung ("Rufumleitung") bei SIP-Endgeräten und SIP-Providern sehr unterschiedlich sein kann. Es kann nicht garantiert werden, dass diese Funktionen in jeder Konstellation aus SIP-Endgeräten und SIP-Providern wunschgemäß arbeiten.

16.6.1 Anrufweiterschaltung (Verbinden und Rufumleitung)

Mit der Integration von SIP-Telefonen und VoIP-Routern in die bestehenden Telefonstrukturen bedürfen auch die bekannten Funktionen wie die Anrufweiterschaltung einer neuen Betrachtung. Anrufweiterschaltung bedeutet, dass ein eigentlich zugestellter (gerouteter) Ruf entweder durch eine spontane Steuerung des Benutzers ("Verbinden") oder eine zuvor

eingestellte automatische Anrufweiterschaltung ("Rufumleitung") zu einem neuen Ziel weitergeleitet wird. Die SIP-basierte VoIP-Telefonie verwendet in einigen Bereichen grundsätzlich andere Verfahren als die bisher verwendeten Technologien. So benötigen ISDN- und Analog-Endgeräte z. B. für die Anrufweiterschaltung immer eine Vermittlungsstelle, die üblicherweise auch nach der Weiterschaltung die Verbindung weiterhin verwaltet. SIP-Telefone können auch ohne Vermittlungsstelle Anrufe weiterschalten: die Geräte bauen eine Verbindung auf dem kürzesten Weg auf, der Call Router beendet seine Verwaltungsfunktion nach dem Herstellen der Verbindung. Die SIP-Vermittlungsstelle kann dabei auch die Aspekte der Signalisierung über SIP und der eigentlichen Datenübertragung über RTP unterschiedlich behandeln.

Aufgrund solcher Unterschiede je nach Art der beteiligten Endgeräte ist es für das Verständnis der Anrufweiterschaltung in einem LANCOM VoIP Router hilfreich, die verschiedenen Szenarien zu betrachten und die verwendeten Begriffe vorzustellen.

16.6.1.1 Aktive und passive Weiterschaltung

Für die Betrachtung der technischen Details ist es von großer Bedeutung, von welcher Seite der Verbindung die Anrufweiterschaltung eingeleitet wird. Dabei gelten in diesem Zusammenhang als "lokal" alle SIP- sowie ISDN- oder Analog-Benutzer, die über den LANCOM VoIP Router im eigenen LAN erreicht werden können. "Extern" sind hingegen alle Endgeräte, die über eine Leitung (SIP-Account, SIP-Trunk, SIP-PBX, ISDN oder Analog) erreicht werden können.

- Aktiv: Ein lokaler Teilnehmer leitet die Weiterschaltung ein.
- Passiv: Ein externer Teilnehmer leitet die Weiterschaltung ein.

16.6.1.2 Anrufweiterschaltung mit und ohne Rückfrage

Der Teilnehmer, der die Anrufweiterschaltung einleitet, kann das aktive Gespräch entweder direkt an einen dritten Teilnehmer übergeben (Anrufweiterschaltung ohne Rückfrage – englisch "Unattended Call Transfer"), oder er kann zunächst ein Gespräch zu einem dritten Teilnehmer aufbauen und erst dann die Weiterschaltung einleiten (Anrufweiterschaltung mit Rückfrage – englisch "Attended Call Transfer").

LANCOM VoIP Router unterstützen die Anrufweiterschaltung ohne Rückfrage ausschließlich über das SIP-Protokoll.

16.6.1.3 Gesprächsgebühren bei Weiterschaltung zu externen Benutzern

Die Anrufweiterschaltung von einem externen Anrufer zu einem dritten, ebenfalls externen Anrufer birgt das Risiko, dass durch die Fortsetzung des Anrufes nach dem Auflegen durch den einleitenden Teilnehmer weiterhin Gebühren anfallen.

16.6.1.4 Aufgabe der LANCOM VoIP Router bei der Anrufweiterschaltung

In Abhängigkeit von den bei der Anrufweiterschaltung beteiligten Endgeräten kann ein LANCOM VoIP Router unterschiedliche Aufgaben übernehmen:

Durchleiten

Beide Teilnehmer der Anrufweiterschaltung sind auf der gleichen Seite der Verbindung, z. B. Weiterschaltung von einem lokalen zu einem weiteren lokalen Teilnehmer.

Delegieren

Die Anrufweiterschaltung wird nicht im LANCOM VoIP Router selbst, sondern in einer übergeordneten Vermittlungsstelle durchgeführt. z. B. in einer VoIP-Telefonanlage, die über eine PBX-Leitung erreicht wird.

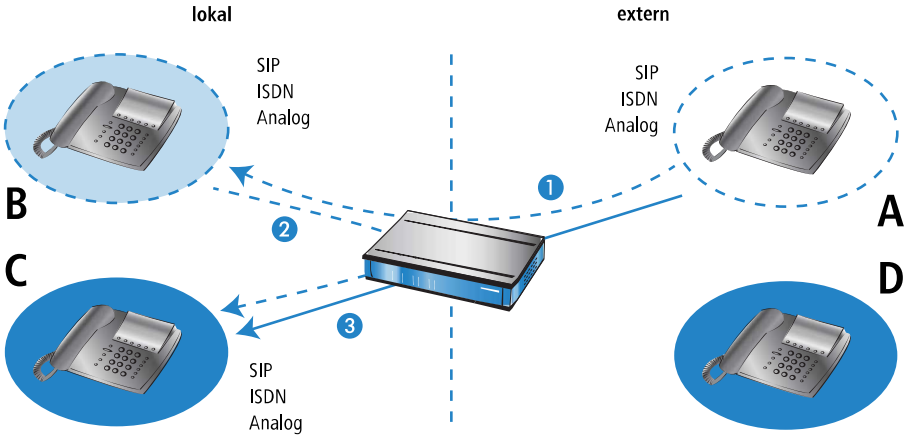
Vermitteln

Der LANCOM VoIP Router übernimmt die Aufgabe der Signalisierung und der Datenübertragung zwischen den Teilnehmern.

16.6.1.5 Aktive Weiterschaltung zu lokalen Benutzern

1. Ein externer Benutzer **A** baut ein Gespräch zu einem internen Benutzer **B** (SIP, ISDN oder Analog) auf.

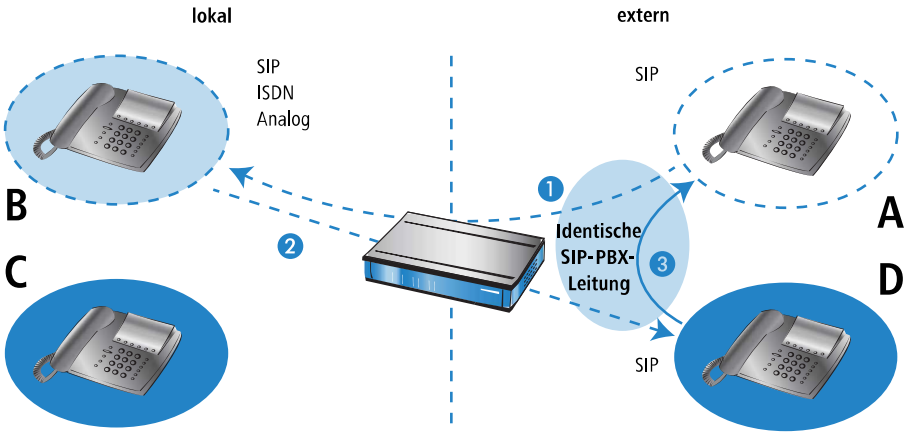
2. **B** baut ein weiteres Gespräch zu einem lokalen Benutzer **C** auf. Die beiden Benutzer können sich direkt erreichen, daher wird nur die Signalisierungsaufgabe über SIP vom LANCOM VoIP Router übernommen, die Datenübertragung über RTP wird abgezweigt und auf dem kürzesten Weg realisiert.
3. Der lokale Benutzer **B** leitet dann die Anrufweiterschaltung (mit Rückfrage) zu **C** ein.
4. Der LANCOM VoIP Router übernimmt die Verwaltung der Weiterschaltung.



Setzt im Fall von SIP beim externen Teilehmer voraus, dass Transfer in SIP (Re-Invite) vollständig und korrekt unterstützt wird.

16.6.1.6 Aktive Weiterschaltung zu externen SIP-Benutzern

1. Ein externer SIP-Benutzer **A** baut ein Gespräch zu einem internen Benutzer **B** (SIP, ISDN oder Analog) auf.
2. **B** baut ein weiteres Gespräch zu einem externen SIP-Benutzer **D** auf.
3. Wenn die beiden externen SIP-Benutzer **A** und **D** über die gleiche SIP-Leitung erreicht werden können, delegiert der LANCOM VoIP Router die Verwaltung der Weiterschaltung an den übergeordneten Provider.

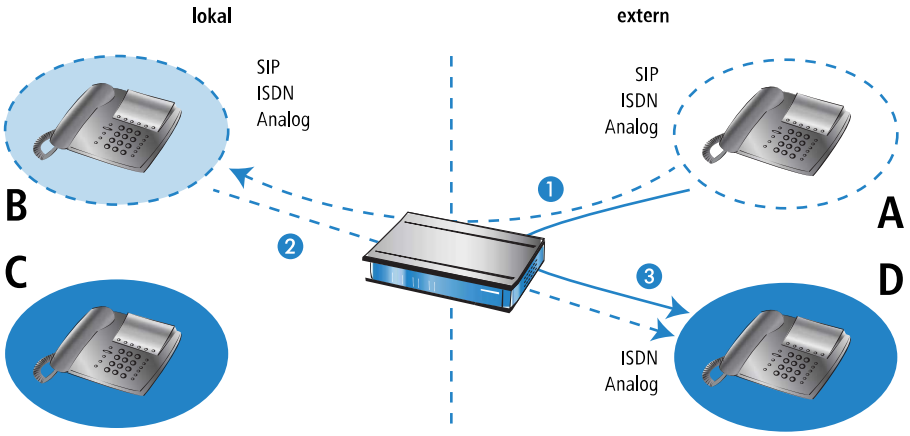


Setzt voraus, dass die VoIP-TK-Anlage Transfers in SIP (Re-Invites) vollständig und korrekt unterstützt.

16.6.1.7 Aktive Weiterschaltung zu externen ISDN-Benutzern

Bei der Anrufweiterschaltung zu externen ISDN-Benutzern kann es vorkommen, dass die übergeordneten Vermittlungsstellen das Delegieren von bestimmten Weiterschaltungsfunktionen nicht unterstützen – oft aufgrund der unklaren Frage der Gebührenübernahme. Aus diesem Grund wird die Anrufweiterschaltung zwischen externen Teilnehmern immer vom LANCOM VoIP Router verwaltet.

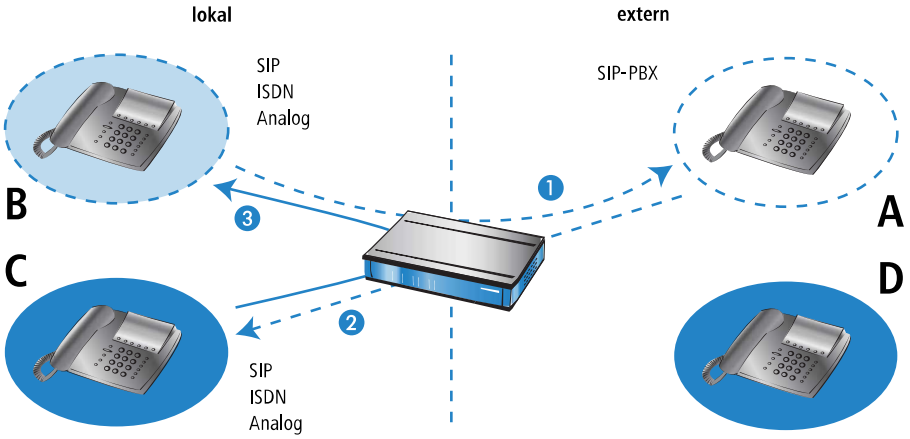
1. Ein externer Teilnehmer **A** (externes SIP, ISDN) baut ein Gespräch zu einem internen Benutzer **B** (SIP, ISDN) auf.
2. **B** baut ein weiteres Gespräch zu einem externen Teilnehmer **D** (ISDN) auf.
3. Der lokale Benutzer **B** leitet dann die Anrufweiterschaltung (mit Rückfrage) zu **A** ein.
4. Wenn die beiden externen Benutzer **A** und **D** unterschiedliche Protokolle (SIP, ISDN) verwenden, übernimmt der LANCOM VoIP Router die Verwaltung und Konvertierung der Daten.
5. Wenn die beiden externen Benutzer **A** und **D** zwar beide SIP verwenden, kann der LANCOM VoIP Router keine Weiterschaltung ermöglichen.



Setzt voraus, dass die VoIP-TK-Anlage Transfers in SIP (Re-Invites) vollständig und korrekt unterstützt.

16.6.1.8 Passive Weiterschaltung innerhalb von lokalen Benutzern

1. Ein interner Benutzer **B** (SIP, ISDN oder Analog) baut ein Gespräch zu einem externen Benutzer **A** (an einer SIP-PBX-Leitung) auf.
2. **A** baut ein weiteres Gespräch zu einem lokalen Benutzer **C** auf.
3. Der externe Benutzer **A** leitet dann die Anrufweiterschaltung zu **C** ein.
4. Der LANCOM VoIP Router übernimmt die Verwaltung der Weiterschaltung. Wenn es sich bei den verbundenen Teilnehmern **B** und **C** um interne Benutzer handelt, kontrolliert der LANCOM VoIP Router nur die SIP-Daten zur Signalisierung und ermöglicht die RTP-Datenübertragung auf dem kürzesten Weg direkt zwischen den SIP-Benutzern.

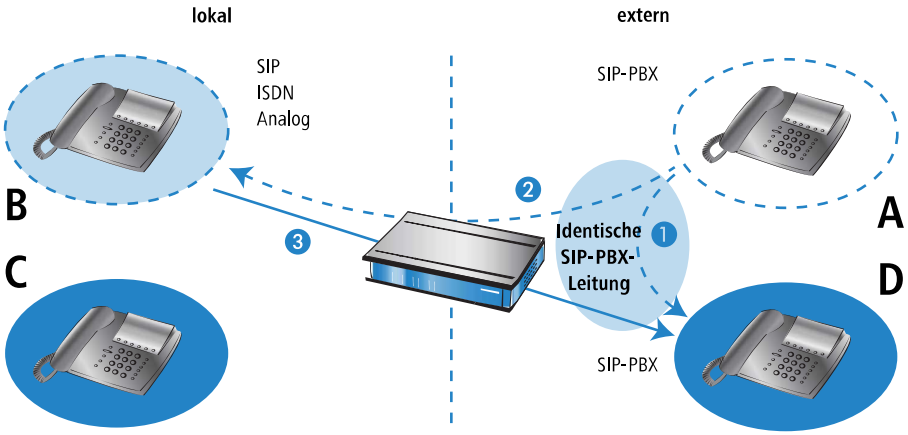


Setzt voraus, dass die VoIP-TK-Anlage Transfers in SIP (Re-Invites) vollständig und korrekt unterstützt.

16.6.1.9 Passive Weiterschaltung von lokalen zu externen Benutzern

1. Ein externer Benutzer **A** (an einer SIP-PBX-Leitung) baut ein Gespräch zu einem internen Benutzer **B** (SIP, ISDN oder Analog) auf.
2. **A** baut ein weiteres Gespräch zu einem externen Benutzer **D** (ebenfalls Teilnehmer an derselben SIP-PBX-Leitung wie **A**) auf.
3. Der externe Benutzer **A** leitet dann die Anrufweiterschaltung von **B** zu **D** ein. Dazu muss der LANCOM VoIP Router eine externe Verbindung zu **D** aufbauen.

Der LANCOM VoIP Router kann diese Verbindung nur dann aufbauen, wenn **D** über dieselbe SIP-PBX-Leitung wie **A** erreicht werden kann, wenn also die externe Anrufweiterschaltung erlaubt ist.



Setzt voraus, dass die VoIP-TK-Anlage Transfers in SIP (Re-Invites) vollständig und korrekt unterstützt.

16.6.2 Spontane Anrufsteuerung durch den Benutzer

16.6.2.1 Funktionen für die spontane Anrufsteuerung

Zur individuellen Steuerung der Anrufe unterstützen LANCOM VoIP Router die Dienstmerkmale, wie sie aus dem ISDN-Netz bekannt sind:

- Beim Halten versetzt der Benutzer eine aktive Gesprächsverbindung in einen Wartezustand. In diesem Zustand kann der Benutzer mit seinem Endgerät z. B. eine weitere Verbindung zu einem anderen Gesprächspartner aufbauen.
- Den Aufbau einer weiteren Verbindung während ein Gespräch gehalten wird, bezeichnet man als Rückfrage. Diese kann wieder beendet und das Gespräch mit dem gehaltenen Ruf herangeholt werden.
- Beim Makeln schaltet der Benutzer zwischen zwei Gesprächsverbindungen hin und her. Der Benutzer kann dabei jeweils nur mit einem Gesprächspartner sprechen, der andere Gesprächspartner wird im Wartezustand gehalten.
- Bei der Anrufweiterschaltung schaltet der Benutzer die aktive Gesprächsverbindung und eine im Wartezustand zusammen. Anschließend sind die beiden Gesprächspartner untereinander verbunden, der Benutzer selbst ist nicht mehr Teilnehmer der Gesprächsverbindung. Der Teilnehmer, der die Anrufweiterschaltung einleitet, kann das aktive Gespräch entweder direkt an einen dritten Teilnehmer übergeben (Anrufweiterschaltung ohne Rückfrage – englisch "Unattended Call Transfer"), oder er kann zunächst ein Gespräch zu dem dritten Teilnehmer aufbauen und erst dann die Weiterschaltung einleiten (Anrufweiterschaltung mit Rückfrage – englisch "Attended Call Transfer").

16.6.2.2 Spontane Anrufsteuerung mit verschiedenen Telefonen nutzen

SIP-Telefone und SIP-Softphones verfügen in der Regel über spezielle Tasten bzw. Menüeinträge zur Steuerung der Anrufe. Je nach Modell bzw. Software können dabei unterschiedliche Bezeichnungen verwendet werden, die Funktionen entsprechen aber den folgenden:

- HALTEN: Versetzt den aktiven Anruf in eine Wartestellung bzw. Makeln zwischen zwei aktiven Anrufen. Bei ISDN- und Analog-Telefonen ist diese Funktion oft als R-Taste (für „Rückfrage", englisch: F-Taste / Flash) ausgeführt.
- AUFLEGEN: Beenden des aktiven Anrufs.
- MAKELN: Makeln zwischen zwei aktiven Anrufen (kann je nach ISDN-Telefonmodell als Auswahl im Displaymenü erscheinen, als spezielle Taste ausgeführt sein oder durch Drücken von „R" ausgelöst werden).
- VERBINDEN: Einleiten der Anrufweiterschaltung (kann auch mit „Transfer" bezeichnet sein oder durch Auflegen bei gehaltenem und aktivem Gespräch ausgelöst werden).[1]

So können Sie diese Funktionen zur Steuerung von Anrufen nutzen:

Halten/Rückfrage und Fortsetzen von Anrufen	SIP	ISDN	Analog
Um während eines Gespräches eine Leitung zu halten, drücken Sie die Halten-Taste (bzw. „R" bei Analog-Telefonen). Der Gesprächsteilnehmer kann Sie nun nicht mehr hören, Sie können ein zweites Gespräch durch Wählen einer Rufnummer führen (Rückfrage).	HALTEN	HALTEN oder R	R
Um den gehaltenen Anruf fortzusetzen, drücken Sie erneut die Halten-Taste (bzw. „R 2").	HALTEN	HALTEN oder R	R 2
Solange das Gespräch zur Rückfrage noch nicht aufgebaut ist, beenden Sie mit dem Auflegen des Hörers die Rückfrage am SIP- oder ISDN-Telefon.[1] Sie können die Rückfrage mit einer entsprechenden Menüfunktion des Telefons (z. B. „Beenden") oder „R 1" (Analog) beenden.[1]	AUFLEGEN (1. Ruf klingelt)	AUFLEGEN (1. Ruf klingelt)	R 1 (zurück zum 1. Ruf)

Makeln	SIP	ISDN	Analog
Um während eines Gespräches eine zweite Leitung aufzubauen, drücken Sie zunächst die Halten-Taste (bzw. „R" bei Analog-Telefonen). Der Gesprächsteilnehmer kann Sie nun nicht mehr hören.	HALTEN	HALTEN oder R	R
Wählen Sie die Rufnummer des zweiten Gesprächspartners, der erste Anruf wird gehalten. Wenn sich der zweite Gesprächspartner nicht meldet, können Sie mit der Halten-Taste oder „R 2" bei Analog-Telefonen zum gehaltenen Anruf zurückkehren.	123456789	123456789	123456789
Sobald Sie gleichzeitig zwei Verbindungen aufgebaut haben, können Sie mit der Halten-Taste (bzw. Makeln-Taste bei ISDN- oder „R" und „2" bei Analog-Telefonen) zwischen den beiden Verbindungen hin- und herschalten. Es können jeweils nur die beiden Teilnehmer der aktiven Verbindung miteinander sprechen, der dritte Gesprächspartner wird gehalten.	HALTEN	HALTEN / MAKELN	R 2
Mit dem Auflegen des Hörers beenden Sie am SIP- oder ISDN-Telefon den aktiven Anruf, am Analogtelefon drücken Sie „R1". Der gehaltene Anruf wird dabei nicht automatisch aktiviert, er wird aber für die Dauer von 15 Sekunden signalisiert (Klingeln).	BEENDEN oder AUFLEGEN[1]	BEENDEN oder AUFLEGEN[1]	R 1

Anrufweiterschaltung mit Rückfrage	SIP	ISDN	Analog
Um während eines Gespräches eine zweite Leitung aufzubauen, drücken Sie zunächst die Halten-Taste (bzw. „R" bei Analog-Telefonen). Der Gesprächsteilnehmer kann Sie nun nicht mehr hören.	HALTEN	HALTEN oder R	R
Wählen Sie die Rufnummer des zweiten Gesprächspartners, der erste Anruf wird gehalten. Wenn sich der zweite Gesprächspartner nicht meldet, können Sie mit der Halten-Taste zum gehaltenen Anruf zurückkehren.	123456789	123456789	123456789
Sobald Sie gleichzeitig zwei Verbindungen aufgebaut haben, können Sie die beiden Gesprächspartner mit der Verbinden-Taste (bzw. „R" und „4" bei Analog-Telefonen) oder durch Auflegen des Hörers verbinden.[1]	VERBINDEN oder AUFLEGEN[1]	VERBINDEN oder AUFLEGEN[1]	R 4 oder AUFLEGEN

Anrufweiterschaltung mit Rückfrage	SIP	ISDN	Analog
Optional können Sie vor der Anrufweiterschaltung auch beliebig oft zwischen den beiden Leitungen makeln. Mit der Anrufweiterschaltung werden immer das aktive und das gehaltene Gespräch verbunden.			

Anrufweiterschaltung ohne Rückfrage	SIP
Um während eines Gespräches eine zweite Leitung aufzubauen, drücken Sie zunächst die Halten-Taste.	HALTEN
Der Gesprächsteilnehmer kann Sie nun nicht mehr hören.	
Wählen sie die Rufnummer des zweiten Gesprächspartners, der erste Anruf wird gehalten.	123456789
Drücken Sie die Verbinden-Taste oder legen Sie den Hörer auf, bevor die zweite Verbindung aufgebaut ist.[1]	VERBINDEN oder AUFLEGEN[1]
Die beiden Gesprächspartner werden nun „im Hintergrund“ verbunden.	

16.6.3 Feste Anrufweiterschaltung konfigurieren

Neben der spontanen Anrufweiterschaltung, die ein Teilnehmer während eines aktiven Gesprächs individuell festlegen kann, sind in vielen Fällen auch feste Anrufweiterschaltungen ("Rufumleitungen") sinnvoll. So soll z. B. oft der Anruf weitergeschaltet werden, wenn ein Anschluss besetzt ist, wenn er sich für eine bestimmte Zeit nicht meldet oder generell, z. B. bei Abwesenheit wegen Urlaub.

Für die Konfiguration der festen Anrufweiterschaltung gibt es zwei Möglichkeiten:

- Über das Telefon bzw. Endgerät selbst mit bestimmten Steuerzeichen
- In der Konfiguration der LANCOM VoIP Router über die üblichen Management-Tools (LANconfig, WEBconfig oder Telnet)

Wenn die feste Anrufweiterschaltung auf beiden Wegen erfolgt, bestimmt die jeweils letzte Aktion das Verhalten der Weiterschaltung.

16.6.3.1 Auslöser für die Anrufweiterschaltung

Als Auslöser oder Bedingung für die fest konfigurierte Anrufweiterschaltung können folgende Ereignisse genutzt werden:

- Sofortige Rufweiterschaltung ohne Bedingung (CFU – Call Forwarding Unconditional)
- Rufweiterschaltung bei "besetzt" (CFB – Call Forwarding Busy)
- Verzögerte Rufweiterschaltung (CFNR – Call Forwarding No Reply; CFNA – Call Forwarding No Answer)
- Keine Weiterschaltung

Alle Typen der Weiterschaltung können parallel mit eigenen Zielrufnummern genutzt werden. Wenn mehrere Weiterschaltungsbedingungen aktiviert sind, gilt die folgende Priorität:

1. CFU
2. CFB
3. CFNR

Wenn z. B. die Weiterschaltung bei "besetzt" aktiviert und ein entsprechendes Weiterschaltungs-Ziel definiert ist, wird der Anruf an dieses Ziel weitergeleitet, bevor das Weiterschaltungs-Ziel für verzögerte Rufweiterschaltung verwendet wird.

Wenn der eingehende Anruf schon von einer anderen Rufnummer weitergeschaltet wurde, findet keine erneute Weiterschaltung statt, um "Weiterschaltungs-Schleifen" zu vermeiden.

1

Ggf. kann bei einem SIP- oder ISDN-Telefon konfiguriert werden, ob ein Auflegen des Hörers die Rückfrage bzw. das aktive Gespräch beendet oder eine Anrufweiterschaltung auslöst („Verbinden“).

16.6.3.2 Konfiguration der Benutzer-Einstellungen über spezielle Zeichenfolgen mit dem Telefon

Zur Konfiguration der Benutzer-Einstellungen über das Telefon bieten die verschiedenen Technologien (SIP, ISDN, Analog) jeweils spezifische Möglichkeiten. Bei ISDN-Telefonen können Weiterschaltungen sowohl über das funktionale Protokoll in der ISDN-Signalisierung als auch über sogenannte Keypads (Zeichenfolgen) gesteuert werden, bei Analogtelefonen werden dieselben Zeichenfolgen als DTMF übertragen. Im SIP-Protokoll ist mit der REFER-Methode eine andere Möglichkeit vorgesehen, die von den meisten SIP-Telefonen und SIP-Softphones unterstützt wird, dabei werden die Weiterleitungen aber nur vom Endgerät verwaltet. Um in gemischten Infrastrukturen ein ähnliches Verhalten der Benutzer zu ermöglichen, bieten die LANCOM VoIP Router eine weitere Variante der Weiterschaltung für die SIP-Endgeräte, wie sie hier im Vergleich mit ISDN- und Analog-Telefonen vorgestellt wird.

Sofortige Rufweiterschaltung	SIP	ISDN	Analog
Einschalten und Weiterschaltungs-Ziel definieren	*21*ZielNr#	*21*ZielNr#	*21*ZielNr#
Ausschalten	#21#	#21#	#21#
Vorübergehend ausschalten, Weiterschaltungs-Ziel beibehalten	#22#	#22#	#22#
Wiedereinschalten, definiertes Weiterschaltungs-Ziel beibehalten	*22#	*22#	*22#

Rufweiterschaltung bei „besetzt“	SIP	ISDN	Analog
Einschalten und Weiterschaltungs-Ziel definieren	*67*ZielNr#	*67*ZielNr#	*67*ZielNr#
Ausschalten	#67#	#67#	#67#

Verzögerte Rufweiterschaltung	SIP	ISDN	Analog
Einschalten und Weiterschaltungs-Ziel definieren	*61*ZielNr#	*61*ZielNr#	*61*ZielNr#
Ausschalten	#61#	#61#	#61#

Bitte beachten Sie bei der Nutzung der Zeichenfolgen für die Konfiguration der Anrufweiterschaltung folgenden Hinweis:

Manche ISDN-Telefone verfügen über spezielle Tasten oder Menüeinträge zur Konfiguration der Anrufweiterschaltung, die alternativ zu den aufgelisteten Zeichenfolgen genutzt werden können. Bitte schlagen Sie dazu ggf. in der entsprechenden Herstellerdokumentation nach.

16.6.4 Rufumleitung (Call Deflection / Partial Rerouting) am SIP-Trunk (SIP 302)

LANCOM Router mit aktiviertem Voice Call Manager können auf SIP-Trunk-Verbindungen eine Rufumleitung im Amt initiieren, indem die von der TK-Anlage gesendeten Informationen an den SIP-Trunk-Provider weitergeleitet werden. Handelt es sich hierbei um ein ISDN-Endgerät, dann wird das Partial Rerouting (PR) in ein entsprechendes „SIP 302 Moved Temporarily“ umgewandelt, bevor es an den Provider übermittelt wird.

In der SIP-Leitungstabelle kann man die externe Anrufweiterschaltung für jede einzelne SIP-Trunk-Leitung konfigurieren, indem für die jeweilige Leitung unter **Voice Call Manager** > **Leitungen** > **SIP-Leitungen** > **Erweitert** die Option **Anrufweiterleitung mit SIP 302** eingeschaltet wird. Ist die Anrufweiterleitung eingeschaltet, dann wird eine vom Endgerät (ISDN / SIP) initiierte Rufumleitung direkt im Amt geschaltet, sofern das Endgerät nicht Teil einer Rufnummerngruppe ist oder der Benutzer mehrfach am LANCOM Router registriert wurde.

Handelt es sich hierbei um ein ISDN-Endgerät, dann wird das Partial Rerouting entsprechend dem Leistungsmerkmal SIP 302 umgewandelt bevor es an den Provider übermittelt wird. Die Rufnummer, auf die ein einkommender Ruf umgeleitet werden soll, wird vom Endgerät übermittelt und muss so angegeben werden, dass diese über Call-Routen erreichbar ist. Die Rufnummer muss also zum Rufnummernplan im Voice Call Manager passen, damit dieser die korrekte Leitung auswählen kann. Daher müssen z. B. Leitungspräfixe mit angegeben werden, die nach Zuordnung der korrekten Leitung vom Voice Call Manager entfernt werden.

Falls auf dem Endgerät eine interne Rufnummer als Weiterleitungsziel eingerichtet wird, dann geschieht die Rufumleitung direkt im Voice Call Manager, so dass hier das Präfix (z. B. **) für interne Rufe verwendet werden muss.

16.6.5 Faxen über T.38 – Fax over IP (FoIP)

Mit der Migration der Telefon-Infrastrukturen in Richtung VoIP steigt auch der Bedarf, die Faxgeräte in die VoIP-Kommunikation einzubinden. Auch im Zeitalter der E-Mail sind Faxübertragungen nach wie vor sehr wichtig, da sie u. a. in rechtlich relevanten Bereichen (Verträge, Rechnungen nach §14 im deutschen Umsatzsteuergesetz) für den Anwender viel einfacher zu handhaben sind als die alternativ möglichen E-Mails mit gültiger elektronischer Signatur. Die Integration der Faxgeräte in die VoIP-Struktur kann dabei auf zwei Wegen umgesetzt werden:

- Die Übertragung der Faxnachricht zur Gegenstelle erfolgt wie beim herkömmlichen Fax über das Festnetz.
- Die Übertragung der Faxnachricht erfolgt über eine Internet-Verbindung. Dabei gibt es folgende Möglichkeiten:
  - Die Faxsignale werden wie Sprachdaten über eine VoIP-Verbindung übermittelt, man spricht von "Fax over VoIP". Für die Faxübertragung sollte dabei nur der Codec G.711 eingesetzt werden – mit anderen Codecs können die eigentlich für analoge Netze entwickelten Faxtöne oft nicht richtig in der digitalen VoIP-Struktur übermittelt werden. Aufgrund der sehr sensiblen Eigenschaften der Faxverbindungen kann diese Variante auch nur bei sehr hoher Verbindungsqualität eingesetzt werden, die Übertragungsgeschwindigkeit ist nicht optimal.
  - Beim so genannten "Store-and-Forward"-Prinzip nach ITU-T.37 werden die Faxnachrichten z. B. vom Fax an ein Gateway übermittelt, in dem das Fax gespeichert und umgewandelt wird. In einem zweiten Schritt wird das Fax an die Gegenstelle übermittelt und dort ggf. wieder zurückgewandelt. Alternativ können Faxnachrichten auch per E-Mail versendet werden (Fax-to-Mail bzw. Mail-to-Fax). Solche Lösungen erfüllen jedoch u. a. nicht die rechtlichen Anforderungen nach §14 UStG, weil keine direkte Verbindung zwischen Sender und Empfänger besteht, und eignen sich daher nicht für die Übermittlung von Rechnungen etc.
  - Beim "Realtime-Routing" von Faxnachrichten wird hingegen eine direkte Verbindung der beiden beteiligten Faxgeräte aufgebaut – alle Daten werden in Echtzeit übertragen, so dass eine virtuelle Verbindung der Faxgeräte über das Internet besteht. Die Kommunikation der beiden Faxgeräte wird dabei über den ITU-T.38-Standard abgewickelt, der die Umwandlung der herkömmlichen Faxsignale übernimmt. Diese Variante ist auch als Fax over IP bekannt (FoIP). Die Faxnachrichten werden dabei nicht als Sprachsignale innerhalb von VoIP übermittelt, sondern in einem speziellen Protokoll, was eine Einbettung in UDP/TCP-Pakete durchführt.

Um eine Faxübertragung nach T.38 zu ermöglichen, müssen die beteiligten Faxgeräte entweder selbst den T.38-Standard unterstützen oder über geeignete Fax-Gateways mit dem Internet verbunden sein. LANCOM VoIP Router unterstützen den T.38-Standard und eignen sich somit als Fax-Gateway in der VoIP-Infrastruktur.

Die Faxgeräte werden über eine geeignete Schnittstelle mit dem LANCOM VoIP Router verbunden. Beim Versenden und Empfangen von Faxnachrichten sorgt das Fax-Gateway im LANCOM VoIP Router für die entsprechende Umwandlung der Signale:

- Umwandlung von T.38-Faxdaten in G.711/T.30
- Umwandlung von G.711/T.30-Faxdaten in T.38
- Durchleiten von G.711/T.30-Faxdaten
- Durchleiten von T.38-Faxdaten

LANCOM Business VoIP Router erkennen ein zu versendendes Fax automatisch, wenn in den Benutzer-Einstellungen der ISDN- und Analog-Benutzer der Gerätetyp "Fax" oder "Telefon/Fax" ausgewählt ist, und versuchen eine Faxübertragung über T.38/FoIP. Falls die Gegenstelle dieses Verfahren nicht unterstützt, nutzt der LANCOM VoIP Router automatisch die Fax over VoIP-Variante mit der Kompression G.711.



Für die erfolgreiche Übertragung der Faxe über FoIP muss auch die genutzte VoIP-Struktur den T.38-Standard unterstützen. Wird also z. B. für die VoIP-Kommunikation ein öffentlicher SIP-Provider eingesetzt, muss auch dieser Provider in seinem Netzwerk T.38 unterstützen.

16.6.6 Gruppenrufe mit Ruf-Verteilung

16.6.6.1 Einleitung

Normalerweise ist ein Anruf an eine Person bzw. deren Rufnummer gerichtet. In manchen Fällen ist es hingegen nicht wichtig, eine bestimmte Person zu erreichen – es wird nur ein Gesprächspartner aus einem Bereich bzw. mit einer Funktion gesucht. In diesen Fällen können mit Rufgruppen mehrere Benutzer der Telefoninfrastruktur zu einer funktionalen Gruppe (Rufgruppe) zusammengefasst werden, die über eine gemeinsame Rufnummer erreicht werden können. Die Gruppenruf-Funktion übernimmt dabei die Aufgabe, die eingehenden Anrufe nach den gewünschten Regeln innerhalb der Rufgruppe zu verteilen bzw. weiterzuleiten.

16.6.6.2 Ruf-Verteilung

In einer Rufgruppe werden zwei oder mehrere Benutzer oder weitere Rufgruppen zusammengefasst, die als Ziel der Anrufe in Frage kommen. Rufgruppen sind vergleichbar mit lokalen Benutzern und haben eine eigene Rufnummer, sie können daher auch im Call Router als Ziel-Nummer verwendet werden.

Zur Verteilung der eingehenden Rufe stehen verschiedene Methoden zur Auswahl, mit denen unterschiedliche Szenarien realisiert werden können:

- Rufe werden gleichzeitig an alle Gruppenmitglieder signalisiert (simultan)
- Rufe werden nach einer definierten Reihenfolge nacheinander an die Gruppenmitglieder signalisiert (sequentiell)

Neben den Mitgliedern der Rufgruppe und der Verteilungs-Methode werden eine Weiterleitungs-Zeit und ein Weiterleitungs-Ziel definiert, die den Ablauf der Ruf-Verteilung steuern. Die Weiterleitungs-Zeit bestimmt die Zeitspanne, in der die angewählten Benutzer einen signalisierten Anruf annehmen können. Das Weiterleitungs-Ziel definiert, an welches Rufziel (Benutzer, Gruppe, interne oder externe Rufnummer) der Anruf weitergeleitet werden soll, wenn keines der Gruppenmitglieder den Anruf innerhalb der Weiterleitungs-Zeit annimmt – ist kein Weiterleitungs-Ziel angegeben, wird der Anruf zurückgewiesen.

16.6.6.3 Kaskadieren von Rufgruppen

Die definierten Rufgruppen können selbst Mitglieder einer übergeordneten Rufgruppe sein, ebenso können Rufgruppen als Weiterleitungs-Ziel einer übergeordneten Rufgruppe eingetragen werden. Diese Optionen ermöglichen den Aufbau einer kaskadierten Rufgruppen-Struktur, mit der auch sehr komplexe Szenarien durch zahlreiche Verzweigungen abgebildet werden können, in denen die Rufgruppen für die Verzweigungen und die Benutzer für die Endpunkte der Struktur stehen. Für solche Strukturen bzw. die Verzweigungen gelten folgende Regeln:

- Wird als Mitglied eine Rufgruppe verwendet, wird durch diese untergeordnete Rufgruppe ein neuer "Zweig" der Struktur geöffnet, sobald das Mitglied an die Reihe kommt.
- Beim Öffnen einer untergeordneten Rufgruppe gelten jeweils die darin definierten Parameter wie z. B. Weiterleitungs-Zeit etc.
- Der Zweig der untergeordneten Rufgruppe bleibt jedoch nur solange geöffnet, wie das Mitglied aufgrund der Einstellungen in der übergeordneten Rufgruppe gerufen wird. Wird in der übergeordneten Rufgruppe das nächste Mitglied erreicht, wird der gesamte Zweig mit allen ggf. vorhandenen weiteren Unterverzweigungen geschlossen. Dabei wird insbesondere nicht auf das komplette Abarbeiten eines Zweiges gewartet. Es können also in einer untergeordneten Rufgruppe Mitglieder definiert sein, die aufgrund der Einstellungen in übergeordneten Gruppen innerhalb der Struktur nicht erreicht werden können.
- Nimmt ein Mitglied einer Rufgruppe den Anruf an, so werden alle geöffneten Zweige geschlossen, alle ablaufenden Weiterleitungs-Zeiten werden gestoppt.
- Sind in einer Rufgruppe (egal ob über- oder untergeordnet) alle Mitglieder innerhalb der verfügbaren Zeit abgearbeitet, wird der Ruf an das Weiterleitungs-Ziel weitergegeben. Damit enden auch alle evtl. in den übergeordneten Rufgruppen laufenden Weiterleitungs-Zeiten! Der Anruf "springt" in diesem Fall aus der Rufgruppen-Struktur heraus und bekommt ein neues Ziel.

Beispiel: Es sind folgende Rufgruppen definiert:

Gruppen-Rufnummer	Kommentar	Mitglieder	Weiterleitungs-Methode	Weiterleitungs-Zeit	Weiterleitungs-Ziel
100	ganze Firma	200, 300, 400	Simultan	10	ext. Rufnummer
200	Abteilung Service	201 bis 209	Simultan	10	100
300	Abteilung Marketing	301 bis 309	Sequentiell	10	200
400	Abteilung Vertrieb	409	Sequentiell	15	100
410	Gruppe Vertrieb Europa	411, 412, 413, 414, 415	Sequentiell	10	400
420	Gruppe Vertrieb Amerika	421, 422, 410	Sequentiell	30	400
430	Gruppe Vertrieb Asien	431, 432, 410	Sequentiell	30	400

Dazu gibt es in den jeweiligen Abteilungen bzw. Gruppen Benutzer, welche die jeweils letzte Ziffer der Rufnummer verwenden, also z. B. 411 bis 419 für die Vertriebsmitarbeiter Europa und 409 für die Team-Assistenz Vertrieb. In der Kommunikation nach aussen werden nur die Gruppen-Rufnummern der Vertriebsteams weitergegeben, da die einzelnen Mitarbeiter auch im Außendienst unterwegs sind. Ziel der Rufgruppen-Struktur ist es, die anrufenden Kunden möglichst zielgerichtet und schnell mit einem kompetenten Mitarbeiter zu verbinden.

Bei einem Anruf auf die Rufnummer 420 für einen Mitarbeiter aus dem Vertrieb Amerika geschieht folgendes:

1. Der Anruf wird nacheinander für jeweils 30 Sekunden an die beiden Benutzer 421 und 422 in dieser Gruppe signalisiert. Nimmt von diesen direkt gerufenen Anschlüssen keiner ab, wird die Rufgruppe 410 für 30 Sekunden aktiviert – es soll sich ein Mitarbeiter aus dem Vertriebsteam Europa um den Kunden kümmern, wenn die Amerika-Kollegen nicht erreichbar sind.
2. Im Vertriebsteam Europa werden die Anrufe der Reihe nach verteilt für jeweils 10 Sekunden. Die Rufgruppe verfügt zwar über fünf Mitglieder, bei einer Weiterleitungs-Zeit von 10 Sekunden kommen hier aber nicht alle möglichen Benutzer zum Zuge: Der Zweig wird durch die übergeordnete Rufgruppe, in diesem Fall die 420, nur für maximal 30 Sekunden geöffnet. Auf diese Weise wird die maximale Wartezeit für den Kunden begrenzt. Wenn sich also die ersten drei gerufenen Mitglieder der untergeordneten Rufgruppe 410 nicht melden, springt der Anruf wieder zurück zur übergeordneten Rufgruppe 420.
3. In der übergeordneten Rufgruppe 420 sind keine weiteren Mitglieder vorhanden, der Anruf wird also an das Weiterleitungs-Ziel 400 weitergeleitet.
4. Über die Rufgruppe 400 wird der Anschluss der Team-Assistenz 409 gerufen. Sollte sich auch hier für die Weiterleitungs-Zeit von 15 Sekunden niemand melden, wird über das Weiterleitungs-Ziel 100 noch ein letzter Versuch in der gesamten Firma unternommen.
5. Über die Rufgruppe 100 werden alle Anschlüsse in den Rufgruppen 200, 300 und 400 gleichzeitig gerufen. Wenn sich auch hier nach 10 Sekunden niemand meldet, leitet die Rufgruppe weiter zu einer externen Rufnummer, z. B. für ein 24/7-Call-Center.

16.6.7 Mehrfachanmeldung (Multi-Login)

Verwendet ein Teilnehmer mehrere Endgeräte, z. B. ein Softphone auf dem PC und ein "normales" Telefon auf dem Schreibtisch, so können sich mehrere SIP-, ISDN- oder Analog-Telefone mit derselben internen Rufnummer beim LANCOM VoIP Router anmelden. Die Telefone mit Mehrfachanmeldung verhalten sich wie ein einzelner Benutzer mit den Eigenschaften einer Rufgruppe, deren Ruf-Verteilung auf 'simultan' gestellt ist:

1. Alle eingehenden Anrufe werden **gleichzeitig an alle** Telefone mit dieser internen Rufnummer signalisiert.
2. Sobald eines der Telefone den Anruf annimmt, endet die Signalisierung bei den anderen Geräten.
3. Weitere eingehende Anrufe werden an alle Telefone signalisiert. Meldet eines der Telefone „besetzt“, so gilt die gesamte Multi-Login-Gruppe als „besetzt“, sofern dies unter *Erweiterte Benutzer-Einstellungen* auf Seite 1472 konfiguriert wurde.
4. Ausgehende Anrufe sind von jedem Telefon aus ohne Einschränkung möglich.
5. Für eine Multi-Login-Gruppe kann nur eine Anrufweiterschaltung (Rufumleitung) gesetzt werden, die für alle Endgeräte gilt und von allen Endgeräten aus gesteuert werden kann.

Zur Nutzung der Mehrfachanmeldung müssen lediglich mehrere Telefone auf dieselbe interne Rufnummer eingestellt werden.

16.7 VoIP-Media-Proxy – Optimierte Verwaltung von SIP-Verbindungen

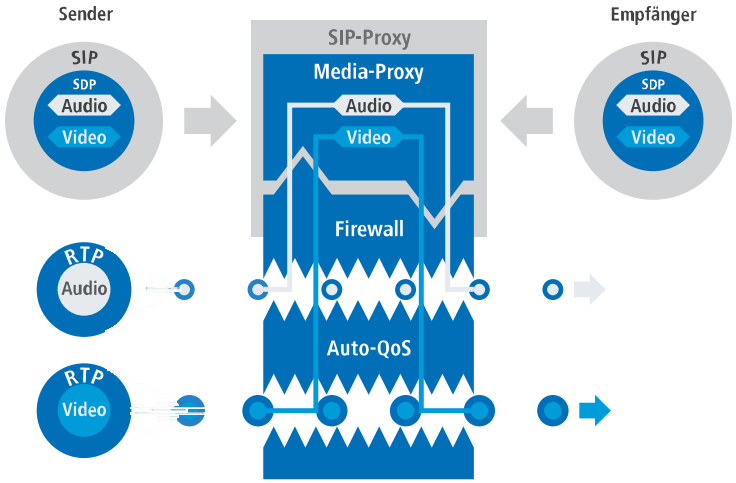
Beim Verbinden von bzw. bei Anrufweiterschaltungen zwischen entfernten Teilnehmern über unterschiedliche SIP-Leitungen versucht der SIP-Proxy im LANCOM VoIP Router, durch einen REFER bzw. einen Re-INVITE die beiden Teilnehmer zu verbinden. Da die beiden externen Teilnehmer sich nicht immer direkt erreichen können, kommt diese Verbindung in machen Situationen nicht zu Stande, da die SIP-Provider die nötigen Anpassungen z. B. bei den Ziel-IP-Adressen nicht wie erforderlich umsetzen. Um das Verhalten in diesen Fällen zu verbessern, wird der SIP-Proxy in den LANCOM VoIP Routern um einen Media-Proxy ergänzt.

Der Media-Proxy hilft, Verbinden und Anrufweiterschaltung auch zwischen solchen Teilnehmern zu ermöglichen, die über verschiedene Leitungs-Typen erreicht werden (z. B. SIP-PBX-Line und SIP-Provider-Line). Dazu bleiben die Media-Streams (i.d.R. RTP-Verbindungen) für die Gegenstellen bei diesen Aktionen unverändert. Der Media Proxy nimmt die erforderlichen Änderungen von Ports und IP-Adressen in den Datenpaketen vor und passt spezielle Media-Endpunkte an die entsprechenden Ziel-Netze an (ARF-Netzwerke, Interface und IP-Adresse).

Mehrere Medien-Ströme in einer SIP-Verbindung

Das SIP-Protokoll kann in einer Sitzung (Session) mehrere Datenströme aushandeln, z. B. einzelne Media-Ströme für Audio und Video. Die einzelnen Ströme werden separat behandelt – jeder Datenstrom wird im Media-Proxy zunächst terminiert und dann "auf der anderen Seite" weitergeführt, der Datenstrom erhält so Endpunkte im Media-Proxy auf der LAN- und WAN-Seite.

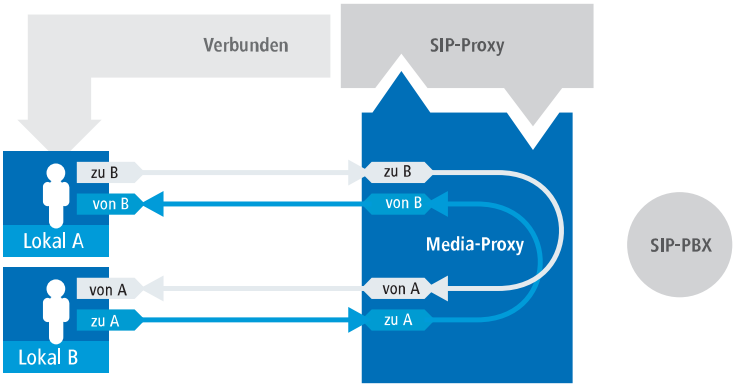
Somit können die Verbindungsinformationen in Richtung der SIP-Provider beibehalten werden, alle notwendigen Änderungen an IP-Adressen oder Ports etc. werden im Media-Proxy ausgeführt.



Dabei werden alle Datenströme auch einzeln durch die Firewall geführt, was u. a. eine differenzierte Regelung der QoS-Einstellungen ermöglicht.

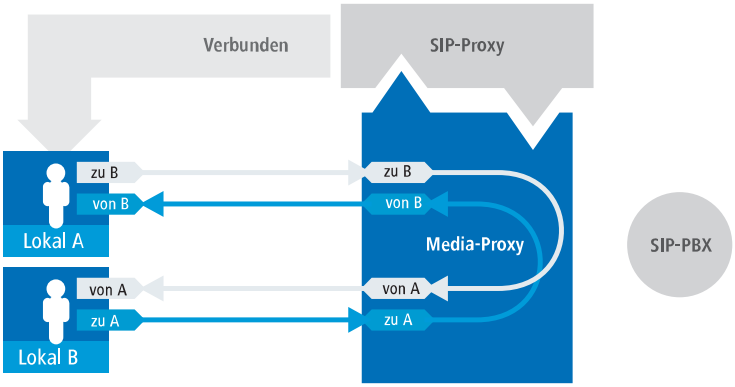
Mit Hilfe dieser Verbindungsverwaltung im Media-Proxy können so alle Teilnehmertypen untereinander verbunden werden, unabhängig von der Leitung, über die sie erreichbar sind. Damit wird auch das Verbinden zwischen SIP, ISDN- oder Analog-Teilnehmern ermöglicht, was über eine reine SIP-Verbindung nicht gelingt. Darüber hinaus können durch

die Überwachung der einzelnen Media-Ströme in der Firewall gezielt bestimmte Anwendungen differenziert je nach Endpunkt der Verbindung erlaubt oder eingeschränkt werden.



Verwaltung der Media-Streams bei übergeordneter SIP-PBX

Beim Anschluss an eine übergeordnete SIP-PBX erzeugt der Media-Proxy auch für zwei Teilnehmer im selben Netz hinter dem LANCOM VoIP Router Datenströme mit separaten Media-Endpunkten jeweils auf der LAN und WAN-Seite (zur SIP-PBX hin).



In diesem Fall ist das Durchleiten der Media-Ströme durch die übergeordnete PBX jedoch nicht erforderlich, der LANCOM VoIP Router kann aufgrund der SIP-Signalisierung neu über den Weg der eigentlichen Verbindungsdaten entscheiden. Die Datenströme können so anhand der Endpunkte im Media-Proxy direkt verschaltet werden, eine Umleitung über die SIP-PBX entfällt.

Diese Entscheidung wird im Media-Proxy auch dann neu getroffen, wenn eine Verbindung von einem lokalen zu einem externen Teilnehmer so verbunden wird, dass anschließend zwei lokale Teilnehmer verbunden sind. Der Media-Proxy ordnet die Endpunkte beim Verbinden neu zu und ermöglicht dann die direkte Übertragung der Datenströme zwischen den lokalen Teilnehmern.

Verwaltung der Media-Streams in der Firewall

Die Media-Streams werden grundsätzlich in der Firewall überwacht. Daher wird pro Media-Stream (Audio, Video etc.) eine Firewall-Regel erstellt, die entsprechend für IP-Adressen und Ports pro Seite (LAN-WAN) eine Verbindung freischaltet und eine Umsetzung entsprechend der vom Media Proxy vorgegebenen IP-Port-Beziehungen durchführt.

Automatische QoS-Regeln für Media-Streams

Der QoS-Mechanismus der Firewall hält automatisch die in der SDP-Verhandlung (SDP – Session Description Protocol) vereinbarte maximal mögliche Bandbreite für die Verbindung frei und die priorisiert die Pakete entsprechend.

Verhalten bei verschiedenartigen Codecs der zu verbindenden Teilnehmer

Beim Verbinden von verschiedenen Teilnehmern gibt es Situationen, in denen die verfügbaren Codecs der zu verbindenden Teilnehmern nicht zusammen passen – die Schnittmenge der Codecs, die aufgrund der SDP-Verhandlung zugelassen sind, ist leer.

Dabei sind folgende Situationen zu beachten:

- Verschalten von Verbindungen mit verschiedenartigen Media-Strömen, z. B. ein Video-Telefonat (Audio + Video), und ein klassisches Telefonat (nur Audio): Der Aufbau dieser Verbindungen wird mit der Meldung "Codec mismatch" abgelehnt.
- Bei gleichen Medientypen (Audio-Audio, Video-Video) passen die Codec-Auswahlen nicht zusammen: Der Aufbau dieser Verbindungen wird mit der Meldung "Codec mismatch" abgelehnt.

Nur wenn Medientypen und Codec-Auswahl zusammen passen, kann der Media-Proxy die Verbindung der entsprechenden Teilnehmer herstellen.

16.8 SIP-ID als Stammnummer bei Trunk-Leitungen

Bisher wurde bei SIP-Trunk-Leitungen die SIP-ID als Stammnummer verwendet und entsprechend die Rufnummer angepasst. Dieser Mechanismus wird jedoch nicht von allen Anbietern der Trunk-Leitungen unterstützt. Daher können Sie – genau wie beim ISDN-Mapping – in der SIP-Mapping-Tabelle explizit angeben, wie die Rufnummern verarbeitet werden sollen.

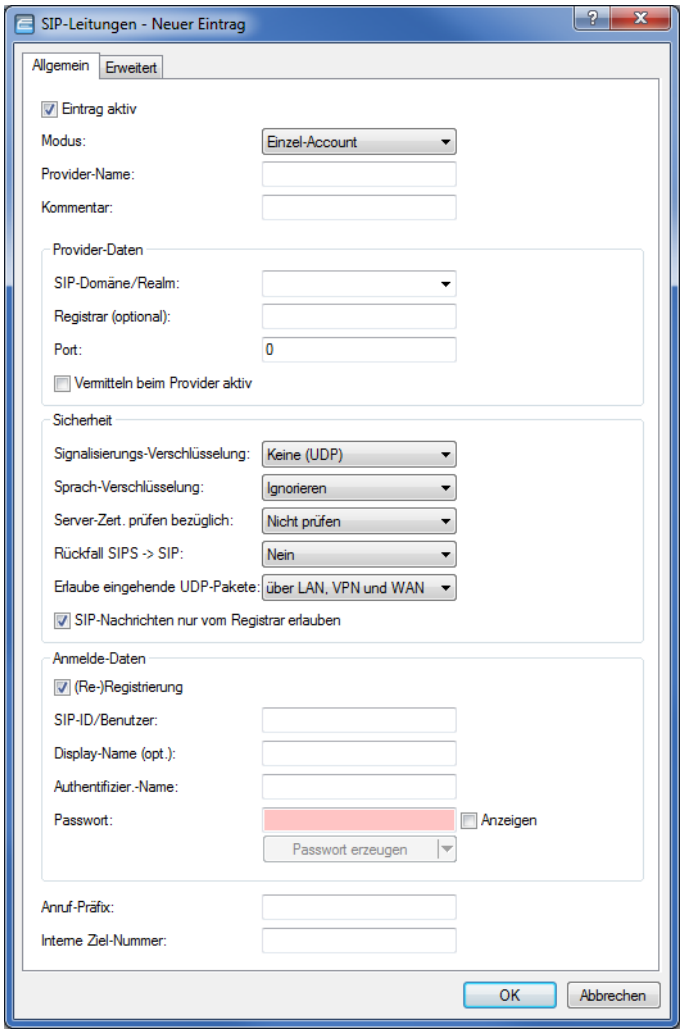
Beispiel: Mit `0123456789# -> #` setzen Sie direkt die Durchwahlnummern des Trunks 1:1 auf interne Rufnummern um.

16.9 Vermittlung beim SIP-Provider

Beim Vermitteln von externen SIP-Verbindungen verwaltet der Call Router im LANCOM VoIP Router normalerweise die Verbindung während der gesamten Verbindungsdauer. Der Call Router behält also auch dann die Kontrolle über die Verbindung, wenn zwei externe Teilnehmer das Gespräch fortführen und der lokale Teilnehmer auf Seiten des LANCOM VoIP Routers die Verbindung beendet hat. In diesem Fall wird auf dem LANCOM VoIP Router weiterhin die Bandbreite zur Verbindung der beiden externen Teilnehmer benötigt.

Wenn die Verbindung zu den beiden externen Teilnehmern über den gleichen SIP-Provider aufgebaut wurde, kann die Vermittlung alternativ an den Provider übertragen werden – im LANCOM VoIP Router wird dann keine Bandbreite mehr benötigt.

Die Vermittlung beim SIP-Provider aktivieren Sie im LANconfig unter **Voice-Call-Manager** > **Leitungen** mit einem Klick auf die Schaltfläche **SIP-Leitungen** und Aktivierung der Option **Vermitteln beim Provider aktiv** in der Ansicht **Allgemein**.



Vermitteln beim Provider aktiv

Bei der Rufvermittlung (Verbindung) von zwei entfernten Gesprächsteilnehmern kann die Vermittlung im Gerät selbst gehalten (Media-Proxy) oder an die Vermittlungsstelle beim Provider übergeben werden, wenn beide zu verbindende Gesprächsteilnehmer über diese SIP-Provider-Leitung erreicht werden. Dies hat den Vorteil, dass im LANCOM VoIP Router keine Bandbreite mehr benötigt wird. Andernfalls übernimmt der Media-Proxy im LANCOM die Vermittlung der Medienströme, z. B. beim Verbinden zwischen zwei SIP-Provider-Leitungen.

Voraussetzung für die Vermittlung beim Provider ist, dass beide Verbindungen über die gleiche Providerleitung aufgebaut wurden.

Eine Übersicht über die wichtigsten SIP-Provider, die diese Funktion unterstützen, finden Sie im Support-Bereich auf der Internet-Seite.

16.10 SIP Application Layer Gateway (SIP-ALG)

SIP setzt sich zunehmend als Grundlage für moderne Echtzeit-Kommunikation in IP-Netzen durch. Unified Communications (UC) und Collaboration, IP-Telefonie, aber auch Video-Übertragung, Kamera-Überwachung, Gegensprechstellen, Durchsage-Einrichtungen und Audioaufzeichnungen verwenden zur Vermittlung und Übertragung SIP und RTP.

Aufgrund der Übermittlung von Adressen in der Signalisierung per SIP und aufgrund des dynamischen Aushandelns der Media-Sessions mit davon abhängigen RTP-Verbindungen via UDP stellt das an Grenzen von LANs typische NAT (Network Address Translation) der Access-Router eine Barriere für die SIP-Kommunikation dar.

Restriktiv konfigurierte Firewalls verhindern die Kommunikation, selbst wenn Client- / Server-seitige Mechanismen zur Überwindung von NAT wie STUN, ICE und TURN zum Einsatz kommen.

Das SIP-ALG (Application Layer Gateway) für LCOS erkennt erwünschte SIP-Verbindungen sowie davon abhängende Medienströme per RTP und transformiert diese entsprechend der NAT-Regeln im Access-Router.

Außerdem überwacht das SIP-ALG die Bandbreiten der SIP-Verbindungen und sorgt für QoS.

16.10.1 Eigenschaften

Das SIP-ALG für LCOS besitzt die folgenden Eigenschaften:

- **Keine lokale Registrierung**

  Der SIP-Proxy bietet keine Möglichkeit, SIP-Endgeräte zu registrieren. Stattdessen übermittelt er die Registrierungen direkt an die erlaubten SIP-Domänen.

  Ein Leitungs-Backup über alternative Sprachanschlüsse (Analog, ISDN) ist deshalb nicht möglich!

- **Transparenz gegenüber SIP-Erweiterungen**

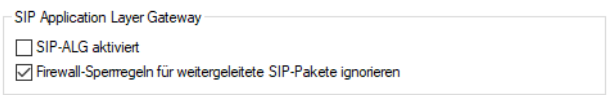
  Das SIP-ALG überträgt auch unbekannte, nicht standardkonforme Header-Elemente, um die Kommunikation der betroffenen SIP-Nachrichten zwischen Endgeräten und SIP-TK-Anlagen zu ermöglichen.

  Das SIP-ALG ermittelt zu jeder SIP-Nachricht ein eindeutiges Ziel. Das sogenannte „Forking", also die Kommunikation zwischen mehreren Endgeräten gleicher Identität, übernimmt die übergeordnete Instanz. Das SIP-ALG leitet diese Datenpakete nur transparent weiter.

16.10.2 Konfiguration

Aktivieren und konfigurieren Sie das SIP Application Layer Gateway (SIP-ALG) in LANconfig unter **Sonstige Dienste** > **Dienste** > **SIP Application Layer Gateway**.

Das SIP-ALG ist in der Default-Einstellung deaktiviert.



SIP-ALG aktiviert

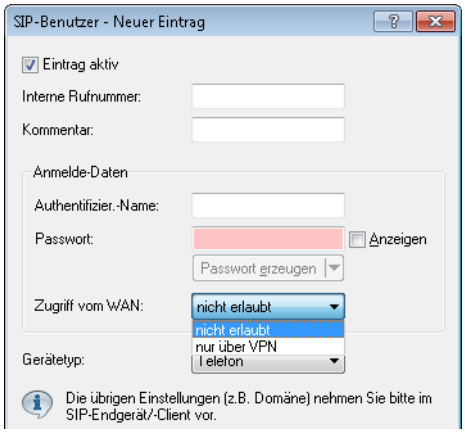
Aktivieren Sie hier das SIP Application Layer Gateway.

Firewall-Sperrregeln für weitergeleitete SIP-Pakete ignorieren

Hier legen Sie fest, ob die Firewall für SIP-Pakete Reject-Regeln beachtet oder ob die Pakete in jedem Fall vom SIP-ALG weitergeleitet werden.

16.11 SIP-Anmeldung über WAN eingrenzen bzw. unterbinden

Sie können unter **Voice-Call-Manager** > **Benutzer** mit einem Klick auf die Schaltfläche **SIP-Benutzer** die SIP-Anmeldung am Voice-Call-Manager über eine WAN-Verbindung einschränken oder auch ganz unterbinden. Die Konfiguration der SIP-Benutzer beinhaltet einen Parameter, der die entsprechende Einschränkung steuert. Sie können eine Anmeldung über VPN erlauben oder sie ganz verbieten.



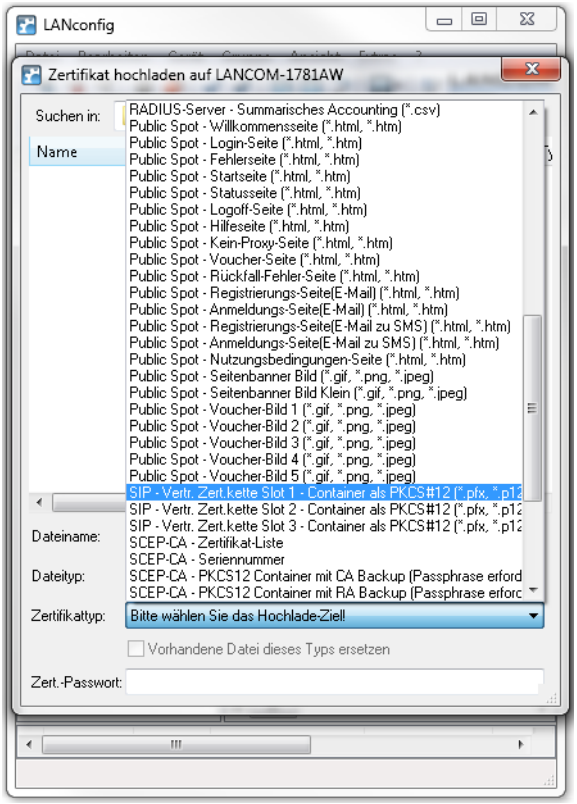
Um die Sicherheit bei der Anmeldung zusätzlich zu erhöhen, ermittelt ein Zähler, wie oft sich ein SIP-Benutzer falsch authentifiziert hat. Sobald der Zähler einen Schwellwert erreicht, sperrt das Gerät das Konto des SIP-Benutzers für eine bestimmte Zeit, so dass dieser sich für die Sperrdauer nicht am Voice-Call-Manager anmelden kann. Sie können unter **Voice-Call-Manager** > **Allgemein** im Abschnitt **WAN Login-Sperre** sowohl den Schwellwert als auch die Zeitspanne der Sperre frei konfigurieren.



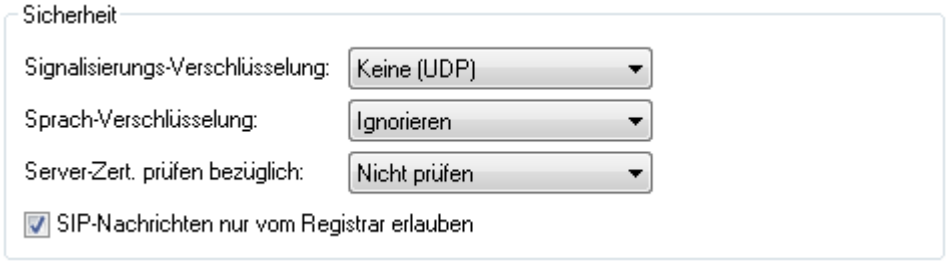
16.12 Zertifikate für verschlüsselte Telefonie

Sie haben die Möglichkeit, Zertifikate für verschlüsselte Telefonie in Ihr Gerät zu laden und zu überprüfen, ob das vorhandene Zertifikat vom SIP-Server beim Aufbau einer TLS-Verbindung als vertrauenswürdig eingestuft und akzeptiert werden soll.

Laden Sie mit LANconfig über **Konfigurations-Verwaltung** > **Zertifikat oder Datei hochladen** das gewünschte SIP-Zertifikat in Ihr Gerät.



Im LANconfig-Dialog unter **Voice Call Manager** > **Leitungen** > **SIP-Leitungen** wählen Sie im Abschnitt "Sicherheit", worauf das SIP-Zertifikat geprüft werden soll :



Server-Zert. prüfen bezüglich:

Mit dieser Einstellung legen Sie fest, ob das Zertifikat des SIP-Servers auf bestimmte Certificate Authorites (CAs) überprüft werden soll. Die CA Zertifikate von global bekannten Zertifikatsketten werden durch LCOS Updates aktualisiert und können zusätzlich durch Truststore Updates manuell auf einen aktuellen Stand gebracht werden.

Server Zertifikat	
Nicht prüfen	Das Serverzertifikat wird nicht überprüft. Alle gültigen Serverzertifikate werden akzeptiert, egal von welcher CA sie unterzeichnet wurden. Insbesondere werden somit selbst-signierte Zertifikate akzeptiert.

Server Zertifikat

Allen vertrauten CAs	Das Serverzertifikat wird gegen alle dem Gerät bekannten CAs geprüft. Dazu zählen alle im LCOS als vertrauenswürdig bekannte CAs und jene aus den VoIP Server Zertifikats Slots 1 bis 3. Nur wenn die Verbindung mit einem dieser Zertifikate erfolgreich überprüft wurde, wird die verschlüsselte Verbindung aufgebaut.
VoIP Zert.-Slot 1	Es wird überprüft, ob das Serverzertifikat von einer CA unterzeichnet wurde, deren Zertifikat in Slot 1 der VoIP Zertifikate hochgeladen wurde.
VoIP Zert.-Slot 2	Es wird überprüft, ob das Serverzertifikat von einer CA unterzeichnet wurde, deren Zertifikat in Slot 2 der VoIP Zertifikate hochgeladen wurde.
VoIP Zert.-Slot 3	Es wird überprüft, ob das Serverzertifikat von einer CA unterzeichnet wurde, deren Zertifikat in Slot 3 der VoIP Zertifikate hochgeladen wurde.
Telekom-Shared-Business-CA4	Mit dieser Einstellung akzeptiert das Gerät nur Serverzertifikate, die von der Telekom Shared Business CA4 CA unterzeichnet wurden. Verwenden Sie diese Einstellung für Telekom SIP-Trunk Anschlüsse.

16.13 Behandlung kanonischer Rufnummern

Kanonische Rufnummern (bekannt aus dem Handy, starten immer mit einem +) wurden bisher immer automatisch in Standard-Rufnummern umgewandelt: + wurde in 00 konvertiert.

Sie können im WEBconfig unter **Extras** > **LCOS-Menübaum** > **Setup** > **Voice-Call-Manager** > **Convert-Canonicals** diese automatische Umwandlung mit der Einstellung **nein** deaktivieren, so dass kanonische Rufnummern in der Call-Routing-Tabelle verarbeitet werden können. Somit können Sie z. B. für kanonische Rufnummern eigene Leitungen definieren.

16.14 Verarbeitung der Ziel-Domänen

Da die VoIP-Implementation im LANCOM VoIP Router alle vermittelten Gespräche als SIP-Gespräche behandelt, enthalten Rufnummern und SIP-Teilnehmer grundsätzlich Domain-Angaben. Darüber hinaus können SIP-Rufnummern auch alphanumerische Zeichen enthalten.

Die SIP-Domains werden im LCOS wie folgt verwendet:

- Bei der Anmeldung von SIP-Teilnehmern an übergeordneten TK-Anlagen oder am LANCOM VoIP Router selbst.
- Beim Verbindungsaufbau von SIP-Teilnehmern.

Dazu unterstützt LCOS folgende festgelegte Domains:

- ISDN für die ISDN-Schnittstellen
- Alle bei den Leitungen eingetragenen Domains

16.14.1 Anmeldung an übergeordneten Vermittlungsstellen

Anmelden können sich lokale SIP-Teilnehmer nur mit den bekannten Domains. Dabei authentifizieren sich die Teilnehmer entsprechend Benutzername und Passwort am lokalen LANCOM VoIP Router. Hiervon ausgenommen sind Domains, die einer übergeordneten SIP-TK Anlage entsprechen. Diese Anmeldungen werden in der übergeordneten SIP-TK-Anlage authentifiziert.

Versucht sich ein Teilnehmer mit einer unbekannten Domain anzumelden, so kann dieses ggf. als lokale Anmeldung akzeptiert werden.

16.14.2 Vermittlung von internen Rufen

Bei der internen Zustellung von Verbindungen ist in der Regel eine Eindeutigkeit über die interne Rufnummer gegeben. Allerdings können sich SIP-Telefone z. B. mit mehreren „Leitungen“ anmelden, z. B. '1011@provider.de' und '1011@isdn.de', um so gezielt einer Leitung auch den gewünschten Verbindungsweg zuordnen zu können.

Bei der internen Vermittlung wird entsprechend stets versucht, einen Teilnehmer zu finden, bei dem Nummer und Domain übereinstimmen. Erst wenn das nicht zum Erfolg geführt hat, wird eine Zustellung des Rufes ausschließlich anhand der Zielrufnummer durchgeführt. Die Domäne bleibt dabei unverändert.

Hierdurch werden z. B. über ISDN ankommende Rufe (von <calling pty id>@isdn) zum Teilnehmer 1011 (zu 1011@isdn) vermittelt. Damit würde der Ruf auf der ISDN-Leitungstaste am SIP-Telefon angezeigt. Ist kein solcher Teilnehmer mit einer solchen Domäne vorhanden, wird der Ruf an den ersten bekannten Teilnehmer '1011' zugestellt.

16.15 Konfiguration der ISDN-Schnittstellen

LANCOM VoIP Router verfügen über mehrere ISDN-Schnittstellen, die Sie wahlweise zum Anschluss an ISDN-Amtsleitungen oder zum Anschluss von ISDN-Endgeräten nutzen können.

ISDN-TE-Schnittstelle ("externer ISDN-Anschluss")

Eine ISDN-Schnittstelle im TE-Modus zum Anschluss an einen ISDN-Bus einer übergeordneten ISDN-TK-Anlage oder einen ISDN-NTBA. Diese ISDN-Schnittstelle kann für Backup-Verbindungen über ISDN oder als Einwahl-Schnittstelle für entfernte Gegenstellen genutzt werden.

ISDN-NT-Schnittstelle ("interner ISDN-Anschluss")

Mit der ISDN-Schnittstelle im NT-Modus stellt der LANCOM VoIP Router selbst einen internen ISDN-Bus zur Verfügung. An diese ISDN-Schnittstelle können ISDN-TK-Anlagen oder ISDN-Telefone angeschlossen werden.

Im Auslieferungszustand befindet sich die einzelne ISDN-Schnittstelle im TE-Modus und wird durch einen Kreuz-Adapter (im Lieferumfang der All-IP-Option enthalten) zum NT-Port gewandelt. Diese Funktion wird bei den LANCOM Business VoIP-Routern über das LCOS gesteuert.

- Mit mehreren TE-Schnittstellen können Sie z. B. bis zu vier B-Kanäle für Backup- oder Einwahlzwecke nutzen.
- Mit mehreren NT-Schnittstellen können Sie z. B. einer untergeordneten ISDN-TK-Anlage bis zu acht B-Kanäle bereitstellen.

Je nach Kombination von ISDN-Schnittstellen im TE- und NT-Modus müssen Sie ggf. die Busterminierung sowie softwareseitig das passende Protokoll einstellen. Die Protokoll-Einstellung berücksichtigt dabei auch den verwendeten ISDN-Anschlusstyp (Punkt-zu-Mehrpunkt oder Punkt-zu-Punkt).

16.15.1 Punkt-zu-Mehrpunkt und Punkt-zu-Punkt-Anschlüsse

LANCOM VoIP Router unterstützen Punkt-zu-Mehrpunkt- und Punkt-zu-Punkt-Anschlüsse:

- Punkt-zu-Mehrpunkt-Anschluss (Point-to-Multipoint): An einen solchen Anschluss können bis zu acht ISDN-Endgeräte direkt angeschlossen werden. Bei den Endgeräten handelt es sich z. B. um ISDN-Telefone, aber auch um

ISDN-TK-Anlagen, an die weitere Endgeräte angeschlossen werden. Alternativ kann auch ein LANCOM VoIP Router an einen Punkt-zu-Mehrpunkt-Anschluss angeschlossen werden.

- Punkt-zu-Punkt-Anschluss (Point-to-Point): An einen solchen Anschluss kann nur ein ISDN-Endgerät (meistens eine ISDN-TK-Anlage) angeschlossen werden. Alternativ kann auch ein LANCOM VoIP Router an einen Punkt-zu-Punkt-Anschluss angeschlossen werden.

Zum Anschluss eines LANCOM VoIP Router wird das verwendete Interface auf den jeweiligen Anschlusstyp eingestellt.

Die Endgeräte an einem ISDN-Anschluss können auf zwei Arten adressiert werden:

- Die Endgeräte werden über eine Multiple Subscriber Number (MSN) angesprochen, die fest mit dem ISDN-Anschluss verbunden ist und nicht beeinflußt werden kann.
- Die Endgeräte werden über eine Direct Dialing In-Nummer (DDI) angesprochen. Dabei ist nur die „Stammnummer" mit dem Anschluss verbunden, die Durchwahlnummern zur Adressierung bestimmter Endgeräte werden frei gewählt und an die Stammnummer angehängt. Dabei darf die Stammnummer mit Durchwahl zusammen mit der Otsnetzvorwahl (ohne führende Null) maximal 11 Zeichen lang sein.

Die Bezeichnungen „Mehrgeräte-Anschluss" und „Anlagen-Anschluss" werden u. a. in Deutschland zur Bezeichnung der technischen Ausführungen Point-to-Multipoint mit MSN bzw. Point-to-Point mit DDI verwendet. In anderen Ländern können die Anschlussarten durchaus andere Kombinationen aus Protokoll und Rufnummerntyp sowie abweichende Namen verwenden. Bitte informieren Sie sich bei Ihrem Netzanbieter über die technischen Spezifikationen Ihres ISDN-Anschlusses.

16.15.2 Busterminierung

Die Konfiguration der Busterminierung erfolgt entweder softwareseitig, oder wie bei der All-IP-Option über die Wahl des mitgelieferten Kreuzadapters.

Die Busterminierung ist in der Regel erforderlich bei einer ISDN-Schnittstelle im NT-Modus.

Für ISDN-Schnittstellen im TE-Modus wird die Busterminierung üblicherweise ausgeschaltet. Falls der LANCOM VoIP Router das letzte Gerät an einem längeren ISDN-Bus ist und dieser nicht selbst terminiert ist, kann ggf. die Aktivierung der Busterminierung für eine ISDN-Schnittstelle im TE-Modus sinnvoll sein.

16.15.3 Protokoll-Einstellung

Die Parameter der ISDN-Schnittstellen werden im LANconfig im Konfigurationsbereich 'Interfaces' auf der Registerkarte 'WAN' eingetragen. Unter WEBconfig, Telnet oder SSH-Client finden Sie die Einstellung der ISDN-Schnittstellen unter `Setup/Interfaces/WAN`.

Wählen Sie das Protokoll für jedes ISDN-Interface je nach Anwendung und Typ des ISDN-Anschlusses. Punkt-zu-Mehrpunkt- sowie Punkt-zu-Punkt-Anschlüsse können an einem LANCOM VoIP Router auch gemischt verwendet werden. Folgende Optionen stehen zur Auswahl:

- **Automatisch** für automatische Auswahl des Betriebsmodus (nur im TE-Modus)
- **DSS1 TE (Euro ISDN)** zum Anschluss an einen ISDN-Bus in Punkt-zu-Mehrpunkt-Ausführung („Mehrgeräte-Anschluss")
- **DSS1 TE Punkt zu Punkt** zum Anschluss an einen ISDN-Bus in Punkt-zu-Punkt-Ausführung („Anlagen-Anschluss")
- **1TR6 TE (nationales ISDN)** zum Anschluss an einen ISDN-Bus nach dem nationalen ISDN-Protokoll in Deutschland
- **DSS1 NT (Euro ISDN)** zur Bereitstellung von Schnittstellen in Punkt-zu-Mehrpunkt-Ausführung („Mehrgeräte-Anschluss")
- **DSS1 NT reverse** zur Bereitstellung von Schnittstellen in Punkt-zu-Mehrpunkt-Ausführung bei gleichzeitiger Übernahme des ISDN-Taktes der angeschlossenen ISDN-Leitung.
- **DSS1 NT Punkt zu Punkt** zur Bereitstellung von Schnittstellen in Punkt-zu-Punkt-Ausführung („Anlagen-Anschluss")
- **DSS1 NT Punkt zu Punkt reverse** zur Bereitstellung von Schnittstellen in Punkt-zu-Punkt-Ausführung („Anlagen-Anschluss") bei gleichzeitiger Übernahme des ISDN-Taktes der angeschlossenen ISDN-Leitung.
- **DSS1 Takt** zur Übernahme des ISDN-Taktes einer angeschlossenen ISDN-Leitung.

- **Aus**

Wenn ein ISDN-Endgerät an einer ISDN-Schnittstelle im Automatik-Modus nicht richtig erkannt wird, stellen Sie das verwendete Protokoll direkt ein.

16.15.4 Taktung der ISDN-Anschlüsse

Zur störungsfreien Übertragung müssen alle Komponenten des ISDN-Systems (LANCOM VoIP Router, über- bzw. untergeordnete ISDN-TK-Anlagen sowie ISDN-Endgeräte) den gleichen ISDN-Takt verwenden. Im LANCOM VoIP Router kann eine ISDN-Schnittstelle im TE-Modus den Takt von der verbundenen ISDN-Leitung übernehmen, da sich das Gerät mit der TE-Schnittstelle selbst wie ein Endgerät verhält. Der LANCOM VoIP Router kann selbst über die ISDN-Schnittstellen im NT-Modus den Takt an angeschlossene Endgeräte oder untergeordnete ISDN-TK-Anlagen weitergeben, da sich das Gerät mit der NT-Schnittstelle wie eine Vermittlungsstelle verhält.

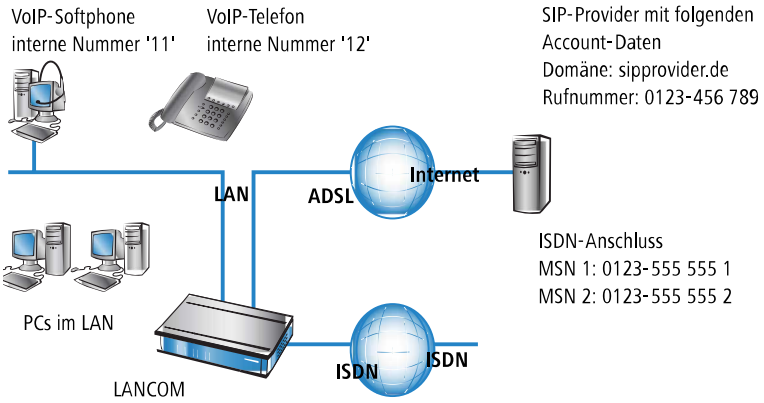
Zur Definition der ISDN-Schnittstelle, über die ein LANCOM VoIP Router den ISDN-Takt empfängt (der dann an alle Geräte an NT-Schnittstellen weitergegeben wird), stehen verschiedene Einstellungen für die ISDN-Schnittstellen zur Verfügung:

- **Automatisch**: Falls keine Schnittstelle manuell zur Taktung ausgewählt wurde, sucht das Gerät automatisch eine Schnittstelle im TE-Modus, die einen Takt liefert. Um die Taktsynchronität zu gewährleisten, versuchen TE-Anschlüsse permanent, die Aktivierung des Anschlusses aufrecht zu erhalten. Damit ist die Taktversorgung auch dann sichergestellt, wenn einmal eine von mehreren vorhandenen TE Leitungen getrennt werden sollte. Sollte kein TE-Anschluss einen Takt liefern, so läuft das Taktsystem „frei“, also nur mit dem internen Takt des LANCOM VoIP Router.
- **DSS1 Takt**: Mit dieser Einstellung wird gezielt der ISDN-Takt an diesem Anschluss für den LANCOM VoIP Router und die über NT-Schnittstellen verbundenen Geräte übernommen. So kann z. B. der Takt parallel zu einer vorhandenen ISDN-TK-Anlage an einem Anlagenanschluss geschaltet werden. Neben der Übernahme des ISDN-Taktes ist die Schnittstelle nicht aktiv.
- **DSS1 NT reverse** oder **DSS1 NT Punkt zu Punkt reverse**: Wenn alle ISDN-Schnittstellen im NT-Modus betrieben werden, läuft das Taktsystem „frei“, da kein ISDN-Takt von einer TE-Schnittstelle übernommen werden kann. Sind die ISDN-Anschlüsse in diesem Fall z. B. mit einer ISDN-TK-Anlage verbunden, die von einer anderen Quelle mit einem ISDN-Takt versorgt wird, kann es zu Übertragungsstörungen kommen, da der Takt des LANCOM VoIP Router nicht mit dem Takt der TK-Anlage synchron ist. In diesem Fall kann mit der Reverse-Einstellung gezielt der ISDN-Takt von einer Schnittstelle im NT-Modus übernommen werden, um den Takt des LANCOM VoIP Router auf das Gesamtsystem zu synchronisieren.

16.16 Konfigurationsbeispiele

16.16.1 VoIP-Telefonie im Stand-alone-Einsatz

Dieses Beispiel zeigt die Konfiguration eines LANCOM, das an einem neuen Standort als zentrales Gerät für den Internetzugang und die VoIP-Telefonie eingesetzt wird.



16.16.1.1 Ziel

- Internes Telefonieren der SIP-Telefone und SIP-Softphones.
- Erreichbarkeit der internen Endgeräte über die MSNs.
- Externes Telefonieren über den SIP-Provider mit Backup über ISDN.
- Gespräche zu Not- und Sonderrufnummern über ISDN.

16.16.1.2 Voraussetzungen

- LANCOM angeschlossen an LAN und WAN, eine ISDN-TE-Schnittstelle ist mit dem ISDN-NTBA verbunden. Der Internetzugang ist eingerichtet.
- Ein Rufnummernplan mit einer eindeutigen internen Rufnummer für jedes anzuschließende Endgerät, hier z. B. die `11` für das VoIP-Softphone und die `12` für das VoIP-Telefon.
- Ein Account bei einem SIP-Provider.

16.16.1.3 Verwendung der Informationen bei der Konfiguration

Die folgende Tabelle zeigt im Überblick, welche Informationen für die Konfiguration benötigt werden und wo sie eingetragen werden. Die Parameter für die SIP-Endgeräte werden bei einem SIP-Telefon über die Tastatur oder über die zugehörige Konfigurationssoftware bzw. bei einem Softphone im Konfigurationsmenü vorgenommen.

	LANCOM	SIP-Endgeräte	ISDN-TK-Anlage	ISDN-Endgeräte
interne VoIP-Domain	✔	✔		
interne Rufnummern	✔	✔	✔	✔
externe SIP-Rufnummer	✔			
Zugangsdaten SIP-Account	✔			

	LANCOM	SIP-Endgeräte	ISDN-TK-Anlage	ISDN-Endgeräte
externe ISDN-Rufnummern (MSNs)			✔	
Landes- und Ortsnetzvorwahl	✔			

16.16.1.4 Konfiguration des Gerätes

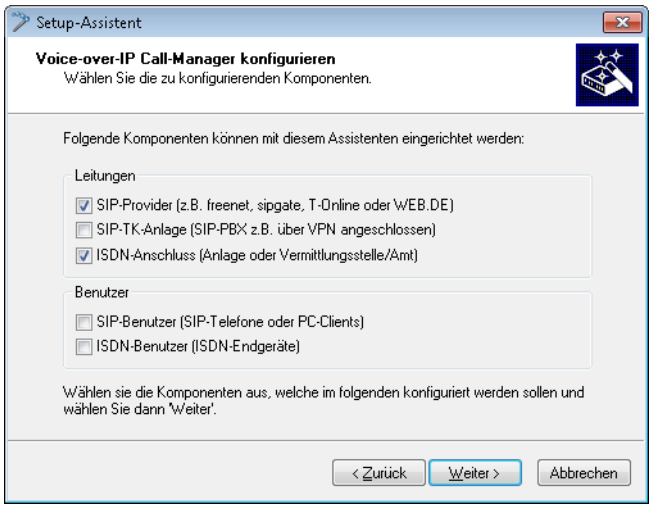
Bei der Konfiguration des Gerätes werden die folgenden Schritte durchführt:

- Einrichten der Leitung zum SIP-Provider
- Aktivieren der ISDN-Schnittstelle und Zuordnung der MSNs zu den internen Rufnummern

In diesem Beispiel ist keine Konfiguration von SIP-Benutzern erforderlich: die SIP-Benutzer können sich allein mit den Einstellungen in den Endgeräten (Softphone und VoIP-Telefon) am LANCOM anmelden!

So konfigurieren Sie das Gerät im Detail:

1. Führen Sie unter LANconfig den Setup-Assistenten zur Konfiguration des Voice-Call-Managers aus. Aktivieren Sie die Optionen **SIP-Provider** und **ISDN-Anschluss**.

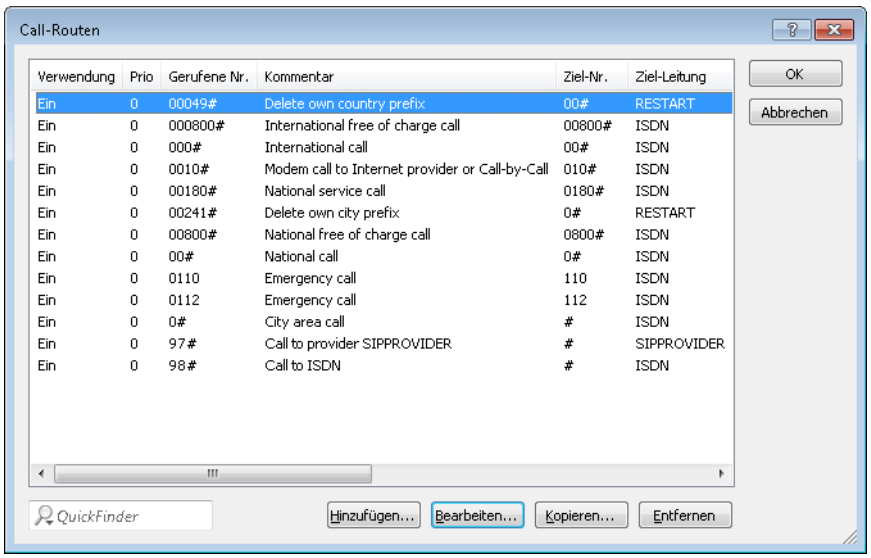


2. Geben Sie als lokale VoIP-Domäne eine eindeutige Domäne an, mit der Sie Ihren lokalen VoIP-Bereich beschreiben (z. B. `mycompany.intern`).
3. Richten Sie eine Leitung zu einem SIP-Provider z. B. mit dem Namen `SIPPROVIDER` mit den folgenden Daten an:
   - Interne Standard-Nummer: an diese interne Rufnummer werden alle Anrufe weitergeleitet, die über den SIP-Provider ankommen. Tragen Sie hier eine interne Rufnummer aus Ihrem Rufnummernplan ein, z. B. die `11`.
   - SIP-Domäne/Realm: Diese Domäne hat Ihnen Ihr SIP-Provider mitgeteilt, sie wird üblicherweise in der Form `sipdomain.tld` eingetragen, ohne den Teil, der einen bestimmten Server bezeichnet.
   - Registrar (FQDN) / -IP (optional)
   - Outbound-Proxy (optional)
   - SIP-ID / Benutzer: Tragen Sie hier die SIP-Rufnummer mit Ortsnetzvorwahl ein, sofern vom SIP-Provider nicht anders angegeben.
   - Display-Name (optional): Der Display-Name ist nur notwendig, wenn er vom SIP-Provider bei der Anmeldung überprüft wird. Wenn Sie hier einen Display-Namen eintragen, wird dieser Name bei der Gegenstelle angezeigt. Wenn das Feld frei bleibt, wird der jeweilige Display-Name der internen Benutzer übertragen.

- Authentifizierungsname (optional): Ein spezieller Authentifizierungsname wird nicht von allen SIP-Providern verwendet. Der Authentifizierungsname ist in vielen Fällen gleich der SIP-ID bzw. dem Benutzernamen. Füllen Sie dieses Feld nur aus, wenn Ihnen der SIP-Provider einen speziellen Authentifizierungsnamen mitgeteilt hat.
- Passwort: Tragen Sie hier das Passwort für den SIP-Zugang ein.

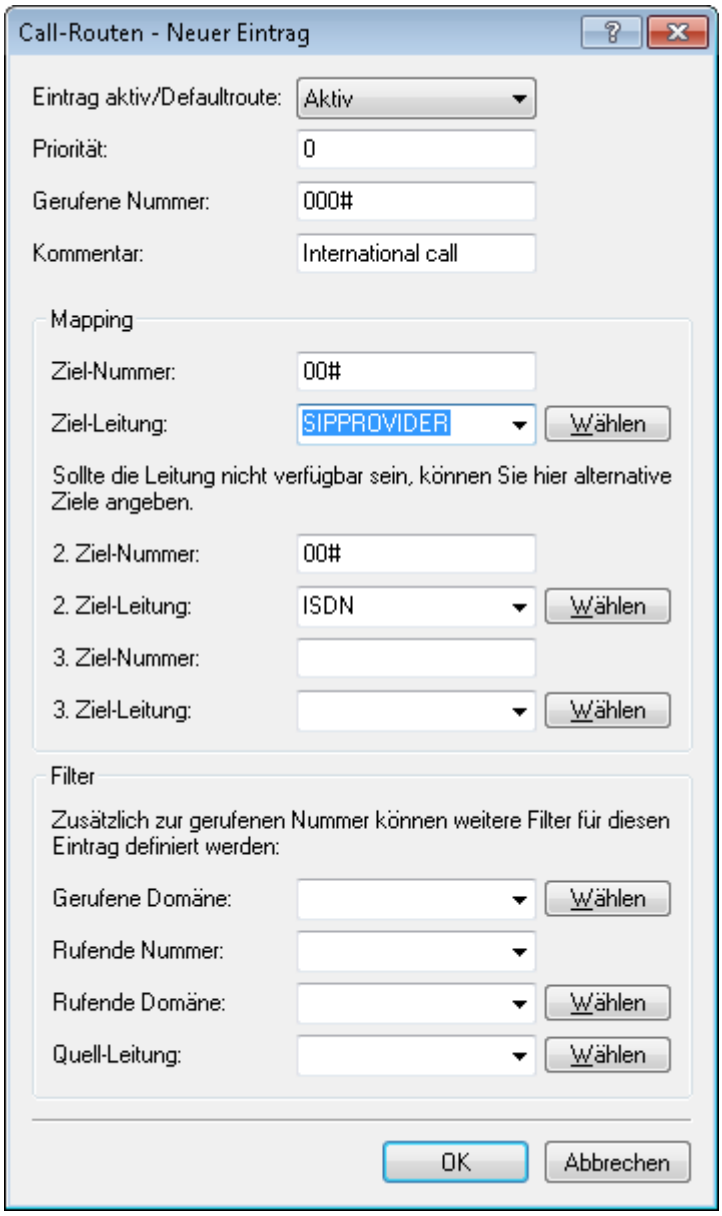
Diese Beschreibung bezieht sich auf eine „benutzerdefinierte Konfiguration". Falls Sie einen speziellen SIP-Provider aus der Liste auswählen, wird ein Teil der Parameter automatisch vorkonfiguriert.

4. Richten Sie eine ISDN-Leitung für die Nutzung der VoIP-Telefonie ein. Legen Sie beim ISDN-Mapping für jede MSN Ihres ISDN-Anschlusses eine Zuordnung zu einer internen Rufnummer Ihres Rufnummernplans fest:
   - MSN 1 `555 555 1` / Interne Rufnummer `11`
   - MSN 2 `555 555 2` / Interne Rufnummer `12`
5. Geben Sie die Orts- und Landesvorwahl für den Standort des Gerätes an. Anhand dieser Informationen kann der Voice-Call-Manager unterscheiden, ob es sich bei abgehenden Anrufen um Ortsgespräche, nationale oder internationale Ferngespräche handelt.
6. Mit den bisherigen Angaben erstellt LANconfig einen Vorschlag für die Call-Routing-Tabelle, den Sie nachfolgend an Ihre Bedürfnisse anpassen können:



Das #-Zeichen steht als Platzhalter für beliebige Zeichenfolgen. Der Eintrag `0#` passt also auf alle gerufenen Nummern, die mit mindestens einer führenden `0` beginnen.

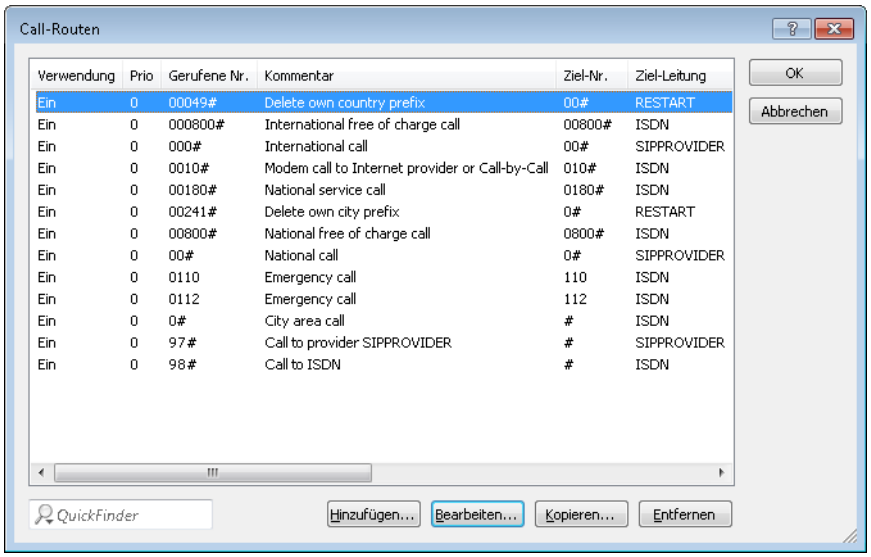
Mit dieser vorgeschlagenen Call-Routing-Tabelle werden zunächst alle externen Gespräche über die ISDN-Leitung geführt. Für internationale und nationale Ferngespräche sowie Ortsgespräche, die nicht zu den eingetragenen Sonder- oder Notfallrufnummern gehören, ist die SIP-Leitung als Backup eingestellt.



Um spezielle Anrufeziele wie z. B. internationale und nationale Ferngespräche über den SIP-Provider zu führen, doppelklicken Sie auf die entsprechenden Einträge in der Tabelle und stellen die verwendete Leitung von `ISDN` auf

`SIPPROVIDER` um. Vergessen Sie nicht, die Backup-Leitung bei Bedarf entsprechend von `SIP` auf `ISDN` umzustellen!

Nach der Anpassung für internationale und nationale Ferngespräche sieht die Call-Routing-Tabelle dann z. B. so aus:



16.16.1.5 Konfiguration der VoIP-Endgeräte

Stellen Sie im Softphone die Anmeldedaten für den ersten SIP-Benutzer ein.

16.16.1.6 Ablauf des Call-Routings bei abgehenden Rufen

Bei abgehenden Anrufen durchsucht der Call-Manager zunächst Call-Routing-Tabellen von oben nach unten. Findet sich dort kein passender Eintrag, verwendet der Call-Manager die Liste der angemeldeten Benutzer:

	Benutzer	wählt	passende Call-Route	passender Benutzer	Mapping, verwendete Nummer	Ziel-Leitung
1	VoIP-Telefon	`11`	keine	VoIP-Softphone	`11`	intern
2	VoIP-Telefon	`0 555 555`	**3** `0#`		`0241#: 0241 555 555`	ISDN
3	VoIP-Telefon	`0 0123 666 666`	**3** `00#`		`0#: 0123 666 666`	SIP-Provider

1. Der Call-Manager findet in der Call-Routing-Tabelle keinen Eintrag, der auf die `11` passt. Also sucht er in der Liste der angemeldeten Teilnehmer und findet dort den internen SIP-Benutzer

   Für das Call-Routing werden nicht nur die im LANCOM konfigurierten Benutzer verwendet, sondern alle tatsächlich am Call-Router angemeldeten Benutzer. Die SIP-Benutzer können sich auch dann erfolgreich am Call-Router anmelden, wenn Sie nicht im LANCOM eingetragen sind. Der Eintrag der internen VoIP-Domäne des LANCOM reicht zur Anmeldung aus, sofern nicht die lokale Authentifizierung vorgeschrieben ist.

2. Der Eintrag **3** der oben abgebildeten Call-Routing-Tabelle passt auf die gewählte Nummer. Der Call-Router entfernt die vorangestellte `0` für die Amtsholung, ergänzt die Vorwahl des eigenen Ortsnetzes und führt den Anruf zu `0241 555 555` über die ISDN-Leitung aus.

   Die Vorwahl des eigenen Ortsnetzes wird ergänzt, weil beim Anruf über SIP-Provider meistens eine Vorwahl mitgewählt werden muss.

3. Hier passt der Eintrag der Call-Routing-Tabelle. Der Call-Router entfernt die vorangestellte `0` für die Amtsholung und führt den Anruf zu `0123 555 555` über die SIP-Leitung aus. Falls die SIP-Leitung nicht verfügbar ist, wird der Anruf über die ISDN-Leitung ausgeführt.

16.16.1.7 Ablauf des Call-Routings bei eingehenden Rufen

Bei eingehenden Anrufen werden von den Vermittlungsstellen in den Telefonnetzen die Vorwahlen der angerufenen Rufnummer (Ziel-Nummer) entfernt. Das LANCOM empfängt also nur die reine Rufnummer, die je nach Quelle unterschiedlich behandelt wird:

- Rufnummern aus dem ISDN-Netz werden anhand der ISDN-Mapping-Tabelle auf die interne Rufnummer umgesetzt, die zur empfangenen MSN eingetragen ist.
- Rufe aus einem SIP-Netz werden auf die interne Zielnummer umgesetzt, die für die jeweilige SIP-Leitung eingetragen ist.

Mit der geänderten Rufnummer durchsucht der Call-Manager zunächst die Call-Routing-Tabelle von oben nach unten. Findet sich dort kein passender Eintrag, wird der Anruf direkt an die interne Rufnummer weitergeleitet:

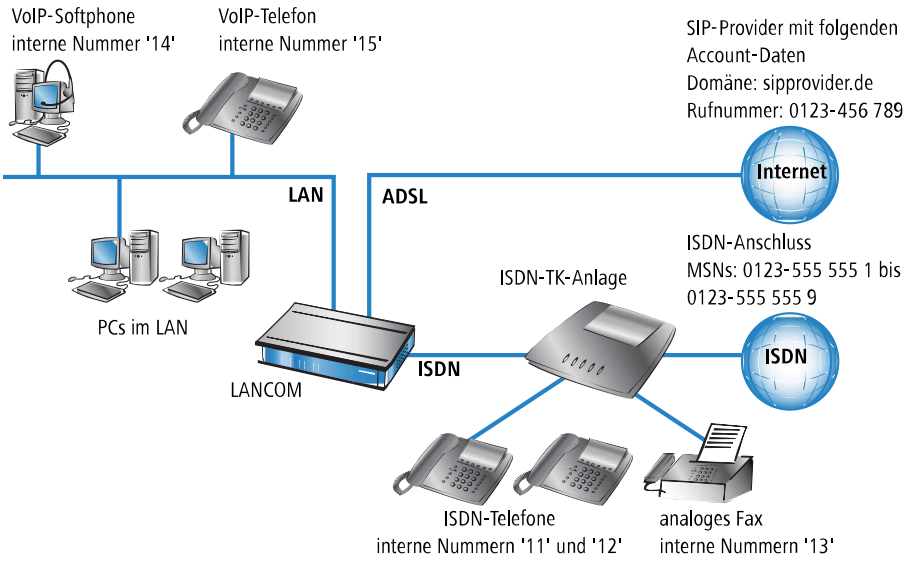
	Gegenstelle wählt	Call-Router empfängt	Zuordnung über	verwendete Nummer	passende Call-Route	Ziel-Leitung
1	`0 123 456 789`	`456 789`	interne Zielnummer für SIP-Leitung	`11`	keine	intern
2	`0 123 555 555`	`555 555 11`	ISDN-Mapping	`11`	keine	intern
3	`0 123 555 555`	`555 555 22`	ISDN-Mapping	`12`	keine	intern

16.16.2 VoIP-Telefonie als Ergänzung zur übergeordneten ISDN-TK-Anlage

Dieses Beispiel zeigt die Konfiguration eines LANCOM, wenn eine übergeordnete ISDN-TK-Anlage um die Möglichkeiten der VoIP-Telefonie erweitert wird. Die MSNs `11` bis `13` des ISDN-Anschlusses werden bisher für zwei ISDN-Telefone und ein analoges Fax verwendet.

Die TK-Anlage ist so konfiguriert, dass die Teilnehmer eine `0` vorwählen müssen, um ein Amt für externe Anrufe zu erhalten.

Das LANCOM Gerät wird an einem Nebenstellenanschluss der TK-Anlage betrieben.



16.16.2.1 Ziel

- Internes Telefonieren der ISDN- und SIP-Telefone sowie SIP-Softphones.
- Externes Telefonieren der VoIP-Endgeräte über den SIP-Provider mit Backup über ISDN.
- Externes Telefonieren der ISDN-Endgeräte an der TK-Anlage. Je nach Funktionsumfang der ISDN-TK-Anlage können die ISDN-Endgeräte dazu auch die SIP-Leitungen im LANCOM VoIP Router nutzen.
- Erreichbarkeit der internen Endgeräte (ISDN und SIP) über die MSNs.
- Gespräche zu Not- und Sonderrufnummern über ISDN.

16.16.2.2 Voraussetzungen

- LANCOM Gerät angeschlossen an LAN und WAN, eine ISDN-TE-Schnittstelle ist mit dem Nebenstelleneingang der ISDN-TK-Analge verbunden. Der Internetzugang ist eingerichtet.
- Ein Rufnummernplan mit einer eindeutigen internen Rufnummer für jedes anzuschließende Endgerät. Die verwendeten Rufnummern werden dabei in der Regel von der TK-Anlage vorgegeben, die in vielen Fällen nur einen bestimmten Rufnummernkreis zulassen.
- Ein Account bei einem SIP-Provider.

16.16.2.3 Verwendung der Informationen bei der Konfiguration

Der Rufnummernplan mit ISDN-TK-Anlagen: Beim Übergang vom ISDN-Netz zu den internen Teilnehmern findet in der ISDN-TK-Anlage eine Umsetzung der externen MSNs zu den internen MSNs statt. Beim Betrieb eines LANCOM VoIP Router am Nebenstelleneingang der ISDN-TK-Anlage findet eine erneute Umsetzung der internen MSNs der TK-Anlage zu den internen Rufnummern im VoIP-Bereich statt. Wir empfehlen aus Gründen der Übersichtlichkeit, für die Endgeräte über alle verbundenen Bereiche hinweg deckungsgleiche interne MSNs/Rufnummern zu verwenden!

Die folgende Tabelle zeigt im Überblick, welche Informationen für die Konfiguration benötigt werden und wo sie eingetragen werden. Die Parameter für die SIP-Endgeräte werden bei einem SIP-Telefon über die Tastatur oder über die zugehörige Konfigurationssoftware bzw. bei einem Softphone im Konfigurationsmenü vorgenommen.

	LANCOM	SIP-Endgeräte	ISDN-TK-Anlage	ISDN-Endgeräte
interne VoIP-Domain	✔	✔		
interne Rufnummern	✔	✔	✔	✔

	LANCOM	SIP-Endgeräte	ISDN-TK-Anlage	ISDN-Endgeräte
externe SIP-Rufnummer	✔			
Zugangsdaten SIP-Account	✔			
externe ISDN-Rufnummern (MSNs)			✔	
Landes- und Ortsnetzvorwahl	✔			

16.16.2.4 Konfiguration des Gerätes

Bei der Konfiguration des LANCOM werden die folgenden Schritte durchgeführt:

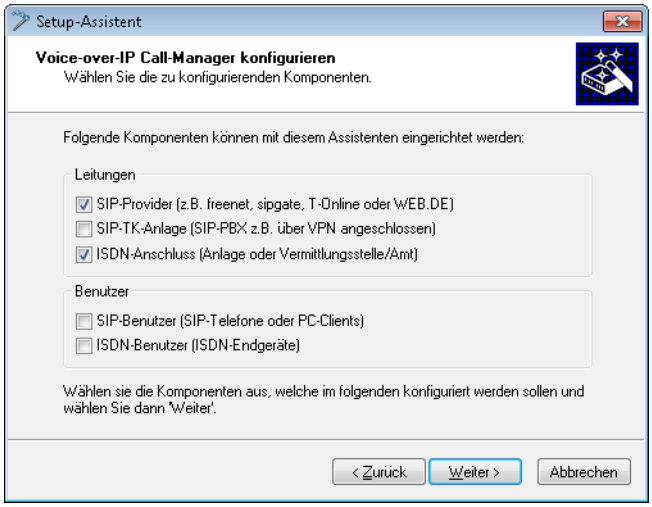
- Einrichten der Leitung zum SIP-Provider
- Aktivieren der ISDN-Schnittstelle und Zuordnung der internen MSNs der TK-Anlage zu den internen Rufnummern im LANCOM VoIP Router
- Anpassen der Call-Routing-Tabelle

In diesem Beispiel ist keine Konfiguration von SIP- oder ISDN-Benutzern erforderlich:

- Die SIP-Benutzer können sich allein mit den Einstellungen in den Endgeräten (Softphone und VoIP-Telefon) am LANCOM anmelden.
  - Die ISDN-Geräte können über einen entsprechenden Eintrag in der Call-Routing-Tabelle erreicht werden.

So konfigurieren Sie das LANCOM Gerät im Detail:

1. Führen Sie unter LANconfig den Setup-Assistenten zur Konfiguration des Voice-Call-Managers aus. Aktivieren Sie die Optionen **SIP-Provider** und **ISDN-Anlage oder -Vermittlungsstelle**.



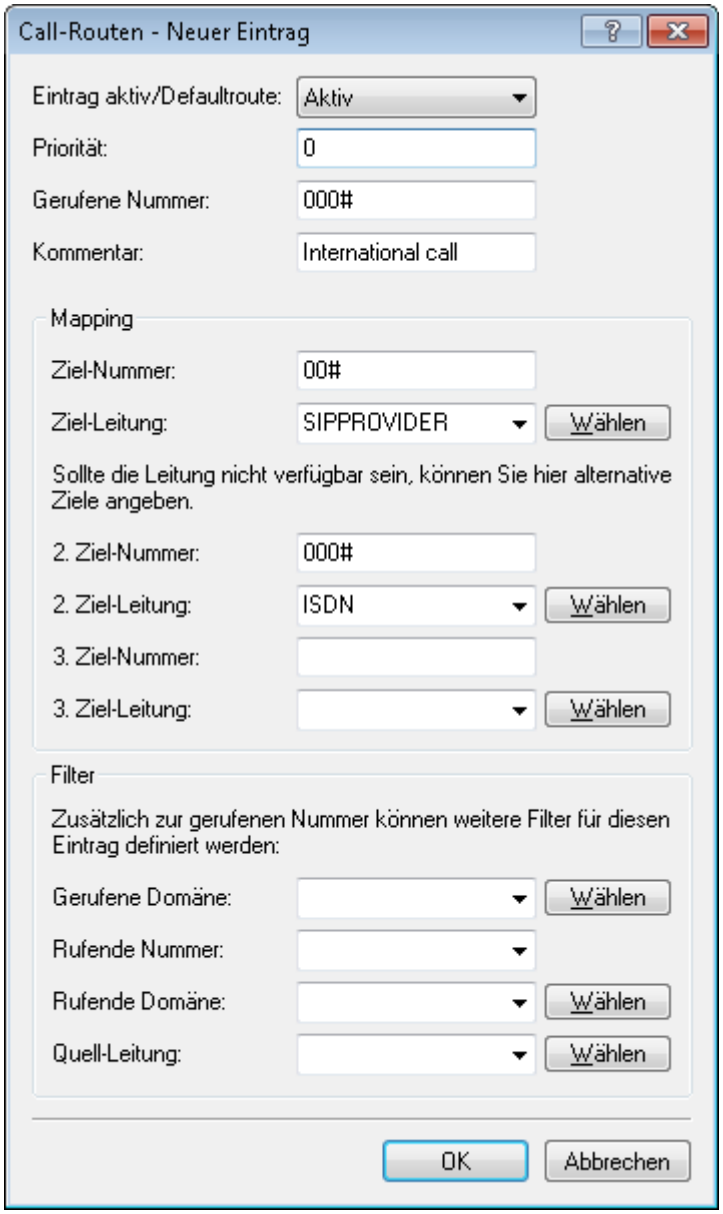
2. Richten Sie ein wie in den vorhergehenden Beispielen beschrieben:

   eindeutige lokale VoIP-Domäne

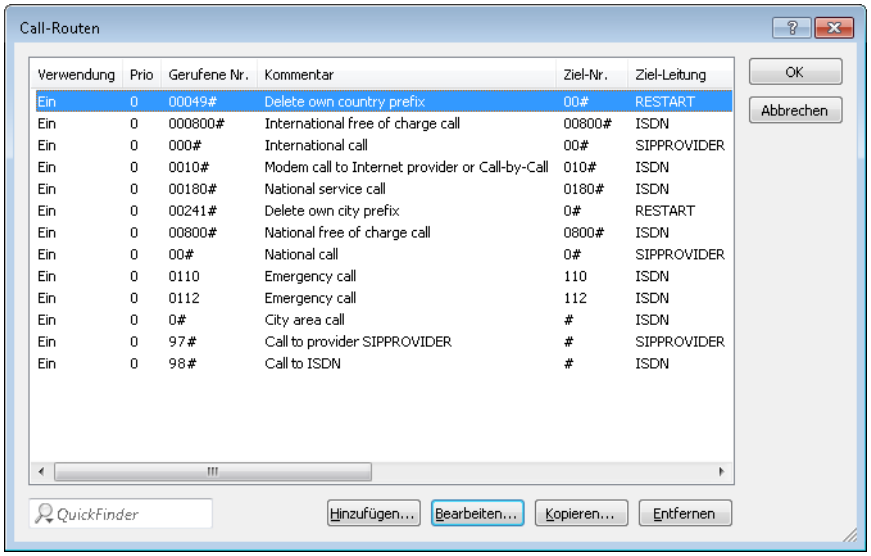
   eine Leitung zu einem SIP-Provider

   ISDN-Leitung

3. Passen Sie die vorgeschlagene Call-Routing-Tabelle an, um spezielle Rufnummern-Ziele automatisch über die Leitung des SIP-Providers zu führen. Das folgende Beispiel zeigt den Eintrag für die Auslandsgespräche.



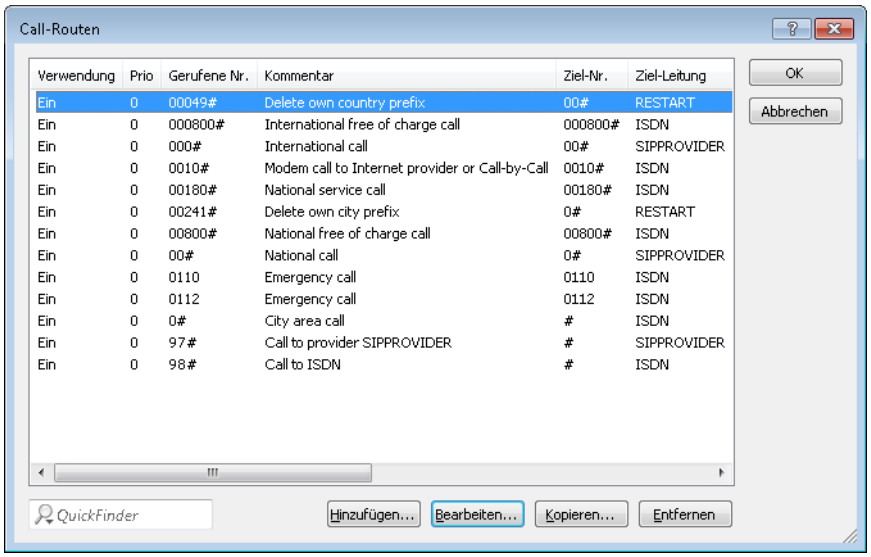
1. Nach der Anpassung sieht die Call-Routing-Tabelle dann z. B. so aus:



   Bei jedem Ferngespräch wird also die führende 0 aus der Rufnummer entfernt, der Ruf wird über den SIP-Provider geführt.

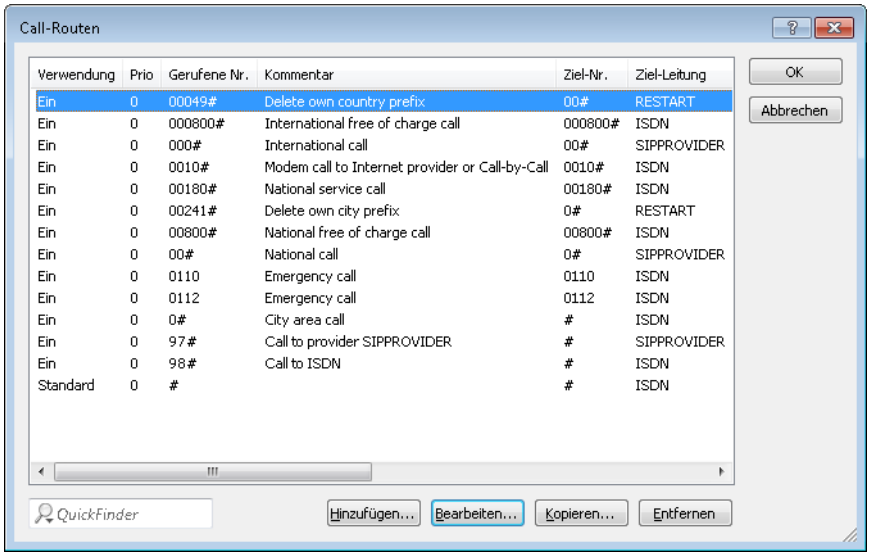
2. Für alle Anrufe über ISDN darf die führende 0 jedoch nicht aus der Ziel-Rufnummer entfernt werden, da die übergeordnete ISDN-TK-Anlage die 0 zur Amtsholung benötigt! Passen Sie daher die Ziel-Nummer bei allen Einträgen mit der Ziel-Leitung 'ISDN' entsprechend an.

   Nach der Anpassung sieht die Call-Routing-Tabelle dann z. B. so aus:



3. Damit die ISDN-Teilnehmer intern von den VoIP-Benutern erreicht werden können, wird zusätzlich eine Standardroute eingerichtet, die alle vorher nicht aufgelösten Rufe ohne Veränderung der Rufnummer auf der ISDN-Leitung ausgibt.

Nach der Anpassung sieht die Call-Routing-Tabelle dann z. B. so aus:



Diese Call-Routing-Tabelle gilt ausdrücklich nur für eine TK-Anlage, an der die Teilnehmer eine `0` vorwählen müssen, um ein Amt für externe Anrufe zu erhalten. Verwendet die TK-Anlage einen anderen Mechanismus zur Amtsholung, muss die Tabelle entsprechend angepasst werden.

16.16.2.5 Konfiguration der VoIP-Endgeräte

Die Konfiguration der VoIP-Endgeräte verläuft so wie in den vorhergehenden Beispielen beschrieben mit interner VoIP-Domäne und internen Rufnummern des eigenen Standortes.

16.16.2.6 Konfiguration der ISDN-TK-Anlage

Bei der Konfiguration der TK-Anlage findet die Zuordnung der externen MSNs zu den internen MSNs statt. Dabei wird auch für jedes VoIP-Endgerät eine freie interne MSN mit einer externen MSN verknüpft.

Externe und interne Anrufe von ISDN-Endgeräten in die VoIP-Telefonie

Die ISDN-Endgeräte übergeben beim Rufaufbau die gewünschte Ziel-Rufnummer zunächst an die ISDN-TK-Anlage. Wenn es sich dabei um eine interne Rufnummer/MSN handelt, gibt die TK-Anlage den Ruf wieder auf dem internen ISDN-Bus aus. Die am LANCOM angeschlossenen SIP-Endgeräte können also nur dann über ein internes Gespräch erreicht werden, wenn die interne Rufnummer der VoIP-Benutzer in der TK-Anlage bekannt ist.

Sofern Ihre TK-Anlage externe Rufnummern über den internen ISDN-Bus ausgeben kann, können die ISDN-Endgeräte auch die im LANCOM konfigurierten Leitungen wie z. B. die Leitung über einen SIP-Provider für abgehende externe Anrufe nutzen.

16.16.2.7 Konfiguration der ISDN-Endgeräte

Die Konfiguration der ISDN-Endgeräte beschränkt sich in der Regel auf den Eintrag der verwendeten internen MSN der TK-Anlage.

16.16.2.8 Ablauf des Call-Routings bei abgehenden Rufen

	Benutzer	wählt	passende Call-Route	passender Benutzer	Mapping, verwendete Nummer	Ziel-Leitung
1	VoIP-Telefon	`14`	keine	VoIP-Softphone	`14`	intern

	Benutzer	wählt	passende Call-Route	passender Benutzer	Mapping, verwendete Nummer	Ziel-Leitung
2	VoIP-Telefon	`11`	**3** # (Standard)		`#: 11`	ISDN
3	ISDN-Telefon	`14`	**1.** TK-Anlage	VoIP-Softphone	`14`	intern
4	VoIP-Telefon	`0 555 555`	**2** `0#`		`00241#: 0 555 555`	ISDN
5	ISDN-Telefon	`0 555 555`	**1.** TK-Anlage		`555 555`	ISDN-Amt
6	VoIP-Telefon	`0 0123 666 666`	**1** `00#`		`0#: 0123 666 666`	SIP-Provider

1. Interner Anruf zwischen zwei VoIP-Endgeräten.
2. Interner Anruf von VoIP nach ISDN. Im ersten Durchlauf (ohne die Standard-Routen) passt keine der Routen auf die Rufnummer `11`, auch in der Liste der angemeldeten Benutzer gibt es keinen passenden Eintrag. Im zweiten Durchlauf trifft die Standard-Route `#` (Eintrag **3** der oben abgebildeten Call-Routing-Tabelle) und gibt den Ruf **unverändert** auf der ISDN-Leitung aus. Die TK-Anlage empfängt den Ruf auf dem internen ISDN-Bus, erkennt die gerufene Nummer als interne MSN und gibt den Ruf wieder auf dem internen ISDN-Bus aus, an den das entsprechende ISDN-Endgerät angeschlossen ist.
3. Interner Anruf von ISDN nach VoIP. Die ISDN-TK-Anlage erkennt die Ziel-Rufnummer `14` als interne MSN und gibt den Ruf auf dem zugehörigen internen ISDN-Bus aus. Der Call-Router empfängt den Ruf zu `14`, findet in der Call-Routing-Tabelle keinen passenden Eintrag, wohl aber in der Liste der angemeldeten Benutzer.
4. Externer Anruf von VoIP ins eigene Ortsnetz. Der Eintrag **2** der oben abgebildeten Call-Routing-Tabelle passt auf die gewählte Nummer. Der Call-Router ergänzt die Vorwahl des eigenen Ortsnetzes und gibt den Anruf auf der ISDN-Leitung aus. Erst die TK-Anlage entfernt die vorangestellte `0` für die Amtsholung und führt den Anruf zu `0241 555 555` über den ISDN-Amtsanschluss aus.
5. Externer Anruf von ISDN ins eigene Ortsnetz. Die ISDN-TK-Anlage erkennt die Zielrufnummer als externes Ziel, entfernt die vorangestellte `0` für die Amtsholung und führt den Anruf zu `555 555` über den ISDN-Amtsanschluss aus.
6. Externer Anruf von VoIP in ein nationales Ortsnetz. Hier passt der Eintrag **2** der Call-Routing-Tabelle. Der Call-Router entfernt die vorangestellte `0` für die Amtsholung und führt den Anruf zu `0123 555 555` über die SIP-Leitung aus. Falls die SIP-Leitung nicht verfügbar ist, wird er über die ISDN-Leitung ausgeführt. In diesem Fall wird die führende `0` nicht aus der Ziel-Rufnummer entfernt, um an der TK-Anlage eine Amtsleitung zu bekommen.

16.16.2.9 Ablauf des Call-Routings bei eingehenden Rufen

	Gegenstelle wählt	Call-Router empfängt	Zuordnung über	verwendete Nummer	passende Call-Route	Ziel-Leitung
1	`0 123 456 789`	`456 789`	interne Zielnummer für SIP-Leitung	`11`	keine	ISDN
2	`0 123 555 555 1`		ISDN-TK-Anlage	`11`		intern
3	`0 123 555 555 14 4`		**1.** ISDN-TK-Anlage **2.** Liste der lokalen Benutzer	`14`	keine	intern

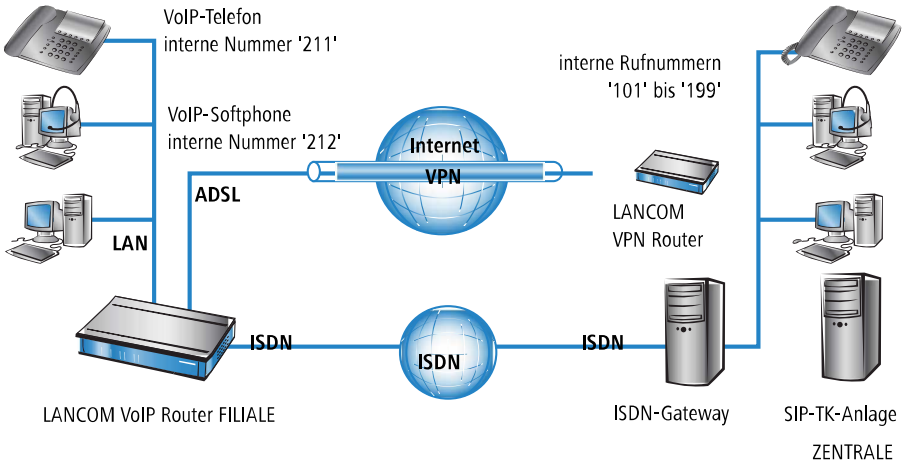
1. Der eingehende Anruf über die Rufnummer der SIP-Leitung wird mit der konfigurierten internen Zielnummer an den Call-Router übergeben. Der Call-Router findet keinen passenden Eintrag in der Call-Routing-Tabelle, jedoch einen

angemeldeten Benutzer mit der passenden internen Rufnummer. Da es sich um einem ISDN-Benutzer handelt, gibt der Call-Router den Ruf auf der ISDN-Leitung aus. Die TK-Anlage empfängt die `11` und kann diesen Ruf als internen Anruf dem angeschlossenen ISDN-Telefon zuordnen.

2. Die eingehenden Anrufe an die MSNs für die angeschlossenen ISDN-Endgeräte können von der TK-Anlage selbst direkt zugeordnet werden, der Call-Router ist hier nicht beteiligt.
3. Die eingehenden Anrufe an die MSNs für die VoIP-Endgeräte werden von der TK-Anlage mit der internen MSN auf dem internen ISDN-Bus ausgegeben. Der Call-Router empfängt diese Anrufe wie interne Rufe und gibt sie an die passenden Benutzer weiter, da auch hier kein Eintrag in der Call-Routing-Tabelle zutrifft.

16.16.3 Anbindung an übergeordnete SIP-TK-Anlage

In diesem Beispiel wird das Netzwerk einer Filiale über VPN an das Netz der Zentrale angebunden. Neben der Datenübertragung wird dabei die Telefonstruktur der Filiale auch mit der zentralen SIP-TK-Anlage verbunden. Im Netz der Filiale kommt ein LANCOM VoIP Router zum Einsatz, im Netz der Zentrale stellt z. B. ein LANCOM VPN Router den VPN-Endpunkt dar. Die Telefonie-Teilnehmer in der Zentrale bekommen interne Rufnummern aus dem Nummerkreis `101` bis `199`, für die Filialen ist jeweils ein 10er-Block aus dem 200er-Bereich vorgesehen, in diesem Beispiel die `211` bis `219`.



16.16.3.1 Ziel

- Internes Telefonieren über alle Standorte hinweg.
- Externes Telefonieren aus der Filiale über die SIP-PBX der Zentrale mit Backup über ISDN.
- Gespräche aus der Filiale ins eigene Ortsnetz über ISDN.
- Gespräche zu Not- und Sonderrufnummern über ISDN.

16.16.3.2 Voraussetzungen

- LANCOM Gerät angeschlossen an LAN und WAN, eine ISDN-TE-Schnittstelle ist mit dem ISDN-NTBA verbunden.
- Der Internetzugang ist eingerichtet, ebenso die Netzkopplung der beiden Standorte über einen VPN-Tunnel. Alle angeschlossenen Endgeräte können sich über die verwendeten IP-Adressen erreichen.
- Ein Rufnummernplan mit einer eindeutigen internen Rufnummer für jedes anzuschließende Endgerät.
- Ein Account bei einem SIP-Provider.

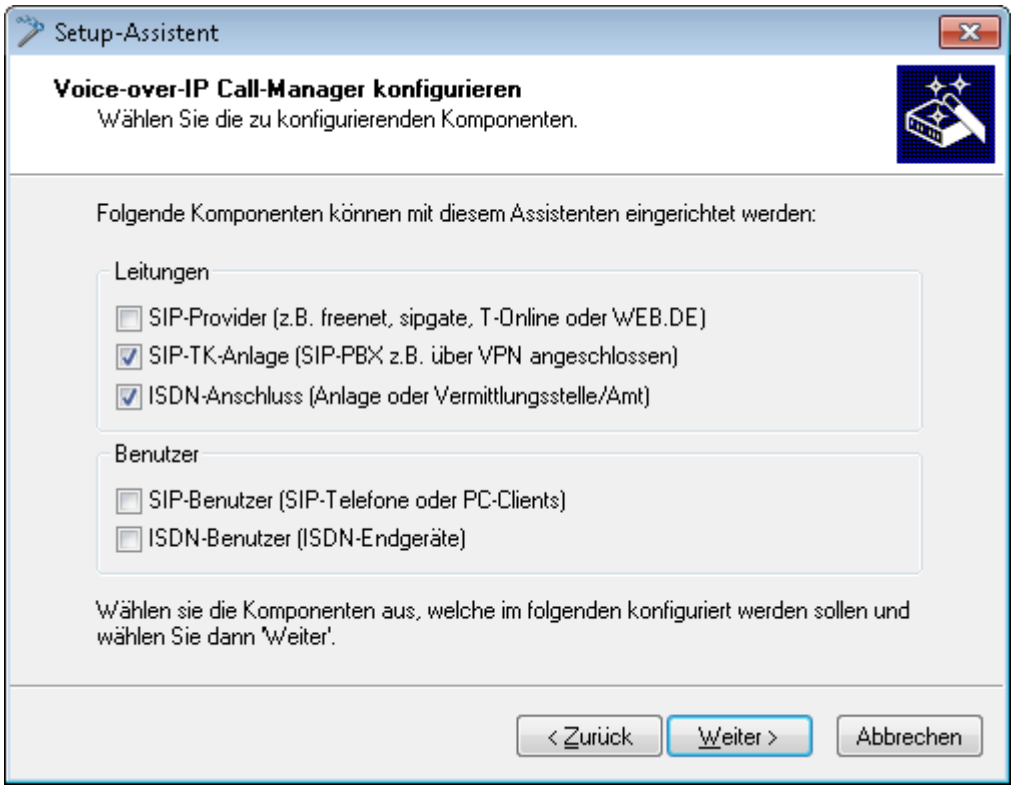
16.16.3.3 Konfiguration des Gerätes

Die folgende Tabelle zeigt im Überblick, welche Informationen für die Konfiguration benötigt werden und wo sie eingetragen werden. Im Prinzip wird lediglich an jedem Standort eine SIP-TK-Leitung "über Kreuz" mit dem entfernten Standort eingerichtet

	LANCOM Filiale	SIP-Endgeräte Filiale	SIP-PBX Zentrale
interne VoIP-Domain	`mycompany.BRANCH01`	`mycompany.HQ`	`mycompany.HQ`
interne Rufnummern der SIP-Teilnehmer in der Filiale		✔	✔
externe ISDN-Rufnummern (MSNs)	✔		
Landes- und Ortsnetzvorwahl	✔		
SIP-PBX-Leitung	HQ		
SIP-PBX-Domäne	`mycompany.HQ`		
Passwort für Anmeldung an der SIP-PBX	✔		✔
Call-Route	1. Gerufene Nummer `2#` 2. `Ziel-Leitung LOCATION_B` 3. Ziel-Nummer `2#`		

So konfigurieren Sie das LANCOM im Detail:

1. Führen Sie unter LANconfig den Setup-Assistenten zur Konfiguration des Voice-Call-Managers aus. Aktivieren Sie die Optionen **SIP-TK-Anlage** und **ISDN-Anschluss**.



2. Richten Sie ein wie in den vorhergehenden Beispielen beschrieben:
   - ISDN-Leitung mit MSN-Mapping
   - Orts- und Landesvorwahl für jeweiligen Standort

3. Geben Sie als lokale VoIP-Domäne eine eindeutige Domäne an, mit der Sie den lokalen VoIP-Bereich der Filiale beschreiben, z. B. `mycompany.BRANCH01` für die erste Filiale.

4. Richten Sie die Leitung zur SIP-TK-Anlage ein mit den folgenden Werten:

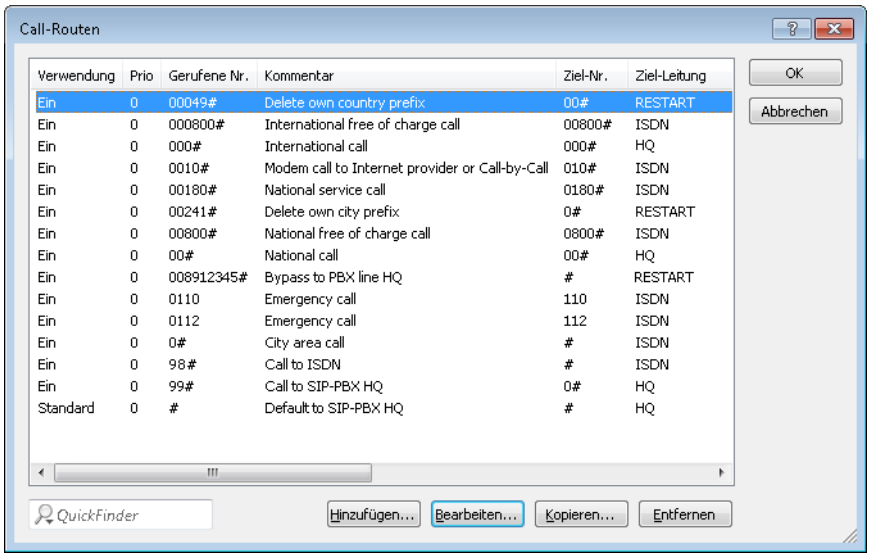
   - SIP-PBX-Leitungs-Name: eindeutiger Name für die Leitung zur SIP-PBX, z. B. `HQ` für "Headquarter".
   - PBX SIP-Domäne/Realm: interne VoIP-Domäne der SIP-PBX, z. B. `mycompany.HQ`.
   - Registrar (FQDN oder IP) (optional): Adresse der SIP-PBX im Netz der Zentrale, falls das Gerät nicht über DNS-Auflösung der VoIP-Domäne (PBX SIP-Domäne/Realm) identifiziert werden kann.

     Verwenden Sie hier die über VPN erreichbare IP-Adresse der SIP-PBX aus dem privaten IP-Adresskreis der Zentrale.
   - Outbound-Proxy (optional): Die Bezeichnung des Outbound-Proxys benötigen Sie in der Regel nicht. Tragen Sie hier nur eine Serverbezeichnung ein, falls SIP-PBX Ihre entsprechenden Adressen benötigt.
   - Gemeinsames PBX-Passwort: Dieses Passwort verwenden alle SIP-Benutzer für die Anmeldung an der SIP-PBX. Falls die Anmeldung mit einem gemeinsamen Passwort nicht erwünscht ist, kann auch für jeden SIP-Benutzer ein eigenes Passwort verwendet werden. In diesem Fall wird jeder SIP-Benutzer im LANCOM mit einem eigenen Passwort konfiguriert.
   - Öffentliche PBX-Nummer: Geben Sie hier die Rufnummer der SIP-PBX an, mit der sie vom Standort des LANCOM aus über das öffentliche Telefonnetz erreicht werden können. Die Rufnummer wird mit den **notwendigen** Vorwahlen, aber ohne eine Durchwalnummer angegeben. Befindet sich z. B. die SIP-PBX in München und das LANCOM in Aachen, lautet die öffentliche PBX-Nummer `089 12345`.

5. Die vom Setup-Assistenten vorgeschlagene Call-Routing-Tabelle berücksichtigt automatisch die Ausführung von internationalen und nationalen Ferngesprächen über die SIP-PBX in der Zentrale.

   Eine **Standard-Route** wird zudem genutzt, um Anrufe aus dem VoIP-Bereich des LANCOM an interne Rufnummern der SIP-PBX über die zugehörige SIP-PBX-Leitung auszuführen.

   Dieser spezielle Eintrag wird erst im zweiten Durchlauf der Call-Routing-Tabelle verwendet, nachdem im ersten Durchlauf bei den "normalen" Routen keine Übereinstimmung erzielt wurde und auch in der Liste der lokalen Benutzer keine passende interne Rufnummer gefunden wurde.



16.16.3.4 Konfiguration der VoIP-Endgeräte

Die Konfiguration der VoIP-Endgeräte verläuft so wie in den vorhergehenden Beispielen beschrieben, hier jedoch mit der VoIP-Domäne der SIP-PBX und den in der SIP-PBX konfigurierten internen Rufnummern.

Automatische Anmeldung der SIP-Benutzer beim LANCOM und bei der SIP-PBX

Durch die Verwendung der SIP-PBX-Domäne in den VoIP-Endgeräten werden zwei Anmeldungen erreicht:

- Da die Anmeldung mit einer im LANCOM definierten gültigen Domäne erfolgt, werden die Endgeräte als "lokale Benutzer" angemeldet.
- Da die verwendete Domäne nicht mit der eigenen VoIP-Domäne des LANCOM übereinstimmt, wird parallel die Anmeldung an der übergeordneten SIP-PBX versucht. Stimmt das dafür verwendete Passwort mit dem in der SIP-PBX hinterlegten Passwort für diesen Benutzer überein, wird auch die Anmeldung an der SIP-PBX erfolgreich durchgeführt.

16.16.3.5 Konfiguration der SIP-PBX

In der SIP-PBX werden alle Benutzer aus dem Netz der Filiale mit der jeweiligen internen Rufnummer eingetragen. Dazu wird entweder das gemeinsame Passwort oder für jeden Benutzer ein separates Passwort vergeben.

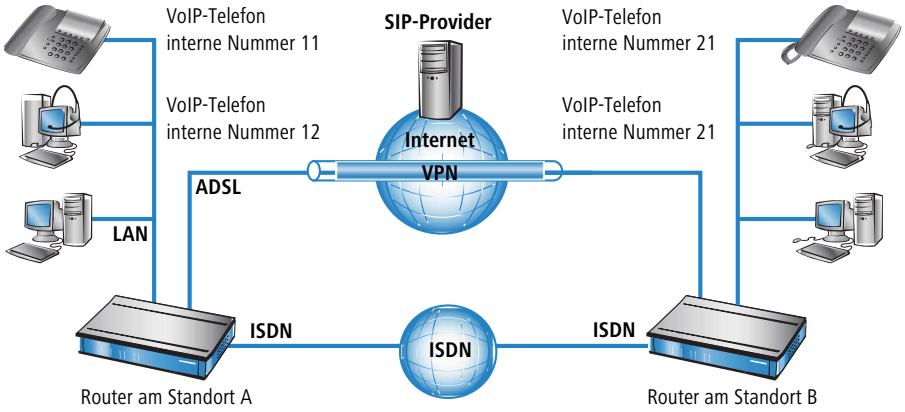
16.16.3.6 Ablauf des Call-Routings bei abgehenden Rufen

	Benutzer	wählt	passende Call-Route	passender Benutzer	Mapping, verwendete Nummer	Ziel-Leitung
1	VoIP-Telefon Filiale	`212`	keine	VoIP-Softphone	`212`	intern
2	VoIP-Telefon Filiale	`199`	**4** `#`	SIP-Teilnehmer in der Zentrale	`#: 199`	SIP-PBX
3	VoIP-Telefon Filiale	`0 555 555`	**3** `0#`		`0241#: 0241 555 555`	ISDN
4	VoIP-Telefon Filiale	`0 0123 666 666`	**2** `00#`		`00#: 0123 666 666`	SIP-PBX

1. Interner Anruf zwischen zwei VoIP-Endgeräten in der Filiale. Die gewählte Nummer `212` passt auf keine Route der Call-Routing-Tabelle. Der Call-Router sucht daher in der Liste der lokalen Benutzer, findet dort den passenden Eintrag und kann den Ruf intern zustellen.
2. Interner Anruf zwischen einem VoIP-Endgerät in der Filiale und dem internen Teilnehmer `199` in der Zentrale. Die gewählte Nummer `199` passt im ersten Durchlauf auf keine Route der Call-Routing-Tabelle, auch in der Liste der lokalen Benutzer wird kein passender Eintrag gefunden. Im zweiten Durchlauf durch die Call-Routing-Tabelle werden auch die Standard-Routen eingesetzt. Die Route mit der gerufenen Nummer `#` (**4**) trifft auf alle Rufe zu, die vorher nicht zugeordnet werden konnten. Der Ruf zu `199` wird daher über die SIP-PBX-Leitung ausgeführt.
3. Externer Anruf aus der Filiale ins eigene Ortsnetz. Die gewählte Nummer `0 555 555` passt auf die Route `0#` (**3**) der Call-Routing-Tabelle. Der Call-Router entfernt die vorangestellte `0` für die Amtsholung, ergänzt die Vorwahl des eigenen Ortsnetzes und führt den Anruf zu `0241 555 555` über die ISDN-Leitung aus.
4. Externer Anruf aus der Filiale in ein nationales Ortsnetz. Die gewählte Nummer `0 0123 555 555` passt auf die Route `00#` (**2**) der Call-Routing-Tabelle. Der Call-Router gibt den Anruf **unverändert** auf der SIP-PBX-Leitung aus. Erst die SIP-TK-Anlage entfernt die vorangestellte `0` für die Amtsholung und führt den Anruf zu `0123 555 555` über den ISDN-Amtsanschluss aus.

16.16.4 VoIP-Kopplung von Standorten ohne SIP-TK-Anlage

Auch verteilte Unternehmen ohne eigene SIP-TK-Anlage können die Vorteile der VoIP-Standortverbindung nutzen. In diesem "Peer-to-Peer"-Szenario werden an beiden Standorten LANCOM VoIP Router eingesetzt.



16.16.4.1 Ziel

- Internes Telefonieren über beide Standorte hinweg.
- Externes Telefonieren über den SIP-Provider mit Backup über ISDN.
- Gespräche zu Not- und Sonderrufnummern über ISDN.

16.16.4.2 Voraussetzungen

- LANCOM angeschlossen an LAN und WAN, eine ISDN-TE-Schnittstelle ist mit dem ISDN-NTBA verbunden.
- Der Internetzugang ist eingerichtet, ebenso die Netzkopplung der beiden Standorte über einen VPN-Tunnel. Alle angeschlossenen Endgeräte können sich über die verwendeten IP-Adressen erreichen.
- Ein Rufnummernplan mit einer eindeutigen internen Rufnummer für jedes anzuschließende Endgerät. Für jeden Standort wird dabei ein separater Rufnummernkreis verwendet, in diesem Beispiel beginnen die internen Rufnummern am Standort A mit einer `1`, am Standort B mit einer `2`.
- Jeder Standort verfügt über einen Account bei einem SIP-Provider.

16.16.4.3 Konfiguration des Gerätes

Die folgende Tabelle zeigt im Überblick, welche Informationen für die Konfiguration benötigt werden und wo sie eingetragen werden. Im Prinzip wird lediglich an jedem Standort eine SIP-TK-Leitung „über Kreuz" mit dem entfernten Standort eingerichtet

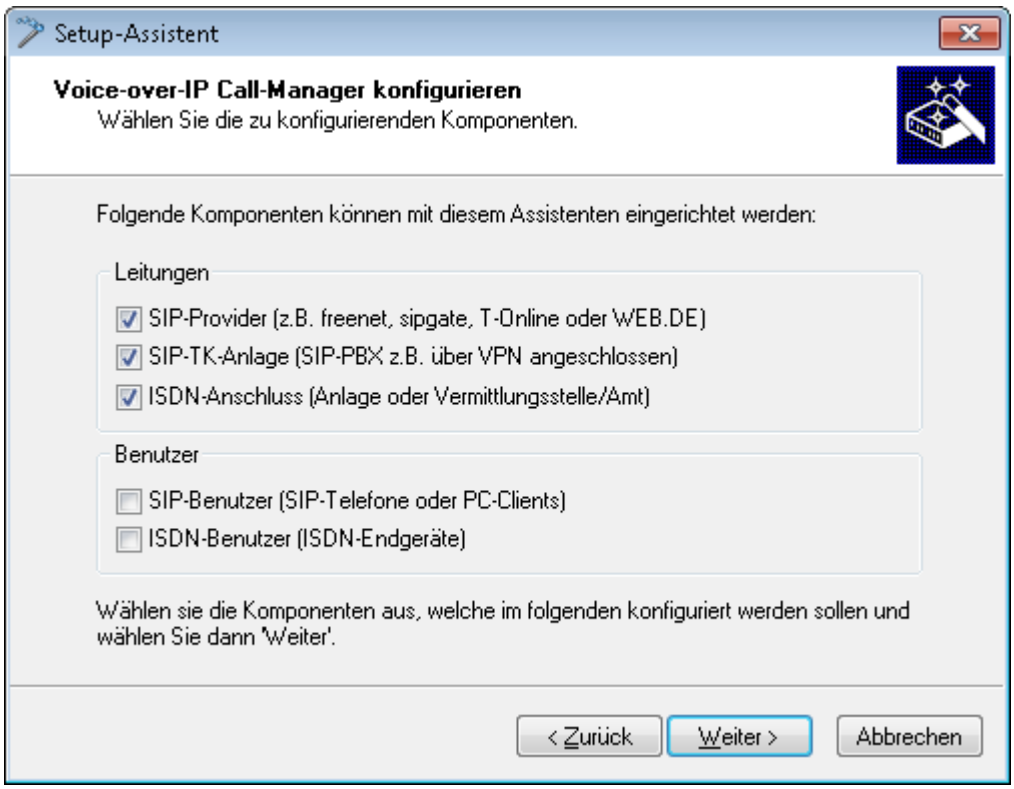
	LANCOM Standort A	SIP-Endgeräte Standort A	LANCOM Standort B	SIP-Endgeräte Standort B
interne VoIP-Domain	`location_A.intern`	`location_A.intern`	`location_B.intern`	`location_B.intern`
interne Rufnummern		`10` bis `19`		`20` bis `29`
externe SIP-Rufnummer	✔		✔	
Zugangsdaten SIP-Account	✔		✔	
externe ISDN-Rufnummern (MSNs)	✔		✔	
Landes- und Ortsnetzvorwahl	✔		✔	

	LANCOM Standort A SIP-Endgeräte Standort A	LANCOM Standort B SIP-Endgeräte Standort B
SIP-PBX-Leitung	`LOCATION_B`	`LOCATION_A`
SIP-PBX-Domäne	`location_B.intern`	`location_A.intern`
Call-Route	**1.** Gerufene Nummer `2#` **2.** Ziel-Leitung `LOCATION_B` **3.** Ziel-Nummer `2#`	**1.** Gerufene Nummer `1#` **2.** Ziel-Leitung `LOCATION_A` **3.** Ziel-Nummer `1#`

Auch wenn in der hier vorgestellten Konfiguration von SIP-TK-Leitungen die Rede ist, können Sie diese Funktion ganz ohne TK-Anlagen nutzen.

So konfigurieren Sie das LANCOM im Detail:

1. Führen Sie unter LANconfig den Setup-Assistenten zur Konfiguration des Voice-Call-Managers aus. Aktivieren Sie die Optionen **SIP-Provider**, **SIP-TK-Anlage** und **ISDN-Anschluss**.



2. Richten Sie ein wie in den vorhergehenden Beispielen beschrieben:
   - eine Leitung zu einem SIP-Provider
   - ISDN-Leitung mit MSN-Mapping
   - Orts- und Landesvorwahl für jeweiligen Standort
3. Geben Sie als lokale VoIP-Domäne eine eindeutige Domäne an, mit der Sie den lokalen VoIP-Bereich des Standortes beschreiben. Beide Standorte verwenden **unterschiedliche** VoIP-Domains, z. B. `location_A.intern` bzw. `location_B.intern`.
4. Richten Sie die Leitung zur SIP-TK-Anlage ein mit den folgenden Werten:

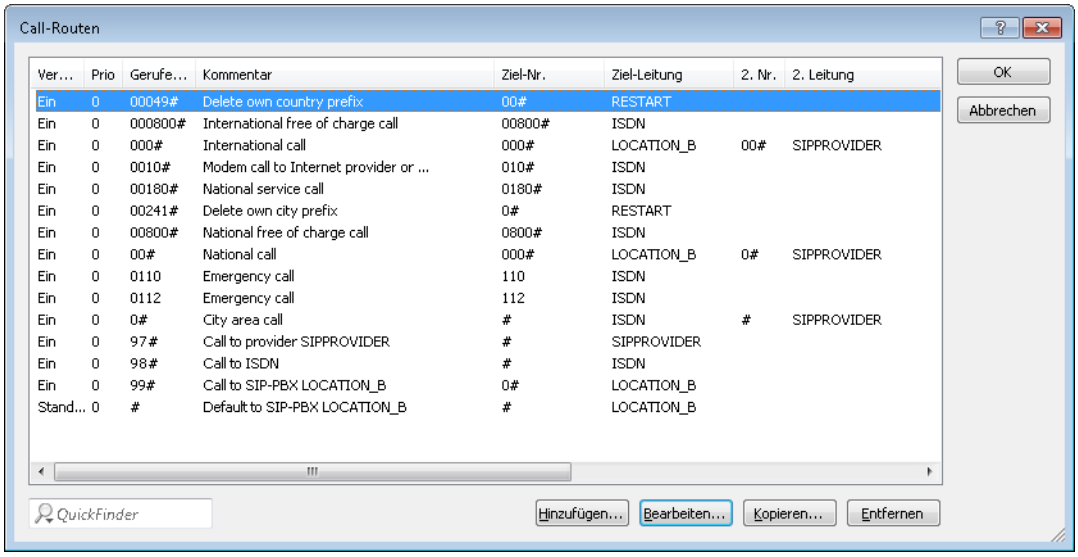
- SIP-PBX-Leitungs-Name: eindeutiger Name für die Leitung zum entfernten Standort.
- PBX SIP-Domäne/Realm: interne VoIP-Domäne des entfernten Standortes.
- Registrar (FQDN oder IP): Adresse des LANCOM am entfernten Standort, falls das Gerät nicht über DNS-Auflösung der VoIP-Domäne (PBX SIP-Domäne/Realm) identifiziert werden kann.

  Verwenden Sie hier die private, über VPN erreichbare IP-Adresse des LANCOM, nicht die öffentliche IP.

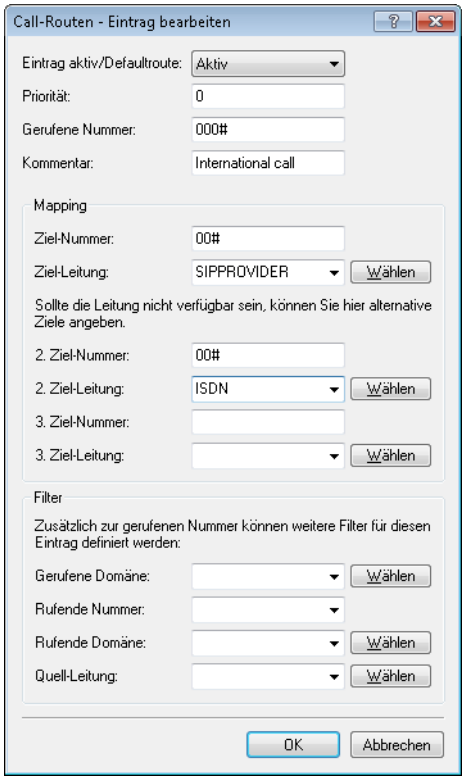
- Lassen Sie das Feld für das gemeinsame Passwort bei der Anmeldung an der SIP-PBX frei.
- Lassen Sie das Feld für die öffentliche PBX-Nummer frei.

5. Die vom Setup-Assistenten vorgeschlagene Call-Routing-Tabelle sieht die Ausführung von internationalen und nationalen Ferngesprächen über die Leitung des entfernten Standortes vor, Ortsgespräche werden über ISDN geleitet.

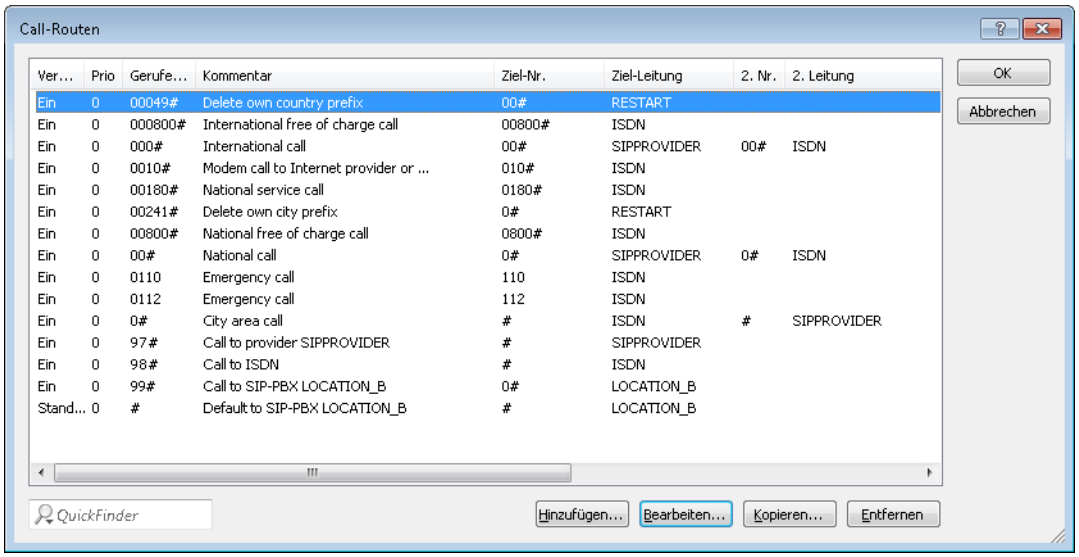
   Eine **Standard-Route** wird zudem genutzt, um alle nicht auflösbaren Rufnummern über die Leitung des entfernten Standortes auszuführen.



6. Passen Sie die vorgeschlagene Call-Routing-Tabelle an, um internationale und nationale Ferngespräche über die Leitung des SIP-Providers mit Backup über ISDN auszuführen. Beachten Sie dabei, dass die führende `0` aus der Rufnummer entfernt werden muss.



Nach der Anpassung für internationale und nationale Ferngespräche sieht die Call-Routing-Tabelle dann z. B. so aus:



7. In diesem Zustand werden alle von der Call-Routing-Tabelle nicht auflösbaren Rufe, für die es auch keinen passenden Eintrag in der Liste der lokalen Benutzer gibt, automatisch an den entfernten Standort weitergeleitet.

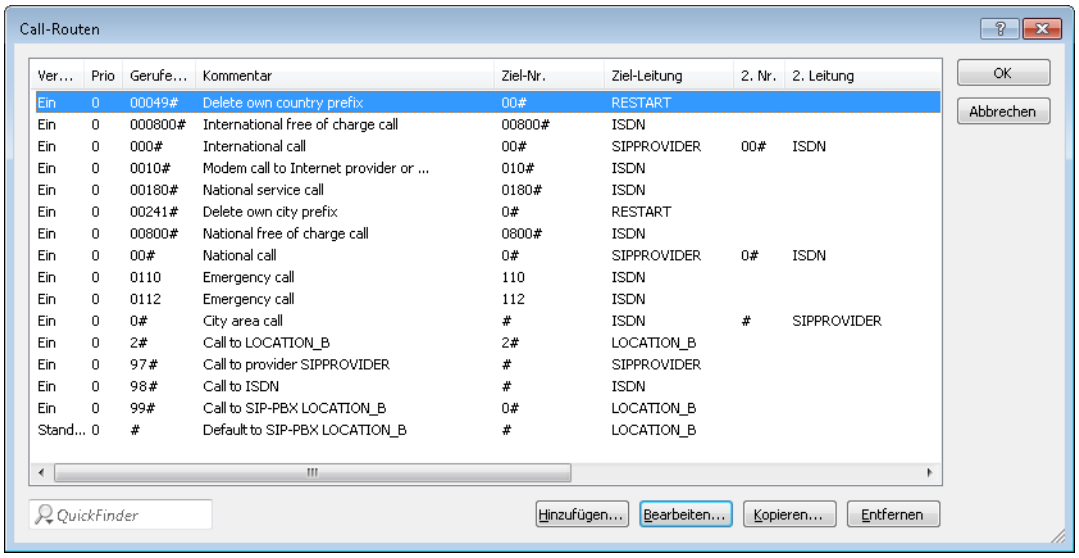
   Falls das nicht gewünscht ist, weil z. B. mehr als zwei Standorte auf diese Weise verbunden werden, kann ein zusätzlicher Eintrag nur die internen Rufe zu einem bestimmten Standort erfassen. Legen Sie dazu (für den

Rufnummernkreis `20` bis `29` am Standort B) einen neuen Eintrag in der Call-Routing-Tabelle mit folgenden Werten an:

- Gerufene Nummer / Name: z. B. `2#` für alle Nummern, die mit einer 2 beginnen.
- Nummer / Name: Die gerufene Nummer wird unverändert als Ziel-Nummer verwendet, also hier z. B. ebenfalls `2#`.
- Leitung: Tragen Sie hier die SIP-PBX-Leitung des entfernten Standortes ein, also z. B. `LOCATION_B`.

Die Standard-Route wird dabei z. B. so angepasst, dass alle nicht auflösbaren Rufe über ISDN ausgegeben werden.

Nach der Anpassung sieht die Call-Routing-Tabelle dann z. B. so aus:



Ver...	Prio	Gerufe...	Kommentar	Ziel-Nr.	Ziel-Leitung	2. Nr.	2. Leitung
Ein	0	00049#	Delete own country prefix	00#	RESTART		
Ein	0	000800#	International free of charge call	00800#	ISDN		
Ein	0	000#	International call	00#	SIPPROVIDER	00#	ISDN
Ein	0	0010#	Modem call to Internet provider or ...	010#	ISDN		
Ein	0	00180#	National service call	0180#	ISDN		
Ein	0	00241#	Delete own city prefix	0#	RESTART		
Ein	0	00800#	National free of charge call	0800#	ISDN		
Ein	0	00#	National call	0#	SIPPROVIDER	0#	ISDN
Ein	0	0110	Emergency call	110	ISDN		
Ein	0	0112	Emergency call	112	ISDN		
Ein	0	0#	City area call	#	ISDN	#	SIPPROVIDER
Ein	0	2#	Call to LOCATION_B	2#	LOCATION_B		
Ein	0	97#	Call to provider SIPPROVIDER	#	SIPPROVIDER		
Ein	0	98#	Call to ISDN	#	ISDN		
Ein	0	99#	Call to SIP-PBX LOCATION_B	0#	LOCATION_B		
Stand...	0	#	Default to SIP-PBX LOCATION_B	#	LOCATION_B		

Dieser Eintrag für `LOCATION_B` wird in der Call-Routing-Tabelle automatisch sehr weit nach unten geschoben, um die allgemeineren Regeln nicht zu beeinflussen. Prüfen Sie dennoch, ob im Zusammenwirken mit den anderen Routen wirklich nur die internen Rufnummern des entfernten Standortes über die entsprechende Leitung ausgeführt werden.

16.16.4.4 Konfiguration der VoIP-Endgeräte

Die Konfiguration der VoIP-Endgeräte verläuft so wie in den vorhergehenden Beispielen beschrieben mit der internen VoIP-Domäne und internen Rufnummern des eigenen Standortes.

16.16.4.5 Ablauf des Call-Routings bei abgehenden Rufen

Die meisten Anrufe bei dieser Anwendung laufen ab wie in den vorhergehenden Beispielen beschieben. Die internen Anrufe zwischen den Standorten werden wie folgt aufgelöst:

	Benutzer	wählt	passende Call-Route	passender Benutzer	Mapping, verwendete Nummer	Ziel-Leitung
1	VoIP-Telefon Standort A	`21`	`2#`	keiner	`21`	`LOCATION_B`

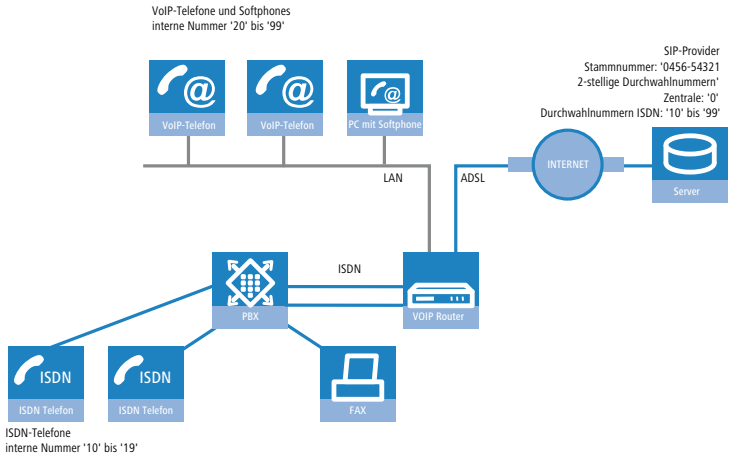
1. Interner Anruf zwischen zwei VoIP-Endgeräten an Standort A und B. Die gewählte Nummer `21` passt auf die Route **5** `2#` der Call-Routing-Tabelle. Der Call-Router führt den Anruf mit der unveränderten Rufnummer über die Leitung zur entfernten SIP-PBX aus.

16.16.5 SIP-Trunking

Unter dem Begriff "Trunking" werden in der Telekommunikation Verfahren bezeichnet, bei denen mehrere Leitungen oder Verbindungen zu einer gemeinsamen Leitung zusammengefasst werden. In der VoIP-Welt offerieren die SIP-Provider vermehrt Angebote, bei denen über einen einzelnen Account mehrere Gespräche gleichzeitig geführt werden können. Verbunden mit der Möglichkeit, die SIP-Teilnehmer über eine gemeinsame Stammnummer mit individuellen Durchwahlen (DDI) zu erreichen, werden solche Accounts auch für Geschäftskunden attraktiv.

Bei Nutzung eines SIP-Accounts mit Trunking gibt es zwei Möglichkeiten:

- Der Kunde behält seinen bisherigen ISDN-Anschluss mit den entsprechenden Rufnummern bei der Telefongesellschaft und bucht bei einem SIP-Provider einen zusätzlichen Account mit einem separaten Rufnummernkreis.
- Der Kunde überträgt (portiert) seine bisher verwendeten Rufnummern von der Telefongesellschaft zum SIP-Provider und nutzt die gleichen Nummern nun über SIP.



In diesem Anwendungsbeispiel betrachten wir ein Unternehmen, das einen SIP-Trunking-Account mit bis zu 10 Durchwahlnummern einrichten möchte.. Die bisher verwendeten ISDN-Endgeräte mit den Durchwahlen des Anlagenanschlusses können beibehalten werden, alle neuen Mitarbeiter bekommen ein SIP-Telefon mit einer Durchwahl über den SIP-Account.

Intern sollen alle Mitarbeiter untereinander telefonieren können, daher werden eindeutige Durchwahlen verwendet. Um eine sanfte Migration in Richtung SIP vorzubereiten, sollen alle ISDN-Endgeräte mit ihrer Durchwahl **parallel** über die Stammnummer des SIP-Accounts erreichbar sein. Ein ISDN-Telefon soll also auf die Rufe an `0456-54321 12` reagieren.

Abgehende Anrufe sollen über den SIP-Account geführt werden.

16.16.5.1 Zielsetzung für den Einsatz des LANCOM VoIP Router

- Anschluss von zusätzlichen SIP-Endgeräten.
- Internes Telefonieren zwischen ISDN- und SIP-Endgeräten.
- Günstiges Telefonieren über einen gemeinsam genutzten SIP-Account.

16.16.5.2 Voraussetzungen

- LANCOM Gerät angeschlossen an LAN und WAN (über DSL/ADSL), ISDN-NT-Schnittstelle(n) sind mit einer ISDN-TK-Anlage verbunden.
- Der Internetzugang ist eingerichtet. Alle angeschlossenen Endgeräte können sich über die verwendeten IP-Adressen erreichen.
- Ein Rufnummernplan mit einer eindeutigen internen Rufnummer für jedes anzuschließende Endgerät.

16.16.5.3 Konfiguration des Gerätes

So konfigurieren Sie das LANCOM für den Betrieb am Anlagenanschluss:

1. Bei der Konfiguration der SIP-Clients wird lediglich die interne VoIP-Domäne des LANCOM VoIP Router und die jeweilige interne Rufnummer eingetragen. Dabei bleiben die bisher für die ISDN-Endgeräte verwendeten Durchwahlen frei.
2. Für den SIP-Account wird eine SIP-Provider-Leitung angelegt. Dabei wird als Betriebsmodus für diese Leitung die Option 'Trunk' ausgewählt.
3. Das Routing der Rufe wird über die Call-Routing-Tabelle geregelt. Bei der Verwendung der Assistenten von LANconfig wird die Call-Routing-Tabelle so vordefiniert, dass alle abgehenden Rufe von ISDN- und SIP-Geräten über den SIP-Trunk-Account geleitet werden.

16.16.5.4 Ablauf des Call-Routing

Das Call-Routing profitiert in diesem Beispiel von den eindeutigen internen Rufnummern.

› Bei ankommenden Rufen wird nur die DDI an den LANCOM VoIP Router übergeben. Da DDI und interne Rufnummern in diesem Beispiel deckungsgleich verwendet werden, können Rufe an eine Durchwahl an die lokal registrierten SIP-Benutzer oder die dynamischen ISDN-Benutzer zugestellt werden.

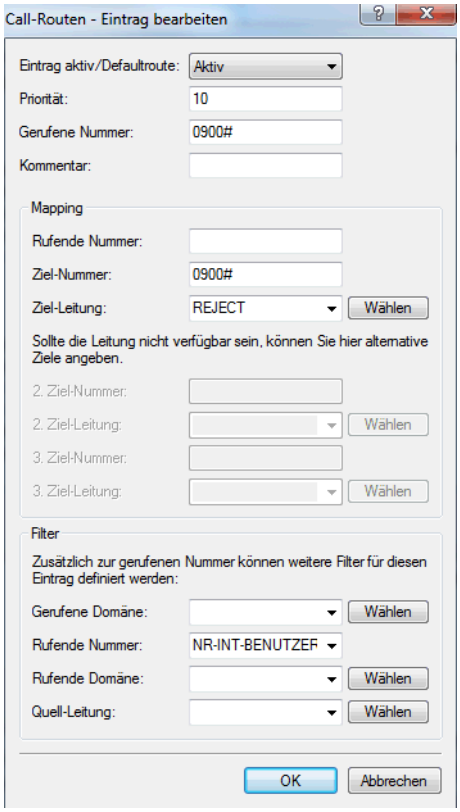
Wenn die gemeldeten DDI nicht direkt als interne Rufnummern verwendet werden können oder sollen, werden in der ISDN- bzw. SIP-Mapping-Tabelle entsprechende Rufnummernumsetzungen definiert.

› In der Standard-Einstellung nach Verwendung der Assistenten gilt SIP als normale Ziel-Leitung (bis auf Ortsgespräche und Sonderrufnummern). Durch das Umstellen eines Eintrags in der Call-Routing-Tabelle können z. B. auch die Ortsgespräche auf SIP umgestellt werden.

Bei den Gesprächsteilnehmern auf der anderen Seite der Verbindung wird in diesem Fall die SIP-Rufnummer angezeigt, auch wenn der Anruf von einem ISDN-Endgerät kommt.

16.16.6 Sperren von abgehenden Rufen zu Sonderrufnummern

Sie haben die Möglichkeit, bestimmte Rufnummern (z. B. kostenpflichtige Hotlines wie 0900) mit folgender Call-Route zu unterbinden:

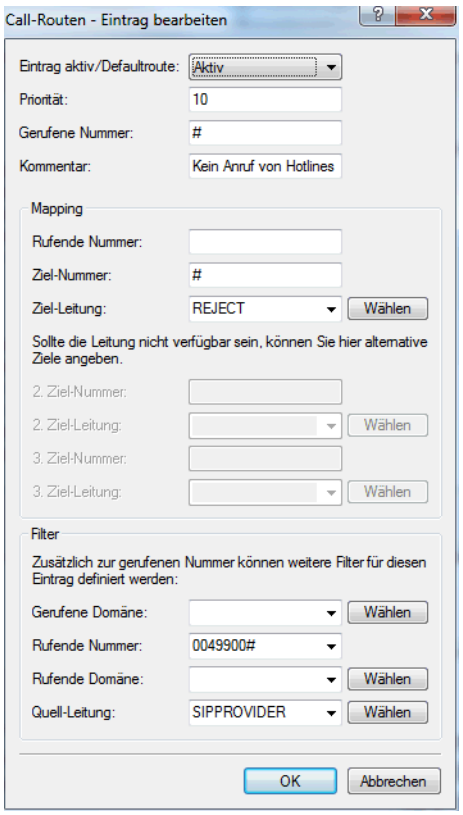


Geben Sie bei der rufenden Nummer einen registrierten Client an, um die Regel nur auf Rufe zu beschränken, die von den jeweiligen Benutzer geführt werden.

Wählen Sie als Quell-Leitung "User.#", "User.ISDN", "User.SIP" oder "User.Analog" aus, haben Sie die Möglichkeit, die Regel auf entsprechende Teilnehmer unabhängig von deren Rufnummer einzuschränken.

16.16.7 Verwerfen von eingehenden Rufen

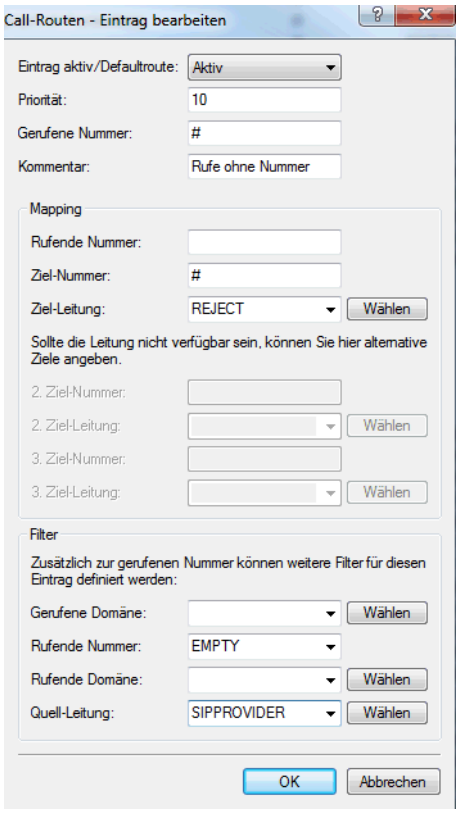
Die Signalisierung ankommender Rufe von z. B. kostenpflichtigen Hotlines (0900) lässt sich durch die folgende Call-Route unterbinden:



Wählen Sie als Quell-Leitung z. B. eine registrierte SIP-Leitung aus, um die Regel nur auf Rufe einzuschränken, die über diese Leitung signalisiert werden.

16.16.8 Rufe ohne übermittelte Rufnummer verwerfen

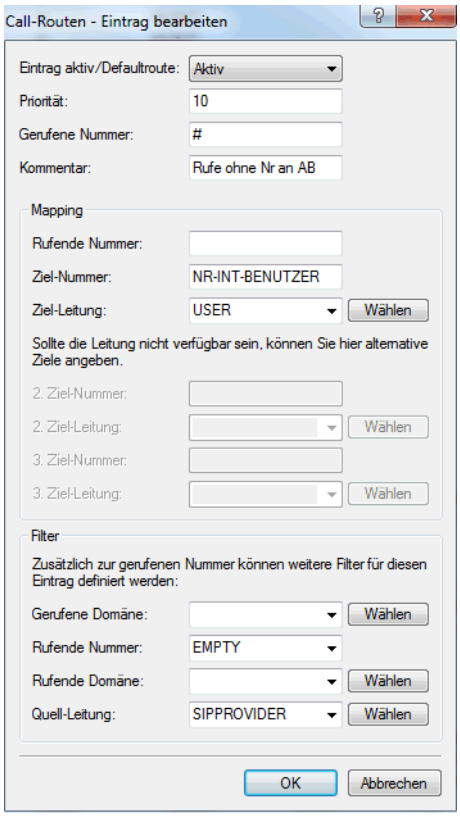
Richten Sie folgende Call-Route ein, um eingehende Anrufe zu verwerfen, die keine Rufnummer übermitteln:



Wählen Sie als Quell-Leitung z. B. eine registrierte SIP-Leitung aus, um die Regel nur auf Rufe einzuschränken, die über diese Leitung signalisiert werden.

16.16.9 Rufe ohne übermittelte Rufnummer umleiten

Richten Sie folgende Call-Route ein, um eingehende Anrufe ohne Rufnummer z. B. an einen Anrufbeantworter umzuleiten:



Wählen Sie als Quell-Leitung z. B. eine registrierte SIP-Leitung aus, um die Regel nur auf Rufe einzuschränken, die über diese Leitung signalisiert werden.

16.17 Diagnose der VoIP-Verbindungen

16.17.1 SIP Traces

Zur Kontrolle der internen Abläufe in den LANCOM Geräten während oder nach der Konfiguration bieten sich Trace-Ausgaben an. Mit einem SIP-Trace werden alle SIP-Informationen angezeigt, die zwischen einem LANCOM VoIP Router und einem SIP-Provider bzw. einer übergeordneten SIP-TK-Anlage ausgetauscht werden. Der SIP-Trace wird mit folgendem Befehl eingeschaltet:

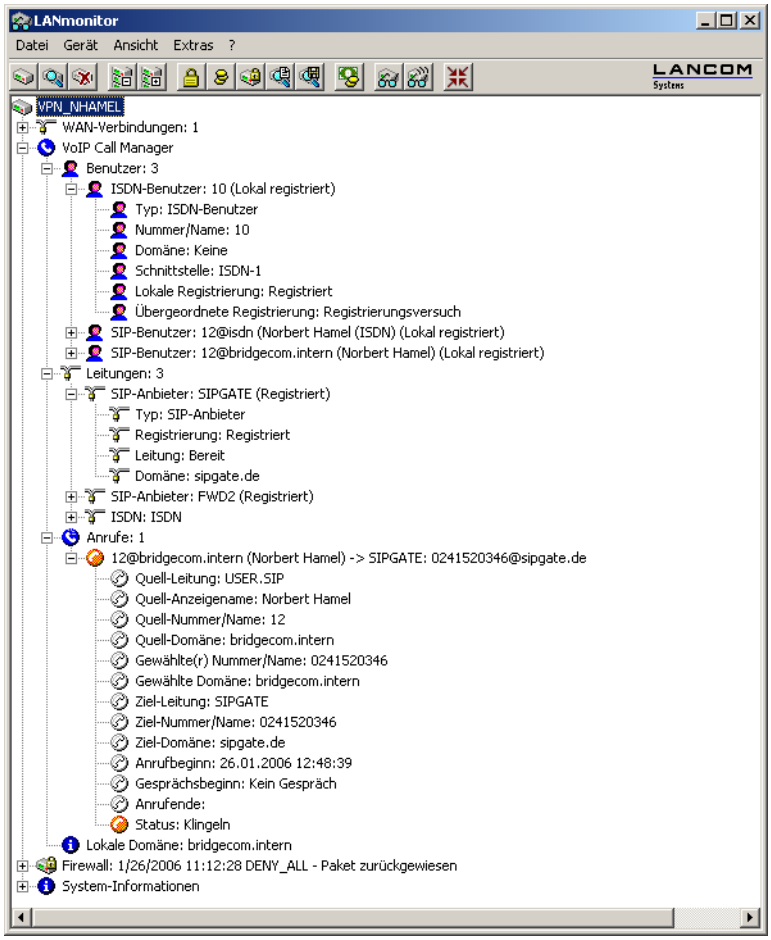
```
trace + sip-packet
```

16.17.2 Diagnose der Verbindungen mit dem LANmonitor

Der LANmonitor zeigt zahlreiche Informationen rund um die Vermittlung von Gesprächen im LANCOM an:

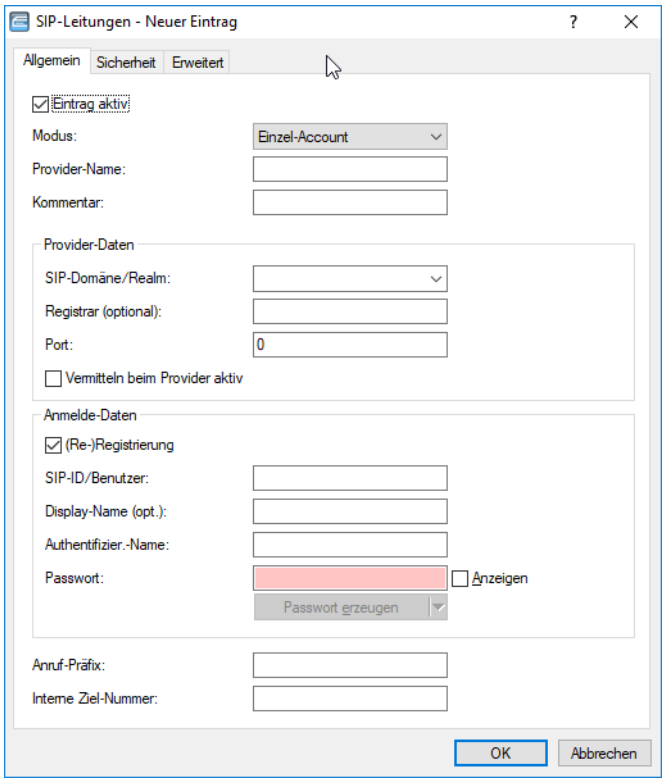
- Informationen über die registrierten Benutzer.
- Informationen über die verfügbaren Leitungen.
- Informationen über die aktuellen Anrufe, dabei wird u. a. die Umsetzung der Rufnummern und Domains durch den Call-Manager deutlich.

› Informationen über die festen und automatischen QoS-Bandbreitenreservierungen bzw. -Einstellungen.



16.18 VoSIP-Unterstützung im Voice Call Manager

LCOS unterstützt Voice over Secure IP (VoSIP). Mit dieser Funktion ist es Ihnen möglich, Signalisierungs- und Sprachdaten zu verschlüsseln. Sie können VoSIP ab LCOS-Version 9.20 auf allen LANCOM Business VoIP-Routern einsetzen.



Signalisierungs-Verschlüsselung

Diese Einstellung legt das Protokoll zur Signalisierungs-Verschlüsselung (SIP/SIPS) bei der Kommunikation mit dem Provider fest.

Automatisch

Zur DNS-Auflösung werden NAPTR (Naming Adress Pointer)-Records verwendet. Der Provider gibt in den DNS-Daten die Verwendung des Transportprotokolls wie UDP, TCP oder TLS vor. Ebenso können Gewichte bzw. Prioritäten durch den Provider vorgegeben werden.

Wenn TLS als Transportprotokoll zur Signalisierungsverschlüsselung durch NAPTR vorgegeben wird, wird automatisch auch Sprachverschlüsselung verwendet, unabhängig von der expliziten Konfigurationseinstellung der Sprachverschlüsselung.

Keine (UDP)

Alle SIP Pakete werden verbindungslos übertragen. Die meisten Anbieter unterstützen diese Einstellung.

Keine (TCP)

Alle SIP Pakete werden verbindungsorientiert übertragen. Das Gerät baut eine TCP Verbindung zum Provider auf und erhält diese für die Dauer der Registrierung aufrecht. Spezielle Anbieter, wie z. B. Anbieter von Trunk Anschlüssen, unterstützen oder erzwingen diese Einstellung.

TLS

Gleiche Übertragungsweise wie bei TCP, allerdings werden alle SIP Pakete zusätzlich durch eine Verschlüsselung bis zum Provider geheim gehalten. Die jeweils in der Konfiguration ausgewählte TLS-Version wird als minimale Anforderung für die TLS-Verschlüsselung verwendet.

Sprach-Verschlüsselung

Diese Einstellung legt fest, ob und wie Sprachdaten (RTP/SRTP) bei der Kommunikation mit dem Provider verschlüsselt werden.

Sprach-Verschlüsselung	
Ablehnen	Eine Verschlüsselung wird bei ausgehenden Gesprächen nicht angeboten. Eingehende Gespräche mit einem Verschlüsselungsvorschlag werden abgelehnt. Der Sprachkanal ist nicht verschlüsselt.
Ignorieren	Eine Verschlüsselung wird bei ausgehenden Gesprächen nicht angeboten. Eingehende Gespräche mit einem Verschlüsselungsvorschlag werden akzeptiert. Der Sprachkanal ist nicht verschlüsselt.
Bevorzugt	Eine Verschlüsselung wird bei ausgehenden Gesprächen angeboten. Eingehende Gespräche ohne einen Verschlüsselungsvorschlag werden akzeptiert. Der Sprachkanal ist nur dann verschlüsselt, wenn auch die Gegenstelle eine Verschlüsselung unterstützt.
Erzwingen	Eine Verschlüsselung wird bei ausgehenden Gesprächen angeboten. Eingehende Gespräche ohne Verschlüsselungsvorschlag werden abgelehnt. Der Sprachkanal ist entweder verschlüsselt oder wird nicht aufgebaut.

Sollen Sprachdaten verschlüsselt übertragen werden, ist es erforderlich, dass auch die Signalisierung über einen verschlüsselten Kanal erfolgt. Beachten Sie aber bitte, dass die Nutzung von SRTP keine Ende-zu-Ende Verschlüsselung garantiert.

16.19 Auto-Provisionierung LANCOM DECT 510 IP

LCOS ermöglicht die automatische Einrichtung und Konfiguration der Basisstation mit bis zu 6 DECT-Mobilteilen. Angeschlossen an einen LANCOM Router lassen sich die Mobilteile des LANCOM DECT 510 IP einfach zu registrieren und Rufnummern individuell zuweisen.

Die LANCOM DECT 510 IP Basisstation ist über WEBconfig konfigurierbar. Dies ist jedoch nicht zwingend erforderlich. Sofern die Provisionierung aktiviert ist, konfiguriert Ihr Router die Basisstation automatisch. Um die Provisionierung auf Ihrem Router zu aktivieren, wählen Sie in LANconfig unter **Management** > **Allgemein** > **Erweitert** > **Provisioning-Server aktivieren** den Wert **ja**. An der Konsole setzen Sie den dazugehörigen Parameter unter **Setup** > **Provisioning-Server** > **Aktiv** (SNMP-ID 2.103.1).

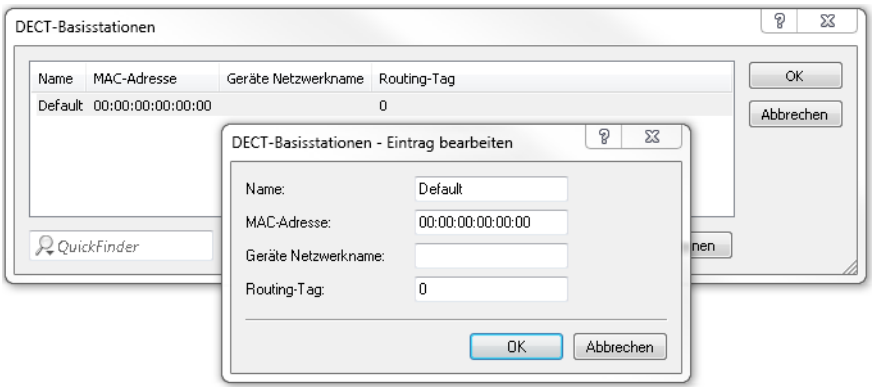
Für die automatische Konfiguration des LANCOM DECT 510 IP müssen die Basisstation mit dem Router verbunden und die Mobilteile an der Basisstation angemeldet sein.

Sie haben zudem die Möglichkeit, die Basisstation durch den All-IP-Wizard zu konfigurieren. Folgen Sie hierzu den Schritten des Setup-Assistenten.

16.19.1 DECT-Basisstation und -Mobilteile mit LANconfig konfigurieren

Konfigurieren Sie in LANconfig die DECT-Basisstation unter **Voice Call Manager** > **Benutzer** > **DECT-Basisstationen**, indem Sie der Tabelle einen neuen Eintrag hinzufügen.

Wenn bei der Autoprovisionierung jede LANCOM DECT 510 IP verwendet werden darf oder gleich konfiguriert werden soll, benötigen Sie in dieser Tabelle keine weiteren Einträge. Die Funktion ist durch den Default Eintrag gegeben.



Name

Geben Sie hier einen eindeutigen Namen für die Basisstation an.

MAC-Adresse

Tragen Sie hier die MAC-Adresse der verfügbaren Basisstation ein.

Wenn Sie eine Kommunikation mit einer beliebige MAC-Adresse erlauben möchten, tragen Sie hier `00:00:00:00:00:00` (Default) ein.

Netzwerk-Name

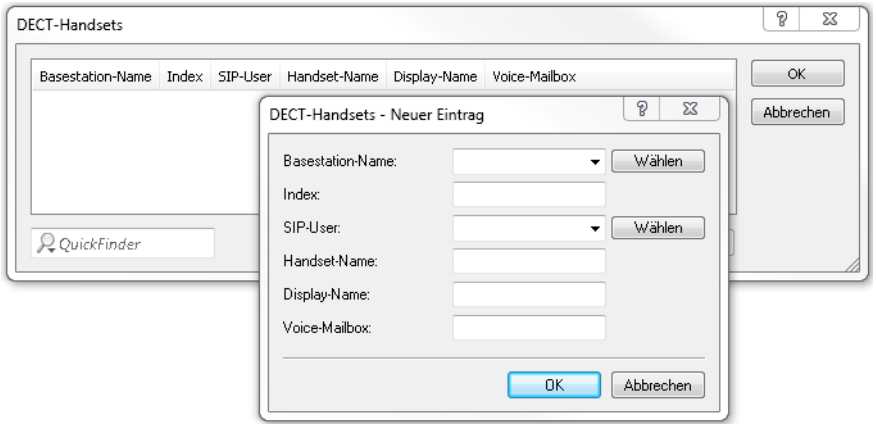
Geben Sie hier optional einen Netzwerknamen an, mit dem die Basisstation im Netzwerk angezeigt wird.

Routing-Tag

Mit dem Schnittstellen-Tag können Sie die Autoprovisionierung der LANCOM DECT Basisstation auf ein bestimmtes Netzwerk begrenzen. Dies ist vor allem dann sinnvoll, wenn Sie in Ihrem Netzwerk bestimmte IP-Bereiche öffentlich zugänglich gemacht haben (z. B. Public Spot oder DMZ). Die Einschränkung verhindert, dass die SIP-Zugangsdaten der DECT Basisstation ungewollt an fremde Geräte übermittelt werden.

Wenn Sie diesen Service für alle Netzwerke nutzen möchten, tragen Sie hier bitte das Routing-Tag "0" ein.

Konfigurieren Sie in LANconfig die DECT-Mobilteile unter **Voice Call Manager** > **Benutzer** > **DECT-Handsets**, indem Sie der Tabelle einen neuen Eintrag hinzufügen.



Basisstation-Name

Wählen Sie hier die Basisstation aus, an der das entsprechende Mobilteil angemeldet ist.

Index

Tragen Sie hier die Nummer des jeweiligen Mobilteils ein (z. B. "0" für Mobilteil 1, "1" für Mobilteil 2 usw).

SIP-User

Wählen Sie hier die Rufnummer des Mobilteils aus.

Handset-Name

Legen Sie hier den Namen fest, der im Display des Mobilteils angezeigt werden soll.

Display-Name

Legen Sie hier den Namen fest, der einem Anrufer übermittelt werden soll.

Voice-Mailbox

Geben Sie hier die Rufnummer Ihres Netzanrufbeantworters an. Durch längeres Drücken der Taste "1" auf dem Mobilteil wird diese Rufnummer angewählt.

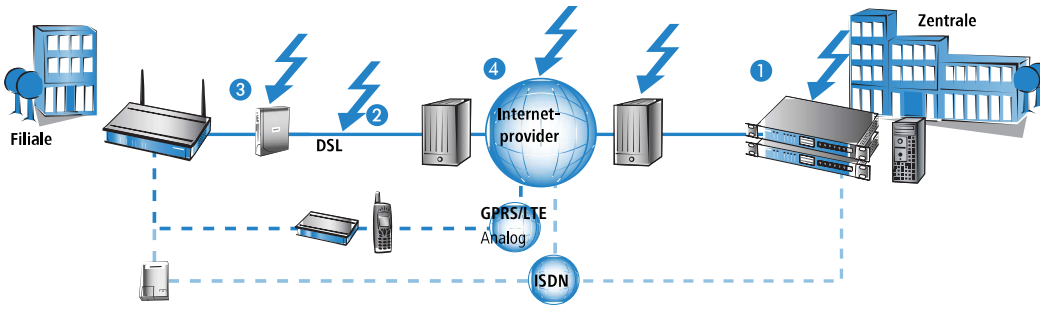
17 Backup-Lösungen

17.1 Hochverfügbarkeit von Netzwerken

Die vernetzte Zusammenarbeit über mehrere Standorte oder sogar über Kontinente hinweg ist aus dem modernen Wirtschaftsleben nicht mehr wegzudenken. Die Kommunikationswege zwischen Zentralen, Filialen oder Außendienstmitarbeitern setzen dabei fast immer auf öffentliche Infrastrukturen auf. VPN hat sich als defacto-Standard für die kostengünstige und sichere Unternehmenskommunikation über das Internet etabliert.

Allerdings können bei diesen Netzwerkstrukturen eine Reihe von notwendigen Elementen von Störungen betroffen sein, die empfindliche Auswirkungen auf den Geschäftsbetrieb haben:

- Das entfernte Internet-Gateway **1** kann ausfallen.
- Die physikalischen Leitungen, über die Verbindungen ins Internet oder zu einem entfernten Netzwerk aufgebaut werden, können betroffen sein:
  - Die Internetzugangsleitung zwischen dem Standort und dem Provider **2** kann ausfallen, z. B. durch Beschädigung des Kabels bei Bauarbeiten.
  - Der DSL-Anschluss an einem Standort **3** kann ausfallen, während die ISDN / LTE-Leitungen noch ihren Dienst versehen.
- Das Netzwerk des Providers **4** kann gestört sein oder ausfallen.



Geräte von LANCOM bieten eine Reihe von Sicherheits- und Backup-Funktionen, mit denen Sie Ihr Netz vor den Folgen dieser Störungen schützen können.

17.1.1 Wie wird die Störung einer Netzwerkverbindung erkannt?

Um eine Netzwerkverbindung vor den Folgen einer Störung schützen zu können, muss zunächst einmal die Störung selbst als solche erkannt werden. Folgende Verfahren bieten sich an, um die Verbindungen zu überprüfen:

- Überprüfen der PPP-Verbindung bis zum Provider mittels PPP LCP Echo Monitoring.
- Überprüfen der Erreichbarkeit beliebiger Gegenstellen über Name oder IP-Adresse mit ICMP Polling (Ping von Ende zu Ende).
- Überprüfen von Tunnelendpunkten mit „Dead-Peer-Detection" (DPD).

17.1.1.1 PPP LCP Echo Monitoring

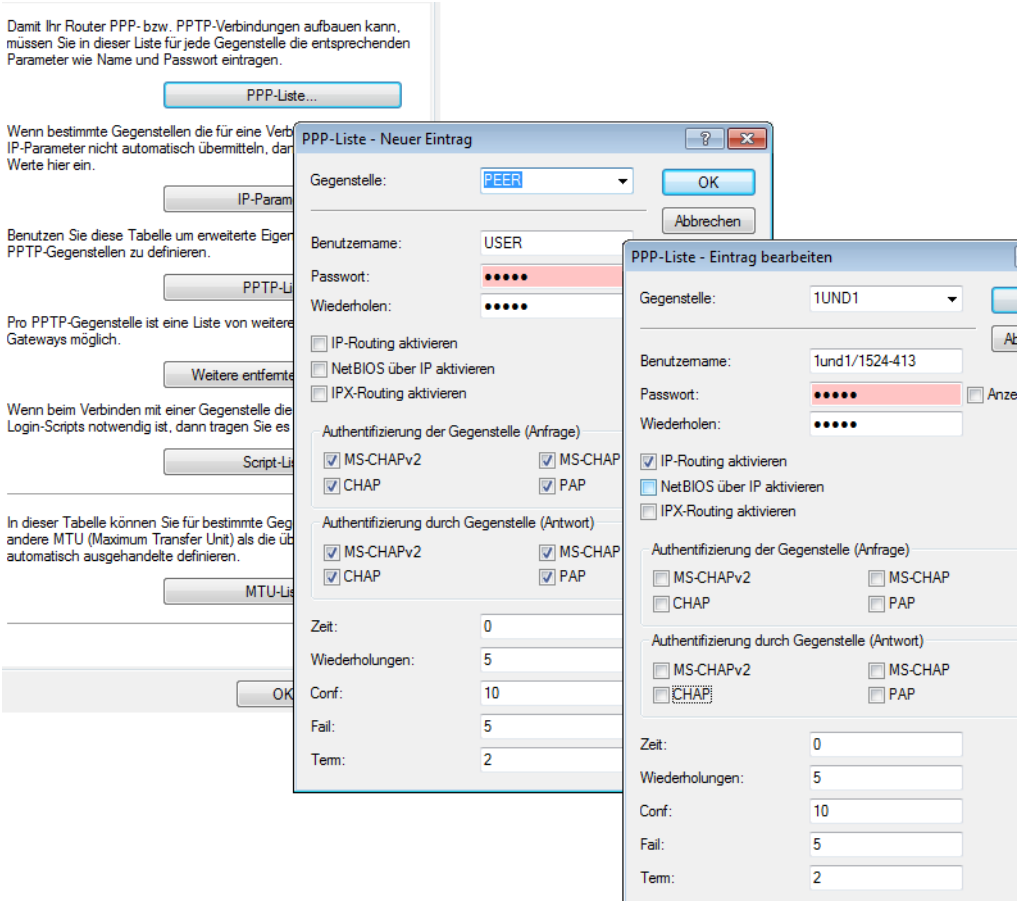
Bei diesem Verfahren wird eine PPP-Verbindung zu einer bestimmten Gegenstelle durch regelmäßige LCP-Anfragen überprüft. Üblicherweise wird mit diesem Verfahren z. B. die Verbindung zum Internet-Provider geprüft. Die LCP-Anfragen werden direkt an den Einwahlknoten gerichtet.

In der PPP-Liste wird dabei für diese Verbindung ein zeitlicher Abstand definiert, in dem die LCP-Anfragen an die Gegenstelle verschickt werden. Außerdem wird die Anzahl der Wiederholungen definiert, mit der bei Ausbleiben der LCP-Antworten erneut eine Anfrage gesendet wird. Erhält der Absender auch auf alle Wiederholungen keine Antwort, gilt die Leitung als gestört.

- **Zeit:** Die in der PPP-Liste eingetragene Zeit muss mit dem Faktor 10 multipliziert werden, um das tatsächliche Intervall zwischen zwei LCP-Anfragen zu erhalten. Ein Eintrag der Zeit von „5“ bedeutet also, das alle 50 Sekunden eine LCP-Anfrage gestartet wird.
- **Wiederholungen:** Bleibt die Antwort auf eine LCP-Anfrage aus, wird die Gegenstelle in kürzeren Intervallen geprüft. Im Sekundentakt versucht das Gerät dann erneut, die Gegenstelle zu erreichen. Die Anzahl der Wiederholungen gibt an, wie oft dieser Versuch wiederholt wird. Ein Eintrag der Wiederholung von „5“ bedeutet also, das die LCP-Anfrage 5-mal wiederholt wird, bevor die Leitung als gestört betrachtet wird.

Mit dem PPP LCP Monitoring wird nur die PPP-Strecke bis zum Internet-Provider geprüft.

Die Einstellungen für das LCP-Monitoring finden Sie in LANconfig im Konfigurationsbereich **Kommunikation** > **Protokolle** > **PPP-Liste**.



Kommandozeile: **Setup** > **WAN** > **PPP**

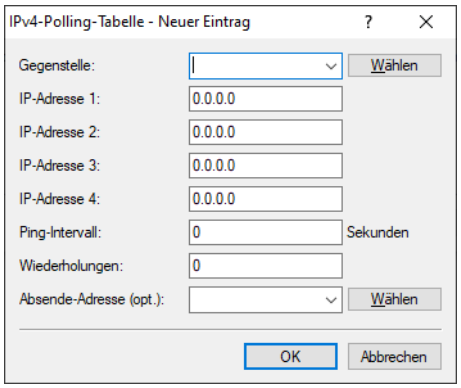
17.1.1.2 ICMP Polling für IPv4

Auch beim ICMP-Polling werden ähnlich dem LCP-Monitoring regelmäßig Anfragen an eine Gegenstelle geschickt. Hier werden ping-Befehle abgesetzt, deren Beantwortung überwacht wird. Anders als beim LCP-Monitoring kann für die ICMP-Pings jedoch die Ziel-Gegenstelle frei definiert werden. Mit einem Ping auf einen Router in einem entfernten Netz kann man so die gesamte Verbindung überwachen, nicht nur bis zum Internet-Provider.

In der Polling-Tabelle wird für die Gegenstelle ein Ping-Intervall definiert, in dem die Anfragen an die Gegenstelle verschickt werden. Außerdem wird die Anzahl der Wiederholungen definiert, mit der bei Ausbleiben der Antworten erneut eine Anfrage gesendet wird. Erhält der Absender auch auf alle Wiederholungen keine Antwort, gilt das Ziel der Ping-Anfragen als nicht erreichbar.

Zu jeder Gegenstelle können dabei bis zu vier verschiedene IP-Adressen eingetragen werden, die parallel im entfernten Netz geprüft werden. Nur wenn alle eingetragenen IP-Adressen nicht erreichbar sind, gilt die Leitung als gestört.

Mit dem ICMP-Polling kann eine komplette Verbindung von Ende zu Ende überwacht werden.



Die Einstellungen für das ICMP-Polling finden Sie in LANconfig im Konfigurationsbereich **Kommunikation** > **Protokolle** > **IPv4-Polling-Tabelle**.

Kommandozeile: **Setup** > **WAN** > **Polling-Tabelle**

Gegenstelle

Name der Gegenstelle, die über diesen Eintrag geprüft werden soll.

IP-Adresse 1-4

IP-Adressen, an die zur Prüfung der Gegenstelle ICMP-Requests gesendet werden.

Wird für eine Gegenstelle keine IP-Adresse eingetragen, die mit einem Ping geprüft werden kann, so wird die IP-Adresse des DNS-Servers geprüft, der bei der PPP-Verhandlung übermittelt wurde.

Ping-Intervall

Die in der Polling-Tabelle eingetragene Zeit gibt das Interval zwischen zwei Ping-Anfragen an. Wird hier eine „0" eingetragen, gilt der Standardwert von 30 Sekunden.

Wiederholungen

Bleibt die Antwort auf einen Ping aus, wird die Gegenstelle in kürzeren Intervallen geprüft. Im Sekundentakt versucht das Gerät dann erneut, die Gegenstelle zu erreichen. Die Anzahl der Wiederholungen gibt an, wie oft dieser Versuch wiederholt wird. Wird hier eine „0" eingetragen, gilt der Standardwert von 5 Wiederholungen.

Absende-Adresse (opt.)

Optionale Absenderadresse, die in den Ping eingetragen wird und auf der auch die Ping-Antwort erwartet wird.

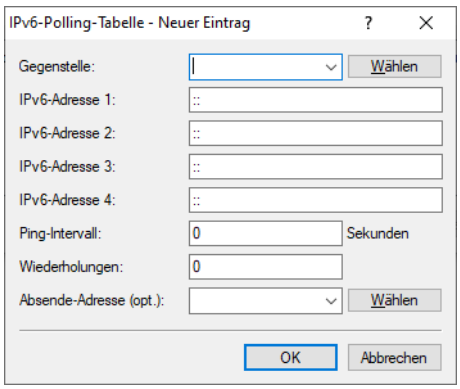
17.1.1.3 ICMPv6-Polling

Beim ICMPv6-Polling werden ähnlich dem LCP-Monitoring oder ICMP-Polling für IPv4 regelmäßig Anfragen an eine Gegenstelle geschickt. Hier werden ping-Befehle abgesetzt, deren Beantwortung überwacht wird. Anders als beim LCP-Monitoring kann für die ICMPv6-Pings jedoch die Ziel-Gegenstelle frei definiert werden. Mit einem Ping auf einen Router in einem entfernten Netz kann man so die gesamte Verbindung überwachen, nicht nur bis zum Internet-Provider.

In der IPv6-Polling-Tabelle wird für die Gegenstelle ein Ping-Intervall definiert, in dem die Anfragen an die Gegenstelle verschickt werden. Außerdem wird die Anzahl der Wiederholungen definiert, mit der bei Ausbleiben der Antworten erneut eine Anfrage gesendet wird. Erhält der Absender auch auf alle Wiederholungen keine Antwort, gilt das Ziel der Ping-Anfragen als nicht erreichbar.

Zu jeder Gegenstelle können dabei bis zu vier verschiedene IPv6-Adressen eingetragen werden, die parallel im entfernten Netz geprüft werden. Nur wenn alle eingetragenen IPv6-Adressen nicht erreichbar sind, gilt die Leitung als gestört.

Die Einstellungen für das ICMPv6-Polling finden Sie in LANconfig unter **Kommunikation** > **Protokolle** > **IPv6-Polling-Tabelle**.



Gegenstelle

Wählen Sie hier den Namen einer Gegenstelle aus der Gegenstellen-Liste.

IPv6-Adresse 1-4

Geben Sie hier bis zu 4 IPv6-Adressen an, welche der Reihe nach für diese Gegenstelle angepingt werden, um die Verbindung zu prüfen. Die Verbindung wird als intakt gewertet, wenn auch nur eine der angegebenen IPv6-Adressen erreicht werden kann.

Wählen Sie auf jeden Fall IPv6-Adressen, die zuverlässig erreichbar sind, da ansonsten unnötige Backup-Verbindungen initiiert würden.

Wenn Sie für alle vier IPv6-Adressen „::" eingeben, wird der per DHCPv6 oder Router Advertisement zugewiesene DNS-Server angepingt.

Ping-Intervall

Geben Sie hier das Ping-Intervall in Sekunden ein.

Wenn sie sowohl hier als auch bei den Wiederholungen 0 eingeben, wird ein Standardintervall von 20 Sekunden bei 5 Wiederholungen verwendet.

Wiederholungen

Geben Sie hier die Anzahl der Wiederholungen ein, die im Sekundentakt durchgeführt werden, wenn auf ein Ping keine Antwort empfangen wurde. Werden auch die wiederholten Pings nicht beantwortet, wird die Verbindung abgebaut.

Wenn sie sowohl hier als auch beim Ping-Intervall 0 eingeben, wird ein Standardintervall von 20 Sekunden bei 5 Wiederholungen verwendet.

Absende-Adresse (opt.)

Hier können Sie optional eine Absende-Adresse konfigurieren, die statt der ansonsten automatisch für die Zieladresse gewählten Absende-Adresse verwendet wird.

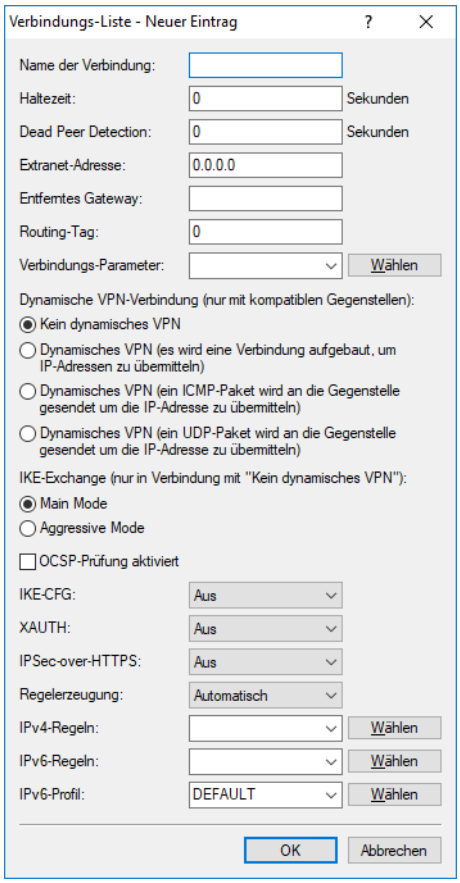
17.1.1.4 Dead-Peer-Detection (DPD)

Diese Verbindungsüberwachung wird bei der Einwahl von VPN-Clients in ein VPN-Gateway eingesetzt. Damit soll sichergestellt werden, dass ein Client ausgebucht wird, wenn die VPN-Verbindung z. B. durch kurzzeitigen Ausfall der Internetverbindung gestört wurde. Ohne eine entsprechende Leitungsüberwachung würde das VPN-Gateway den Client weiter in der Liste der eingebuchten Gegenstelle führen. Eine erneute Einwahl des Clients würde damit verhindert, weil z. B. beim WLANmonitor eine erneute Einwahl mit der gleichen Seriennummer nicht möglich ist.

Aus dem gleichen Grunde würde ohne Leitungsüberwachung die Einwahl eines Benutzers mit gleicher „Identity" – also gleichem Usernamen – verhindert, da der entsprechende Benutzer weiterhin in der Liste der eingebuchten Clients geführt würde.

Bei der Dead-Peer-Detection tauschen Gateway und Client während der Verbindung regelmäßig „Keep-Alive"-Pakete aus. Bleiben die Antworten aus, bucht das Gateway den Client aus und ermöglicht so nach dem Wiederherstellen der VPN-Verbindung eine erneute Anmeldung mit der gleichen Identity. Für VPN-Clients wird die DPD-Zeit üblicherweise auf 60 Sekunden eingestellt. Mögliche Werte: 0 – DPD deaktiviert; 30 bis 4.294.967.294 Sekunden.

Die Einstellungen für die Dead-Peer-Detection finden Sie in LANconfig unter **VPN** > **IKE/IPSec** > **Verbindungs-Liste**.



Kommandozeile: **Setup** > **VPN** > **VPN-Gegenstellen**

17.1.2 Hochverfügbarkeit der Leitungen – die Backup-Verbindung

Wenn eine Verbindung zum Internet-Provider oder zu einem entfernten Netzwerk gestört ist, dann kann eine Backup-Verbindung temporär die Aufgaben der eigentlichen Datenleitung übernehmen. Voraussetzung dafür ist eine zweite physikalische Leitung, über die die entsprechende Gegenstelle erreicht werden kann. Als typische Backup-Leitungen kommen z. B. in Frage:

- Mobilfunkverbindungen über integrierte 4G/5G-Modems

17.1.2.1 Konfiguration der Backup-Verbindung

Zur Definition einer Backup-Verbindung sind im Prinzip die folgenden Konfigurationsschritte notwendig:

1. Für die Backup-Verbindung wird auf der entsprechenden WAN-Schnittstelle die Gegenstelle so eingerichtet, dass sie über diesen alternativen Weg erreichbar ist. Soll z. B. die ISDN-Leitung als Backup-Verbindung dienen, wird die Gegenstelle als ISDN-Gegenstelle angelegt (mit den zugehörigen Einträgen bei den Kommunikations-Layern und in der PPP-Liste).
2. Gegebenenfalls müssen Sie zur Überwachung der Verbindung noch einen Eintrag in der Polling-Tabelle anlegen, wenn die Gegenstelle nicht über LCP-Anfragen geprüft werden kann.
3. Zuordnung der neuen Backup-Verbindung zu der Gegenstelle, die über das Backup abgesichert werden soll. Diesen Eintrag nehmen Sie in der Backup-Tabelle vor. Für die Backup-Verbindung werden keine eigenen Einträge in der Routing-Tabelle benötigt. Die Backup-Verbindung übernimmt die Quell- und Ziel-Netze automatisch von der Gegenstelle, die im störungsfreien Betrieb die Daten routet.

   In der Backup-Tabelle können einer Gegenstelle auch mehrere Backup-Leitungen zugeordnet werden. Dabei wird dann festgelegt, welche der Backup-Leitungen im Bedarfsfall zuerst aufgebaut werden soll:

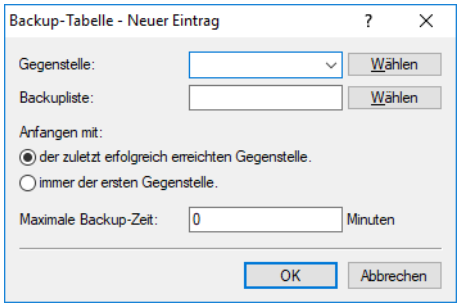
   - Die zuletzt erfolgreich erreichte Gegenstelle
   - Immer die erste Gegenstelle in der Liste

Die **maximale Backup-Zeit** gibt die maximale Zeitspanne in Minuten an, die der Backup-Zustand aufrecht erhalten wird. Wenn hier eine Zeit angegeben ist, so wird die Backup-Verbindung nach Ablauf dieser Zeit getrennt und der Backup-Zustand beendet.

Bei Backup-Szenarien mit Mobilfunk-Verbindungen (Multi-SIM), bei denen das Mobilfunk-Modul aus technischen Gründen zu jeder Zeit nur genau eine Verbindung haben kann, löst erst das Ende des Backup-Zustands einen erneuten Verbindungs-Versuch der Haupt-Verbindung aus.

Unabhängig vom Szenario tritt der Backup-Fall erneut ein, wenn die Haupt-Verbindung nach der außerhalb dieses Dialoges eingestellten Backup-Verzögerung nicht wieder aufgebaut werden kann.

Die Backup-Tabelle finden Sie in LANconfig unter **Kommunikation** > **Backup** in der **Backup-Tabelle**.



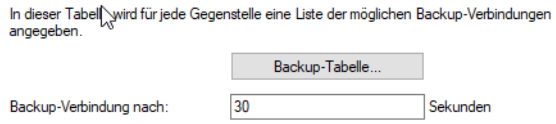
17.1.2.2 Auslösen der Backup-Verbindung

Der Backup-Fall wird ausgelöst, wenn der für die Verbindung definierte Überwachungsmechanismus (LCP- oder ICMP-Polling) keine Rückmeldung von den überwachten Gegenstellen erhält.

Die Backup-Verbindung wird dann aufgebaut, wenn:

- Die Backup-Verzögerungszeit abgelaufen ist und
- entweder
  - ein Datenpaket übertragen werden soll oder
  - für die Backup-Verbindung eine Haltezeit von 9999 Sekunden definiert wurde.

Die Backup-Verzögerungszeit wird unter LANconfig im Konfigurationsbereich **Kommunikation** > **Backup** > **Backup-Verbindung nach** eingetragen oder alternativ über die Kommandozeile unter **Setup** > **WAN** > **Backup-St.-Sekunden**.



Der Backup-Timer steuert ebenfalls die VRRP-Umschaltzeit.

17.1.2.3 Rückkehr zur Standard-Verbindung

Während die Backup-Verbindung die Datenübertragung übernimmt, versucht der Router permanent die Standard-Verbindung wieder aufzubauen. Sobald die Standard-Leitung wieder steht, wird die Backup-Verbindung beendet und die Leitungsüberwachung über LCP- oder ICMP-Polling setzt wieder ein.

Nur Keep-Alive-Verbindungen kommen automatisch zurück!

Die über eine Backup-Verbindung abgesicherte Standard-Verbindung wird nach dem Backup-Fall nur dann automatisch wieder aufgebaut, wenn die Haltezeit der Verbindung richtig konfiguriert ist:

- Eine Haltezeit mit dem Wert „0“ bedeutet, dass die Verbindung nicht aktiv getrennt wird. Wird die Verbindung jedoch durch eine Störung abgebaut oder abgebrochen, wird sie nicht automatisch neu aufgebaut. Erst wenn eine Kommunikation über die Verbindung angefordert wird, wird diese wieder aufgebaut.
- Eine Haltezeit mit dem Wert „9999“ bedeutet, dass die Verbindung permanent offen gehalten wird. Bei einer Trennung wird sie sofort wieder aktiv aufgebaut. Dieses Verhalten wird auch als **Keep-Alive** bezeichnet.

Stellen Sie sowohl für die Verbindung zum Internet-Provider (in der entsprechenden Namen-Liste) als auch für backup-gesicherte VPN-Verbindungen (in der VPN-Verbindungsliste) die Haltezeit auf „9999“, damit die Verbindung nach Beenden der Störung automatisch wieder aufgebaut wird und die Datenübertragung übernimmt.

17.1.3 Hochverfügbarkeit der Gateways – redundante Gateways mit VPN Load-Balancing

Neben den Leitungen zum Provider oder in ein anderes Netzwerk kann auch das eigene Gateway ausfallen. Besonders nachhaltige Folgen hat das z. B. dann, wenn ein zentrales VPN-Gateway ausfällt, über das sich viele Netzwerke von Außenstellen mit dem Netzwerk der Zentrale verbinden.

Um auch in diesem Fall die Erreichbarkeit der Zentrale zu gewährleisten, können mehrere VPN-Endpunkte (i. d. R. gleich konfigurierte, parallel betriebene zentrale VPN-Gateways) installiert werden. Sobald die Leitungsüberwachung (über Dead-Peer-Detection oder ICMP-Polling) fehlschlägt, kann nach verschiedenen Strategien (z. B. per zufälliger Auswahl aus den verfügbaren Gateways) ein neuer VPN-Endpunkt angesprochen werden. Innerhalb der Zentrale werden die in diesem Fall veränderten Routen über das lokale Default-Gateway mittels dynamischem Routing (RIP V2) propagiert.

Damit die zusätzlichen VPN-Gateways in einer solchen Installation nicht als „tote Leitungen“ auf ihren Einsatz warten, können sich alle verfügbaren Geräte auch im Normalbetrieb die Last der ein- und ausgehenden Verbindungen teilen und so einen intelligenten „Lastenausgleich“ realisieren.

17.1.4 Hochverfügbarkeit des Internetzugangs – Multi-PPPoE

Als dritte grundsätzlich verschiedene Störungsmöglichkeit betrachten wir den Fall, in dem sowohl die eigenen Gateways als auch die Verbindungsleitungen in Ordnung sind, es aber zu zeitweiligen Störungen im Netzwerk des Providers kommt.

Für diesen Fall können in einem Gerät mehrere PPPoE-Verbindungen auf einem physikalischen Interface eingerichtet werden (Multi-PPPoE).

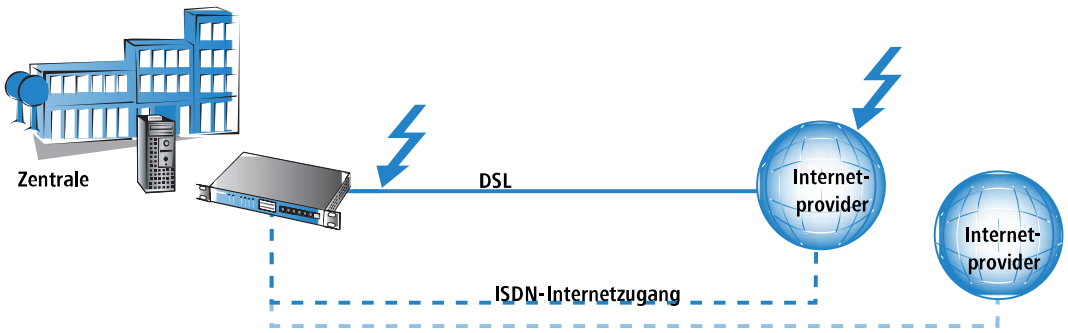
Zur Definition dieser Backup-Lösungen als alternative Internetzugänge richten Sie in Ihrem Gerät z. B. über die Setup-Assistenten nacheinander zwei Internet-Zugänge ein. Der Internet-Zugang, der im Normalfall verwendet werden soll, wird dabei als letzter konfiguriert. Dadurch werden die Einträge in der Routing-Tabelle mit der richtigen Gegenstelle verbunden.

Zusätzlich wird dann in der Backup-Tabelle ein Eintrag gemacht, mit dem die Gegenstelle des Standard-Providers mit dem alternativen Internetzugang abgesichert wird.

17.1.5 Anwendungsbeispiele

17.1.5.1 DSL-Internetzugang mit ISDN-Internetzugang absichern

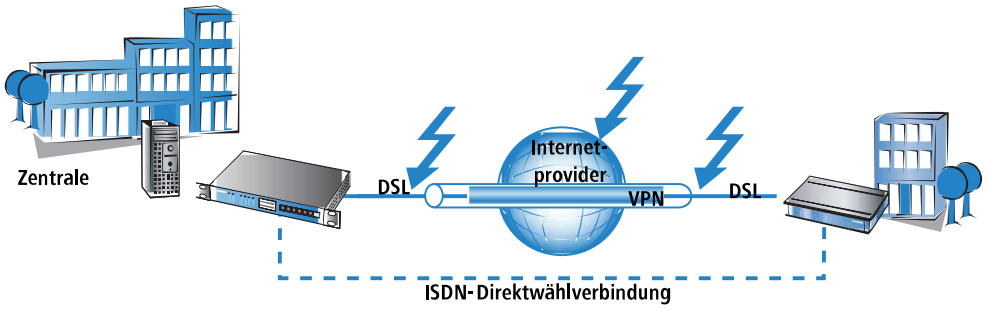
In diesem recht einfachen Backup-Szenario wird der Internetzugang über einen DSL-Zugang realisiert. Für den Fall einer Störung des Internetzugangs über DSL wird eine ISDN-Verbindung als Backup-Leitung definiert.



Diese Backup-Lösung kann z. B. mit Hilfe der Setup-Assistenten von LANconfig sehr komfortabel eingerichtet werden. Als zusätzliche Sicherheit kann für die Backup-Verbindung ein anderer Provider gewählt werden als für den Standard-Zugang: Mit dieser Lösung wird auch der Fall abgedeckt, dass das Netz des Providers gestört ist und der Fehler nicht in der DSL-Leitung zu finden ist.

17.1.5.2 Dynamic-VPN-Netzwerkkopplung mit ISDN-Direktwählverbindung absichern

Bei der Anbindung einer Filiale über eine VPN-Verbindung an die Zentrale kann es sinnvoll sein, die internetbasierte VPN-Verbindung durch eine direkte ISDN-Wählverbindung abzusichern. Falls die Internetverbindung bei einem der beiden Router ausfällt, kann die Datenübertragung über die ISDN-Kopplung fortgesetzt werden.



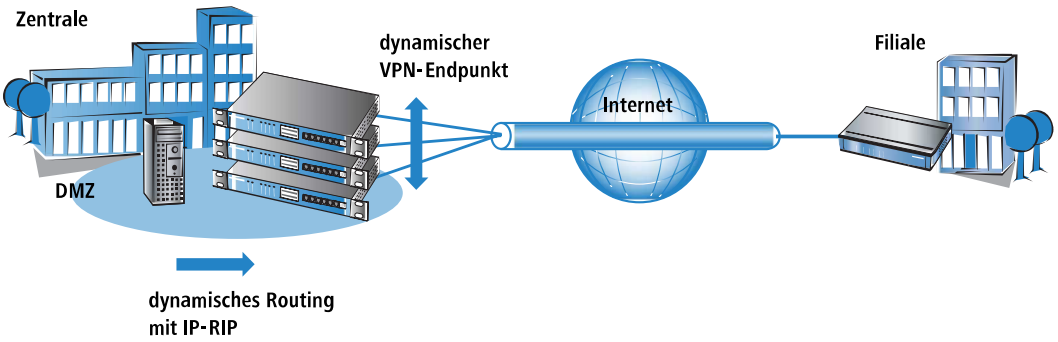
In diesem Szenario gehen wir von einer vollständig konfigurierten VPN-Verbindung zwischen den beiden Netzwerken aus.

- Zusätzlich wird dann eine LAN-LAN-Kopplung über ISDN zwischen den beiden Netzwerken angelegt. Verwenden Sie für diese Netzwerkkopplung **nicht** die Setup-Assistenten! Die Assistenten würden auch die Einträge in der Routing-Tabelle verändern und damit die funktionierende VPN-Netzwerkverbindung stören. Legen Sie die ISDN-Netzwerkkopplung in den Routern auf beiden seiten von Hand an – mit den entsprechenden Einträgen für die Gegenstellen in der Gegenstellenliste, der PPP-Liste und mit den benötigten Rufnummern und Zugangskennungen.
- Legen Sie im Gateway der Zentrale einen Eintrag in der Backup-Tabelle an, der die VPN-Gegenstelle über die direkt anzuwählende ISDN-Gegenstelle absichert.
- Außerdem legen Sie in der Polling-Tabelle im Router der Zentrale einen Eintrag an, der eine Gegenstelle im Netzwerk der Zentrale überwacht: üblicherweise die LAN-IP-Adresse des entfernten VPN-Gateways. Mit diesem Eintrag wird sichergestellt, dass der Router in der Zentrale umgehend auf eine Störung der VPN-Verbindung reagieren kann.

Wird nun die Verbindung zwischen Zentrale und Filiale irgendwo gestört (auf den Strecken zum Internetprovider oder beim Provider selbst) kann die ISDN-Leitung die Datenübertragung unabhängig vom Internet selbst übernehmen.

17.1.5.3 Redundante VPN-Gateways

In verteilten Unternehmensstrukturen, die auf Vernetzung der Standorte über VPN setzen, kommt der Verfügbarkeit der zentralen VPN-Gateways eine besondere Bedeutung zu. Nur wenn diese zentralen Einwahlknoten einwandfrei funktionieren, kann die betriebliche Kommunikation reibungslos ablaufen.



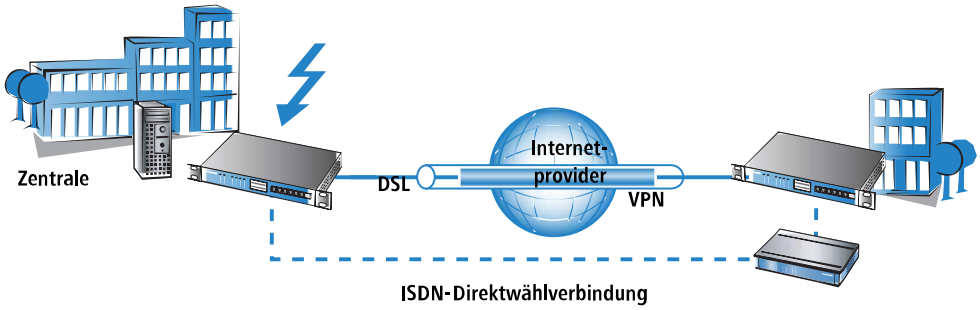
Mit der Möglichkeit, mehrere „Remote-Gateway"-Adressen als „dynamischer VPN-Endpunkt" für eine VPN-Verbindung zu konfigurieren, bieten LANCOM VPN-Gateways eine hohe Verfügbarkeit durch den Einsatz redundanter Geräte. Dabei werden in der Zentrale mehrere Gateways mit gleicher VPN-Konfiguration eingesetzt. In den Außenstellen werden alle vorhandenen Gateways als mögliche Gegenstellen für die gewünschte VPN-Verbindung eingetragen. Falls eines der Gateways nicht erreichbar ist, weicht der entfernte Router automatisch auf eine der anderen Gegenstellen aus.

Damit die Rechner im LAN der Zentrale auch wissen, welche Aussenstelle gerade über welches VPN-Gateway erreicht werden kann, werden die jeweils aktuellen Outbound-Routen zu den verbundenen Gegenstellen über RIPv2 im Netzwerk der Zentrale propagiert.

Wenn die Außenstellen so konfiguriert werden, dass sie beim Aufbau der VPN-Verbindung die Gegenstelle zufällig auswählen, wird mit diesem Mechanismus ein leistungsfähiger Lastenausgleich zwischen den VPN-Gateways in der Zentrale realisiert („VPN Load-Balancing").

17.1.5.4 VPN-Gateway mit ISDN-Gateway über RIP absichern

In einem weiteren Schritt können auch die VPN-Gateways selbst gegen Störungen gesichert werden. In diesem Fall betrachten wir eine VPN-Verbindung über zwei entsprechende Gateways. Falls eines der beiden VPN-Geräte gestört ist, soll eine ISDN-Verbindung die Datenübertragung übernehmen, in diesem Fall eine direkte Wählverbindung.



Zur Konfiguration dieser Lösung gehen wir wieder von einer funktionierenden VPN-Kopplung der beiden Netzwerke aus. Zusätzlich sind noch folgende Schritte erforderlich:

- Zwischen den beiden ISDN-Routern wird eine normale ISDN-Netzwerkkopplung eingerichtet, die die gleichen Netzbereiche routet wie die VPN-Verbindung. In der Routing-Tabelle wird dabei jedoch eine Distanz eingetragen, die mindestens um 1 höher ist als die entsprechende Route des VPN-Gateways.
- In allen beteiligten Routern wird das lokale RIP (RIP V2) aktiviert. Damit können die VPN- und ISDN-Router jeweils die bekannten Routen zu den Gegenstellen austauschen. Mit der höheren Distanz ist die Route im ISDN-Gateway dabei im Normalfall die schlechtere Route.
- In diesem Fall müssen keine Backup-Verbindungen definiert werden, da im Bedarfsfalle ein anderes Gerät die Datenübertragung übernehmen soll.

Wird nun die Verbindung zwischen den beiden VPN-Geräten gestört, ändert sich automatisch der Wert für die Distanz der entsprechenden Routen: eine nicht erreichbare Route wird mit der Distanz 16 markiert. Dadurch wird die im ISDN-Router eingetragene Route automatisch die „bessere" Lösung, alle Datenpakete werden nun über die ISDN-Strecke geführt. Sobald die VPN-Verbindung wieder hergestellt ist, ändert sich die Distanz wieder auf einen Wert unterhalb der ISDN-Verbindung, der Backup-Fall endet wie gewünscht.

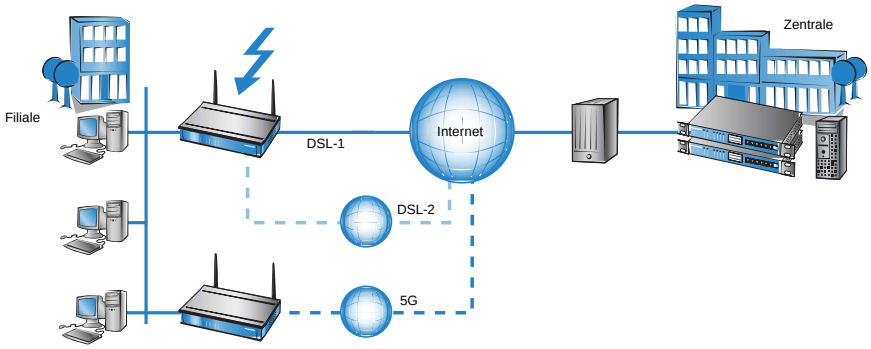
17.2 Backup-Lösungen und Load-Balancing mit VRRP

17.2.1 Einleitung

Die hohe Verfügbarkeit von Datenverbindungen stellen vor allem im geschäftlichen Umfeld eine unverzichtbare Anforderung an die eingesetzten Netzwerkkomponenten dar. Die Geräte stellen verschiedene Mechanismen zur Sicherung der Datenübertragung als Backup-Lösungen bereit:

- Die verschiedenen WAN-Schnittstellen (DSL, Glasfaser, 4G/5G) ermöglichen die Datenübertragung über ein zweites physikalisches Medium, falls die Hauptleitung ausfällt oder gestört ist.
- Zum Schutz vor Störungen im Netz des Internetproviders lassen sich über Multi-PPPoE verschiedene Internetzugänge konfigurieren.
- Mehrere VPN-Gateways in einem Netzwerk können sich untereinander die benötigten VPN-Tunnel teilen und so auch bei zeitweisem Ausfall eines VPN-Endpunktes den Datenverkehr aufrecht erhalten.
- Mit VRRP kann nun zusätzlich ein ausgefeiltes Backup-System zum Schutz vor Hardware-Ausfällen der Router realisiert werden. Dabei werden in einem Netzwerk zwei oder mehr Router installiert, die sich beim Ausfall eines Gerätes gegenseitig vertreten können.
- Zusätzlich zum normalen VRRP kann das Auslösen des Backup-Falls an die Verfügbarkeit einer Datenverbindung geknüpft werden. Mit dieser Zusatzfunktion können die Geräte mit mehreren WAN-Interfaces (z. B. zwei DSL-Interfaces)

sehr flexibel in Backuplösungen eingesetzt werden. Der Backup-Fall wird dabei z. B. dann ausgelöst, wenn die Default-Route über das erste DSL-Interface nicht mehr erreichbar ist. Das 5G-Interface des Gerätes kann aber einen weiteren Platz in der Backup-Kette einnehmen, wenn auch der Backup-Router gestört ist.



Die VRRP-Umschaltzeit wird über den Backup-Timer (siehe *Auslösen der Backup-Verbindung* auf Seite 1542) beeinflusst.

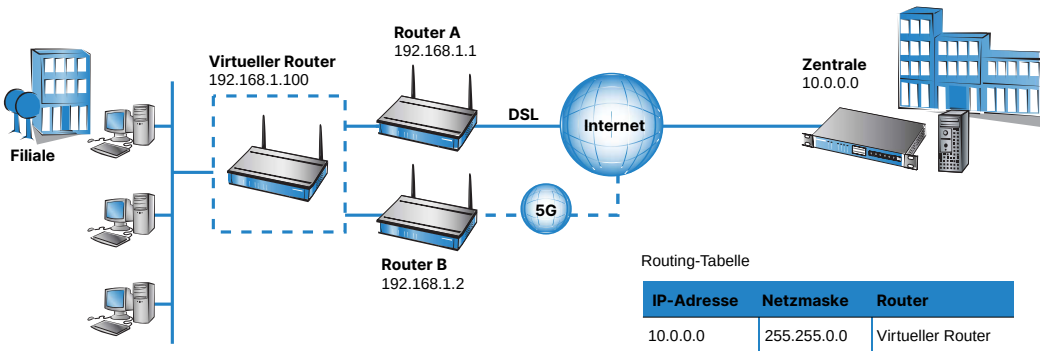
17.2.2 Das Virtual Router Redundancy Protocol

VRRP – das Virtual Router Redundancy Protocol – dient dazu, mehrere physikalische Router wie einen einzigen „virtuellen" Router erscheinen zu lassen. Von den vorhandenen physikalischen Routern ist immer einer der „Master". Der Master ist der einzige Router, der eine Datenverbindung z. B. ins Internet herstellt und Daten überträgt. Erst wenn der Master ausfällt (z. B. aufgrund einer Hardwarestörung oder weil seine Internetanbindung nicht mehr verfügbar ist), dann kommen die anderen Router ins Spiel. Über das Protokoll VRRP, das im *RFC 3768* beschrieben ist, handeln sie aus, welches Gerät die Rolle des Masters übernehmen soll. Der neue Master übernimmt vollständig die Aufgaben des bisherigen Masters.

17.2.2.1 Virtuelle und physikalische Router

Dynamische Routing-Protokolle wie RIP o. ä. passen die Einträge in den dynamischen Routing-Tabellen an, wenn z. B. eine Route nicht mehr verfügbar ist. Beim Einsatz von VRRP können die Hosts im LAN eine statische Routing-Tabelle verwenden, obwohl sich die IP-Adresse des Gateways ändert, wenn ein Gerät z. B. durch Defekt ausfällt und ein anderes seine Aufgaben übernimmt. Damit die Teilnehmer im Netzwerk trotzdem immer das richtige Gateway finden, verwendet VRRP „virtuelle Router" in den Routing-Tabellen. Ein solcher virtueller Router wird im Netzwerk wie ein „normaler" Router mit seiner IP-Adresse '192.168.1.100' bekannt gemacht und übernimmt die Aufgabe eines Gateways zu bestimmten Gegenstellen. Die tatsächliche Arbeit der Datenübertragung übernehmen die physikalischen Router hinter dem virtuellen Router.

- Im störungsfreien Betrieb stellt z. B. Router A mit der IP-Adresse '192.168.1.1' die Verbindung zum Internet her.
- Fällt der Router A aus, übernimmt der Router B mit der IP-Adresse '192.168.1.2' die Aufgaben von Router A. Die Clients im Netzwerk bemerken von diesem Wechsel gar nichts, für sie ist nach wie vor der „virtuelle" Router '192.168.1.100' das Gateway.



Routing-Tabelle

IP-Adresse	Netzmaske	Router
10.0.0.0	255.255.0.0	Virtueller Router

Etwas technischer betrachtet benötigt ein Router in einem Netzwerk neben der IP-Adresse natürlich auch eine eindeutige MAC-Adresse. Bei der Definition eines virtuellen Routers wird daher gleichzeitig eine virtuelle MAC-Adresse festgelegt, auf die der virtuelle Router reagiert. Die virtuelle MAC-Adresse wird gebildet zu '00-00-54-00-01-xx', wobei 'xx' für die eindeutige Router-ID steht.

Zur Unterscheidung, welcher physikalische Router auf die Kombination aus virtueller IP- und MAC-Adresse reagiert, werden Prioritäten für die physikalischen Router verwendet. Hierzu wird jedem physikalischen Router eine Priorität zugewiesen. Der Router mit der höchsten Priorität übernimmt als Master die Aufgaben des virtuellen Routers und reagiert somit auf die virtuellen IP- und MAC-Adressen. Haben zwei physikalische Router die gleiche Priorität, dann wird der Router mit der „höheren" physikalischen IP-Adresse als Master betrachtet.

Alle physikalischen Router melden in regelmäßigen Intervallen ihre Bereitschaft, so dass bei einem Ausfall des aktuellen Masters spätestens nach Ablauf dieses Intervalls der Router mit der nächst-höheren Priorität das Routing übernehmen kann. Wenn ein Gerät selbst feststellt, dass es die anstehenden Aufgaben nicht erfüllen kann, kann es sich schon vor Ablauf des Intervalls aktiv abmelden und somit die Übernahme der Masterrolle durch den nächst-priorisierten Router auslösen.

Der große Vorteil der virtuellen Router besteht in der Möglichkeit, sehr flexible Szenarien mit Backup- und Load-Balancing-Funktionen einzurichten, die quasi unbemerkt vom LAN ablaufen. So wählen die Clients im lokalen Netz aus den verfügbaren DHCP-Servern zufällig einen aus und beziehen von diesem Server die benötigten Adressinformationen.

Adresszuweisung über DHCP mit mehreren DHCP-Servern im LAN

In einem LAN können durchaus mehrere DHCP-Server nebeneinander betrieben werden, ohne sich gegenseitig zu stören. Die DHCP-Clients fordern beim Aufbau der Netzwerkverbindung eine IP-Adresse an und wählen dazu einen der verfügbaren DHCP-Server aus. Der angesprochende DHCP-Server prüft vor der Zuweisung der Adresse, ob die angefragte Adresse im LAN schon verwendet wird oder frei ist. Durch diese Prüfung werden Adresskonflikte auch beim Betrieb mehrerer DHCP-Server verhindert.

Für die Clients ist es unerheblich, welcher physikalische Router anschließend die Datenverbindung herstellt. Ebenso bemerken die LAN-Clients nicht den Ausfall eines Routers oder eines WAN-Interfaces, da ein anderer Router in diesem Fall unter den gleichen virtuellen Adressen wie zuvor für das LAN einspringt.

17.2.2.2 Geräte-, Leitungs- oder Gegenstellen-Backup

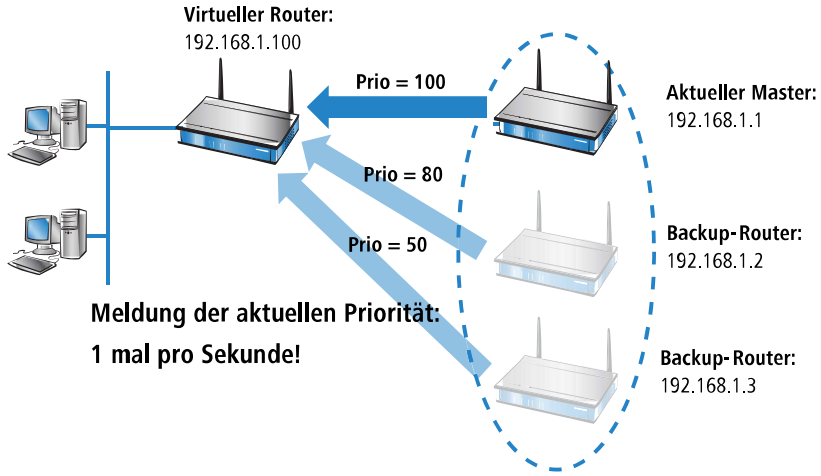
Die Möglichkeit, dass sich ein Gerät selbst aus dem VRRP-Verbund abmelden kann, deutet schon darauf hin, dass sich die Möglichkeiten von VRRP nicht nur auf den kompletten Ausfall eines Gerätes beziehen können.

VRRP stellt grundsätzlich nur einen Backup-Mechanismus bereit, der den Ausfall eines Gerätes absichert. In der Praxis führen aber auch der Ausfall eines physikalischen Datenübertragungsmediums (z. B. DSL oder 5G) oder die Unerreichbarkeit einer Gegenstelle dazu, dass ein Router seine Aufgaben nicht mehr wie geplant wahrnehmen kann. Aus diesem Grund stellen die LANCOM spezifischen Erweiterungen zu VRRP die Möglichkeit bereit, als auslösendes Ereignis für den Backup-Fall auch die Verfügbarkeit einer Gegenstelle zu definieren – unabhängig davon, ob die Datenverbindung durch Geräte-, Leitungs- oder Gegenstellenprobleme nicht zustande kommt.

Zur Definition eines virtuellen Routers sind mindestens die IP-Adresse nötig, unter der er erreichbar ist, sowie seine Priorität und seine logische Router-ID. Die Router-ID dient dazu, dass die regelmäßigen Meldungen der physikalischen Router den jeweiligen virtuellen Routern zugeordnet werden können.

- Die Router-ID kann einen Wert zwischen 1 und 255 annehmen. Aus der Router-ID ergibt sich auch die virtuelle MAC-Adresse des Routers zu 00:00:5E:00:01:Router-ID. Die Router-ID 0 ist unzulässig.
- Die IP-Adresse des virtuellen Routers ist frei wählbar, sie muss sich natürlich innerhalb des lokalen Netzes befinden. Wenn die Adresse des virtuellen Routers gleich der des physikalischen Routers ist, dann ist der physikalische Router der „Haupt-Master" des Systems. Der Haupt-Master hat automatisch die höchste Priorität, d. h. wenn er sich Betriebsbereit meldet, wird er sofort zum aktiven Master.

- Die Priorität kann Werte zwischen 1 und 255 annehmen. Die Werte 0 und 255 haben Sonderbedeutungen: Mit der Priorität 0 ist der virtuelle Router nicht aktiv, mit 255 ist dieser virtuelle Router der Haupt-Master.

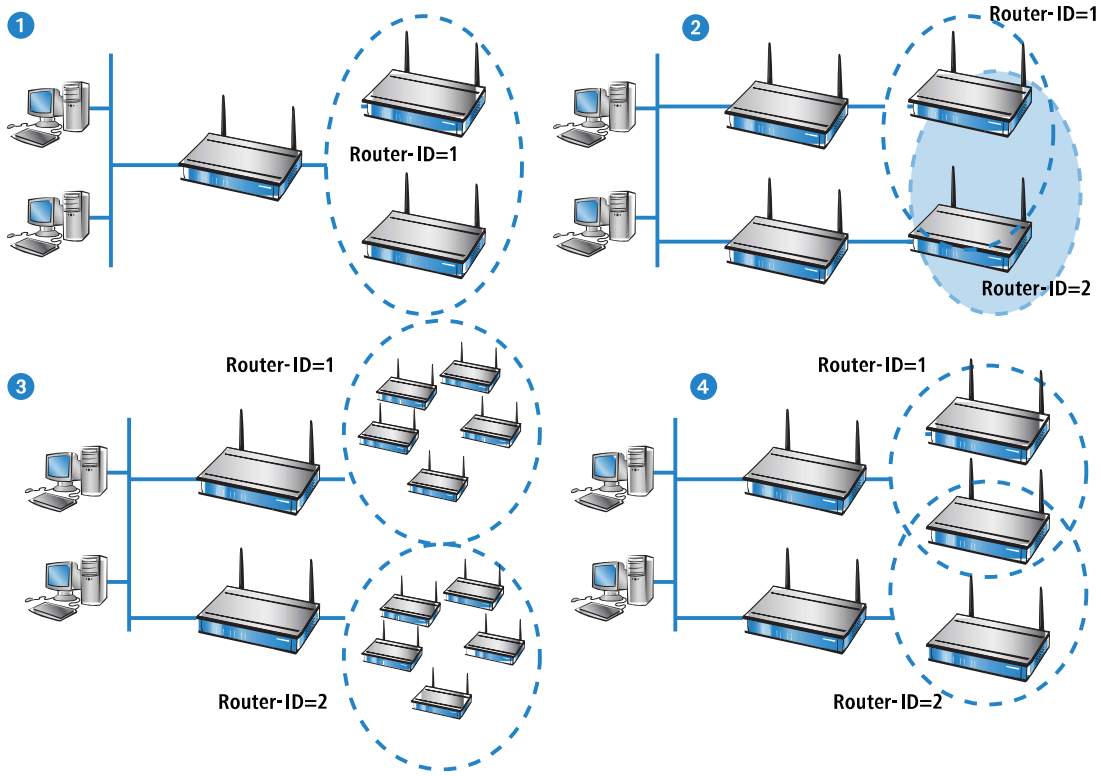


17.2.2.3 Router-ID definiert „Standby-Gruppen“

Mit der bei der Definition eines virtuellen Routers festgelegten Router-ID können die physikalischen Router den virtuellen Routern zugeordnet werden. Alle Geräte, in denen virtuelle Router mit der gleichen Router-ID angelegt sind, bilden eine „Standby-Gruppe“, in denen sich die Geräte gegenseitig vertreten können. Drei verschiedene Muster für Standby-Gruppen sind üblich:

- Im einfachen Backup-Szenario bilden zwei oder mehr Router **eine** Standby-Gruppe. In allen physikalischen Routern wird ein virtueller Router mit der gleichen Router-ID und der gleichen virtuellen IP-Adresse konfiguriert (Position **1** im folgenden Bild).
- Zur Realisierung eines Load-Balancings werden so viele virtuelle Router mit unterschiedlichen IDs und IPs definiert, wie physikalische Router für den VRRP-Verbund vorgesehen sind. Zwei Geräte würden z. B. zu jeweils **zwei** Standby-Gruppen gehören (**2**).
- Möglich sind auch anspruchsvolle Kombinationen mit vielen Geräten. So können z. B. zwei Geräte eine eigene Standby-Gruppe mit der Router-ID 1 bilden und zwei weitere Geräte eine andere Gruppe mit der ID 2 (**3**). Auch die

wahlweise Zuordnung von einigen Geräten zu nur einer Gruppe, während andere Geräte zu allen Gruppen gehören, ist damit je nach Bedarf möglich (**4**).



17.2.2.4 Das System der Prioritäten

VRRP steuert mit der Auswertung der Prioritäten die Reihenfolge, in der die physikalischen Router die Aufgabe des Masters in einem VRRP-Verbund einnehmen. Dabei betrachtet VRRP nur den Ausfall eines kompletten Gerätes als Auslöser für den Backup-Fall.

Da zahlreiche Geräte über mehr als ein WAN-Interface verfügen, betrachtet die VRRP-Anwendung im LCOS nicht nur den Ausfall eines Gerätes, sondern auch Störungen der Leitung bzw. die Unerreichbarkeit einer Gegenstelle als Auslöser für den Backupfall. Um das Backupverhalten der Geräte und den Aufbau von Backup-Ketten zu ermöglichen, werden jedem virtuellen Router zwei Prioritäten zugeordnet: eine Haupt- und eine Backup-Priorität.

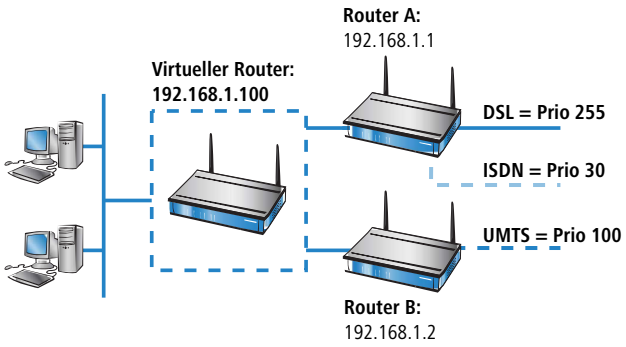
- Die Haupt-Priorität wird verwendet (ins Netzwerk propagiert), solange sich das Gerät im normalen Betriebszustand befindet (also die Gegenstelle der Hauptverbindung noch erreichbar ist).
- Die Backup-Priorität wird propagiert, wenn sich das Gerät im Backup-Zustand befindet (d. h. das Backup-Delay ist abgelaufen ohne dass die Verbindung erneut aufgebaut werden konnte).
- Wenn als Backup-Priorität 0 eingetragen ist, meldet sich der Router bis zum Ende des Backup-Falls gar nicht mehr, d. h. das Gerät steht bei Unerreichbarkeit der Gegenstelle nicht für den VRRP-Router-Verbund zur Verfügung.

Da VRRP selbst nur „Prioritäten" kennt und keine Unterscheidung nach Haupt- oder Backup-Priorität vornimmt, wertet es einfach die Priorität aus, die gerade vom Gerät propagiert wird. Das Gerät mit der aktuell höchsten Priorität wird als Master betrachtet.

Üblicherweise werden die Prioritäten so konfiguriert, dass die Haupt-Prioritäten der Geräte in einem VRRP-Verbund größer sind als die verwendeten Backup-Prioritäten. Diese Regel ist allerdings keine Vorschrift. Die Haupt-Priorität eines Routers A kann durchaus kleiner sein als die Backup-Priorität eines anderen Gerätes B. In diesem Fall wird die Backup-Verbindung von Gerät B **vor** der Hauptverbindung des Routers A in der Backup-Kette eingesetzt.

Die Zuordnung der Prioritäten zu den verschiedenen WAN-Interfaces der Geräte ergibt sich aus der Konfiguration der Backup-Verbindungen in der **Backup-Tabelle** (unter LANconfig in **Kommunikation** > **Backup**.

- Die Haupt-Priorität bezieht sich auf das Interface, auf dem die Hauptverbindung konfiguriert ist.
- Die Backup-Priorität bezieht sich auf das Interface, auf dem die Backupverbindung konfiguriert ist.



VRRP-Liste Router A:

Haupt-Prio	Backup-Prio	Gegenstelle
255	30	INTERNET-DSL

Backup-Liste Router A:

Gegenstelle	Backup-Liste
INTERNET-DSL	INTERNET-ISDN

VRRP-Liste Router B:

Haupt-Prio	Backup-Prio	Gegenstelle
100	0	INTERNET-UMTS

Ein aufgrund der Prioritätenlage aktivierter Master versucht nun die Verbindung aufzubauen, wenn diese als Keep-Alive-Verbindung konfiguriert wurde. Ist die Verbindung als normale Verbindung mit Haltezeit eingerichtet, dann wird sie erst mit dem nächsten zu übertragenden Paket aufgebaut. Scheitert dieser Verbindungsaufbau und löst dadurch den Backup-Fall aus, so meldet sich auch der Router ab und propagiert sich selbst wiederum mit seiner Backup-Priorität.

17.2.2.5 Backup-Ketten

Durch die Verwendung von Zweitprioritäten wird der Aufbau von flexiblen Backup-Ketten ermöglicht, bei denen jeder physikalische Router nicht nur einen Platz in der Kette einnimmt, sondern einen Platz für jedes physikalische WAN-Interface:

- Der erste physikalische Router, der Haupt-Router im Netz, verfügt z. B. über ein DSL- und ein ISDN-Interface, der zweite Router (Backup-Router) über ein DSL- und ein UMTS-Interface.
- Für den ersten Router wird als Haupt-Priorität die 255 eingetragen, er wird damit zum Haupt-Router, als Backup-Priorität die 50.
- Für den zweiten Router wird als Haupt-Priorität die 150 eingetragen, als Backup-Priorität die 100.

Im Normalbetrieb wird der Datenverkehr über das DSL-Interface des ersten Routers abgewickelt. Fällt der Router oder dieses Interface aus, versucht der zweite Router (aufgrund der nächst-höheren Haupt-Priorität) die Verbindung über sein eigenes DSL-Interface aufzunehmen. Gelingt dies nicht, propagieren beide Geräte ihre Backup-Priorität. Da der zweite Router über die höhere Backup-Priorität verfügt, wird die Verbindung also über das dort vorhandene UMTS-Interface aufgebaut. Erst wenn auch dieses Interface keine Verbindung aufbauen kann, wird das ISDN-Interface des ersten Routers (mit der geringeren Backup-Priorität) eingesetzt.

Nur Keep-Alive-Verbindungen kommen automatisch zurück!

Die über eine Backup-Verbindung abgesicherte Standard-Verbindung wird nach dem Backup-Fall nur dann automatisch wieder aufgebaut, wenn die Haltezeit der Verbindung richtig konfiguriert ist:

- Eine Haltezeit mit dem Wert 0 bedeutet, dass die Verbindung nicht aktiv getrennt wird. Wird die Verbindung jedoch durch eine Störung abgebaut oder abgebrochen, wird sie nicht automatisch neu aufgebaut. Erst wenn eine Kommunikation über die Verbindung angefordert wird, wird diese wieder aufgebaut.
- Eine Haltezeit mit dem Wert 9999 bedeutet, das die Verbindung permanent offen gehalten wird. Bei einer Trennung wird sie sofort wieder aktiv aufgebaut. Dieses Verhalten wird auch als **Keep-Alive** bezeichnet.

Stellen Sie sowohl für die Verbindung zum Internet-Provider (in der entsprechenden Namen-Liste) als auch für backup-gesicherte VPN-Verbindungen (in der VPN-Verbindungsliste) die Haltezeit auf 9999, damit die Verbindung nach Beenden der Störung automatisch wieder aufgebaut wird und die Datenübertragung übernimmt.

17.2.2.6 Die Rückkehr in den VRRP-Verbund

Nach einer einstellbaren Zeit (Reconnect-Delay) versucht ein abgemeldeter Router erneut, seine Haupt- oder Backup-Verbindung aufzubauen, ohne vorher seine Priorität zu propagieren. Wenn die Haupt-Verbindung aufgebaut werden konnte, wird der Backup-Fall beendet und der Router propagiert wieder seine Haupt-Priorität. Wurde nur die Backup-Verbindung aufgebaut, fällt der Router in den normalen Backup-Fall zurück und propagiert wieder seine Backup-Priorität.

Sobald ein Gerät seine Hauptverbindung wieder aufbauen kann, propagiert sich der Router wieder mit seiner Haupt-Priorität und wird zum Master:

- Geräte im Backup-Zustand mit einer niedrigeren Haupt-Priorität als der aktive Master können damit ebenfalls den Backup-Zustand verlassen und ihre Haupt-Priorität propagieren, da ihre Backup-Verbindung in diesem Zustand nicht benötigt wird.
- Geräte im Backup-Zustand mit einer höheren Haupt-Priorität als der aktive Master verbleiben im Backup-Zustand, solange sie ihre höher-priorisierte Hauptverbindung noch nicht aufbauen können.
- Geräte, die sich aufgrund der Unerreichbarkeit der VRRP-Gegenstelle über die Backup-Verbindung vollständig aus dem VRRP-Verbund abgemeldet haben, fallen in den normalen Backup-Zustand zurück.

17.2.2.7 Der Verbindungsaufbau

Damit Verbindungsaufbauten koordiniert ablaufen und nicht alle Standby-Router ständig versuchen, Verbindungen aufzubauen, werden Verbindungen von einem Router nur dann aufgebaut, wenn dieser Router

- Master ist **oder**
- er sich im Backup-Fall befindet und seine Hauptverbindung mit Keep-Alive konfiguriert ist **oder**
- er sich völlig abgemeldet hat und der Timer für den erneuten Verbindungs-Versuch (Reconnect-Delay) abläuft.

Diese einfache Regel ermöglicht es, auch in Standby-Routern die Hauptverbindung als Keep-Alive-Verbindung zu konfigurieren. Ebenso erlaubt ist es, auch im Haupt-Router nur Verbindungen mit Haltezeit zu verwenden.

Verbindungen werden immer abgebaut, wenn alle mit der Gegenstelle verbundenen virtuellen Router in den Standby-Zustand gewechselt sind. Dies geschieht entweder dadurch, dass ein anderer Router eine höhere Priorität propagiert oder beim Verlust der LAN-Verbindung.

17.2.3 Anwendungsszenarien

VRRP wird üblicherweise in zwei verschiedenen Anwendungsfällen eingesetzt:

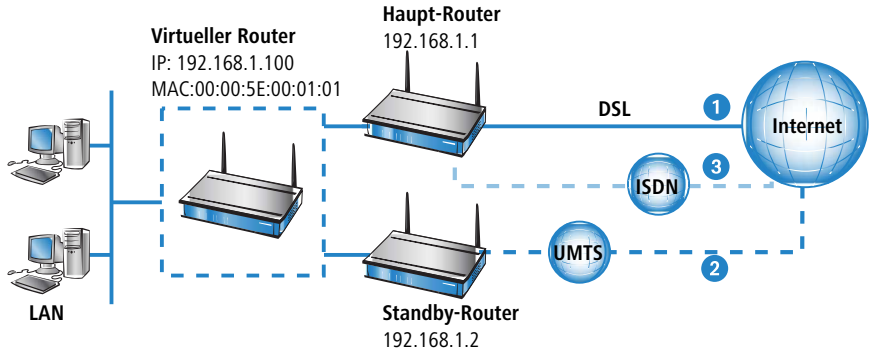
- Im einfachen Backup-Fall mit zwei Routern stellt ein Gerät im normalen Betrieb die Verbindung ins Internet her. Das zweite Gerät wird nur als „Standby-Gerät" im Wartezustand betrieben und übernimmt die Aufgabe des Haupt-Routers, wenn dieser ausfällt.
- Im zweiten Fall arbeiten zwei oder mehr Geräte parallel als Router im gleichen Netzwerk und verteilen im Rahmen eines statischen Load-Balancings die anfallenden Datenverbindungen. Fällt eines der Geräte aus, kann einer der anderen Router im Verbund die Aufgaben des ausgefallenen Gerätes mit übernehmen.

17.2.3.1 Backup-Lösung mit VRRP

Die wohl wichtigste Anwendung von VRRP ist die Bereitstellung von Backup-Verbindungen, wobei ein oder mehrere Router als Backup für den Haupt-Router dienen. Diese Router können unterschiedliche physikalische Medien für die Internet-Verbindung nutzen, wie z. B. DSL im Haupt-Router und UMTS oder ISDN in den Backup-Routern. Eine übliche Backup-Kette sieht dann wie folgt aus:

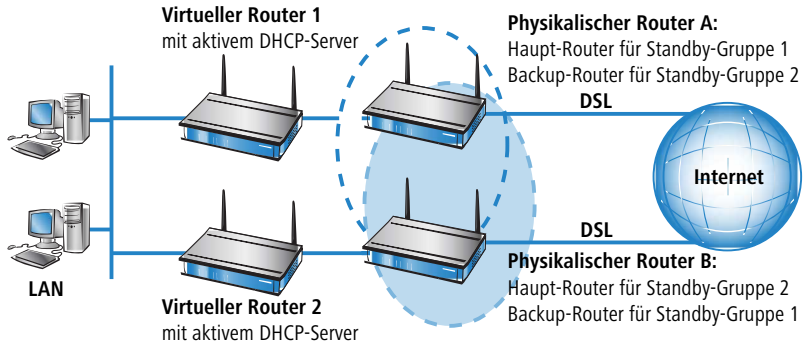
- Bei Ausfall der DSL-Verbindung **1** übernimmt der UMTS-Router **2** die Aufgabe.
- Bei Ausfall der UMTS-Verbindung **2** übernimmt der ISDN-Router **3** die Aufgabe.

Da fast alle LANCOM Geräte mit DSL-Interface gleichzeitig auch ein ISDN-Interface haben, kann der Haupt-Router auch das ISDN-Backup am Ende der Backup-Kette übernehmen – solange kein vollständiger Ausfall der Hardware vorliegt.



17.2.3.2 Load-Balancing

Beim Load-Balancing existieren mehrere Router, welche die gleichen Ziele erreichen können. Diese Router werden den Rechnern im LAN über die in jedem Router aktiven DHCP-Server gleichmäßig verteilt als Default-Gateway bekannt gegeben. Fällt einer der Router aus, so kann der andere seine Aufgabe übernehmen, wenn beide Router VRRP beherrschen. Dazu werden auf jedem Router genau so viele virtuelle Router definiert, wie es auch reale Router gibt. Den Rechnern im LAN wird als Gateway jeweils einer der virtuellen Router zugeordnet. Über die Prioritäten der virtuellen Router wird nun festgelegt, in welcher Reihenfolge die anderen Router beim Ausfall eines Masters die Rolle übernehmen. Auch hier kann über Haupt- und Backup-Priorität eine Backup-Kette aufgebaut werden.



17.2.3.3 Anwendungsbeispiel: Absicherung eines Internetzugangs mit zwei DSL / ISDN-Kombi-Routern

Das LAN wird über zwei sich gegenseitig absichernde, im Load-Balancing betriebene Default-Gateways an zwei DSL-Leitungen betrieben. Im Schnitt buchen sich 50 % der LAN-Stationen auf Router 1 ein und 50 % auf Router 2. Bei Ausfall eines Routers oder der Nichtverfügbarkeit einer Leitung übernimmt jeweils der andere Router die Aufgaben komplett.

Im Normalbetrieb ist also jeder Router für den Internetzugang von durchschnittlich 50 % der Teilnehmer im LAN zuständig (Prio 250 für den DSL-Zugang). Fällt ein Router oder eine DSL-Leitung aus, so wird die entsprechende Last auf den anderen Router verteilt (Prio 100 für den DSL-Zugang des Backup-Routers). Fallen beide DSL-Leitungen aus, so wird der Traffic über die ISDN-Leitungen geführt (jeweils Backup-Prio 50, ISDN-Leitungen nicht im Bild eingezeichnet).

Hinweise für die Konfiguration der virtuellen Router:

Router A		Router B	
	DHCP = Ein (10.1.1.x)		DHCP = Ein (10.1.1.x)
Router-ID = 1	Router IP = 10.1.1.1	Router-ID=1	Router IP=10.1.1.1

Router A		Router B	
	Prio = 250		Prio = 100
	Backup-Prio = 50		Backup-Prio = 50
	Gegenstelle = DSL-INTERNET		Gegenstelle = DSL-INTERNET
	Kommentar: Haupt-Router f. Gruppe1		Kommentar: Backup-Router f. Gruppe1
Router-ID = 2	Router IP = 10.1.1.2	Router-ID = 2	Router IP = 10.1.1.2
	Prio = 100		Prio = 250
	Backup-Prio = 50		Backup-Prio = 50
	Gegenstelle = DSL-INTERNET		Gegenstelle = DSL-INTERNET
	Kommentar: Backup-Router f. Gruppe 2		Kommentar: Haupt-Router f. Gruppe 2

17.2.4 Zusammenspiel mit internen Diensten

Da bei Verwendung von VRRP virtuelle Router mit virtuellen IP- und MAC-Adressen verwendet werden, hat dies auch Einfluss auf interne Dienste der LANCOM Geräte. Diese müssen sich unterschiedlich verhalten, je nachdem, ob ein virtueller Router oder ein physikalischer Router angesprochen wird. Je nach verwendetem Dienst oder Protokoll müssen die Antworten auf Adressanfragen verändert oder ganz abgelehnt werden.

17.2.4.1 ARP

Das wichtigste Protokoll im Umgang mit virtuellen Routern ist ARP (Address Resolution Protocol), das eine Zuordnung von logischen Adressen wie IP-Adressen zu Hardware-Adressen wie den MAC-Adressen ermöglicht. Durch die Verwendung von virtuellen und physikalischen IP- und MAC-Adressen kommt dem Verhalten der Router auf ARP-Abfragen eine große Bedeutung zu:

- Ein ARP-Request auf die Adresse des virtuellen Routers darf nur beantwortet werden, wenn der LANCOM Router selbst der Master ist. Diese Anfrage muss mit der zugehörigen virtuellen MAC-Adresse beantwortet werden. Alle anderen Anfragen müssen ignoriert werden.
- ARP-Requests, die als Absenderadresse, die Adresse eines virtuellen Routers haben, müssen ignoriert werden.
- Bei Verwendung von Proxy-ARP muss bei einem ARP-Request geprüft werden, ob mit der Gegenstelle, über die die angefragte Adresse erreicht werden kann, ein virtueller Router assoziiert ist. Wenn ja, dann darf der Request nur beantwortet werden, wenn der LANCOM Router selbst der Master ist. Dies gilt auch für virtuelle Gegenstellen (also PPTP oder VPN), wenn diese als physikalische Verbindung eine Gegenstelle verwenden, die mit einem virtuellen Router assoziiert ist.
- ARP-Requests, die der LANCOM Router selbst verschickt, sendet es immer mit seiner realen Absenderadresse, solange diese nicht die Adresse eines virtuellen Routers ist. In diesem Fall muss die virtuelle MAC-Adresse im ARP-Request eingetragen werden.

Routen von lokalen Diensten / ARP-Handling schaltbar

Einleitung

Antwortpakete für interne Dienste (z. B. telnet, http/https, tftp, …) des Gerätes an Empfänger im Ethernet (LAN oder WAN) wurden bis zur LCOS-Version 7.80 immer direkt an die entsprechenden Absender gesandt, so dass dadurch z. B. auch Geräte von beliebigen LANs heraus gefunden werden konnten.

Ab der LCOS-Version 7.80 ist schaltbar, ob anstelle der direkten Adressierung eine vorherige ARP-Anfrage und das daraus resultierende Routing verwendet werden soll.

Soll beispielsweise ein LANCOM Router auch ohne Kenntnis bzw. Konfiguration der LAN-Topologie durch LANconfig gefunden werden können, so empfiehlt sich das bisherige Verhalten. In diesem Fall antwortet der Router direkt per Unicast an den Absender des TFTP-Broadcasts (hier: Gerätesuche in LANconfig).

In Szenarien, in denen wechselnde, virtuelle MAC- und IP-Adressen im LAN zum Einsatz kommen – beispielsweise bei Nutzung von VRRP-Komponenten im LAN – kann es mit der direkten Adressierung zu Fehlauflösungen kommen, sollte beispielsweise das Redundanzprotokoll eine andere MAC- / IP-Zuordnung vorgenommen haben. In diesen Fällen empfiehlt sich die Einstellung „Interne Dienste routen".

Konfiguration

Mit einer entsprechenden Option in den Einstellungen für das IP-Routing können die internen Dienste des LANCOM Gerätes über den Router geleitet werden.

Kommandozeile: **Setup** > **IP-Router** > **Routing-Methode**

Interne-Dienste-routen

Wählen Sie hier aus, ob die internen Dienste über den Router geleitet werden sollen. Mögliche Werte:

Ja

Die Pakete für die internen Dienste werden über den Router geleitet.

Nein

(Default) Die Pakete werden direkt an den Absender zurückgeschickt.

17.2.4.2 ICMP

Bei ICMP muss zwischen Echo-Requests und -Replies auf der einen und Fehlermeldungen auf der anderen Seite unterschieden werden. Bei den Fehlermeldungen bedarf der ICMP-Redirect einer zusätzlichen Betrachtung.

- Auf einen ICMP-Echo-Request, der an die Adresse eines virtuellen Routers gerichtet ist, darf der LANCOM Router nur antworten, wen er selbst der Master ist.
- ICMP-Redirects dürfen auch von virtuellen Routern versendet werden, als Absenderadresse muss aber die Adresse des virtuellen Routers eingetragen sein, an den das Paket gesendet wurde. Diese ist über die Ziel-MAC-Adresse des Pakets zu ermitteln.
- Wird der LANCOM Router unter seiner physikalischen MAC-Adresse angesprochen und ist das Ziel des Pakets mit einem virtuellen Router verknüpft, dessen Adresse direkt an das empfangende Interface gebunden ist, so wird ein ICMP-Redirect zurückgeschickt und dem Absender die Adresse des virtuellen Routers übermittelt.
- Bei allen anderen Fehlermeldungen ist es letztendlich egal, ob als Absenderadresse die Adresse des virtuellen Routers oder die reale Adresse verwendet wird. Der Einfachheit halber wird immer die reale Adresse verwendet.

Mit der Implementation von VRRP im LCOS wird die bisherige Option 'lokales Routing' im IP-Router Menü ersetzt durch 'ICMP-Redirects senden'. Wenn diese Option aktiviert ist, werden ICMP-Redirects versendet, bei deaktivierter Option werden die Pakete immer weitergeleitet.

17.2.4.3 DHCP

- Gateway-Adresse

  Auch wenn die Rechner im LAN über ICMP-Redirects den korrekten virtuellen Router erlernen können, ist es sinnvoll, in der DHCP-Verhandlung direkt den richtigen Router als Gateway zuzuweisen. Daher wird die zuzuweisende Gateway-Adresse nun wie folgt bestimmt:

  - Wenn für das Interface im DHCP-Modul ein Gateway explizit angegeben ist, dann wird nur dieses zugewiesen.
  - Existiert keine explizite Gateway-Vorgabe, wird in der Routing-Tabelle die Default-Route gesucht. Wenn die Default-Route existiert und mit einem virtuellen Router verbunden ist, der direkt an das Interface gebunden ist, über das die DHCP-Anfrage empfangen wird, wird die Adresse des virtuellen Routers als Gateway zugewiesen.
  - Sollten weitere Gegenstellen mit virtuellen Routern verknüpft sein, so werden diese nicht über DHCP zugewiesen, da es nur ein Default-Gateway geben kann. Ein Host kann die zugehörenden Routen nur über ICMP-Redirects lernen.

- Ansonsten wird die zum Adresspool bzw. Interface passende Adresse (Intranet oder DMZ) zugewiesen.

Sollten mehrere virtuelle Router mit der Default-Route verbunden sein, so wird immer die Adresse des Routers mit der höchsten Priorität zugewiesen. Hierdurch wird ein Load-Balancing automatisch über die Auswahl des DHCP-Servers durch den jeweiligen Client realisiert. Dazu wird auf allen am Load-Balancing beteiligten Routern der DHCP-Server aktiviert. Alle Router definieren entsprechend viele virtuelle Router mit jeweils unterschiedlichen Prioritäten. Wenn der Client nun aus allen antwortenden DHCP-Servern zufällig auswählt, wird ihm auch zufällig einer der virtuellen Router zugewiesen.

Beispiel mit zwei Routern

Router A definiert folgende virtuellen Router:

Router-ID	virt. Addresse	Prio	B-Prio	Peer
1	10.0.0.1	100	50	INTERNET
2	10.0.0.2	60	50	INTERNET

und Router B entsprechend:

Router-ID	virt. Addresse	Prio	B-Prio	Peer
1	10.0.0.1	60	30	INTERNET
2	10.0.0.2	100	30	INTERNET

Einem DHCP-Client wird nun, je nachdem ob er sich für Router A oder Router B entscheidet, als Gateway die 10.0.0.1 bzw. die 10.0.0.2 zugewiesen und somit zunächst auf beide Router verteilt.

An diesem Beispiel wird auch deutlich, wie das Load-Balancing mit dem Backup verknüpft werden kann: Fällt Router A in den Backup-Fall, so wird Router B für alle Clients zum Master. Sollte nun noch Router B ausfallen, so wird Router A zum Master für alle und versucht seinen Backup aufzubauen. Scheitert dies, so kommt nun wieder LANCOM B zum Zuge (damit ist das Ende der Backup-Kette erreicht).

- weitere Adressen

Wenn der DHCP-Server für bestimmte Dienste, die das Gerät zur Verfügung stellt, wie z. B. DNS-Server, explizit Adressen zuweisen soll, dann werden entweder die konfigurierten Adressen oder aber die reale Adresse des jeweiligen Interfaces zugewiesen. Eine Zuweisung eines virtuellen Routers verstößt gegen den RFC, der verbietet, dass ein virtueller Router weitere Dienste anbietet. Ein Gerät darf nur dann auf eine virtuelle Adresse reagieren, wenn es auch der „Eigentümer" dieser Adresse ist, d. h. wenn diese Adresse auch die reale Adresse des Interfaces ist. Dies bedeutet gleichzeitig, dass es für DNS eine Sonderbehandlung geben muss.

17.2.4.4 DNS-Server

Da der RFC es verbietet, dass ein virtueller Router zusätzliche Dienste anbietet, wenn der physikalische Router nicht „Eigentümer" der virtuellen IP-Adresse ist, bedarf es einer Sonderbehandlung für den DNS-Server des LANCOM Routers. Das Gerät stellt zwei Varianten zur Verfügung.

- Die RFC-konforme Lösung arbeitet im DNS-Forwarder. Wenn als primärer oder sekundärer DNS-Server eine externe IP-Adresse eingetragen ist, dann funktioniert das Weiterleiten an den zuständigen virtuellen Router automatisch im Rahmen der ICMP-Redirect-Behandlung, da das Paket einfach an den virtuellen Router weitergeleitet wird.

  Ist jedoch keine Adresse eingetragen und keine Verbindung zur Gegenstelle aufgebaut, an die das Paket weitergeleitet werden soll, so prüft der DNS-Forwarder, ob mit der Gegenstelle ein virtueller Router verbunden ist.

  - Wenn dies der Fall ist und das Gerät auch selbst Master für einen der virtuellen Router ist, so wird die Verbindung aufgebaut und das Paket an den auf dieser Verbindung zugewiesenen DNS-Server weitergeleitet.
  - Ist das Gerät selbst nicht Master aller verbundenen Router, so wird das Paket an den Master des ersten verbundenen Routers weitergeleitet.

Dieses Verfahren funktioniert nur, wenn sich alle Router RFC-konform verhalten und Port-Forwarding einsetzen. Wenn es sich bei allen beteiligten Routern um LANCOM Geräte handelt, ist diese Voraussetzung erfüllt.

- Bei der zweiten Variante reagiert ein virtueller Router selbst auf DNS-Anfragen.
  - Zum Aktivieren dieses Verhaltens muss die Option „Internal Services" aktiviert werden. Das LANCOM Gerät akzeptiert die Anfragen auf die internen Dienste (wie z. B. hier DNS) über die virtuellen Adressen so, als wenn es unter der physikalischen Adresse angesprochen würde.
  - In der Einstellung **Aus** verhält sich das LANCOM Gerät RFC-konform und verwirft die zugehörigen Pakete.
  - Die Default-Einstellung ist **An**.

  Ist bei Verwendung der internen Dienste ein virtueller Router mit der Default-Route verbunden, so wird dieser vom DHCP-Server des LANCOM Routers als DNS-Server zugewiesen. Sind mehrere virtuelle Router mit der Default-Route verbunden, so wird derjenige mit der höchsten Priorität zugewiesen (wie bei den Gateway-Adressen).

Diese Variante kann nur dann einen reibungslosen Ablauf garantieren, wenn es sich bei allen beteiligten Routern um LANCOM Geräte handelt.

17.2.4.5 RIP

Einen besonders starken Einfluss hat die Verwendung von VRRP auf RIP, über das Informationen über die erreichbaren Routen und die zugehörigen Router propagiert werden.

- Zum einen müssen Routen zu Gegenstellen, die über einen virtuellen Router erreicht werden können, im Netz bekannt gemacht werden.
- Zum anderen müssen die Routen ignoriert werden, die von den virtuellen Routern selbst propagiert werden.
- Schließlich ist die propagierte Information noch abhängig von dem Interface, auf dem sie weitergegeben werden soll.

Für die Bekanntmachung der Routinginformationen über RIP gelten die folgenden Regeln:

- Routen werden auf allen virtuellen und physikalischen Interfaces propagiert, dabei gilt jeder virtuelle Router als eigenes virtuelles Interface.
- Werden aktuell Routen auf einem physikalischen Interface (LAN / DMZ) propagiert und eine zu propagierende Route ist mit einem virtuellen Router verbunden, dann müssen zwei Fälle unterschieden werden:
  - Wenn der virtuelle Router auf dem Interface aktiv ist, d. h. seine Adresse liegt im Adresskreis auf dem entsprechenden Interface, wird die Route nicht propagiert.
  - Wenn der virtuelle Router auf dem Interface nicht aktiv ist, dann wird die Route ganz normal propagiert, d. h. die physikalische Adresse des Interfaces wird als beste Route propagiert.
- Werden Routen auf einem virtuellen Router propagiert, dann dürfen nur die Routen propagiert werden, die mit diesem virtuellen Router verbunden sind.
- Werden Routen auf einem WAN-Interface propagiert, werden alle Routen propagiert.
- Beim Empfang eines RIP-Pakets muss die Absenderadresse des RIP-Pakets berücksichtigt werden. Die in dem Paket enthaltenen Routen müssen ignoriert werden, wenn sie von einem im LANCOM Router bekannten virtuellen Router propagiert werden.
- Wenn der LANCOM Router keine Verbindung zu einer Gegenstelle aufbauen kann, weil alle Kanäle belegt sind, dann propagiert das RIP die über diese Gegenstelle erreichbaren Routen als „unerreichbar".
  - Zusätzlich wird in diesem Fall das VRRP-Modul darüber informiert, damit es den mit dieser Gegenstelle verbundenen virtuellen Router abmeldet und ein neuer Master ermittelt werden muss.
  - Genauso wird das VRRP darüber informiert, wenn die Verbindung wieder möglich ist, um den virtuellen Router wieder mit seiner jeweiligen Haupt- oder Backup-Priorität propagieren zu können

17.2.4.6 NTP

Wenn der Schalter „Internal-Services" aktiviert ist, dann akzeptiert das LANCOM Gerät auch (S)NTP-Anfragen, die an virtuelle Router gestellt werden, da die genaue Adresse der Zeit-Quelle für einen NTP-Client unerheblich ist.

17.2.4.7 Weitere Dienste

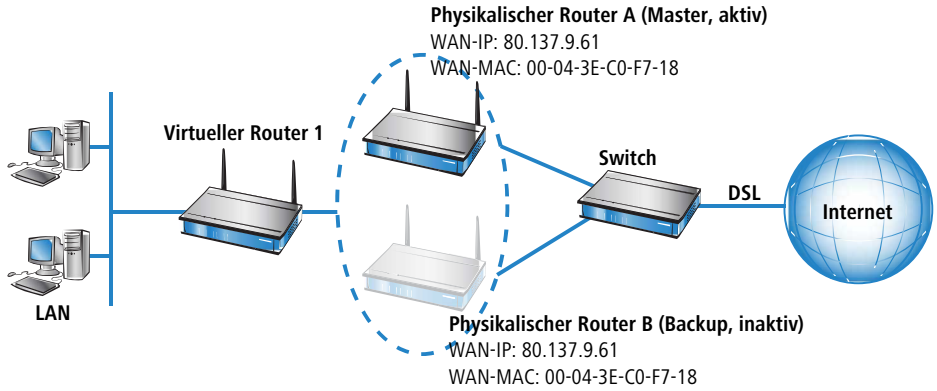
Alle anderen Dienste bearbeitet das LANCOM Gerät nur, wenn es unter seiner physikalischen Adresse angesprochen wurde.

17.2.5 VRRP im WAN

Die Beschreibung von VRRP bezieht sich zunächst nur auf die LAN-Seite von Datennetzen und überlässt die Regelung der WAN-Seite dynamischen Routing-Protokollen wie z. B. RIP. Um trotzdem auch mit VRRP eine WAN-seitige Ausfallsicherung zu ermöglichen, sieht das VRRP im LANCOM Router zwei Möglichkeiten vor.

17.2.5.1 Gleiche IP- und MAC-Adressen

Die erste Möglichkeit besteht darin, allen Routern im VRRP-Verbund auf der WAN-Seite sowohl die gleiche MAC- als auch die gleiche IP-Adresse zuzuweisen. Die Router werden dann z. B. über einen Switch mit einer gemeinsam genutzten DSL-Leitung verbunden. Um Adresskonflikte zu vermeiden, darf dabei immer nur ein Router tatsächlich auf seiner WAN-Seite auf diese Adressen reagieren, was durch die Verwendung von VRRP realisiert wird.



- Da der Router seine WAN-Verbindung abbaut, wenn der letzte virtuelle Router in den Backup-Zustand wechselt, ist diese Bedingung garantiert erfüllt, wenn insgesamt nur ein virtueller Router definiert wurde.
- Auch im Backup-Szenario ist die notwendige Bedingung erfüllt, da hier die Hauptverbindung garantiert abgebaut wurde ehe der Backup-Router zum Master wird.

17.2.5.2 Routing-Protokolle

Im Load-Balancing-Szenario sind jedoch zwei verschiedene WAN-Strecken gleichzeitig online, weshalb hier die Verwendung gleicher MAC- und IP-Adressen von vorneherein ausscheidet. Hier muss als zweite Möglichkeit ein Routing-Protokoll wie RIP, OSPF oder BGP eingesetzt werden.

Um die Umschaltung über das recht langsame RIP zu beschleunigen, propagiert ein LANCOM Router vor dem Verbindungsabbau noch alle Netze als nicht mehr erreichbar ins WAN und sorgt so für eine schnelle Änderung der Routing-Prioritäten.

17.2.6 Interaktion mit dem WAN-Backup-Modul

Das VRRP-Modul ist eng an das WAN-Backup-Modul angebunden, um eine Interaktion der beiden Funktionalitäten zu ermöglichen. Grundsätzlich passiert die Interaktion in beide Richtungen: Das VRRP kann einerseits abhängig vom Zustand der virtuellen Router den Aufbau von WAN-Verbindungen anfordern oder unterbinden, und andererseits kann der

Verbindungszustand einer WAN-Verbindung (aufgebaut/Backup/abgebaut) einen Einfluss darauf haben, welche Priorität die virtuellen Router verwenden.

Ein virtueller Router im VRRP interagiert dabei mit maximal einer WAN-Verbindung (und ihren Backup-Verbindungen), und zwar genau dann, wenn der Name der WAN-Verbindung in der Spalte **Überwachte Gegenstelle** in der Konfigurationstabelle **Virtuelle Router** eingetragen ist. Ist dort für einen virtuellen Router kein Eintrag vorhanden, interagiert dieser Router nicht mit dem WAN-Backup-Modul.

17.2.7 Steuerung des WAN/WAN-Backup durch das VRRP

Wenn virtuelle Router, die ein WAN-Interface überwachen, existieren, und keiner von diesen im Zustand „Master" ist, fordert das VRRP einen Verbindungsabbau des überwachten WAN an, und unterbindet einen Wiederaufbau. Sobald einer der Router den Zustand zu Master wechselt, wird der Verbindungsaufbau freigegeben und ein Verbindungsversuch gestartet. Da WAN-Verbindungen für IPv4 und IPv6 gemeinsam auf- und abgebaut werden, spielt hierbei die IP-Version der virtuellen Router keine Rolle. Generell gilt: Wenn der VRRP-Schalter **VRRP aktiviert** nicht eingeschaltet wurde, dann findet keinerlei Beeinflussung des WAN-Backup-Moduls durch das VRRP statt.

Beachten Sie hier auch den Schalter **Setup** > **VRRP** > **WAN-Verbindungskontrolle** (2.141.7).

17.2.8 Konfiguration von VRRPv3

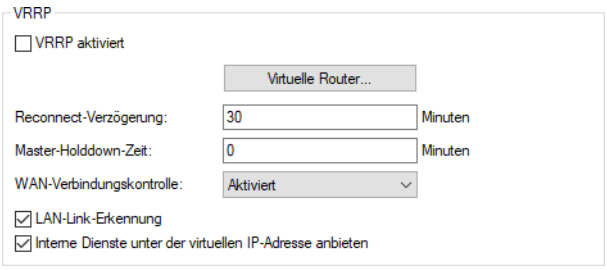
LCOS unterstützt VRRPv2 und VRRPv3 (*RFC 5798* sowie *RFC 9568*) für IPv4 und IPv6.

VRRP mit IPv6 funktioniert nur mit statischen Adressen oder Network Prefix Translation (NPTv6) in Richtung des Internetproviders.

VRRP arbeitet für IPv4 und IPv6 jeweils unabhängig, auch wenn es gemeinsam in einer Zeile konfiguriert wurde. Dies ist sogar empfehlenswert, damit das Advert.-Intervall und die Prioritäten konsistent sind.

Die Einstellungen für das VRRP finden Sie in LANconfig unter **IP-Router** > **VRRP**.

Kommandozeile: **Setup** > **VRRP**



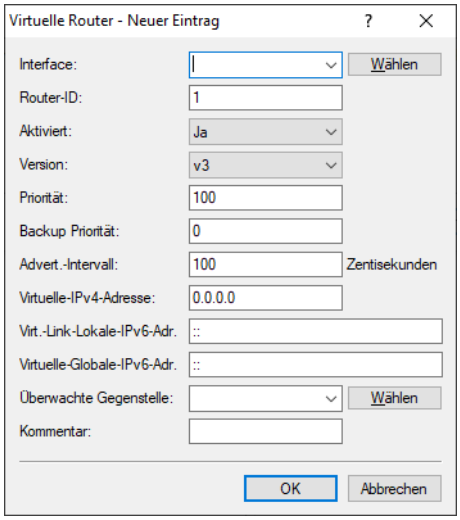
Zur Konfiguration von Ausfallsicherung (Router-Redudanz) oder Load-Balancing über VRRP können folgende Parameter eingestellt werden:

VRRP aktiviert

Mit diesem Schalter lässt sich das VRRP-Modul ein- und ausschalten (Default: Aus).

Virtuelle Router

In der Tabelle Virtuelle Router können die virtuellen Router pro Interface definiert werden.



Interface

Logisches IPv4- oder IPv6-Interface bzw. Netzwerk, auf dem VRRP aktiviert werden soll. Grundsätzlich sind nur LAN-Interfaces sinnvoll. Andere Schnittstellen lassen sich zwar auswählen, führen aber zu einem underfinierten Verhalten.

Router-ID

Eindeutige ID des virtuellen Routers. Es sind Werte zwischen 1 und 255 möglich. Mit der Router-ID werden mehrere physikalische Router zu einen virtuellen Router bzw. einer Standby-Gruppe zusammengefasst. Manchmal wird die Router-ID auch VRRP-ID oder kurz VRID genannt.

Aktiviert

Aktiviert oder deaktiviert VRRP für diesen Konfigurationseintrag.

Version

Definiert welche VRRP-Version verwendet werden soll. Es werden VRRPv2, VRRPv3 oder VRRPv2 und VRRPv3 unterstützt. IPv6 wird nur bei VRRPv3 unterstützt. IPv4 wird sowohl bei VRRPv2 als auch bei VRRPv3 unterstützt.

Der Modus v2+v3 ist als Übergangslösung für die Transition von einem VRRPv2- zu einem VRRPv3-Betrieb unter IPv4 gedacht und sorgt für ein verdoppeltes Paketaufkommen, da ein so konfigurierter Virtueller Router Advertisements in beiden Protokollversionen versendet.

Ein Virtueller Router, der auf eine Protokollversion konfiguriert wurde, verwirft Advertisements anderer Router, wenn sie die falsche Protokollversion haben, und gibt eine Ausgabe auf dem VRRP-Packet Trace aus und trägt einen zugehörigen Eintrag in die Event-Log-Tabelle ein.

Priorität

Gibt die Priorität an, mit der der Virtuelle Router arbeitet. Diese wird in den Advertisements übertragen und bestimmt maßgeblich, welches Gerät der zuständige Master für eine VRRP-Verbund ist. Die angegebene Priorität muss größer als 0 sein. Der Wert 255 hat eine Sonderbedeutung:

- Der Wert 255 wird automatisch eingestellt, wenn die Adresse des virtuellen Routers gleich der Adresse des Interfaces ist, an das der Router gebunden ist. In allen anderen Fällen wird die Priorität automatisch herabgesetzt.

Backup-Priorität

Die Backup-Priorität des virtuellen Routers bezieht sich auf das Interface, für das eine Backup-Verbindung konfiguriert ist, also z. B. bei Routern mit DSL- und Mobilfunk-Unterstützung auf das Mobilfunk-Interface. Es sind Werte zwischen 0 und der konfigurierten Priorität zulässig. Der Wert 0 hat eine Sonderbedeutung:

- 0 deaktiviert den virtuellen Router im Backup-Fall. Es wird in regelmäßigen Abständen geprüft, ob die Hauptverbindung wieder aufgebaut werden kann. Das Prüf-Intervall wird im Reconnect-Delay festgelegt.

Wenn im Backup-Fall auch die Backup-Verbindung nicht aufgebaut werden kann meldet sich der virtuelle Router vollständig ab und versucht ebenfalls in, über die Reconnect-Verzögerung angegebenen, Intervallen entweder die Haupt- oder die Backup-Verbindung erneut aufzubauen.

Advert.-Intervall

Das Advertisement-Intervall gibt an, nach welcher Zeit ein virtueller Router neu propagiert wird. Der Defaultwert beträgt 100 Zentisekunden (1 Sekunde).

Zusätzlich muss bei Version v2 oder v2+v3 das Intervall ein Ganzzahliges von 100 sein, da bei VRRPv2 das Intervall eine ganzzahlige Sekundenzahl darstellen muss. Wird die Version nachträglich geändert, dann wird das Advert.-Intervall automatisch auf einen gültigen Wert angepasst und sollte überprüft werden.

Mit einer Propagationszeit von 1 Sekunde erzielen die Router im VRRP-Verbund einen sehr schnellen Wechsel beim Ausfall eines Gerätes oder eines Interfaces. Eine Unterbrechung in dieser Größenordnung wird von den meisten Anwendungen unbemerkt bleiben, da normalerweise auch die TCP-Verbindung nicht unterbrochen wird. Andere Routingprotokolle benötigen bis zu 5 Minuten oder länger, um den Wechsel auf einen Backup-Router durchzuführen.

Virtuelle IPv4-Adresse

Definiert die virtuelle IPv4-Adresse des virtuellen Routers. Die Adresse muss auf allen Router des VRRP-Verbunds identisch sein.

Verwenden Sie als virtuelle IP-Adressen ausschließlich IP-Adressen, die nicht dynamisch an Endgeräte vergeben werden, die kein VRRP sprechen, um Konflikte zu vermeiden.

Wenn die vergebene Virtuelle-IPv4 der physikalischen Adresse des Geräts auf dem LAN-Interface entsprechen, werden die konfigurierten Prioritäten und Backup-Prioritäten ignoriert und stattdessen gemäß RFC immer die Priorität 255 verwendet.

Eine unspezifizierte IPv4-Adresse (0.0.0.0) deaktiviert für diesen Konfigurationseintrag IPv4.

Virtuelle Link Lokale IPv6-Adresse

Definiert die virtuelle Link-lokale IPv6-Adresse des virtuellen Routers, z. B. fe80::1. Die Adresse muss auf allen Router des VRRP-Verbunds identisch sein. Diese Adresse wird für als Absendeadresse für das Versenden der Router Advertisements verwendet. Der Parameter wird nur im VRRPv3-Modus unterstützt.

Die Vergabe einer virtuellen link lokalen Adresse ist zwingend notwendig, um einen virtuellen Router für IPv6 zu definieren.

Wenn die vergebene virtuelle Link-lokale IPv6-Adresse der physikalischen Adresse des Geräts auf dem LAN-Interface entsprechen, werden die konfigurierten Prioritäten und Backup-Prioritäten ignoriert und stattdessen gemäß RFC immer die Priorität 255 verwendet.

Eine unspezifizierte IPv6-Adresse (::) deaktiviert für diesen Konfigurationseintrag IPv6.

Virtuelle Globale IPv6-Adresse

Definiert die optionale globale IPv6-Adresse des virtuellen Routers, z. B. 2001:db8::1. Die Adresse muss auf allen Router des VRRP-Verbunds identisch sein. Der Parameter wird nur im VRRPv3-Modus unterstützt.

Für den VPN-Loadbalancer ist diese Adresse notwendig, wenn dieser mit IPv6 arbeiten soll.

Überwachte Gegenstelle

Name der Gegenstelle, die das Verhalten des virtuellen Routers steuert. Die Gegenstelle kann auch weiteren virtuellen Routern zugeordnet werden.

Die Angabe der Gegenstelle ist optional. Mit der Bindung der Backup-Bedingung an eine Gegenstelle wird die LANCOM spezifische Erweiterung von VRRP genutzt, nicht nur den Ausfall eines Gerätes (VRRP-Standard), sondern zusätzlich auch die Störung eines Interfaces oder einer Gegenstelle abzusichern.

Kommentar

Vergeben Sie einen Kommentar für diesen Eintrag.

Reconnect-Verzögerung

Hier geben Sie an, nach wie vielen Minuten ein abgemeldeter virtueller Router versucht, seine Hauptverbindung wieder aufzubauen. Bei diesem Aufbauversuch bleibt der Router abgemeldet. Erst wenn die Verbindung erfolgreich aufgebaut werden konnte, meldet er sich wieder mit seiner Haupt- oder Backup-Priorität an. Der Defaultwert beträgt 30 Minuten. Eingabe erfolgt als <Minuten>:<Sekunden>

Master-Holddown-Zeit

Wenn hier eine Zeit konfiguriert ist, wechselt der virtuelle Router in den Zustand „Hold-Down“, sobald die überwachte WAN-Verbindung mit einem Fehler abgebaut wird und das Backup-Delay abläuft (also in den Backupzustand wechselt). Im Zustand „Hold-Down“ kann die überwachte WAN-Verbindung nicht mehr aufgebaut werden. Des Weiteren werden keine VRRP-Advertisements mehr geschickt.

Sobald die „Master-Holddown-Zeit“ abläuft, wechselt der virtuelle Router in den Zustand „Standby“, in dem die überwachte WAN-Verbindung wiederaufgebaut werden kann.

Die „Master-Holddown-Time“ ist ein String von maximal 6 Zeichen, der die Ziffern 0-9 und den Doppelpunkt enthalten kann. Damit können Zeiten von maximal 999 Minuten 59 Sekunden (999:59) eingegeben werden.

Ist kein Doppelpunkt vorhanden (z. B. „30“) dann wird die Angabe als Minuten interpretiert. Hier ist dennoch maximal „999“ möglich.

Ist ein Doppelpunkt vorhanden, müssen nach dem Doppelpunkt zwei Zeichen kommen, die als Sekunden interpretiert werden. Hier sind maximal „59“ möglich.

Korrekte Zeitangaben sind also z. B. „5“ (5 Minuten), „5:30“ (5 Minuten, 30 Sekunden) oder „0:30“ (30 Sekunden).

Ein Wert von „0“ oder „0:00“ deaktiviert den Master-Holddown.

WAN-Verbindungskontrolle

Definiert, ob VRRP den Verbindungsaufbau der überwachten WAN-Gegenstelle in der Standby-Rolle unterdrücken soll. Mögliche Werte:

Aktiviert

In der Rolle Standby wird der Aufbau der überwachten WAN-Gegenstelle nicht unterdrückt und die WAN-Verbindung wird aufgebaut. Desweiteren werden in diesem Fall auch die Routen zum überwachten WAN nicht umgeschaltet, wenn der virtuelle Router in den Standby wechselt.

Pakete, die an die physikalische MAC-Adresse des Routers geschickt werden, werden im Standby-Zustand nicht zum Master weitergeleitet.

Deaktiviert

In der Rolle Standby wird der Aufbau der überwachten WAN-Gegenstelle unterdrückt.

LAN-Link-Erkennung

Definiert, ob im Falle, dass keine LAN-Verbindung besteht, der Aufbau der WAN-Verbindung nicht unterdrückt werden soll.

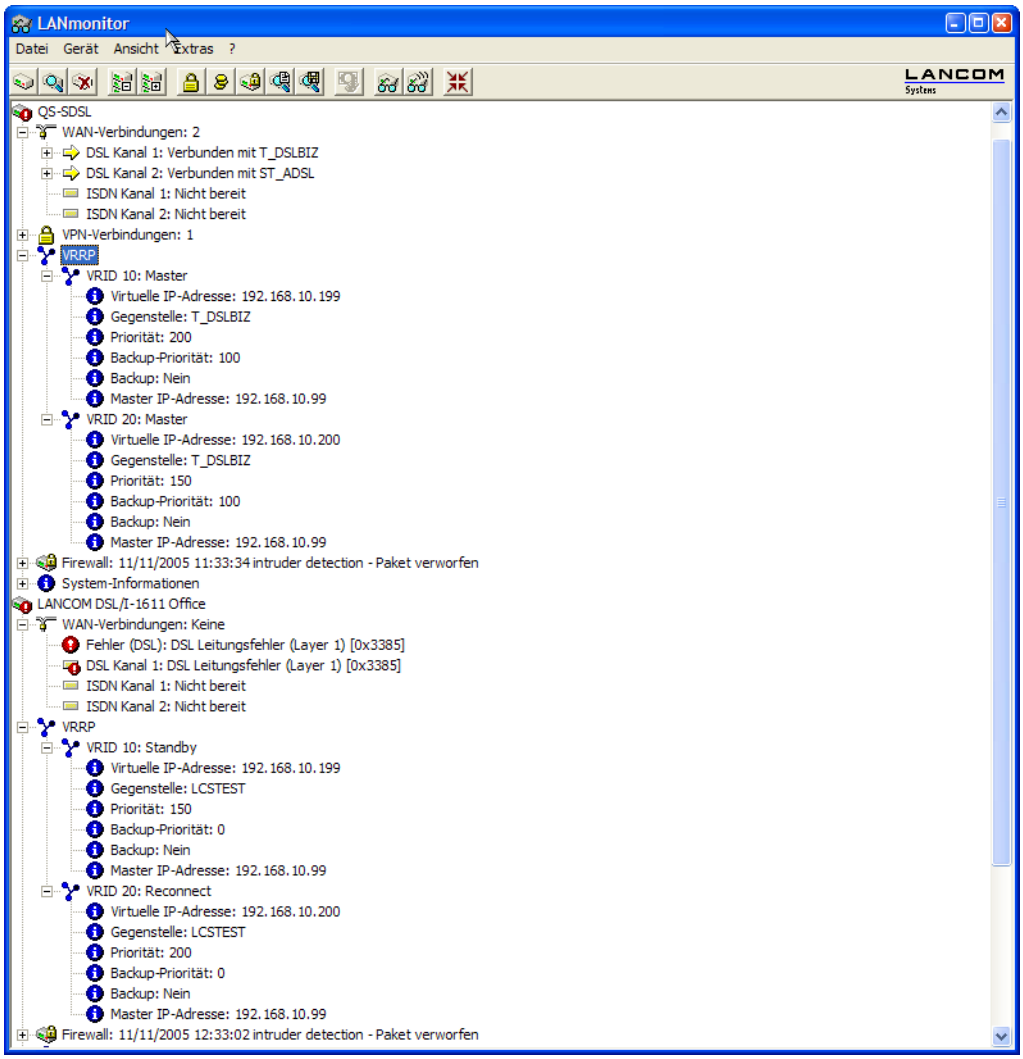
Die Funktion ist für ein Szenario relevant, wo der Router noch ohne LAN-Verbindung in Betrieb ist, aber eine Verwaltung des Routers über die WAN-Verbindung möglich sein soll. In diesem Szenario muss die LAN-Link-Erkennung deaktiviert werden.

Interne Dienste unter der virtuellen IP anbieten

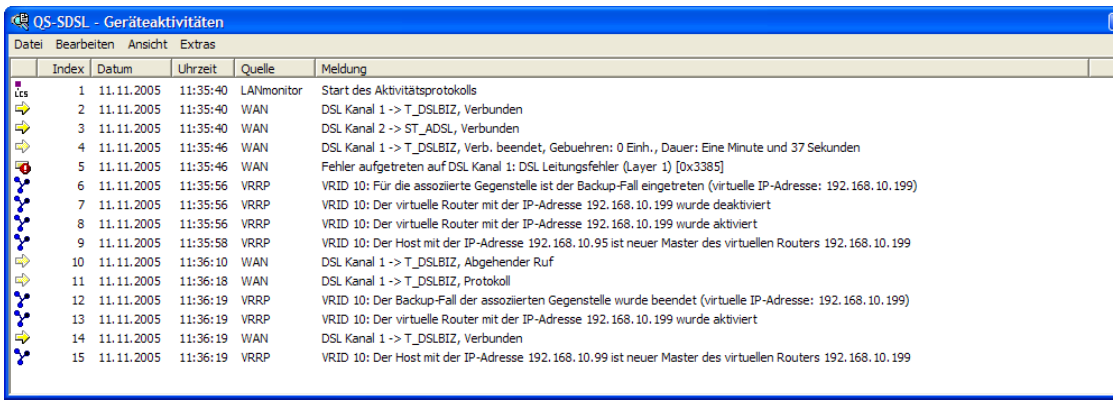
Dieser Schalter steuert, ob der virtuelle Router im DHCPv4, DHCPv6 und Router-Advertisement als DNS-Server zugewiesen wird.

17.2.9 Statusinformationen

Der aktuelle Status der Geräte im VRRP-Verbund wird im LANmonitor angezeigt, sofern das VRRP-Modul aktiviert ist:



Im Geräteaktivitätslog können die VRRP-Ereignisse im zeitlichen Verlauf betrachtet werden.



Die Statusinformationen zu VRRP befinden sich im Status-Menü des IP-Routers und bieten folgende Einträge an:

- Die Werte Rx und Tx zählen die empfangenen bzw. gesendeten VRRP-Pakete.

- Error zählt alle schweren Protokoll-Fehler, die mitgeloggt werden.
- Drop zählt alle VRRP-Pakete, die verworfen wurden, z. B. weil ein schwerwiegender Fehler auftrat.

In der Tabelle Virtual-Router sind alle aktiven virtuellen Router mit ihrem jeweiligen Zustand aufgelistet. Diese Tabelle hat die folgenden Felder:

- **Router-ID**: Eindeutige ID des virtuellen Routers.
- **virt.-Address**: IP-Adresse des virtuellen Routers.
- **Prio**: Haupt-Priorität des virtuellen Routers.
- **B-Prio**: Backup-Priorität des virtuellen Routers.
- **Peer**: Name der Gegenstelle, die das Verhalten des virtuellen Routers steuert.
- **State**: Zustand des virtuellen Routers. Es sind folgende Zustände Möglich:
  - Init: Der Router wird gerade angelegt.
  - Listen: Der Router lernt gerade zum ersten, wer der Master ist.
  - Standby: Der Router ist Standby-Router.
  - Master: Der Router ist der Master.
  - Down: Der Router ist deaktiviert.
  - Reconnect: Der Reconnect-Timer läuft und der Router propagiert sich gerade nicht
- **Backup**: Zeigt an, ob sich die Gegenstelle (Peer) im Backup-Fall befindet oder nicht. Wenn sich die Gegenstelle im Backup-Fall befindet, propagiert das Gerät seine Backup-Priorität, ansonsten seine Haupt-Priorität.
- **Master**: Zeigt an, welcher physikalische Router gerade der Master ist.

In der Tabelle MAC-List befinden sich die MAC-Adressen der virtuellen Router, die gerade Master sind. Diese Tabelle hat die folgenden Felder:

- **virt.-Address**: IP-Adresse des virtuellen Routers.
- **MAC-Address**: MAC-Adresse des virtuellen Routers.
- **Router-ID**: eindeutige ID des virtuellen Routers.

17.3 Schnittstellen-Bündelung mit LACP

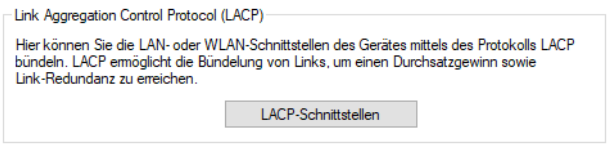
Einen enormen Mehrwert in puncto Ausfallsicherheit und Performance bietet Ihnen der unterstützte Standard LACP (Link Aggregation Control Protocol). LACP ermöglicht Ihnen die Bündelung von GB-Ports zu einem virtuellen Link. Physikalische GB-Verbindungen lassen sich zu einer logischen Verbindung zusammenfassen, sodass die Geschwindigkeit der Datenübertragung stark erhöht und die verfügbare Bandbreite optimal ausgenutzt wird.

Ein Datendurchsatz von über 1 GBit/s netto pro Access Point wird z. B. mit 11ac Wave 2 (4x4 MIMO) erreicht.

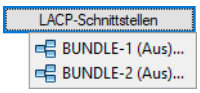
Neben einem echten Performance-Gewinn im Netzwerk dient LACP zugleich als ideale Redundanzoption, denn sobald eine physikalische Verbindung ausfällt, wird der Datenverkehr auf der anderen Leitung weiterhin übertragen.

17.3.1 Konfiguration der LACP-Schnittstellen

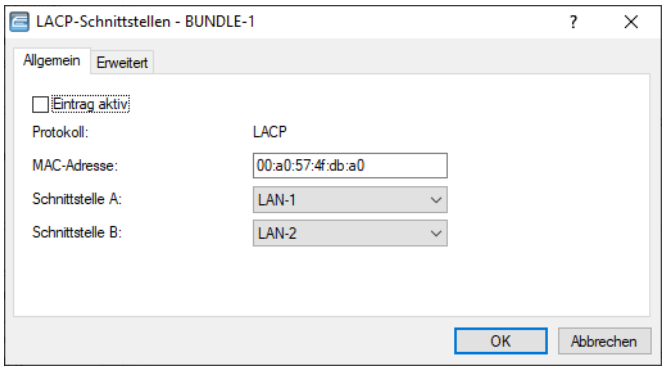
In LANconfig konfigurieren Sie LACP-Schnittstellen unter **Schnittstellen** > **LAN** im Abschnitt **Link Aggregation Control Protocol**.



1. Klicken Sie die Schaltfläche **LACP-Schnittstellen**, um auf die Liste der verfügbaren Bündel zuzugreifen.



2. Wählen Sie ein Bündel aus.



3. Tragen Sie die MAC-Adresse des Gerätes in das Eingabefeld **MAC-Adresse** ein.

Die MAC-Adresse wird benutzt, um den LACP-Partner innerhalb der LAG zu identifizieren. Bleibt sie leer bzw. 0, wird automatisch die LAN-MAC-Adresse des Gerätes gesetzt. Die MAC-Adresse muss nicht zwingend zu einer Schnittstelle des Bündels gehören. Bei einem Reset der Konfiguration wird automatisch die systemweite MAC-Adresse dort als Default eingetragen.

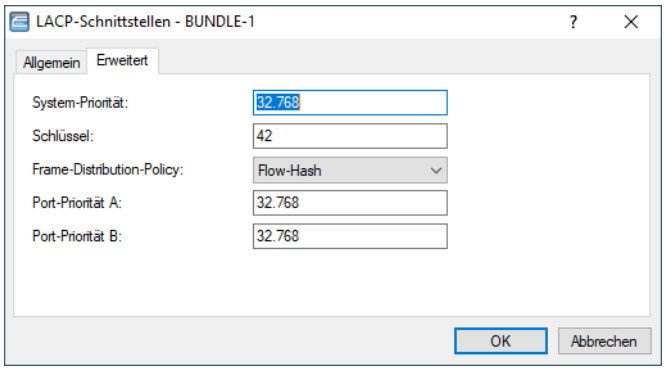
4. Wählen Sie die erste Schnittstelle aus dem Auswahlmenü **Schnittstelle A** aus.
5. Wählen Sie die zweite Schnittstelle aus dem Auswahlmenü **Schnittstelle B** aus.
6. Aktivieren Sie das Bündel durch Setzen des Häkchens in der Checkbox **Eintrag aktiv**.

Die weiteren Schritte sind optional.

Die Standard-Einstellungen wurden angepasst an die meisten Anwendungen.

Bitte führen Sie eine individuelle Konfiguration nur als erfahrener Netzwerk-Techniker durch.

7. Navigieren Sie in die erweiterten Konfigurationsmöglichkeiten per Klick auf **Erweitert**.



8. Tragen Sie in das Eingabefeld **System-Priorität** ein Vielfaches von 4.096 ein. Der Standardwert lautet 32.768.
9. Machen Sie eine Eintragung in der Eingabezeile **Schlüssel**.

Der Schlüssel ist eine Zahl von 1 bis 54 und dient als Kennzeichnung des Bündels.

10. Wählen Sie eine Frame-Verteilungs-Regel in dem Auswahlmenü **Frame-Distribution-Policy**. Die für die meisten Szenarien empfohlene Default-Einstellung ist Flow-Hash.
11. Tragen Sie in das Eingabefeld **Port-Priorität A** ein Vielfaches von 4.096 ein. Der Standardwert lautet 32.768.

12. Tragen Sie in das Eingabefeld **Port-Priorität B** ein Vielfaches von 4.096 ein. Der Standardwert lautet 32.768.

17.4 Unterstützung von vRouter-Redundanz in Amazon AWS

Cloud-Anbieter zur Auslagerung von virtuellen Maschinen in die Cloud wie Amazon AWS unterstützen keine Layer 2-Protokolle wie z. B. VRRP. Damit sind gängige Router-Redundanz-Konzepte nicht ohne weiteres möglich und müssen anders realisiert werden. Amazon AWS bietet stattdessen dazu eine API an, mit der Routen-Einträge im Failover-Fall auf einen sekundären Router umgeschaltet werden können.

Das Szenario ist wie folgt aufgebaut: Es existieren eine oder mehrere private virtuelle Maschinen (EC2-Instanzen). Zwei redundante vRouter haben ein privates Subnetz zu den virtuellen Maschinen und ein öffentliches Subnetz zum Internet. Beide vRouter besitzen je einen VPN-Tunnel zum Kundenstandort und ermöglichen so den Zugriff auf die privaten Maschinen. Ein vRouter ist primärer Router (aktiv), der zweite Router ist sekundär (passiv) und nur im Failover-Fall am aktiven Routing beteiligt. Eine EC2-Instanz kann immer nur einen Router als nächsten Hop im privaten Subnetz besitzen, der im Failover-Fall vom primären auf den sekundären vRouter per AWS-API in der AWS-Routingtabelle umgeschaltet wird. Ist der primäre vRouter wieder verfügbar, so wird wieder auf den primären Router zurückgeschaltet.

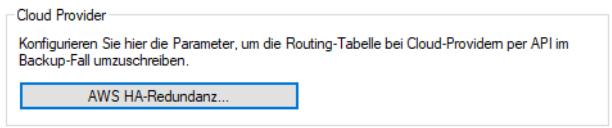
Die vRouter benötigen für den Zugriff auf die AWS-API eine AWS Identity and Access Management (IAM)-Rolle.

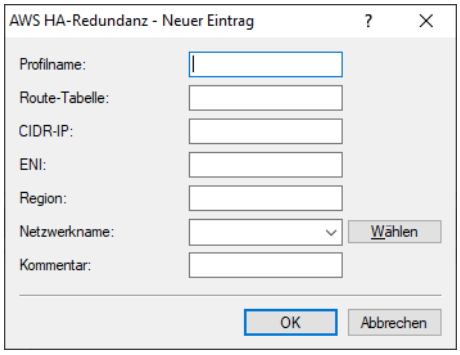
Um den Ausfall des primären Routers zu erkennen, wird ein VPN-Tunnel zwischen beiden vRoutern aufgebaut. Durch die Aktionstabelle im sekundären vRouter werden AWS-API-Kommandos gesendet, wenn erkannt wird, dass der VPN-Tunnel zum primären vRouter abgebaut wird bzw. aufgebaut wird. Der VPN-Tunnel dient nur zum Erkennen der Verfügbarkeit des primären Routers. Daten werden über diesen VPN-Tunnel nicht übertragen.

Für den Zugriff auf die AWS-API benötigt der vRouter Zugang zum Internet.

17.4.1 Konfiguration

Konfigurieren Sie die vRouter-Redundanz für AWS in LANconfig unter **Sonstige Dienste** > **Dienste** > **Cloud Provider** > **AWS HA-Redundanz**oder auf der Kommandozeile unter **/Setup/Cloud-Provider/AWS/** in der Tabelle **HA-Redundancy**.





Profilname

Eindeutiger Name des Profils. Über diesen Namen wird das Profil im Kommando zur Änderung der Route referenziert.

Route-Tabelle

Name der Routing-Tabelle die in AWS geändert werden soll, z. B. „rtb-099605ce6cb4ac319“. Diesen Wert erhalten Sie aus der AWS-Management-Oberfläche.

CIDR IP

Präfix in der Routing-Tabelle, für das der Next-Hop geändert werden soll, z. B. „0.0.0.0/0“.

ENI

Name des AWS-Netzwerkadapters (Elastic Network Interface) der als Next-Hop durch das Kommando gesetzt werden soll, z. B. „eni-00c734d6da1fd8968“. Diesen Wert erhalten Sie aus der AWS-Management-Oberfläche.

Region

Region, in der sich die AWS Routing-Tabelle befindet, z. B. „eu-central-1“

Netzwerkname

Name des Interfaces bzw. der Gegenstelle im vRouter über die der vRouter die AWS-API erreichen kann, z. B. „INTERNET“.

Kommentar

Vergeben Sie einen aussagekräftigen Kommentar für diesen Eintrag.

17.4.2 Kommandos

Unter **/Setup/Cloud-Provider/AWS** stehen zwei Kommandos zur Verfügung:

- Switch-Route

  ```
  do /Setup/Cloud-Provider/AWS/Switch-Route <Profile-Name>
  ```

  Dieses Kommando schaltet per AWS-API das Präfix in der AWS-Routingtabelle auf den neuen Next-Hop um, der unter <Profilname> in der Tabelle `/Setup/Cloud-Provider/AWS/` konfiguriert ist.

- Get-Remote-Route-Table

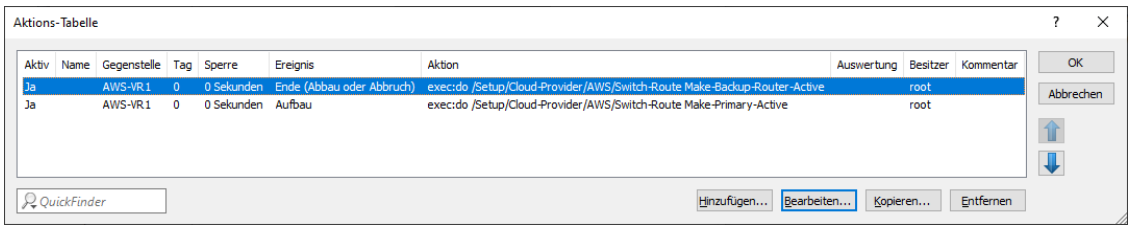
  ```
  do /Setup/Cloud-Provider/AWS/Get-Remote-Route-Table <route-table-id>
     <region> <outgoing-network>
  ```

  Dieses Kommando liefert den aktuellen Status der AWS-Routingtabelle <route-table-id> per AWS API. Beispiel:

  ```
  do Get-Remote-Route-Table rtb-099605ce6cb4ac319 eu-central-1 INTERNET
  ```

Beispiel: Verwendung der Kommandos in der Aktionstabelle

Der Backup-vRouter hat folgende Einträge in der Aktionstabelle (**Kommunikation** > **Allgemein** > **Aktions-Tabelle**) konfiguriert:



Es existieren zwei Profile in der HA-Redundanz-Tabelle, die in der Aktionstabelle im Kommando Switch-Route referenziert werden. Der erste Eintrag bewirkt, dass beim Abbau oder Abbruch des VPN-Tunnels (Gegenstelle AWS-VR1) zum primären Router der Backup-vRouter sich selbst zum aktiven Router in der AWS-Routing-Tabelle macht. Wird der VPN-Tunnel wieder aufgebaut, d. h. der primäre Router ist wieder verfügbar, so wird der primäre Router in der Routing-Tabelle wieder als Next-Hop gesetzt.

17.4.3 IAM-Rolle konfigurieren in AWS

Rufen Sie in AWS das IAM-Dashboard auf und klicken Sie auf **Rollen** > **Rolle erstellen**.

Die folgenden Berechtigungen in der IAM-Rolle für den sekundären vRouter sind notwendig:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AssociateRouteTable",
                "ec2:CreateRoute",
                "ec2:CreateRouteTable",
                "ec2:DeleteRoute",
                "ec2:DeleteRouteTable",
                "ec2:DescribeRouteTables",
                "ec2:DescribeVpcs",
                "ec2:ReplaceRoute",
                "ec2:DisassociateRouteTable",
                "ec2:ReplaceRouteTableAssociation"
            ],
            "Resource": "*"
        }
    ]
}
```

Legen Sie eine neue Richtlinie an und weisen Sie die Richtlinien dem sekundären vRouter zu, so dass dieser über die korrekten Berechtigungen für den Aufruf der API verfügt.

18 RADIUS

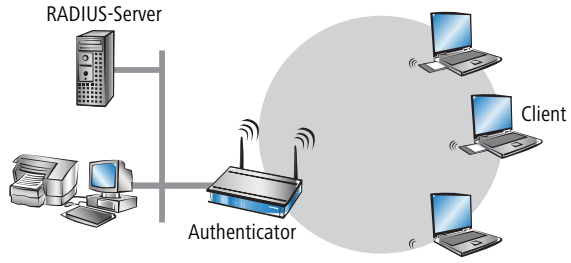
RADIUS steht für „Remote Authentication Dial-In User Service“ und wird als „Triple-A-Protokoll“ bezeichnet. Dabei stehen die drei „A“ für

- Authentication (Authentifizierung)
- Authorization (Autorisierung)
- Accounting (Abrechnung)

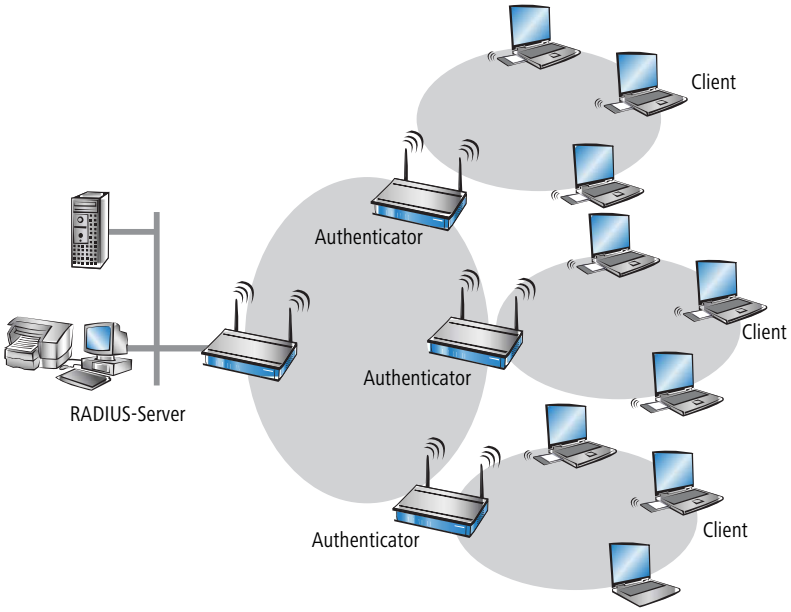
Sie können mit diesem Protokoll Benutzern Zugang zu einem Netz gewähren, ihnen bestimmte Rechte zuweisen und ihre Aktionen verfolgen. Gegebenenfalls können Sie auch die in Anspruch genommenen Leistungen gegenüber dem Benutzer mit Hilfe des RADIUS-Servers abrechnen (z. B. bei WLAN Hotspots). Für jede Aktion, die vom Benutzer durchgeführt wird, kann der RADIUS-Server eine Autorisierung durchführen, und so den Zugriff auf Netzwerkressourcen je nach Benutzer freigeben oder sperren.

Damit RADIUS funktioniert, sind 3 verschiedene Geräte nötig.

- Client: Das ist ein Gerät (PC, Notebook etc.) über das der Benutzer sich in das Netz einwählen möchte.
- Authenticator: Eine Netzwerkkomponente, welche die Authentifizierung weiterleitet und zwischen dem Netz und dem Client liegt. Diese Aufgabe kann z. B. ein Access Point übernehmen. Der Authenticator wird auch als Network Access Server (NAS) bezeichnet.



- Authentication-Server: RADIUS-Server, auf dem die Daten für die Benutzer konfiguriert sind. Dieser steht gewöhnlich in dem Netz, für das er Zugangsberechtigungen erteilen soll. Er ist für den Client über den Authenticator erreichbar. Auch für diese Aufgabe kann in entsprechenden Szenarien ein Access Point eingesetzt werden.



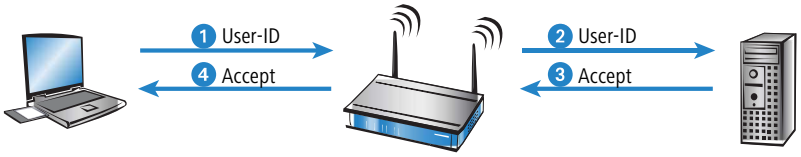
Der Authenticator hat zunächst keine Informationen über die Clients, die sich anmelden wollen. Diese sind alle in einer Datenbank des RADIUS-Servers gespeichert. Welche Anmeldeinformationen der RADIUS-Server für die Authentifizierung benötigt, ist dort in der Datenbank hinterlegt und kann von Netzwerk zu Netzwerk variieren. Der Authenticator hat nur die Aufgabe, die Informationen zwischen dem Client und dem RADIUS-Server zu übertragen.

Der Zugang zu einem RADIUS-Server kann über verschiedene Wege aufgebaut werden:

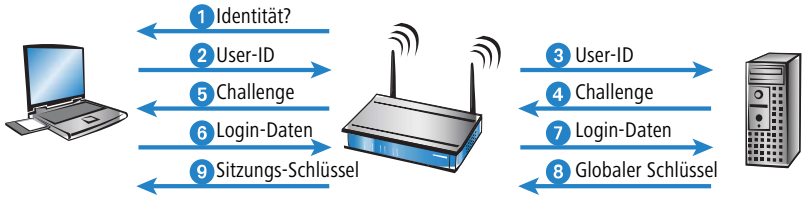
- Über PPP bei der Einwahl in ein Netzwerk
- Über WLAN
- Über einen Public Spot für Benutzer, die sich per Browser anmelden
- über das 802.1X-Protokoll

18.1 Funktionsweise von RADIUS

Die Authentifizierung eines Clients mit Hilfe eines Authenticators an einem RADIUS-Server kann je nach Implementation unterschiedlich detailliert ablaufen. In einem einfachen Anwendungsfall schickt der Client seine Anmeldedaten über den Authenticator an den RADIUS-Server und erhält von dort eine Bestätigung („Accept“) oder eine ablehnende Fehlernachricht („Reject“).



In erweiterten Anwendungen kann der RADIUS-Server mit Hilfe einer so genannten „Challenge“ weitere Anmeldeinformationen anfordern, die Verhandlungsphase sieht dann z. B. so aus:



18.2 Über RADIUS in die LCOS-Verwaltungsoberfläche einloggen

Aktuell existieren drei Methoden, sich in die Verwaltungsoberfläche des Geräts einzuloggen:

- intern: Das Gerät übernimmt die komplette Benutzerverwaltung mit Anmeldename, Passwort sowie Zugriffs- und Funktionsrechte-Zuordnung.
- TACACS+: Die Benutzerverwaltung erfolgt über einen TACACS+-Server im Netzwerk.
- RADIUS: Die Benutzerverwaltung erfolgt über einen RADIUS-Server im Netzwerk.

Mit RADIUS kann sich der Benutzer über die folgenden Verbindungen einloggen:

- Telnet
- SSH
- WEBconfig
- TFTP
- Outband

Eine RADIUS-Authentifizierung über SNMP ist derzeit nicht unterstützt.

Eine RADIUS-Authentifizierung über LL2M (LANCOM Layer 2 Management Protokoll) ist nicht unterstützt, da LL2M Klartext-Zugriff auf das im Gerät gespeicherte Passwort benötigt.

Der RADIUS-Server übernimmt die Verwaltung der Benutzer in den Bereichen Authentifizierung, Authorisierung und Accounting (Triple-A-Protokoll), was bei umfangreichen Netzwerk-Installationen mit mehreren Routern die Verwaltung von Admin-Zugängen stark vereinfacht.

Die Anmeldung über einen RADIUS-Server läuft wie folgt ab:

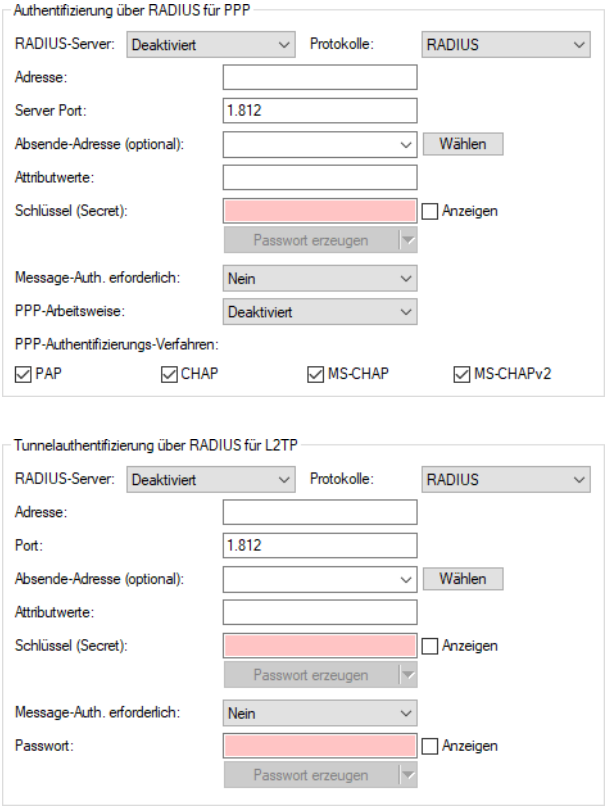
1. Bei der Anmeldung sendet das Gerät die eingegebenen Anmeldedaten des Benutzers an den RADIUS-Server im Netz. Die Server-Daten sind dazu im Gerät gespeichert.
2. Der Server prüft die Anmeldedaten auf Gültigkeit.
3. Bei ungültigen Daten sendet er dem Gerät eine entsprechende Nachricht, und das Gerät bricht den Anmeldevorgang mit einer Fehlernachricht ab.
4. Bei gültigen Anmeldedaten sendet der Server dem Gerät mit der Zugangserlaubnis auch die Zugriffs- und Funktionsrechte, so dass der Anwender nur auf die entsprechend freigeschalteten Funktionen und Verzeichnisse zugreifen kann.
5. Falls die Sitzungen des Anwenders durch den RADIUS-Server budgetiert sind (Bereich Accounting), speichert das Gerät die Sitzungsdaten wie Start, Ende, Benutzername, Authentifizierungsmodus und, wenn vorhanden, den genutzen Port.

18.3 RADIUS als Authenticator bzw. Network Access Server (NAS)

Das RADIUS-Protokoll wird von den Geräten in unterschiedlichen Anwendungsfällen unterstützt. Für jeden dieser Fälle gibt es einen eigenen Satz von Parametern, der unabhängig von den anderen Anwendungen konfiguriert werden kann. Zusätzlich gibt es allgemeine Parameter, die für jede dieser Anwendungen konfiguriert werden müssen. Nicht alle Geräte unterstützen jede Anwendung.

18.3.1 Allgemeine Einstellungen

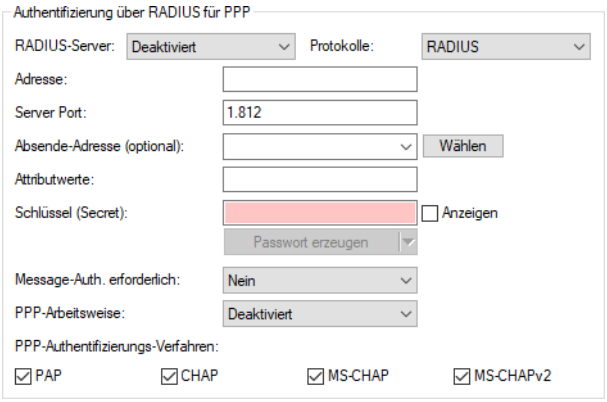
Die allgemeinen Einstellungen unter **Kommunikation** > **RADIUS** gelten für alle RADIUS-Anwendungen. Die Default-Werte sind so gewählt, dass sie im Normalfall nicht geändert werden müssen.



Die Angabe einer RADIUS-Serveradresse ist als IPv4- oder IPv6-Adresse sowie alternativ als DNS-Name möglich.

18.3.2 Einwahl über PPP und RADIUS

Bei der Einwahl über das PPP-Protokoll (Point-to-Point-Protocol) kann die Zugangsberechtigung der Clients mittels RADIUS geprüft werden. Ein Client kann sich dabei von einem beliebigen Ort in das Netz einwählen. Die anschließende Datenübertragung zwischen dem Client und dem Authenticator wird verschlüsselt



Die Konfiguration erfolgt im LANconfig unter **Kommunikation** > **RADIUS**.

Radius-Server

Bei der Authentifizierung via RADIUS wird die Benutzerverwaltung und Authentifizierung von einem RADIUS-Server übernommen.

- Deaktiviert: Die RADIUS-Funktion ist ausgeschaltet, es werden keine Anfragen an den RADIUS-Server weitergeleitet (Default).
- Aktiviert: Die RADIUS-Funktion ist eingeschaltet, es können Anfragen an den konfigurierten RADIUS-Server weitergeleitet werden. Je nach Einstellung können auch andere Quelle für die Authentifizierung verwendet werden (z. B. PPP-Liste).
- Exklusiv: Die RADIUS-Funktion ist eingeschaltet, die Authentifizierung wird ausschließlich über RADIUS durchgeführt.

Für die Nutzung der RADIUS-Funktion muss der entsprechende RADIUS-Server konfiguriert sein. Alle Benutzerangaben wie Benutzername und Passwort werden im RADIUS-Server eingetragen.

Protokolle

Als Protokolle kann zwischen dem UDP-basierten RADIUS und dem TCP-basierte RADSEC ausgewählt werden. Siehe auch *RADSEC* auf Seite 1609.

Adresse

Geben Sie hier die IP-Adresse (IPv4, IPv6) oder den Host-Namen des RADIUS-Servers an, mit dem Sie zentral die Benutzer verwalten.

Server Port

Geben Sie hier den Port an, über den Sie mit Ihrem RADIUS-Server kommunizieren (Default: 1.812).

Absende-Adresse

Das Gerät ermittelt automatisch die richtige Absende-IP-Adresse für das Zielnetzwerk. Wollen Sie stattdessen eine fest definierte Absende-IP-Adresse verwenden, tragen Sie diese symbolisch oder direkt hier ein.

Attributwerte

LCOS ermöglicht es, die RADIUS-Attribute für die Kommunikation mit einem RADIUS-Server (sowohl Authentication als auch Accounting) zu konfigurieren.

Die Angabe der Attribute erfolgt als semikolon-separierte Liste von Attribut-Nummern oder -Namen und einem entsprechenden Wert in der folgenden Form:

`<Attribut_1>=<Wert_1>;<Attribut_2>=<Wert_2>`

Da die Anzahl der Zeichen begrenzt ist, lässt sich der Name abkürzen. Das Kürzel muss dabei eindeutig sein. Beispiele:

- `NAS-Port=1234` ist nicht erlaubt, da das Attribut nicht eindeutig ist (`NAS-Port`, `NAS-Port-Id` oder `NAS-Port-Type`).
- `NAS-Id=ABCD` ist erlaubt, da das Attribut eindeutig ist (`NAS-Identifier`).

Als Attribut-Wert ist die Angabe von Namen oder RFC-konformen Nummern möglich. Für das Gerät sind die Angaben `Service-Type=Framed` und `Service-Type=2` identisch.

Die Angabe eines Wertes in Anführungszeichen (`"<Wert>"`) ist möglich, um Sonderzeichen wie Leerzeichen, Semikolon oder Gleichheitszeichen mit angeben zu können. Das Anführungszeichen innerhalb des Wertes erhält einen umgekehrten Schrägstrich vorangestellt (`\"`), der umgekehrte Schrägstrich ebenfalls (`\\`).

Als Werte sind auch die folgenden Variablen erlaubt:

`%n`

Gerätename

`%e`

Seriennummer des Gerätes

`%%`

Prozentzeichen

`%{name}`

Original-Name des Attributes, wie ihn die RADIUS-Anwendung überträgt. Damit lassen sich z. B. Attribute mit originalen RADIUS-Attributen belegen: `Called-Station-Id=%{NAS-Identifier}` setzt das Attribut `Called-Station-Id` auf den Wert, den das Attribut `NAS-Identifier` besitzt.

Schlüssel (Shared-Secret)

Geben Sie hier den Schlüssel an, mit dem die Kodierung der Daten vorgenommen werden soll. Der Schlüssel muss ebenfalls im RADIUS-Server konfiguriert sein.

Message-Authenticator erforderlich

Definiert, ob das Vorhandensein des Message-Authenticator-Attributs in RADIUS-Nachrichten auf Client-Seite erforderlich ist. Die Client-Seite ist die Seite, die den RADIUS-Accept/Fail empfängt.

PPP-Arbeitsweise

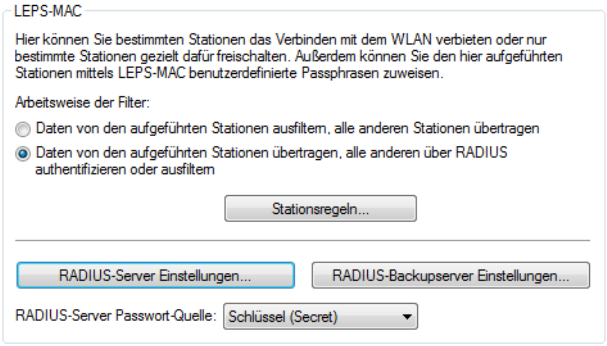
Bei der Einwahl über PPP kann ein RADIUS-Server zur Authentifizierung genutzt werden.

- Deaktiviert: PPP-Clients werden nicht über RADIUS authentifiziert, sie werden **ausschließlich** anhand der PPP-Liste geprüft (Default).
- Aktiviert: Die RADIUS-Authentifizierung für PPP-Clients ist eingeschaltet. Die von den Clients gelieferten Benutzerdaten werden **zuerst** über die PPP-Liste geprüft. Ist in der PPP-Liste kein passender Eintrag vorhanden, dann wird der Client über den RADIUS-Server geprüft. Verläuft die Prüfung in PPP-Liste **oder** RADIUS-Server positiv, ist die Authentifizierung erfolgreich.
- Exklusiv: Die RADIUS-Authentifizierung für PPP-Clients ist eingeschaltet. Die von den Clients gelieferten Benutzerdaten werden **ausschließlich** über den RADIUS-Server geprüft. In dieser Einstellung werden

lediglich die erweiterten Einstellungen der PPP-Liste für den Benutzer ausgewertet (z. B. Prüfung nach PAP/CHAP bzw. erlaubte Protokolle wie IP).

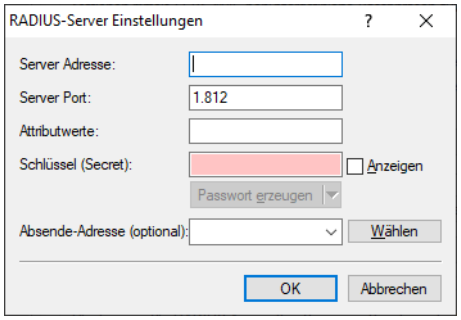
18.3.3 Einwahl über WLAN und RADIUS

Bei der Verwendung eines RADIUS-Servers zur Authentifizierung von WLAN-Clients prüft der RADIUS-Server die Berechtigungen der Clients über die MAC-Adresse.



Zur Nutzung der RADIUS-Funktion für WLAN-Clients muss im Bereich **LEPS-MAC** die Option **Daten von den aufgeführten Stationen übertragen, alle anderen über RADIUS authentifizieren oder ausfiltern** ausgewählt sein.

Die Konfiguration erfolgt im LANconfig unter **Wireless-LAN** > **Stationen/LEPS**. Dort wird unter **RADIUS-Server Einstellungen** definiert, wie der RADIUS-Server erreicht werden kann. Unter **RADIUS-Backupserver Einstellungen** erfolgt analog die Konfiguration eines entsprechenden Backup-Servers.



Server Adresse

Geben Sie hier die IP-Adresse (IPv4, IPv6) oder den Host-Namen des RADIUS-Servers an, mit dem Sie zentral die Benutzer verwalten.

Server Port

Geben Sie hier den Port an, über den Sie mit Ihrem RADIUS-Server kommunizieren (Default: 1.812).

Attributwerte

LCOS ermöglicht es, die RADIUS-Attribute für die Kommunikation mit einem RADIUS-Server (sowohl Authentication als auch Accounting) zu konfigurieren.

Die Angabe der Attribute erfolgt als semikolon-separierte Liste von Attribut-Nummern oder -Namen und einem entsprechenden Wert in der folgenden Form:

```
<Attribut_1>=<Wert_1>;<Attribut_2>=<Wert_2>
```

Da die Anzahl der Zeichen begrenzt ist, lässt sich der Name abkürzen. Das Kürzel muss dabei eindeutig sein. Beispiele:

- `NAS-Port=1234` ist nicht erlaubt, da das Attribut nicht eindeutig ist (`NAS-Port`, `NAS-Port-Id` oder `NAS-Port-Type`).
- `NAS-Id=ABCD` ist erlaubt, da das Attribut eindeutig ist (`NAS-Identifier`).

Als Attribut-Wert ist die Angabe von Namen oder RFC-konformen Nummern möglich. Für das Gerät sind die Angaben `Service-Type=Framed` und `Service-Type=2` identisch.

Die Angabe eines Wertes in Anführungszeichen (**"**`<Wert>`**"**) ist möglich, um Sonderzeichen wie Leerzeichen, Semikolon oder Gleichheitszeichen mit angeben zu können. Das Anführungszeichen innerhalb des Wertes erhält einen umgekehrten Schrägstrich vorangestellt (`\`**"**), der umgekehrte Schrägstrich ebenfalls (`\\`).

Als Werte sind auch die folgenden Variablen erlaubt:

`%n`

Gerätename

`%e`

Seriennummer des Gerätes

`%%`

Prozentzeichen

`%{name}`

Original-Name des Attributes, wie ihn die RADIUS-Anwendung überträgt. Damit lassen sich z. B. Attribute mit originalen RADIUS-Attributen belegen: `Called-Station-Id=%{NAS-Identifier}` setzt das Attribut `Called-Station-Id` auf den Wert, den das Attribut `NAS-Identifier` besitzt.

Schlüssel (Secret)

Geben Sie hier den Schlüssel an, mit dem die Kodierung der Daten vorgenommen werden soll. Der Schlüssel muss ebenfalls im RADIUS-Server konfiguriert sein.

Backup-Server Adresse

Geben Sie hier die IP-Adresse (IPv4, IPv6) oder den Host-Namen des Backup-RADIUS-Servers an, mit dem Sie zentral die Benutzer verwalten.

Backup-Server Port

Geben Sie hier den Port an, über den Sie mit Ihrem Backup-RADIUS-Server kommunizieren (Default: 1.812).

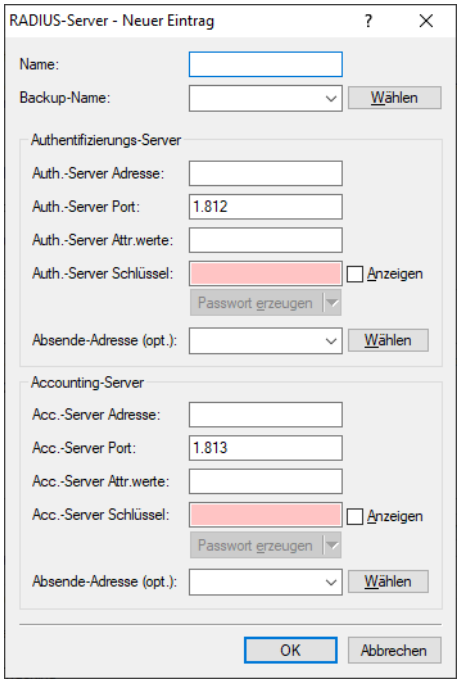
Absende-Adresse

Das Gerät ermittelt automatisch die richtige Absende-IP-Adresse für das Zielnetzwerk. Wollen Sie stattdessen eine fest definierte Absende-IP-Adresse verwenden, tragen Sie diese symbolisch oder direkt hier ein.

18.3.4 Einwahl über einen Public Spot und RADIUS

Bei der Konfiguration eines Public-Spot (Aktivierung über Software-Option für die Access Points, siehe auch *Public Spot* auf Seite 1251) können die Benutzer-Anmeldedaten an einen oder mehrere RADIUS-Server weitergeleitet werden. Diese

werden in der Anbieter-Liste konfiguriert. Welche Anmeldedaten die einzelnen RADIUS-Server von den Clients benötigen, ist für den Access Point nicht wichtig, da diese Daten transparent an den RADIUS-Server weitergereicht werden.



Die Konfiguration erfolgt im LANconfig unter **Public-Spot** > **Benutzer** > **Benutzer und RADIUS-Server** > **RADIUS-Server**.

Name

Name des Anbieters, für den der RADIUS-Server definiert werden soll.

Backup-Name

Als Backup kann der Name eines anderen Anbieters aus der aktuellen Tabelle ausgewählt werden. Durch solche Einträge können komfortabel Backup-Ketten von mehreren RADIUS-Servern konfiguriert werden.

Die allgemeinen Werte für Wiederholung und Timeout müssen ebenfalls konfiguriert werden.

Authentifizierungs-Server

Auth.-Server Adresse

Geben Sie hier die IP-Adresse (IPv4, IPv6) oder den Host-Namen des RADIUS-Servers für diesen Anbieter an.

Auth.-Server Port

Der Port, über den der Access Point mit dem RADIUS-Server für diesen Anbieter kommunizieren kann.

Auth.-Server Attr.werte

Hier können sie RADIUS-Attribute mit benutzerdefinierten Werten versehen. Die einzelnen Namen-Werte-Paare müssen der Form <Name>=<Wert> entsprechen und sind durch Semikola voneinander getrennt.

<Name> identifiziert dabei das RADIUS-Attribut durch seinen Namen oder seine Nummer. Die zugehörigen Attributnamen finden Sie in den entsprechenden RADIUS RFCs. Attributsnamen können abgekürzt werden, solange die Bezeichner eindeutig sind.

Da die Anzahl der Zeichen begrenzt ist, lässt sich der Name abkürzen. Das Kürzel muss dabei eindeutig sein. Beispiele:

- `NAS-Port=1234` ist nicht erlaubt, da das Attribut nicht eindeutig ist (`NAS-Port`, `NAS-Port-Id` oder `NAS-Port-Type`).
- `NAS-Id=ABCD` ist erlaubt, da das Attribut eindeutig ist (`NAS-Identifier`).

Als Attribut-Wert ist die Angabe von Namen oder RFC-konformen Nummern möglich. Für das Gerät sind die Angaben `Service-Type=Framed` und `Service-Type=2` identisch.

Die Angabe eines Wertes in Anführungszeichen (`"<Wert>"`) ist möglich, um Sonderzeichen wie Leerzeichen, Semikolon oder Gleichheitszeichen mit angeben zu können. Das Anführungszeichen innerhalb des Wertes erhält einen umgekehrten Schrägstrich vorangestellt (`\"`), der umgekehrte Schrägstrich ebenfalls (`\\`).

Zusätzlich ist es möglich eine Reihe von Platzhalter einzusetzen:

- `%n` – wird ersetzt durch den konfigurierten Gerätenamen.
- `%e` – wird ersetzt mit der Seriennummer des Gerätes, wie man sie aus dem sysinfo des Gerätes kennt.
- `%%` – wird ersetzt durch ein einzelnes %-Zeichen.
- `%{name}` – wird ersetzt durch den ursprünglichen Wert des entsprechenden RADIUS-Attributes. Etwaige Neu / Um-Definitionen innerhalb dieser Attributsliste werden nicht beachtet! Der Bezeichner kann gekürzt werden, solange er eindeutig bleibt.

Auth. Server Schlüssel

Schlüssel (Shared Secret) für den Zugang zum RADIUS-Server des Anbieters. Der Schlüssel muss ebenfalls im entsprechenden RADIUS-Server konfiguriert sein.

Absende-Adresse

Das Gerät ermittelt automatisch die richtige Absende-IP-Adresse für das Zielnetzwerk. Wollen Sie stattdessen eine fest definierte Absende-IP-Adresse verwenden, tragen Sie diese symbolisch oder direkt hier ein.

Accounting-Server

Acc.-Server Adresse

Geben Sie hier die IP-Adresse (IPv4, IPv6) oder den Host-Namen des RADIUS-Accounting-Servers für die Zugänge zum Public-Spot an.

Acc.-Server Port

Der Port, über den der Access Point mit dem Accounting-Server kommunizieren kann.

Acc.-Server Attr.werte

Hier können sie RADIUS-Attribute mit benutzerdefinierten Werten versehen. Die einzelnen Namen-Werte-Paare müssen der Form <Name>=<Wert> entsprechen und sind durch Semikola voneinander getrennt.

<Name> identifiziert dabei das RADIUS-Attribut durch seinen Namen oder seine Nummer. Die zugehörigen Attributnamen finden Sie in den entsprechenden RADIUS RFCs. Attributsnamen können abgekürzt werden, solange die Bezeichner eindeutig sind.

Da die Anzahl der Zeichen begrenzt ist, lässt sich der Name abkürzen. Das Kürzel muss dabei eindeutig sein. Beispiele:

- `NAS-Port=1234` ist nicht erlaubt, da das Attribut nicht eindeutig ist (`NAS-Port`, `NAS-Port-Id` oder `NAS-Port-Type`).
- `NAS-Id=ABCD` ist erlaubt, da das Attribut eindeutig ist (`NAS-Identifier`).

Als Attribut-Wert ist die Angabe von Namen oder RFC-konformen Nummern möglich. Für das Gerät sind die Angaben `Service-Type=Framed` und `Service-Type=2` identisch.

Die Angabe eines Wertes in Anführungszeichen (`"<Wert>"`) ist möglich, um Sonderzeichen wie Leerzeichen, Semikolon oder Gleichheitszeichen mit angeben zu können. Das Anführungszeichen innerhalb des Wertes erhält einen umgekehrten Schrägstrich vorangestellt (`\"`), der umgekehrte Schrägstrich ebenfalls (`\\`).

Zusätzlich ist es möglich eine Reihe von Platzhalter einzusetzen:

- `%n` – wird ersetzt durch den konfigurierten Gerätenamen.
- `%e` – wird ersetzt mit der Seriennummer des Gerätes, wie man sie aus dem sysinfo des Gerätes kennt.
- `%%` – wird ersetzt durch ein einzelnes %-Zeichen.
- `%{name}` – wird ersetzt durch den ursprünglichen Wert des entsprechenden RADIUS-Attributes. Etwaige Neu / Um-Definitionen innerhalb dieser Attributsliste werden nicht beachtet! Der Bezeichner kann gekürzt werden, solange er eindeutig bleibt.

Acc.-Server Schlüssel

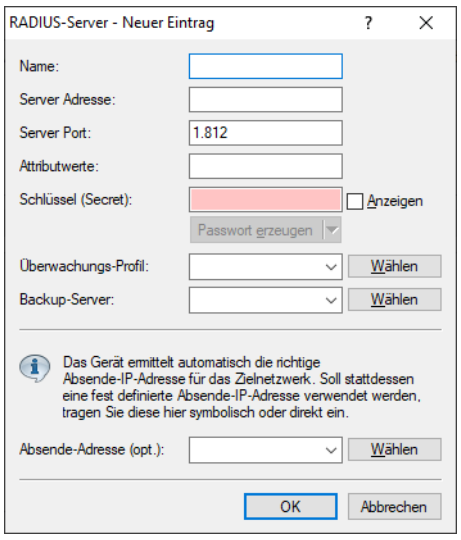
Schlüssel (Shared Secret) für den Zugang zum Accounting-Server. Der Schlüssel muss ebenfalls im Accounting-Server konfiguriert sein.

Absende-Adresse

Das Gerät ermittelt automatisch die richtige Absende-IP-Adresse für das Zielnetzwerk. Wollen Sie stattdessen eine fest definierte Absende-IP-Adresse verwenden, tragen Sie diese symbolisch oder direkt hier ein.

18.3.5 Einwahl über 802.1X und RADIUS

WLAN-Clients können sich über das 802.1X-Protokoll in ein Netzwerk anmelden. Der Access Point kann die Anmeldung über dieses Protokoll an den RADIUS-Server weiterleiten. Die MAC-Adresse wird zur Identifizierung der Benutzer verwendet.



Die Konfiguration erfolgt im LANconfig unter **Schnittstellen** > **802.1X** > **RADIUS-Server**.

Name

Geben Sie jedem RADIUS-Server einen in dieser Tabelle eindeutigen Namen. Der Name 'DEFAULT' ist reserviert für alle WLAN-Netze, deren Authentifizierung nach IEEE 802.1X erfolgt, und die keinen eigenen RADIUS-Server angegeben haben.

Jedem WLAN-Netz, dessen Authentifizierung nach IEEE 802.1X erfolgt, kann im Feld 'Schlüssel 1/Passphrase' ein eigener RADIUS-Server zugewiesen werden, indem dort der hier definierte Name eingesetzt wird.

Server Adresse

Geben Sie hier die IP-Adresse (IPv4, IPv6) oder den Host-Namen des RADIUS-Servers an, mit dem Sie zentral die Benutzer verwalten.

Server Port

Geben Sie hier den Port an, über den Sie mit Ihrem RADIUS-Server kommunizieren.

Attributwerte

Hier können sie RADIUS-Attribute mit benutzerdefinierten Werten versehen. Die einzelnen Namen-Werte-Paare müssen der Form <Name>=<Wert> entsprechen und sind durch Semikola voneinander getrennt.

<Name> identifiziert dabei das RADIUS-Attribut durch seinen Namen oder seine Nummer. Die zugehörigen Attributnamen finden Sie in den entsprechenden RADIUS RFCs. Attributsnamen können abgekürzt werden, solange die Bezeichner eindeutig sind.

Da die Anzahl der Zeichen begrenzt ist, lässt sich der Name abkürzen. Das Kürzel muss dabei eindeutig sein. Beispiele:

- `NAS-Port=1234` ist nicht erlaubt, da das Attribut nicht eindeutig ist (`NAS-Port`, `NAS-Port-Id` oder `NAS-Port-Type`).
- `NAS-Id=ABCD` ist erlaubt, da das Attribut eindeutig ist (`NAS-Identifier`).

Als Attribut-Wert ist die Angabe von Namen oder RFC-konformen Nummern möglich. Für das Gerät sind die Angaben `Service-Type=Framed` und `Service-Type=2` identisch.

Die Angabe eines Wertes in Anführungszeichen (`"<Wert>"`) ist möglich, um Sonderzeichen wie Leerzeichen, Semikolon oder Gleichheitszeichen mit angeben zu können. Das Anführungszeichen erhält einen umgekehrten Schrägstrich vorangestellt (`\"`), der umgekehrte Schrägstrich ebenfalls (`\\`).

Zusätzlich ist es möglich eine Reihe von Platzhalter einzusetzen:

- `%n` – wird ersetzt durch den konfigurierten Gerätenamen.
- `%e` – wird ersetzt mit der Seriennummer des Gerätes, wie man sie aus dem sysinfo des Gerätes kennt.
- `%%` – wird ersetzt durch ein einzelnes %-Zeichen.
- `%{name}` – wird ersetzt durch den ursprünglichen Wert des entsprechenden RADIUS-Attributes. Etwaige Neu / Um-Definitionen innerhalb dieser Attributsliste werden nicht beachtet! Der Bezeichner kann gekürzt werden, solange er eindeutig bleibt.

Schlüssel (Shared-Secret)

Geben Sie hier den Schlüssel an, mit dem die Kodierung der Daten vorgenommen werden soll. Der Schlüssel muss ebenfalls im RADIUS-Server konfiguriert sein.

Überwachungsprofil

Geben Sie hier ein Profil an, über das eine Erreichbarkeitsüberwachung des RADIUS-Servers durchgeführt wird. Siehe auch *Erreichbarkeitsprüfung für externe RADIUS-Server* auf Seite 1582.

Backup-Server

Namen des Backup-Servers aus der Liste der bisher konfigurierten RADIUS-Server.

Die allgemeinen Werte für Wiederholung und Timeout müssen ebenfalls konfiguriert werden.

Im RADIUS-Server müssen die WLAN-Clients folgendermaßen eingetragen sein:

Der Benutzername ist die MAC-Adresse im Format AABBCC-DDEEFF. Das Passwort ist für alle Benutzer identisch mit dem Schlüssel (Shared-Secret) für den RADIUS-Server.

Absende-Adresse

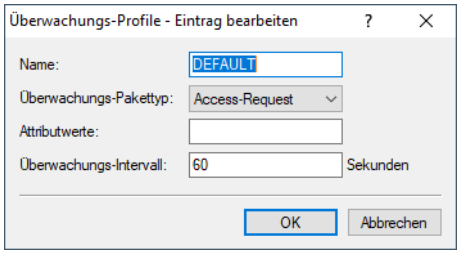
Das Gerät ermittelt automatisch die richtige Absende-IP-Adresse für das Zielnetzwerk. Wollen Sie stattdessen eine fest definierte Absende-IP-Adresse verwenden, tragen Sie diese symbolisch oder direkt hier ein.

18.3.5.1 Erreichbarkeitsprüfung für externe RADIUS-Server

Überwachen Sie mit diesem Feature, ob ein RADIUS-Server erreichbar ist. Hierzu werden regelmäßig RADIUS-Requests gesendet, es wird also geprüft, ob der RADIUS-Dienst funktional ist.

Die Überprüfung kann folgendermaßen geschehen:

- durch das Senden von Status-Server-Requests (DEFAULT). Diese dienen speziell der Erreichbarkeitsüberprüfung von RADIUS-Diensten. Sie werden aber nicht von allen RADIUS-Servern unterstützt (ein Positivbeispiel ist FreeRADIUS).
- durch das Senden von Access-Requests ("Dummy-Requests"). Diese Methode sollte nur verwendet werden, wenn der Server keine Status-Server-Requests unterstützt.



Die Konfiguration erfolgt im LANconfig unter **Schnittstellen** > **802.1X** > **Erreichbarkeitsüberwachung der RADIUS-Server** > **Überwachungs-Profile**.

Name

Hier können Sie einen benutzerdefinierten Namen für das Überwachungsprofil vergeben.

Überwachungs-Pakettyp

Hier haben sie die Wahl zwischen folgenden Typen:

Access-Request (Default)

Dieser Typ sollte nur verwendet werden, wenn der Server keine Status-Server-Requests unterstützt.

Status-Server

Dieser Typ dient speziell der Erreichbarkeitsüberprüfung von RADIUS-Diensten, wird aber nicht von allen RADIUS-Servern unterstützt.

Attributwerte

Ein Attribut ist nur für Access-Requests erforderlich. Für Status-Server-Requests ist es entbehrlich.

Hier können sie RADIUS-Attribute mit benutzerdefinierten Werten versehen. Die einzelnen Namen-Werte-Paare müssen der Form <Name>=<Wert> entsprechen und sind durch Semikola voneinander getrennt.

<Name> identifiziert dabei das RADIUS-Attribut durch seinen Namen oder seine Nummer. Die zugehörigen Attributnamen finden Sie in den entsprechenden RADIUS RFCs. Attributsnamen können abgekürzt werden, solange die Bezeichner eindeutig sind.

Da die Anzahl der Zeichen begrenzt ist, lässt sich der Name abkürzen. Das Kürzel muss dabei eindeutig sein. Beispiele:

- `NAS-Port=1234` ist nicht erlaubt, da das Attribut nicht eindeutig ist (`NAS-Port`, `NAS-Port-Id` oder `NAS-Port-Type`).
- `NAS-Id=ABCD` ist erlaubt, da das Attribut eindeutig ist (`NAS-Identifier`).

Als Attribut-Wert ist die Angabe von Namen oder RFC-konformen Nummern möglich. Für das Gerät sind die Angaben `Service-Type=Framed` und `Service-Type=2` identisch.

Die Angabe eines Wertes in Anführungszeichen (`"<Wert>"`) ist möglich, um Sonderzeichen wie Leerzeichen, Semikolon oder Gleichheitszeichen mit angeben zu können. Das Anführungszeichen innerhalb des Wertes erhält einen umgekehrten Schrägstrich vorangestellt (`\"`), der umgekehrte Schrägstrich ebenfalls (`\\`).

Zusätzlich ist es möglich eine Reihe von Platzhalter einzusetzen:

- `%n` – wird ersetzt durch den konfigurierten Gerätenamen.
- `%e` – wird ersetzt mit der Seriennummer des Gerätes, wie man sie aus dem sysinfo des Gerätes kennt.
- `%%` – wird ersetzt durch ein einzelnes %-Zeichen.
- `%{name}` – wird ersetzt durch den ursprünglichen Wert des entsprechenden RADIUS-Attributes. Etwaige Neu / Um-Definitionen innerhalb dieser Attributsliste werden nicht beachtet! Der Bezeichner kann gekürzt werden, solange er eindeutig bleibt.

Überwachungs-Intervall

Hier legen Sie das Intervall in Sekunden fest, innerhalb dessen die Erreichbarkeit des RADIUS-Servers überprüft wird.

Die so überwachten RADIUS-Server sowie deren Status können Sie in der Tabelle **Status** > **TCP-IP** > **RADIUS-Supervision-Servers** > **Servers** einsehen. Alternativ ist die Statustabelle auch unter **Status** > **SLA-Monitor** > **RADIUS** > **Servers** einsehbar.

18.3.6 Zusätzliche Source-Ports für Access-Requests

Der RADIUS-Client nutzt einen Source-Port (UDP-Listener) zur Verhandlung von Access-Requests mit dem RADIUS-Server. Dieser Port ermöglicht die gleichzeitige Verhandlung von bis zu 256 IDs. Bei vielen Anfragen und gleichzeitig weit entferntem RADIUS-Server ist es möglich, dass alle 256 Access-Requests gleichzeitig offen sind und der RADIUS-Client entsprechend keine weitere Anfrage annehmen würde. Das kommt z. B. in umfangreichen Eduroam-Umgebungen vor.

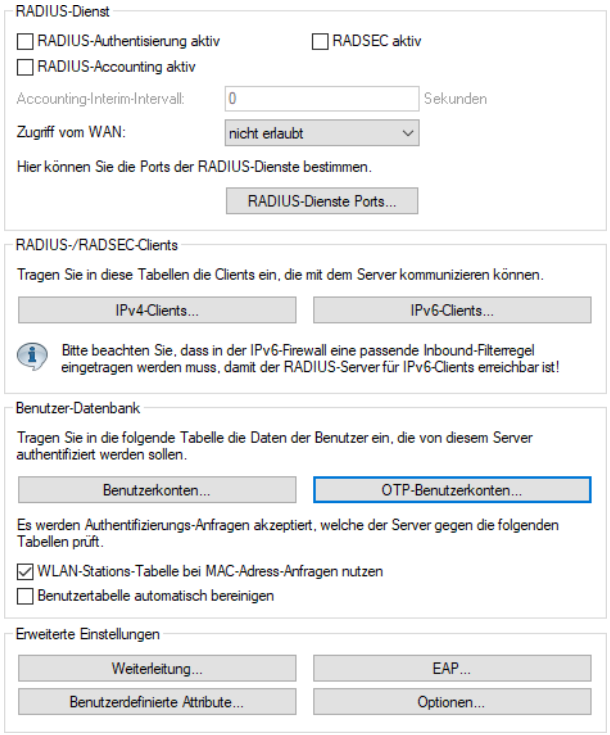
In diesem Fall öffnet der RADIUS-Client den nächsthöheren Source-Port und ermöglicht die Access-Request-Verhandlung weiterer IDs. Das geschieht automatisch und ist nicht konfigurierbar.

18.4 RADIUS-Server

Neben der Funktion als RADIUS-Authenticator oder NAS kann ein Access Point auch als RADIUS-Server arbeiten. In dieser Betriebsart stellt das Gerät seine eigenen Informationen über die anmeldeberechtigten Benutzer den anderen Access Points im Authenticator-Modus zur Verfügung.

Die Konfiguration des RADIUS-Servers beinhaltet, welcher Authenticator auf den RADIUS-Server zugreifen darf, welches Kennwort er für diesen Zugang benötigt und über welchen offenen Port er mit dem RADIUS-Server kommunizieren kann. Der Authentifizierungs-Port gilt dabei global für alle Authenticatoren.

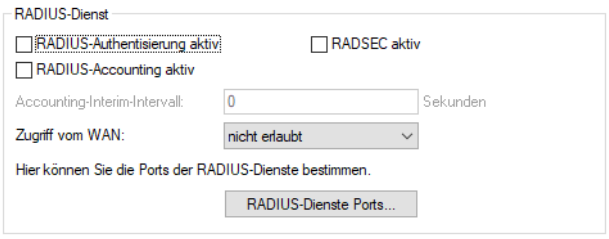
Die Konfiguration des Servers erfolgt über **RADIUS** > **Server**



18.4.1 RADIUS-Dienst

Die Konfiguration des RADIUS-Servers beinhaltet, welcher Authenticator auf den RADIUS-Server zugreifen darf, welches Kennwort er für diesen Zugang benötigt und über welchen offenen Port er mit dem RADIUS-Server kommunizieren kann. Der Authentifizierungs-Port gilt dabei global für alle Authenticatoren.

Die Konfiguration der RADIUS-Dienste erfolgt über **RADIUS** > **Server** > **RADIUS-Dienst**



RADIUS-Authentisierung aktiv

Aktivieren Sie den RADIUS-Authentifizierungs-Dienst.

RADIUS-Accounting aktiv

Aktivieren Sie den RADIUS-Accounting-Dienst.

RADSEC aktiv

Aktivieren Sie den RADSEC-Dienst. Siehe auch *RADSEC* auf Seite 1609.

Accounting-Interim-Intervall

Geben Sie hier an, welchen Wert der RADIUS-Server bei erfolgreicher Authentifizierung als Accounting-Interim-Intervall ausgeben soll. Sofern das anfragende Gerät dieses Attribut unterstützt, steuert dieser Wert, in welchem Intervall (in Sekunden) der Accounting-RADIUS-Server ein Update der Accounting-Daten erhält.

Zugriff vom WAN

Geben Sie hier an, auf welche Weise der RADIUS-Server aus dem WAN erreichbar ist.

Gilt ausschließlich für Zugriffe aus dem IPv4-Netz. Zugriffe aus dem IPv6-Netz steuert die eingebundene Firewall. Standardmäßig verbietet die IPv6-Firewall den WAN-Zugriff auf den RADIUS-Server.

RADIUS-Dienste Ports

Authentifizierungs-Port

Geben Sie hier den TCP-Port an, über den die Authenticatoren mit dem RADIUS-Server im Access Point kommunizieren. Üblicherweise ist das der Port '1812'.

Accounting-Port

Geben Sie hier den TCP-Port an, über den der RADIUS-Server Accounting-Informationen entgegennimmt. Üblicherweise ist das der Port '1813'.

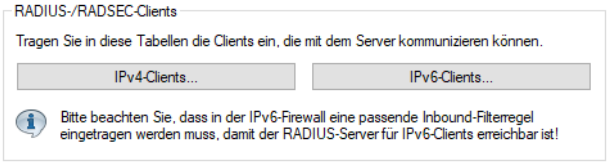
RADSEC-Port

Geben Sie hier an, über welchen TCP-Port der Server über RADSEC verschlüsselte Accounting- oder Authentifizierungsanfragen annimmt. Üblicherweise ist das der Port '2083'.

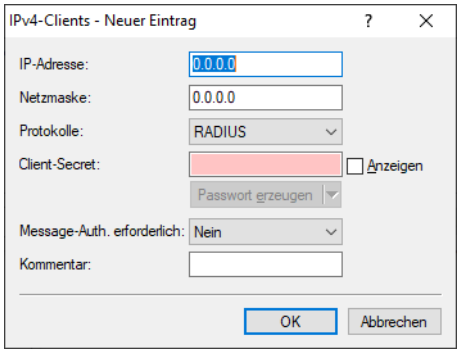
18.4.2 RADIUS- / RADSEC-Clients

Tragen Sie in diese Tabellen die Clients ein, die mit dem Server kommunizieren können. Verwenden Sie je nach Netzwerkprotokoll die entsprechende Tabelle.

Die Konfiguration der RADIUS- / RADSEC-Clients erfolgt über **RADIUS** > **Server** > **RADIUS- / RADSEC-Clients** unter **IPv4-Clients** bzw. **IPv6-Clients**.



IPv4-Clients



Folgende Werte sind je Client einzutragen:

IP-Adresse

IP-Adresse (oder Adressbereich) der Clients, für die das in diesem Dialog eingetragene Passwort gilt.

Netzmaske

IP-Netzmaske der Clients.

Protokolle

Protokoll für die Kommunikation zwischen dem internen Server und den Clients.

Client-Secret

Passwort, das die Clients für den Zugang zum internen Server benötigen.

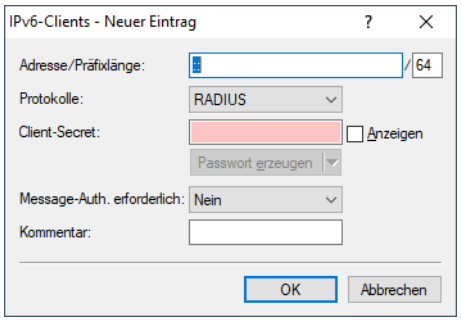
Message-Authenticator erforderlich

Definiert, ob das Vorhandensein des Message-Authenticator-Attributs in RADIUS-Nachrichten auf Client-Seite erforderlich ist. Die Client-Seite ist die Seite, die den RADIUS-Accept/Fail empfängt.

Kommentar

Kommentar zu diesem Eintrag.

IPv6-Clients



Folgende Werte sind je Client einzutragen:

Adresse / Präfixlänge

IP-Adresse (oder Adressbereich) der Clients, für die das in diesem Dialog eingetragene Passwort gilt.

Für die Verwendung einer Adresse muss die Präfix-Länge 128 Bit betragen. Der Eintrag „fd00::/64" z. B. erlaubt das gesamte Netzwerk, der Eintrag „fd00::1/128" erlaubt hingegen nur genau einen Client.

Protokolle

Protokoll für die Kommunikation zwischen dem internen Server und den Clients.

Client-Secret

Passwort, das die Clients für den Zugang zum internen Server benötigen.

Message-Authenticator erforderlich

Definiert, ob das Vorhandensein des Message-Authenticator-Attributs in RADIUS-Nachrichten auf Client-Seite erforderlich ist. Die Client-Seite ist die Seite, die den RADIUS-Accept/Fail empfängt.

Kommentar

Kommentar zu diesem Eintrag.

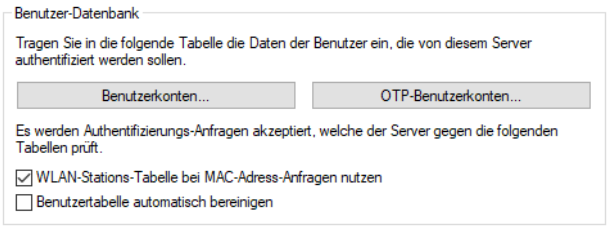
Damit der RADIUS-Server für IPv6-Clients erreichbar ist, muss ggf. in der IPv6-Firewall eine entsprechende Inbound-Regel eingetragen sein.

18.4.3 Benutzer-Datenbank

In der RADIUS-Benutzerdatenbank tragen Sie die Benutzerkonten ein, die der RADIUS-Server ohne weitere Datenbanken authentifizieren kann. Diese Datenbank verwendet der RADIUS-Server für lokale Anfragen, also für Anfragen mit Benutzernamen ohne Realm.

Bitte beachten Sie, dass die Anzahl der Benutzer, die die Datenbank aufnehmen kann, modellabhängig ist. Die maximale mögliche Anzahl der Benutzerkonten entnehmen Sie der Produktbeschreibung Ihres Gerätes. Bei Geräten ohne Limitierung ist eine Obergrenze von max. 2.500 Benutzern empfehlenswert.

Die Konfiguration der RADIUS-Benutzerdatenbank erfolgt über **RADIUS** > **Server** > **Benutzer-Datenbank**.



WLAN-Stations-Tabelle bei MAC-Adress-Anfragen nutzen

Dieser Parameter gibt an, ob die WLAN-Zugangsliste als Informationsquelle für den RADIUS-Server im Access Point verwendet werden soll. Die WLAN-Zugriffsliste enthält den Benutzernamen in Form der MAC-Adresse und das Kennwort („WPA-Passphrase"). Neben diesen Zugangsdaten liefert die Zugriffsliste Information wie Bandbreitenbeschränkung oder Zugehörigkeit zu einem bestimmten VLAN.

Die WLAN-Zugangsliste finden Sie unter **Wireless-LAN** > **Stationen / LEPS** > **LEPS-MAC** > **Stationsregeln**. In ihr können 512 WLAN-Clients eingetragen werden, die sich an einem Access Point anmelden dürfen. In der Betriebsart als RADIUS-Server kann diese Liste auch verwendet werden, um über RADIUS Clients zu prüfen, die sich an anderen Access Points anmelden wollen. In einer Installation mit mehreren Access Points kann so die Zugangsberechtigung der Clients an einer zentralen Stelle gepflegt werden.

Ein einmal angemeldeter WLAN-Client bleibt nach der Authentifizierung über RADIUS solange aktiv, bis er sich selbst wieder abmeldet oder vom RADIUS-Server abgemeldet wird. Der RADIUS-Server kann mit der Vorgabe eines Prüfzyklus [Minuten] regelmäßig prüfen, ob die angemeldeten WLAN-Clients noch in der Zugangsliste enthalten sind. Wird ein WLAN-Client aus der Zugangsliste entfernt, bleibt er maximal bis zum nächsten Ablauf des Prüfzyklus im WLAN angemeldet. Den Prüfzyklus können Sie über die Konsole unter **Setup** > **WLAN** > **RADIUS-Zugriffspruefung** > **Pruef-Zyklus** anpassen.

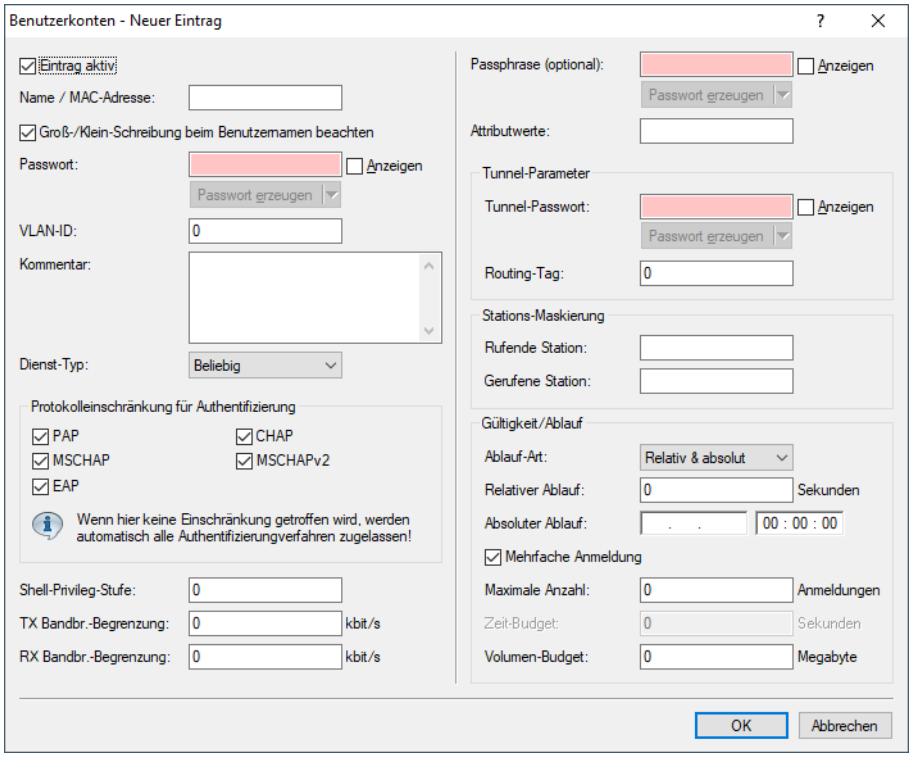
Ein Prüfzyklus von '0' schaltet die regelmäßige Prüfung aus, die WLAN-Clients bleiben solange angemeldet, bis sie sich selbst abmelden.

Benutzertabelle automatisch bereinigen

Ist diese Option eingeschaltet werden abgelaufene Benutzerkonten automatisch aus der Kontentabelle gelöscht. Dabei werden sowohl Konten mit absoluter als auch mit relativer Gültigkeit berücksichtigt.

Für die Bearbeitung von Konten mit relativer Gütigkeit und Konten mit Zeit- oder Volumen-Budget muss das Gerät nicht nur als Authentifizierungs-Server sondern auch als Accounting-Server arbeiten.

Über **Benutzerkonten** definieren Sie dann die Einträge für lokale Anfragen.



Eintrag aktiv

Über diese Option aktivieren bzw. deaktivieren Sie gezielt ein RADIUS-Benutzerkonto. Auf diese Weise lassen sich z. B. einzelne Benutzerkonten temporär abschalten, ohne dafür das komplette Konto zu löschen.

Name / MAC-Adresse

Geben Sie hier den Namen des Benutzers oder eine MAC-Adresse ein.

Die MAC-Adresse wird zusammen mit der Passphrase für die Authentifizierung mittels LEPS-MAC verwendet.

Groß- / Kleinschreibung beim Benutzernamen beachten

Bei aktivierter Option unterscheidet der RADIUS-Server nach Groß- und Kleinschreibung. „User12345“ und „user12345“ sind somit zwei unterschiedliche Benutzer.

Passwort

Passwort des Benutzers.

VLAN-ID

Mit dieser Option kann dem Benutzer bei erfolgreicher Authentifizierung eine bestimmte VLAN-ID zugewiesen werden. Durch den Wert 0 wird dem Benutzer keine VLAN-ID zugewiesen.

Kommentar

Zusätzliche Informationen zum Benutzer.

Dienst-Typ

Der Dienst-Typ ist ein spezielles Attribut des RADIUS-Protokolls, welches der NAS (Network Access Server) mit dem Authentication Request übermittelt. Der Request wird nur dann positiv beantwortet, wenn der angefragte Dienst-Typ mit dem Dienst-Typ des Benutzerkontos übereinstimmt. Mögliche Werte sind u. a.:

- `Beliebig`: Der Dienst-Typ kann ein beliebiger Sein.

- `Framed`: Für Prüfung von WLAN-MAC-Adressen über RADIUS bzw. bei IEEE 802.1X.
- `Anmeldung`: Für Public-Spot-Anmeldungen.
- `Nur Authentifizierung`: Für Einwahl-Gegenstellen über PPP, die mit RADIUS authentifiziert werden.
- und diverse weitere, die vom RADIUS-Protokoll definiert werden.

Beachten Sie, dass in Abhängigkeit vom Gerät die Anzahl der Einträge mit dem Dienst-Typ `Beliebig` oder `Anmeldung` begrenzt sein kann. Ist Ihr Gerät z. B. dazu in der Lage, insgesamt 64 Public-Spot-Benutzer zu verwalten, dann verweigert LANconfig nach dem 64. Benutzerkonto mit dem Dienst-Typ `Beliebig` / `Anmeldung` die Anlage weiterer Benutzerkonten mit diesen Dienst-Typen.

Protokolleinschränkung für Authentifizierung

Mit dieser Option können Sie die für den Benutzer erlaubten Authentifizierungsverfahren einschränken. Mögliche Werte sind:

PAP

Der NAS übermittelt den Benutzernamen und das Passwort. Der RADIUS-Server durchsucht seine Datensätze nach einem passenden Eintrag für den Benutzernamen, vergleicht dann das Passwort und antwortet mit einem RADIUS-Accept oder RADIUS-Reject.

CHAP

Der NAS übermittelt den Benutzernamen, die CHAP-Aufforderung (Challenge) und die Passwort-Eigenschaften (nicht das Passwort selbst!). Der RADIUS-Server durchsucht seine Datensätze nach einem passenden Eintrag für den Benutzernamen und errechnet aus dem zugehörigen Passwort und der vom NAS übermittelten CHAP-Challenge die CHAP-Antwort. Wenn die berechnete Antwort mit der vom Client über den NAS gesendeten Antwort übereinstimmt sendet der RADIUS-Server einen RADIUS-Accept, ansonsten einen RADIUS-Reject.

MSCHAP

Der NAS übermittelt den Benutzernamen, die MS-CHAP-Challenge und die MS-CHAP-Passwort-Eigenschaften. Der weitere Vorgang ist der gleiche wie bei CHAP, die Antworten sind dabei allerdings nach dem MS-CHAP-Algorithmus berechnet (*RFC 2433*).

MSCHAPv2

Der NAS übermittelt den Benutzernamen, die MS-CHAP-Challenge und die MS-CHAP2-Antwort. Der weitere Vorgang ist der gleiche wie bei CHAP und MS-CHAP, die Antworten sind dabei allerdings nach dem MS-CHAPv2-Algorithmus berechnet (*RFC 2759*). Außerdem überträgt der RADIUS-Server eine MS-CHAP2-Bestätigung, wenn die Authentifizierung erfolgreich durchgeführt wurde. Diese Bestätigung enthält die Antwort des Servers auf die Aufforderung des Clients und ermöglicht so eine gegenseitige Authentifizierung.

EAP

Der NAS übermittelt den Benutzernamen und eine EAP-Nachricht. Im Gegensatz zu allen vorherigen Methoden ist EAP nicht zustandslos, d. h. der RADIUS-Server kann mit einer eigenen Aufforderung (Challenge) statt nur mit einem Access-Accept oder Access-Reject antworten und so weitere Anforderungen vor dem Abschluss der Authentifizierung stellen. EAP ist selbst ein modulares Authentifizierungsprotokoll, das unterschiedliche Authentifizierungsverfahren erlaubt.

Shell-Privileg-Stufe

Vendor spezifisches RADIUS-Attribut, um in einem RADIUS-Accept die Privilegstufe des Nutzers zu kommunizieren (Default: 0).

TX-Bandbr.-Begrenzung

Begrenzung der Bandbreite beim Senden von Daten.

RX-Bandbr.-Begrenzung

Begrenzung der Bandbreite beim Empfangen von Daten

Die Bandbreitenbegrenzung für Senden und Empfangen gilt unabhängig vom verwendeten Interface (LAN und WLAN).

Passphrase

Die die jeweilig zugeordnete WPA-Passphrase des registrierten Benutzers. Somit kann auch ein LAN-gebundenes Gerät als zentraler RADIUS-Server dienen und die Vorteile von LEPS-MAC (LANCOM Enhanced Passphrase Security MAC) nutzen.

Bei der Konfiguration von LEPS-MAC wird jeder MAC-Adresse eines im WLAN zugelassenen Clients eine eigene Passphrase zugeordnet. Dies kann entweder als Eintrag in der Liste unter **Wireless-LAN** > **Stationen/LEPS** > **LEPS-MAC** > **Stationsregeln** (siehe *LANCOM Enhanced Passphrase Security MAC (LEPS-MAC)* auf Seite 970) oder im RADIUS-Server geschehen. Pro MAC-Adresse wird ein Eintrag erzeugt – im Sinne des RADIUS-Servers ist die jeweilige MAC-Adresse also ein Benutzer. Zusätzlich muss unter **Wireless-LAN** > **Allgemein** > **Interfaces** > **Logische WLAN-Einstellungen** der MAC-Filter aktiviert sein, d. h., die Daten von den hier eingetragenen WLAN-Clients werden übertragen.

Als Passphrase können Zeichenketten mit 8 bis 64 Zeichen verwendet werden. Wir empfehlen als Passphrasen zufällige Zeichenketten von mindestens 32 Zeichen Länge.

Bei Speicherung der client-spezifischen Passphrasen in der Benutzertabelle eines RADIUS-Servers kann auch ein LAN-gebundenes Gerät als zentraler RADIUS-Server dienen und die Vorteile von LEPS-MAC nutzen.

Attributwerte

Hier können sie RADIUS-Attribute mit benutzerdefinierten Werten versehen. Die einzelnen Namen-Werte-Paare müssen der Form <Name>=<Wert> entsprechen und sind durch Semikola voneinander getrennt.

<Name> identifiziert dabei das RADIUS-Attribut durch seinen Namen oder seine Nummer. Die zugehörigen Attributnamen finden Sie in den entsprechenden RADIUS RFCs. Attributsnamen können abgekürzt werden, solange die Bezeichner eindeutig sind.

Da die Anzahl der Zeichen begrenzt ist, lässt sich der Name abkürzen. Das Kürzel muss dabei eindeutig sein. Beispiele:

- `NAS-Port=1234` ist nicht erlaubt, da das Attribut nicht eindeutig ist (`NAS-Port`, `NAS-Port-Id` oder `NAS-Port-Type`).
- `NAS-Id=ABCD` ist erlaubt, da das Attribut eindeutig ist (`NAS-Identifier`).

Als Attribut-Wert ist die Angabe von Namen oder RFC-konformen Nummern möglich. Für das Gerät sind die Angaben `Service-Type=Framed` und `Service-Type=2` identisch.

Die Angabe eines Wertes in Anführungszeichen (`"<Wert>"`) ist möglich, um Sonderzeichen wie Leerzeichen, Semikolon oder Gleichheitszeichen mit angeben zu können. Das Anführungszeichen innerhalb des Wertes erhält einen umgekehrten Schrägstrich vorangestellt (`\"`), der umgekehrte Schrägstrich ebenfalls (`\\`).

Zusätzlich ist es möglich eine Reihe von Platzhalter einzusetzen:

- `%n` – wird ersetzt durch den konfigurierten Gerätenamen.
- `%e` – wird ersetzt mit der Seriennummer des Gerätes, wie man sie aus dem sysinfo des Gerätes kennt.
- `%%` – wird ersetzt durch ein einzelnes %-Zeichen.

- `%{name}` – wird ersetzt durch den ursprünglichen Wert des entsprechenden RADIUS-Attributes. Etwaige Neu / Um-Definitionen innerhalb dieser Attributsliste werden nicht beachtet! Der Bezeichner kann gekürzt werden, solange er eindeutig bleibt.

Tunnel-Passwort

Legen Sie mit diesem Eintrag das Verbindungs-Kennwort für den jeweiligen Benutzer fest.

Routing-Tag

Geben Sie hier das Routing-Tag für diese Verbindung an.

Rufende Station

Diese Maske schränkt die Gültigkeit des Eintrags auf bestimmte IDs ein, die die rufende Station (WLAN-Client) übermittelt. Bei der Authentifizierung über 802.1X wird die MAC-Adresse der rufenden Station im ASCII-Format (nur Großbuchstaben) übertragen, dabei werden Zeichenpaare durch einen Bindestrich getrennt (z. B. „00-10-A4-23-19-C0“).

Gerufene Station

Diese Maske schränkt die Gültigkeit des Eintrags auf bestimmte IDs ein, die die gerufende Station (BSSID und SSID des Access-Points) übermittelt. Bei der Authentifizierung über 802.1X werden die MAC-Adresse (BSSID) der gerufenen Station im ASCII-Format (nur Großbuchstaben) übertragen, dabei werden Zeichenpaare durch einen Bindestrich getrennt. Die SSID wird nach einem Doppelpunkt als Trennzeichen angehängt (z. B. „00-10-A4-23-19-C0:AP1“).

Ablauf-Art

Diese Option legt die Art der Gültigkeitsdauer des Benutzer-Accounts fest. Mögliche Werte sind:

- `Relativ & absolut`
- `Relativ`
- `Absolut`
- `Niemals`

Relativer Ablauf

Gültigkeit in Sekunden ab der ersten erfolgreichen Anmeldung.

Absoluter Ablauf

Gültigkeit in Stunden, Minuten und Sekunden ab einem bestimmten Datum.

Mehrfache Anmeldung

Aktiviert die Möglichkeit für den Client, sich mehrfach anmelden zu können.

Maximale Anzahl

Maximale Anzahl der gleichzeitigen Anmeldungen des Clients.

Zeit-Budget

Legt das Zeit-Budget in Sekunden fest, das dem Client zur Verfügung steht, wenn keine **mehrfache Anmeldung** aktiviert ist.

Volumen-Budget

Legt das Datenvolumen fest, das dem Client zur Verfügung steht.

18.4.3.1 Im- / Export von RADIUS-Benutzerdaten per CSV-Datei

Der interne RADIUS-Server ist im Prinzip eine Benutzerdatenbank. Daher soll hier eine einfache Möglichkeit gezeigt werden, mit der Sie Benutzereinträge im- und exportieren können. Insbesondere ist dies für Public-Spot-Benutzer relevant, die z. B. in größerer Zahl von einem externen System erzeugt werden. Aber auch für LEPS-MAC können Sie hier die Daten

vereinfacht importieren. Als Format für den Datenaustausch wird csv (comma separated values) genommen, wobei als Default-Separator der einzelnen Datenfelder ein Semikolon dient.

Export von RADIUS-Benutzerdaten per CSV-Datei

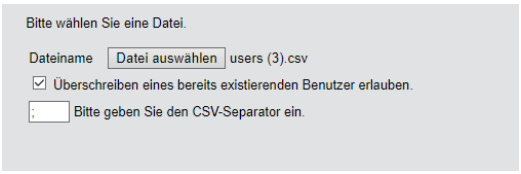
Um die Benutzerdaten des RADIUS-Servers über WEBconfig zu exportieren, gehen Sie folgendermaßen vor.

Klicken Sie auf **Extras** > **RADIUS-Benutzer exportieren**.
Die Benutzerdaten werden als Datei `users.csv` heruntergeladen. Als Trennzeichen dient das Semikolon; in der ersten Zeile sind die Bezeichner der Datenbankfelder.

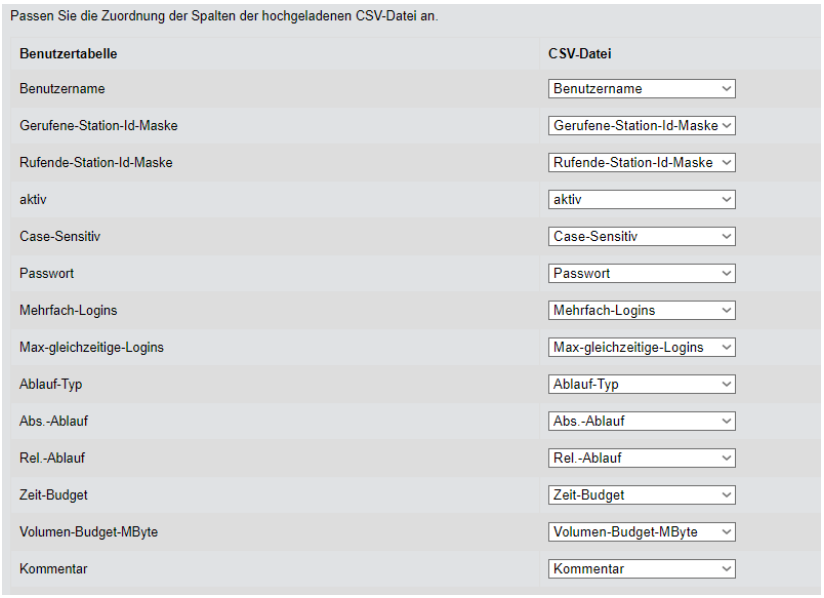
Import von RADIUS-Benutzerdaten per CSV-Datei

Um die Benutzerdaten des RADIUS-Servers über WEBconfig zu importieren, gehen Sie folgendermaßen vor.

1. Führen Sie wie in *Export von RADIUS-Benutzerdaten per CSV-Datei* auf Seite 1592 beschrieben einen Export der Benutzerdaten durch, um die korrekte Kopfzeile mit den Bezeichnern der Datenbankfelder zu erhalten.
2. Erstellen Sie eine CSV-Importdatei mit einer Kopfzeile, welche die im vorigen Schritt ermittelten korrekten Bezeichner der Datenbankfelder beinhaltet. Die Importdatei muss nicht alle Spalten enthalten.
3. Wechseln Sie zum Menüpunkt **Extras** > **RADIUS-Benutzer importieren**.
4. Wählen Sie mit **Datei auswählen** die zu importierende CSV-Datei aus.
5. Geben Sie den CSV-Separator ein. Standardmäßig ist bereits „;“ voreingestellt.



6. Starten Sie den Upload.
7. Kontrollieren Sie nun die Zuordnung der unterstützten Spalten zu den in der CSV-Datei erkannten Spalten. Die Zuordnung kann in diesem Dialog angepasst werden. Wenn Sie die Spaltennamen aus der zuvor exportierten CSV-Datei übernommen haben, ist keine Anpassung notwendig.

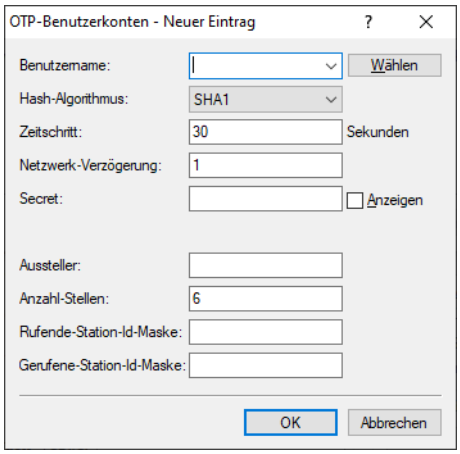


8. Wählen Sie **Import starten**, um den Vorgang abzuschließen und die Benutzerdaten zu übernehmen.

18.4.3.2 OTP-Benutzerkonten

In der Tabelle OTP-Benutzerkonten werden die OTP-Benutzer definiert. Für EAP-OTP muss der Benutzer mit seinem normalen Passwort in der Tabelle der *RADIUS-Benutzerkonten* angelegt werden, sowie zusätzlich in dieser Tabelle mit dem OTP-Secret angelegt werden.

Die Konfiguration der OTP-Benutzerkonten erfolgt über **RADIUS** > **Server** > **Benutzer-Datenbank** > **OTP-Benutzerkonten**.



Benutzername

Geben Sie hier den Namen des OTP-Benutzers ein. Dieser muss in der Tabelle RADIUS-Benutzerkonten bereits mit gleichem Namen enthalten sein.

Hash-Algorithmus

Definiert den verwendeten Hash-Algorithmus.

Beachten Sie, dass die Authenticator-App den maximal möglichen Hash-Algorithmus unterstützt. Der Google Authenticator unterstützt aktuell z. B. auf bestimmten Android-Plattformen nur SHA1.

Zeitschritt

Definiert das Intervall in Sekunden, nach dem ein neues OTP berechnet wird. Default: 30 Sekunden

Netzwerk-Verzögerung

Definiert, um wie viele Zeitschritte die Uhr des Clients maximal abweichen darf. Der RADIUS-Server prüft das um diesen Wert ältere bzw. neuere OTP.

Secret

Definiert das eigentliche Shared Secret, das mit der Authenticator-App geteilt werden muss. Das Secret muss für jeden Benutzer unterschiedlich sein. Es gibt aktuell in der Tabelle drei Eingabemöglichkeiten:

Base32 (Default)

Präfix „base32:“ und danach das Base32-kodierte Secret. Der Präfix „base32:“ darf auch weggelassen werden.

Hexadezimal

Präfix „hex:“ und danach eine gerade Anzahl von Hex-Digits.

Plain text passphrase

Präfix „ascii:“ und danach die Zeichen.

Für den Google Authenticator muss das Secret 16 Zeichen (80 Bit, Base32 codiert) lang sein, z. B. E3U5IDWEE3KFCJ7G

Aussteller

Frei definierbarer Text, der im Authenticator dazu dient, mehrere Schlüssel auseinanderzuhalten, wenn der gleiche Benutzername verwendet wird. Darf keinen Doppelpunkt enthalten.

Anzahl Stellen

Länge der OTPs. Default: 6.

Für den Google-Authenticator sollte der Wert 6 verwendet werden.

Rufende Station

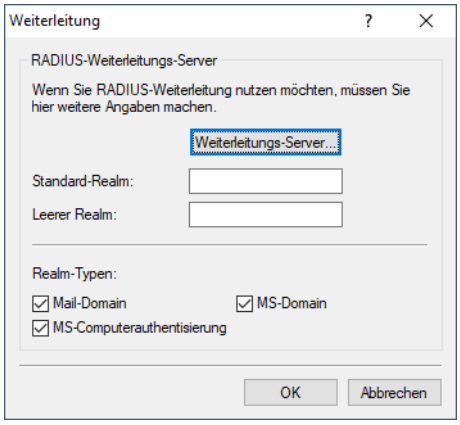
Diese Maske schränkt die Gültigkeit des Eintrags auf bestimmte IDs ein, die die rufende Station übermittelt.

Gerufene Station

Diese Maske schränkt die Gültigkeit des Eintrags auf bestimmte IDs ein, die die gerufene Station übermittelt.

18.4.4 Weiterleitung

Die Konfiguration der Weiterleitung erfolgt über **RADIUS** > **Server** > **Erweiterte Einstellungen** > **Weiterleitung**



Bei den „mehrschichtigen" EAP-Protokollen wie TTLS oder PEAP kann die eigentliche „innere" Authentifizierung auf einem separaten RADIUS-Server erfolgen. Das ermöglicht z. B. die Weiterverwendung eines existierenden RADIUS-Servers, der nur die Benutzertabellen bereitstellt, selbst aber nicht EAP(/TLS)-fähig ist. Der TLS/TTLS/PEAP-Tunnel wird in diesem Fall vom LCOS-RADIUS-Server verwaltet.

Die Konfiguration von solchen mehrschichtigen Protokollen ist Teil einer allgemeinen Methode zur Weiterleitung von RADIUS-Anfragen, mit der ein LCOS-RADIUS-Server auch als RADIUS-Proxy verwendet werden kann. Die Weiterleitung von Anfragen bzw. die Proxy-Funktion basieren auf dem Konzept der „Realms". Ein Realm ist eine Zeichenkette, welche die Gültigkeit einer Reihe von Benutzerkonten definiert. Das Gerät betrachtet die folgenden Bestandteile eines Benutzernamens als Realm:

Mail-Domain

`user@company.com`; `company.com` bildet den Realm und ist durch ein @-Zeichen vom Benutzernamen getrennt.

MS-Computerauthentisierung

`company\user`; `company` bildet den Realm und ist durch einen Backslash („\") vom Benutzernamen getrennt. Diese Authentifizierung ist z. B. bei einem Windows-Login gebräuchlich.

MS-Domain

`host/user.company.com`; Beginnt der Benutzername mit dem String `host/` und enthält der restliche Name mindestens einen Punkt, dann betrachtet das Gerät alles hinter dem ersten Punkt als Realm (in diesem Fall also `company.com`).

Der Realm kann als Hinweis auf den RADIUS-Server verstanden werden, auf dem das Benutzerkonto verwaltet wird. Vor dem Durchsuchen der Benutzertabelle auf dem RADIUS-Server wird der Realm wieder entfernt. Mit der Nutzung von Realms können ganze Netzwerke, die untereinander als vertrauenswürdig gelten, die RADIUS-Server in den Partner-Netzen nutzen und so auch zwischen den Netzen wechselnde Benutzer authentifizieren. Der LCOS-RADIUS-Server speichert die verbundenen RADIUS-Server mit Angabe des zugehörigen Realms in einer Weiterleitungs-Tabelle. Diese Tabelle wird nach dem – in Verbindung mit dem Benutzernamen übermittelten – Realm durchsucht. Wenn keine Übereinstimmung gefunden wird, wird die Anfrage mit einem Access Reject beantwortet. Ein leerer Realm wird als lokale Anfrage gewertet, d. h. der LCOS-RADIUS-Server durchsucht seine eigenen Benutzer-Tabellen und erzeugt daraus die entsprechende Antwort.

Zur Unterstützung der Realm-Verarbeitung verwendet der LCOS-RADIUS-Server zwei spezielle Realms:

Standard-Realm

Dieser Realm wird verwendet, wenn ein Realm übermittelt wird, für den kein expliziter Weiterleitungs-Server definiert ist. Für den Standard-Realm selbst muss in der Weiterleitungs-Tabelle allerdings ein entsprechender Eintrag angelegt werden.

Leerer Realm

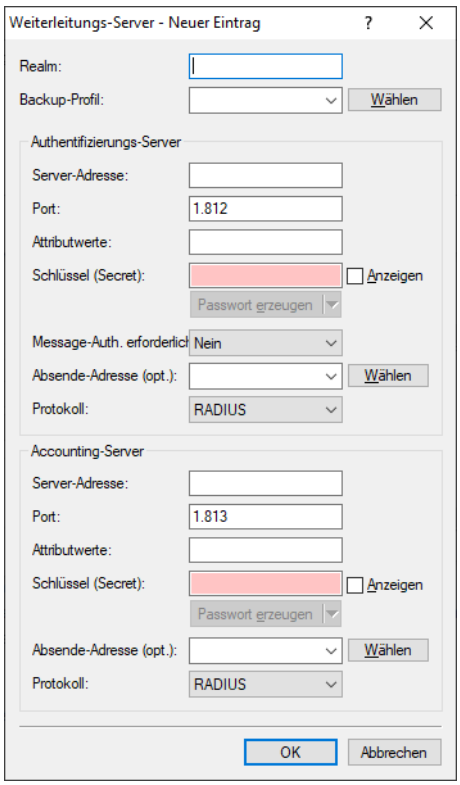
Dieser Realm wird verwendet, wenn **kein** Realm, sondern nur der Benutzername übermittelt wird.

Im Default-Zustand enthält die Weiterleitungs-Tabelle keine Einträge, der Standard- und der Leere Realm sind leer. Das bedeutet das alle Anfragen als lokale Anfragen behandelt werden und ggf. übermittelte Realms werden ignoriert. Um den LCOS-RADIUS-Server als reinen Weiterleitungs-Server bzw. RADIUS-Proxy zu verwenden, müssen der Standard- und der Leere Realm auf einen Wert gesetzt werden, für den in der Weiterleitungs-Tabelle ein entsprechender Server definiert ist.

Bitte beachten Sie, dass die Weiterleitung von RADIUS-Anfragen den übermittelten Benutzernamen nicht verändert – es wird weder ein Realm hinzugefügt, noch verändert oder abgeschnitten. Der Server, an den die Anfrage weitergeleitet wird, muss nicht der letzte der Weiterleitungs-Kette sein, und er benötigt möglicherweise den Realm selbst für eine korrekte Weiterleitung. Nur der RADIUS-Server, der letztlich die Anfrage bearbeitet, löst den Realm aus dem Benutzernamen und durchsucht erst dann die Tabellen mit den Benutzerkonten. Dementsprechend löst der LCOS-RADIUS-Server den Realm vom Benutzernamen, wenn die Anfragen lokal verarbeitet werden.

Zur Verarbeitung von getunnelten EAP-Anfragen im Zusammenhang mit TTLS und PEAP wird ein spezieller EAP-Tunnel-Server verwendet – auch in Form eines Realms. Wählen Sie hier einen Realm, der nicht mit anderen verwendeten Realms in Konflikt steht. Wenn kein EAP-Tunnel-Server angegeben ist, leitet der LCOS-RADIUS-Server Anfragen an sich selbst weiter, was bedeutet, dass sowohl die innere als auch die äußere EAP-Authentifizierung vom LCOS-RADIUS-Server selbst bearbeitet werden.

Richten Sie ggfs. die **Weiterleitungs-Server** ein.



Realm

Zeichenkette, mit der das Weiterleitungs-Ziel identifiziert wird.

Backup-Profil

Alternativer Weiterleitungs-Server, an den Anfragen weitergeleitet werden, wenn der erste Weiterleitungs-Server nicht erreichbar ist.

Authentifizierungs-Server bzw. Accounting-Server

Für die beiden möglichen RADIUS-Anwendungen Zugangsverwaltung (Access) und Abrechnung (Accounting) können Sie hier Parameter konfigurieren, damit der Router entsprechende RADIUS-Anfragen an einen externen RADIUS-Server weiterleiten kann.

Soll keine Weiterleitungsfunktionalität für die Zugangsverwaltung oder Abrechnung genutzt werden, so lassen Sie das entsprechende Adressfeld leer.

Server-Adresse

IP-Adresse des RADIUS-Servers, an den die Anfrage weitergeleitet werden soll.

Port

Für den Port muss die gleiche Port-Nummer eingestellt werden, die im entsprechenden RADIUS-Server konfiguriert ist. Das ist im Allgemeinen 1812 für Zugangsverwaltung (Access) und 1813 für Abrechnung (Accounting).

Attributwerte

Hier können sie RADIUS-Attribute mit benutzerdefinierten Werten versehen. Die einzelnen Namen-Werte-Paare müssen der Form <Name>=<Wert> entsprechen und sind durch Semikola voneinander getrennt.

<Name> identifiziert dabei das RADIUS-Attribut durch seinen Namen oder seine Nummer. Die zugehörigen Attributnamen finden Sie in den entsprechenden RADIUS RFCs. Attributsnamen können abgekürzt werden, solange die Bezeichner eindeutig sind.

Da die Anzahl der Zeichen begrenzt ist, lässt sich der Name abkürzen. Das Kürzel muss dabei eindeutig sein. Beispiele:

- `NAS-Port=1234` ist nicht erlaubt, da das Attribut nicht eindeutig ist (`NAS-Port`, `NAS-Port-Id` oder `NAS-Port-Type`).
- `NAS-Id=ABCD` ist erlaubt, da das Attribut eindeutig ist (`NAS-Identifier`).

Als Attribut-Wert ist die Angabe von Namen oder RFC-konformen Nummern möglich. Für das Gerät sind die Angaben `Service-Type=Framed` und `Service-Type=2` identisch.

Die Angabe eines Wertes in Anführungszeichen (`"<Wert>"`) ist möglich, um Sonderzeichen wie Leerzeichen, Semikolon oder Gleichheitszeichen mit angeben zu können. Das Anführungszeichen innerhalb des Wertes erhält einen umgekehrten Schrägstrich vorangestellt (`\"`), der umgekehrte Schrägstrich ebenfalls (`\\`).

Zusätzlich ist es möglich eine Reihe von Platzhalter einzusetzen:

- `%n` – wird ersetzt durch den konfigurierten Gerätenamen.
- `%e` – wird ersetzt mit der Seriennummer des Gerätes, wie man sie aus dem sysinfo des Gerätes kennt.
- `%%` – wird ersetzt durch ein einzelnes %-Zeichen.
- `%{name}` – wird ersetzt durch den ursprünglichen Wert des entsprechenden RADIUS-Attributes. Etwaige Neu / Um-Definitionen innerhalb dieser Attributsliste werden nicht beachtet! Der Bezeichner kann gekürzt werden, solange er eindeutig bleibt.

Schlüssel (Secret)

Der Schlüssel (Secret) muss ebenfalls mit dem im RADIUS-Server konfigurierten übereinstimmen, damit die Authentifizierung dieses Routers gegenüber dem angesprochenen RADIUS-Server funktioniert.

Message-Authenticator erforderlich

Definiert, ob das Vorhandensein des Message-Authenticator-Attributs in RADIUS-Nachrichten auf Client-Seite erforderlich ist. Die Client-Seite ist die Seite, die den RADIUS-Accept/Fail empfängt.

Absende-Adresse

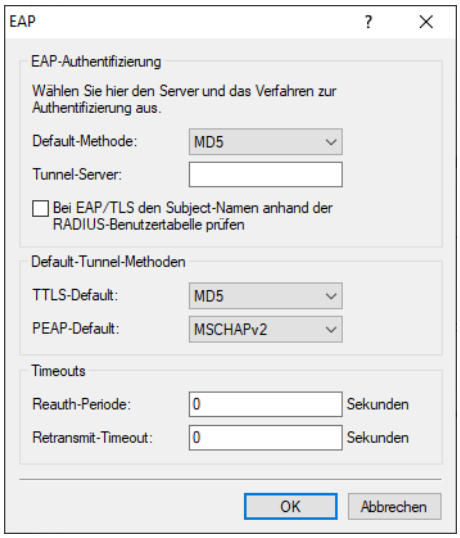
Hier können Sie optional eine Absendeadresse konfigurieren, die statt der ansonsten automatisch für die Zieladresse gewählten Absendeadresse verwendet wird.

Protokoll

Protokoll für die Kommunikation zwischen dem internen RADIUS-Server und dem Weiterleitungs-Server.

18.4.5 EAP-Authentifizierung

Die Konfiguration der EAP-Authentifizierung erfolgt über **RADIUS** > **Server** > **Erweiterte Einstellungen** > **EAP**



EAP ist kein festes Authentifizierungsverfahren sondern es bietet einen Rahmen für beliebige Authentifizierungsverfahren.

Default-Methode

Der LCOS-RADIUS-Server unterstützt eine Reihe von EAP-Verfahren:

MD5

Definiert in *RFC 2284*. EAP/MD5 ist ein einfaches Challenge / Response-Protokoll. Es erlaubt weder eine gegenseitige Authentifizierung noch bietet es dynamische Schlüssel an, wie sie für die 802.1X-Authentifizierung in drahtlosen Netzwerken (WLANs) benötigt werden. Es wird daher nur für die Authentifizierung von nicht-wireless Clients benötigt oder als getunneltes Verfahren innerhalb von TTLS.

GTC

Generic Token Card. EAP-GTC ist eine im *RFC 3748* definierte EAP-Methode, die auch als PEAPv1 bekannt ist. Sie basiert auf einer von einem Authentifizierungsserver versendeten Text, der von einem Security-Token bearbeitet zurückgeschickt werden muss. Die gesamte Übertragung wird nicht verschlüsselt.

MSCHAPv2

Im Gegensatz zu EAP/MD5 erlaubt EAP/MSCHAPv2 zwar die gegenseitige Authentifizierung, unterstützt aber keine dynamischen Schlüssel und ist daher ähnlich anfällig für Dictionary Attacks (Wörterbuchattacken) wie EAP/MD5. Dieses Verfahren wird üblicherweise innerhalb von PEAP-Tunneln genutzt.

TLS

Definiert in *RFC 2716*. Der Einsatz von EAP/TLS erfordert ein Root-Zertifikat, ein Geräte-Zertifikat und einen privaten Schlüssel (Private Key) im Gerät. EAP/TLS bietet hervorragende Sicherheit und die für Wireless-Verbindungen benötigten dynamischen Schlüssel, ist allerdings aufwendig in der Einführung, weil für jeden Client ein Zertifikat und ein Private Key erstellt werden müssen.

Bitte beachten Sie, dass die TLS-Implementation im LCOS weder Zertifikatsketten noch Zertifikats-Rückruflisten (Certificate Revocation Lists – CRL) unterstützt.

TTLS

TTLS basiert auf TLS, verzichtet aber auf Client-Zertifikate und verwendet den schon aufgebauten TLS-Tunnel zur Authentifizierung des Clients. Der LCOS-RADIUS-Server unterstützt die folgenden TTLS-Verfahren:

- PAP
- CHAP
- MSCHAP
- MSCHAPv2
- EAP, vorzugsweise EAP/MD5

PEAP

Ähnlich wie TTLS setzt PEAP auf TLS auf und arbeitet mit einer EAP-Verhandlung im TLS-Tunnel.

Bitte beachten sie, dass PEAP zwar beliebige Authentifizierungsverfahren ermöglicht, der LCOS-RADIUS-Server aber nur MSCHAPv2 als Tunnelmethode unterstützt.

OTP

One Time Password. Dieser Wert muss bei EAP-OTP für die *Zwei-Faktor-Authentifizierung im VPN* verwendet werden, da beim LANCOM Advanced VPN-Client die EAP-Methode vom EAP-Server vorgegeben wird.

Aktuell kann kein Authentifizierungsverfahren unterdrückt werden – der EAP-Supplicant und der RADIUS-Server handeln die EAP-Methode über den Standard-EAP-Mechanismus aus. Sollte der Client eine nicht unterstützte EAP-Methode anfordern, wird er vom RADIUS-Server abgewiesen.

Tunnel-Server

Um getunnelte EAP Anfragen zu bearbeiten, die für TTLS und PEAP auftreten, geben Sie einfach ein Konto an, dass in der Weiterleitungs-Tabelle gelistet ist.

Wählen Sie einen Realm, der keinen Konflikt mit anderen konfigurierten Realms hat. Wenn das Feld leer bleibt, übernimmt der lokale RADIUS-Server die Anfrage selbst. Das bedeutet, die innere und äußere EAP-Phase wird vom lokalen RADIUS-Server durchgeführt.

Bei EAP/TLS den Subject-Namen anhand der RADIUS-Benutzertabelle prüfen

Bei TLS authentifiziert sich der Client alleine über sein Zertifikat. Ist diese Option aktiviert, so prüft der RADIUS-Server zusätzlich, ob der im Zertifikat hinterlegte Benutzername (Common-Name CN im Subject) in der RADIUS-Benutzertabelle enthalten ist.

Ist im passenden Eintrag der RADIUS-Benutzertabelle eine VLAN-ID definiert, so wird diese ebenfalls an den Authenticator übermittelt.

Default-Tunnel-Methoden

TTLS-Default / PEAP-Default

Bei der Verwendung von TTLS bzw. PEAP werden zwei Authentifizierungmethoden ausgehandelt. Zunächst wird über EAP ein sicherer TLS-Tunnel ausgehandelt. In diesem Tunnel wird dann wiederum ein zweites Authentifizierungverfahren ausgehandelt. Bei diesen Verhandlungen bietet der Server jeweils ein Verfahren an, welches der Client annehmen (ACK) oder ablehnen (NAK) kann. Lehnt der Client ab, schickt er dem Server einen Vorschlag mit einem Verfahren, welches er gerne nutzen würde. Ist das vom Client vorgeschlagene Verfahren im Server erlaubt, so wird es verwendet, ansonsten bricht der Server die Verhandlung ab.

Mit diesem Parameter wird das Verfahren festgelegt, das der Server den Clients als Authentifizierungverfahren im TLS-Tunnel anbieten soll. Durch diese Vorgabe können abgelehnte Vorschläge bei der Verhandlung vermieden und so die Verhandlung beschleunigt werden.

Timouts

Reauth-Periode

Wenn der interne RADIUS-Server auf die Anfrage eines Clients mit einem CHALLENGE antwortet (Verhandlung des Authentifizierungsverfahrens ist noch nicht abgeschlossen), kann der RADIUS-Server dem Authenticator

mitteilen, wie lange (in Sekunden) er auf eine Antwort des Clients warten soll, bevor der CHALLENGE erneut zugestellt wird.

Durch den Wert 0 wird kein Timeout an den Authenticator übermittelt.

Retransmit-Timeout

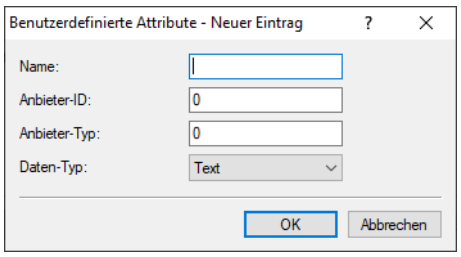
Wenn der interne RADIUS-Server auf die Anfrage eines Clients mit einem ACCEPT antwortet (Verhandlung des Authentifizierungsverfahrens ist erfolgreich abgeschlossen), kann der RADIUS-Server dem Authenticator mitteilen, nach welcher Zeit (in Sekunden) er eine erneute Authentifizierung des Clients auslösen soll.

Durch den Wert 0 wird kein Timeout an den Authenticator übermittelt.

18.4.6 Benutzerdefinierte Attribute

RADIUS-Attribute werden in einem sog. Dictionary verwaltet. Von Haus aus unterstützt LCOS bereits viele verschiedene Attribute; allerdings gibt es eine unüberschaubare Menge von herstellerspezifischen Attributen, die hier durch durch den Administrator in die LCOS-Konfiguration eingetragen werden können. Diese Attribute können dadurch an allen Stellen im LCOS verwendet werden, an denen Attribute zu einer RADIUS-Anfrage bzw. -Antwort hinzugefügt werden können, wie z .B. in der RADIUS-Benutzerverwaltung.

Die Konfiguration der benutzerdefinierten Attribute erfolgt über **RADIUS** > **Server** > **Erweiterte Einstellungen** > **Benutzerdefinierte Attribute**



Name

Der Name, unter dem das Attribut an weiteren Stellen im LCOS referenziert wird.

Anbieter-ID

Die spezifische Anbieter-ID (Vendor-ID) des Attributs.

Anbieter-Typ

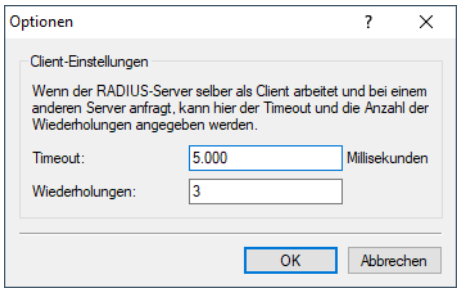
Die spezifische Typ-ID des Attributs.

Daten-Typ

Der Daten-Typ des Attributs.

18.4.7 Optionen

Die Konfiguration der EAP-Authentifizierung erfolgt über **RADIUS** > **Server** > **Erweiterte Einstellungen** > **Optionen**



Wenn der RADIUS-Server selber als Client arbeitet und bei einem anderen Server anfragt, dann können hier entsprechende Einstellungen vorgenommen werden.

Timeout / Wiederholungen

Diese Werte geben an, nach wievielen Millisekunden eine erneute RADIUS-Authentifizierung versucht werden soll und wieviele Versuche insgesamt vollzogen werden, bevor eine Ablehnung erfolgt.

18.5 RADIUS-Attribute

Der RADIUS-Client kann RADIUS-Attribute wie „Framed-IP-Address" etc. von einem externen RADIUS-Server anfragen und diese dann z. B. dem PPPoE-Server zur Verfügung stellen, um diese am PPPoE-, PPTP- oder L2TP-Server zu authentifizieren.

Mehr Informationen zu RADIUS-Attributen finden Sie in den folgenden technischen Dokumenten:

- *RFC 2865*
- *RFC 3162*
- *RFC 4679*
- *RFC 4818*
- *RFC 7268*

Die folgenden Attribute werden vom Gerät in Access-Request-Nachrichten übertragen:

Tabelle 44: Übersicht aller unterstützten RADIUS-Attribute

ID	Bezeichnung	Bedeutung	Mögliche Werte in LCOS
1	User-Name	Der vom Benutzer eingegebene Name.	Verwendet bei 802.1X WLAN, PPPoE-Server, L2TP, PPTP, VPN
2	User-Password	Das vom Benutzer eingegebene Passwort.	Verwendet bei 802.1X WLAN, PPPoE-Server, L2TP, PPTP, VPN
4	NAS-IP-Address	Gibt die IPv4-Adresse des Gerätes an, das den Zugang für einen Anwender anfragt.	<IPv4-Adresse des Gerätes>
6	Service-Type	Gibt den Service-Typ an, den das Gerät anfragt oder als Antwort erwartet.	› Authenticate-Only › Framed

ID	Bezeichnung	Bedeutung	Mögliche Werte in LCOS
7	Framed-Protocol	Gibt an, welches Protokoll zu verwenden ist.	PPP
8	Framed-IP-Address	Gibt die dem Client zugewiesene IP-Adresse an.	<IP-Adresse des Clients>
26	Vendor 2356(LCS) Id 2	MAC-Adresse des Clients, sofern die Authentifizierung über MAC-Adresse stattfindet. Im Gegensatz zur Calling-Station-ID wird dieser Wert als ein 6-Byte Binär-String ausgegeben. Dieses Attribut existiert ausschließlich im Anmeldungsmodus **Anmeldung mit Name, Passwort und MAC-Adresse**.	<MAC-Adresse des Clients>
30	Called-Station-Id	Gibt die ID der gerufenen Station an (z. B. des VPN-Servers).	› Server-IP-Adresse (bei VPN-Verbindungen über PPTP oder L2TP) › Dienst-Name (bei PPPoE) › BSSID:SSID (bei WLAN) › MAC-Adresse des Gerätes (bei Public Spot)
31	Calling-Station-Id	Gibt die ID der rufenden Station an (z. B. des VPN-Clients).	› Client-IP-Adresse (bei VPN-Verbindungen über PPTP oder L2TP) › Client-MAC-Adresse (bei PPPoE, WLAN und Public Spot)
32	NAS-Identifier	Gibt den Namen des Gerätes an, für das der RADIUS-Server den Zugang verwaltet.	<Geräte-Name>
61	NAS-Port-Type	Gibt den physikalischen Port an, über den das Gerät den Benutzer authentifiziert.	› Virtual (bei VPN-Verbindungen über PPTP oder L2TP) › Ethernet (bei PPPoE) › Wireless-802.11 (bei WLAN)
64	Tunnel-Type	Definiert das Tunneling-Protokoll, welches für die Sitzung verwendet wird.	› 13 (VLAN; bei Public Spot)
65	Tunnel-Medium-Type	Definiert das Transportmedium, über das eine getunnelte Sitzung hergestellt wird.	› 6 (IEEE 802; bei Public Spot)
81	Tunnel-Private-Group-Id	Definiert die Gruppen-ID, falls die Sitzung getunnelt ist.	› 1-4096 (bei Public Spot)
87	NAS-Port-Id	Bezeichnung des Interfaces, über welches ein Client mit Ihrem Gerät verbunden ist. Dies kann sowohl eine physische als auch logische Schnittstelle sein.	z. B. › LAN-1 › WLAN-1-5 › WLC-TUNNEL-27
95	NAS-IPv6-Address	Gibt die IPv6-Adresse des Gerätes an, das den Zugang für einen Anwender anfragt.	<IPv6-Adresse des Gerätes>
96	Framed-Interface-ID	Das Attribut definiert den IPv6-Interface-Identifier, der für den Benutzer im IPv6CP festgelegt werden soll.	
97	Framed-IPv6-Prefix	Präfix, welches dem Benutzer über Router Advertisements übermittelt wird.	
99	Framed-IPv6-Route	Dieses Attribut definiert die Route, die für diesen Benutzer festgelegt werden soll. Das Gerät legt in der IPv6-Routing-Tabelle diese Route mit Next-Hop zu diesem Benutzer an.	

ID	Bezeichnung	Bedeutung	Mögliche Werte in LCOS
100	Framed-IPv6-Pool	Angabe des IPv6-Pools, aus dem ein Präfix für den Benutzer bereitgestellt werden soll. Der IPv6-Pool wird per Name referenziert und muss unter **IPv6** > **Router Advertisement** > **Präfix-Pool** vorhanden sein.	
123	Delegated-IPv6-Prefix	Präfix, welches dem Benutzer über DHCPv6 Präfix Delegierung übermittelt wird.	
177	Mobility-Domain-ID	Kennzeichnet die Mobility-Domain, in der sich der Client befindet.	
181	WLAN-HESSID	Enthält die HESSID der 802.11u SSID.	
182	WLAN-Venue-Info	Enthält Informationen zur Kategorie des Standortes.	Zu konfigurieren unter **Wireless-LAN** > **802.11u** > **Standortinformationen**.
183	WLAN-Venue-Language	Enthält Informationen zur Sprache des Standortes.	Zu konfigurieren unter **Wireless-LAN** > **802.11u** > **Standortinformationen**.
184	WLAN-Venue-Name	Enthält die Bezeichnung des Standortes (Standort-Name).	Zu konfigurieren unter **Wireless-LAN** > **802.11u** > **Standortinformationen**.
186	WLAN-Pairwise-Cipher	Enthält Informationen über den paarweisen Schlüssel, den Client und AP verwenden.	
187	WLAN-Group-Cipher	Enthält Informationen über den Gruppenschlüssel, den Client und AP verwenden.	
188	WLAN-AKM-Suite	Enthält Informationen über die Zugriffsverwaltung (Authentication and Key Management) zwischen Client und AP.	
189	WLAN-Group-Mgmt-Cipher	Enthält Informationen über den Gruppenverwaltungsschlüssel, der eine Verbindung über RSNA (Robust Security Network Association) zwischen AP und mobilem Client absichert.	
190	WLAN-RF-Band	Enthält Informationen über das Frequenzband, das der Client verwendet.	

Neben diesen Attributen gibt es eine schier unüberschaubare Anzahl an herstellerspezifischen Attributen. LCOS erlaubt durch eine entsprechende Definition die Verwendung dieser Attribute. Siehe *Benutzerdefinierte Attribute* auf Seite 1600

Ein Beispiel für einen PPP-Benutzer `test` mit IPv6 im FreeRADIUS lautet wie folgt:

```
test Cleartext-Password := "1234"
     Service-Type := Framed-User,
     Framed-Protocol := PPP,
     Framed-IPv6-Prefix := "fec0:1:2400:1::/64",
     Delegated-IPv6-Prefix := "fec0:1:2400:1100::/56",
     Framed-IP-Address := 172.16.3.33
```

Der Benutzer `test` erhält in einer Dual Stack PPP-Session die IPv4-Adresse `172.16.3.33`, per Router Advertisement das Präfix `fec0:1:2400:1::/64` sowie per DHCPv6-Präfix Delegation das Präfix `fec0:1:2400:1100::/56`.

Für die folgenden herstellerspezifischen RADIUS-Attribute wird die IANA Private Enterprise Number „3561“ des Broadband-Forums verwendet. Bei den übrigen Einträgen handelt es sich um LANCOM spezifische Attribute!

Tabelle 45: Übersicht aller unterstützten Hersteller spezifischen RADIUS-Attribute im Access-Request

ID	Bezeichnung	Bedeutung	Mögliche Werte in LCOS
1	ADSL-Agent-Circuit-Id, Vendor 3561	Gibt die Schnittstelle des Gerätes an, für das der RADIUS-Server den Zugang verwaltet. Wird nur übertragen, wenn Agent-Relay-Infos im PPPoED-Paket enthalten sind (siehe *PPPoE-Snooping*).	<Schnittstelle des Gerätes>
2	ADSL-Agent-Remote-Id, Vendor 3561	Gibt die Bezeichnung des Gerätes an, für das der RADIUS-Server den Zugang verwaltet. Wird nur übertragen, wenn Agent-Relay-Infos im PPPoED-Paket enthalten sind (siehe *PPPoE-Snooping*).	<Bezeichnung des Gerätes>
16	LCS-Orig-NAS-Identifier, Vendor 2356	NAS-Identifier des ursprünglichen Access Points im WLC-Betrieb.	<Geräte-Name>
17	LCS-Orig-NAS-IP-Address, Vendor 2356	NAS-IP-Adresse des ursprünglichen Access Points im WLC-Betrieb.	<IPv4-Adresse des Gerätes>
18	LCS-Orig-NAS-IPv6-Address, Vendor 2356	NAS-IPv6-Adresse des ursprünglichen Access Points im WLC-Betrieb.	<IPv6-Adresse des Gerätes>

Eine Übersicht der im Rahmen der Unterstützung von RADIUS mit IKEv2 verwendeten Attribute finden Sie unter *RADIUS-Unterstützung für IKEv2* auf Seite 912.

18.5.1 RADIUS-Attribute konfigurierbar

LCOS ermöglicht es, die RADIUS-Attribute für die Kommunikation mit einem RADIUS-Server (sowohl Authentication als auch Accounting) zu konfigurieren.

Die Angabe der Attribute erfolgt als semikolon-separierte Liste von Attribut-Nummern oder -Namen (gem. *RFC 2865*, *RFC 3162*, *RFC 4679*, *RFC 4818*, *RFC 7268*) und einem entsprechenden Wert in der folgenden Form:

`<Attribut_1>=<Wert_1>;<Attribut_2>=<Wert_2>`

Da die Anzahl der Zeichen begrenzt ist, lässt sich der Name abkürzen. Das Kürzel muss dabei eindeutig sein. Beispiele:

- `NAS-Port=1234` ist nicht erlaubt, da das Attribut nicht eindeutig ist (`NAS-Port`, `NAS-Port-Id` oder `NAS-Port-Type`).
- `NAS-Id=ABCD` ist erlaubt, da das Attribut eindeutig ist (`NAS-Identifier`).

Als Attribut-Wert ist die Angabe von Namen oder RFC-konformen Nummern möglich. Für das Gerät sind die Angaben `Service-Type=Framed` und `Service-Type=2` identisch.

Die Angabe eines Wertes in Anführungszeichen (`"<Wert>"`) ist möglich, um Sonderzeichen wie Leerzeichen, Semikolon oder Gleichheitszeichen mit angeben zu können. Das Anführungszeichen innerhalb des Wertes erhält einen umgekehrten Schrägstrich vorangestellt (`\"`), der umgekehrte Schrägstrich ebenfalls (`\\`).

Als Werte sind auch die folgenden Variablen erlaubt:

`%n`

Gerätename

`%e`

Seriennummer des Gerätes

%%

Prozentzeichen

%{name}

Original-Name des Attributes, wie ihn die RADIUS-Anwendung überträgt. Damit lassen sich z. B. Attribute mit originalen RADIUS-Attributen belegen: `Called-Station-Id=%{NAS-Identifier}` setzt das Attribut `Called-Station-Id` auf den Wert, den das Attribut `NAS-Identifier` besitzt.

18.5.2 Erweiterung der RADIUS-Attribute für IPv6-RAS-Dienste

Der RADIUS-Client kann RADIUS-Attribute wie „Framed-IP-Address" etc. von einem externen RADIUS-Server anfragen und diese dann z. B. dem PPPoE-Server zur Verfügung stellen, um diese am PPPoE-, PPTP- oder L2TP-Server zu authentifizieren. Die folgenden Attribute werden vom Gerät in Access-Accept-Nachrichten akzeptiert:

96

Framed-Interface-ID

Das Attribut definiert den IPv6-Interface-Identifier, der für den Benutzer im IPv6CP festgelegt werden soll.

97

Framed-IPv6-Prefix

Präfix, welches dem Benutzer über Router Advertisements übermittelt wird.

99

Framed-IPv6-Route

Dieses Attribut definiert die Route, die für diesen Benutzer festgelegt werden soll. Das Gerät legt in der IPv6-Routing-Tabelle diese Route mit Next-Hop zu diesem Benutzer an.

100

Framed-IPv6-Pool

Angabe des IPv6-Pools, aus dem ein Präfix für den Benutzer bereitgestellt werden soll. Der IPv6-Pool wird per Name referenziert und muss unter **IPv6** > **Router Advertisement** > **Präfix-Pool** vorhanden sein.

123

Delegated-IPv6-Prefix

Präfix, welches dem Benutzer über DHCPv6 Präfix Delegierung übermittelt wird.

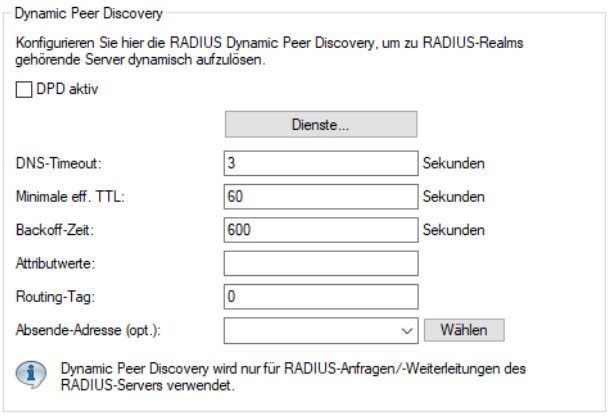
Die neu verfügbaren RADIUS-Attribute sind nach *RFC 3162* und *RFC 4818* implementiert. Ein Beispiel für einen PPP-Benutzer `test` mit IPv6 im FreeRADIUS lautet wie folgt:

```
test Cleartext-Password := "1234"
     Service-Type := Framed-User,
     Framed-Protocol := PPP,
     Framed-IPv6-Prefix := "fec0:1:2400:1::/64",
     Delegated-IPv6-Prefix := "fec0:1:2400:1100::/56",
     Framed-IP-Address := 172.16.3.33
```

Der Benutzer "test" erhält in einer Dual Stack PPP-Session die IPv4-Adresse 172.16.3.33, per Router Advertisement das Präfix fec0:1:2400:1::/64 sowie per DHCPv6-Präfix Delegation das Präfix fec0:1:2400:1100::/56.

18.6 Dynamic Peer Discovery

Unterstützung für das *RFC 7585* „Dynamic Peer Discovery for RADIUS/TLS and RADIUS/DTLS Based on the Network Access Identifier (NAI)". Statt RADIUS-Requests statisch zu einem oder mehreren RADIUS-Servern weiterzuleiten ermöglicht Dynamic Peer Discovery dynamisch anhand des Realms / NAIs den richtigen RADIUS-Server zu finden. Kommt ein Request, so wird per DNS NAPTR/SRV-Record der richtige Server gefunden.



LANconfig: **RADIUS** > **Dyn. Peer Discovery**

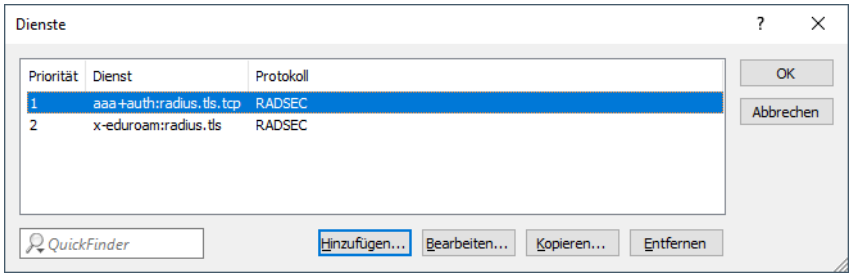
Konsole: **Setup** > **RADIUS** > **Dynamic-Peer-Discovery**

DPD aktiv

Dynamic Peer Discovery ein- bzw. ausschalten. Sobald Dynamic Peer Discovery eingeschaltet ist, verzweigt der RADIUS-Server zur dynamischen Auflösung, falls ein bestimmter Realm / NAI nicht in seiner Weiterleitungs-Tabelle definiert ist. Lokale Definitionen für Realms haben also immer Vorrang.

Dienste

Tabelle mit den Diensten. Der Dienst ist das, was in der NAPTR-Antwort im Service geliefert wird. Es werden alle NAPTR-Einträge extrahiert und weiter aufgelöst, die als Service den mit der höchsten Priorität aus dieser Tabelle haben. Werden mit der Default-Einstellung z. B. NAPTR-Records für beide Service-Typen geliefert, so werden die für „x-eduroam:radius.tls" ignoriert. Die Tabelle wird vom LCOS automatisch sortiert, so dass höher priorisierte Services weiter oben stehen. Das Protokoll, das zu so einem Server genutzt werden muss (RADIUS oder RADSEC), wird explizit vorgegeben. Für den Fall, daß die NAPTR-Anfrage keine verwendbaren Records liefert, hat diese Tabelle noch die Bedeutung, welcher Präfix dem NAI für die Fallback-SRV-Anfrage vorangestellt wird. Es wird der höchspriorisierte Eintrag aus der Tabelle genommen, für den in einer intern fix definierten Tabelle ein Präfix definiert ist. Aktuell sind die Services radius.tls, radius.tls.tcp, radsec.tcp und radius.udp definiert, die auf ein Präfix von _radiustls._tcp., _radsec.tcp. bzw. _radius._udp. mappen.



Priorität

Die Priorität dieses Dienstes.

Dienst

Die Dienste selbst. Voreingestellt sind „aaa+auth:radius.tls.tcp“ und „x-eduroam:radius.tls“.

Protokoll

Das Protokoll (RADIUS oder RADSEC), das zu diesem Dienst genutzt wird.

DNS-Timeout

Die Zeitspanne in Sekunden, innerhalb der alle DNS-Anfragen für einen NAI abgehandelt sein müssen. Das schließt auch die zweistufige Variante über NAPTR- und nachfolgende SRV-Anfragen ein. Default: 3 Sekunden

Minimale eff. TTL

Vom DNS-Server gemeldete TTL-Werte, die kürzer als diese Zeit sind, werden auf diesen Wert angehoben. Default: 60 Sekunden

Backoff-Zeit

Falls eine Auflösung in einem Fehler endet (DNS-Antwort mit Fehler, Timeout…), ist dies die Zeit in Sekunden, für die keine neuen Auflöseversuche für diesen Realm gemacht werden sollen. Default: 600 Sekunden

Attributwerte

RADIUS-Attribute, die bei Weiterleitungen an per Dynamic Peer Discovery ermittelte Server hinzugefügt oder geändert werden sollen.

Routing-Tag

Das Routing-Tag, welches Dynamic Peer Discovery für seine DNS-Anfragen nutzen soll. Default: 0

Abesende-Adresse (opt.)

Die Loopback-Adresse, die bei den Weiterleitungen der per Dynamic Peer Discovery ermittelten RADIUS-Server benutzt werden soll.

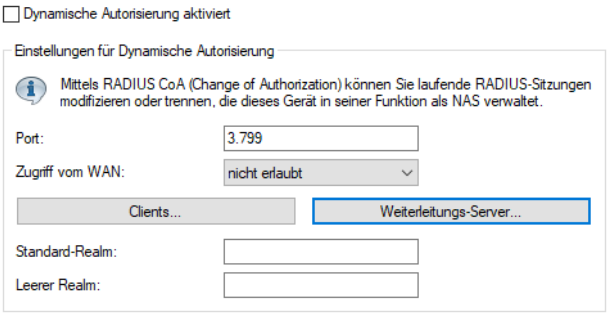
18.7 Dynamische Autorisierung durch RADIUS CoA (Change of Authorization)

Mit der dynamischen Autorisierung ist es möglich, aktuelle RADIUS-Sitzungen zu bearbeiten. Dazu übermittelt der jeweilige CoA Client eine CoA Nachricht an das NAS. Diese Nachricht enthält neben der identifizierenden Merkmale für die Session, die Sie ändern möchten, die zu bearbeitenden Attribute und deren neue Werte.

Zudem besteht die Möglichkeit, die jeweilige Sitzung zu trennen. Dies erfolgt durch eine Disconnect Message (DM), die an das NAS gesendet wird – das NAS trennt daraufhin die gewünschte Verbindung.

18.7.1 Dynamische Autorisierung mit LANconfig konfigurieren

Um die dynamische Autorisierung (CoA) mit LANconfig zu konfigurieren, öffnen Sie die Ansicht **RADIUS** > **Dyn. Autorisierung**.



Dynamische Autorisierung aktiviert

Hier aktivieren oder deaktivieren Sie die dynamische Autorisierung.

Port

Enthält den Standard-Port, auf dem CoA-Nachrichten angenommen werden.

Zugriff vom WAN

Dieser Eintrag legt fest, ob Nachrichten vom WAN zugelassen sind, nur über VPN angenommen werden oder verboten sind.

Clients

Tragen Sie hier alle CoA-Clients ein, die Nachrichten an das NAS senden dürfen.

Weiterleitungs-Server

Sollen CoA-Nachrichten weitergeleitet werden, ist es erforderlich, die Weiterleitungen hier anzugeben.

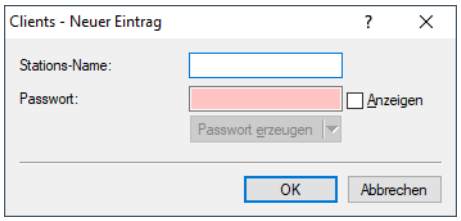
Standard-Realm

Dieser Realm gilt alternativ, wenn der übermittelte Benutzername einen unbekannten Realm verwendet, der nicht in der Liste der Weiterleitungs-Server enthalten ist.

Leerer Realm

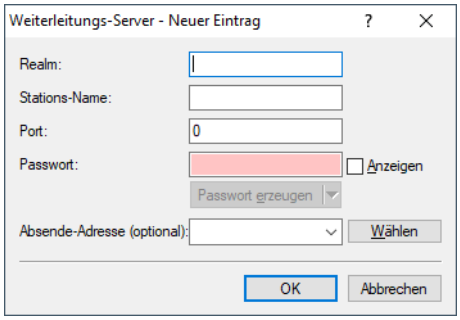
Dieser Realm gilt alternativ, wenn der übermittelte Benutzername keinen Realm enthält.

Um CoA-Clients für die dynamische Autorisierung hinzuzufügen, klicken auf die Schaltfläche **Clients** und fügen Sie der Tabelle einen neuen Eintrag hinzu.



Tragen Sie einen Stationsnamen für den Client ein und definieren Sie ein Passwort, das der Client für den Zugang zum NAS benötigt.

Um neue Weiterleitungs-Server für die dynamische Autorisierung hinzuzufügen, klicken Sie auf die Schaltfläche **Weiterleitungs-Server** und fügen Sie der Tabelle einen neuen Eintrag hinzu.



Realm

Tragen Sie hier den Realm ein, mit dem der RADIUS-Server das Weiterleitungs-Ziel identifiziert.

Verwenden Sie ggf. bereits vorhandene Weiterleitungs-Server, die unter **RADIUS** > **Server** > **Erweiterte Einstellungen** > **Weiterleitung** > **Weiterleitungs-Server** definiert sind.

Stations-Name

Geben Sie den Hostnamen des Weiterleitungs-Servers an.

Port

Legen Sie den Port des Servers fest, über den die Anfragen weitergeleitet werden.

Passwort

Legen Sie ein Passwort fest, das der Client für den Zugang zum RADIUS-Server benötigt.

Absende-Adresse (optional)

Geben Sie optional eine Absendeadresse an.

Legen Sie fest, welche logischen WLAN-Schnittstellen die dynamische Autorisierung verwenden dürfen. Aktivieren oder deaktivieren Sie hierfür im Reiter "Netzwerk" unter **Wireless-LAN** > **Allgemein** > **Logische WLAN-Einstellungen** > **Netzwerk** beim jeweiligen Interface die Checkbox **RADIUS CoA aktiviert**.

18.8 RADSEC

RADIUS hat sich als Standard für serverbasierte Authentifizierung, Autorisierung und Abrechnung etabliert. Mittlerweile wird RADIUS z. B. im Zusammenspiel mit EAP/802.1X in Anwendungen eingesetzt, für die es ursprünglich nicht entwickelt wurde, und weist daher einige Mängel auf:

- RADIUS läuft über UDP und bietet daher kein natives Verfahren zur Prüfung von Paketverlusten. Dieser Aspekt ist in einer LAN-Umgebung nicht problematisch, gewinnt aber bei Übertragungen über WAN-Strecken oder das Internet an Bedeutung.
- RADIUS verfügt nur über einfache Verfahren zur Authentifizierung über ein „Shared Secret“ und nur über geringe Vertraulichkeit.

Mit RADSEC steht ein alternatives Protokoll zur Verfügung, welches die RADIUS-Pakete durch einen TLS-verschlüsselten Tunnel überträgt. TLS setzt auf TCP auf und bringt somit einen erprobten Mechanismus zur Überwachung verlorener Pakete mit. Ausserdem verfügt TLS über hohe Vertraulichkeit und ein Verfahren zur gegenseitigen Authentifizierung über X.509-Zertifikate.

18.8.1 Konfiguration von RADSEC für den Client

18.8.1.1 Gerät als RADIUS-Client

In der Funktion als RADIUS-Client wird ein Gerät auf die Verwendung von RADIUS über UDP oder RADSEC über TCP mit TLS eingestellt. Zusätzlich wird der zu verwendende Port angegeben: 1812 für Authentifizierung über RADIUS, 1813 für die Abrechnung über RADIUS und 2083 für RADSEC.

Die Auswahl des RADSEC-Protokolls kann an allen Stellen vorgenommen werden, an denen ein Gerät als RADIUS-Client konfiguriert wird.

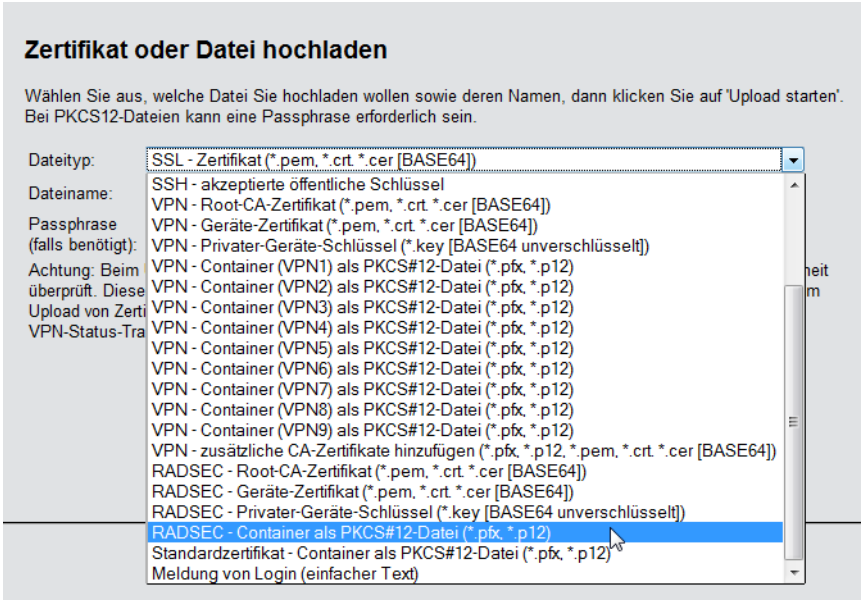
18.8.1.2 Gerät als RADIUS-Server

Arbeitet ein Gerät selbst als RADIUS-Server, kann der RADSEC-Port konfiguriert werden, auf dem der Server RADSEC-Anmeldungen erwartet. Darüber hinaus kann für alle RADIUS-Clients in der Client-Liste das zu verwendende Protokoll (RADIUS, RADSEC oder alle) eingestellt werden. Auf diese Weise kann z. B. auf der einen Seite RADIUS für die Clients im LAN eingesetzt werden. Zusätzlich kann dann die zuverlässigere RADSEC-Variante über TCP für externe Anmeldungen über das Internet genutzt werden.

18.8.2 Zertifikate für RADSEC

Für die TLS-Verschlüsselung der RADSEC-Verbindung werden separate X.509-Zertifikate benötigt. Die einzelnen Zertifikate (Root-Zertifikat, Geräte-Zertifikat und privater Schlüssel) können entweder einzeln oder als PKCS#12-Container in das Gerät geladen werden.

WEBconfig: **Zertifikat oder Datei hochladen**



19 IoT – Das Internet der Dinge (Internet of Things – IoT)

Hier finden Sie die Einstellungen für vom LCOS unterstützte IoT-Technologien wie z. B. Wireless ePaper, iBeacon und Bluetooth Low Energy.

Beim IoT werden physische und virtuelle Gegenstände miteinander vernetzt und entstehende Daten und Informationen ausgetauscht. Sensoren, smarte Hausgeräte, digitale Raumbeschilderung oder auch elektronische Preisschilder im Einzelhandel sind typische Beispiele. Die Vernetzung von IoT-Geräten geschieht meist über Funk, zum Einsatz kommen die unterschiedlichsten Funktechnologien wie modifizierte ZigBee-Varianten (Retail IoT), Bluetooth Low Energy (BLE) oder diverse Mobilfunk-Ableger. Einen einheitlichen „IoT-Funkstandard" gibt es nicht, zudem tauchen in kurzen Zyklen neue IoT-Funktechnologien auf.

Die speziellen Einstellungen für IoT erfolgen in LANconfig unter **IoT**.

19.1 Wireless ePaper

LANCOM Wireless ePaper Displays bieten Ihnen vielfältige Möglichkeiten zur Anzeige von Informationen – aktualisieren Sie den Belegungsplan Ihres Konferenzraums automatisch und aus der Ferne, erstellen Sie dynamische Wegweiser und Hinweisschilder oder regulieren Sie die Preise Ihrer Waren zentral und in Echtzeit. Die umfangreichen Einstellungsmöglichkeiten erlauben eine individuelle Anpassung an Ihren persönlichen Anwendungsfall.

Die speziellen Einstellungen für den Betrieb der Wireless ePaper Displays erfolgen in LANconfig unter **Extras** > **Optionen** > **Wireless ePaper**. Unter IP/Hostname tragen Sie die IP des Wireless ePaper Servers sowie den zugehörigen Port ein. Der einzustellende Port ist die 8001.

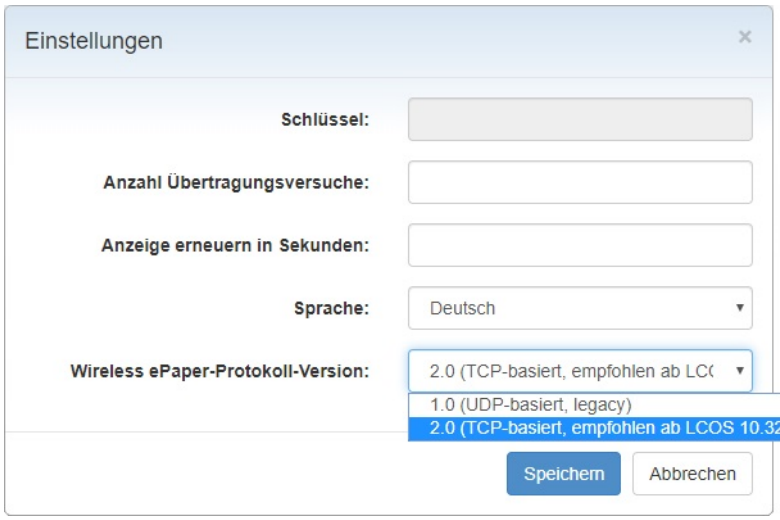
Die Wireless ePaper-Verwaltung starten Sie aus LANconfig über **Extras** > **Wireless ePaper-Verwaltung starten**.

Zentrale Verwaltung Ihrer Wireless ePaper-Infrastruktur

Ab LCOS 10.32 unterstützen die LANCOM Access Points mit Wireless ePaper-Unterstützung ein neues Protokoll, welches eine effizientere und zuverlässigere Kommunikation zwischen Wireless ePaper Server und Access Point gewährleistet. Dank der Unterstützung dieses neuen Protokolls können Sie Ihre LANCOM Wireless ePaper Displays nun auch remote über den Wireless ePaper Server in der Zentrale managen und über VPN ansteuern. Wenn beide Seiten das neue Protokoll unterstützen und es im Wireless ePaper Server aktiviert wurde, wird das neue Protokoll verwendet.

Ab LCOS 10.40 unterstützen die LANCOM Access Points mit Wireless ePaper-Unterstützung eine Erweiterung des TCP-Protokolls, welches den Verbindungsaufbau (Wireless ePaper Access Point bzw. Router mit USB-Schnittstelle und Wireless ePaper USB-Stick) zum Wireless ePaper Server zulässt und die Verbindung mittels TLS verschlüsselt. Um diese Erweiterung einzusetzen sind sowohl der Wireless ePaper Server als auch auf das Wireless ePaper-Gerät (Access Point bzw. Router mit Wireless ePaper USB) zu konfigurieren.

In der rechten, oberen Ecke der Wireless ePaper-Verwaltung können Sie auf das Zahnrad-Symbol und dann **Einstellungen** klicken, um allgemeine Einstellungsmöglichkeiten zum Wireless ePaper Server zu erreichen. Dort können Sie das neue Protokoll aktivieren.



Im LANmonitor in der Anzeige des entsprechenden Gerätes unter **IoT** > **Wireless ePaper** > **Protokollversion** wird das verwendete Protokoll angezeigt:

- Keine – Es besteht keine Verbindung zu einem Controller / Server
- ThinAP1.0/UDP – Protokollversion 1.0 (UDP-basiert, legacy)
- ThinAP2.0/TCP – Protokollversion 2.0 (TCP-basiert, ab LCOS 10.32)

Aktivierung eines TCP-basierten Protokolls auf dem Wireless ePaper Server

Der Wireless ePaper Server unterstützt „Protokollversion 2.0“ ab Version 1.91 und ab Version 1.101 die darauf aufbauende TLS-Verschlüsselung. Falls Sie einen unterstützten Wireless ePaper Server bereits einsetzen und trotzdem hier nur „Protokollversion 1.0“ oder ab Version 1.101 nur „Protokollversion 2.0“ sehen, dann wurde ggf. das Protokoll in den Einstellungen des Wireless ePaper Servers nicht aktiviert. In diesem Fall müssen Sie die Protokollversion erst aktivieren.

Gehen Sie wie folgt vor, um „Protokollversion 2.0 (ThinAP2.0/TCP)“ zu aktivieren:

1. Überprüfen Sie die folgenden Voraussetzungen:
   - LANCOM Wireless ePaper Server in der Version 1.91 oder höher ist installiert
   - cURL ist installiert
2. Öffnen Sie in Ihrem Betriebsystem eine Kommandozeile und geben Sie den folgenden Befehl ein:

   ```
   curl -X PUT http://<server-ip>:8001/service/configuration/lancomUseTcpThinMode?value=true
   ```
3. Starten Sie den Wireless ePaper Server neu.
4. Geben Sie anschließend den folgenden Befehl ein, um zu überprüfen, ob die Aktivierung erfolgreich war:

   ```
   curl -X GET http://<server-ip>:8001/service/configuration/lancomUseTcpThinMode
   ```

Eine erfolgreiche Aktivierung liefert die Ausgabe:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Configuration key="lancomUseTcpThinMode" type="BOOLEAN" defaultValue="false" value="true"/>
```

Gehen Sie wie folgt vor, um „Protokollversion 2.0 (ThinAP2.0/TLS)“ zu aktivieren:

1. Überprüfen Sie die folgenden Voraussetzungen:
   - LANCOM Wireless ePaper Server in der Version 1.101 oder höher ist installiert
   - cURL ist installiert
   - „Protokollversion 2.0 (ThinAP2.0/TCP)“ ist aktiviert

› Die Wireless ePaper Server Adresse ist im Wireless ePaper unterstützenden Gerät konfiguriert.

Der LANCOM Wireless ePaper Server muss die Verbindung annehmen bzw. das Wireless ePaper unterstützende Gerät muss die Verbindung aufbauen, daher ist auch das Gerät zu konfigurieren.

2. Öffnen Sie in Ihrem Betriebsystem eine Kommandozeile und geben Sie die folgenden Befehle ein:

```
curl -X PUT http://<server-ip>:8001/service/configuration/accessPointUseThinMode?value=true
curl -X PUT http://<server-ip>:8001/service/configuration/lancomUseTcpThinOutboundMode?value=true
curl -X PUT http://<server-ip>:8001/service/configuration/accessPointThinUseOutboundMode?value=true
```

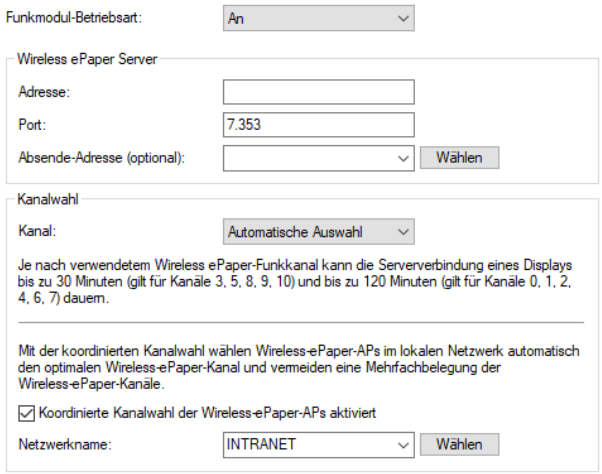
3. Starten Sie den Wireless ePaper Server neu.
4. Geben Sie anschließend analog zur Überprüfung beim TCP-Protokoll alle drei Parameter mit „GET“ als Befehl ein, um zu überprüfen, ob die Aktivierung erfolgreich war. Als Ausgabe muss jeweils „`value="true"`“ angezeigt werden

Um die Funktion zu deaktivieren sind auf der Kommandozeile die Befehle mit dem Parameter „`value=false`“ anstelle des Parameters „`value=true`“ aufzurufen. Der Befehl sieht dann z. B. so aus:

```
curl -X PUT http://<server-ip>:8001/service/configuration/lancomUseTcpThinMode?value=false
```

19.1.1 Einstellungen für Wireless ePaper

Aktivieren Sie das Wireless ePaper-Funkmodul in LANconfig unter **IoT** > **Wireless ePaper**.



Funkmodul-Betriebsart

Wählen Sie hier die grundsätzliche Betriebsart Ihres Wireless ePaper Funkmoduls:

Managed (via WLC)

In dieser Betriebsart wird das Funkmodul des Gerätes von einem zentralen WLAN-Controller (WLC) konfiguriert. Hier gemachte Einstellungen werden dadurch überstimmt.

An (autonom)

Das Funkmodul des Gerätes ist eingeschaltet und arbeitet autonom.

Aus

Das Funkmodul des Gerätes ist ausgeschaltet.

Wireless ePaper Server

Ab LCOS 10.40 unterstützen die LANCOM Access Points mit Wireless ePaper-Unterstützung eine Erweiterung des TCP-Protokolls, welches den Verbindungsaufbau (Wireless ePaper Access Point bzw. Router mit USB-Schnittstelle und Wireless ePaper USB-Stick) zum Wireless ePaper Server zulässt und die Verbindung mittels TLS verschlüsselt. Dazu muss auf dem Wireless ePaper Server das Protokoll ThinAP2.0/TLS eingerichtet sein (siehe *Aktivierung eines TCP-basierten Protokolls auf dem Wireless ePaper Server* auf Seite 1612) und die IP-Adresse des Wireless ePaper Servers hier angegeben werden.

Adresse

IP-Adresse des Wireless ePaper Servers.

Port

Hier stellen Sie den Port zur Kommunikation zwischen Wireless ePaper-Gerät, z. B. Access Point oder Router, und Wireless ePaper Server ein. Der Default-Port ist 7353 für den Verbindungsaufbau vom Wireless ePaper Server zum Wireless ePaper-Gerät. Wenn der Verbindungsaufbau vom Wireless ePaper-Gerät zum Wireless ePaper Server mittels TLS erfolgen soll, dann stellen Sie den Port 7354 ein.

Absende-Adresse

Geben Sie hier die Loopback-Adresse an.

Kanalwahl

Entweder lassen Sie das Funkmodul automatisch einen Kanal auswählen oder geben einen festen Kanal vor.

Koordinierte Kanalwahl

Die koordinierte Kanalwahl benötigen Sie insbesondere dann, wenn Sie mit mehreren Wireless ePaper Access Points innerhalb eines Standorts arbeiten.

Da jeder Access Point einen eigenen ePaper-Kanal benötigt, darf es nicht zu Kollisionen / Mehrfachbelegungen kommen.

Daher ermitteln die ePaper Access Points innerhalb einer Broadcast-Domain automatisch über ein auf TCP basierendem Protokoll, welches in einer Multicast-Gruppe übertragen wird, benachbarte ePaper Access Points. Aus diesen Access Points wird automatisch ein Master-AP bestimmt. Die übrigen Access Points werden zu Slave-APs. Fällt der Master-AP aus, wird automatisch einer der Slave-APs zum Master-AP ernannt.

Die Slave-APs übermitteln dem Master-AP regelmäßig eine Beurteilung des aktuellen ePaper-Kanals. Der Master entscheidet daraufhin unter Berücksichtigung der Beurteilungen sämtlicher Slaves, ob ein Kanalwechsel des Slaves stattfinden muss oder nicht.

Der ePaper-AP erstellt eine Beurteilung aller ePaper-Kanäle. Dabei wird sowohl der lokal verwendete WLAN-Kanal (den der ePaper-Kanal nicht überlappen sollte) berücksichtigt, als auch, ob es sich bei dem ePaper-Kanal um einen bevorzugten Kanal handelt.

Bevorzugte Kanäle sind: 3,5,8,9 und 10.

Anhand der erhaltenen Kanalbeurteilungen wird eine Optimierung der ePaper-Kanäle folgendermaßen erreicht:

Der Master-AP wählt aus den noch nicht vergebenen Kanälen denjenigen mit der besten Bewertung aus und weist ihn dem ePaper-AP mit der niedrigsten ePaper-AP-ID zu. Der Master weist sich selbst ebenfalls einen Kanal zu. Dies wird sukzessive für alle ePaper-APs fortgeführt.

Bei einer Neuverteilung wird ein Kanal nur gewechselt, wenn die Bewertung des konkurrierenden Kanals um einen konfigurierbaren Threshold besser ist. Auf diese Weise werden unnötige Kanalwechsel vermieden.

Gibt es im Netzwerk ePaper-APs mit statisch zugewiesenem ePaper-Kanal, so kann die koordinierte Kanalwahl trotzdem durchgeführt werden. Ist diese auch auf dem Access Point mit statischem Kanal eingeschaltet, wird

der Master bei der Kanalzuweisung beachten, dass dieser Kanal bereits vergeben ist und ihn keinem anderen Access Point zuweisen.

Das Status-Menü des Features Wireless ePaper enthält eine Peer-Tabelle. In dieser werden die über die Kanal-Koordinierung erfassten Access Points aufgelistet.

Die Peer-Tabelle enthält die ePaper-AP-ID, die Rolle des Access Points (Slave oder Master), die Kanalbeurteilung sowie den zugewiesenen ePaper-Kanal.

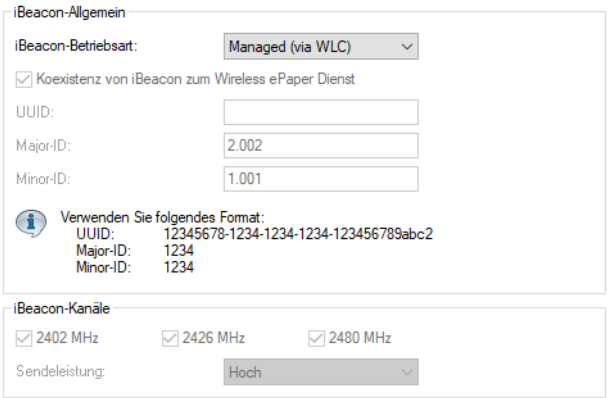
Die Kanalbeurteilung ist als Liste der ePaper-Kanäle 0 bis 10 dargestellt, dahinter jeweils die Beurteilung. Der Wertebereich beträgt 0 bis 255, wobei ein höherer Wert einer besseren Bewertung entspricht.

```
root@LN-830E PM:/Status/Wireless-ePaper
> ls -a Channel-Coordination/Peer-Table/

ID    State    IP-Address    Rtg-Tag  Connected  Assessment  Assignment
==============-------------------------------------------------------------
66122  SLAVE  172.16.26.7      1        Yes       0:108|1:096|2:073|3:196
66123  MASTER 172.16.26.6      1        No                  3
66124  SLAVE  172.16.26.8      1        Yes       0:127|1:127|2:127:3:255
```

19.2 iBeacon

Beacon bedeutet Leuchtfeuer und dieser Begriff beschreibt im Prinzip die Funktion von iBeacons. iBeacon basiert auf einem Sender-Empfänger-Prinzip. Dazu werden im Raum kleine Sender (Beacons) als Signalgeber platziert, die in festen Zeitintervallen Signale senden. Kommt ein Empfänger – z. B. ein Smartphone mit einer installierten App, die für den Empfang von iBeacon Signalen konfiguriert ist – in die Reichweite eines Senders, kann die Universally Unique Identifier (UUID) des Senders identifiziert und seine Signalstärke gemessen werden. Sind mindestens drei Beacons in Reichweite des Endgeräts, lässt sich die Position des Empfängers im zweidimensionalen Raum errechnen. Zur Ermittlung eines Standortes in einem dreidimensionalen Raum sind vier Beacons in Reichweite erforderlich. iBeacons können selber keine Push-Benachrichtigungen auf Empfangsgeräte senden, Nutzerdaten sammeln oder speichern. Sie senden lediglich Informationen zur eigenen Identität (die Werte UUID, Major und Minor). Die Datenübertragung geschieht hierbei über Bluetooth Low Energy (BLE), welches extrem stromsparend arbeitet. Zudem können abhängig vom Standort gezielt Informationen auf dem Smartphone angezeigt werden. iBeacon-Module erreichen eine Reichweite von bis zu 30 Metern und zeichnen sich durch einen geringen Stromverbrauch aus.

Die Einstellungen für iBeacon bei Geräten der E-Serie erfolgen in LANconfig unter **IoT** > **iBeacon**.



iBeacon-Betriebsart

Wählen Sie hier die grundsätzliche Betriebsart Ihres iBeacon-Funkmoduls:

Managed (via WLC)

In dieser Betriebsart wird das Funkmodul des Gerätes von einem zentralen WLAN-Controller (WLC) konfiguriert. Hier gemachte Einstellungen werden dadurch überstimmt.

An (autonom)

Das Funkmodul des Gerätes ist eingeschaltet und arbeitet autonom.

Aus

Das Funkmodul des Gerätes ist ausgeschaltet.

Koexistenz von iBeacon zum Wireless ePaper Dienst

Legen Sie hier fest, ob iBeacon parallel mit dem Wireless ePaper Dienst betrieben werden soll.

UUID

Weisen Sie dem iBeacon-Modul einen „Universally Unique Identifier" (UUID) zu.

Major-ID

Weisen Sie dem iBeacon-Modul eine eindeutige Major-ID zu.

Minor-ID

Weisen Sie dem iBeacon-Modul eine eindeutige Minor-ID zu.

iBeacon-Kanäle

Wählen Sie hier die Kanäle, auf denen das iBeacon ausgestrahlt werden soll.

Sendeleistung

Wählen Sie hier die Sendeleistung. Die genaue Bedeutung der auswählbaren Werte ist in der iBeacon-Spezifikation erläutert. Folgende Werte sind möglich:

Hoch

Das Modul sendet mit maximaler Leistung (Default).

Mittel

Das Modul sendet mit durchschnittlicher Leistung.

Gering

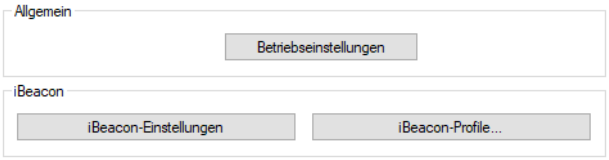
Das Modul sendet mit minimaler Leistung.

19.3 BLE-Scanner und -Beacon

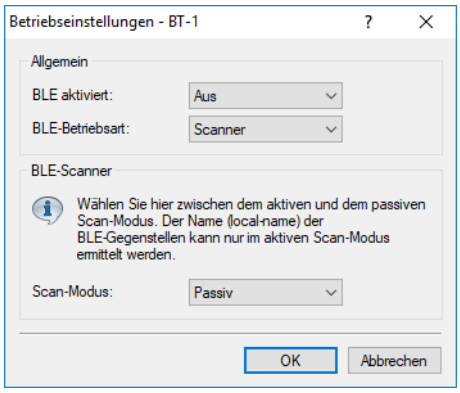
WLAN-Geräte der B-Serie verfügen über Bluetooth Low Energy-Unterstützung (BLE) für folgende Technologien: Aussenden von Beacons wie z. B. iBeacon sowie das Scannen der BLE-Umgebung, wodurch zusammen mit einem geeigneten Auswertungssystem Anwendungsfälle wie Asset Tracking oder Besucherzählung ermöglicht werden.

19.3.1 Einstellungen für BLE

Die Einstellungen für Bluetooth LE erfolgen in LANconfig unter **IoT** > **Bluetooth LE**.



Betriebseinstellungen



BLE aktiviert

Aktivieren Sie hier das BLE-Modul.

BLE-Betriebsart

Dieser Eintrag bietet Ihnen die Möglichkeit, die Betriebsart des BLE-Moduls einzustellen. Wählen Sie, ob die Bluetooth-Schnittstelle zum Aussenden von Beacons, oder zum Scannen der Umgebung verwendet werden soll.

Ein gleichzeitiger Betrieb der beiden Betriebsarten ist nicht möglich.

Scanner

Das BLE-Modul wird für den Umgebungsscan verwendet.

BLE-Beacon

Das BLE-Modul sendet Beacons aus.

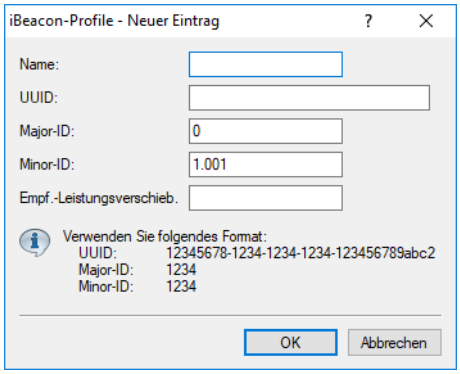
Scan-Modus

Wählen Sie hier, ob aktiv oder passiv gescannt werden soll. Beim aktiven Scan werden aktiv Scan Requests gesendet, welche die BLE-Clients in der Umgebung beantworten. Dies ist z. B. notwendig, um Namen der Clients zu ermitteln.

Beachten Sie, dass sich das ständige Beantworten der Scan Requests auf die Batterielaufzeit der Clients auswirken kann. Beim passiven Scan werden keine Scan Requests gesendet, sondern lediglich passiv gelauscht.

iBeacon-Profile

Definieren Sie Profile, welche Sie dann bei einem BLE-Interface zuordnen können.



Name

Geben Sie dem iBeacon-Profil einen Namen.

UUID

Ein 16 Byte langer Identifikator, der dazu dient, größere Gruppen von Beacons zusammenzufassen. Beispielhaft könnten alle iBeacons eines Unternehmens die gleiche iBeacon-UUID haben.

Major-ID

Ein 2 Byte langer Identifikator, der dazu dient, Untergruppen von iBeacons zu unterscheiden. Beispielhaft könnten alle iBeacons einer Filiale eines Unternehmens den gleiche Major-Identifikator haben.

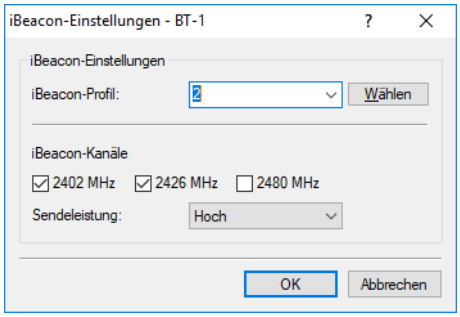
Minor-ID

Ein 2 Byte langer Identifikator, der dazu dient, einzelne iBeacons unterscheiden zu können. Beispielhaft könnte jedes einzele iBeacon in einer Filiale einen eigenen Minor-Identifikator haben.

Empfangsleistungsverschiebung

Normalerweise wird ein entsprechend der eingestellten Sendeleistung gemessener Leistungswert verwendet, um die Annäherung und exakte Entfernung von Geräten zu erkennen, die einen Beacon aussenden. Auf Basis vom entsprechenden Messreihen kann eine Abweichung zwischen gemessener Empfangsleistung und tatsächlicher Entfernung des Gerätes, welches den Beacon aussendet, festgestellt werden. Auf Basis dieser Abweichung kann hier von Experten eine Verschiebung des Referenzwertes des Gerätes angegeben werden, um die Messgenauigkeit zu erhöhen.

iBeacon-Einstellungen



iBeacon-Profil

Wählen Sie hier das iBeacon-Profil aus, um u. a. UUID, Major-ID und Minor-ID zu bestimmen.

iBeacon-Kanäle

Wählen Sie hier die Kanäle, auf denen das iBeacon ausgestrahlt werden soll.

Sendeleistung

Wählen Sie hier die Sendeleistung. Die genaue Bedeutung der auswählbaren Werte ist in der iBeacon-Spezifikation erläutert. Folgende Werte sind möglich:

Hoch

Das Modul sendet mit maximaler Leistung (Default).

Mittel

Das Modul sendet mit durchschnittlicher Leistung.

Gering

Das Modul sendet mit minimaler Leistung.

19.3.2 Monitoring

19.3.2.1 Monitoring auf der Kommandozeile

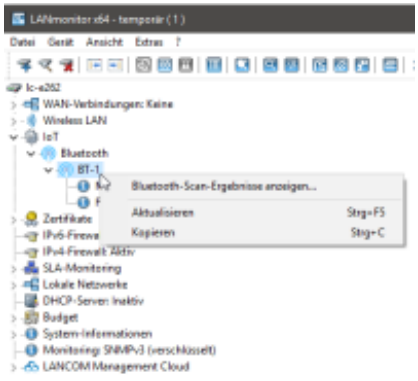
Im Scanning-Modus können die Scan-Ergebnisse in der Tabelle **Status** > **IoT** > **Bluetooth** > **Scan-Resultate** eingesehen werden.

Beachten Sie, dass die iBeacon betreffenden Werte nur gefüllt sind, wenn es sich bei dem gescannten Client tatsächlich um ein iBeacon handelt.

Zur Realisierung der meisten Anwendungsfälle, z. B. Asset Tracking, müssen diese Werte durch ein externes System ausgelesen werden. Hierzu können die üblichen Standardmethoden zum Zugriff auf LANCOM Geräte, vorzugsweise SNMP, verwendet werden.

19.3.2.2 Monitoring via LANmonitor

Im Scanning-Modus können die Scan-Ergebnisse im LANmonitor in Tabellenform eingesehen werden. Die Scanergebnis-Tabelle ist über das Kontextmenü des entsprechenden Bluetooth-Moduls erreichbar:



Beachten Sie, dass die iBeacon betreffenden Werte nur gefüllt sind, wenn es sich bei dem gescannten Client tatsächlich um ein iBeacon handelt.

Zur Realisierung der meisten Anwendungsfälle, z. B. Asset Tracking, müssen diese Werte durch ein externes System ausgelesen werden. Hierzu können die üblichen Standardmethoden zum Zugriff auf LANCOM Geräte, vorzugsweise SNMP, verwendet werden.

20 Weitere Dienste

Ein Gerät bietet eine Reihe von Diensten für PCs im LAN an. Es handelt sich dabei um zentrale Funktionen, die von Arbeitsplatzrechnern genutzt werden können. Im Einzelnen handelt es sich u. a. um:

- Automatische Adressverwaltung mit DHCP
- Namensverwaltung von Rechnern und Netzen mit DNS
- Protokollierung von Netzverkehr mit SYSLOG
- Gebührenerfassung
- Zeit-Server

20.1 Automatische IP-Adressverwaltung mit DHCP

20.1.1 Einleitung

20.1.1.1 DHCP-Server

Für einen reibungslosen Betrieb in einem TCP/IP-Netzwerk benötigen alle Geräte in einem lokalen Netzwerk eindeutige IP-Adressen. Zusätzlich brauchen sie noch die Adressen von DNS-Servern sowie eines Standard-Gateways, über das Datenpakete von lokal nicht erreichbaren Adressen geroutet werden sollen.

Bei einem kleinen Netzwerk ist es durchaus noch denkbar, diese Adressen bei allen Rechnern im Netz manuell einzutragen. Bei einem großen Netz mit vielen Arbeitsplatzrechnern wird das jedoch leicht zu einer unüberschaubaren Aufgabe. In solchen Fällen bietet sich die Verwendung des DHCP (Dynamic Host Configuration Protocol) an. Über dieses Protokoll kann ein DHCP-Server in einem TCP/IP-basierten LAN den einzelnen Stationen die benötigten Adressen dynamisch zuweisen.

Die Geräte verfügen über einen eingebauten DHCP-Server, der die Zuweisung der IP-Adressen im LAN übernehmen kann. Dabei teilt er den Arbeitsplatzrechnern u. a. die folgenden Parameter mit:

- IP-Adresse
- Netzmaske
- Broadcast-Adresse
- Standard-Gateway
- DNS-Server
- Gültigkeitsdauer der zugewiesenen Parameter

Damit der DHCP-Server den Rechnern im Netz IP-Adressen zuweisen kann, muss er zunächst einmal wissen, welche Adressen er für diese Zuweisung verwenden darf. Für die Auswahl der möglichen Adressen gibt es drei verschiedene Optionen:

- Die IP-Adresse kann aus dem eingestellten Adress-Pool genommen werden (Start-Adress-Pool bis Ende-Adress-Pool). Hier können beliebige im jeweiligen IP-Netzwerk gültige Adressen eingegeben werden.
- Wird stattdessen „0.0.0.0" eingegeben, so ermittelt der DHCP-Server selbstständig die jeweiligen Adressen (Start bzw. Ende) aus den Einstellungen für das IP-Netzwerk (Netzadresse und Netzmaske).
- Wenn in dem Gerät noch keine IP-Netzwerke definiert sind, befindet es sich in einem besonderen Betriebszustand. Es verwendet dann selbst die IP-Adresse „172.23.56.254" und den Adress-Pool „172.23.56.x" für die Zuweisung der IP-Adressen im Netz.

Wenn nun ein Rechner im Netz gestartet wird, der mit seinen Netzwerk-Einstellungen über DHCP eine IP-Adresse anfordert, wird ihm ein Gerät mit aktiviertem DHCP-Server die Zuweisung einer Adresse anbieten. Als IP-Adresse wird dabei eine

gültige Adresse aus dem Pool genommen. Wurde dem Rechner in der Vergangenheit bereits eine IP-Adresse zugewiesen, so fordert er eben diese Adresse wieder an, und der DHCP-Server versucht ihm diese Adresse wieder zuzuweisen, wenn sie nicht bereits einem anderen Rechner zugewiesen wurde.

Der DHCP-Server prüft zusätzlich, ob die ausgesuchte Adresse im lokalen Netz noch frei ist. Sobald die Eindeutigkeit einer Adresse festgestellt wurde, wird dem anfragenden Rechner die gefundene Adresse zugewiesen.

Im einfachsten Fall müssen Sie nur das neue Gerät im Auslieferungszustand in einem Netz ohne andere DHCP-Server anschließen und einschalten. Der DHCP-Server regelt im Zusammenspiel mit LANconfig über einen Assistenten dann alle weiteren Adresszuweisungen im lokalen Netz selbst.

Die DHCP-Einstellungen können für jedes Netzwerk unterschiedlich sein. Im Zusammenhang mit dem Advanced Routing and Forwarding (ARF) können in LCOS mehrere IP-Netzwerke definiert werden. Die DHCP-Einstellungen beziehen sich daher – bis auf einige allgemeine Einstellungen – auf ein bestimmtes IP-Netzwerk.

20.1.1.2 DHCP-Relay

Wenn im lokalen Netz schon ein anderer DHCP-Server vorhanden ist, kann ein Gerät alternativ im DHCP-Client-Modus selbst die benötigten Adress-Informationen von dem anderen DHCP-Server beziehen.

Darüber hinaus kann ein Gerät sowohl als DHCP-Relay-Agent als auch als DHCP-Relay-Server arbeiten.

DHCP-Relay-Agent

Als DHCP-Relay-Agent leitet das Gerät DHCP-Anfragen an einen weiteren DHCP-Server weiter.

DHCP-Relay-Server

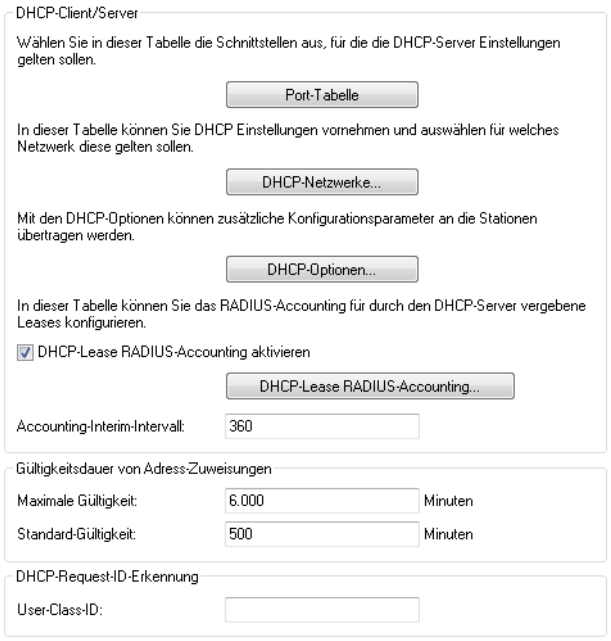
Als DHCP-Relay-Server kann das Gerät von DHCP-Relay-Agents weitergeleitete DHCP-Anfragen bearbeiten.

20.1.1.3 BOOTP

Über das Bootstrap-Protokoll (BOOTP) können einer Station beim Starten eine bestimmte IP-Adresse und weitere Parameter übermittelt werden. Stationen ohne Festplatten können über BOOTP ein Boot-Image und damit ein komplettes Betriebssystem von einem Bootserver laden (ARF).

20.1.2 Konfiguration der DHCPv4-Parameter mit LANconfig

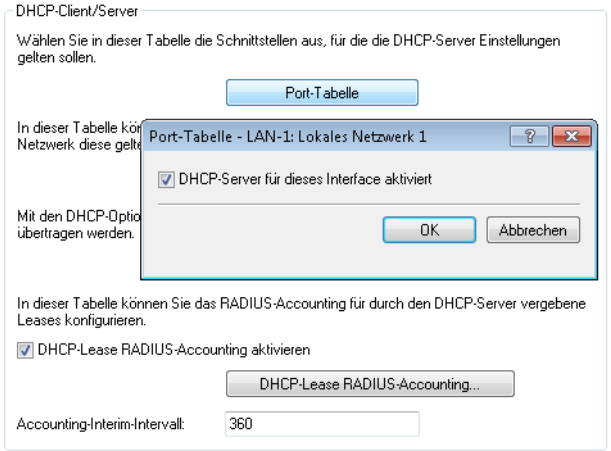
Die DHCPv4-Einstellungen konfigurieren Sie in LANconfig unter **IPv4** > **DHCPv4**.



Informationen zur Konfiguration der DHCPv6-Einstellungen finden Sie im Kapitel *IPv6*.

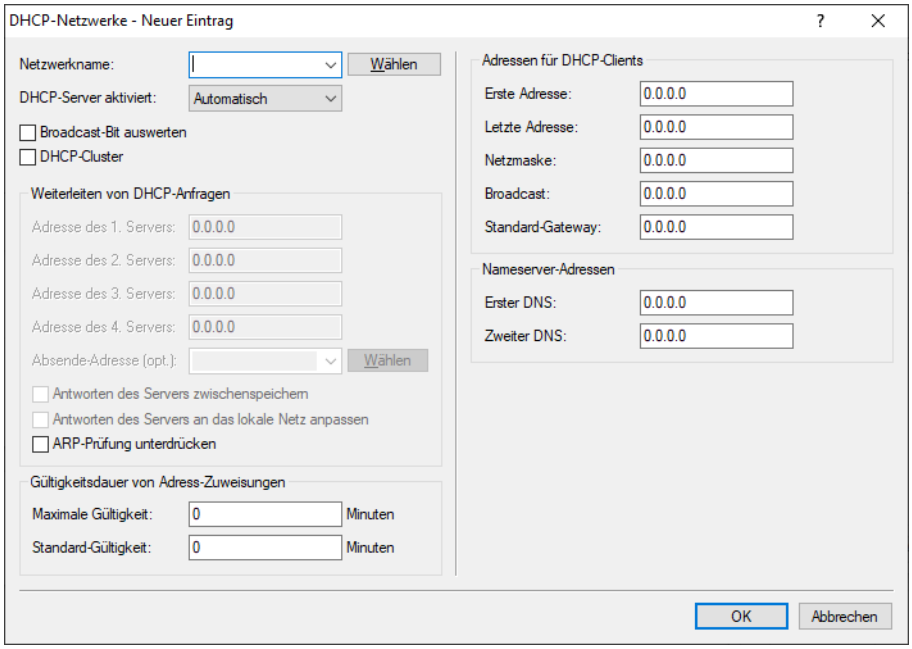
20.1.2.1 Port-Tabelle

Die Aktivierung bzw. Deaktivierung des DHCP-Servers ist für jedes logische Interface (z. B. LAN-1, WLAN-1, P2P-1-1 etc.) separat möglich. Wählen Sie dazu im Konfigurationsmenü unter **IPv4** > **DHCPv4** > **Port-Tabelle** das entsprechende logische Interface aus und schalten Sie den DHCP-Server für dieses Interface ein oder aus.



20.1.2.2 DHCP-Netzwerke

Für jedes im Gerät definierte IP-Netzwerk lassen sich die zugehörigen DHCP-Einstellungen separat festlegen. Die Parameter zur Definition der DHCP-Netzwerke finden Sie mit einem Klick auf **DHCP-Netzwerke**.



Netzwerkname

Wählen Sie hier den Netzwerknamen des Netzes aus, für das die Einstellungen gelten sollen.

Die Konfiguration IP-Netzwerke finden Sie in LANconfig im Konfigurationsmenü unter **IPv4** > **Allgemein** > **IP-Netzwerke**.

DHCP-Server aktiviert

Der DHCP-Server kann die folgenden verschiedenen Zustände annehmen:

Ein

Der DHCP-Server ist dauerhaft eingeschaltet. Bei der Eingabe dieses Wertes wird die Konfiguration des Servers (Gültigkeit des Adress-Pools) überprüft.

- Bei einer korrekten Konfiguration bietet das Gerät sich als DHCP-Server im Netz an.
- Bei einer fehlerhaften Konfiguration (z. B. ungültige Pool-Grenzen) wird der DHCP-Server wieder abgeschaltet und wechselt in den Zustand „Aus".

Verwenden Sie diese Einstellung nur dann, wenn sichergestellt ist, dass kein anderer DHCP-Server im LAN aktiv ist.

Aus

Der DHCP-Server ist dauerhaft abgeschaltet.

Automatisch (Default)

In diesem Zustand sucht das Gerät regelmäßig im lokalen Netz nach anderen DHCP-Servern. Diese Suche ist erkennbar durch ein kurzes Aufleuchten der LED „LAN-Rx/Tx" am Gerät.

- Wird mindestens ein anderer DHCP-Server gefunden, schaltet das Gerät seinen eigenen DHCP-Server aus. Ist für den Router noch keine IP-Adresse konfiguriert, dann wechselt er in den DHCP-Client-Modus und

bezieht eine IP-Adresse vom DHCP-Server. Das verhindert u. a., dass ein nicht konfiguriertes Gerät nach dem Einschalten im Netz unerwünscht Adressen vergibt.

- Werden keine anderen DHCP-Server gefunden, schaltet das Gerät seinen eigenen DHCP-Server ein. Wird zu einem späteren Zeitpunkt ein anderer DHCP-Server im LAN eingeschaltet, wird der DHCP-Server im Router deaktiviert.

Client-Modus

Der DHCP-Server ist ausgeschaltet, das Gerät verhält sich als DHCP-Client und bezieht seine Adress-Informationen von einem anderen DHCP-Server im LAN.

Verwenden Sie diese Einstellung nur dann, wenn sichergestellt ist, dass ein anderer DHCP-Server im LAN aktiv ist und die Zuweisung der IP-Adress-Informationen übernimmt.

Anfragen weiterleiten

Der DHCP-Server ist eingeschaltet und das Gerät nimmt die Anfragen der DHCP-Clients im lokalen Netz entgegen. Das Gerät beantwortet diese Anfragen jedoch nicht selbst, sondern leitet sie an einen zentralen DHCP-Server in einem anderen Netzwerkabschnitt weiter.

Stateless-Relay

Das Gerät nimmt die Anfragen der DHCP-Clients im lokalen Netz entgegen. Das Gerät beantwortet diese Anfragen jedoch nicht selbst, sondern leitet sie an einen zentralen DHCP-Server in einem anderen Netzwerkabschnitt weiter (Betriebsart DHCP-Relay-Agent).

Der Stateless Relay Agent modifiziert DHCP-Pakete vom Client zum Server und zurück nicht. Insbesondere wird der DHCP-Server Identifier, im Gegensatz zum Relay Agent, nicht modifiziert.

Der Zustand des DHCP-Servers ist den DHCP-Statistiken zu entnehmen.

Broadcast-Bit auswerten

Wählen Sie hier, ob der DHCP-Server das vom Client gemeldete Broadcast-Bit auswerten soll oder nicht.

Wenn das Bit nicht ausgewertet wird, dann werden alle DHCP-Antworten als Broadcast gesendet.

DHCP-Cluster

Aktivieren bzw. deaktivieren Sie hier den Betrieb eines DHCP-Servers im Cluster.

Aktiviert

Wenn der Cluster-Betrieb aktiviert ist, verfolgt der DHCP-Server alle im Netz laufenden DHCP-Verhandlungen mit und trägt auch Stationen in seine Tabelle ein, die sich nicht bei ihm, sondern bei anderen DHCP-Servern in Cluster angemeldet haben. Diese Stationen werden in der DHCP-Tabelle mit dem Flag „cache" gekennzeichnet.

Deaktiviert (Default)

Der DHCP-Server verwaltet nur Informationen über die bei ihm selbst angeschlossenen Stationen.

Wenn die Lease-Time der über DHCP zugewiesenen Informationen abläuft, schickt eine Station eine Anfrage zur Erneuerung an den DHCP-Server, von dem sie die Informationen erhalten hat (Renew-Request). Falls der ursprüngliche DHCP-Server auf diesen Request nicht antwortet, versendet die Station eine Anfrage nach einer neuen DHCP-Anbindung (Rebinding Request) als Broadcast an alle erreichbaren DHCP-Server. Renew-Requests werden von den DHCP-Servern im Cluster ignoriert – so wird ein Rebinding erzwungen, damit alle im Cluster vorhandenen DHCP-Server über den Broadcast ihren Eintrag für die Station erneuern können. Auf den Rebind-Request antwortet zunächst nur der DHCP-Server, bei dem die Station ursprünglich registriert war. Wird der Rebind-Request von einer Station wiederholt, dann gehen alle DHCP-Server im Cluster davon aus, das der ursprünglich zuständige

DHCP-Server im Cluster nicht mehr aktiv ist und beantworten die Anfrage. Diese Antwort enthält zwar die gleiche IP-Adresse für die Station, kann aber unterschiedliche Gateway- und DNS-Serveradressen enthalten. Die Station sucht sich nun aus den Antworten einen neuen DHCP-Server aus, an den sie von nun an gebunden ist und übernimmt von ihm Gateway und DNS-Server (sowie alle anderen zugewiesenen Parameter).

Weiterleiten von DHCP-Anfragen

Adresse des 1., 2. 3. und 4. Servers

Konfigurieren Sie die IP-Adressen von bis zu vier übergeordneten DHCP-Servern, an die das Gerät DHCP-Anfragen weiterleitet, wenn für das Netzwerk die DHCP-Betriebsart „Anfragen weiterleiten" aktiv ist.

Absende-Adresse (opt.)

Weisen Sie hier einem Relay-Agent eine optionale Absende-Adresse (Name eines ARF-Netzes, benannte Loopbackadresse) zu, die für die Weiterleitung von Client-Nachrichten verwendet wird.

Antworten des Servers zwischenspeichern

Wenn Sie diese Option aktivieren, dann speichert das Gerät die Antworten des übergeordneten DHCP-Servers zwischen, damit es spätere Anfragen direkt beantworten kann.

So vermeiden Sie unnötige Verbindungen, wenn sich der übergeordnete Server in einem entfernten Netz befindet.

Antworten des Servers an das lokale Netz anpassen

Wenn Sie diese Option aktivieren, dann modifiziert das Gerät die Antworten des übergeordneten DHCP-Servers, um sie dem lokalen Netz anzupassen.

Dabei ersetzt es die Werte für „Standard-Gateway" und „DNS-Server".

ARP-Prüfung unterdrücken

Normalerweise wird vor der Zuweisung einer IP-Adresse durch den DHCP-Server über einen ARP-Request überprüft, ob diese Adresse bereits vergeben ist. Nach 3 Sekunden ohne Antwort auf den ARP-Request wird dann die Zuweisung durchgeführt. In normalen Netzen, gerade wenn Rechner hochgefahren werden, ist diese Abfrage sinnvoll, da dort auch mit festen IP-Adressen gearbeitet wird. Bei einem Public Spot Netzwerk, in dem z. B. ein Smartphone noch erkennen muss, dass keine Internetverbindung besteht, um dann das Login-Popup anzuzeigen, verzögert dieser ARP-Request diese Zeit unnötig. Gerade für solche Szenarien lässt sich diese Überprüfung hier abschalten.

Gültigkeitsdauer von Adress-Zuweisungen

Neben der global konfigurierten Gültigkeitsdauer unter **IPv4** > **DHCPv4** ist hier die Konfiguration einer Gültigkeitsdauer nur für dieses DHCP-Netzwerk möglich.

Maximale Gültigkeit

Geben Sie hier die maximale Gültigkeitsdauer an, die ein Client anfordern darf.

Standard-Gültigkeit

Wenn ein Client IP-Adressdaten anfordert, ohne eine Gültigkeitsdauer für diese Daten zu fordern, erhält er als Gültigkeitsdauer den hier eingestellten Wert vom DHCP-Client zugewiesen.

Adressen für DHCP-Clients

Erste Adresse

Geben Sie hier die erste IP-Adresse des Adressbereiches ein, den Sie den DHCP-Clients zur Verfügung stellen wollen.

Wenn Sie keinen Bereich angeben, verwendet der DHCP-Server automatisch alle freien Adressen in seinem eigenen Netz.

Letzte Adresse

Geben Sie hier die letzte IP-Adresse des Adressbereiches ein, den Sie den DHCP-Clients zur Verfügung stellen wollen.

Netzmaske

Geben Sie hier die zu dem ausgewählten Adressbereich zugehörige Netzmaske ein.

Wenn Sie keine Netzmaske eingeben, wird ermittelt das Gerät die Netzmaske nach Möglichkeit aus der eigenen Adresse und Netzmaske.

Broadcast

In der Regel wird im lokalen Netz für Broadcast-Pakete eine Adresse verwendet, die sich aus den gültigen IP-Adressen und der Netzmaske ergibt. Nur in Sonderfällen (z. B. bei Verwendung von Sub-Netzen für einen Teil der Arbeitsplatzrechner) kann es nötig sein, eine andere Broadcast-Adresse zu verwenden. In diesem Fall tragen Sie die zu verwendende Broadcast-Adresse an dieser Stelle ein.

Die Änderung der Voreinstellung für die Broadcast-Adresse ist nur für erfahrene Netzwerk-Spezialisten empfohlen. Eine Fehlkonfiguration in diesem Bereich kann zu einem unerwünschten, ggf. kostenpflichtigen Verbindungsaufbau führen.

Standard-Gateway

Das Gerät weist dem anfragenden Rechner standardmäßig seine eigene IP-Adresse in diesem Netzwerk als Gateway-Adresse zu. Falls erforderlich, können Sie durch den Eintrag einer entsprechende IP-Adresse auch ein anderes Gateway konfigurieren.

Nameserver-Adressen

Erster/zweiter DNS

Geben Sie hier die Adressen eines Nameservers und eines alternativen Nameservers ein, an die DNS-Anfragen weitergeleitet werden sollen.

Nutzen Sie einen Internetprovider oder eine andere Gegenstelle, die dem Router beim Einloggen automatisch einen Nameserver zuweist, dann können Sie diese Felder leer lassen.

Bei der Konfiguration der DHCP-Netzwerke werden die Adressen definiert, die den DHCP-Clients zugewiesen werden (IP-Adress-Pool). Wenn ein Client im Netz gestartet wird, der mit seinen Netzwerk-Einstellungen über DHCP eine IP-Adresse anfordert, wird ihm ein Gerät mit aktiviertem DHCP-Server die Zuweisung einer Adresse anbieten. Als IP-Adresse wird dabei eine gültige Adresse aus dem Pool genommen. Wurde dem Rechner in der Vergangenheit schon mal eine IP-Adresse zugewiesen, so fordert er eben diese Adresse wieder an, und der DHCP-Server versucht ihm diese Adresse wieder zuzuweisen, wenn sie nicht bereits einem anderen Rechner zugewiesen wurde.

Der DHCP-Server prüft zusätzlich, ob die ausgesuchte Adresse im lokalen Netz noch frei ist. Sobald die Eindeutigkeit einer Adresse festgestellt wurde, wird dem anfragenden Rechner die gefundene Adresse zugewiesen.

Im Auslieferungs-Zustand sind in den Geräten die IP-Netzwerke 'Intranet' und 'DMZ' angelegt, sind aber noch nicht mit IP-Adresse und Netzmaske ausgestattet – das Gerät befindet sich in einem besonderen Betriebszustand. Es verwendet dann selbst die IP-Adresse „172.23.56.254“ und den Adress-Pool „172.23.56.x“ für die Zuweisung der IP-Adressen im Netz.

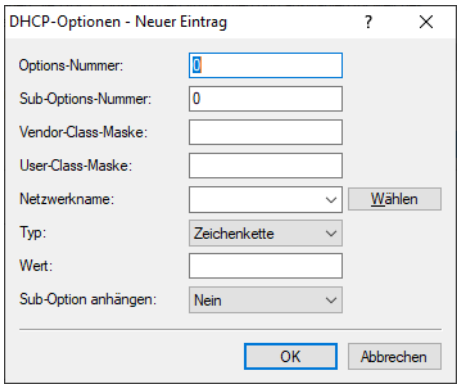
Mehrere Netzwerke auf einem Interface: Mit der Konfiguration der IP- und DHCP-Netzwerke können auf einem logischen Interface mehrere Netzwerke mit unterschiedlichen DHCP-Einstellungen aktiv sein. In diesem Fall

werden die DHCP-Einstellungen aus dem ersten passenden Netzwerk verwendet. Hierfür ist ggf. eine Priorisierung der Netzwerke notwendig.

20.1.2.3 DHCP-Optionen

Mit den DHCP-Optionen überträgt der DHCP-Server zusätzliche Konfigurationsparameter an die DHCP-Clients. Der Vendor-Class-Identifier (DHCP-Option 60) zeigt z. B. den Gerätetyp an. Die DHCP-Option 43 wird von verschiedenen Geräteherstellern verwendet, um während der Erstinbetriebnahme via DHCP weitere Informationen an Netzwerkgeräte zu verteilen. Die entsprechenden Parameter sind herstellerspezifisch. Für den LANCOM Rollout-Agent z. B. siehe hierzu *Konfiguration des Zero-Touch-Rollouts* auf Seite 151.

Die Konfiguration der DHCP-Optionen in LANconfig befindet sich unter **IPv4** > **DHCPv4** > **DHCP-Optionen**. Klicken Sie auf **Hinzufügen**, um einen neuen Eintrag anzulegen.



Options-Nummer

Nummer der Option, die an die DHCP-Clients übermittelt werden soll. Die Options-Nummer beschreibt die übermittelte Information, z. B. „17" (Root Path) für den Pfad zu einem Boot-Image für einen PC ohne eigene Festplatte, der über BOOTP sein Betriebssystem bezieht.

Eine Liste aller DHCP-Optionen finden Sie im *RFC 2132 – DHCP Options and BOOTP Vendor Extensions* der Internet Engineering Task Force (IETF).

Sub-Options-Nummer

Nummer der Sub-Option, die an die DHCP-Clients übermittelt werden soll. Eine DHCP-Option kann über Sub-Optionen weiter aufgeteilt werden. Z. B. wird Netzwerkgeräten wie SIP-Telefonen über die DHCP-Option 43 häufig mitgeteilt, wo ihre Firmware und Konfiguration heruntergeladen werden kann. Die dafür einzustellenden Sub-Optionen werden dann durch den jeweiligen Hersteller definiert.

Vendor-Class-Maske

Einige DHCP-Clients übermitteln bei Anfragen an DHCP-Server eine Vendor-Class-Id und / oder eine User-Class-ID. Diese erlauben es normalerweise, den Client eindeutig einem Hersteller oder sogar einer bestimmten Geräteklasse zuzuordnen – so enthalten die DHCP-Anfragen von LANCOM Geräten immer den String „LANCOM" in der Vendor-Class-ID, ggf. ergänzt um den genauen Gerätetyp. Der DHCP-Server kann diese Information nutzen, um jedem Gerätetyp nur die jeweils passenden DHCP-Optionen zu übermitteln. Dies ist insbesondere bei der DHCP-Option 43 relevant, da deren Inhalt nicht standardisiert ist, sondern Vendor-spezifisch – je nach Hersteller oder Geräte-Art müssen unterschiedliche Informationen vom DHCP-Server übermittelt werden. Dazu können die beiden Felder „Vendor-Class-Maske" und „User-Class-Maske" als Filter verwendet werden. Hier können Strings eingetragen werden, auf deren Vorhandensein der DHCP-Server eingehende Anfragen prüft. Nur wenn der konfigurierte Filter zur DHCP-Anfrage passt, wird anschließend die DHCP-Option ausgeliefert. Es darf mit den Wildcards „*" (beliebig viele Zeichen) und „?" (genau ein beliebiges Zeichen) gearbeitet werden. Bleiben die Felder leer, werden sie nicht beachtet und die Option wird immer ausgeliefert.

Für LANCOM Geräte würde hier also z. B. „*LANCOM*“ eingetragen.

User-Class-Maske

Filterkriterium, das von einigen Herstellern bei Anfragen an den DHCP-Server verwendet wird. Siehe auch Vendor-Class-Maske. Hier können Strings eingetragen werden, auf deren Vorhandensein der DHCP-Server eingehende Anfragen prüft. Nur wenn der konfigurierte Filter zur DHCP-Anfrage passt, wird anschließend die DHCP-Option ausgeliefert. Es darf mit den Wildcards „*“ (beliebig viele Zeichen) und „?“ (genau ein beliebiges Zeichen) gearbeitet werden. Bleiben die Felder leer, werden sie nicht beachtet und die Option wird immer ausgeliefert.

Netzwerkname

Name des IP-Netzwerks, in dem diese DHCP-Option verwendet werden soll.

Typ

Typ des Eintrags. Dieser Wert ist abhängig von der jeweiligen Option. RFC 2132 definiert z. B. die Option „35“ (ARP Cache Timeout) wie folgt:

```
ARP Cache Timeout Option
This option specifies the timeout in seconds for ARP cache entries.
The time is specified as a 32-bit unsigned integer.
The code for this option is 35, and its length is 4.
Code Len Time
+-----+-----+-----+-----+-----+-----+
| 35  | 4   | t1  | t2  | t3  | t4  |
+-----+-----+-----+-----+-----+-----+
```

Aus dieser Beschreibung können Sie ablesen, dass für diese Option der Typ „32-Bit-Integer“ verwendet wird.

Den Typ der Option entnehmen Sie bitte dem entsprechenden RFC bzw. bei herstellerspezifischen DCHP-Optionen der jeweiligen Herstellerdokumentation.

Wert

In diesem Feld definieren Sie den Inhalt der DHCP-Option.

IP-Adressen werden in der üblichen Schreibweise von IPv4-Adressen angegeben, also z. B. als „123.123.123.100“, Integer-Typen werden als normale Dezimalzahlen eingetragen, Strings als einfacher Text.

Mehrere Werte in einem Feld werden mit Kommas separiert, also z. B. „123.123.123.100, 123.123.123.200“.

Die mögliche Länge des Optionswertes entnehmen Sie bitte dem entsprechenden RFC bzw. bei herstellerspezifischen DCHP-Optionen der jeweiligen Herstellerdokumentation.

Sub-Option anhängen

Für jede Sub-Option der Option 43 wird eine eigene Option angelegt und übermittelt. Über diesen Schalter ist es möglich, mehrere DHCP-Option-43-Sub-Optionen zusammenzufassen. Dazu hier auf **Ja** stellen. Das Zusammenfassen geschieht, wenn:

- **Options-Nummer** gleich 43 ist
- **Sub-Options-Nummer** ungleich Null ist
- Davor in der Tabelle bereits eine Option 43 mit Sub-Options-Nummer ungleich Null steht

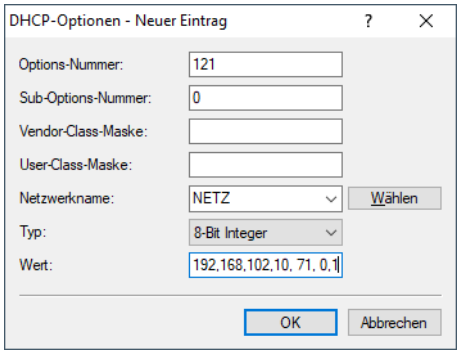
Beachten Sie die maximale Länge von 255 Zeichen für eine Option.

Beispiel: Option „Classless Static Route“ im DHCP-Server übertragen

Um die Route 192.168.102.0/24 via 10.71.0.1 als Classless Static Route Option (121) im DHCP-Server zu übertragen, legen Sie folgenden Eintrag in der Tabelle **IPv4** > **DHCPv4** > **DHCP-Optionen** an:

- **Options-Nummer** – 121

- **Netzwerkname** – Name des Netzes, in dem die Option an Clients übertragen werden soll.
- **Typ** – 8 Bit Integer
- **Wert** – 24,192,168,102,10, 71, 0,1

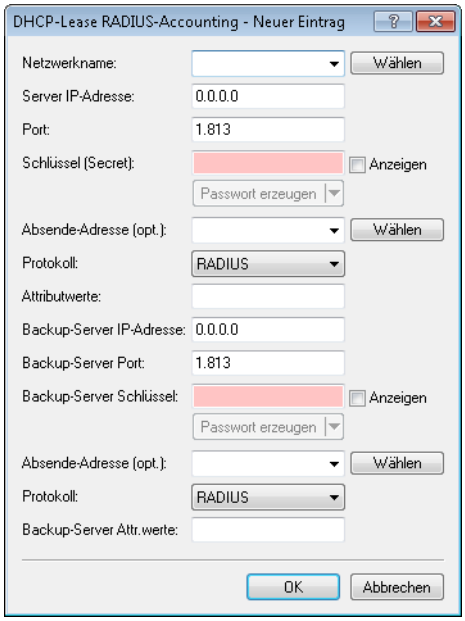


20.1.2.4 DHCP-Lease RADIUS-Accounting

Weist der DHCP-Server einem DHCP-Client eine IP-Adresse zu, sendet er bei aktiviertem RADIUS-Accounting dem entsprechend zugewiesenen Accounting-Server (bzw. dem Backup-RADIUS-Server) ein `RADIUS Accounting Start`. Läuft die Gültigkeit der Adresszuweisung (DHCP-Lease) mangels Verlängerung ab, sendet der DHCP-Server ein `RADIUS Accounting Stop`. Zwischen diesen beiden Ereignissen sendet der DHCP-Server dem RADIUS-Server regelmäßig in einem konfigurierbaren Intervall ein `RADIUS Accounting Interim Update`.

Das RADIUS-Accounting für den DHCP-Server aktivieren oder deaktivieren Sie unter **IPv4** > **DHCPv4** mit einem Klick auf die Option **DHCP-Lease RADIUS-Accounting aktivieren**.

Das Intervall für die RADIUS-Interim-Updates konfigurieren Sie im Eingabefeld **Accounting-Interim-Intervall**. Den RADIUS-Accounting-Server und den entsprechenden Backup-Server konfigurieren Sie mit einem Klick auf **DHCP-Lease RADIUS-Accounting**.



Netzwerkname

Wählen Sie hier den Netzwerknamen des Netzes aus, für das RADIUS-Accounting-Nachrichten gesendet werden sollen.

Server IP-Adresse

Geben Sie hier die IP-Adresse oder den DNS-Namen des RADIUS-Servers an (IPv4 oder IPv6).

Port

Geben Sie hier den TCP-Port an, über den der RADIUS-Server Accounting-Informationen entgegennimmt. Üblicherweise ist das der Port „1813".

Schlüssel

Geben Sie hier den Schlüssel (Shared Secret) für den Zugang zum RADIUS-Accounting-Server an. Stellen Sie sicher, dass dieser Schlüssel im entsprechenden Accounting-Server übereinstimmend konfiguriert ist.

Absende-Adresse (opt.)

Standardmäßig schickt der RADIUS-Server seine Antworten zurück an die IP-Adresse Ihres Gerätes, ohne dass Sie diese hier angeben müssen. Durch Angabe einer optionalen alternativen Absende-Adresse verändern Sie die Quelladresse bzw. Route, mit der das Gerät den RADIUS-Server anspricht. Dies kann z. B. dann sinnvoll sein, wenn der Server über verschiedene Wege erreichbar ist und dieser einen bestimmten Weg für seine Antwort-Nachrichten wählen soll.

Protokoll

Über diesen Eintrag geben Sie das Protokoll an, dass der DHCP-Server für die Kommunikation mit dem RADIUS-Accounting-Server verwendet.

Attributwerte

LCOS ermöglicht es, die RADIUS-Attribute für die Kommunikation mit einem RADIUS-Server (sowohl Authentication als auch Accounting) zu konfigurieren.

Die Angabe der Attribute erfolgt als semikolon-separierte Liste von Attribut-Nummern oder -Namen und einem entsprechenden Wert in der folgenden Form:

`<Attribut_1>=<Wert_1>;<Attribut_2>=<Wert_2>`

Da die Anzahl der Zeichen begrenzt ist, lässt sich der Name abkürzen. Das Kürzel muss dabei eindeutig sein. Beispiele:

- `NAS-Port=1234` ist nicht erlaubt, da das Attribut nicht eindeutig ist (`NAS-Port`, `NAS-Port-Id` oder `NAS-Port-Type`).
- `NAS-Id=ABCD` ist erlaubt, da das Attribut eindeutig ist (`NAS-Identifier`).

Als Attribut-Wert ist die Angabe von Namen oder RFC-konformen Nummern möglich. Für das Gerät sind die Angaben `Service-Type=Framed` und `Service-Type=2` identisch.

Die Angabe eines Wertes in Anführungszeichen (`"<Wert>"`) ist möglich, um Sonderzeichen wie Leerzeichen, Semikolon oder Gleichheitszeichen mit angeben zu können. Das Anführungszeichen erhält einen umgekehrten Schrägstrich vorangestellt (`\"`), der umgekehrte Schrägstrich ebenfalls (`\\`).

Als Werte sind auch die folgenden Variablen erlaubt:

`%n`

Gerätename

`%e`

Seriennummer des Gerätes

%%

Prozentzeichen

%{name}

Original-Name des Attributes, wie ihn die RADIUS-Anwendung überträgt. Damit lassen sich z. B. Attribute mit originalen RADIUS-Attributen belegen: `Called-Station-Id=%{NAS-Identifier}` setzt das Attribut `Called-Station-Id` auf den Wert, den das Attribut `NAS-Identifier` besitzt.

Backup-Server IP-Adresse

Geben Sie hier die IP-Adresse oder den DNS-Namen des Backup-RADIUS-Servers an.

Backup-Server Port

Geben Sie hier den TCP-Port an, über den der Backup-RADIUS-Server Accounting-Informationen entgegennimmt. Üblicherweise ist das der Port „1813".

Backup-Server Schlüssel

Geben Sie hier den Schlüssel (Shared Secret) für den Zugang zum Backup-RADIUS-Accounting-Server an. Stellen Sie sicher, dass dieser Schlüssel im entsprechenden Accounting-Server übereinstimmend konfiguriert ist.

Absende-Adresse (opt.)

Geben Sie hier optional eine alternative Absende-Adresse an, die der DHCP-Server an den Backup-RADIUS-Server überträgt.

Protokoll

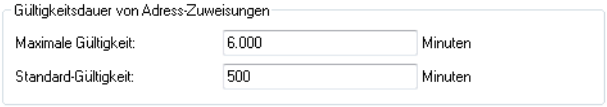
Über diesen Eintrag geben Sie das Protokoll an, dass der DHCP-Server für den Backup-RADIUS-Server verwendet.

Backup-Server Attr.werte

Geben Sie hier die zusätzlichen Attributwerte für die RADIUS-Kommunikation mit dem Backup-Server an.

20.1.2.5 Gültigkeitsdauer von Adress-Zuweisungen

Wenn ein DHCP-Client eine IP-Adresse bei einem DHCP-Server anfragt, kann er eine Gültigkeitsdauer für diese Adresse anfordern. In diesem Abschnitt konfigurieren Sie, wie der DHCP-Server diese Anfragen behandelt.



Maximale Gültigkeit

Dieser Wert kontrolliert die maximale Gültigkeitsdauer, die ein Client anfordern darf.

Standard-Gültigkeit

Wenn ein Client eine IP-Adresse anfragt, ohne eine Gültigkeitsdauer für diese Adresse zu fordern, weist der DHCP-Server dieser Adresse als Gültigkeitsdauer den hier eingestellten Wert zu.

20.1.2.6 Vendor-Class- und User-Class-Identifier im DHCP-Client

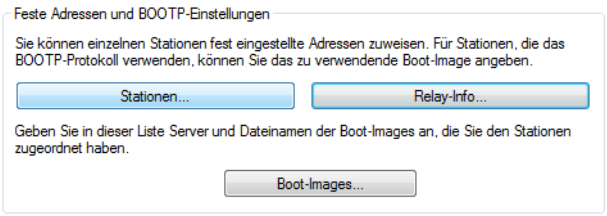
Der DHCP-Client im Gerät kann in den versendeten DHCP-Requests zusätzliche Angaben einfügen, die eine Erkennung der Requests im Netzwerk erleichtern.

- Der Vendor-Class-Identifier (DHCP-Option 60) zeigt den Gerätetyp an. Die Vendor-Class-ID wird immer übertragen.
- Der User-Class-Identifier (DHCP-Option 77) gibt einen benutzerdefinierten String an, der unter `Setup/DHCP` oder im LANconfig im Konfigurationsbereich **IPv4** > **DHCPv4** im Feld **User-Class-ID** eingetragen werden kann (Default: leer). Die User-Class-ID wird nur übertragen, wenn der Benutzer einen Wert konfiguriert hat.

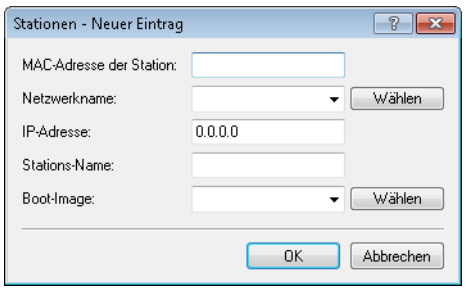


20.1.2.7 BOOTP: Zuweisung von festen IP-Adressen an bestimmte Stationen konfigurieren

Die Parameter zur Konfiguration von BOOTP finden Sie in LANconfig im Konfigurationsmenü unter **IPv4** > **BOOTP**.



Definieren Sie in der Liste der **Stationen** die MAC-Adresse einer Station, der Sie eine bestimmte IP-Adresse zuweisen möchten.



MAC-Adresse der Station

Geben Sie hier die Node-ID des Clients ein.

Die Node-ID ist die physikalische Kennung des Client-Netzwerkadapters und entspricht der MAC-Adresse.

Netzwerkname

Wählen Sie hier den Netzwerknamen des ARF-Netzes aus, für das die Einstellungen gelten sollen.

Wenn Sie diesen Eintrag leer lassen, weist das Gerät die konfigurierte Adresse aus dem ARF-Netz zu, aus dem die DHCP-Anfrage erfolgte. Erfolgt die Anfrage aus einem ARF-Netz, für das Sie keine spezielle Adresse konfiguriert haben, so weist das Gerät eine Adresse dynamisch aus dem Adress-Pool zu.

Wenn eine zugewiesene IP-Adresse nicht im Adressbereich des konfigurierten ARF-Netzes liegt, so wird die Zuweisung verworfen und anstelle dessen eine IP-Adresse aus dem Adress-Pool des ARF-Netzes verwendet, aus dem die Anfrage erfolgte.

IP-Adresse

Geben Sie hier die IP-Adresse ein, die das Gerät dem Client zuweist.

Stations-Name

Geben Sie hier einen Namen ein, mit dem das Gerät den Client identifiziert.

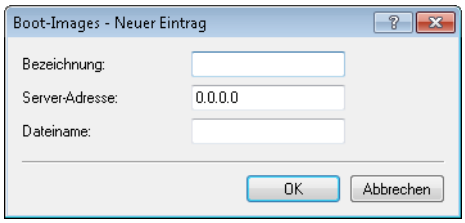
Wenn ein Client seinen Namen nicht übermittelt, verwendet das Gerät den hier eingetragenen Namen.

Boot-Image

Wenn der Client das BOOTP-Protokoll verwendet, dann können Sie ein Boot-Image auswählen, über das der Client sein Betriebssystem laden soll.

Den Server, der das Boot-Image zur Verfügung stellt, sowie den Namen der Datei auf dem Server müssen Sie in der Boot-Image-Tabelle eingeben.

Definieren Sie in der Liste der **Boot-Images** ein Boot-Image, dass Sie optional einer Station zuweisen möchten.



Bezeichnung

Geben Sie eine Bezeichnung an, die diesen Eintrag eindeutig kennzeichnet.

Server-Adresse

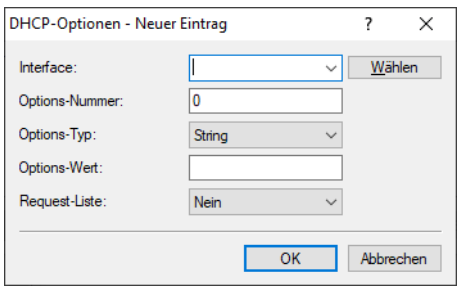
Bestimmen Sie die IP-Adresse des Servers, der das Boot-Image zur Verfügugn stellt.

Dateiname

Geben Sie den Namen der Datei an, die das Boot-Image enthält.

20.1.2.8 DHCPv4-Client Optionen

Sie können für den DHCPv4-Client bestimmte Optionen konfigurieren, die dann übertragen werden. Dies ist erforderlich, wenn der Internet-Provider bestimmte Daten in DHCP-Nachrichten erwartet. Die Optionen können in der Tabelle DHCP-Optionen unter **IPv4** > **DHCPv4** > **DHCP-Client** > **DHCP-Optionen** frei konfiguriert werden.



Interface

Interface auf dem der DHCPv4-Client diese Option verwenden soll, z. B. WAN-Gegenstelle oder IPv4-LAN-Netzwerk.

Options-Nummer

Definiert die vergebene IANA-Nummer der DHCP-Option wie diese im RFC definiert ist.

Options-Typ

Definiert den Typ der DHCP-Option. Mögliche Werte: String, Integer8, Integer16, Integer32 oder IP-Adresse

Options-Wert

Definiert den Inhalt der DHCP-Option

Dabei kann, außer bei String, auch eine Komma- und/oder Space-separierte Liste angegeben werden. Für Integerwerte gelten die C-Codierungen, für Zahlen, d. h. 0x ergibt einen Hexwert und wenn die Zahl mit 0 beginnt ist es ein Oktal-Wert. Zusätzlich kann beim Typ Integer8 auch ein einzelner Hex-String (mit gerader Länge) ohne Separator angegeben werden. Vorhandene in den Standard-Optionen können überschrieben werden. Die folgenden Optionen können nicht überschrieben bzw. konfiguriert werden: padding (0), overload (52), message-type (53), server-id (54), request-list (55), message-size (57) und end (255).

Request-Liste

Definiert, ob die Optionsnummer im DHCP-Request angefragt werden soll. Das Verhalten wird über das jeweilige RFC der DHCP-Option definiert. Mögliche Werte: Ja, Nein

20.1.3 Konfiguration der DHCP-Clients

Standardmäßig sind fast alle Einstellungen in der Netzwerkumgebung von Windows so eingestellt, dass die benötigten Parameter über DHCP angefragt werden. Überprüfen Sie die Windows-Einstellungen mit einem Klick auf **Start** > **Einstellungen** > **Systemsteuerung** > **Netzwerk**. Wählen Sie den Eintrag für **TCP/IP** Ihres Netzwerkadapters, und öffnen Sie die **Eigenschaften**. Auf den verschiedenen Registerkarten können Sie nun nachsehen, ob spezielle Einträge z. B. für die IP-Adresse oder das Standard-Gateway vorhanden sind. Wenn Sie alle Werte vom DHCP-Server zuweisen lassen wollen, löschen Sie nur die entsprechenden Einträge.

Sollte ein Rechner andere Parameter verwenden als die ihm zugewiesenen (z. B. ein anderes Standard-Gateway), so müssen diese Parameter direkt am Arbeitsplatzrechner eingestellt werden. Der Rechner ignoriert dann die entsprechenden Parameter in der Zuweisung durch den DHCP-Server. Unter Windows geschieht das z. B. über die Eigenschaften der Netzwerkumgebung. Klicken Sie auf **Start** > **Einstellungen** > **Systemsteuerung** > **Netzwerk**. Wählen Sie den Eintrag für **TCP/IP** an Ihrem Netzwerkadapter und öffnen die **Eigenschaften**. Auf den verschiedenen Registerkarten können Sie nun die gewünschten Werte eintragen.

20.1.4 DHCP-Client-Option Classless Static Route

Über die Classless Static Route DHCPv4-Option kann ein DHCP-Server eine Liste von statischen Routen an einen DHCP-Client übermitteln, der diese Routen dann in seine Routing-Tabelle einträgt. Die Routen dieser Liste sind „Classless", d. h. zu jeder Route wird eine Subnetzmaske bzw. Präfixlänge übermittelt. Nach *RFC 3442* wird hierzu die Optionsnummer 121 verwendet.

Der DHCP-Client installiert dann beim Empfang keine Default-Route zum spezifizierten Router, sondern nur die Liste der statischen Route in die Routing-Tabelle.

Diese Funktion wird beispielsweise von Internet-Providern in Szenarien verwendet, bei denen mehrere virtuelle Verbindungen nach Dienst über VLAN getrennt werden, z. B. jeweils ein VLAN für Internet, VoIP und IPTV. In diesem Fall wird für die Internetverbindung (z. B. über PPPoE oder DHCP) die Default-Route verwendet, die notwendigen Routen für IPTV über ein anderes VLAN per DHCP als Classless Static Route Option.

Der LANCOM DHCPv4-Client fragt standardmäßig sowohl Router als auch die Option „Classless Static Routes" an. Wird vom DHCP-Server eine Option „Classless Static Routes" ausgeliefert, so wird eine ggf. vorhandene Router-Option ignoriert und nur die Liste der Routen installiert. Dieses Verhalten ist RFC-konform nach RFC 3442.

Für ein Provider-Szenario mit IPTV legen Sie dazu eine neue DSL-Gegenstelle mit Haltezeit 9999, Layer DHCPOE sowie dem entsprechenden VLAN nach Providervorgaben an. Aktivieren Sie den Schalter **Gegenstelle auch ohne Route aufbauen (Keepalive ohne Route)** unter **Kommunikation** > **Gegenstellen**. Es ist kein Eintrag in der Routing-Tabelle nötig, da der DHCP-Client die notwendigen Routen per Option „Classless Static Route" empfängt.

Der LANCOM DHCP-Server kann die Option „Classless Static Route" per benutzerdefinierter Option ebenfalls an DHCP-Clients vergeben. Informationen dazu finden Sie im Abschnitt *DHCP-Optionen* auf Seite 1627.

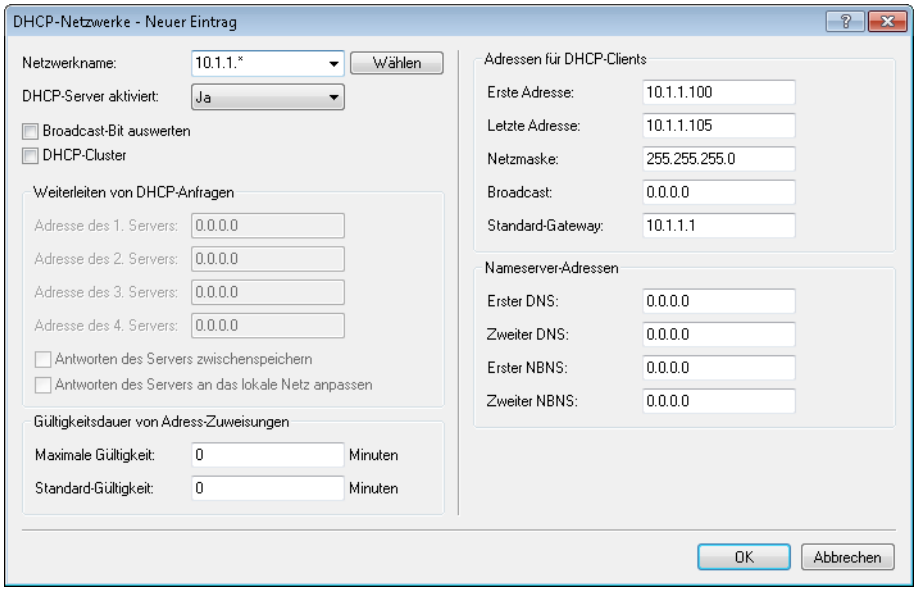
20.1.5 DHCP-Relay-Server

Ein Gerät kann nicht nur DHCP-Anfragen an einen übergeordneten DHCP-Server weiterleiten, es kann auch selbst als zentraler DHCP-Server fungieren (DHCP-Relay-Server).

Um ein Gerät als DHCP-Relay-Server für andere Netzwerke anzubieten, wird die Relay-Agent-IP-Adresse (GI-Adresse) als Netzwerkname in die Tabelle der IP-Netzwerke eingetragen.

Wenn das gleiche Netz von mehreren Relay-Agents verwendet wird (z. B. mehrere Access Points leiten die Anfragen auf einen zentralen DHCP-Server weiter), dann kann die GI-Adresse auch mit einem „*" abgekürzt werden. Wenn z. B. Clients im entfernten Netz `10.1.1.0/255.255.255.0` Adressen zugewiesen werden sollen und in diesem Netz mehrere

Relay-Agents stehen, die alle das Gerät als übergeordneten DHCP-Server verwenden, dann kann die Zuweisung von IP-Adressen und Standard-Gateway an die Clients so erfolgen:



Für die Betriebsart als DHCP-Relay-Server ist die Angabe des Adress-Pools und der Netzmaske zwingend erforderlich.

20.1.5.1 DNS-Auflösung von über DHCP gelernten Namen

Der DNS-Server berücksichtigt bei der Auflösung von über DHCP gelernten Namen die Interface-Tags, d. h. es werden nur Namen aufgelöst, die aus einem Netz mit dem gleichen Interface-Tag gelernt wurden wie das Netz des Anfragenden. Kommt die Anfrage aus einem ungetaggten Netz, so werden alle Namen – also auch die, die von getaggten Netzen gelernt wurden – aufgelöst. Ebenso sind für getaggte Netze alle Namen sichtbar, die von ungetaggten Netzen gelernt wurden.

Namen, die von Relay-Agents gelernt wurden, werden immer so behandelt, als wären sie von einem ungetaggten Netz gelernt worden, d. h. diese Namen sind für alle Netze sichtbar.

20.1.6 Anzeige von Statusinformationen des DHCP-Servers

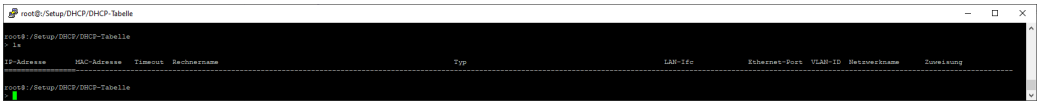
Eine Übersicht über die IP-Adressen im LAN gibt die Status-Tabelle des DHCP-Servers. Sie zeigt folgende Informationen über die Geräte an, denen der DHCP-Server eine IP-Adresse zugewiesen hat:

- IP-Adresse, welche der DHCP-Server dem Netzwerkgerät zugewiesen hat
- MAC-Adresse des Netzwerkgerätes
- Timeout, verbleibende Gültigkeitsdauer in Minuten
- Rechnername
- Typ der Adresszuweisung, dynamisch oder aus dem Cache
- LAN-Ifc, logische Schnittstelle über welche der DHCP-Server dem Netzwerkgerät die IP-Adresse zugewiesen hat
- Ethernet-Port, physikalische Schnittstelle über welche der DHCP-Server dem Netzwerkgerät die IP-Adresse zugewiesen hat
- VLAN-ID des Netzwerks

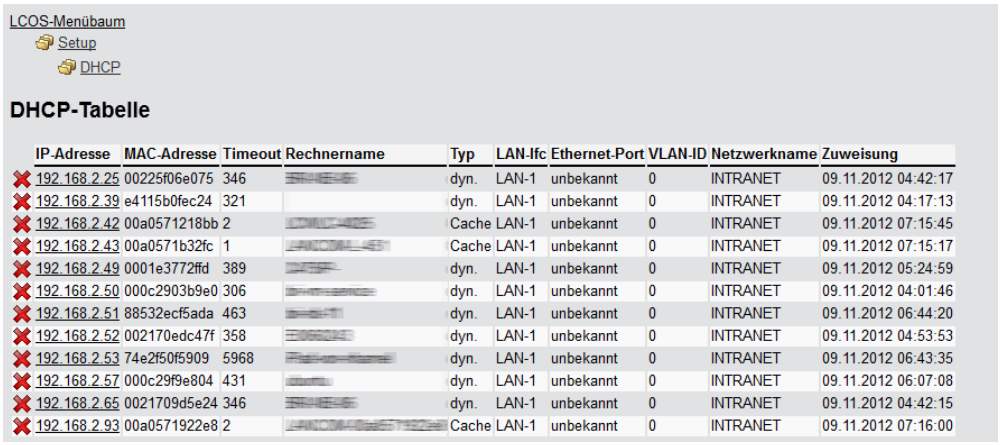
- Netzwerkname
- Zuweisung, Zeitpunkt zu dem der DHCP-Server dem Netzwerkgerät die IP-Adresse zugewiesen hat

Sie finden die Statusinformationen des DHCP-Servers an folgenden Stellen:

- CLI: **Setup** > **DHCP** > **DHCP-Tabelle**

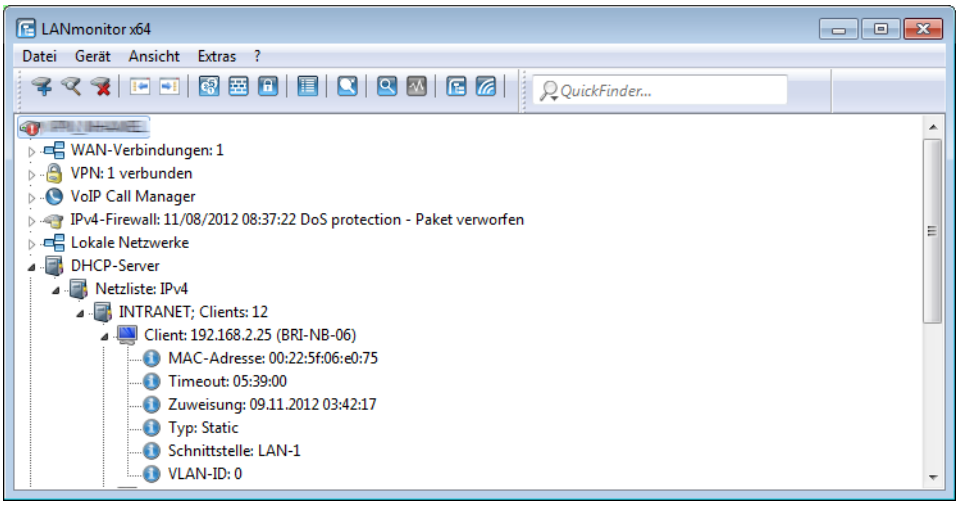


- Webconfig: **Setup** > **DHCP** > **DHCP-Tabelle**



IP-Adresse	MAC-Adresse	Timeout	Rechnername	Typ	LAN-Ifc	Ethernet-Port	VLAN-ID	Netzwerkname	Zuweisung
192.168.2.25	00225f06e075	346	[redacted]	dyn.	LAN-1	unbekannt	0	INTRANET	09.11.2012 04:42:17
192.168.2.39	e4115b0fec24	321		dyn.	LAN-1	unbekannt	0	INTRANET	09.11.2012 04:17:13
192.168.2.42	00a0571218bb	2	[redacted]	Cache	LAN-1	unbekannt	0	INTRANET	09.11.2012 07:15:45
192.168.2.43	00a0571b32fc	1	[redacted]	Cache	LAN-1	unbekannt	0	INTRANET	09.11.2012 07:15:17
192.168.2.49	0001e3772ffd	389	[redacted]	dyn.	LAN-1	unbekannt	0	INTRANET	09.11.2012 05:24:59
192.168.2.50	000c2903b9e0	306	[redacted]	dyn.	LAN-1	unbekannt	0	INTRANET	09.11.2012 04:01:46
192.168.2.51	88532ecf5ada	463	[redacted]	dyn.	LAN-1	unbekannt	0	INTRANET	09.11.2012 06:44:20
192.168.2.52	002170edc47f	358	[redacted]	dyn.	LAN-1	unbekannt	0	INTRANET	09.11.2012 04:53:53
192.168.2.53	74e2f50f5909	5968	[redacted]	dyn.	LAN-1	unbekannt	0	INTRANET	09.11.2012 06:43:35
192.168.2.57	000c29f9e804	431	[redacted]	dyn.	LAN-1	unbekannt	0	INTRANET	09.11.2012 06:07:08
192.168.2.65	0021709d5e24	346	[redacted]	dyn.	LAN-1	unbekannt	0	INTRANET	09.11.2012 04:42:15
192.168.2.93	00a0571922e8	2	[redacted]	Cache	LAN-1	unbekannt	0	INTRANET	09.11.2012 07:16:00

- LANmonitor: Aufgeteilt nach Netzwerkname unter **DHCP-Server** > **Netzliste**



20.1.7 DHCP-Cluster

Wenn mehrere DHCP-Server in einem Netz aktiv sind, dann „verteilen“ sich die Stationen im Netz gleichmäßig auf diese Server. Der DNS-Server der Geräte löst allerdings nur die Namen der Stationen richtig auf, denen der eigene DHCP-Server die Adressinformationen zugewiesen hat. Damit der DNS-Server auch die Namen anderer DHCP-Server auflösen kann, können die DHCP-Server im Cluster betrieben werden. In dieser Betriebsart verfolgt der DHCP-Server alle im Netz laufenden

DHCP-Verhandlungen mit und trägt auch Stationen in seine Tabelle ein, die sich nicht bei ihm, sondern bei anderen DHCP-Servern im Cluster angemeldet haben.

Die Einstellung zu DHCP-Cluster aktivieren Sie unter **IPv4** > **DHCPv4** in den Einstellungen der **DHCP-Netzwerke**.

20.1.8 Alternative DHCP-Server zur Weiterleitung

Der DHCP-Server erlaubt verschiedene Betriebsarten. Im Weiterleitungs-Modus agiert das Gerät im lokalen Netz als DHCP-Relay und leitet Anfragen an einen oder mehrere konfigurierte DHCP-Server weiter. Diese Einstellung erlaubt den Betrieb von zentralen DHCP-Servern in einem anderen Netz.

Alle DHCP-Nachrichten, welche die DHCP-Clients als Broadcast senden, werden an alle konfigurierten DHCP-Server weitergeleitet. Der Client wählt dann den ersten Server der antwortet und sendet alle weiteren Nachrichten als Unicast, die gezielt an den zuständigen Server weitergeleitet werden. Falls der gewählte Server nicht erreichbar ist, versendet der Client erneut Broadcast-Nachrichten und wählt einen anderen DHCP-Server.

Die DHCP-Weiterleitungsserver konfigurieren Sie unter **IPv4** > **DHCPv4** in den Einstellungen der **DHCP-Netzwerke**.

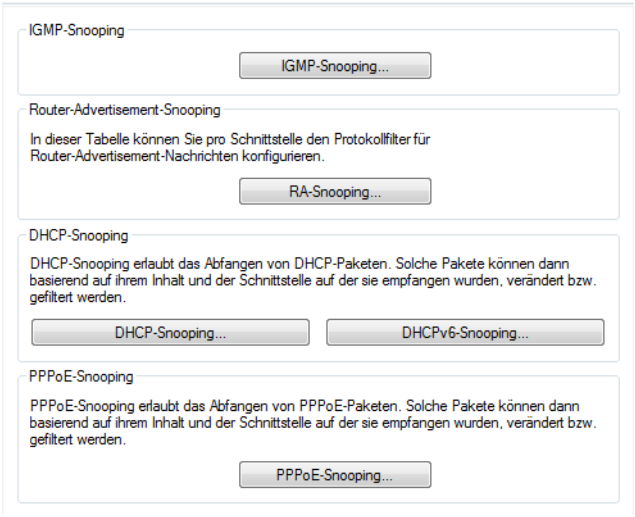
20.1.9 DHCP-Snooping und DHCP-Option 82

DHCP verfügt ursprünglich über keine Sicherheitsmechanismen zum Schutz von Angriffen auf die Zuweisung der Netzkonfiguration. Sendet z. B. ein Client ein DHCP-Discover-Paket ins Netz, um von einem DHCP-Server eine gültige Netzkonfiguration zu erhalten, kann ein Angreifer gefälschte DHCP-Offer-Pakete an diesen Client senden und ihm so z. B. ein präpariertes Default-Gateway vorsetzen (DHCP-Spoofing).

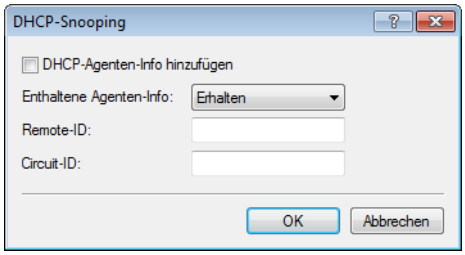
Das DHCP-Snooping ermöglicht Geräten, die DHCP-Pakete empfangen und weiterleiten, diese Datenpakete zu analysieren, zu verändern und anhand bestimmter Kriterien zu filtern. Die zusätzlich eingefügten Informationen über die Herkunft von DHCP-Paketen ermöglichen es einem DHCP-Server einerseits, umfangreiche Netzen besser zu verwalten. Anderseits kann ein Angreifer, in dessen DHCP-Paketen diese Zusatzinformationen fehlen, nicht mehr einfach in DHCP-Verhandlungen zwischen DHCP-Server, DHCP-Relay-Agent und DHCP-Client stören.

Der Access Point unterstützt DHCP-Snooping auf Layer-2. Damit ist es ihm z. B. möglich, Informationen (z. B. die SSID) in die empfangenen DHCP-Pakete des Clients auf dem WLAN einzufügen, bevor er sie anschließend in das LAN weiterleitet. Der Access Point fügt dazu die DHCP Relay Agent Information Option (Option 82) nach RFC 3046 ein.

Im LANconfig können Sie das DHCP-Snooping unter **Schnittstellen** > **Snooping** mit einem Klick auf **DHCP-Snooping** für jede Schnittstelle separat festlegen.



Nach Auswahl der entsprechenden Schnittstelle können Sie die folgenden Einstellungen festlegen:



DHCP-Agenten-Info hinzufügen

Bestimmen Sie hier, ob der DHCP-Relay-Agent den ankommenden DHCP-Paketen die DHCP-Option "Relay Agent Info" (Option 82) anfügen bzw. eine vorhandene "Relay Agent Info" bearbeiten soll, bevor er die Anfrage an einen DHCP-Server weiterleitet.

Die "Relay Agent Info" setzt sich aus den Werten für **Remote-ID** und **Circuit-ID** zusammen.

Erhaltene Agenten-Info

Bestimmen Sie hier, wie der DHCP-Relay-Agent mit der "Relay Agent Info" in ankommenden DHCP-Datenpaketen umgehen soll. Folgende Einstellungen sind möglich:

- erhalten: In dieser Einstellung leitet der DHCP-Relay-Agent ein DHCP-Paket mit vorhandener "Relay Agent Info" ohne Veränderung an den DHCP-Server weiter.
- ersetzen: In dieser Einstellung ersetzt der DHCP-Relay-Agent eine vorhandene "Relay Agent Info" durch die in den Feldern **Remote-ID** und **Circuit-ID** vorgegebenen Werte.
- Paket verwerfen: In dieser Einstellung löscht der DHCP-Relay-Agent ein DHCP-Paket, das eine "Relay Agent Info" enthält.

Remote-ID

Die Remote-ID ist eine Unteroption der "Relay Agent Info"-Option und kennzeichnet eindeutig den Client, der einen DHCP-Request stellt.

Circuit-ID

Die Circuit-ID ist eine Unteroption der "Relay Agent Info"-Option und kennzeichnet eindeutig die Schnittstelle, über die ein Client einen DHCP-Request stellt.

Sie können die folgenden Variablen für **Remote-Id** und **Circuit-Id** verwenden:

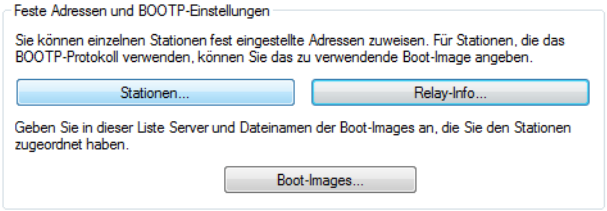
- `%%`: fügt ein Prozent-Zeichen ein.
- `%c`: fügt die MAC-Adresse der Schnittstelle ein, auf der der Relay-Agent den DHCP-Request erhalten hat. Handelt es sich um eine WLAN-SSID, ist das die entsprechende BSSID.
- `%i`: fügt den Namen der Schnittstelle ein, auf der der Relay-Agent den DHCP-Request erhalten hat.
- `%n`: fügt den Namen des DHCP-Relay-Agents ein, wie er z. B. unter **Setup** > **Name** festgelegt ist.
- `%v`: fügt die VLAN-ID des DHCP-Request-Pakets ein. Diese VLAN-ID stammt entweder direkt aus dem VLAN-Header des DHCP-Datenpakets oder aus der VLAN-ID-Zuordnung für diese Schnittstelle.
- `%p`: fügt den Namen der Ethernet-Schnittstelle ein, die das DHCP-Datenpaket empfangen hat. Diese Variable ist hilfreich bei Geräten mit eingebautem Ethernet-Switch oder Ethernet-Mapper, da diese mehr als eine physikalische Schnittstelle auf eine logische Schnittstelle mappen können. Bei anderen Geräten sind `%p` und `%i` identisch.
- `%r`: fügt die schnittstellenunabhängige und systemweit gültige MAC-Adresse des Gerätes ein, welches den DHCP-Request erhalten hat.
- `%s`: fügt die WLAN-SSID ein, wenn das DHCP-Paket von einem WLAN-Client stammt. Bei anderen Clients enthält diese Variable einen leeren String.

- `%e`: fügt die Seriennummer des Relay-Agents ein, wie sie z. B. unter **Status** > **Hardware-Info** > **Seriennummer** zu finden ist.

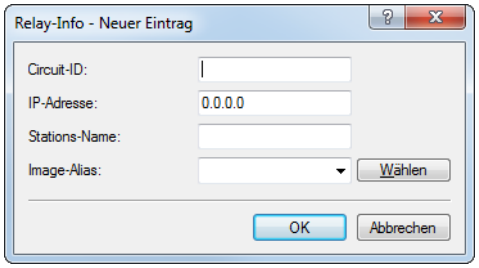
20.1.10 Zuweisung von IP-Adressen basierend auf DHCP-Option 82

IP-Adressen können mittels DHCP unter Nutzung der Option 82 in Abhängigkeit des Switchports zugewiesen werden, an den das Endgerät angeschlossen ist. Der jeweilige Switch fügt an die DHCP-Anfrage per DHCP-Option 82 die Circuit-ID hinzu, die den Port bezeichnet, an dem dieses Gerät angeschlossen ist. Diese Information kann dann von DHCP-Server verwendet werden, um eine bestimmte IP-Adresse zuzuweisen. Dadurch wird ein Bezug zwischen einer IP-Adresse und einem Ort hergestellt. Dadurch wird die Netzüberwachung vereinfacht.

Im LANconfig können Sie die Zuweisung der IP-Adressen basierend auf dem Switchport unter **IPv4** > **BOOTP** mit einem Klick auf **Relay-Info** für jeden Port separat festlegen.



Nach Auswahl des per DHCP-Option 82 automatisch hinzugefügten Switchports können Sie die folgenden Einstellungen festlegen:



Circuit-ID

Hier wird die vom Relay-Agent oder Switch per DHCP-Option 82 eingefügte „Circuit-ID" abgelegt, die zur Auswahl der Adresszuweisung dienen soll. Der enthaltene String wird case-sensitive ausgewertet. Abhängig von dem jeweiligen Switch wird die „Circuit-ID" vom Relay-Agent in verschiedenen Formaten geliefert und dementsprechend abgelegt. Dies kann ein kompletter Hexadezimaler-String mit führendem 0x sein. Alternativ kann die Syntax genutzt werden, die es auch beim User-Class-Identifier oder Vendor-Class-Identifier erlaubt, Binärwerte einzugeben:

Dabei werden Binärwerte in der Form `{Wert/Bitlänge}` angegeben. Der Wert kann dabei dezimal, hexadezimal (führendes 0x) oder oktal (führende 0) angegeben werden, während für die Bitlänge die Stufen 8, 16, 24, 32, 48 und 64 zur Verfügung stehen. Der Wert wird dabei in Big-Endian-Darstellung abgelegt. Soll der Wert in Little-Endian-Darstellung abgelegt werden, so sind „negative" Bitlängen anzugeben: -8, -16, -24, -32, -48 oder -64

Eine Circuit-ID (00 02 00 1e 4d 45 53 2d 33 37 32 38) kann somit in einer der folgenden Darstellungen abgelegt werden:

- 0x0002001e4d45532d33373238
- {0/8}{2/8}{30/16}MES-3728
- {0x00/8}{0x02/8}{0x1e/16}MES-3728
- {00/8}{02/8}{036/16}MES-3728

IP-Adresse

Geben Sie hier die IP-Adresse ein, die dem Host an diesem Port zugewiesen wird. Diese Spalte darf nicht unspezifiert (0.0.0.0) sein. Das führt letztendlich dazu, daß sich pro Circuit-ID immer nur ein Host anmelden darf. Solange also hier Eintrag in der DHCP-Tablle existiert, werden alle DHCP-Nachrichten anderer Hosts auf der gleichen Circuit-ID ignoriert. D. h., will man einen anderen Host an dem Port betreiben, so muss sich der bisherige entweder korrekt abmelden (z. B. unter Microsoft Windows: `ipconfig /release`) oder aber der Eintrag muss aus der DHCP-Tabelle gelöscht werden.

Stationsname

Geben Sie hier einen Namen ein, mit dem die Station identifiziert werden soll. Wenn eine Station ihren Namen nicht übermittelt, verwendet das Gerät den hier eingetragenen Namen.

Image-Alias

Wenn die Station das BOOTP-Protokoll verwendet, dann können Sie ein Boot-Image auswählen, über das die Station ihr Betriebssystem laden soll.

Geben Sie den Server, der das Boot-Image zur Verfügung stellt und den Namen der Datei auf dem Server in der Boot-Image-Tabelle ein.

20.1.11 Parameter der LANCOM Management Cloud durch den DHCP-Server ausliefern

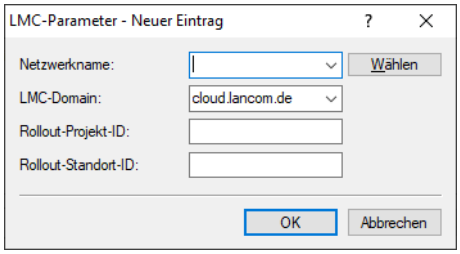
Der DHCP-Server verteilt in seinen DHCP-Paketen auch die DHCP-Option 43 (Vendor Specific Option) an anfragende Clients im Netz. Hierin enthalten ist der Domain-Name, welcher für den Betrieb des Gerätes durch die LANCOM Management Cloud (LMC) erforderlich ist. Auf diese Weise kann ein Gerät direkt mit einer privaten LMC-Installation kommunizieren, ohne vorab konfiguriert zu sein.

Wenn Sie ein LCOS-Gerät als DHCP-Server verwenden, hinterlegen Sie die LMC-Domain im Klartext in der Konfiguration. Der LCOS-interne DHCP-Server fügt die Domain der DHCP-Option 43 hinzu und liefert sie im Antwortpaket an anfragende LCOS-Geräte aus. Dazu wertet der DHCP-Server die DHCP-Option 60 (Vendor Class Identifier) in den DHCP-Requests der Clients aus. Eine so konfigurierte DHCP-Option 43 hat Vorrang vor einer in der DHCP-Options-Tabelle des DHCP-Servers manuell konfigurierten DHCP-Option 43.

Der Vendor Class Identifier muss im Request `LANCOM` beinhalten. Stellt das Gerät eines anderen Herstellers einen Request an den LCOS-internen DHCP-Server, wird ihm die DHCP-Option 43 im Antwortpaket nicht angeboten.

20.1.11.1 Konfiguration

Die LMC-Domain konfigurieren Sie für die einzelnen Netze in LANconfig unter **IPv4** > **DHCPv4** > **LMC-Parameter**.



Netzwerkname

Geben Sie hier das Netz an, in welches das Gerät die LMC-Domain über die DHCP-Option 43 ausliefert.

LMC-Domain

Geben Sie hier den Domain-Namen der LANCOM Management Cloud an.

Standardmäßig ist die Domain für den ersten Verbindungsaufbau mit der public LMC eingetragen. Möchten Sie Ihr Gerät von einer eigenen Management Cloud verwalten lassen ("private Cloud" oder "on premise installation"), tragen Sie bitte die entsprechende LMC-Domain ein.

20.2 Domain-Name-Service (DNS)

Der Domain-Name-Service (DNS) stellt in TCP/IP-Netzen die Verknüpfung zwischen Rechnernamen bzw. Netzwerknamen (Domains) und IP-Adressen her. Dieser Service ist auf jeden Fall erforderlich für die Kommunikation im Internet. Aber auch innerhalb eines lokalen Netzes oder bei der LAN-Kopplung ist es sinnvoll, die IP-Adressen im LAN den Namen der Rechner eindeutig zuordnen zu können.

20.2.1 Was macht ein DNS-Server?

Die bei einem DNS-Server nachgefragten Namen bestehen aus mehreren Teilen: Ein Teil besteht aus dem eigentlichen Namen des Hosts oder Dienstes, der angesprochen werden soll, ein anderer Teil kennzeichnet die Domain. Innerhalb eines lokalen Netzes ist die Angabe der Domain optional. Diese Namen können also z. B. „www.domain.com“ oder „ftp.domain.com“ heißen.

Ohne DNS-Server im lokalen Netz wird jeder lokal unbekannte Name über die Default-Route gesucht. Durch die Verwendung eines DNS-Servers können alle Namen, die mit ihrer IP-Adresse bekannt sind, direkt bei der richtigen Gegenstelle gesucht werden. Der DNS-Server kann dabei im Prinzip ein separater Rechner im Netz sein. Folgende Gründe sprechen jedoch dafür, die Funktionen des DNS-Servers direkt im Gerät anzusiedeln:

- Das Gerät kann in der Betriebsart als DHCP-Server die IP-Adressen für die Rechner im lokalen Netz selbstständig verteilen. Der DHCP-Server kennt also schon alle Rechner im eigenen Netz, die ihre IP-Adresse per DHCP beziehen, mit Rechnername und IP-Adresse. Ein externer DNS-Server hätte bei der dynamischen Adressvergabe des DHCP-Servers möglicherweise Schwierigkeiten, die Zuordnung zwischen IP-Adresse und Namen aktuell zu halten.
- Der DNS-Server im Gerät kann gleichzeitig als sehr komfortabler Filtermechanismus eingesetzt werden. Anfragen nach bestimmten Domains, die nicht besucht werden dürfen, können durch die einfache Angabe des Domain-Namens für das ganze LAN, nur für Teilnetze (Subnetze) oder sogar für einzelne Rechner gesperrt werden.

20.2.1.1 Wie reagiert der DNS-Server auf eine Anfrage?

Der DNS-Server bezieht bei Anfragen nach bestimmten Namen alle Informationen in die Suche mit ein, die ihm zur Verfügung stehen:

- Zuerst prüft der DNS-Server, ob der Zugriff auf diesen Namen nicht durch die Filterliste verboten ist. Wenn das der Fall ist, wird der anfragende Rechner mit einer Fehlermeldung darüber informiert, dass er auf diesen Namen nicht zugreifen darf.
- Dann sucht er in der eigenen statischen DNS-Tabelle nach Einträgen für den entsprechenden Namen.
- Steht in der DNS-Tabelle kein Eintrag für diesen Namen, wird die dynamische DHCP-Tabelle durchsucht. Die Verwendung der DHCP-Informationen kann bei Bedarf ausgeschaltet werden.
- Schließlich prüft der DNS-Server, ob die Anfrage über ein WAN-Interface an einen anderen DNS-Server weitergeleitet werden soll (Spezielles DNS-Forwarding über die DNS-Destinationstabelle).

Sollte der gesuchte Name in allen verfügbaren Informationen nicht gefunden werden, leitet der DNS-Server die Anfrage über den generellen DNS-Forwarding-Mechanismus an einen anderen DNS-Server (z. B. beim Internet-Provider) weiter oder schickt dem anfragenden Rechner eine Fehlermeldung.

20.2.2 DNS-Forwarding

Wenn eine Anfrage nicht aus den eigenen DNS-Tabellen bedient werden kann, leitet der DNS-Server die Anfrage an andere DNS-Server weiter. Dieser Vorgang heißt DNS-Forwarding (DNS-Weiterleitung).

Dabei unterscheidet man zwischen

- speziellem DNS-Forwarding

  Anfragen nach bestimmten Namensbereichen werden an bestimmte DNS-Server weitergeleitet.

- generellem DNS-Forwarding

  Alle anderen nicht näher spezifizierten Namen werden an den „übergeordneten" DNS-Server weitergeleitet.

20.2.2.1 Spezielles DNS-Forwarding

Beim speziellen DNS-Forwarding können Namensbereiche definiert werden, für deren Auflösung festgelegte DNS-Server angesprochen werden.

Ein typischer Anwendungsfall für spezielles DNS-Forwarding ergibt sich beim Heimarbeitsplatz: Der Benutzer möchte gleichzeitig sowohl auf das firmeneigene Intranet als auch direkt auf das Internet zugreifen können. Die Anfragen ins Intranet müssen an den DNS-Server der Firma, alle anderen Anfragen an den DNS-Server des Internet-Providers geleitet werden.

20.2.2.2 Generelles DNS-Forwarding

Alle DNS-Anfragen, die nicht auf sonstige Weise aufgelöst werden können, werden an einen generellen DNS-Server weitergeleitet. Diese können in den folgenden Menüs bzw. Konsolen-Pfaden konfiguriert werden:

LANconfig	**IPv4** > **Adressen** > **Nameserver-Adressen** > **Erster DNS** | **Zweiter DNS**
CLI	**Setup** > **TCP-IP** > **DNS-Default**
	Setup > **TCP-IP** > **DNS-Backup**

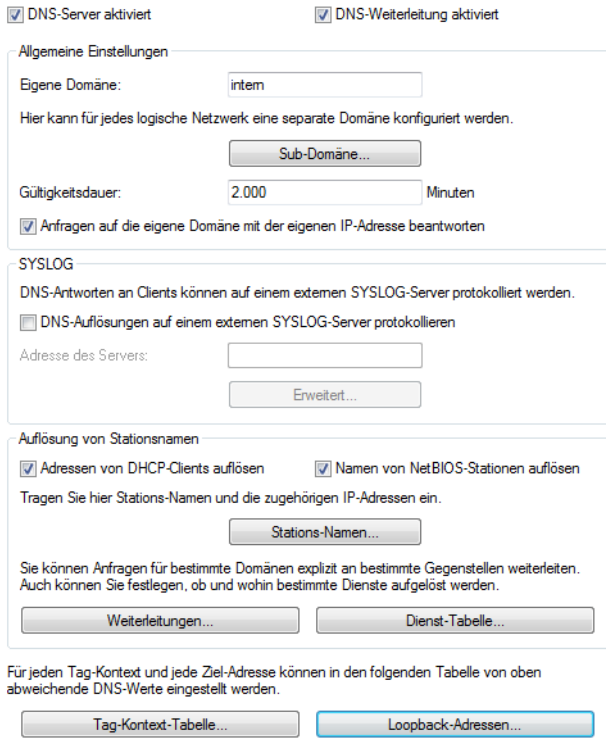
Wird hier ein DNS-Server angegeben, muss dieser als **Erster DNS** hinterlegt werden. Optional kann ein zweiter DNS-Server zwecks Redundanz als **Zweiter DNS** hinterlegt werden.

- Für das DNS-Forwarding wird immer zuerst ein DNS-Server herangezogen, der der Internet-Verbindung zugewiesen wurde (manuell oder automatisch).
- Falls der Internet-Verbindung kein DNS-Server zugewiesen wurde oder keiner der zugewiesenen DNS-Server antwortet, erfolgt ein Fallback auf den generellen DNS-Server.

Durch dieses Verfahren benötigen Sie keine Kenntnisse über die Adressen eines DNS-Servers. Der Eintrag der Intranet-Adresse Ihres Routers als DNS-Server bei den Arbeitsplatzrechnern reicht aus, um die Namenszuordnung zu ermöglichen. Außerdem wird damit die Adresse des DNS-Servers automatisch aktualisiert. Sollte z. B. der Provider, der diese Adresse mitteilt, seinen DNS-Server umbenennen, oder sollten Sie zu einem anderen Provider wechseln, erhält Ihr lokales Netz stets die aktuellen Informationen.

20.2.3 So stellen Sie den DNS-Server ein

Die Einstellungen für den DNS-Server finden Sie in LANconfig unter **DNS** > **Allgemein**.



1. Aktivieren Sie den DNS-Server, indem Sie die Option **DNS-Server aktiviert** markieren.

   Soll der DNS-Server die DNS-Anfrage an einen anderen DNS-Server weiterleiten (DNS-Forwarding), markieren Sie zusätzlich die Option **DNS-Weiterleitung aktiviert**.

2. Geben Sie die eigene Domain ein, in der sich der DNS-Server befindet.

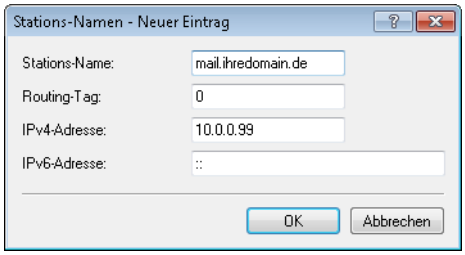
   Mit Hilfe dieser Domain erkennt der DNS-Server bei DNS-Anfragen, ob sich der gesuchte Name im eigenen LAN befindet oder nicht. Die Angabe der Domain ist optional.

3. Geben Sie an, ob der DNS-Server die Client-Informationen aus dem DHCP-Server verwenden soll.
4. Tragen Sie bekannte Gegenstellen und deren IP-Adressen in die Tabelle **Stations-Namen** ein.

   Der DNS-Server dient hauptsächlich dazu, Anfragen nach öffentlichen Adressen im Internet von den Anfragen nach Adressen bei anderen Gegenstellen zu trennen. Tragen Sie daher alle Rechner in die Tabelle ein,

   - deren Name und IP-Adresse Sie kennen,
   - die nicht im eigenen LAN liegen,
   - die nicht im Internet liegen und
   - die über den Router erreichbar sind.

Wenn Sie z. B. in einem externen Büro oder in einer Filiale arbeiten und die Mitarbeiter über den Router den Mailserver in der Zentrale (Name: „mail.ihredomain.de“, IP: „10.0.0.99“) erreichen wollen, tragen Sie ein:



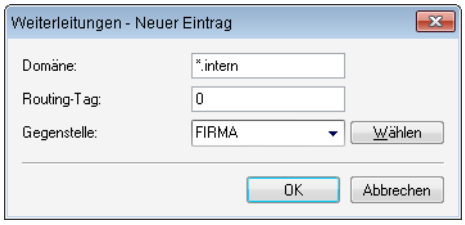
Die Angabe der Domain ist dabei optional, aber zu empfehlen.

Wenn ein Mitarbeiter nun sein Mailprogramm startet, sucht es automatisch den Server „mail.ihredomain.de“ . Der DNS-Server gibt daraufhin die IP-Adresse „10.0.0.99“ zurück. Das Mailprogramm startet dann eine Verbindung zu dieser IP-Adresse. Mit entsprechenden Einträgen in der IP-Routing-Tabelle und Gegenstellenliste des Routers baut das Mailprogramm die Verbindung zum Mailserver im Netz der Zentrale auf.

5. Um ganze Namensbereiche von einem anderen DNS-Server auflösen zu lassen, fügen Sie einen Weiterleitungseintrag bestehend aus Namensbereich und Gegenstelle hinzu.

   Bei der Angabe der Namensbereiche dürfen Sie die Wildcards „?“ für einzelne Zeichen und „*“ für mehrere Zeichen verwenden.

   Um alle Domains mit der Endung „.intern“ auf einen DNS-Server im LAN der Gegenstelle „FIRMA“ umzuleiten, erstellen Sie folgenden Eintrag:



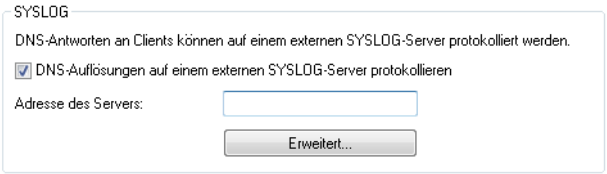
Der DNS-Server kann entweder über den Name der Gegenstelle (für automatische Konfiguration über PPP) oder die explizite IP-Adresse des zuständigen Nameservers angegeben werden.

20.2.4 Protokollierung von DNS-Anfragen über SYSLOG

Um Anfragen von Clients an den DNS-Server zu dokumentieren, besteht die Möglichkeit, dass der DNS-Server im Gerät die Antworten an den Client auch laufend in Form einer SYSLOG-Meldung an einen SYSLOG-Server sendet.

Bitte beachten Sie, dass eine Aufzeichnung der DNS-Anfragen nur gemäß der in ihrem Land gültigen Datenschutzbestimmungen erfolgen darf.

In LANconfig konfigurieren Sie die Dokumentation von DNS-Anfragen unter **DNS** > **Allgemein** im Abschnitt **SYSLOG**.



DNS-Auflösungen auf einem externen SYSLOG-Server protokollieren

Diese Option aktiviert oder deaktiviert (Default-Einstellung) den Versand von SYSLOG-Meldungen bei DNS-Anfragen.

Dieser Schalter ist unabhängig vom globalen Schalter im Syslog-Modul unter **Meldungen** > **Allgemein** > **SYSLOG**. D. h., wenn Sie hier die Option zur Aufzeichnung der DNS-Anfragen aktivieren, sendet der DNS-Server auch bei global deaktiviertem SYSLOG-Modul die entsprechenden SYSLOG-Meldungen an einen SYSLOG-Server.

Jede DNS-Auflösung (`ANSWER`-Record oder `ADDITIONAL`-Record) erzeugt jeweils eine SYSLOG-Meldung mit dem Aufbau `PACKET_INFO: DNS for IP-Address, TID {Hostname}: Ressource-Record`.

Dabei haben die Parameter die folgenden Bedeutungen:

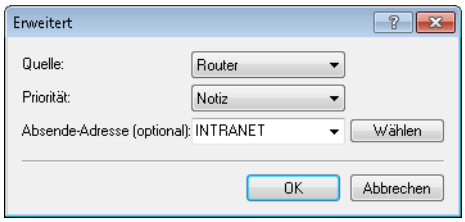
- Die `TID` (Transaction-ID) enthält einen 4-stelligen Hexadezimal-Code.
- Der `{Hostname}` ist nur dann Bestandteil der Meldung, wenn der DNS-Server ihn ohne DNS-Anfrage auflösen kann (wie auch im Firewall-Log).
- Die `Ressource-Record` besteht aus drei Teilen: Der Anfrage, dem Typ bzw. der Klasse und der IP-Auflösung (z. B. `www.mydomain.com STD A resolved to 193.99.144.32`)

Adresse des Servers

Geben Sie hier die Adresse des SYSLOG-Servers ein. Die Eingabe als IPv4-/IPv6-Adresse oder als DNS-Name ist möglich.

Die Angabe der IP-Adressen `127.0.0.1` und `::1` ist generell nicht erlaubt, um so die Nutzung eines externen Servers zu erzwingen.

Um die SYSLOG-Meldung zu konfigurieren, klicken Sie auf **Erweitert**.



Quelle

Wählen Sie hier aus, welche Quelle in den SYSLOG-Meldungen eingetragen ist.

Priorität

Wählen Sie hier aus, welche Priorität in den SYSLOG-Meldungen eingetragen ist.

Absende-Adresse (optional)

Geben Sie hier optional eine andere Adresse (Name oder IP) an, mit der Ihr Gerät gegenüber dem SYSLOG-Server als Absender auftritt. Standardmäßig verwendet Ihr Gerät seine Adresse aus dem jeweiligen ARF-Kontext, ohne dass Sie diese hier angeben müssen. Durch Angabe einer optionalen Loopback-Adresse verändern Sie die Quelladresse bzw. Route, mit der Ihr Gerät die Gegenstelle anspricht. Dies kann z. B. dann sinnvoll sein, falls Ihr Gerät über verschiedene Wege erreichbar ist und die Gegenstelle einen bestimmten Weg für ihre Antwort-Nachrichten wählen soll.

Sofern die hier eingestellte Absende-Adresse eine Loopback-Adresse ist, wird diese auch auf maskiert arbeitenden Gegenstellen **unmaskiert** verwendet.

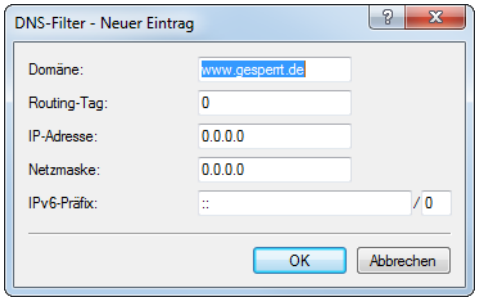
Mehr Informationen über SYSLOG und die zur Verfügung stehenden Einstellungen finden Sie im Abschnitt *Das SYSLOG-Modul*.

20.2.5 URL-Blocking

1. Mit der Filterliste können Sie schließlich den Zugriff auf bestimmte Namen oder Domains sperren.

   Um die Domain (in diesem Fall den Web-Server) „www.gesperrt.de“ für alle Rechner im LAN zu sperren, sind die folgenden Befehle und Eingaben notwendig:

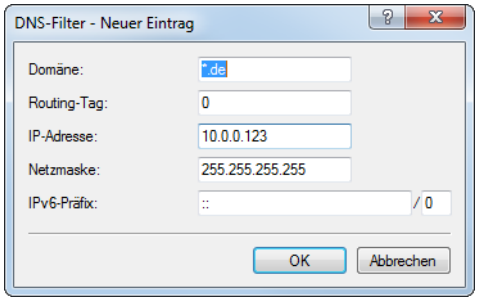
LANconfig	**DNS** > **Filter/Aliase** > **DNS Filter** > **Hinzufügen**
CLI	`cd Setup/DNS/Filter-Liste set 001 www.gesperrt.de 0.0.0.0 0.0.0.0`



   Der Index „001“ kann bei der Konfiguration über CLI frei gewählt werden und dient nur der eindeutigen Bezeichnung des Eintrags.

   Bei der Eingabe der Domäne sind auch die Wildcards '?' (steht für genau ein Zeichen) und '*' (für beliebig viele Zeichen) erlaubt.

   Um nur einem bestimmten Rechner (z. B. mit IP 10.0.0.123) den Zugriff auf DE-Domains zu sperren, tragen Sie folgende Werte ein:



   Im Konsolenmodus lautet der Befehl:

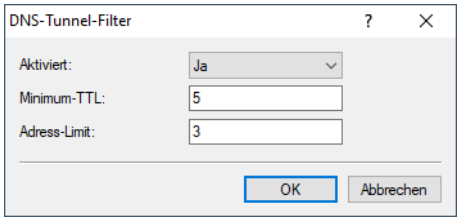
   ```
   set 002 *.de 10.0.0.123 255.255.255.255
   ```

   Die Hitliste in der DNS-Statistik zeigt Ihnen die 64 Namen, die am häufigsten nachgefragt werden, und bietet Ihnen damit eine gute Basis für die Einstellung der Filter-Liste.

Durch die geeignete Wahl von IP-Adressen und Netzmasken können bei der Verwendung von Subnetting in Ihrem LAN auch einzelne Abteilungen gefiltert werden. Dabei steht die IP-Adresse „0.0.0.0“ jeweils für alle Rechner in einem Netz, die Netzmaske „0.0.0.0“ für alle Netze.

20.2.6 DNS-Filter für DNS-Datentunnel

Es gibt Verfahren und Tools, mit denen man durch DNS-Pakete Daten schleusen kann, um so bestimmte Prüfungen z. B. in der Firewall zu umgehen. Durch diesen Datentunnel können dann beliebige Daten über das DNS-Protokoll transportiert werden. Diese Methode ist zwar laut Protokoll standardkonform, in bestimmten Szenarien soll der Aufbau dieser Tunnel aber verhindert werden. Die Datentunnel werden an bestimmten Merkmalen bzw. Eigenschaften der DNS-Pakete erkannt.



LANconfig: **DNS** > **Filter/Aliase** > **DNS-Tunnel-Filter**

Konsole: **Setup** > **DNS** > **Tunnel-Filter**

Aktiviert

Über diesen Schalter kann der Tunnel-Filter aus- bzw. eingeschaltet werden.

Minimum-TTL

Minimale TTL ab der Ressource-Records akzeptiert werden. Wenn ein Record (mit Ausnahme von A und AAAA) eine kleinere TTL hat, so wird das komplette Paket verworfen.

Bereich: 0-99; Default: 5

Adress-Limit

Maximale Anzahl von A und AAAA Recordes mit einer TTL kleiner als Minimum-TTL, die noch akzeptiert werden, bevor das komplette Paket verworfen wird.

Bereich: 0-99; Default: 3

20.2.7 Dynamic DNS

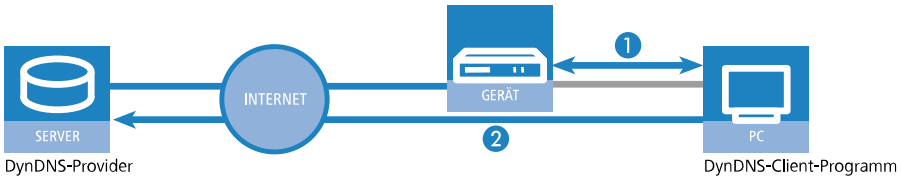
Damit auch Systeme mit dynamischen IP-Adressen über das WAN – also beispielsweise über das Internet – erreichbar sind, existieren eine Reihe von sog. Dynamic DNS-Server-Anbietern (z. B. www.dynDNS.org) oder der entsprechende Dienst der LANCOM Management Cloud.

Damit wird ein Gerät immer unter einem bestimmten Namen (FQDN – Fully Qualified Domain Name) erreichbar (z. B. „http://MyDevice.dynDNS.org“).

Der Vorteil liegt auf der Hand: Wenn Sie z. B. über den VPN-Client auf eine Außenstelle mit dynamischer IP-Adresse zugreifen wollen, dann brauchen Sie lediglich den Dynamic DNS-Namen zu kennen.

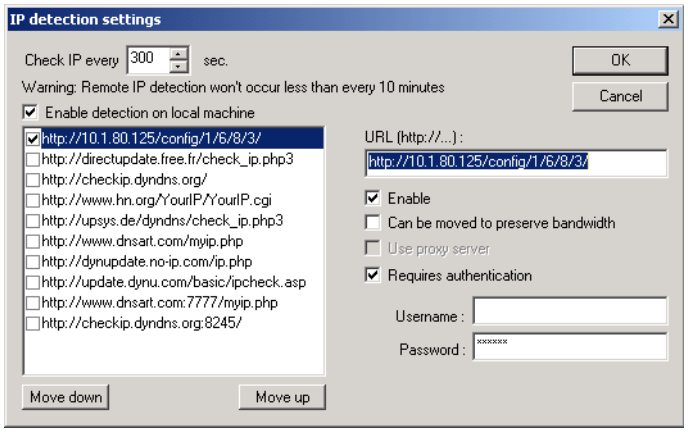
20.2.7.1 Wie gelangt die aktuelle IP-Adresse zum Dynamic-DNS-Server?

Dynamic-DNS-Anbieter unterstützen eine Reihe von PC-Clientprogrammen, die über verschiedene Methoden die aktuell zugewiesene IP-Adresse eines Geräts ermitteln können **1**, und im Falle einer Änderung an den jeweiligen Dynamic-DNS-Server übertragen **2**.

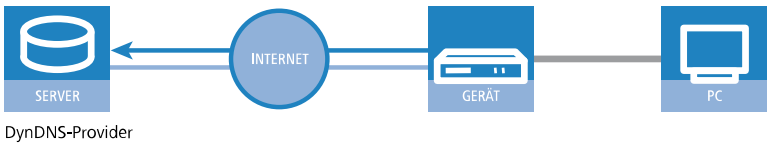


Die aktuelle WAN-seitige IP-Adresse eines Geräts kann unter folgender Adresse ausgelesen werden:

```
http://<Adresse des Geräts>/config/1/6/8/3/
```



Alternativ kann das Gerät die aktuelle WAN-IP auch direkt an den DynDNS-Anbieter übertragen:

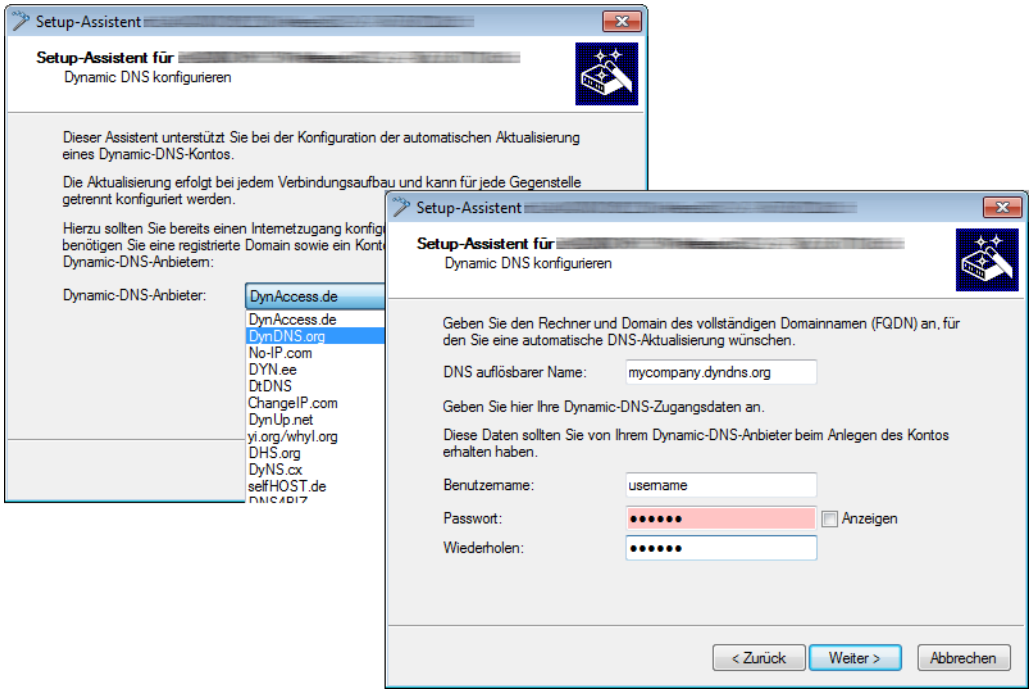


Dazu wird eine Aktion definiert, die z. B. nach jedem Verbindungsaufbau automatisch eine HTTP-Anfrage an den DynDNS-Server sendet, dabei die benötigten Informationen über das DynDNS-Konto übermittelt und so ein Update der Registrierung auslöst. Eine solche HTTP-Anfrage an den Anbieter DynDNS.org sieht z. B. so aus:

› http://Username:Password@members.dyndns.org/nic/update?system=dyndns&hostname=%h&myip=%a

Damit werden der Hostname der Aktion und die aktuelle IP-Adresse des Geräts an das durch Username und Password spezifizierte Konto bei DynDNS.org übermittelt, der entsprechende Eintrag wird aktualisiert.

Die dazu notwendigen Einstellungen können komfortabel mit dem Setup-Assistenten von LANconfig vorgenommen werden:



Der Setup-Assistent ergänzt die beschriebene Basis-Aktion um weitere anbieterspezifische Parameter, die hier nicht näher beschrieben werden. Außerdem legt der Setup-Assistent weitere Aktionen an, mit denen das Verhalten des Geräts gesteuert wird für den Fall, dass die Aktualisierung nicht im ersten Durchlauf erfolgreich durchgeführt werden konnte.

20.3 Accounting

In der Accounting-Tabelle werden Informationen über die Verbindungen der Clients im eigenen Netzwerk zu verschiedenen Gegenstellen mit Angabe der Verbindungszeit und der übertragenen Datenvolumen gespeichert. Mit Hilfe von Accounting-Snapshots können die Accounting-Daten zu bestimmten Zeitpunkten regelmäßig für eine weitere Auswertung festgehalten werden.

Neben IPv4 wird natürlich auch IPv6 unterstützt. Zusätzlich gibt es eine Funktion zur Darstellung des aktuellen Datendurchsatzes von einzelnen Stationen oder logischen Schnittstellen im Netzwerk. Diese Funktion ist besonders zu Analysezwecken geeignet, wenn geprüft werden soll, welche Station im Netzwerk zur aktuellen Zeit welchen Datenverkehr versursacht. Damit können z. B. Stationen identifiziert werden, die die Internetverbindung auslasten oder über welche Schnittstelle wie viel Datenverkehr zum aktuellen Zeitpunkt läuft.

Aus Performance-Gründen wird empfohlen, diese Funktion nur zur Zeit der laufenden Analyse zu aktivieren und danach wieder zu deaktivieren. Für eine umfangreichere Überwachung des Datenverkehrs wird Netflow in Zusammenhang mit einem externen Collector empfohlen.

Um die Analyse-Funktion zu nutzen, verwenden Sie die Kommandozeile und setzen unter /setup/accounting den Schalter „Aktiv“ auf „Ja“. Setzen Sie das „Intermittent-Reporting-Intervall“ auf einen kleinen Wert in Sekunden, z. B. 5 Sekunden.

Um die Funktion nach der Analyse wieder zu deaktivieren, setzen Sie den Schalter „Aktiv“ auf „Nein“.

Verwenden Sie zur Anzeige des aktuellen Durchsatzes pro Benutzer das Kommando „show accounting users“.

```
show accounting users

Username   Interface      Rx-Total     Tx-Total      Rx-IPv4      Tx-IPv4  Rx-IPv6  Tx-IPv6
=============================================================================================
```

```
192.168.1.7 INTERNET       0 Bit/s    115 Bit/s      0 Bit/s    115 Bit/s  0 Bit/s  0 Bit/s
192.168.1.9 INTERNET   9.38 KBit/s  3.92 KBit/s  9.38 KBit/s  3.92 KBit/s  0 Bit/s  0 Bit/s

Next update of accounting bandwidth data in: 3s
```

Alternativ zum Show-Kommando kann auch die Status-Tabelle /status/accounting/benutzer-bandbreitenverbauch aufgerufen werden.

Das Show-Kommando hat mehre Optionen, die mit ? angezeigt werden können:

```
> show accounting ?
Anzeige von Kurzzeit-Bandbreiten-Statistikdaten des Accountings.
HINWEIS: Das Accounting muss eingeschaltet und das Intermittent-Reporting-Intervall gesetzt sein. Alle
Bandbreiten-Daten werden in diesem Intervall aktualisiert.
VERWENDUNG:
show accounting-bandwidth <BEFEHL> [FLAGS]:

BEFEHLE:
  interfaces:             Im Accounting aufgezeichneter Bandbreitenverbrauch, aufgeschluesselt nach Interfaces

  users:                   Im Accounting aufgezeichneter Bandbreitenverbrauch, aufgeschluesselt nach Benutzern
 und Interfaces

FLAGS:
  -bps:                    Gibt alle Werte in der Einheit Bit/s ohne Nachkommastellen aus
  -kbps:                   Gibt alle Werte in der Einheit KBit/s mit 3 festen Nachkommastellen aus
  -mbps:                   Gibt alle Werte in der Einheit MBit/s mit 3 festen Nachkommastellen aus
  -gbps:                   Gibt alle Werte in der Einheit GBit/s mit 3 festen Nachkommastellen aus
        HINWEIS: Nur eines der Einheiten-Flags kann gleichzeitig angegeben werden. Wird keines angegeben, wird
 die Einheit automatisch bestimmt und die Ausgabe erfolgt mit 3 signifikanten Stellen.
  -compact:               Beschraenkt die Ausgabe auf den Gesamt-Bandbreitenverbrauch je Uebertragungsrichtung

 -totals-only:            (nur fuer Befehl 'users') Zeigt die Benutzer-Bandbreiten nicht fuer jedes Interface
 gesondert an, sondern aufsummiert
```

Beispiele:

„show accounting interfaces" zeigt die Auslastung bzw. aktuellen Datendurchsatz der Interfaces an. Diese Information findet sich auch in der Tabelle /Status/Accounting/Interface-Bandbreitenverbauch.

Mit dem Befehl „repeat 5 show accounting users" auf der Konsole können Sie das Kommando alle 5 Sekunden automatisch anzeigen lassen.

20.3.1 Arbeitsweise

Accounting-Benutzer werden über ihren Benutzernamen identifiziert. Potentielle Accounting-Benutzer sind:

- Alle Stationen im LAN (Benutzername ist ihre IPv4 oder IPv6-Adresse, oder, sofern er dem Router über DNS bekannt ist, der Hostname der Station)
- Alle VPN-Gegenstellen (Benutzername ist der Gegenstellenname)
- Alle eingewählten RAS-Clients (Benutzername ist die RAS-Client-ID; Mehrfacheinwahlen werden der selben ID zugeordnet)

Der vom Accounting gezählte Datenverkehr ist jeder Datenverkehr, der zwischen einem Benutzer und einer IP-Adresse hinter einem der folgenden Interfacetypen stattfindet (unabhängig ob Rx- oder Tx-Traffic):

- WAN
- RAS
- VPN

Bei einer Verbindung von z. B. VPN zu VPN wird der Traffic gezählt und für beide VPN-Benutzer getrennt verbucht.

Das Accounting zeichnet für jeden Benutzer den Datenverkehr mit jeder Gegenstelle separat auf. Das heißt: Datenverkehr von z. B. VPN zu WAN1 und Datenverkehr von VPN zu WAN2 sind separate Datensätze.

Das Accounting zeichnet jeweils aus Sicht des Benutzers sowohl eingehende und ausgehende Daten als auch IPv4- und IPv6-Traffic getrennt auf. Das bedeutet, dass ein IPv6-Datenpaket von z. B. VPN1 zu VPN2 für VPN1 als IPv6-Tx, und für VPN2 als IPv6-Rx gezählt wird.

Außerdem zeichnet das Accounting die Anzahl der aufgetretenen Datenströme (Sessions) auf, diese allerdings nicht getrennt nach Rx und Tx.

Bidirektionaler Datenverkehr wird als 2 Sessions gezählt, da 2 Datenströme vorliegen. Je ein aus Benutzersicht eingehender und ein ausgehender Datenstrom.

20.3.2 Ein- bzw. Ausschalten des Accountings im laufenden Betrieb

Die Prüfung, ob eine Datenverbindung vom Accounting gezählt wird, wird mit dem Aufbau der Verbindung (erstes Datenpaket) getroffen. Datenverbindungen, die bereits bestehen, wenn das Accounting eingeschaltet wird, werden vom Accounting nicht betrachtet.

Wird das Accounting im laufenden Betrieb ausgeschaltet, so werden die Datenverbindungen, die aktuell laufen, nicht mehr in die Accounting-Daten aufgenommen.

20.3.3 Zählung des Datenverkehrs

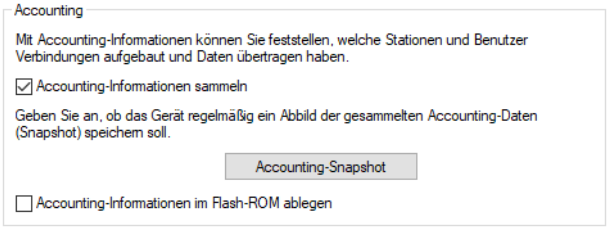
In der Standardeinstellung wird Traffic immer dann beim Accounting gemeldet, wenn eine Datenverbindung (in Form einer Firewallsession) endet, also etwa nach einem Timeout innerhalb der Firewall oder beim Schließen einer TCP-Verbindung. Bei lange laufenden Verbindungen kann das zu einer erheblichen Verzögerung führen, bis Datenverkehr tatsächlich in den Accounting-Statustabellen erscheint. Um dieses Problem zu behandeln, wurde eine Zwischenmeldungs-Funktionalität namens „Intermittent-Reporting" in das Accounting integriert, welche Teilaufzeichnungen in festen Intervallen beim Accounting einträgt. Wie oft dies passiert, wird über das Intermittent-Reporting-Intervall konfiguriert. Im Default ist dies auf 0 eingestellt; d. h. die Funktionalität ist deaktiviert. Wird dort ein Wert zwischen 1 und 30 eingetragen, so definiert diese Einstellung das Intervall in Sekunden, in dem Datenverbindungs-Zwischenmeldungen beim Accounting eingehen.

Die Zwischenmeldungen erhöhen die Systemlast abhängig von der Anzahl der aktiven Datenverbindungen. Die Zwischenmeldungen der Datenverbindungen werden unabhängig voneinander durchgeführt (also nicht alle auf einmal), um Lastspitzen zu vermeiden.

Das Intermittent Reporting kann bei laufendem Accounting jederzeit eingeschaltet werden, die erste Zwischenmeldung enthält dann den kompletten bis zum Einschaltzeitpunkt gemessenen Datenverkehr der einzelnen Datenflüsse.

20.3.4 Konfiguration des Accounting

Bei der Konfiguration des Accounting werden die allgemeinen Parameter festgelegt:



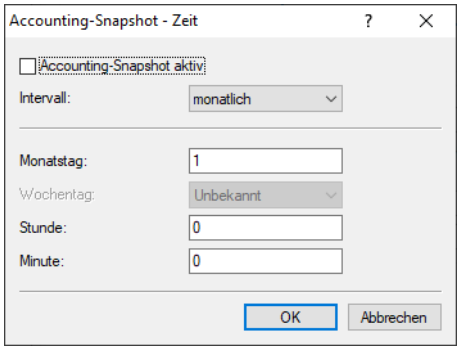
Konfigurationstool	Aufruf
LANconfig	**Management** > **Kosten**
CLI	**Setup** > **Accounting**

Accounting-Informationen sammeln

Accounting ein- oder ausschalten.

Accounting-Snapshot

Bei der Konfiguration des Snapshots wird das Intervall festgelegt, in dem die Accounting-Daten in einem Snapshot zwischengespeichert werden:



Accounting-Snapshot aktiv

Zwischenspeichern der Accounting-Daten ein- oder ausschalten.

Die Snapshot-Funktion kann nur dann genutzt werden, wenn das Gerät über eine gültige Systemzeit verfügt.

Intervall

Täglich, wöchentlich oder monatlich.

Monatstag

Der Tag im Monat, an dem die Zwischenspeicherung vorgenommen wird. Nur beim Intervall **monatlich** von Bedeutung.

Wochentag

Der Wochentag, an dem die Zwischenspeicherung vorgenommen wird. Nur beim Intervall **wöchentlich** von Bedeutung.

Stunde

Die Stunde, zu der die Zwischenspeicherung vorgenommen wird: 0 bis 23

Minute

Die Minute, zu der die Zwischenspeicherung vorgenommen wird: 0 bis 59

Accounting-Informationen im Flash-ROM ablegen

Accounting-Daten im Flashspeicher ein- oder ausschalten. Wenn die Accounting-Daten im Flash gespeichert werden, gehen sie auch bei Stromausfall nicht verloren.

20.4 Gebührenmanagement

Die Eigenschaft des Routers, Verbindungen selbstständig zu allen gewünschten Gegenstellen aufzubauen und sie mit dem Ende der Übertragung automatisch wieder zu beenden, ermöglicht dem Benutzer sehr komfortablen Zugriff z. B. auf das Internet. Bei der Datenübertragung über kostenpflichtige Leitungen können jedoch durch Fehlkonfiguration des Routers (z. B. bei der Filterkonfiguration) oder durch übermäßigen Gebrauch des Angebots (z. B. andauerndes Surfen im Internet) recht hohe Kosten entstehen.

Um diese Kosten zu begrenzen, bietet LCOS verschiedene Möglichkeiten:

› Die verfügbaren Online-Minuten können für eine bestimmte Periode eingeschränkt werden.

20.4.1 Verbindungs-Begrenzung für DSL und Kabelmodem

Auch wenn sich eine DSL- oder eine Kabelmodem-Verbindung wie eine Festverbindung verhält, bei der kein Verbindungsaufbau notwendig ist (und damit auch eigentlich weder Anfang noch Ende der Verbindung erkennbar sind), werden die Kosten je nach Provider zeitabhängig berechnet.

Im weiteren Verlauf dieses Abschnitts wird nur noch von DSL-Verbindungen die Rede sein. Die Ausführungen gelten aber genauso für jede andere Verbindung, die über den Ethernet-WAN-Anschluss des Geräts erfolgt, beispielsweise für Kabelmodem-Verbindungen.

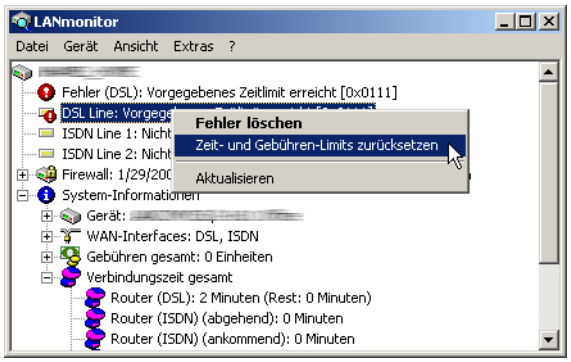
Um die Kosten begrenzen zu können, kann die maximale Verbindungsdauer mit Hilfe der Zeit gesteuert werden. Dazu wird ein Zeit-Limit für DSL-Verbindungen in einer Periode vereinbart. Im Auslieferungszustand dürfen die DSL-Verbindungen z. B. für maximal 600 Minuten in sechs Tagen genutzt werden.

Wird die Grenze eines Budgets erreicht, werden automatisch alle offenen DSL-Verbindungen beendet. Erst nach dem Ablauf der aktuellen Periode werden die Budgets wieder freigegeben und Verbindungen ermöglicht. Der Administrator kann die Budgets natürlich auch vorzeitig wieder freigeben!

Wenn für die Verbindung, die mit dem Gebührenbudget begrenzt werden soll, in der Gegenstellenliste eine Haltezeit von „0“ oder „9999“ Sekunden eingestellt ist, wird die Gebührenüberwachung ausgeschaltet, die Verbindung trotz Erreichen des Limits nicht unterbrochen.

Wenn Sie für einmalige Aktionen das Online-Budget verlängern wollen, z. B. um eine sehr große Datei aus dem Internet zu laden, müssen Sie nicht unbedingt das Zeit-Limit verändern. Sie können für solche Fälle manuell das Limit zurücksetzen.

Klicken Sie dazu mit der rechten Maustaste auf die Fehlermeldung im LANmonitor und wählen Sie im Kontextmenü den Eintrag **Zeit- und Gebührenlimit zurücksetzen**.



Sollten Sie in LANmonitor die System-Informationen nicht sehen, aktivieren Sie die entsprechende Anzeige mit **Ansicht** > **Anzeigen** > **System-Informationen**.

In WEBconfig und in der Konsole lauten die Befehle zur Freischaltung des zusätzlichen Zeit-Limits:

Konfigurationstool	Aufruf
WEBconfig	**LCOS-Menübaum** > **Setup** > **Gebuehren** > **Aktivieren-Reserve**

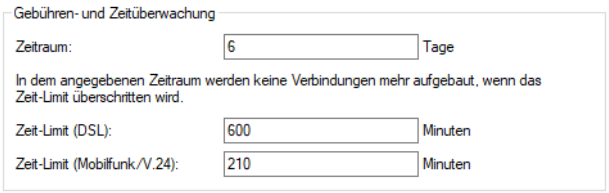
CLI	`cd /Setup/Gebuehren`
	
	`do Aktivieren-Reserve`

Bei Aktivierung des zusätzlichen Zeit-Limits wird dieses für die aktuelle Periode freigeschaltet. In der nächsten Periode gilt wieder das normale Zeit-Limit.

20.4.2 Einstellungen im Gebührenmodul

Im Gebührenmodul können Sie die Onlinezeit überwachen und für den Aufbauschutz nutzen.

Konfigurationstool	Aufruf
LANconfig	**Management** > **Kosten**
CLI	**Setup** > **Gebuehren**



Zeitraum

Dauer einer Überwachungsperiode in Tagen angegeben.

Online-Minuten-Budget

Maximale Online-Minuten in einer Überwachungsperiode.

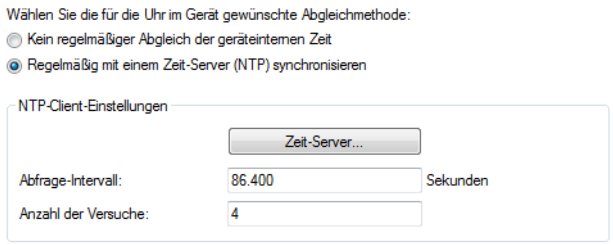
Die Informationen über die Gebühren und Verbindungszeiten werden über einen Bootvorgang hinaus gesichert (z. B. beim Einspielen einer neuen Firmware) und gehen erst verloren, wenn das Gerät ausgeschaltet wird. Alle hier erwähnten Zeitangaben werden in Minuten gemacht.

20.5 Zeit-Server für das lokale Netz

Router können hochgenaue Zeitinformationen entweder über ISDN oder über öffentlich zugängliche Zeit-Server im Internet (NTP-Server mit „Open Access"-Policy, z. B. von der Physikalisch-Technischen Bundesanstalt) beziehen. Die so ermittelte Zeit stellt das Gerät allen Stationen im lokalen Netz zur Verfügung.

20.5.1 Konfiguration des Zeit-Servers unter LANconfig

Damit ein Gerät die aktuelle Zeit im Netzwerk bekannt machen kann, aktivieren Sie unter **Datum/Zeit** > **Synchronisierung** den regelmäßigen Abgleich mit einem Zeitserver.



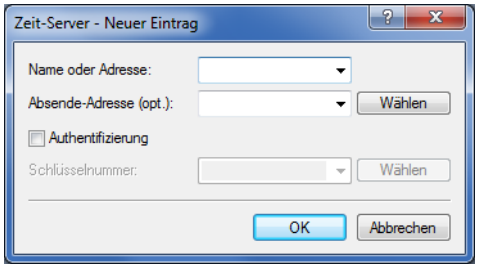
Abfrage-Intervall

Geben Sie hier das Zeitintervall in Sekunden an, nach dem eine Überprüfung und gegebenenfalls Neusynchronisierung der internen Uhr des Gerätes mit einem der angegebenen Zeit-Server (NTP) erfolgen soll.

Anzahl der Versuche

Geben Sie hier an, wie oft das Gerät eine Synchronisation mit dem Zeit-Server versuchen soll. Bei Angabe einer Null versucht das Gerät solange eine Verbindung, bis es eine gültige Synchronisation erreicht hat.

Im Abschnitt **NTP-Einstellungen** konfigurieren Sie anschließend unter **Zeit-Server** die Einstellungen für den Zeitabgleich mit dem entsprechenden Server.



Name oder Adresse

Geben Sie hier einen Zeit-Server (NTP) an, den das Gerät abfragen soll. Der Zeit-Server sollte über eines der vorhandenen Interfaces erreichbar sein.

Die Angabe einer Adresse ist möglich als FQDN, IPv4- oder IPv6-Adresse. Liefert die DNS-Namensauflösung für den Zeit-Server eine IPv6-Adresse zurück, bevorzugt das Gerät diese IPv6-Adresse.

Die Reihenfolge, in der das Gerät mehrere angegebene Zeit-Server abfragt, bestimmen Sie in der Übersicht der Einträge

Absende-Adresse (opt.)

Konfigurieren Sie hier optional eine Absendeadresse, die das Gerät statt der ansonsten automatisch für die Zieladresse gewählten Absendeadresse verwendet. Falls Sie z. B. Loopback-Adressen konfiguriert haben, geben Sie diese hier als Absendeadresse an.

Sofern die hier eingestellte Absendeadresse eine Loopback-Adresse ist, verwendet das Gerät diese auch auf maskiert arbeitenden Gegenstellen unmaskiert.

Als Adresse akzeptiert das Gerät verschiedene Eingabeformate:

- Name des IP-Netzwerkes (ARF-Netz), dessen Adresse eingesetzt werden soll.
- "INT" für die Adresse des ersten Intranets.
- "DMZ" für die Adresse der ersten DMZ (Achtung: Wenn es eine Schnittstelle Namens "DMZ" gibt, dann nimmt das Gerät deren Adresse).
- LB0 ... LBF für eine der 16 Loopback-Adressen oder deren Name.
- Eine beliebige IPv4- oder IPv6-Adresse

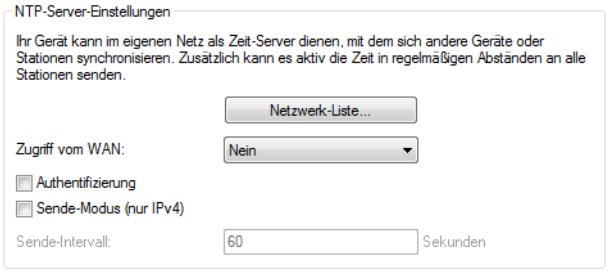
Authentifizierung

Aktiviert bzw. deaktiviert die MD5-Authentifizierung durch den Client.

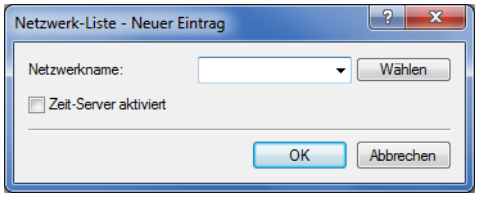
Schlüsselnummer

Kennzeichnet den Schlüssel, den der Client zur MD5-Authentifizierung verwendet.

Mit diesen Einstellungen bezieht zunächst nur das Gerät selbst die Zeit von den öffentlichen Zeitservern. Um die aktuelle Zeit auch im LAN den anderen Geräte bekannt zu machen, aktivieren Sie unter **Datum/Zeit** > **Synchronisierung** im Abschnitt **NTP-Server-Einstellungen** den Zeit-Server im Gerät.



Die Liste der Netzwerke, an welche Ihr Gerät die aktuelle Zeit weiterleitet, konfigurieren Sie unter **Netzwerkliste**.



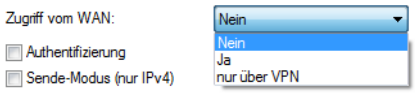
Netzwerkname

Definiert den Namen des Netzwerks.

Zeitserver aktiviert

Legt fest, ob die Zeitserver-Funktion Ihres Gerätes für das ausgewählte Netzwerk aktiviert ist.

Den Zugriff vom WAN konfigurieren Sie über die Auswahlliste **Zugriff vom WAN**.



Mögliche Optionen sind:

Nein

Der Zugriff vom WAN auf den NTP-Server ist deaktiviert.

Ja

Der Zugriff vom WAN auf den NTP-Server ist möglich über unmaskierte Verbindungen, jedoch grundsätzlich nicht möglich bei maskierten WAN-Verbindungen.

Nur über VPN

Der Zugriff über VPN auf den NTP-Server ist aktiviert.

Die Unterstützung für die MD5-Authentifizierung aktivieren Sie unter **Authentifizierung**.

Sende-Modus (nur IPv4)

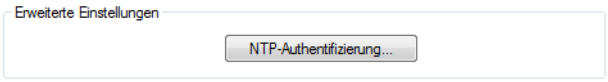
Soll das Gerät regelmäßig als Zeit-Server an alle Stationen im Netz die aktuelle Zeit senden, aktivieren Sie den „Sende-Modus".

Der Sende-Modus des Gerätes unterstützt nur IPv4-Adressen.

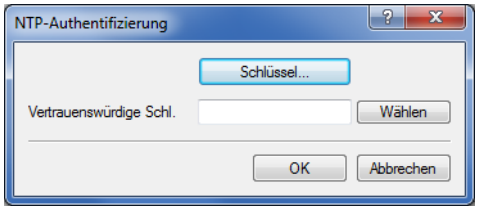
Sende-Intervall

Geben Sie den zeitlichen Abstand in Sekunden an, in welchem der Zeit-Server des Gerätes die aktuelle Zeit an die erreichbaren Stationen im Netz senden soll.

Die Liste der vertrauenswürdigen Schlüssel konfigurieren Sie im Abschnitt **Erweiterte Einstellungen**

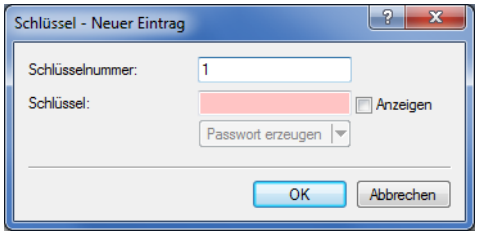


unter **NTP-Authentifizierung**.



Die zur Verfügung stehenden Schlüssel befinden sich in der Liste **Vertrauenswürdige Schl.** und werden über **Wählen** ausgewählt.

Das Bearbeiten bzw. Hinzufügen eines Schlüssels erfolgt über **Schlüssel**.

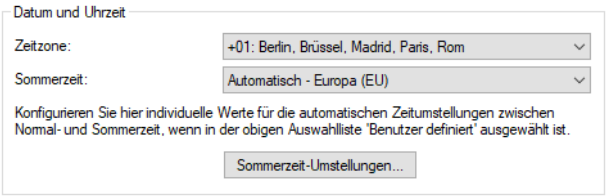


20.5.2 Konfiguration der NTP-Clients

Die NTP-Clients müssen so konfiguriert sein, dass sie die Zeitinformationen des Geräts verwenden. Nicht alle Betriebssysteme verfügen über einen integrierten NTP-Client: bei Linux-Distributionen muss NTP entsprechend mitinstalliert sein.

Die **Datums und Uhrzeiteinstellungen** in einem Windows-System werden mit einem Doppelklick auf die Uhrzeit unten rechts im Bildschirm geöffnet. In den Einstellungen kann dort der Server zur Synchronisation der Zeit ausgewählt werden, falls dies nicht bereits über eine Gruppenrichtlinie vorgegeben wurde.

Das Gerät arbeitet intern mit der koordinierten Weltzeit (UTC). Für Protokollausgaben und zeitbezogene Einstellungen (z. B. cron-Jobs) wird die lokale Uhrzeit verwendet, die über die eingestellte Zeitzone berechnet wird. Zur Berücksichtigung der lokalen Sommerzeit-Einstellungen können die benötigten Anpassungen konfiguriert werden.



LANconfig: **Datum/Zeit** > **Allgemein**

Sommerzeit

Aus

Es wird keine Korrektur der Systemzeit bzgl. der Sommerzeit vorgenommen.

Ein

Solange diese Option aktiviert ist, wird statisch eine Stunde zur aktuellen Systemzeit (Gebildet aus UTC und Zeitzone) hinzuaddiert.

Automatisch – Europa (EU)

In dieser Einstellung wird die Sommerzeit automatisch in Anpassung an die verwendete Zeitzone am Gerätestandort vorgenommen.

Automatisch – USA

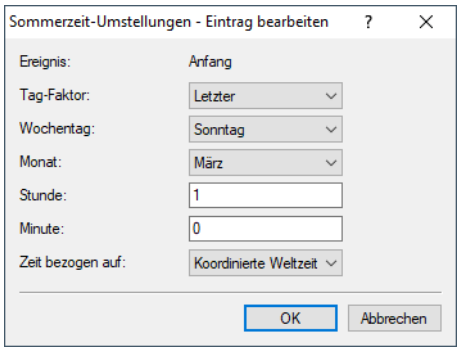
In dieser Einstellung wird die Sommerzeit automatisch in Anpassung an die verwendete Zeitzone am Gerätestandort vorgenommen.

Automatisch – Benutzerdefiniert

Falls sich das Gerät an einem nicht aufgeführten Standort befindet, können die Optionen für die Sommerzeitumstellung benutzerdefiniert vorgenommen werden.

20.5.2.1 Benutzerdefinierte Sommerzeitumstellung

Für den Beginn und das Ende der automatischen Sommerzeitumstellung können benutzerdefinierte Werte festgelegt werden.



LANconfig: **Datum/Zeit** > **Allgemein** > **Sommerzeit-Umstellungen**

Tag-Faktor

Erster, Zweiter, Dritter, Vierter, Letzter, Zweitletzter, Drittletzter, Viertletzter: An diesem wiederkehrenden Tag des Monats wird die Umstellung ausgeführt.

Wochentag

Montag bis Sonntag: Tag, an dem die Umstellung ausgeführt wird.

Monat

Januar bis Dezember: Monat, an dem die Umstellung ausgeführt wird.

Stunde

0 bis 23: Stunde, zu der die Umstellung ausgeführt wird.

Minute

0 bis 59: Minute, zu der die Umstellung ausgeführt wird.

Zeit bezogen auf

Lokale Normalzeit oder UTC: Definiert die Zeitzone, auf die sich die Angaben beziehen.

In der letzten Stunde der Sommerzeit bzw. der darauffolgenden ersten Stunde der Normalzeit besteht eine Mehrdeutigkeit der Uhrzeit. Wird in dieser Zeit die Uhrzeit z. B. per ISDN geholt oder manuell gesetzt, wird immer angenommen, dass es sich um eine Zeitangabe gemäß Sommerzeit handelt.

20.5.3 Beziehen der Gerätezeit über GPS

Sie können die Gerätezeit alternativ zu einem NTP-Server auch über GPS automatisch beziehen. Voraussetzungen für des Beziehen der Gerätezeit über GPS sind:

- Die Betriebsart des Mobilfunk-Modems ist auf WWAN eingestellt
- Das GPS-Modul ist aktiviert
- Die Hol-Methode für die Gerätezeit ist auf GPS eingestellt

Die aktuelle GPS-Zeit finden Sie im LANmonitor (*Anzeige der GPS-Zeit*) oder im Statusbereich des Gerätes.

Diese Funktion ist nur auf Geräten mit internem WWAN-Modul verfügbar. Bitte informieren Sie sich in den technischen Daten zu Ihrem Modell, ob Ihr Gerät diese Funktion unterstützt.

Die Zeit steht erst zur Verfügung, sobald das Gerät erfolgreich einen „GPS-Fix" ausgerührt hat. Hierzu ist der Empfang von mindestens 4 Satelliten in ausreichender Qualität erforderlich.

Die über GPS empfangene Zeit weicht aufgrund von Laufzeitschwankungen möglicherweise um einige Sekunden von der tatsächlichen Zeit ab.

20.6 Scheduled Events

20.6.1 Zeitautomatik für LCOS-Befehle

Dieses Feature erlaubt dem Gerät, bestimmte Befehle zu bestimmten, benutzerdefinierten Zeitpunkten auszuführen. Die Funktionalität entspricht dabei dem unter UNIX bekannten Cron-Dienst. Ausgeführt werden kann dabei **jede** beliebige Kommandozeilenfunktion. Es können damit also alle Features mit einer zeitlichen Steuerung versehen werden.

Anwendungsbeispiele:

- Verbindungsauf- und -abbauten zu bestimmten Zeiten:

  Bei vielen Flatrate-Tarifen für die Internetnutzung wird die Verbindung durch den Provider automatisch nach 24 Stunden "Dauerbetrieb" getrennt. Diese Zwangstrennung kann zu unerwünschten Störungen führen, wenn diese tagsüber zu nicht festgelegten Zeitpunkten stattfindet und dabei VPN-Tunnel abgebaut und die IP-Adresse des Geräts geändert werden. Um die Zwangstrennung zeitlich zu steuern, kann z. B. jede Nacht um 24 Uhr ein manueller Abbau der Internetverbindung angestoßen werden. Die Zwangstrennung erfolgt dann nicht mehr tagsüber zu ungeeigneten Zeitpunkten.

  Als zweites Beispiel können die Geräte in einer verteilten Netzwerkstruktur, die nur über dynamische IP-Adressen verfügen, zu bestimmten Zeitpunkten eine Verbindung zum VPN-Gateway in der Zentrale aufbauen, damit über diese Verbindung Daten sicher aus den Netzen der Filialen ausgelesen werden können. Auf diese Weise ist ein geschützter Zugriff z. B. auf die Kassendaten der Filialen auch ohne ISDN-Verbindungen möglich.

- Ein- und Ausschalten von Firewall-Regeln oder QoS-Regeln

  Die Regeln für Firewall und QoS sind zunächst einmal zeitlich konstant. Je nach Tageszeit oder Wochentag kann es aber sein, dass unterschiedliche Einstellungen in diesem Bereich Sinn machen. Außerhalb der Bürozeiten oder am

Wochenende können z. B. andere Prioritäten für die garantierten Bandbreiten gelten als zwischen 9:00 und 17:00 Uhr.

› Durchführung regelmäßiger Firmware- oder Konfigurationsupdates

Die Zeitautomatik erlaubt nicht nur das Setzen einzelner Werte in der Konfiguration, auch das komplette Umschalten auf eine andere Konfiguration ist möglich. Mit dieser Möglichkeit können Sie eine ganze Reihe von Befehlen bündeln und mit einem Kommando ändern. Der Wechsel der Gerätekonfiguration mit vollständig anderen Werten für das Wochenende und wieder zurück in der Nacht zum Montag gelingt so mit einer einzigen Zeile in der Zeitautomatik.

Auch das regelmäßige Update auf die neueste Firmware von einer festen Quelle aus ist so über die Zeitsteuerung zu realisieren.

› E-Mail-Benachrichtigungen

Mit der Zeitautomatik kann das Gerät nicht nur bei bestimmten Firewall-Ereignissen E-Mails an den Administrator versenden, sondern auch zu festgelegten Zeitpunkten. Die E-Mail kann so z. B. über den erfolgreichen Aufbau der Internetverbindung nach der Zwangstrennung informieren oder nach dem Booten des Gerätes über den Grund des Neustarts informieren.

› Ein- und Ausschalten von Interfaces

Zu den Möglichkeiten für die Zeitautomatik gehört auch das Ein- und Ausschalten von einzelnen Schnittstellen in festen zeitlichen Intervallen. Damit kann z. B. ein WLAN-Interface nur zu bestimmten Zeiten den drahtlosen Zugang zum Netzwerk erlauben.

› Löschen von bestimmten Tabellen

Bei manchen Tabellen im LCOS macht es Sinn, die Inhalte regelmäßig zu löschen. So können Sie z. B. mit dem monatlichen Löschen der Accounting-Tabelle den Überblick über das jeden Monat verbrauchte Datenvolumen behalten.

20.6.2 CRON-Jobs mit Zeitverzögerung

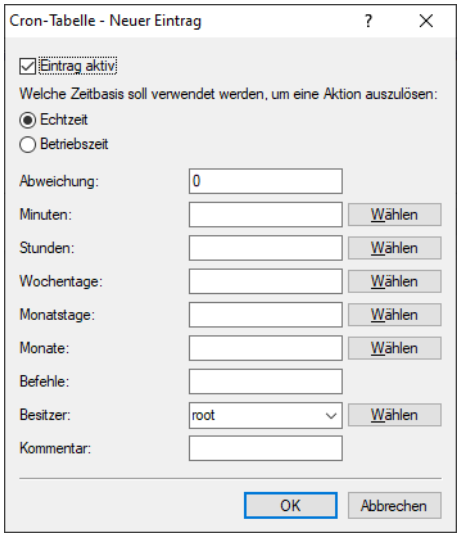
Mit Hilfe von CRON-Jobs lassen sich regelmäßige Aktionen zu bestimmten Zeiten automatisch auf einem Gerät ausführen. Sind in einer Installation sehr viele Geräte aktiv, die zu einem gemeinsamen Zeitpunkt über einen CRON-Job die gleiche Aktion ausführen (z. B. eine Konfiguration per Script aktualisieren), kann das zu unerwünschten Effekten führen, weil z. B. alle Geräte gleichzeitig die VPN-Verbindungen abbauen. Um diesen Effekt zu vermeiden, können die CRON-Jobs mit einer zufälligen Verzögerungszeit von 0 bis 59 Minuten definiert werden.

20.6.3 Konfiguration der Zeitautomatik

Das folgende Tutorial zeigt Ihnen, wie Sie einen neuen CRON-Job anlegen und welche Parameter Ihnen dabei zur Verfügung stehen.

1. Öffnen Sie in LANconfig die Konfiguration für Ihr Gerät.

2. Öffnen Sie die **Cron-Tabelle** im Dialog **Datum/Zeit** > **Allgemein** und klicken Sie **Hinzufügen**, um einen neuen CRON-Job zu erstellen.



3. Geben Sie eine Zeitbasis an.
   Die Zeitbasis bestimmt, ob LCOS die zeitliche Steuerung der künftigen Aktion auf Grundlage der Echtzeit oder der Systemlaufzeit des Gerätes ausführt. In der Einstellung **Echtzeit** wertet das System sämtliche Zeit- und Datumsangaben aus. In der Einstellung **Betriebszeit** wertet das System nur die Minuten- und Stundenangaben seit dem letzten Gerätestart aus.
4. Geben Sie unter **Abweichung** eine Zeit in Minuten an, um welche die Ausführung eines CRON-Jobs gegenüber der festgelegten Startzeit maximal verzögert wird.
   Die tatsächliche Verzögerungszeit erkennt das Gerät zufällig; sie liegt zwischen Null und der hier eingetragenen Zeit. Bei einer Variation von Null wird der CRON-Job exakt zur festgelegten Zeit ausgeführt.

   Echtzeit-basierte Regeln sind ausschließlich dann ausführbar, wenn Ihr Gerät über einen gültigen Zeitbezug verfügt, also z. B. via NTP.
5. Geben Sie den/die Minute(n), Stunde(n), Wochentag(e), Monatstag(e) und Monat(e), an denen Ihr Gerät das festgelegte Kommando ausführt.

   Wenn Sie keinen Wert eingeben, zieht Ihr Gerät den betreffenden Zeitwert auch nicht in die Steuerung mit ein. Für jeden Parameter haben Sie optional auch die Möglichkeit, eine kommaseparierte Liste von Werten oder einen Wertebereich (in Form von als `<Tag>-<Tag>`, Beispiel: 1-5) anzugeben. Mit / kann eine Schrittweite angegeben werden. Falls ein Bereich vor der Schrittweite angegeben wird, dann bezieht sich diese auf den angegebenen Bereich.

   Die Syntax des Feldes **Wochentage** entspricht dabei der üblichen CRON-Interpretation:

Sonntag	Montag	Dienstag	Mittwoch	Donnerstag	Freitag	Samstag
0	1	2	3	4	5	6

   Das Wochentagsfeld ist auch für Regeln bedeutend, die auf die Betriebszeit bezogen sind. Das ist sinnvoll für Aktionen, die Sie nur einmal beim Start des Gerätes (also bei Null Tagen Betriebszeit) ausführen. So gleichen Sie z. B. den Wochentag gegen die Tage der Betriebszeit ab.
6. Geben Sie unter **Befehle** das auszuführende Kommando oder eine kommaseparierte Liste von Kommandos ein.
   Ausgeführt werden kann **jede** beliebige Kommandozeilenfunktion.
7. Geben Sie den **Besitzer** des CRON-Jobs an.
   Als Besitzer lässt sich ein im Gerät definierter Administrator auswählen. Sofern ein Besitzer angegeben ist, werden die Befehle des Cron-Jobs mit den Rechten des Besitzers ausgeführt.
8. Geben Sie im Feld **Kommentar** eine kurze Beschreibung zu dem CRON-Job ein.

9. Klicken Sie **OK**, um den Eintrag zu speichern. Schreiben Sie anschließend die Konfiguration zurück auf das Gerät.

Weitere Konfigurationsbeispiele:

Zeitbasis	Min.	Std.	W.-Tage	M.-Tage	Monate	Befehl
Echtzeit	0	4	0-6	1-31	1-12	do /so/man/abbau internet
Echtzeit	59	3	0-6	1-31	1-12	mailto:admin@beispiel.de?subject=Zwangstrennung?body=Manuelles Trennen der Internetverbindung
Echtzeit	0	0		1		do /setup/accounting/loeschen
Echtzeit	0	18	1,2,3,4,5			do /so/man/aufbau ZENTRALE
Echtzeit	/10					do kommando

- Der erste Eintrag trennt jeden Morgen um 4:00 Uhr die Verbindung zum Internetprovider (Zwangstrennung).
- Der zweite Eintrag sendet jeden Morgen um 3:59 Uhr, also kurz vor der Zwangstrennung, eine Info-Mail an den Admin.
- Der dritte Eintrag löscht an jedem 1. eines Monats die Accounting-Tabelle.
- Der vierte Eintrag baut an jedem Werktag um 18:00 Uhr eine Verbindung zur Zentrale auf.
- Der fünfte Eintrag f ührt alle 10 Minuten ein Kommando aus.

Das Gerät führt zeitgesteuerte Regeln mit einer Genauigkeit von einer Minute aus. Bitte achten Sie darauf, dass die Sprache der eingetragenen Befehle zur eingestellten Konsolensprache passt, da das Gerät ansonsten die Kommandos der Zeitautomatik ignoriert.

20.7 PPPoE-Server

20.7.1 Einleitung

Im Zuge der DSL-Verbreitung sind mittlerweile in allen Betriebssystemen PPPoE-Clients integriert oder verfügbar. Diese können für eine „Anmeldung am Netzwerk“ sowie eine damit einhergehende Zugriffsrechteverwaltung auf Dienste wie Internet, E-Mail oder bestimmte Gegenstellen benutzt werden.

20.7.2 PPPoE ist nur auf einem Netzwerksegment einsetzbar

PPPoE ist als so genannte „Layer-2“-Technologie nur innerhalb eines Netzwerksegments einsetzbar, d. h. nicht über IP-Subnetze hinweg. Die PPPoE-Verbindung kann nicht über die Grenzen des Netzwerksegments, also z. B. über einen Router, hinaus aufgebaut werden.

Nach dem Einloggen eines Benutzers im LAN (z. B. Username: 'Einkauf', Password: 'geheim') über eine vorgeschriebene PPPoE-Anmeldung können weitere Rechte über die Firewall geregelt werden. Dabei wird der PPPoE-Benutzername als 'Gegenstelle' in der Firewall eingetragen. Mit einer Deny-All-Regel und einer PPPoE-Regel der folgenden Form kann dem Benutzer Mustermann die Nutzung des Internets mit Web und FTP erlaubt werden:

- Quelle: Mustermann
- Ziel: alle Stationen
- Dienste: WWW, FTP

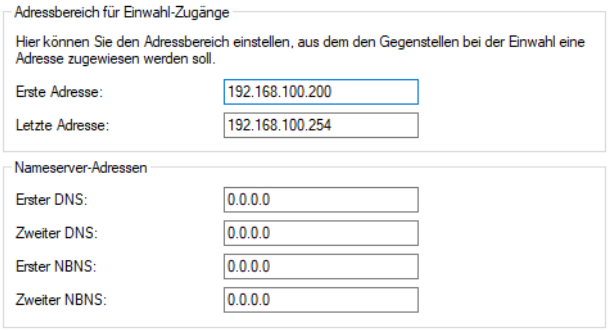
20.7.3 Anwendungsbeispiel

Alle Mitarbeiter der Abteilung 'Einkauf' müssen sich per PPPoE erst am Gerät authentisieren (IP-Routing, Prüfung mit PAP), damit sie auf das Internet zugreifen dürfen.

Randbedingung: Das Gerät ist als Router, Firewall und Gateway für die Benutzer im LAN direkt zu erreichen, d. h. es sind keine weiteren Router dazwischengeschaltet.

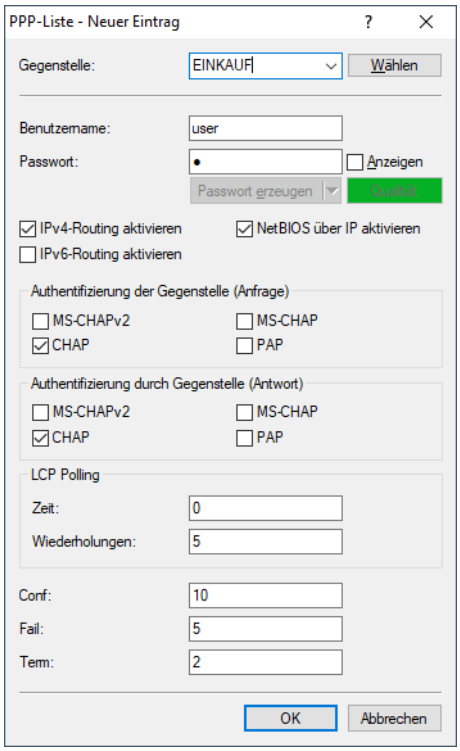
Die Rechner im Einkauf bekommen über die Liste der Adressen für Einwahlzugänge (LANconfig: **IPv4** > **Adressen**) eine IP-Adresse aus einem bestimmten Adressbereich zugewiesen (z. B. 192.168.100.200 bis 192.168.100.254).

Das Gerät selbst steht dabei in einem anderem IP-Adressbereich!



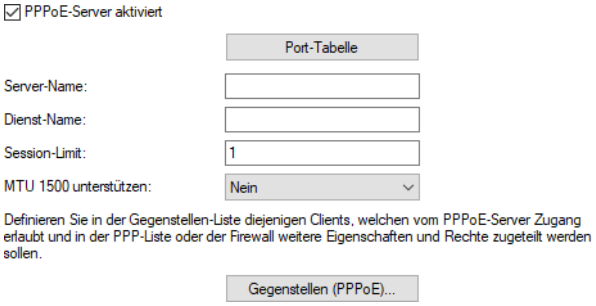
Damit die Anwender die Authentifizierung nicht umgehen können, wird in der Firewall eine DENY-ALL-Regel angelegt, die alle lokalen Verbindungen unterbindet.

Dazu wird der Benutzer 'Einkauf' als Gegenstelle ohne Benutzername, aber mit einem gemeinsamen Kennwort für alle Mitarbeiter in der Abteilung in der PPP-Liste angelegt (LANconfig: **Kommunikation** > **Protokolle** > **PPP-Liste**) und die Authentifizierung (verschlüsselt) über CHAP vorgegeben. Für diesen PPP-Benutzer wird das IP-Routing aktiviert:

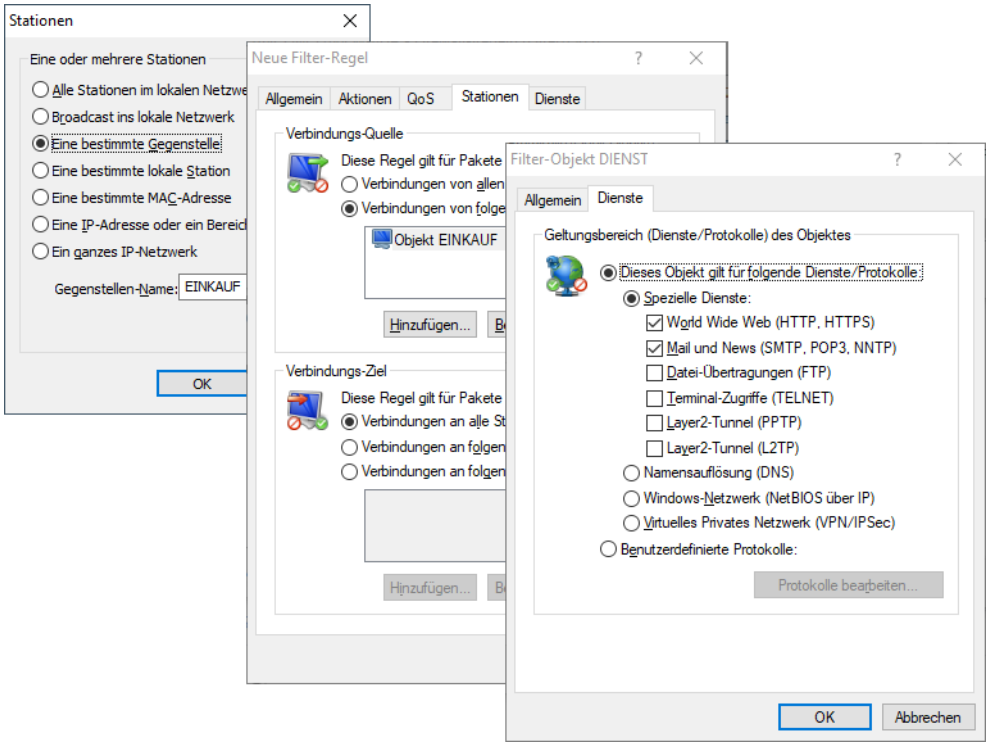


Neben der Aktivierung des PPPoE-Servers (LANconfig: **Kommunikation** > **Allgemein** > **PPPoE-Server aktiviert**) können weitere Einschränkungen (z. B. auf die erlaubten MAC-Adressen) ebenfalls im PPPoE-Server definiert werden. Dieses

Beispiel nutzt aber den dort vorhandenen Eintrag DEFAULT mit der MAC-Adresse 00:00:00:00:00:00, so dass alle MAC-Adressen erlaubt sind.

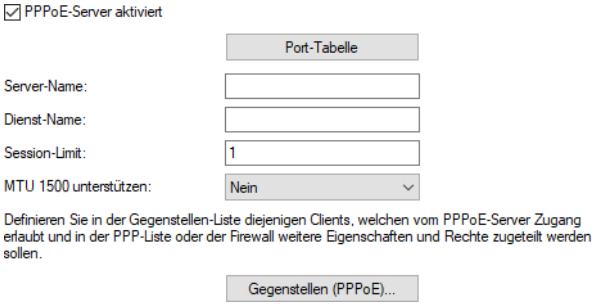


Mit Hilfe der Firewall (LANconfig: **Firewall/QoS** > **IPv4-Regeln** > **Regeln**) können die erlaubten Dienste für die Mitarbeiter des Einkaufs gesteuert werden (z. B. nur Freischalten von HTTP und EMAIL).



20.7.4 Konfiguration

Die Einstellungen für den PPPoE-Server nehmen Sie in LANconfig unter **Kommunikation** > **Allgemein** vor.



In dieser Ansicht haben Sie folgende Konfigurationsmöglichkeiten:

PPPoE-Server aktiviert

Über diese Einstellung schalten Sie den PPPoE-Server global ein- oder aus.

Port-Tabelle

Über diese Tabelle lässt sich der PPPoE-Server für jede physikalische sowie logische Schnittstelle getrennt aktivieren oder deaktivieren.

Server-Name

Über dieses Eingabefeld haben Sie optional die Möglichkeit, dem PPPoE-Server einen eigenen Namen unabhängig vom Gerätenamen zuzuweisen (AC-Name = Access Concentrator Name). Sofern Sie dieses Feld leer lassen, verwendet der PPPoE-Server den Gerätenamen als Server-Namen.

Dienst-Name

In diesem Eingabefeld tragen Sie den Namen des angebotenen Dienstes ein. Der Dienst-Name ermöglicht einem PPPoE-Client die Auswahl eines bestimmten PPPoE-Servers. Dazu konfigurierenn Sie den Dienst-Namen direkt auf dem Clients.

Session-Limit

Über diese Einstellung geben Sie an, wie oft ein Client mit der gleichen MAC-Adresse gleichzeitig angemeldet sein kann. Ist das Limit erreicht, antwortet der Server nicht mehr auf empfangene Anfragen des Clients. Ein Session-Limit von `0` steht für eine unbegrenzte Session-Anzahl.

MTU 1500 unterstützen

Definiert, ob das Gerät im PPPoE eine MTU von 1500 nach *RFC 4638* verhandeln soll. Die Gegenseite muss diese Erweiterung ebenfalls unterstützen.

Gegenstellen (PPPoE)

Über diese Tabelle definieren Sie die einzelnen Clients, denen der PPPoe-Server den Zugang zu den gewünschten Diensten (wie Internet, E-Mail) oder bestimmten Gegenstellen erlaubt.

Die **MAC-Adresse** `000000000000` erlaubt einer Gegenstelle, sich mit einer beliebigen MAC-Adresse am Gerät anzumelden. Ist eine spezifische MAC-Adresse eingetragen, so wird die PPP-Verhandlung abgebrochen, wenn sich der User von einer anderen MAC-Adresse anmeldet.

Nach der Anmeldung versucht das Gerät, die **Haltezeit** der Gegenstelle zu setzen. Existiert kein Eintrag, so verwendet das Gerät die Gegenstelle `DEFAULT`.

Zusätzlich zu dieser Tabelle müssen Sie für die Benutzer einen Eintrag in der PPP-Tabelle vornehmen, in welchem Sie das Passwort, die Rechte (IP) und sonstige PPP-Parameter (LCP-Polling etc.) hinterlegen. Alternativ haben Sie auch die Möglichkeit, die Benutzer über einen RADIUS-Server zu authentifizieren. Dazu konfigurieren Sie den Server unter **Kommunikation** > **RADIUS** > **Authentifizierung über RADIUS für PPP** und setzen dessen Betriebsart auf **Exklusiv** (ausschließlich RADIUS) oder **Aktiv** (gemischte Datenhaltung RADIUS/PPP-Tabelle).

20.7.5 PPPoE-Snooping

Das PPPoE-Snooping ermöglicht Geräten, die PPPoE-Discovery-Pakete (PPPoED) empfangen und weiterleiten, diese Datenpakete zu analysieren und mit zusätzlichen Informationen zu versehen. Diese Informationen ermöglichen es einem PPPoE Access Concentrator (AC), die PPPoED-Datenpakete entsprechend zu verarbeiten. Diese Rolle wird als „PPPoE-Intermediate-Agent" bezeichnet.

PPPoE-Snooping im LCOS verarbeitet die folgenden PPPoED-Pakete:

- PADI (PPPoE Active Discovery Indication)
- PADR (PPPoE Active Discovery Request)
- PADT (PPPoE Active Discovery Terminate)

Der für das PPPoE-Snooping zuständige PPPoE Intermediate Agent erweitert das PPPoED-Paket um Hersteller spezifische Attribute (Circuit-ID und Remote-ID) oder ersetzt diese IDs durch eigene Werte, falls sie bereits im empfangenen Datenpaket enthalten sind.

- Remote-ID: kennzeichnet eindeutig den Client, der einen PPPoE-Request stellt.
- Circuit-ID: kennzeichnet eindeutig die Schnittstelle, über die ein Client einen PPPoE-Request stellt.

Die Konfiguration von PPPoE-Snooping erfolgt pro LAN/WLAN-Schnittstelle.

20.8 Simple Network Management Protocol (SNMP)

Das Simple Network Management Protocol (SNMP) ermöglicht die Überwachung und Konfiguration von Geräten in einem Netzwerk von einer zentralen Instanz aus. Seit der ersten Veröffentlichung von SNMPv1 im Jahr 1988 entwickelte es sich im Laufe der Zeit über die Version SNMPv2 bis zur Version SNMPv3 weiter, um einer immer komplexeren Netzwerk-Infrastruktur sowie gesteigerten Ansprüchen an Sicherheit, Flexibilität und Komfort gerecht zu werden.

Mit Hilfe des Protokolls SNMP (Simple Network Management Protocol) werden höchste Ansprüche, wie das simple Management und Monitoring eines Netzwerks erfüllt. Es ermöglicht die frühzeitige Erkennung von Problemen und Störungen in einem Netzwerk und unterstützt bei deren Beseitigung. Das Simple Network Management Protocol ermöglicht die Überwachung und Konfiguration von Geräten in einem Netz von einer zentralen Instanz aus und regelt die Kommunikation zwischen den überwachten Geräten und der Überwachungsstation. Dadurch lassen sich Parameter wie der Zustand des Gerätes, CPU-Auslastung, Temperatur eines Geräts, Verbindungsstatus, Störungen, etc. z. B. über LANmonitor überwachen und auswerten. Der Administrator wird aktiv bei der Netzwerkverwaltung unterstützt und kann Probleme frühzeitig in seinem Monitoringsystem erkennen. Die neueste Version des Protokolls SNMPv3 ermöglicht im Gegensatz zu den Vorgängerversionen SNMPv1 und SNMPv2 eine verschlüsselte Datenkommunikation zwischen Netzwerk und Managementsystem und bietet damit einen entscheidenden Sicherheitsfaktor. Die integrierte Nutzerverwaltung bietet zusätzlich, dank verschiedener Benutzer-Accounts, eine Authentifizierung für die optimale Zugriffskontrolle bei Konfigurationen. So lassen sich Rechte über verschiedene Zugriffsebenen für Administratoren präzise steuern und das Netzwerk ist optimal geschützt.

SNMP-Komponenten

Die typische SNMP-Architektur besteht aus drei Komponenten:

SNMP-Manager

Der SNMP-Manager sendet SNMP-Anfragen an den SNMP-Agent und wertet dessen SNMP-Antworten aus. Als solche SNMP-Manager fungieren z. B. LANconfig und LANmonitor. Da LCOS-Geräte sich an die Standards von SNMPv1, SNMPv2 und SNMPv3 halten, ist auch der Einsatz einer alternativen SNMP-Verwaltungs- und Management-Software möglich.

SNMP-Agent

Der SNMP-Agent ist ein Modul, das auf dem verwalteten Gerät aktiviert ist. Er nimmt die Anfragen des SNMP-Managers entgegen, sammelt entsprechend der Anfrage die Zustandsdaten des Geräts aus dessen MIB und sendet diese Daten als „SNMP Response" zurück an den SNMP-Manager. Je nach Konfiguration sendet der SNMP-Agent bei bestimmten Zustandsänderungen im verwalteten Gerät auch eigenständig einen sogenannten „SNMP Trap" an den SNMP-Manager. Die Benachrichtigung in Form einer SYSLOG-Meldung oder einer E-Mail an den Administrator des Geräts ist ebenfalls möglich.

Verwaltetes Gerät

Die Zustände dieses Gerätes finden sich in seiner Management Information Base (MIB). Auf Anfrage des SNMP-Agenten liest das Gerät die entsprechenden Daten aus und gibt sie an den SNMP-Agenten zurück.

Die Übertragung von SNMP-Requests und SNMP-Responses zwischen SNMP-Manager und SNMP-Agent erfolgt standardmäßig im User Datagram Procol (UDP) über den Port 161. Die Übertragung von SNMP-Traps erfolgt standardmäßig im UDP über Port 162.

SNMP-Versionen

Die Unterschiede zwischen den verschiedenen SNMP-Versionen lassen sich wie folgt zusammenfassen:

SNMPv1

Die Version 1 startete in 1988 und galt lange Zeit als De-Facto-Standard für Netzwerk-Management. Die Authentifizierung des SNMP-Managers am SNMP-Agent erfolgt bei SNMPv1 über einen Community-String, der in beiden Komponenten identisch sein muss. Diese Sicherheit ist allerdings stark eingeschränkt, da die Übertragung des Community-Strings im Klartext erfolgt. Nicht zuletzt die gesteigerten Anforderungen an eine sichere Netzwerk-Kommunikation machten eine Überarbeitung der Version 1 notwendig.

SNMPv2

In die Version 2 flossen seit 1993 hauptsächlich Verbesserungen im Komfortbereich ein. Mehrere Zwischenschritte und wieder verworfene Konzepte führten letztendlich zur Version SNMPv2c. Diese Version ermöglicht die komfortable Abfrage von großen Datenmengen über einen `GetBulkRequest`-Befehl und

die Kommunikation von SNMP-Managern untereinander. Der Austausch des Community-Strings erfolgt allerdings wie bei der Version 1 weiterhin im Klartext.

SNMPv3

Die Version 3 erfüllt schließlich ab 1999 die mittlerweile dringend notwendigen Sicherheitsanforderungen. U. a. erfolgt die Kommunikation verschlüsselt, und auch die Kommunikationspartner müssen sich zuvor authentifizieren und autorisieren. Darüber hinaus ist der SNMP-Aufbau modularer geworden, so dass z. B. Modernisierungen bei Verschlüsselungstechnologien in SNMPv3 einfließen können, ohne den Standard komplett neu gestalten zu müssen.

LCOS unterstützt die folgenden SNMP-Versionen:

- SNMPv1
- SNMPv2c
- SNMPv3

20.8.1 SNMPv3-Grundlagen

Die Protokoll-Struktur von SNMP hat sich in der Version 3 grundlegend geändert. SNMPv3 ist in mehrere Module mit klar definierten Interfaces aufgeteilt, die untereinander kommunizieren. Die drei wichtigsten Elemente in SNMPv3 sind „Message Processing and Dispatch (MPD)", „User-based Security Model (USM)" und „View-based Access Control Mechanism (VACM)".

MPD

Das MPD-Modul ist verantwortlich für die Verarbeitung (processing) und die Weiterbeförderung (dispatch) der ein- und ausgehenden SNMP-Meldungen.

USM

Das USM-Modul verwaltet Sicherheitsfunktionen, die die Authentifizierung der Nutzer sowie die Verschlüsselung und Integrität der Daten sicherstellen. SNMPv3 hat das Prinzip des „Security Models" eingeführt, so dass in der SNMP-Konfiguration von LCOS hauptsächlich das Security-Model „SNMPv3" zum Einsatz kommt. Aus Kompatibilitätsgründen kann es jedoch notwendig sein, auch die Versionen SNMPv2c oder sogar SNMPv1 zu berücksichtigen und entsprechend als „Security-Model" auszuwählen.

VACM

Der VACM stellt sicher, dass der Sender einer SNMP-Anfrage berechtigt ist, die angefragte Information zu erhalten. Die entsprechenden Zugriffsberechtigungen finden sich in den folgenden Einstellungen und Parametern:

SNMPv3-Views

„SNMPv3-Views" fassen Inhalte, Statusmeldungen und Aktionen der Management Information Base (MIB) zusammen, die eine SNMP-Anfrage mit entsprechenden Zugriffsrechten erhalten bzw. ausführen darf. Diese Ansichten können einzelne Werte, aber auch komplette Pfade der MIB sein. Die Angabe dieser Inhalte erfolgt anhand der jeweiligen OIDs der MIB-Einträge.

Auf diese Weise erhält der Sender einer SNMP-Anfrage auch nach erfolgreicher Authentifizierung nur Zugriff auf die Daten, für die er gemäß SNMPv3-Views die Zugriffsrechte besitzt.

SNMPv3-Groups

„SNMPv3-Groups" fassen Nutzer mit gleichen Zugriffsrechten in einer jeweiligen Gruppe zusammen.

Security-Levels

„Security Levels" bestimmen die Sicherheitsstufe für den Austausch von SNMP-Nachrichten. Die folgenden Stufen sind auswählbar:

NoAuth-NoPriv

Die SNMP-Anfrage ist ohne die Verwendung von speziellen Authentifizierungs-Verfahren gültig. Als Authentifizierung genügt die Zugehörigkeit zu einer SNMP-Community (bei SNMPv1 und SNMPv2c) bzw. die Angabe des Benutzernamens (bei SNMPv3). Die Übertragung der Daten erfolgt unverschlüsselt.

Auth-NoPriv

Für die Verarbeitung der SNMP-Anfrage ist eine Authentifizierung mittels HMAC-MD5- oder HMAC-SHA-Algorithmus notwendig, die Datenübertragung erfolgt jedoch unverschlüsselt.

Auth-Priv

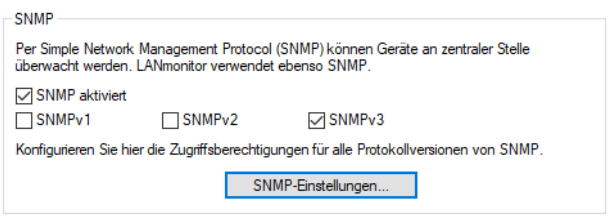
Für die Verarbeitung der SNMP-Anfrage ist eine Authentifizierung mittels HMAC-MD5- oder HMAC-SHA-Algorithmus notwendig, die Datenübertragung erfolgt zusätzlich verschlüsselt über DES- oder AES-Algorithmen.

Kontext

Der „Kontext" ist dafür vorgesehen, die einzelnen SNMP-Entities voneinander zu unterscheiden.

20.8.2 SNMP konfigurieren

In LANconfig konfigurieren Sie SNMP unter **Meldungen/Monitoring** > **Protokolle** im Abschnitt **SNMP**.



SNMP aktiviert

Aktivieren Sie SNMP für die im Folgenden angegebenen SNMP-Protokollversionen, die das Gerät bei SNMP-Anfragen und SNMP-Traps unterstützen soll.

SNMPv1

Aktiviert SNMPv1.

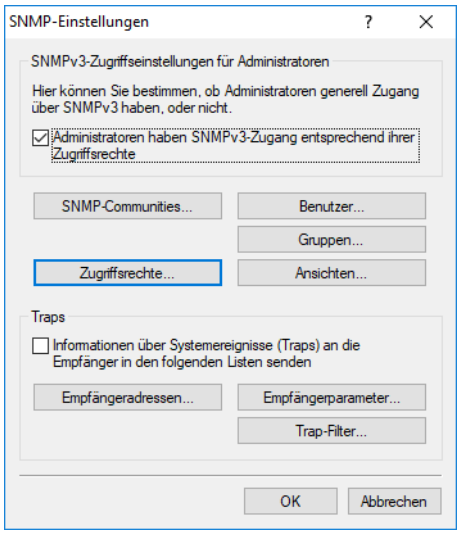
SNMPv2

Aktiviert SNMPv2c.

SNMPv3

Aktiviert SNMPv3.

Mit einem Klick auf **SNMP-Einstellungen** öffnen Sie die Konfigurationeinstellungen.



20.8.2.1 SNMP-Einstellungen

SNMPv3-Zugriffseinstellungen für Administratoren

Administratoren haben SNMPv3-Zugang entsprechend ihrer Zugriffsrechte

Sollen registrierte Administratoren auch den Zugriff über SNMPv3 erhalten, aktivieren Sie diese Option.

Passwortregeln

Erzwinge Passwortregeln

Mit diesem Eintrag haben Sie die Möglichkeit, das Erzwingen von Passwort-Regeln zu aktivieren oder zu deaktivieren. Es gelten dann die folgenden Regeln für die SNMPv3-Authentifizierung und das Passwort für SNMPv3-Verschlüsselung:

- Die Länge des Passworts muss mindestens 16 Zeichen betragen.
- Das Passwort muss mindestens 3 der 4 Zeichenklassen Kleinbuchstaben, Großbuchstaben, Zahlen und Sonderzeichen enthalten.

Beachten Sie, dass beim Einschalten dieser Funktion die aktuellen Passwörter nicht unmittelbar überprüft werden. Nur bei zukünftigen Änderungen der Passwörter werden diese auf ihre Übereinstimmung mit der Richtlinie überprüft.

SNMP-Communities

Auch bei der Verwaltung von Netzwerken mit SNMP-Management-Systemen lassen sich die Rechte über verschiedene Zugriffsebenen für Administratoren präzise steuern. SNMP kodiert dazu bei den Versionen SNMPv1 und SNMPv2c die Zugangsdaten als Teil einer sogenannten „Community“, welche die Bedeutung eines Passworts bzw. Zugangsschlüssels inne hat. Die Authentifizierung kann hierbei wahlweise

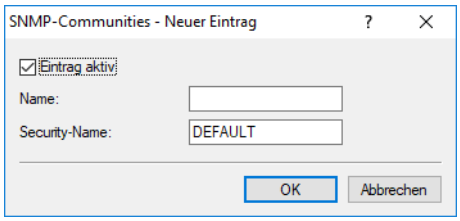
- über die Community `public` (uneingeschränkter SNMP-Lesezugriff),
- ein Master-Passwort (beschränkter SNMP-Lesezugriff), oder
- eine Kombination aus Benutzername und Passwort, getrennt durch einen Doppelpunkt (beschränkter SNMP-Lesezugriff),

erfolgen.

Eine Communitiy fasst somit bestimmte SNMP-Hosts zu Gruppen zusammen, um diese einerseits einfacher verwalten zu können. Andererseits bieten SNMP-Communities eine eingeschränkte Sicherheit beim Zugriff über SNMP, da ein SNMP-Agent nur SNMP-Anfragen von Teilnehmern akzeptiert, deren Community ihm bekannt ist.

Standardmäßig beantwortet Ihr Gerät alle SNMP-Anfragen, die es von LANmonitor oder einem anderen SNMP-Management-System mit der Community `public` erhält. Da dies jedoch (v. a. bei externer Erreichbarkeit) ein potentielles Sicherheitsrisiko darstellt, haben Sie die Möglichkeit, in LANconfig eigene Communities zu definieren.

Diese Konfiguration ist nur für die SNMP-Versionen v1 und v2c relevant.



Eintrag aktiv

Aktiviert oder deaktiviert diese SNMP-Community.

Name

Vergeben Sie hier einen aussagekräftigen Namen für diese SNMP-Community.

Security-Name

Geben Sie hier die Bezeichnung für die Zugriffsrichtlinie ein, die die Zugriffsrechte für alle Community-Mitglieder festlegt.

Als Standard ist die SNMP-Community `public` eingerichtet, die den uneingeschränkten SNMP-Lesezugriff ermöglicht.

Um eine autorisierte Abfrage von Zugangsdaten beim SNMP-Lesezugriff über SNMPv1 oder SNMPv2c zu erzwingen, deaktivieren Sie die Community `public` in der Liste der SNMP-Communities. Dadurch lassen sich Informationen über den Zustand des Gerätes, aktuelle Verbindungen, Reports, etc. erst dann via SNMP auslesen, nachdem sich der betreffende Benutzer am Gerät authentifiziert hat. Die Autorisierung erfolgt wahlweise über die Zugangsdaten des Administrator-Accounts oder über den in der individuellen SNMP-Community definierten Zugang.

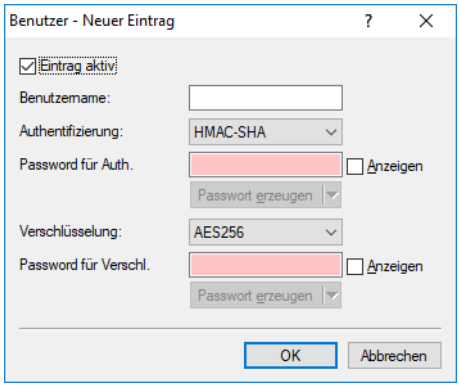
Das Deaktivieren der Community `public` hat keine Auswirkung auf den Zugriff über eine weitere angelegte Community.

Eine individuelle SNMP Read-Only Community bleibt z. B. stets ein alternativer Zugangsweg, der nicht an ein Administrator-Konto gebunden ist.

Der SNMP-Schreibzugriff bleibt ausschließlich Administratoren mit entsprechenden Berechtigungen vorbehalten.

Benutzer

Neben den am Gerät registrierten Administratoren ist der Zugriff auch für einzelne Nutzer möglich. Hier konfigurieren Sie die Einstellungen für Authentifizierung und Verschlüsselung für diese Anwender bei Nutzung von SNMPv3.



Eintrag aktiv

Aktiviert oder deaktiviert diesen Benutzer.

Benutzername

Vergeben Sie hier einen aussagekräftigen Namen für diesen Benutzer.

Authentifizierung

Bestimmen Sie, mit welchem Verfahren sich der Benutzer am SNMP-Agent authentifizieren muss. Zur Verfügung stehen die folgenden Verfahren:

Keine

Eine Authentifizierung des Benutzers ist nicht notwendig.

HMAC-MD5

Die Authentifizierung erfolgt mit dem Hash-Algorithmus HMAC-MD5-96 (Hash-Länge 128 Bits).

HMAC-SHA (Default)

Die Authentifizierung erfolgt mit dem Hash-Algorithmus HMAC-SHA (Hash-Länge 160 Bits).

HMAC-SHA224

Die Authentifizierung erfolgt mit dem Hash-Algorithmus HMAC-SHA-224 (Hash-Länge 224 Bits).

HMAC-SHA256

Die Authentifizierung erfolgt mit dem Hash-Algorithmus HMAC-SHA-256 (Hash-Länge 256 Bits).

HMAC-SHA384

Die Authentifizierung erfolgt mit dem Hash-Algorithmus HMAC-SHA-384 (Hash-Länge 384 Bits).

HMAC-SHA512

Die Authentifizierung erfolgt mit dem Hash-Algorithmus HMAC-SHA-512 (Hash-Länge 512 Bits).

Passwort für Auth.

Geben Sie hier das für die Authentifizierung notwendige Passwort des Benutzers ein und wiederholen Sie es im Feld darunter.

Verschlüsselung

Bestimmen Sie, nach welchem Verschlüsselungsverfahren die Kommunikation mit dem Benutzer verschlüsselt sein soll. Zur Verfügung stehen die folgenden Verfahren:

Keine

Die Kommunikation erfolgt unverschlüsselt.

DES

Die Verschlüsselung erfolgt mit DES (Schlüssellänge 56 Bits).

AES128

Die Verschlüsselung erfolgt mit AES128 (Schlüssellänge 128 Bits)

AES192

Die Verschlüsselung erfolgt mit AES192 (Schlüssellänge 192 Bits)

AES256 (Default)

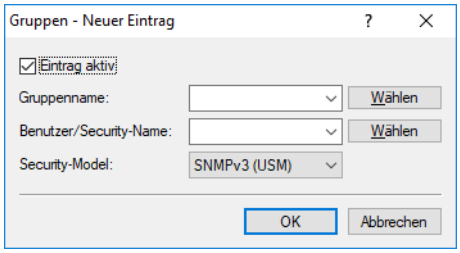
Die Verschlüsselung erfolgt mit AES256 (Schlüssellänge 256 Bits)

Passwort für Verschl.

Geben Sie hier das für die Verschlüsselung notwendige Passwort des Benutzers ein und wiederholen Sie es im Feld darunter.

Gruppen

Durch die Konfiguration von SNMP-Gruppen lassen sich Authentifizierung und Zugriffsrechte für mehrere Benutzer komfortabel verwalten und zuordnen. Als Standardeintrag ist die Konfiguration für den SNMP-Zugriff über den LANmonitor bereits voreingestellt.



Eintrag aktiv

Aktiviert oder deaktiviert diese Gruppe.

Gruppenname

Vergeben Sie hier einen aussagekräftigen Namen für diese Gruppe. Diesen Namen verwenden Sie anschließend bei der Konfiguration der Zugriffsrechte.

Benutzer / Security-Name

Wählen Sie hier einen Security-Namen aus, den Sie einer SNMP-Community zugeordnet haben. Auch die Angabe des Namens eines bereits konfigurierten Benutzers ist möglich.

Security-Model

SNMPv3 hat das Prinzip des „Security Models" eingeführt, so dass in der SNMP-Konfiguration von LCOS hauptsächlich das Security-Model „SNMPv3" zum Einsatz kommt. Aus Kompatibilitätsgründen kann es jedoch notwendig sein, auch die Versionen SNMPv2c oder sogar SNMPv1 zu berücksichtigen und entsprechend als „Security-Model" auszuwählen. Entsprechend wählen Sie hier einen der folgenden Einträge aus:

SNMPv1

Die Übertragung der Daten erfolgt über SNMPv1. Die Authentifizierung des Benutzers erfolgt ausschließlich über den Community-String in der SNMP-Nachricht. Eine Verschlüsselung der Kommunikation findet nicht statt. Das entspricht der Sicherheitsstufe „Keine Authentifizierung und keine Verschlüsselung".

SNMPv2

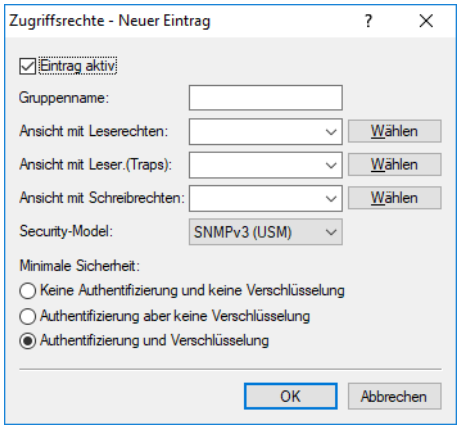
Die Übertragung der Daten erfolgt über SNMPv2c. Die Authentifizierung des Benutzers erfolgt ausschließlich über den Community-String in der SNMP-Nachricht. Eine Verschlüsselung der Kommunikation findet nicht statt. Das entspricht der Sicherheitsstufe „Keine Authentifizierung und keine Verschlüsselung".

SNMPv3 (USM)

Die Übertragung der Daten erfolgt über SNMPv3. Für Anmeldung und Kommunikation des Benutzers sind Sicherheitsstufen möglich, die bei den **Zugriffsrechten** aktiviert werden.

Zugriffsrechte

Diese Tabelle führt die verschiedenen Konfigurationen für Zugriffsrechte, Security-Modelle und Ansichten zusammen.



Eintrag aktiv

Aktiviert oder deaktiviert diesen Eintrag.

Gruppenname

Wählen Sie hier den Namen einer Gruppe aus, für die diese Zugriffsrechte gelten soll.

Ansicht mit Leserechten

Bestimmen Sie die Ansicht der MIB-Einträge, für die diese Gruppe die Leserechte erhalten soll.

Ansicht mit Leserechten (Traps)

Bestimmen Sie die Ansicht der MIB-Einträge, für die diese Gruppe die Leserechte für Traps erhalten soll.

Ansicht mit Schreibrechten

Bestimmen Sie die Ansicht der MIB-Einträge, für die diese Gruppe die Schreibrechte erhalten soll.

Security-Model

Aktivieren Sie hier das entsprechende Security-Model.

Minimale Sicherheit

Geben Sie die minimale Sicherheit an, die für Zugriff und Datenübertragung gelten soll.

Keine Authentifizierung und keine Verschlüsselung

Die Authentifizierung erfolgt nur über die Angabe und Auswertung des Benutzernamens. Eine Verschlüsselung der Datenübertragung findet nicht statt.

Authentifizierung, aber keine Verschlüsselung

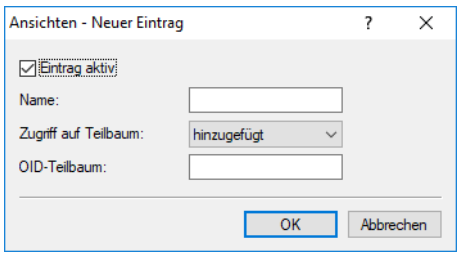
Die Authentifizierung erfolgt über die für den Benutzer eingestellten Hash-Algorithmen. Eine Verschlüsselung der Datenübertragung findet nicht statt.

Authentifizierung und Verschlüsselung

Die Authentifizierung erfolgt über die für den Benutzer eingestellten Hash-Algorithmen. Die Verschlüsselung der Datenübertragung erfolgt über DES- oder AES-Algorithmen.

Ansichten

Hier fassen Sie verschiedene Werte oder ganze Zweige der MIB des Gerätes zusammen, die ein Benutzer gemäß seiner Zugriffsrechte einsehen oder verändern kann.



Eintrag aktiv

Aktiviert oder deaktiviert diese Ansicht.

Name

Vergeben Sie hier der Ansicht einen aussagekräftigen Namen.

Zugriff auf Teilbaum

Bestimmen Sie, ob die nachfolgend angegebenen OID-Teilbäume Bestandteil („hinzugefügt“) oder kein Bestandteil („entfernt“) der Ansicht sind.

OID-Teilbaum

Bestimmen Sie durch komma-separierte Angabe der jeweiligen OIDs, welche Werte und Aktionen der MIB diese Ansicht ein- bzw. ausschließen soll.

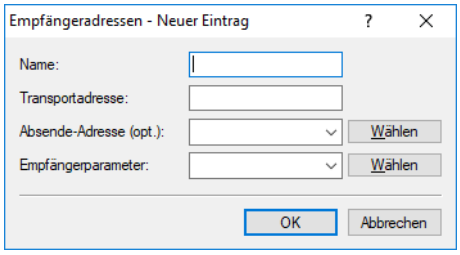
Die OIDs entnehmen Sie bitte der Geräte-MIB, die Sie im WEBconfig unter **Extras** > **SNMP-Geräte-MIB abrufen** herunterladen können.

Traps

Wenn Sie die Option **Informationen über Systemereignisse (Traps) an die Empfänger in den folgenden Listen senden** aktivieren, dann bekommen die unter **Empfängeradressen** und **Empfängerparameter** konfigurierten Empfänger entsprechende Informationen. Die Systemereignisse, die eine Meldung auslösen, lassen sich über Trap-Filter einschränken.

Empfängeradressen

In der Liste der Empfängeradressen konfigurieren Sie die Empfänger, an die der SNMP-Agent die SNMP-Traps versendet.



Name

Vergeben Sie hier dem Eintrag einen aussagekräftigen Namen.

Transportadresse

Konfigurieren Sie hier die Adresse des Empfängers. Diese Adresse beschreibt die IP-Adresse und Port-Nummer eines SNMP-Trap-Empfängers und wird in der Syntax „<IP-Adresse>:<Port>“ angegeben (z. B. 128.1.2.3:162). Der UDP-Port 162 wird für SNMP-Traps verwendet.

Absendeadresse

Hier können Sie optional eine Absendeadresse konfigurieren, die statt der ansonsten automatisch für die Zieladresse gewählten Absendeadresse verwendet wird.

Falls Sie z. B. Loopback-Adressen konfiguriert haben, können Sie diese hier als Absendeadresse angeben.

Als Adresse werden verschiedene Eingabeformen akzeptiert:

- Name des IP-Netzwerks (ARF-Netz), dessen Adresse eingesetzt werden soll.
- „INT“ für die Adresse des ersten Intranets.
- „DMZ“ für die Adresse der ersten DMZ

  Wenn es eine Schnittstelle Namens „DMZ“ gibt, dann wird deren Adresse genommen.

- LB0…LBF für eine der 16 Loopback-Adressen oder deren Name.
- Desweiteren kann eine beliebige IP-Adresse in der Form x.x.x.x angegeben werden.

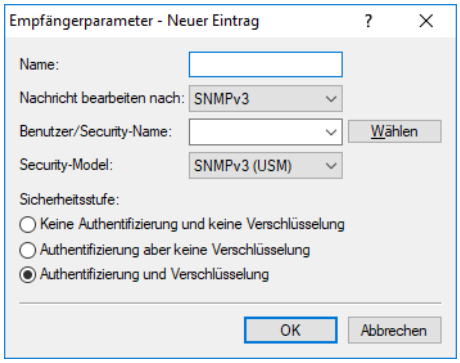
Sofern die hier eingestellte Absendeadresse eine Loopback-Adresse ist, wird diese auch auf maskiert arbeitenden Gegenstellen unmaskiert verwendet.

Empfängerparameter

Wählen Sie hier den gewünschten Eintrag aus der Liste der Empfängerparameter aus.

Empfängerparameter

In dieser Tabelle konfigurieren Sie, wie der SNMP-Agent die SNMP-Traps behandelt, die er an die Empfänger versendet.



Name

Vergeben Sie hier dem Eintrag einen aussagekräftigen Namen.

Nachricht bearbeiten nach

Bestimmen Sie hier, nach welchem Protokoll der SNMP-Agent die Nachricht strukturiert.

Benutzer / Security-Name

Wählen Sie hier einen Security-Namen aus, den Sie einer SNMP-Community zugeordnet haben. Auch die Angabe des Namens eines bereits konfigurierten Benutzers ist möglich.

Security-Model

SNMPv3 hat das Prinzip des „Security Models" eingeführt, sodass in der SNMP-Konfiguration von LCOS hauptsächlich das Security-Model „SNMPv3" zum Einsatz kommt. Aus Kompatibilitätsgründen kann es jedoch notwendig sein, auch die Versionen SNMPv2c oder sogar SNMPv1 zu berücksichtigen und entsprechend auszuwählen. Entsprechend wählen Sie hier einen der folgenden Einträge aus:

SNMPv1

Die Übertragung der Daten erfolgt über SNMPv1. Die Authentifizierung des Benutzers erfolgt ausschließlich über den Community-String in der SNMP-Nachricht. Eine Verschlüsselung der Kommunikation findet nicht statt. Das entspricht der Sicherheitsstufe „NoAuthNoPriv".

SNMPv2

Die Übertragung der Daten erfolgt über SNMPv2c. Die Authentifizierung des Benutzers erfolgt ausschließlich über den Community-String in der SNMP-Nachricht. Eine Verschlüsselung der Kommunikation findet nicht statt. Das entspricht der Sicherheitsstufe „NoAuthNoPriv".

SNMPv3 (USM)

Die Übertragung der Daten erfolgt über SNMPv3. Dies kann ausschließlich zusammen mit SNMP-Benutzern gewählt werden. Die effektive mögliche Sicherheitsstufe hängt von den gewählten Authentifizierungs- und Verschlüsselungsmethoden des Benutzers ab.

Sicherheitsstufe

Legen Sie die Sicherheitsstufe fest, die für den Erhalt der SNMP-Trap beim Empfänger gelten soll.

Keine Authentifizierung und keine Verschlüsselung

Die SNMP-Anfrage ist ohne die Verwendung von speziellen Authentifizierungs-Verfahren gültig. Als Authentifizierung genügt die Zugehörigkeit zu einer SNMP-Community (bei SNMPv1 und SNMPv2c) bzw. die Angabe des Benutzernamens (bei SNMPv3). Die Übertragung der Daten erfolgt unverschlüsselt.

Authentifizierung, aber keine Verschlüsselung

Die Authentifizierung erfolgt über die für den Benutzer eingestellten Hash-Algorithmen. Eine Verschlüsselung der Datenübertragung findet nicht statt.

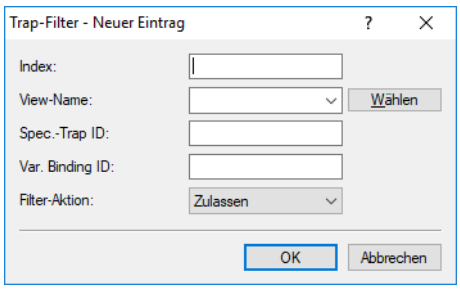
Authentifizierung und Verschlüsselung

Die Authentifizierung erfolgt über die für den Benutzer eingestellten Hash-Algorithmen. Die Verschlüsselung der Datenübertragung erfolgt über DES- oder AES-Algorithmen.

Trap-Filter

Bestimmte SNMP-Traps bzw. eine große Anzahl von SNMP-Traps können auf den empfangenden Servern mitunter ungewünscht sein. Daher lässt sich eine SNMP-Filterliste hinzufügen, die es erlaubt, SNMP-Traps basierend auf ihren Hersteller-spezifischen OIDs oder den in den Variable Bindings enthaltenen OIDs wahlweise durchzulassen oder zurückzuhalten.

Traps für den Benutzer „root" können nicht gefiltert werden. Für die Filterung muss ein separater SNMP-Benutzer verwendet werden.



Index

Die Position dieses Eintrags in der Filterliste. Die Liste wird vom kleinsten zum größten Wert überprüft bis zum ersten

Treffer.

View-Name

Der **View-Name** ist der Name einer **Ansicht**, für den diese Filterregel gültig ist. Ist der **Zugriff auf Teilbaum** der betreffenden Ansicht auf „hinzugefügt" gesetzt, dann lassen sich mit einer zugehörigen Filterregel mit der **Filter-Aktion** „Ablehnen" die entsprechenden Traps verhindern. Ist der **Zugriff auf Teilbaum** der betreffenden Ansicht hingegen auf „entfernt" gesetzt, so lassen sich mit der **Filter-Aktion** „Zulassen" die Meldungen dennoch als Ausnahme senden. Da in den **Ansichten** mehrere Eintrgäge gleichen Namens mit verschiedenen Zugriffseinstellungen erlaubt sind, muss die **Filter-Aktion** unabhängig vom Wert der jeweiligen Einstellung des **Zugriff auf Teilbaum** gesetzt werden können.

Spec.-Trap ID

Gibt eine spezifische Trap-ID an, die Wildcards und Bereiche enthalten darf. Ein leerer Eintrag gilt für alle spezifischen Trap IDs des Gerätes. Siehe Beispiele in der folgenden Tabelle.

OID	Beschreibung
	Trifft auf jede OID zu.
1.2.3	Trifft auf alle OIDs zu, die mit „1.2.3" beginnen.

OID	Beschreibung
1.*.3	Trifft auf alle OIDs zu, die mit „1“ beginnen, dann einen beliebigen Wert haben und dann mit „3“ fortgesetzt werden.
1.2-3.4	Trifft auf alle OIDs zu, die mit „1“ beginnen, dann mit einer Stelle im Bereich „2 bis 3“ gefolgt von einer „4“ fortgesetzt werden.
1.2.3-4,7-8	Trifft auf alle OIDs zu, die mit „1.2“ beginnen und dann mit einer Stelle im Bereich „3 bis 4“ oder „7 bis 8“ fortgesetzt werden.

Wildcards und Bereichsangaben dürfen an jeder beliebigen Stelle einer OID vorkommen und eine OID darf auch mehrere Wildcards oder Bereichsangaben enthalten. An jeder Stelle darf aber nur entweder eine Wildcard oder eine Bereichsangabe stehen.

Ein LANCOM Gerät bildet die generischen Trap-OIDs des SNMP-Protokolls auf bestimmte Herstellerspezifische OIDs ab:

Bezeichnung	Generische OID	OID bei LANCOM
Kaltstart (coldStart)	0	1.3.6.1.6.3.1.1.5.1
Warmstart (warmStart)	1	1.3.6.1.6.3.1.1.5.2
Link Down (linkDown)	2	1.3.6.1.6.3.1.1.5.3
Link Up (linkUp)	3	1.3.6.1.6.3.1.1.5.4
Authentifizierungsfehler (authenticationFailure)	4	1.3.6.1.6.3.1.1.5.5
EGP-Nachbar (Exterior Gateway Protocol) verloren (egpNeighborLoss)	5	1.3.6.1.6.3.1.1.5.6

Var. Binding ID

Gibt eine OID an, die in den Variable Bindings des Traps enthalten sein muss und die wiederum Wildcards und Bereiche enthalten darf. Siehe hierzu auch **Spec.-Trap ID**. Ein leerer Eintrag gilt für alle variablen Bindings des Gerätes.

Filter-Aktion

Bei einer Übereinstimmung mit den oben eingestellten IDs können Sie den Trap entweder „Zulassen“, also senden oder „Ablehnen“, also verwerfen.

20.9 Netflow / IPFIX

NetFlow ist eine Technik, bei der Netzwerkgeräte wie Router oder Switches Informationen über den ein- und ausgehenden IP-Datenverkehr innerhalb des Geräts per UDP als sogenannte IP-Flows exportieren. Ein IP-Flow enthält u. a. Informationen über Quell-IP-Adresse, Ziel-IP-Adresse, Ports, Zeitstempel sowie Paketzähler. Diese Informationen werden auf einem NetFlow-Kollektor empfangen, gespeichert und verarbeitet. NetFlow kann entweder dauerhaft oder temporär zur Netzwerkanalyse eingesetzt werden.

LANCOM unterstützt die Standards NetFlow 9 (*RFC 3954*) sowie IPFIX (*RFC 7011*), welches eine Erweiterung von Netflow Version 9 darstellt, über das Transportprotokoll UDP.

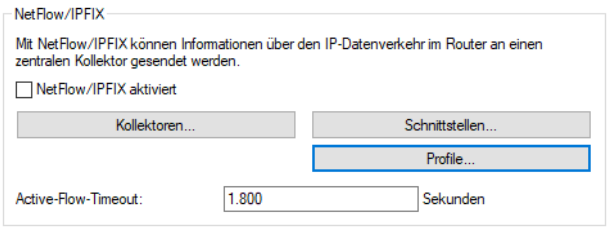
Hinweise zum Einsatz:

› Es wird ein externer NetFlow-Kollektor benötigt, der NetFlow 9 oder IPFIX unterstützt.

- Die Firewall muss grundsätzlich aktiviert sein.
- Bei IPv4 werden nur Flow-Informationen gesammelt, die von einer logischen Schnittstelle zu einer anderen logischen Schnittstelle weitergeleitet werden. Pakete, die der Router selbst erzeugt bzw. an den Router selbst gerichtet sind, werden nicht erfasst. Bei IPv6 gilt diese Einschränkung nicht.
- Es werden nur Unicast IP-Flow-Informationen gesammelt, Multicast (z. B. IPTV) wird nicht unterstützt.
- Je nach Szenario erhöht die Verwendung von NetFlow / IPFIX die CPU-Auslastung und reduziert die Gesamt-Performance des Routers.

20.9.1 NetFlow / IPFIX konfigurieren

In LANconfig konfigurieren Sie NetFlow / IPFIX unter **Meldungen/Monitoring** > **Protokolle** im Abschnitt **NetFlow / IPFIX**.



NetFlow / IPFIX aktiviert

Aktivieren Sie NetFlow / IPFIX auf dem Gerät.

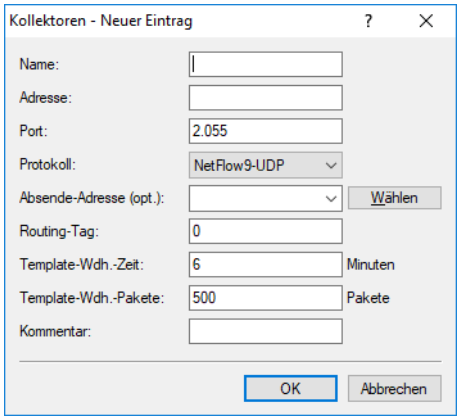
Active-Flow-Timeout

Definiert das Intervall in Sekunden nachdem ein laufender Datenstrom per Netflow exportiert wird. Damit ist es möglich, länger laufende Sessions, z. B. große Downloads, schon während der Laufzeit zu exportieren. Der weitere Datenverkehr wird dann als ein neuer Datenfluss gewertet und die Aufzeichnung des Datenverkehrs für die Meldung beim Collector beginnt von neuem.

Mögliche Werte: 60-1800 Sekunden (0 schaltet die Funktion aus)

20.9.1.1 Kollektoren

Die Kollektoren für NetFlow / IPFIX konfigurieren Sie unter **Meldungen/Monitoring** > **Protokolle** > **NetFlow / IPFIX** > **Kollektoren**.



Name

Eindeutiger Name des NetFlow-Kollektors. Der Name wird in weiteren Tabellen referenziert.

Adresse

IPv4-, IPv6-Adresse oder Hostname des Kollektors.

Port

Port des NetFlow-Kollektors. Meistens Port 2055 für NetFlow 9 und 4739 für IPFIX.

Protokoll

Protokollversion, die vom NetFlow-Kollektor verwendet wird. Mögliche Werte sind NetFlow 9 über UDP oder IPFIX über UDP.

Absende-Adresse

Geben Sie optional eine Absendeadresse an.

Routing-Tag

Geben Sie ein Routing-Tag an, falls eine bestimmte Route zum Kollektor verwendet werden soll.

Template-Wdh.-Zeit

Definiert die Zeit in Minuten, nach der ein NetFlow-Template-Record wiederholt übertragen wird. Der Wert 0 deaktiviert das regelmäßige Senden von Template-Records basierend auf einem Zeitintervall.

Eine Wiederholung der Übertragung des Netflow-Template-Pakets findet entweder nach der definierten Zeit in Minuten oder nach der entsprechenden Anzahl von Flow-Paketen statt, je nachdem welches Ereignis früher eintritt.

Template-Wdh.-Pakete

Definiert die Anzahl von Paketen, nach der ein NetFlow-Template-Record wiederholt übertragen wird. Der Wert 0 deaktiviert das regelmäßige Senden von Template-Records basierend auf einem Paketzähler.

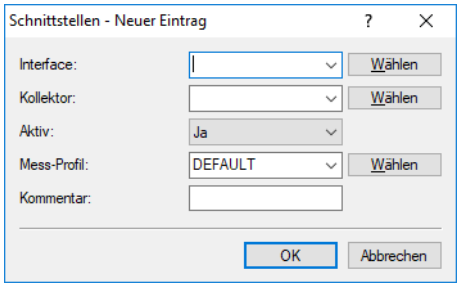
Eine Wiederholung der Übertragung des Netflow-Template-Pakets findet entweder nach der definierten Zeit in Minuten oder nach der entsprechenden Anzahl von Flow-Paketen statt, je nachdem welches Ereignis früher eintritt.

Kommentar

Vergeben Sie optional einen sinnvollen Kommentar als Beschreibung.

20.9.1.2 Schnittstellen

Die Schnittstellen für NetFlow / IPFIX konfigurieren Sie unter **Meldungen/Monitoring** > **Protokolle** > **NetFlow / IPFIX** > **Schnittstellen**.



Interface

Logische Schnittstelle, auf der NetFlow / IPFIX aktiviert werden soll. Mögliche Werte: IPv4-, IPv6-LAN-Schnittstellen, Gegenstellen, IPv6-RAS-Template. Für IPv4-Gegenstellen kann eine Wildcard verwendet werden, z. B. Firma*

Kollektor

Referenziert einen Eintrag aus der Tabelle Kollektoren.

Aktiv

Aktiviert / Deaktiviert NetFlow / IPFIX für diesen Eintrag für die Schnittstelle und den Kollektor.

Mess-Profil

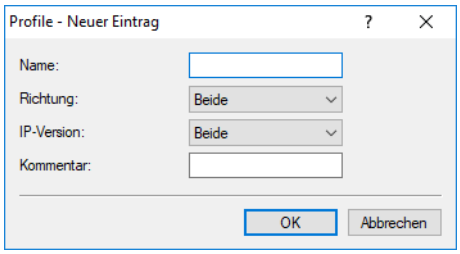
Referenziert einen Eintrag aus der Tabelle Profile.

Kommentar

Vergeben Sie optional einen sinnvollen Kommentar als Beschreibung.

20.9.1.3 Profile

Die Profile für NetFlow / IPFIX konfigurieren Sie unter **Meldungen/Monitoring** > **Protokolle** > **NetFlow / IPFIX** > **Profile**.



Name

Eindeutiger Name des Mess-Profils. Der Name wird in weiteren Tabellen referenziert.

Richtung

IP-Flow-Richtung, die von NetFlow / IPFIX berücksichtigt werden soll. Mögliche Werte jeweils aus der Sicht von NetFlow / IPFIX: Eingehend, Ausgehend, Beide

IP-Version

IP-Protokoll-Version(en), die von NetFlow / IPFIX berücksichtigt werden soll, Mögliche Werte: IPv4, IPv6, Beide

Kommentar

Vergeben Sie optional einen sinnvollen Kommentar als Beschreibung.

20.10 Betrieb von Druckern am USB-Anschluss des Gerätes

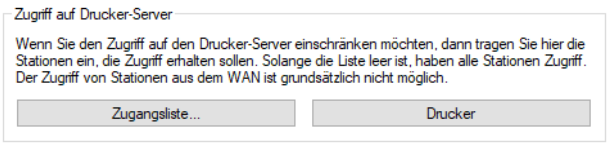
Über den bei verschiedenen Modellen vorhandenen USB-Port können Drucker an das Gerät angeschlossen und so im gesamten Netzwerk verfügbar gemacht werden. Das Gerät stellt dazu einen Printserver zur Verfügung, der die Druckaufträge aus dem Netzwerk verwaltet. Dabei werden die Protokolle RawIP und LPR / LPD unterstützt.

Parallele Druckaufträge von verschiedenen Stationen werden auf den jeweiligen Rechnern gespeichert. Der Printserver im Gerät arbeitet die anliegenden Aufträge nacheinander ab.

20.10.1 Konfiguration des Printservers im Gerät

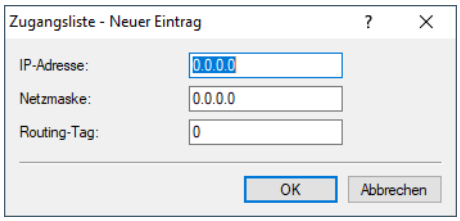
Bei der Konfiguration des USB-Ports für den Anschluss eines Druckers werden in erster Linie die Ports festgelegt, auf denen Druckaufträge über die möglichen Protokolle angenommen werden.

In LANconfig konfigurieren Sie den Printserver unter **Management** > **Erweitert** im Abschnitt **Zugriff auf Drucker-Server**.



20.10.1.1 Zugangs-Liste

In der Zugangsliste werden bis zu 16 Netzwerke eingetragen, die Zugriff auf die konfigurierten Drucker haben. In LANconfig konfigurieren Sie den Printserver unter **Management** > **Erweitert** > **Zugangsliste**.



IP-Adresse

IP-Adresse des Netzwerks, dessen Clients Zugriff auf den Drucker haben dürfen.

Wenn die Zugangsliste keine Einträge enthält, können Rechner mit beliebigen IP-Adressen einen Drucker am USB-Port des Gerätes nutzen.

Der Zugang zu einem Drucker am USB-Port des Gerätes über das WAN ist aus Sicherheitsgründen grundsätzlich nicht möglich.

Netzmaske

Netzmaske zu den erlaubten Netzwerken.

Routing-Tag

Routing-Tag des Netzwerks.

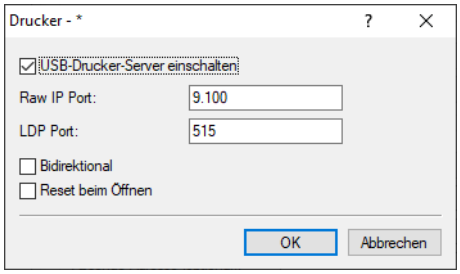
Wenn sie ein Routing-Tag für diese Zugriffs-Regel angeben, so werden nur solche Pakete angenommen, die entweder in der Firewall mit dem gleichen Tag markiert oder über ein Netzwerk mit passendem Schnittstellen-Tag empfangen wurden.

Die Verwendung von Routing-Tags ist folglich nur in Kombination mit entsprechend begleitenden Regeln in der Firewall oder getaggten Netzwerken sinnvoll.

20.10.1.2 Drucker

In der Regel müssen die Einstellungen für den Drucker nicht verändert werden. In der Voreinstellung arbeitet der Printserver sowohl mit RawIP als auch mit LPR/LDP und reagiert auf die Standard-Ports, die von Windows bei der Konfiguration des Druckeranschlusses vorgeschlagen werden. Falls diese Einstellungen keinen erfolgreichen Druckerbetrieb zulassen,

können die Druckerparameter angepasst werden. In LANconfig konfigurieren Sie die Einstellungen für die angeschlossenen Drucker unter **Management** > **Erweitert** > **Drucker**.



USB-Drucker-Server einschalten

Aktivieren Sie hier den Printserver.

Raw-IP-Port

Über diesen Port können Druckaufträge über Raw-IP angenommen werden.

Raw-IP wird von Windows als Standard verwendet und kann für den Betrieb von Druckern am USB-Port empfohlen werden.

LDP-Port

Über diesen Port können Druckaufträge über LDP angenommen werden.

Die hier eingetragenen Optionen zu Protokoll und Port müssen mit den Einstellungen des Druckeranschlusses im Betriebssystem der entsprechenden Rechner übereinstimmen.

Bidirektional

Wenn Sie diese Option aktivieren, dann versendet das Gerät die Statusinformationen des Druckers in regelmäßigen Abständen an die angeschlossenen Rechner.

Reset beim Öffnen

Wenn diese Option aktiviert ist, sendet das Gerät vor dem Öffnen einer Drucker-Session einen Reset-Befehl an den Drucker.

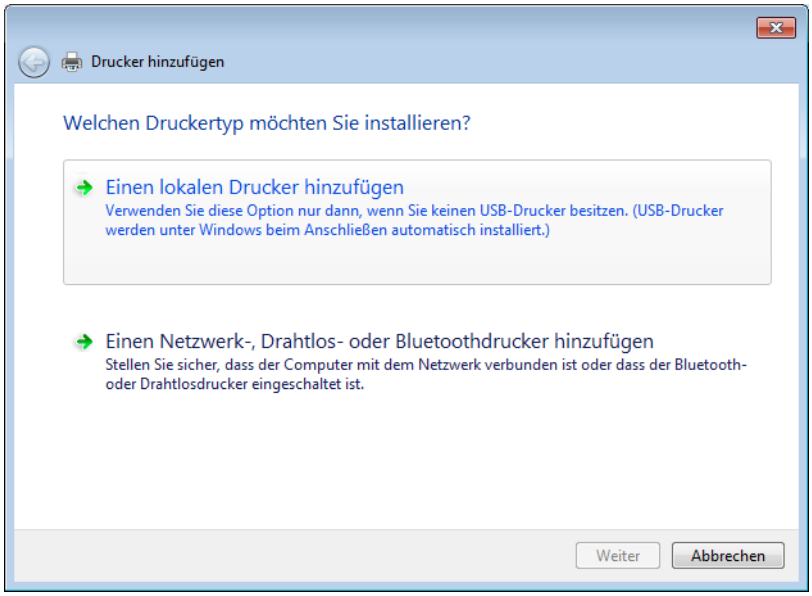
Aktivieren Sie diese Option, wenn der Verbindungsaufbau zum Drucker nicht wie erwartet funktioniert.

20.10.2 Konfiguration der Drucker auf dem Rechner

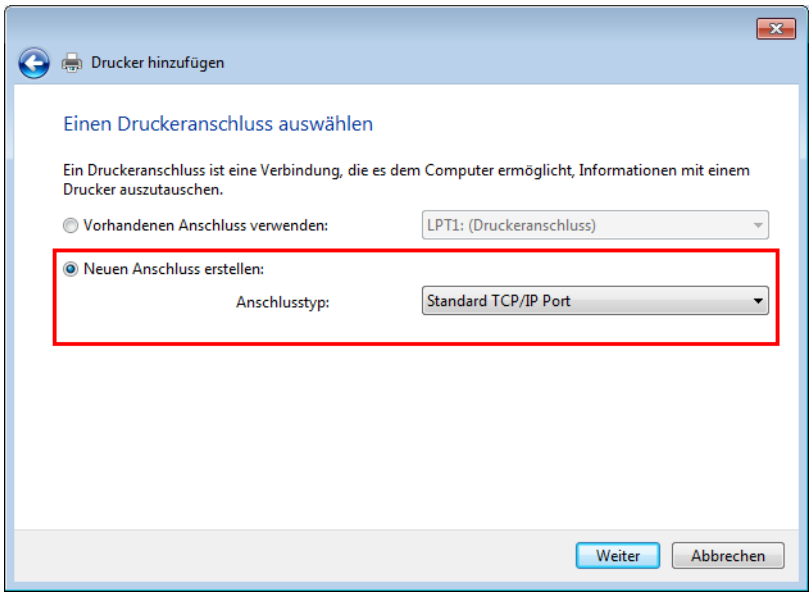
Zur Nutzung des Druckers am USB-Port über das Netzwerk muss auf den Rechnern der Druckertreiber mit einem entsprechenden Druckeranschluss verbunden werden. Die nachfolgende Beschreibung zeigt die Einrichtung unter Windows XP, die Konfiguration unter Windows 2000 verläuft sehr ähnlich. Ältere Windows-Versionen unterstützen die Druckeransteuerung über TCP/IP-Ports nur unzureichend.

1. Öffnen Sie den Dialog zur Konfiguration eines neuen Druckers in der Systemsteuerung und starten Sie den Assistenten zum Hinzufügen eines neuen Druckers.

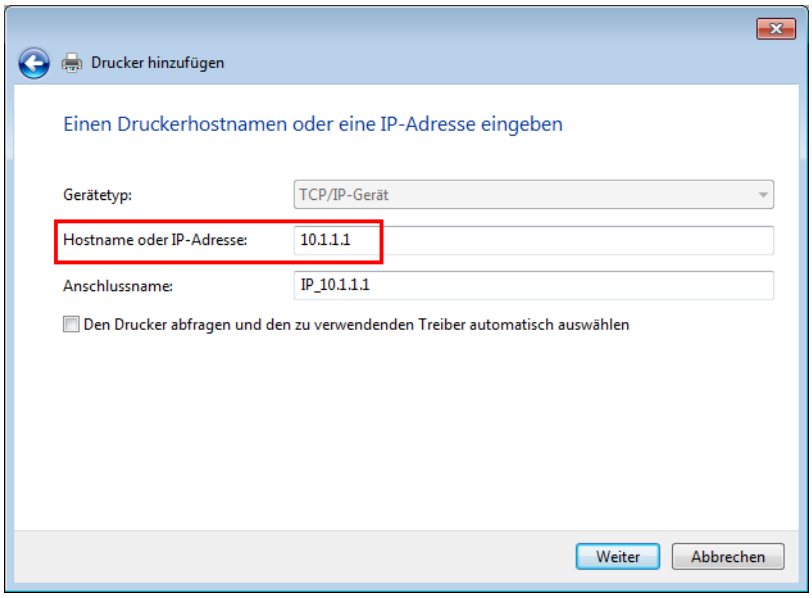
2. Wählen Sie die Option für einen lokalen Drucker und deaktivieren Sie den Plug and Play-Mechanismus.



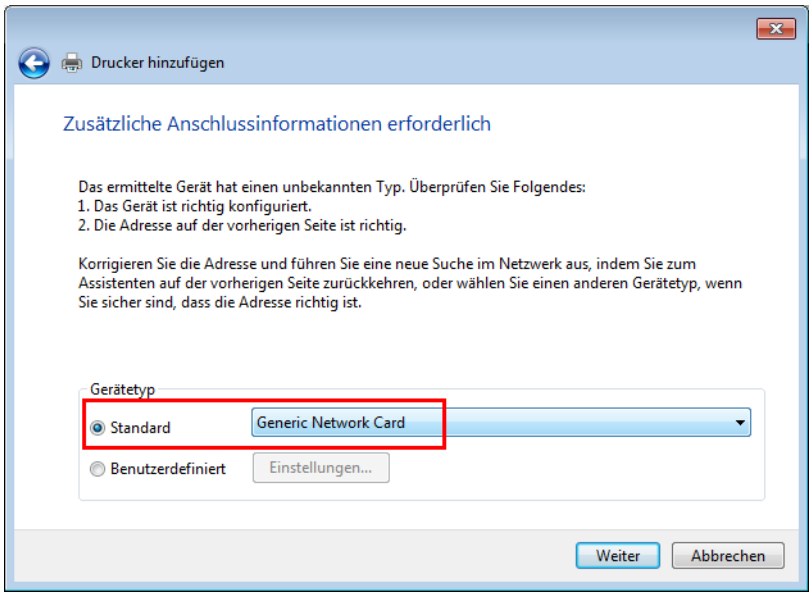
3. Wählen Sie die Option zum Erstellen eines neuen Druckeranschlusses.



4. Geben Sie die IP-Adresse des LCOS-Geräts als IP-Adresse für den Druckeranschluss ein. Der Name des Druckeranschlusses wird automatisch mit `IP_<IP-Address>` vorbelegt.

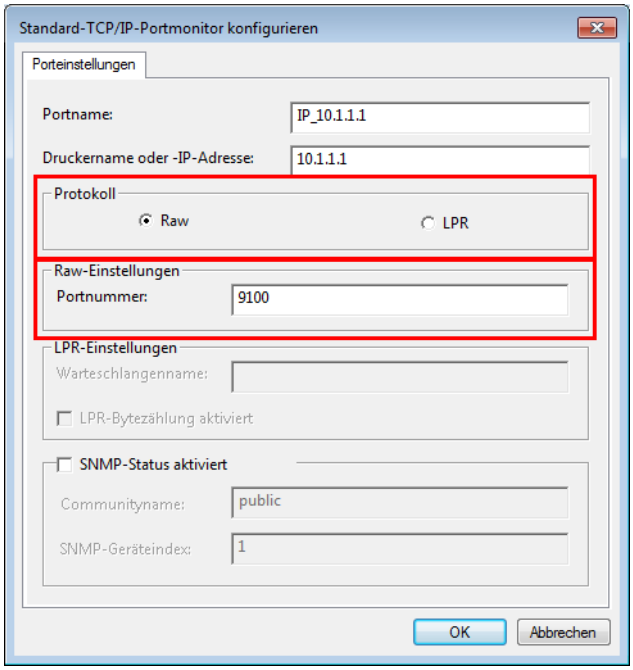


5. Wählen Sie als Gerätetyp die Option 'Standard' für eine 'Generic Network Card' aus. Wenn Sie die Standardeinstellungen beibehalten möchten (empfohlen), öffnen Sie mit der Schaltfläche **Weiter** den nächsten Dialog.



6. Alternativ können Sie mit der Auswahl 'Benutzerdefiniert' und der Schaltfläche **Einstellungen** einen zusätzlichen Dialog aufrufen. In diesem Dialog können Sie das Protokoll auswählen, das für die Übertragung der Druckaufträge

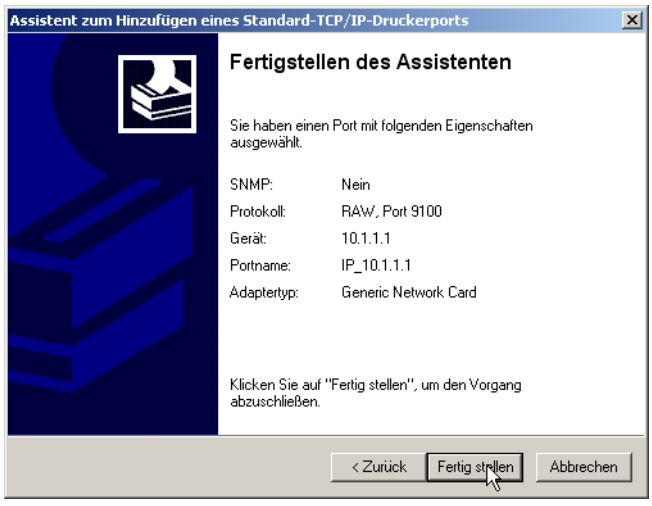
zum Drucker am USB-Port des LCOS-Geräts verwendet werden soll ('Raw' – RawIP oder 'LPR'). Außerdem kann hier der zu verwendende Port (nur bei RawIP) eingetragen werden. Bei LPR wird immer der Standard-Port '515' verwendet.



Die hier eingetragenen Optionen zu Protokoll und Port müssen mit den Einstellungen des Druckers in der LCOS-Konfiguration übereinstimmen.

Der Dialog zur Auswahl von Protokoll und Port kann auch später in der Systemsteuerung über die Eigenschaften eines Druckers auf der Registerkarte 'Anschlüsse' aufgerufen werden.

1. Mit diesen Einstellungen ist der Druckeranschluss fertig eingerichtet. Der Assistent fährt nun fort mit der Auswahl des Druckertreibers.



Weitere Informationen über die Installation des Druckertreibers entnehmen Sie bitte der Dokumentation des Drucker-Herstellers.

20.11 LANCOM Content Filter

20.11.1 Einleitung

Mit dem LANCOM Content Filter können Sie bestimmte Inhalte in Ihrem Netzwerk filtern und dadurch den Zugriff auf z. B. illegale, gefährliche oder anstößige Internetseiten verhindern. Weiterhin können Sie das private Surfen auf bestimmten Seiten während der Arbeitszeit unterbinden. Das steigert nicht nur die Produktivität der Mitarbeiter und die Sicherheit des Netzwerks, sondern sorgt auch dafür, dass die volle Bandbreite ausschließlich für Geschäftsprozesse zur Verfügung steht.

Der LANCOM Content Filter ist ein intelligenter Webseitenfilter und arbeitet dynamisch. Er kontaktiert einen Bewertungsserver, der gemäß den von Ihnen ausgewählten Kategorien die Bewertung der Internetseiten zuverlässig und korrekt vornimmt.

Die Funktion des LANCOM Content Filters basiert auf der Überprüfung der IP-Adressen, die anhand der eingegebenen URL ermittelt werden. Innerhalb einer Domain wird bei vielen Seiten außerdem nach dem Pfad unterschieden, so dass bestimmte Bereiche einer URL unterschiedlich bewertet werden können.

Die Anwender können die Prüfung der aufgerufenen Webseiten durch den LANCOM Content Filter nicht umgehen, indem sie die IP-Adresse zu einer Webseite ermitteln und diese in den Browser eingeben. Der LANCOM Content Filter prüft sowohl unverschlüsselte (HTTP) als auch verschlüsselte Webseiten (HTTPS).

Ab LCOS 10.70 ist das BPjM-Modul ein Bestandteil des Content Filters. Das BPjM-Modul wird von der Bundeszentrale für Kinder- und Jugendmedienschutz herausgegeben und sperrt Domains, die Kindern und Jugendlichen in Deutschland nicht zugänglich gemacht werden dürfen.

Die von Ihnen erworbene Lizenz für den LANCOM Content Filter gilt für eine bestimmte Anzahl Benutzer und einen bestimmten Zeitraum (jeweils für ein Jahr oder drei Jahre). Sie werden rechtzeitig über den Ablauf Ihrer Lizenz informiert. Die Anzahl der aktuellen Benutzer wird im Gerät geprüft, dabei werden die Benutzer über die IP-Adresse identifiziert. Sie können das Verhalten bei Lizenzüberschreitung einstellen: Entweder wird der Zugriff verboten oder es wird eine ungeprüfte Verbindung hergestellt. Das enthaltene BPjM-Modul ist, unabhängig von der Anzahl der lizenzierten Content Filter-Benutzer, nicht nutzerlimitiert.

Sie können den LANCOM Content Filter auf jedem Router testen, der diese Funktion unterstützt. Hierfür müssen Sie für jedes Gerät einmalig eine zeitlich befristete 30-Tage-Demo-Lizenz aktivieren. Demo-Lizenzen werden direkt aus LANconfig heraus erstellt. Klicken Sie mit der rechten Maustaste auf das Gerät, wählen Sie im Kontextmenü den Eintrag **Software-Option aktivieren** und im folgenden Dialog die Schaltfläche **Demolizenz**

registrieren. Sie werden automatisch mit der Webseite des LANCOM Registrierungsservers verbunden, auf der Sie die gewünschte Demo-Lizenz auswählen und für das Gerät registrieren können.



Über die Kategorieprofile speichern Sie alle Einstellungen bezüglich der Kategorien. Dabei wählen Sie aus vordefinierten Haupt- und Unterkategorien in Ihrem LANCOM Content Filter: 59 Kategorien sind zu 14 Gruppen thematisch zusammengefasst, z. B. „Pornographie / Nacktheit“, „Einkaufen“ oder „Kriminelle Aktivitäten“. Für jede dieser Gruppen lassen sich die enthaltenen Kategorien aktivieren oder deaktivieren. Die Unterkategorien für „Pornographie/Nacktheit“ sind z. B. „Pornographie / Erotik / Sex“, „Bademoden / Dessous“.

Zusätzlich kann der Administrator bei der Konfiguration für jede dieser Kategorien die Option des Override aktivieren. Bei aktivem Override kann der Benutzer den Zugriff auf eine verbotene Seite durch einen Klick auf eine entsprechende Schaltfläche für eine bestimmte Zeitspanne freischalten – allerdings erhält der Administrator in diesem Fall eine Benachrichtigung per E-Mail, SYSLOG und / oder SNMP-Trap.

Mit dem von Ihnen erstellten Kategorieprofil, der Whitelist und der Blacklist können Sie ein Content-Filter-Profil anlegen, welches über die Firewall gezielt Benutzern zugeordnet werden kann. Beispielsweise können Sie das Profil „Mitarbeiter_Abteilung_A“ anlegen, welches dann allen Computern der entsprechenden Abteilung zugeordnet wird.

Bei der Installation des LANCOM Content Filters werden sinnvolle Standardeinstellungen automatisch eingerichtet, die für den ersten Start nur aktiviert werden müssen. In weiteren Schritten können Sie das Verhalten des LANCOM Content Filters weiter an Ihren speziellen Anwendungsfall anpassen.

Auch für das BPjM-Modul werden sinnvolle Standardeinstellungen automatisch eingerichtet. So existiert in der IPv4- bzw. IPv6-Firewall eine Default-Firewall-Regel mit dem System-Objekt „BPJM“ als Zielstation. Definieren Sie als Quell-Stationen die Netzwerke, die durch das BPjM-Modul geschützt werden sollen. Durch Aktivierung der Regel wird das BPjM-Modul gestartet.

Der Content Filter arbeitet mit einem Concurrent User Modell. Dieses Modell lizenziert die Anzahl der **gleichzeitigen** Benutzer des Content Filters. Dabei hält der Content Filter einen angemeldeten Benutzer nur für 5 Minuten in der internen Benutzerliste. Aufgrund dieser Tatsache haben auch wechselnde Benutzer innerhalb eines Tages die Möglichkeit, den Content Filter zu nutzen. Ihre Lizenz prüft dabei nur die Anzahl der tatsächlich gleichzeitigen Benutzer (innerhalb des Zeitraums von 5 Minuten).

20.11.2 Voraussetzungen für die Benutzung des LANCOM Content Filters

Folgende Voraussetzungen müssen erfüllt sein, damit Sie den LANCOM Content Filter benutzen können:

1. Die LANCOM Content Filter Option ist aktiviert.
2. Die Firewall muss aktiviert sein.
3. Eine Firewall-Regel muss das Content-Filter-Profil auswählen.
4. Das gewählte Content-Filter-Profil muss für jeden Zeitraum des Tages ein Kategorieprofil und nach Wunsch eine White- und / oder Blacklist festlegen. Um die verschiedenen Zeiträume abzudecken, kann ein Content-Filter-Profil aus mehreren Einträgen bestehen.

   Wird ein bestimmter Zeitraum des Tages nicht über einen Eintrag abgedeckt, so ist in diesem Zeitraum ein ungeprüfter Zugriff auf die Webseiten möglich.

Wenn das Content-Filter-Profil nachträglich umbenannt wird, muss die Firewallregel ebenfalls angepasst werden.

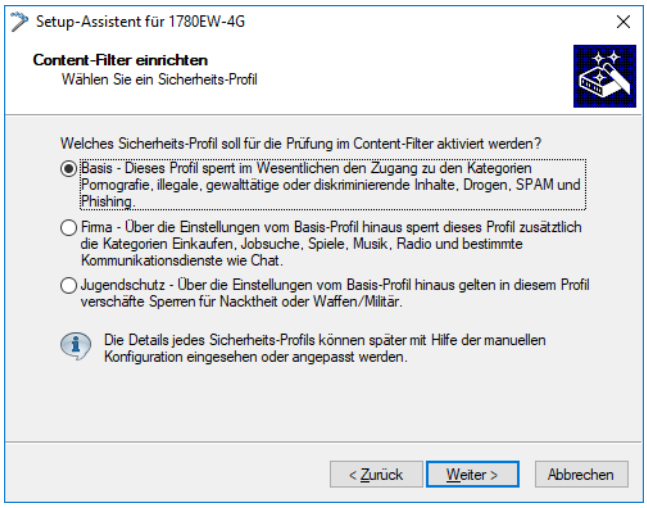
20.11.3 Schnellstart

Nach der Installation des LANCOM Content Filters sind alle Einstellungen für eine schnelle Inbetriebnahme vorbereitet.

Der Betrieb des LANCOM Content Filters kann durch die Datenschutzrichtlinien in Ihrem Land oder Betriebsvereinbarungen in Ihrem Unternehmen eingeschränkt sein. Bitte prüfen Sie vor Inbetriebnahme die geltenden Regelungen.

Aktivieren Sie den Content Filter in den folgenden Schritten:

1. Rufen Sie für das entsprechende Gerät den Setup-Assistenen auf.
2. Wählen Sie den Setup-Assistenten zur Konfiguration des Content Filters.



3. Wählen Sie eines der vordefinierten Sicherheitsprofile (Basis-Profil, Firmen-Profil, Jugendschutz-Profil):
   - Basis-Profil: Diese Profil sperrt im Wesentlichen den Zugang zu den Kategorien Pornografie, illegale, gewalttätige oder diskriminierende Inhalte, Drogen, SPAM und Phishing
   - Firmen-Profil: Über die Einstellungen des Basis-Profils hinaus sperrt dieses Profil zusätzlich die Kategorien Einkaufen, Jobsuche, Spiele, Musik, Radio und bestimmte Kommunikationsdienste wie Chat.
   - Jugendschutz-Profil: Über die Einstellungen des Basis-Profils hinaus gelten in diesem Profil verschärfte Sperren für Nacktheit oder Waffen / Militär.

   Falls die Firewall ausgeschaltet ist, schaltet der Assistent die Firewall ein. Dann prüft der Assistent, ob die Firewall-Regel für den Content Filter richtig eingestellt ist und korrigiert diese, sofern nötig. Mit diesen Schritten haben Sie den Content Filter aktiviert, es gelten immer die Standardeinstellungen für alle Stationen im Netzwerk mit dem

ausgewählten Content-Filter-Profil und den noch leeren Black- und Whitelists. Passen Sie diese Einstellungen ggf. an Ihre Bedürfnisse an. Der Assistent aktiviert den Content Filter für den Zeitrahmen ALWAYS.

20.11.4 Die Standardeinstellungen im LANCOM Content Filter

In der Standardeinstellung sind im LANCOM Content Filter folgende Elemente angelegt:

Firewall-Regel

Die voreingestellte Firewall-Regel hat den Namen CONTENT-FILTER und verwendet das Aktionsobjekt CONTENT-FILTER-BASIC.

Firewall-Aktions-Objekte

Es existieren drei Firewall-Aktions-Objekte:

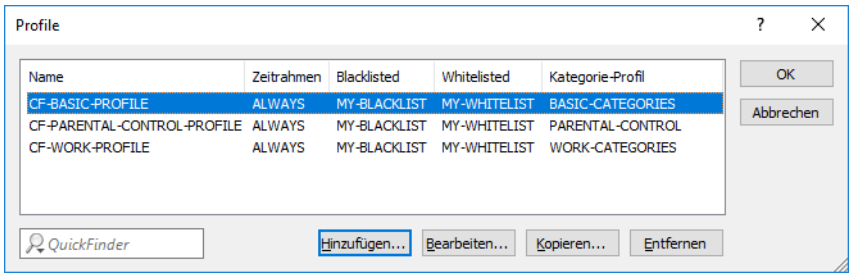
- CONTENT-FILTER-BASIC
- CONTENT-FILTER-WORK
- CONTENT-FILTER-PARENTAL-CONTROL

Diese Aktionsobjekte greifen auf die entsprechenden Content-Filter-Profile zurück.

Content-Filter-Profile

Es existieren drei Content-Filter-Profile. Alle Content Filter-Profile nutzen den Zeitrahmen ALWAYS, die Blacklist MY-BLACKLIST und die Whitelist MY-WHITELIST. Jedes Content-Filter-Profil nutzt eines der vordefinierten Kategorie-Profile:

- CF-BASIC-PROFILE: Dieses Content-Filter-Profil verfügt nur über geringe Einschränkungen und nutzt das Kategorie-Profil BASIC-CATEGORIES.
- CF-PARENTAL-CONTROL-PROFILE: Mit diesem Content-Filter-Profil können Minderjährige (z. B. Auszubildende) vor ungeeigneten Internetinhalten geschützt werden, es nutzt das Kategorie-Profil PARENTAL-CONTROL.
- CF-WORK-PROFILE: Dieses Content-Filter-Profil ist für den Einsatz in Unternehmen gedacht und sperrt z. B. die Kategorien Jobsuche oder Chat, es nutzt das Kategorie-Profil WORK-CATEGORIES.



Zeitrahmen

Es gibt zwei definierte Zeitrahmen:

- ALWAYS: 00.00-23.59 Uhr
- NEVER: 00.00-0.00 Uhr

Blacklist

Die voreingestellte Blacklist hat den Namen MY-BLACKLIST und ist leer. Tragen Sie hier optional die URLs ein, die für Ihre Anwendung verboten werden sollen.

Whitelist

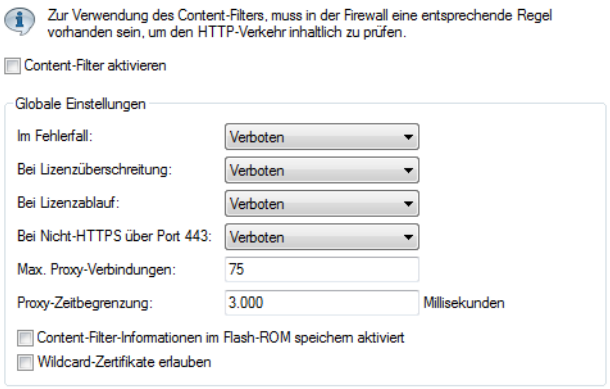
Die voreingestellte Whitelist hat den Namen MY-WHITELIST und ist leer. Tragen Sie hier optional die URLs ein, die für Ihre Anwendung erlaubt werden sollen.

Kategorieprofile

Es existieren drei Kategorieprofie: BASIC-CATEGORIES, WORK-CATEGORIES und PARENTAL-CONTROL. Das Kategorie-Profil enthält die Angaben darüber, welche Kategorien erlaubt und verboten sind und für welche ein sogenannter Override aktiviert ist.

20.11.5 Allgemeine Einstellungen

Die globalen Einstellungen des LANCOM Content Filters nehmen Sie in LANconfig unter **Content-Filter** > **Allgemein** vor:



Content Filter aktivieren

Hier können Sie den LANCOM Content Filter aktivieren.

Im Fehlerfall

Hier können Sie bestimmen, was bei einem Fehler passieren soll. Kann der Bewertungsserver beispielsweise nicht kontaktiert werden, kann der Benutzer in Folge dieser Einstellung entweder ungehindert surfen oder aber es wird der komplette Webzugriff verboten.

Bei Lizenzüberschreitung

Hier können Sie bestimmen, was bei Überschreitung der lizensierten Benutzeranzahl passieren soll. Die Benutzer werden über die IP-Adresse identifiziert. Das heißt, dass die IP-Adressen, die eine Verbindung durch den LANCOM Content Filter aufbauen, gezählt werden. Baut z. B. bei einer 10er-Option ein elfter Benutzer eine Verbindung auf, findet keine Prüfung mehr durch den LANCOM Content Filter statt. Der Benutzer, für den keine Lizenz mehr zur Verfügung steht, kann in Folge dieser Einstellung entweder ungehindert surfen oder aber es wird der komplette Webzugriff verboten.

Die Benutzer des Content Filters werden automatisch aus der Benutzerliste entfernt, wenn von dieser IP-Adresse seit 5 Minuten keine Verbindung durch den Content Filter mehr aufgebaut wurde.

Bei Lizenzablauf

Die Lizenz zur Nutzung des LANCOM Content Filters gilt für einen bestimmten Zeitraum. Sie werden 30 Tage, eine Woche und einen Tag vor Ablauf der Lizenz an die auslaufende Lizenz erinnert (an die E-Mailadresse, die in LANconfig konfiguriert ist unter **Meldungen** > **Allgemein** > **E-Mail-Adressen** > **Für Lizenz-Ablauf-Erinnerung**.

Hier können Sie bestimmen, ob Webseiten nach Ablauf der Lizenz blockiert oder ungeprüft durchgelassen werden sollen. Der Benutzer kann in Folge dieser Einstellung nach Ablauf der für ihn verwendeten Lizenz entweder ungehindert surfen oder aber es wird der komplette Webzugriff verboten.

Damit die Erinnerung auch tatsächlich an die angegebene E-Mailadresse versendet wird, müssen Sie das entsprechende SMTP-Konto konfigurieren.

Nicht-HTTPS-Traffic über Port 443

Verboten

Lässt Nicht-HTTPS-Traffic über Port 443 nicht zu.

Erlaubt

Lässt Nicht-HTTPS-Traffic über Port 443 zu.

Der TCP-Port 443 ist standardmäßig ausschließlich für HTTPS-Verbindungen reserviert.

Einige Applikationen, die nicht HTTPS nutzen, verwenden dennoch TCP-Port 443. Für diesen Fall haben Sie hier die Möglichkeit, den TCP-Port 443 auch für Nicht-HTTPS-Verbindungen zu öffnen.

Falls Sie Nicht-HTTPS-Verbindungen über Port 443 zulassen, wird der Traffic nicht weiter klassifiziert, sondern ganz pauschal zugelassen. Per Default werden Nicht-HTTPS-Verbindungen über Port 443 nicht zugelassen.

Max. Proxy-Verbindungen

Stellen Sie hier die Anzahl der Proxy-Verbindungen ein, die maximal gleichzeitig aufgebaut werden dürfen. Die Last kann somit auf dem System eingeschränkt werden. Es wird eine Benachrichtigung ausgelöst, wenn diese Anzahl überschritten wird. Die Art der Benachrichtigung können Sie unter **Content Filter** > **Optionen** > **Ereignisse** einstellen.

Proxy-Zeitbegrenzung

Stellen Sie hier die Zeit in Millisekunden ein, die der Proxy maximal für die Bearbeitung benötigen darf. Wird diese Zeit überschritten, wird dies durch eine entsprechende Zeitüberschreitungs-Fehlerseite quittiert.

Content-Filter-Informationen im Flash-ROM speichern aktiviert

Wenn Sie diese Option aktivieren, können Sie die Content-Filter-Informationen zusätzlich im Flash-ROM des Gerätes speichern.

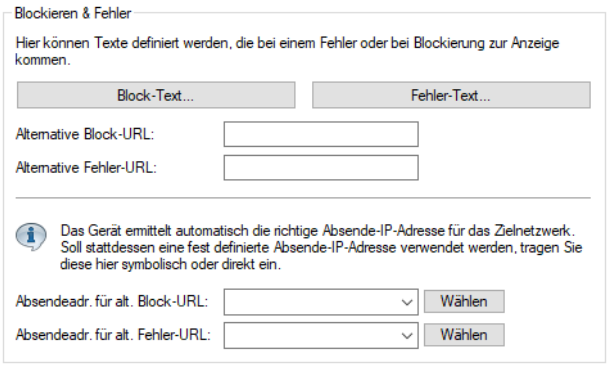
Wildcard-Zertifikate erlauben

Bei Webseiten mit Wildcard-Zertifikaten (bestehend aus CN-Einträgen wie z. B. `*.mydomain.de`) wird durch das Einschalten dieser Funktion die Haupt-Domain (`mydomain.de`) zur Prüfung herangezogen. Die Prüfung erfolgt dabei in dieser Reihenfolge:

- Prüfung des Servernamens im „Client Hello“ (abhängig vom verwendeten Webbrowser)
- Prüfung des CN im empfangenen SSL-Zertifikat
- Einträge mit Wildcards werden dabei ignoriert
- Ist der CN nicht verwertbar, wird das Feld „Alternative Name“ ausgewertet
- DNS Reverse Lookup der zugehörigen IP-Adresse und Prüfung des so erlangten Hostnamens
- Sind im Zertifikat Wildcards enthalten, wird stattdessen die Haupt-Domain geprüft (entspricht der oben beschriebenen Funktion)
- Prüfung der IP-Adresse

20.11.6 Einstellungen für das Blockieren

Die Einstellungen für das Blockieren von Webseiten nehmen Sie hier vor:



LANconfig: **Content-Filter** > **Blockieren / Override** > **Blockieren 6amp; Fehler**

Kommandozeile: **Setup** > **UTM** > **Content-Filter** > **Globale-Einstellungen**

Alternative Block-URL:

Hier können Sie eine alternative URL-Adresse eintragen. Im Falle des Blockierens wird dann statt der Standard-Webseite die hier eingetragene URL aufgerufen. In der externen HTML-Seite können Sie z. B. das Corporate Design Ihres Unternehmens abbilden oder weitere Funktionen wie JavaScript etc. nutzen. Außerdem können hier auch die gleichen HTML-Tags wie im Block-Text verwendet werden. Wenn Sie an dieser Stelle keinen Eintrag vornehmen, wird die im Gerät hinterlegte Standard-Webseite aufgerufen.

Mögliche Werte:

- gültige URL-Adresse

Default:

- leer

Alternative Fehler-URL:

Hier können Sie eine alternative URL-Adresse eintragen. Im Falle eines Fehlers wird dann statt der Standard-Webseite die hier eingetragene URL aufgerufen. In der externen HTML-Seite können Sie z. B. das Corporate Design Ihres Unternehmens abbilden oder weitere Funktionen wie JavaScript etc. nutzen. Außerdem können hier auch die gleichen HTML-Tags wie im Fehler-Text verwendet werden. Wenn Sie an dieser Stelle keinen Eintrag vornehmen, wird die im Gerät hinterlegte Standard-Webseite aufgerufen.

Mögliche Werte:

- gültige URL-Adresse

Default:

- leer

Absendeadr. für alt. Block-URL:

Hier können Sie optional eine Absende-Adresse konfigurieren, die statt der ansonsten automatisch für die Ziel-Adresse gewählten Absende-Adresse verwendet wird. Falls Sie z. B. Loopback-Adressen konfiguriert haben, können Sie diese hier als Absende-Adresse angeben.

Mögliche Werte:

- Name der IP-Netzwerke, deren Adresse eingesetzt werden soll
- INT für die Adresse des ersten Intranets
- DMZ für die Adresse der ersten DMZ

Wenn es eine Schnittstelle Namens DMZ gibt, dann wird deren Adresse genommen!

- LB0…LBF für die 16 Loopback-Adressen
- GUEST
- Beliebige IP-Adresse in der Form x.x.x.x

Default:

- leer

Die hier eingestellte Absende-Adresse wird für jede Gegenstelle unmaskiert verwendet.

Absendeadr. für alt. Fehler-URL:

Hier können Sie optional eine Absende-Adresse konfigurieren, die statt der ansonsten automatisch für die Ziel-Adresse gewählten Absende-Adresse verwendet wird. Falls Sie z. B. Loopback-Adressen konfiguriert haben, können Sie diese hier als Absende-Adresse angeben.

Mögliche Werte:

- Name der IP-Netzwerke, deren Adresse eingesetzt werden soll
- INT für die Adresse des ersten Intranets
- DMZ für die Adresse der ersten DMZ

Wenn es eine Schnittstelle Namens DMZ gibt, dann wird deren Adresse genommen!

- LB0…LBF für die 16 Loopback-Adressen
- GUEST
- Beliebige IP-Adresse in der Form x.x.x.x

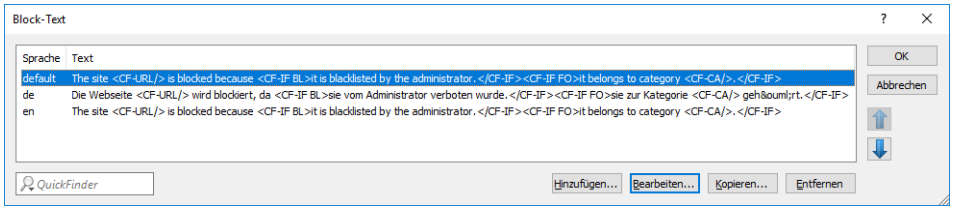
Default:

- leer

Die hier eingestellte Absende-Adresse wird für jede Gegenstelle unmaskiert verwendet.

20.11.6.1 Block-Text

Hier können Sie einen Text definieren, der bei Blockierung angezeigt wird. Für unterschiedliche Sprachen kann jeweils ein eigener Block-Text definiert wird. Die Auswahl des verwendeten Block-Textes wird anhand der übermittelten Spracheinstellung des Browsers (User Agents) vorgenommen.



Sprache

Damit der Anwender alle Meldungen in seiner voreingestellten Browser-Sprache erhält, kann hier der entsprechende Country-Code eingetragen werden. Wird der im Browser eingestellte Country-Code hier gefunden, kommt der dazu passende Text zur Anzeige.

Weitere Sprachen können nach Belieben hinzugefügt werden.

Der Country-Code sieht dafür z. B. folgendermaßen aus:

- de-DE: Deutschsprachig-Deutschland
- de-CH: Deutschsprachig-Schweiz
- de-AT: Deutschsprachig-Österreich
- en-GB: Englischsprachig-Großbritannien
- en-US: Englischsprachig-Vereinigte Staaten

Der Country-Code muss genau der Spracheinstellung des Browsers entsprechen, z. B. muss für Deutsch „de-DE" eingegeben werden (es reicht nicht „de"). Wird der im Browser eingestellte Country-Code in dieser Tabelle nicht gefunden oder der dafür hinterlegte Text gelöscht, so wird der bereits vordefinierte Standardtext (Default) verwendet. Den Default-Text können Sie bearbeiten.

Mögliche Werte:

- 10 alphanumerische Zeichen

Default:

- leer

Text

Geben Sie hier den Text ein, der als Block-Text für diese Sprache verwendet werden soll.

Mögliche Werte:

- 254 alphanumerische Zeichen

Default:

- leer

Besondere Werte:

Sie können für den Block-Text auch spezielle Tags verwenden, wenn Sie unterschiedliche Seiten anzeigen wollen, je nachdem, aus welchem Grund (z. B. verbotene Kategorie oder Eintrag in der Blacklist) die Seite verboten wurde.

Für die einzusetzenden Werte können Sie folgende Tags verwenden:

- <CF-URL/> für die verbotene URL
- <CF-CATEGORIES/> für die Liste der Kategorien aufgrund der die Webseite verboten wurde
- <CF-PROFILE/> für den Profilnamen
- <CF-OVERRIDEURL/> für die URL zum Freischalten des Overrides (diese kann in ein einfaches <a>-Tag oder einen Button eingebaut werden)
- <CF-LINK/> fügt einen Link zum Freischalten des Overrides ein
- <CF-BUTTON/> für einen Button zum Freischalten des Overrides
- <CF-IF att1 att2> … </CF-IF> zum Ein- und Ausblenden von Teilen des HTML-Dokuments. Die Attribute sind:
  - BLACKLIST: wenn die Seite verboten wurde, weil sie auf der Blacklist des Profils steht
  - CATEGORY: wenn die Seite aufgrund einer ihrer Kategorien verboten wurde
  - ERR: wenn ein Fehler aufgetreten ist.
  - OVERRIDEOK: wenn dem Benutzer ein Override erlaubt wurde (in diesem Fall sollte die Seite eine entsprechende Schaltfläche anzeigen)

    Da es getrennte Texttabellen für die Blockseite und die Fehlerseite gibt, ist das Attribut nur sinnvoll, wenn Sie eine alternative Block-URL konfiguriert haben.

Werden in einem Tag mehrere Attribute angegeben, dann wird der Bereich eingeblendet, wenn mindestens eine dieser Bedingungen erfüllt ist. Alle Tags und Attribute lassen sich mit den jeweils ersten zwei Buchstaben abkürzen (z. B. CF-CA oder CF-IF BL). Das ist notwendig, weil der Block-Text nur maximal 254 Zeichen lang sein darf.

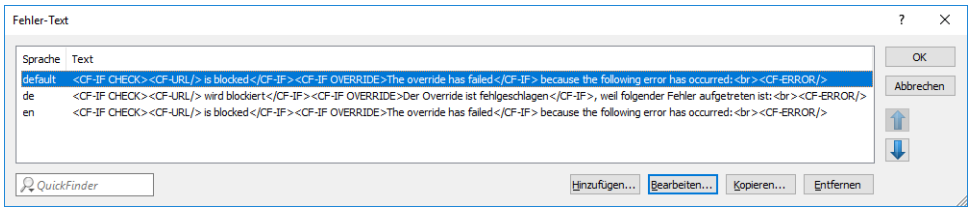
- Beispiel:

  <CF-URL/> wird wegen der Kategorien <CF-CA/> verboten.
Ihr Contentfilterprofil ist <CF-PR/>.
<CF-IF OVERRIDEOK>
<CF-BU/></CF-IF>

Die hier beschriebenen Tags können auch in externen HTML-Seiten (alternative Block-URL) verwendet werden.

20.11.6.2 Fehler-Text

Hier können Sie einen Text definieren, der bei einem Fehler zur Anzeige kommt.



Sprache

Damit der Anwender alle Meldungen in seiner voreingestellten Browser-Sprache erhält, kann hier der entsprechende Country-Code eingetragen werden. Wird der im Browser eingestellte Country-Code hier gefunden, kommt der dazu passende Text zur Anzeige.

Weitere Sprachen können nach Belieben hinzugefügt werden.

Der Country-Code sieht dafür z. B. folgendermaßen aus:

- de-DE: Deutschsprachig-Deutschland
- de-CH: Deutschsprachig-Schweiz
- de-AT: Deutschsprachig-Österreich
- en-GB: Englischsprachig-Großbritannien
- en-US: Englischsprachig-Vereinigte Staaten

Der Country-Code muss genau der Spracheinstellung des Browsers entsprechen, z. B. muss für Deutsch „de-DE" eingegeben werden (es reicht nicht „de"). Wird der im Browser eingestellte Country-Code in dieser Tabelle nicht gefunden oder der dafür hinterlegte Text gelöscht, so wird der bereits vordefinierte Standardtext (Default) verwendet. Den Default-Text können Sie bearbeiten.

Mögliche Werte:

- 10 alphanumerische Zeichen

Default:

- leer

Text

Geben Sie hier den Text ein, der als Fehler-Text für diese Sprache verwendet werden soll.

Mögliche Werte:

- 254 alphanumerische Zeichen

Default:

- leer

Besondere Werte:

Sie können für den Fehler-Text auch HTML-Tags verwenden.

Für die einzusetzenden Werte können Sie folgende Empty-Element-Tags verwenden:

- <CF-URL/> für die verbotene URL
- <CF-PROFILE/> für den Profilnamen
- <CF-ERROR/> für die Fehlermeldung
- Beispiel:

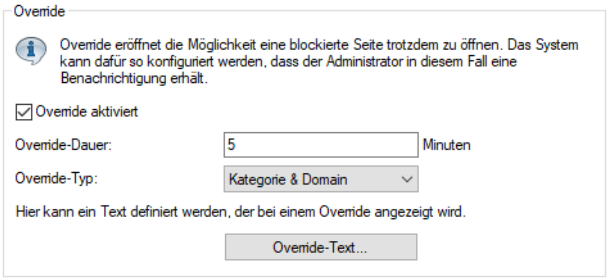
  <CF-URL/> wird verboten, weil ein Fehler aufgetreten ist:
<CF-ERROR/>

20.11.7 Override-Einstellungen

Die Override-Funktion ermöglicht, eine Webseite zu öffnen, obwohl sie zu einer verbotenen Kategorie gehört. Wenn die verbotene Seite geöffnet werden soll, muss der Benutzer dies mit einem Klick auf den Override-Button anfordern. Sie können die Konfiguration so einstellen, dass der Administrator bei Klick auf den Override-Button eine Benachrichtigung erhält (LANconfig: **Content Filter** > **Optionen** > **Ereignisse**).

Durch den Klick auf den Override-Button schaltet der Benutzer, wenn der Override-Typ „Kategorie" aktiviert ist, **alle** Kategorien frei, zu denen die aufgerufene URL gehört. Auf der zunächst angezeigten Blockseite wird nur eine Kategorie angezeigt, aufgrund derer der Zugriff auf die URL gesperrt werden soll. Wenn der Override-Typ „Domain" aktiviert ist, wird die Domain freigeschaltet.

Die Einstellungen für die Override-Funktion finden Sie hier:



LANconfig: **Content-Filter** > **Blockieren / Override** > **Override**

Kommandozeile: **Setup** > **UTM** > **Content-Filter** > **Globale-Einstellungen**

Override aktiviert

Hier können Sie die Override-Funktion aktivieren und weitere Einstellungen für diese Funktion vornehmen.

Override-Dauer

Der Override kann hier zeitlich begrenzt werden. Nach Ablauf der Zeitspanne wird jedes Betreten der gleichen Domain und / oder Kategorie wieder verboten. Mit einem erneuten Klick auf den Override-Button kann die Seite wieder für die Override-Dauer betreten werden, der Administrator erhält je nach Einstellung eine erneute Benachrichtigung.

Mögliche Werte:

- 1-1440 (Minuten)

Default:

- 5 (Minuten)

Override-Typ

Hier können Sie den Override-Typ einstellen, für den der Override gelten soll. Er kann für die Domain oder die Kategorie der zu blockierenden Seite oder für beides erlaubt werden.

Mögliche Werte:

Kategorie

Während der Override-Dauer sind alle URLs erlaubt, die unter die angezeigten Kategorien fallen (zuzüglich derer, die auch ohne den Override schon erlaubt gewesen wären).

Domain

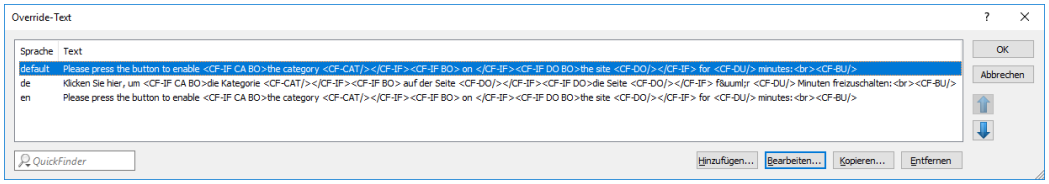
Während der Override-Dauer sind alle URLs unter der besuchten Domain erlaubt, egal zu welchen Kategorien sie gehören.

Kategorie und Domain

Während der Override-Dauer sind alle URLs erlaubt, die sowohl zu dieser Domain als auch zu den freigeschalteten Kategorien gehören. Dies ist die stärkste Einschränkung.

20.11.7.1 Override-Text

Hier können Sie einen Text definieren, der als Bestätigung für den Benutzer bei einem Override angezeigt wird.



Sprache

Damit der Anwender alle Meldungen in seiner voreingestellten Browser-Sprache erhält, kann hier der entsprechende Country-Code eingetragen werden. Wird der im Browser eingestellte Country-Code hier gefunden, kommt der dazu passende Text zur Anzeige.

Weitere Sprachen können nach Belieben hinzugefügt werden.

Der Country-Code sieht dafür z. B. folgendermaßen aus:

- de-DE: Deutschsprachig-Deutschland
- de-CH: Deutschsprachig-Schweiz
- de-AT: Deutschsprachig-Österreich
- en-GB: Englischsprachig-Großbritannien
- en-US: Englischsprachig-Vereinigte Staaten

Der Country-Code muss genau der Spracheinstellung des Browsers entsprechen, z. B. muss für Deutsch „de-DE“ eingegeben werden (es reicht nicht „de“). Wird der im Browser eingestellte Country-Code in dieser Tabelle nicht gefunden oder der dafür hinterlegte Text gelöscht, so wird der bereits vordefinierte Standardtext (Default) verwendet. Den Default-Text können Sie bearbeiten.

Mögliche Werte:

- 10 alphanumerische Zeichen

Default:

- leer

Text

Geben Sie hier den Text ein, der als Override-Text für diese Sprache verwendet werden soll.

Mögliche Werte:

- 254 alphanumerische Zeichen

Default:

- leer

Besondere Werte:

Sie können für den Block-Text auch HTML-Tags verwenden, wenn Sie unterschiedliche Seiten anzeigen wollen, je nachdem aus welchem Grund (z. B. verbotene Kategorie oder Eintrag in der Blacklist) die Seite verboten wurde.

Für die einzusetzenden Werte können Sie folgende Tags verwenden:

- <CF-URL/> für die ursprünglich verbotene URL, die jetzt aber freigeschaltet ist
- <CF-CATEGORIES/> für die Liste der Kategorien, die durch diesen Override freigeschaltet sind (außer bei Domain-Override).
- <CF-BUTTON/> zeigt einen Override-Button, der auf die ursprünglich aufgerufene URL weiterleitet.
- <CF-LINK/> zeigt einen Override-Link an, der auf die ursprünglich aufgerufene URL weiterleitet.
- <CF-HOST/> oder <CF-DOMAIN/> zeigen den Hostteil bzw. die Domain der freigeschalteten URL an. Die Tags sind gleichwertig und können wahlweise verwendet werden.
- <CF-ERROR/> erzeugt eine Fehlermeldung, falls der Override fehlschlägt.
- <CF-DURATION/> zeigt die Override-Dauer in Minuten.
- <CF-IF att1 att2> … </CF-IF> zum Ein- und Ausblenden von Teilen des HTML-Dokuments. Die Attribute sind:
  - CATEGORY wenn der Override-Typ „Kategorie“ ist und der Override erfolgreich war
  - DOMAIN wenn der Override-Typ „Domain“ ist und der Override erfolgreich war
  - BOTH wenn der Override-Typ „Kategorie und Domain“ ist und der Override erfolgreich war
  - ERROR falls der Override fehlgeschlagen ist
  - OK falls entweder CATEGORY oder DOMAIN oder BOTH zutreffend sind

  Werden in einem Tag mehrere Attribute angegeben, dann sollte der Bereich eingeblendet werden, wenn mind. eine dieser Bedingungen erfüllt ist. Alle Tags und Attribute lassen sich mit den jeweils ersten zwei Buchstaben abkürzen (z. B. CF-CA oder CF-IF BL). Das ist notwendig, weil der Text nur maximal 254 Zeichen lang sein darf.

  - Beispiel:

    <CF-IF CA BO>Die Kategorien <CF-CAT/> sind</CF-IF><CF-IF BO> in der Domain <CF-DO/></CF-IF><CF-IF DO>Die Domain <CF-DO/> ist</CF-IF><CF-IF OK> für <CF-DU/> Minuten freigeschaltet.
<CF-LI/></CF-IF><CF-IF ERR>Override-Fehler:
<CF-ERR/></CF-IF>

20.11.8 Profile des LANCOM Content Filters

Unter **Content-Filer** > **Profile** können Sie Content-Filter-Profile erstellen, die zur Überprüfung von Webseiten auf nicht zugelassene Inhalte genutzt werden. Ein Content-Filter-Profil hat immer einen Namen und ordnet verschiedenen Zeitabschnitten das jeweils gewünschte Kategorieprofil sowie optional eine Black- und eine Whitelist zu.

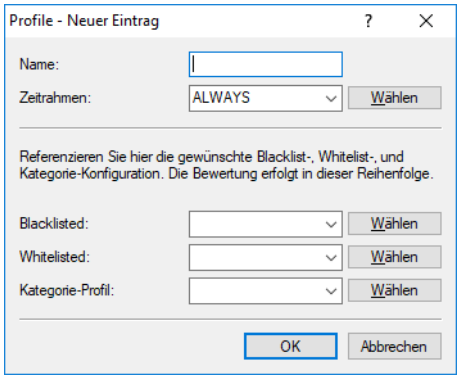
Um verschiedene Zeiträume unterschiedlich zu definieren, werden mehrere Content-Filter-Profileinträge mit dem gleichen Namen angelegt. Das Content-Filter-Profil besteht dann aus der Summe aller Einträge mit dem gleichen Namen.

Das Content-Filter-Profil wird über die Firewall angesprochen.

Bitte beachten Sie, dass Sie zur Nutzung der Profile im LANCOM Content Filter entsprechende Einstellungen in der Firewall vornehmen müssen.

20.11.8.1 Profile

Die Einstellungen für die Profile finden Sie hier:



LANconfig: **Content-Filer** > **Profile** > **Profile**

Kommandozeile: **Setup** > **UTM** > **Content-Filter** > **Profile** > **Profile**

Name

Hier muss der Name des Profils angegeben werden, über das es in der Firewall referenziert wird.

Zeitrahmen

Wählen Sie den Zeitrahmen für das folgende Kategorieprofil und optional die Blacklist und die Whitelist. Voreingestellt sind die Zeitrahmen ALWAYS und NEVER. Weitere Zeitrahmen können Sie konfigurieren unter:

LANconfig: **Datum/Zeit** > **Allgemein** > **Zeitrahmen**

Kommandozeile: **Setup** > **Zeit** > **Zeitrahmen**

Zu einem Profil kann es auch mehrere Zeilen mit unterschiedlichen Zeitrahmen geben.

Mögliche Werte:

- Always
- Never
- Name eines Zeitrahmenprofils

Wenn sich bei der Verwendung von mehreren Einträgen für ein Content-Filter-Profil die Zeitrahmen überlappen, werden in diesem Zeitraum alle Seiten gesperrt, die durch einen der aktiven Einträge erfasst werden. Bleibt bei der Verwendung von mehreren Einträgen für ein Content-Filter-Profil ein Zeitraum undefiniert, ist in diesem Zeitraum der ungeprüfte Zugriff auf alle Webseiten möglich.

Blacklisted

Name des Blacklist-Profils, das für dieses Content-Filter-Profil während dieser Zeit gelten soll. Es kann ein neuer Name eingegeben oder ein vorhandener aus der Blacklist-Tabelle ausgewählt werden.

Mögliche Werte:

- Name eines Blacklist-Profils
- Neuer Name

Whitelisted

Name des WhiteList-Profils, das für dieses Content-Filter-Profil während dieser Zeit gelten soll. Es kann ein neuer Name eingegeben oder ein vorhandener aus der Whitelist-Tabelle ausgewählt werden.

Mögliche Werte:

- Name eines Whitelist-Profils
- Neuer Name

Kategorie-Profil

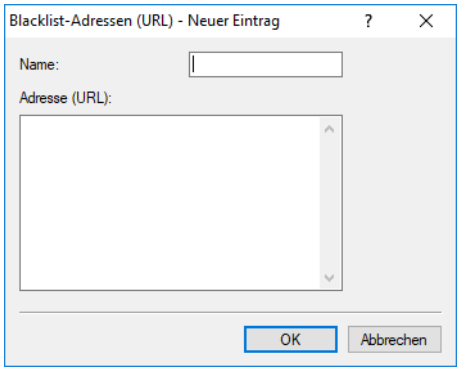
Name des Kategorie-Profils, das für dieses Profil während dieser Zeit gelten soll. Es kann ein neuer Name eingegeben oder ein vorhandener aus der Kategorietabelle ausgewählt werden.

Mögliche Werte:

- Name eines Kategorie-Profils
- Neuer Name

20.11.8.2 Blacklist-Adressen (URL)

Hier können Sie Webseiten konfigurieren, die anschließend verboten werden sollen.



LANconfig: **Content-Filer** > **Profile** > **Blacklist-Adressen (URL)**

Kommandozeile: **Setup** > **UTM** > **Content-Filter** > **Profile** > **Blacklists**

Name

Hier muss der Name der Blacklist angegeben werden, über den sie im Content-Filter-Profil referenziert wird.

Mögliche Werte:

- Name einer Blacklist

Adresse (URL)

Hier werden die URLs eingetragen, die über diese Blacklist verboten werden sollen.

Mögliche Werte:

- gültige URL-Adresse

Es können auch folgende Wildcards zum Einsatz kommen:

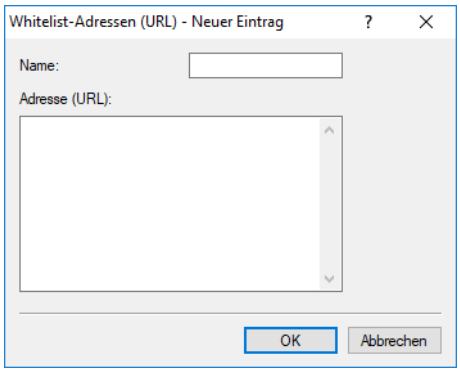
- * für mehrere beliebige Zeichen (z. B. findet www.lancom.* die Webseiten www.lancom.de, www.lancom.com, www.lancom.eu, www.lancom.es etc.)
- ? für ein beliebiges Zeichen (z. B. findet www.lancom.e* die Webseiten www.lancom.eu und www.lancom.es)

Bitte geben Sie die URL **ohne** führendes http:// ein. Beachten Sie, dass bei vielen URLs häufig automatisch ein Schrägstrich am Ende der URL angehängt wird, z. B. „www.mycompany.de/". Daher empfiehlt sich für die Eingabe an dieser Stelle die Form: „www.mycompany.de*".

Einzelne URLs werden mit Leerzeichen getrennt.

20.11.8.3 Whitelist-Adressen (URL)

Hier können Sie Webseiten konfigurieren, die gezielt erlaubt werden sollen.



LANconfig: **Content-Filer** > **Profile** > **Whitelist-Adressen (URL)**

Kommandozeile: **Setup** > **UTM** > **Content-Filter** > **Profile** > **Whitelists**

Name

Hier muss der Name der Whitelist angegeben werden, über den diese im Content-Filter-Profil referenziert wird.

Mögliche Werte:

- Name einer Whitelist

Adresse (URL)

Hier können Sie Webseiten konfigurieren, die lokal geprüft und anschließend akzeptiert werden sollen.

Mögliche Werte:

- gültige URL-Adresse

Es können auch folgende Wildcards zum Einsatz kommen:

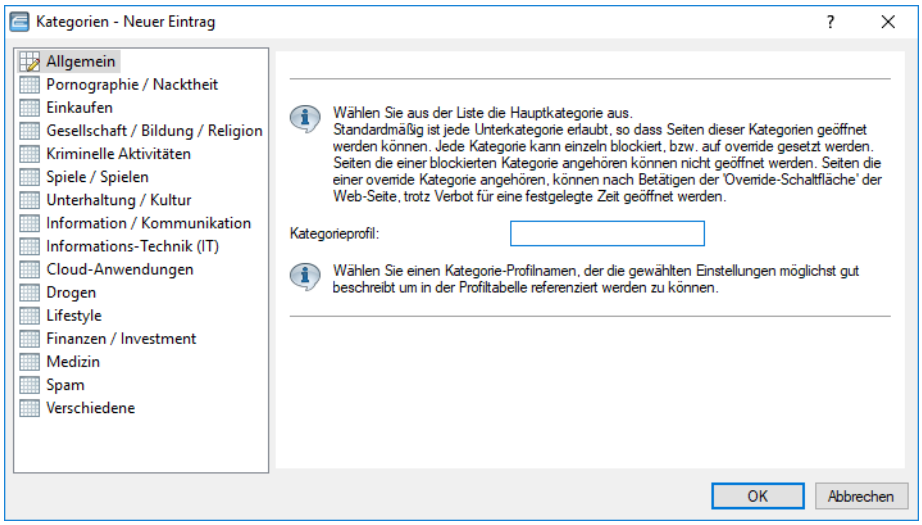
- * für mehrere beliebige Zeichen (z. B. findet www.lancom.* die Webseiten www.lancom.de, www.lancom.com, www.lancom.eu, www.lancom.es etc.)
- ? für ein beliebiges Zeichen (z. B. findet www.lancom.e* die Webseiten www.lancom.eu und www.lancom.es)

Bitte geben Sie die URL **ohne** führendes http:// ein. Beachten Sie, dass bei vielen URLs häufig automatisch ein Schrägstrich am Ende der URL angehängt wird, z. B. „www.mycompany.de/". Daher empfiehlt sich für die Eingabe an dieser Stelle die Form: „www.mycompany.de*".

Einzelne URLs werden mit Leerzeichen getrennt.

20.11.8.4 Kategorien

Hier erstellen Sie ein Kategorieprofil und legen fest, welche Kategorien bzw. Gruppen bei der Bewertung der Webseiten berücksichtigt werden. Für jede Gruppe können Sie die einzelnen Kategorien erlauben, verbieten oder die Override-Funktion aktivieren.



LANconfig: **Content-Filer** > **Profile** > **Kategorien**

Kommandozeile: **Setup** > **UTM** > **Content-Filter** > **Profile** > **Kategorieprofile**

Kategorieprofil

Hier wird der Name der Kategorieprofils angegeben, über den dieses im Content-Filter-Profil referenziert wird.

Mögliche Werte:

- Name eines Kategorieprofils

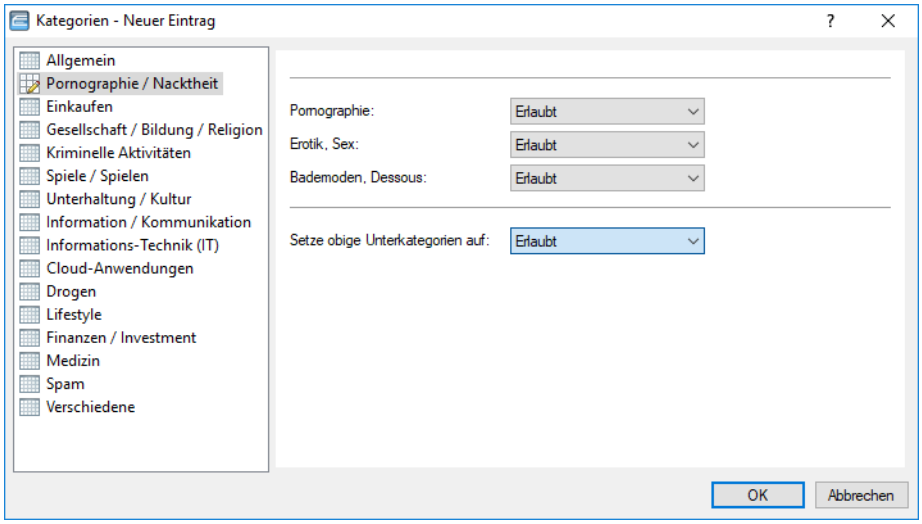
Kategorieeinstellungen

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

Folgende Hauptkategorien können konfiguriert werden:

- Pornographie / Nacktheit
- Einkaufen
- Gesellschaft / Bildung / Religion
- Kriminelle Aktivitäten
- Spiele / Spielen
- Unterhaltung / Kultur
- Information / Kommunikation
- Informations-Technik (IT)
- Cloud-Anwendungen
- Drogen
- Lifestyle
- Finanzen / Investement
- Medizin
- Spam

- Verschiedene



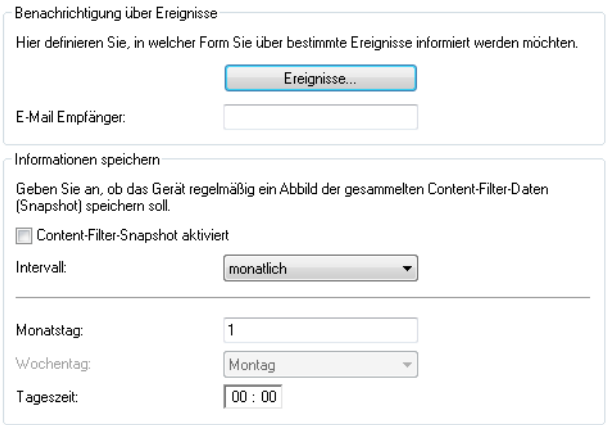
Das Kategorieprofil muss anschließend zusammen mit einem Zeitrahmen einem Content-Filter-Profil zugewiesen werden, um aktiv zu werden.

Mögliche Werte:

- Erlaubt, Verboten, Override

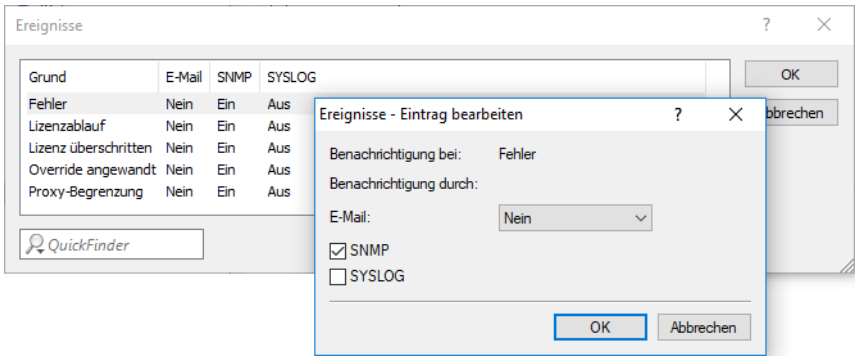
20.11.9 Optionen des LANCOM Content Filters

Unter **Content-Filter** > **Optionen** können Sie einstellen, ob Sie über Ereignisse benachrichtigt werden und wo die Informationen des LANCOM Content Filters gespeichert werden sollen.



Ereignisse

Hier definieren Sie, in welcher Form Sie über bestimmte Ereignisse informiert werden. Die Benachrichtigung kann erfolgen durch E-Mail, SNMP oder SYSLOG. Für verschiedene Ereignisse kann separat definiert werden, ob und in welcher Menge Meldungen ausgegeben werden sollen.



E-Mail

Definieren Sie hier, ob und wie eine E-Mail-Benachrichtigung erfolgt:

- **Nein**

  Für dieses Ereignis erfolgt keine E-Mail-Benachrichtigung.

- **Unverzüglich**

  Die Benachrichtigung erfolgt, sobald das Ereignis eintritt.

- **Täglich**

  Die Benachrichtigung erfolgt einmal am Tag.

Die folgenden Ereignisse stehen für Benachrichtigungen zur Verfügung:

Fehler

Bei SYSLOG: Quelle „System", Priorität „Alarm".

Default: Benachrichtigung SNMP

Lizenzablauf

Bei SYSLOG: Quelle „Verwaltung", Priorität „Alarm".

Default: Benachrichtigung SNMP

Lizenz überschritten

Bei SYSLOG: Quelle „Verwaltung", Priorität „Alarm".

Default: Benachrichtigung SNMP

Override angewandt

Bei SYSLOG: Quelle „Router", Priorität „Alarm".

Default: Benachrichtigung SNMP

Proxy-Begrenzung

Bei SYSLOG: Quelle „Router", Priorität „Info".

Default: Benachrichtigung SNMP

E-Mail Empfänger

Um die E-Mail-Benachrichtigungsfunktion zu nutzen, muss ein SMTP-Client entsprechend konfiguriert sein. Sie können den Client in diesem Gerät dazu verwenden oder einen anderen Ihrer Wahl.

Wenn kein E-Mail-Empfänger angegeben wird, dann wird keine E-Mail verschickt.

Content-Filter-Snapshot

Hier können Sie den Content-Filter-Snapshot aktivieren und bestimmen, wann und wie häufig er stattfindet. Der Schnappschuss kopiert die Tabelle der Kategoriestatistik in die Letzter-Schnappschuss-Tabelle, dabei wird der alte Inhalt der Schnappschuss-Tabelle überschrieben. Die Werte der Kategoriestatistik werden dann auf 0 gesetzt.

Intervall

Wählen Sie hier, ob der Schnappschuss monatlich, wöchentlich oder täglich angefertigt werden soll.

Mögliche Werte:

- Monatlich
- Wöchentlich
- Täglich

Monatstag

Ist eine monatliche Ausführung des Schnappschuss gewünscht, wählen Sie hier den Tag, an dem der Schnappschuss angefertigt werden soll. Mögliche Werte:

- 1-31

Wählen Sie als Monatstag sinnvollerweise eine Zahl zwischen 1 und 28, damit der Tag in jedem Monat vorkommt.

Wochentag

Ist eine wöchentliche Ausführung des Schnappschuss gewünscht, selektieren Sie hier den Wochentag, an dem der Schnappschuss angefertigt werden soll. Mögliche Werte:

- Montag, Dienstag, Mittwoch, Donnerstag, Freitag, Samstag, Sonntag

Tageszeit

Ist eine tägliche Ausführung des Schnappschuss gewünscht, tragen Sie hier die Tageszeit in Stunden und Minuten ein. Mögliche Werte:

- Format HH:MM (Default: 00:00)

20.11.10 Zusätzliche Einstellungen für den LANCOM Content Filter

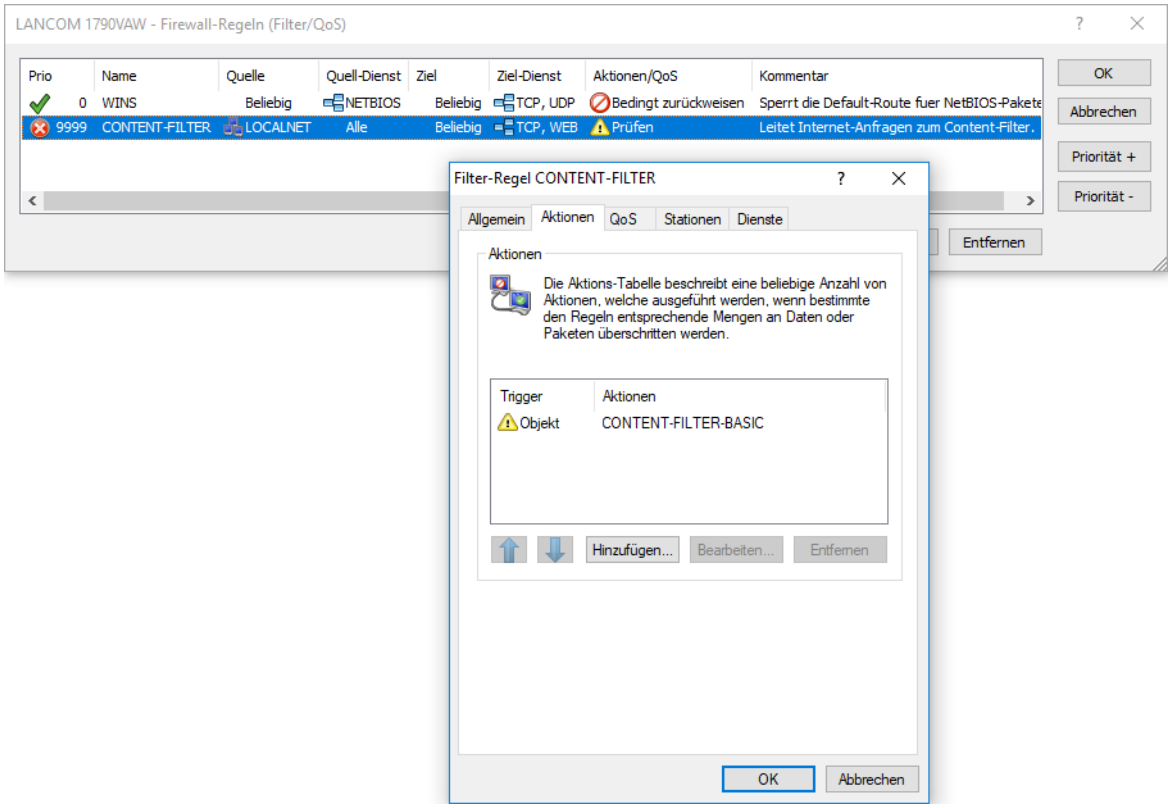
20.11.10.1 Firewall-Einstellungen für den Content Filter

Die Firewall muss aktiviert sein, damit der LANCOM Content Filter arbeiten kann. Sie aktivieren die Firewall unter:

LANconfig: **Firewall/QoS** > **Allgemein**

Kommandozeile: **Setup** > **IP-Router** > **Firewall**

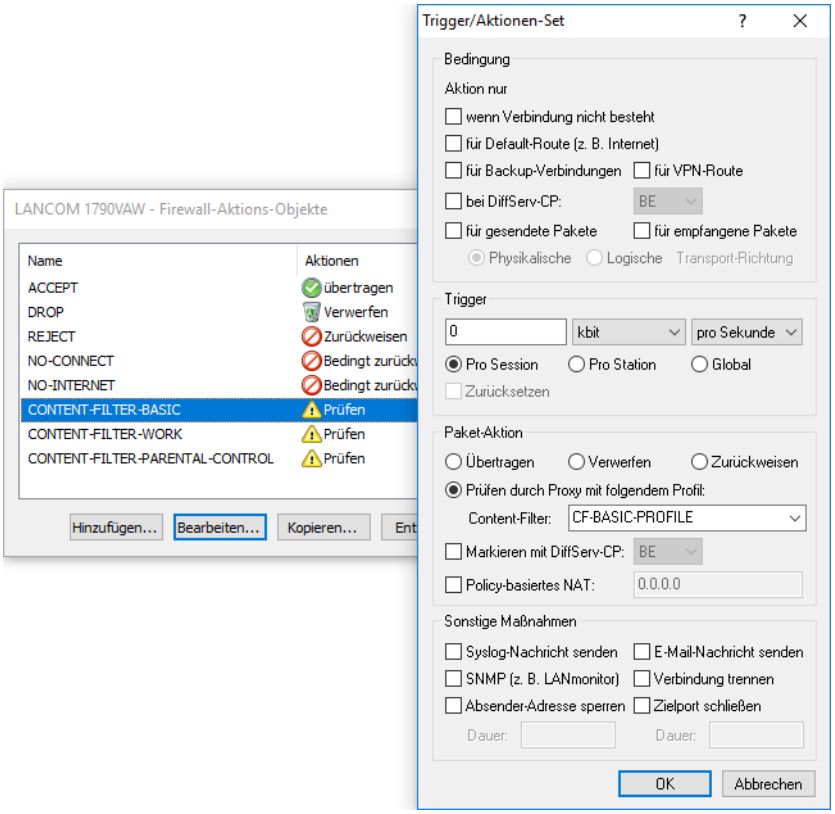
In der Default-Einstellung finden Sie die Firewall-Regel CONTENT-FILTER, die auf das Aktionsobjekt CONTENT-FILTER-BASIC zurückgreift:



Die Firewall-Regel sollte auf die Zieldienste HTTP und HTTPS beschränkt werden, damit nur ausgehende HTTP- und HTTPS-Verbindungen erfasst werden. Ohne diese Einschränkung werden alle Pakete über den Content Filter geprüft, was zu einer Beeinträchtigung der Performance im Gerät führt.

Eine Firewall-Regel für den Content Filter muss ein spezielles Aktionsobjekt verwenden, das über die Paket-Aktionen die Daten mit einem Content-Filter-Profil prüft. In der Default-Einstellung finden Sie die Aktionsobjekte CONTENT-FILTER-BASIC,

CONTENT-FILTER-WORK und CONTENT-FILTER-PARENTAL-CONTROL, die auf jeweils passende Content-Filter-Profile zurückgreifen:



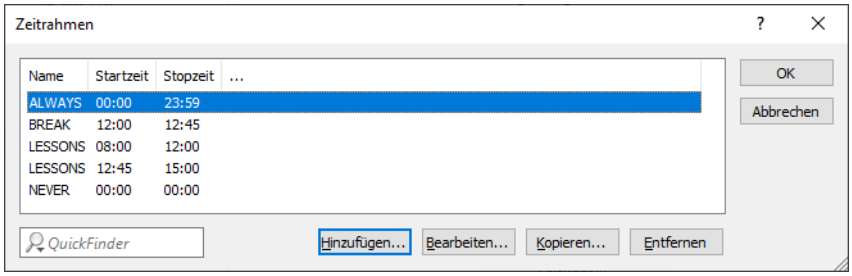
Beispiel: Beim Öffnen einer Webseite durchlaufen die Datenpakete die Firewall und werden von der Regel CONTENT-FILTER erfasst. Das Aktionsobjekt CONTENT-FILTER-BASIC prüft die Datenpakete mit dem Content-Filter-Profil CONTENT-FILTER-BASIC.

20.11.10.2 Zeitrahmen

Zeitrahmen werden beim Content Filter verwendet, um die Gültigkeitsdauer von Content-Filter-Profilen zu definieren. Zu einem Profil kann es auch mehrere Zeilen mit unterschiedlichen Zeitrahmen geben. Dabei sollten sich die Zeitrahmen unterschiedlicher Zeilen ergänzen, d. h. wenn Sie eine ARBEITSZEIT festlegen, wollen Sie wahrscheinlich auch einen Zeitrahmen FREIZEIT festlegen, der die Zeit außerhalb der Arbeitszeit umfasst.

Zeitrahmen können auch verwendet werden, um eine WLAN-SSID nicht dauerhaft auszustrahlen. Dazu kann dieser bei den logischen WLAN-Einstellungen hinzugefügt werden.

Voreingestellt sind die Zeitrahmen ALWAYS und NEVER. Weitere Zeitrahmen können Sie konfigurieren unter:



LANconfig: **Datum/Zeit** > **Allgemein** > **Zeitrahmen**

Kommandozeile: **Setup** > **Zeit** > **Zeitrahmen**

Name

Hier muss der Name des Zeitrahmens angegeben werden, über den dieser im Content-Filter-Profil oder bei einer WLAN-SSID referenziert wird. Mehrere Einträge gleichen Namens ergeben dabei ein gemeinsames Profil.

Mögliche Werte:

- Name eines Zeitrahmens

Startzeit

Hier kann die Startzeit (Tageszeit) angegeben werden, ab der das gewählte Profil gelten soll.

Mögliche Werte:

- Format HH:MM (Default: 00:00)

Stoppzeit

Hier kann die Stoppzeit (Tageszeit) angegeben werden, ab der das gewählte Profil nicht mehr gültig sein soll.

Mögliche Werte:

- Format HH:MM (Default: 23:59)

Eine Stoppzeit von HH:MM geht normalerweise bis HH:MM:00. Eine Ausnahme ist die Stoppzeit 00:00, die als 23:59:59 interpretiert wird.

Wochentage

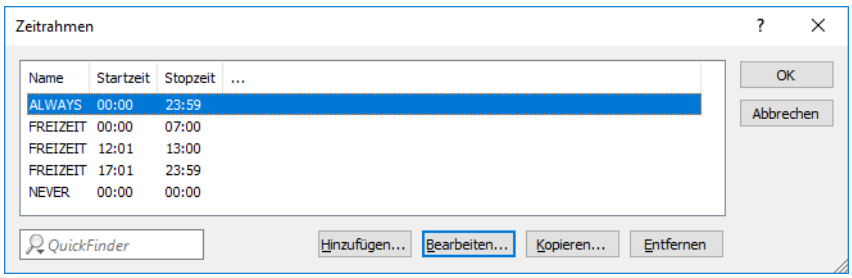
Hier können Sie die Wochentage auswählen, an denen der Zeitrahmen gültig sein soll.

Mögliche Werte:

- Montag, Dienstag, Mittwoch, Donnerstag, Freitag, Samstag, Sonntag, Feiertag

Die Feiertage werden unter **Datum/Zeit** > **Allgemein** > **Feiertage** eingestellt.

Zeitschemata lassen sich mit gleichem Namen, aber unterschiedlichen Zeiten auch über mehrere Zeilen hinweg definieren:



20.12 BPjM-Modul

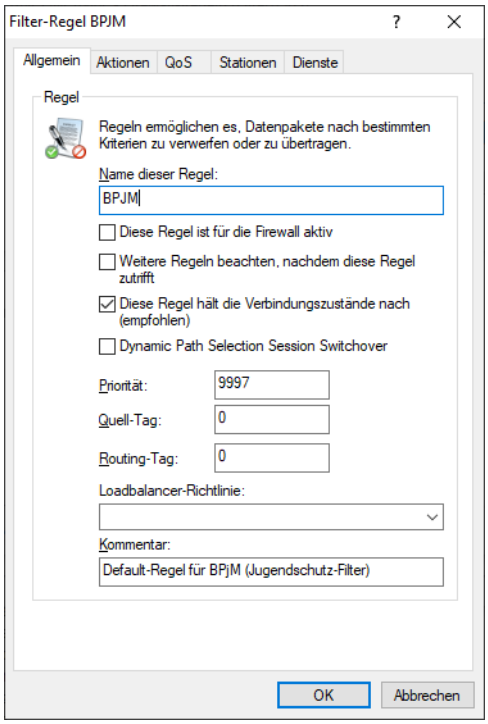
Das BPjM-Modul wird von der Bundeszentrale für Kinder- und Jugendmedienschutz herausgegeben und sperrt Webseiten, die Kindern und Jugendlichen in Deutschland nicht zugänglich gemacht werden dürfen. Diese Funktion ist besonders für Schulen und Bildungseinrichtungen mit minderjährigen Schülern relevant. Damit sind DNS-Domains, deren Inhalte offiziell als jugendgefährdend eingestuft werden, für die entsprechende Zielgruppe in Deutschland nicht erreichbar. Eine automatische und regelmäßige Aktualisierung und Erweiterung dieser Auflistung ist dabei gewährleistet. Das BPJM-Modul

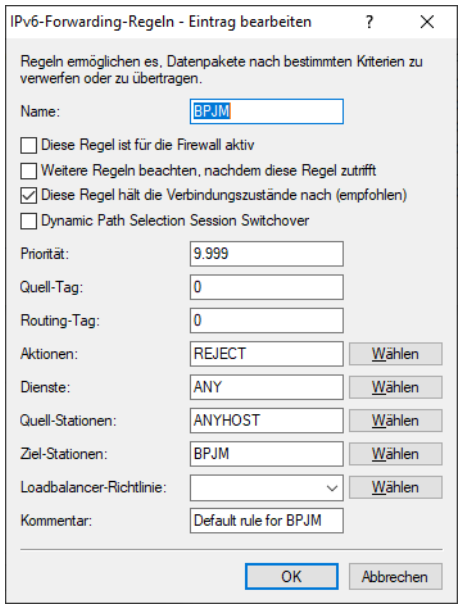
sperrt DNS-Domains die auf der offiziellen Webseiten-Liste der Bundesprüfstelle für jugendgefährdende Medien (BPjM) stehen. Eine Sperrung nach Kategorie oder Override (Erlauben) ist hierbei nicht möglich.

Das BPJM-Modul ist Teil der LANCOM Content Filter Option oder separat über die Software-Option LANCOM BPjM Filter Option erhältlich.

In der IPv4- bzw. IPv6-Firewall existiert dazu eine Default-Firewall-Regel, die aktiviert werden kann und pro Netz konfiguriert werden kann. So ist beispielsweise möglich, nur das Schülernetz mit diesem Filter auszustatten, andere Netze aber davon auszunehmen.

In der IPv6-Firewall existiert eine neue Default-Regel BPJM, die standardmäßig deaktiviert ist mit dem System-Objekt „BPJM" als Zielstation. In der IPv4-Firewall existiert dazu analog eine Regel. Definieren Sie als Quell-Stationen die Netzwerke, die durch das BPjM-Modul geschützt werden sollen.





Weitere Einstellungen finden Sie in LANconfig unter **Sonstige Dienste** > **Dienste** > **BPjM-Filter**.



Absende-Adresse

Absende-Adresse, die vom BPjM-Modul verwendet wird, um den Server für BPjM-Signatur-Updates zu erreichen.

20.12.1 Einsatzempfehlungen

Sollen Content-Filter und BPJM-Filter gemeinsam verwendet werden, müssen beide Regeln mit unterschiedlichen Prioritäten konfiguriert werden, so dass diese nacheinander durchlaufen werden.

Ebenso muss bei der ersten Regel darauf geachtet werden, dass der Punkt „Weitere Regeln beachten, nachdem diese Regel zutrifft" aktiviert ist.

In seltenen Fällen kann es dazu kommen, dass das BPJM-Modul gewünschte Domains blockiert, da nur (DNS-)Domains und keine URL-Verzeichnisebenen aufgrund von TLS geprüft werden können. In diesem Fall können diese gewünschten Domains in der „BPJM-Allow-Liste" hinzugefügt werden, z. B. *.example.com.

Der LANCOM Router muss als DNS-Server bzw. DNS-Forwarder im Netz dienen, d. h. Clients im lokalen Netzwerk müssen den Router als DNS-Server verwenden. Zusätzlich muss die direkte Nutzung von DNS-over-TLS und DNS-over-HTTPS (ggf. browserintern) mit externen DNS-Servern durch Clients verhindert werden.

Dies kann wie folgt erreicht werden:

- Der DHCP-Server muss die IP-Adresse des Routers als DNS-Server verteilen (wird standardmäßig vom Internet-Wizard eingerichtet)
- Einrichtung von Firewall-Regeln, die die direkte Nutzung von externen DNS-Servern verhindern, z. B. durch Sperrung des ausgehenden Ports 53 (UDP) für Clients aus dem entsprechenden Quellnetzwerk
- Einrichtung von Firewall-Regeln, die die direkte Nutzung von externen DNS-Servern mit Unterstützung von DNS-over-TLS verhindern, z. B. durch Sperrung des ausgehenden Ports 853 (TCP) für Clients aus dem entsprechenden Quellnetzwerk
- DNS-over-HTTPS (DoH) im Browser deaktivieren

Hinweise zur Synchronisierung der DNS-Datenbank der Firewall:

Da die Firewall ihre Informationen aus den DNS-Anfragen der Clients lernt, kann es in bestimmten Situationen dazu kommen, dass die DNS-Datenbank noch nicht vollständig ist. Dies kann in folgenden Situationen passieren:

- Es wird eine neue Firewall-Regel hinzugefügt, der Client hat aber noch einen DNS-Eintrag zwischengespeichert
- Kurz nach Neustart des Routers und der Client hat aber noch einen DNS-Eintrag zwischengespeichert

In diesen Fällen hilft ein Leeren des DNS-Cache auf dem Client, ein Reboot des Clients oder ein Timeout des DNS-Eintrags auf dem Client.

Wenn unterschiedliche DNS-Namen auf dieselbe IP-Adresse aufgelöst werden, dann können diese nicht unterschieden werden. In diesem Fall trifft immer die erste Regel zu, die einen dieser DNS-Namen referenziert. Das sollte bei großen Dienstanbietern kein Problem sein. Bei kleinen Webseiten, die vom selben Anbieter gehostet werden, könnte es jedoch auftreten.

20.12.2 Menüaktion zum Löschen der BPjM-Signaturdefinition

Über die CLI können Sie die BPjM-Signaturdefinition im Dateisystem des Routers löschen. Führen Sie dazu das Kommando `do /Status/Firewall/BPJM/Werte-loeschen` aus.

20.13 TACACS+

20.13.1 Einleitung

TACACS+ (Terminal Access Control Access Control Server) ist ein Protokoll für Authentifizierung, Autorisierung und Accounting (AAA), es stellt also den Zugang zu Netzwerkkomponenten nur für bestimmte Nutzer sicher, regelt die Berechtigungen der Benutzer und überträgt Daten für die Protokollierung der Netzwerknutzung. TACACS+ ist also eine Alternative zu anderen AAA-Protokollen wie RADIUS.

Der Einsatz von TACACS+ ist eine Voraussetzung für die Einhaltung der PCI-Compliance (Payment Card Industry).

Die Regelung der Zugriffsmöglichkeiten für die Anwender stellt in modernen Netzwerken mit zahlreichen Diensten und Netzwerkkomponenten eine große Herausforderung dar. Gerade in größeren Szenarien ist es kaum noch möglich, die Zugangsdaten der Benutzer auf jedem Gerät bzw. in jedem Dienst einzutragen und auf Dauer konsistent zu halten. Aus diesem Grund bietet sich die zentrale Bereitstellung der Benutzerdaten auf einem entsprechenden Server an.

In einem einfachen Anwendungsbeispiel möchte sich ein Anwender auf einem Router anmelden und übermittelt dazu seine Zugangsdaten (User-ID) an den Router. Der Router fungiert in diesem Fall als Network Access Server (NAS): er

überprüft die Zugangsdaten nicht selbst, sondern leitet diese an den zentralen AAA-Server weiter, der die Daten nach der Prüfung mit einer positiven Bestätigung (Accept) oder einer Ablehnung (Reject) beantwortet.



Zu den erweiterten Funktionen von TACACS+ gehört u. a. die Möglichkeit, den Benutzer zum Wechseln des Kennworts aufzufordern (z. B. beim ersten Login oder nach Ablauf einer bestimmten Frist). Die entsprechenden Meldungen werden vom NAS an den Benutzer weitergereicht.

Bitte beachten Sie, dass LANconfig nicht alle Meldungen des erweiterten Login-Dialogs auswerten kann. Falls LANconfig die Anmeldung an einem Gerät trotz korrekter Eingabe der Benutzerdaten ablehnt, melden Sie sich bitte über einen alternativen Konfigurationsweg an (WEBconfig oder Telnet).

Neben den weit verbreiteten RADIUS-Servern bietet sich als AAA-Server auch TACACS+ an. Die Tabelle zeigt einige wesentliche Unterschiede zwischen RADIUS und TACACS+:

TACACS+	RADIUS
Verbindungsorientierte Datenübertragung über TCP	Verbindungslose Datenübertragung über UDP
Gesamte Datenübertragung wird verschlüsselt	Nur Kennwort wird verschlüsselt, Inhalte bleiben unverschlüsselt
Vollständige Trennung von Authentifizierung, Autorisierung und Accounting möglich	Authentifizierung und Autorisierung sind kombiniert

- Die Übertragung über TCP macht TACACS+ zuverlässiger als RADIUS, da die Kommunikation zwischen NAS und AAA-Server bestätigt wird und der NAS somit informiert wird, wenn der AAA-Server nicht erreichbar ist.
- TACACS+ verschlüsselt neben dem Kennwort die gesamten Nutzdaten (bis auf den TACACS+-Header). Dadurch können auch Informationen wie der Benutzername oder die erlaubten Dienste nicht abgehört werden. TACACS+ benutzt zur Verschlüsselung ein One-Time-Pad, welches auf MD5-Hashes basiert.
- Die Trennung der drei AAA-Funktionen erlaubt unter TACACS+ schließlich die Nutzung anderer Server. Während bei RADIUS Authentifizierung und Autorisierung immer zusammen gehören, kann TACACS+ Authentifizierung und Autorisierung getrennt verwenden. So kann z. B. der TACACS+-Server nur für die Authentifizierung eingesetzt werden, dabei müssen auch nur die Benutzer, nicht aber die erlaubten Kommandos gepflegt werden.

Bitte beachten Sie: Auch wenn TACACS+ gezielt dazu genutzt wird, die Benutzerkonten nicht auf den einzelnen Geräten, sondern zentral auf einem AAA-Server abzulegen, sollten Sie auf jeden Fall für die Geräte ein sicheres Kennwort für den Root-Zugang definieren. Wenn kein Root-Kennwort gesetzt ist, kann der Konfigurationszugang zu den Geräten aus Sicherheitsgründen gesperrt werden, wenn die Verbindung zu den TACACS+-Servern nicht verfügbar ist! In diesem Fall muss das Gerät möglicherweise in den Auslieferungszustand zurückgesetzt werden, um wieder Zugang zur Konfiguration zu erhalten.

20.13.2 Konfiguration der TACACS+-Parameter

Die Parameter für die Konfiguration von TACACS+ finden Sie :

Kommandozeile: **Setup** > **TACACS+**

Accounting

Aktiviert das Accounting über einen TACACS+-Server. Wenn das TACACS+-Accounting aktiviert ist, werden alle Accounting-Daten über das TACACS+-Protokoll an den konfigurierten TACACS+-Server übertragen.

Mögliche Werte:

- aktiviert, deaktiviert

Default

› deaktiviert

Das TACACS+-Accounting wird nur dann aktiviert, wenn ein erreichbarer TACACS+-Server definiert ist.

Authentifizierung

Mit der Einführung der Authentifizierung über RADIUS ist dieser Menüpunkt entfallen. Die Authentifizierung über TACACS+ wird nun unter **Setup** > **Config** > **Authentifizierung** aktiviert. Wenn die TACACS+-Authentifizierung aktiviert ist, werden alle Authentifizierung-Anfragen über das TACACS+-Protokoll an den konfigurierten TACACS+-Server übertragen.

Die TACACS+-Authentifizierung wird nur dann aktiviert, wenn ein erreichbarer TACACS+-Server definiert ist. Der Rückgriff auf lokale Benutzer kann dabei nur genutzt werden, wenn für das Gerät ein Root-Kennwort gesetzt ist. Bei Geräten ohne Root-Kennwort muss der Rückgriff auf lokale Benutzer deaktiviert werden, da sonst bei Ausfall der Netzwerkverbindung (TACACS+-Server nicht erreichbar) ein Zugriff ohne Kennwort auf das Gerät möglich wäre.

Autorisierung

Aktiviert die Autorisierung über einen TACACS+-Server. Wenn die TACACS+-Autorisierung aktiviert ist, werden alle Autorisierungs-Anfragen über das TACACS+-Protokoll an den konfigurierten TACACS+-Server übertragen.

Mögliche Werte:

› aktiviert, deaktiviert

Default

› deaktiviert

Die TACACS+-Autorisierung wird nur dann aktiviert, wenn ein erreichbarer TACACS+-Server definiert ist. Wenn die TACACS+-Autorisierung aktiviert ist, wird für jedes Kommando beim TACACS+-Server eine Anfrage gestellt, ob der Benutzer diese Aktion ausführen darf. Dementsprechend erhöht sich der Datenverkehr bei der Konfiguration, außerdem müssen die Rechte für die Benutzer im TACACS+-Server definiert sein.

Rückgriff_auf_lokale_Benutzer

Für den Fall, dass die definierten TACACS+-Server nicht erreichbar sind, kann ein Rückgriff auf die lokalen Benutzerkonten im Gerät erlaubt werden. So ist der Zugriff auf die Geräte auch bei Ausfall der TACACS+-Verbindung möglich, z. B. um die TACACS+-Nutzung zu deaktivieren oder die Konfiguration zu korrigieren.

Mögliche Werte:

› erlaubt, verboten

Default

› erlaubt

Der Rückgriff auf lokale Benutzerkonten stellt ein Sicherheitsrisiko dar, wenn kein Root-Kennwort im Gerät gesetzt ist. Daher kann die TACACS+-Authentifizierung mit Rückgriff auf lokale Benutzerkonten nur aktiviert werden, wenn ein Root-Kennwort definiert ist. Wenn kein Root-Kennwort gesetzt ist, kann der Konfigurationszugang zu den Geräten aus Sicherheitsgründen gesperrt werden, wenn die Verbindung zu den TACACS+-Servern nicht verfügbar ist! In diesem Fall muss das Gerät möglicherweise in den Auslieferungszustand zurückgesetzt werden, um wieder Zugang zur Konfiguration zu erhalten.

Shared-Secret

Das Kennwort für die Verschlüsselung der Kommunikation zwischen NAS und TACACS+-Server.

Mögliche Werte:

- 31 alphanumerische Zeichen

Default

- Leer

Das Kennwort muss im Gerät und im TACACS+-Server übereinstimmend eingetragen werden. Eine Nutzung von TACACS+ ohne Verschlüsselung ist nicht zu empfehlen.

SNMP-GET-Anfragen-Accounting

Zahlreiche Netzwerkmanagementtools nutzen SNMP, um Informationen aus den Netzwerkgeräten abzufragen. Auch der LANmonitor greift über SNMP auf die Geräte zu, um Informationen über aktuelle Verbindungen etc. darzustellen oder Aktionen wie das Trennen einer Verbindung auszuführen. Da über SNMP ein Gerät auch konfiguriert werden kann, wertet TACACS+ diese Zugriffe als Vorgänge, die eine Autorisierung voraussetzen. Da LANmonitor diese Werte regelmäßig abfragt, würde so eine große Zahl von eigentlich unnötigen TACACS+-Verbindungen aufgebaut. Wenn Authentifizierung, Autorisierung und Accounting für TACACS+ aktiviert sind, werden für jede Anfrage drei Sitzungen auf dem TACACS+-Server gestartet.

Mit diesem Parameter kann das Verhalten der Geräte bei SNMP-Zugriffen geregelt werden, um TACACS+-Sitzungen für das Accounting zu reduzieren. Eine Authentifizierung über den TACACS+-Server bleibt dennoch erforderlich, sofern die Authentifizierung für TACACS+ generell aktiviert ist.

Mit dem Eintrag einer Read-Only-Community unter **Setup** > **SNMP** kann auch die Authentifizierung über TACACS+ für den LANmonitor deaktiviert werden. Die dort definierte Read-Only-Community wird dazu im LANmonitor als Benutzername eingetragen.

Mögliche Werte:

- nur_für_SETUP_Baum: In dieser Einstellung ist nur bei SNMP-Zugriff auf den Setup-Zweig von LCOS ein Accounting über den TACACS+-Server erforderlich.
- alle: In dieser Einstellung wird für alle SNMP-Zugriffe ein Accounting über den TACACS+-Server durchgeführt. Werden z. B. Status-Informationen regelmäßig abgefragt, erhöht diese Einstellung deutlich die Last auf dem TACACS+-Server.
- keine: In dieser Einstellung ist für die SNMP-Zugriffe kein Accounting über den TACACS+-Server erforderlich.

Default:

- nur_für_SETUP_Baum

SNMP-GET-Anfragen-Autorisierung

Mit diesem Parameter kann das Verhalten der Geräte bei SNMP-Zugriffen geregelt werden, um TACACS+-Sitzungen für die Autorisierung zu reduzieren. Eine Authentifizierung über den TACACS+-Server bleibt dennoch erforderlich, sofern die Authentifizierung für TACACS+ generell aktiviert ist.

Mögliche Werte:

- nur_für_SETUP_Baum: In dieser Einstellung ist nur bei SNMP-Zugriff auf den Setup-Zweig von LCOS eine Autorisierung über den TACACS+-Server erforderlich.
- alle: In dieser Einstellung wird für alle SNMP-Zugriffe eine Autorisierung über den TACACS+-Server durchgeführt. Werden z. B. Status-Informationen regelmäßig abgefragt, erhöht diese Einstellung deutlich die Last auf dem TACACS+-Server.
- keine: In dieser Einstellung ist für die SNMP-Zugriffe keine Autorisierung über den TACACS+-Server erforderlich.

Default:

› nur_für_SETUP_Baum

Verschlüsselung

Aktiviert oder deaktiviert die Verschlüsselung der Kommunikation zwischen NAS und TACACS+-Server.

Mögliche Werte:

› aktiviert, deaktiviert

Default

› aktiviert

Eine Nutzung von TACACS+ ohne Verschlüsselung ist nicht zu empfehlen. Wenn die Verschlüsselung hier aktiviert wird, muss außerdem das Kennwort für die Verschlüsselung passend zum Kennwort auf dem TACACS+-Server eingetragen werden.

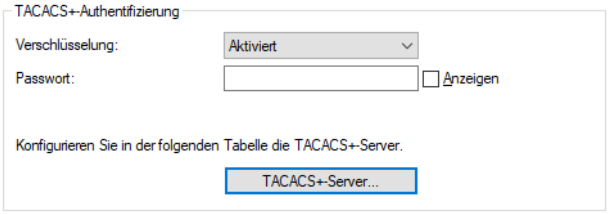
20.13.3 Konfiguration der TACACS+-Server

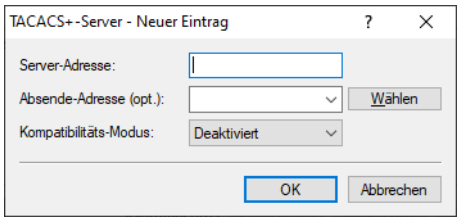
Zur Nutzung der TACACS+-Funktionen können zwei Server definiert werden. Dabei dient ein Server als Backup, falls der andere Server ausfällt. Beim Login über Telnet oder WEBconfig kann der Anwender den zu benutzenden Server auswählen.

Die Parameter für die Konfiguration der TACACS+-Server finden Sie unter:

LANconfig: **Management** > **Authentifizierung** > **TACACS+-Authentifizierung** > **TACACS+-Server**

Kommandozeile: **Setup** > **TACACS+** > **Server**





Server-Adresse

Adresse des TACACS+-Server, an den die Anfragen für Authentifizierung, Autorisierung und Accounting weitergeleitet werden sollen.

Mögliche Werte:

› Gültiger DNS-auflösbarer Name oder gültige IPv4- oder IPv6-Adresse.

Default

› Leer

Absende-Adresse (opt.)

Hier können Sie optional eine Loopback-Adresse konfigurieren.

Mögliche Werte:

- Name der IP-Netzwerke, deren Adresse eingesetzt werden soll
- „INT“ für die Adresse des ersten Intranets
- „DMZ“ für die Adresse der ersten DMZ
- LB0 bis LBF für die 16 Loopback-Adressen
- Beliebige gültige IP-Adresse

Default

- Leer

Kompatibilitäts-Modus

TACACS+-Server werden in einer freien und in einer kommerziellen Version angeboten, die jeweils unterschiedliche Nachrichten verwenden. Der Kompatibilitätsmodus ermöglicht die Verarbeitung der Nachrichten von den freien TACACS+-Servern.

Mögliche Werte:

- Aktiviert, Deaktiviert

Default

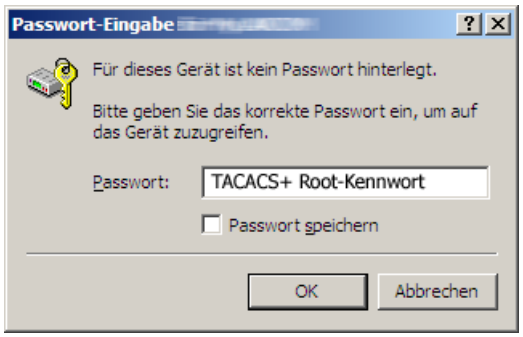
- Deaktiviert

20.13.4 Anmelden am TACACS+-Server

Sobald die Verwendung von TACACS+ für die Authentifizierung und ggf. Autorisierung aktiviert ist, werden alle Logins auf dem Gerät an den TACACS+-Server weitergeleitet. Der weitere Ablauf des Logins unterscheidet sich je nach Zugangsart.

20.13.4.1 TACACS+-Anmeldung über LANconfig

Die Anmeldung über LANconfig an einem Gerät mit aktivierter TACACS+-Authentifizierung gelingt ausschließlich über den Benutzer mit dem Namen root. Der Benutzer root muss entsprechend im TACACS+-Server konfiguriert sein. Geben Sie beim Login über LANconfig das Kennwort ein, dass im TACACS+-Server für den Benutzer root konfiguriert ist.



Der Benutzer root ist der einzige Benutzer, der nach Authentifizierung über TACACS+ automatisch über die vollen Rechte eines Supervisors verfügt und somit die Konfiguration ohne Wechsel des Rechteniveaus bearbeiten darf. Wenn die Autorisierung benutzt wird entscheidet dies der TACACS+-Server.

Wenn für das Gerät neben der Authentifizierung auch die Autorisierung aktiviert ist, müssen im TACACS+-Server für den Benutzer root die Befehle “readconfig” und “writeconfig” erlaubt werden, damit der Benutzer die Konfiguration aus dem Gerät auslesen und nach Änderung wieder einspielen kann (*Rechtezuweisung unter TACACS+* auf Seite 1718).

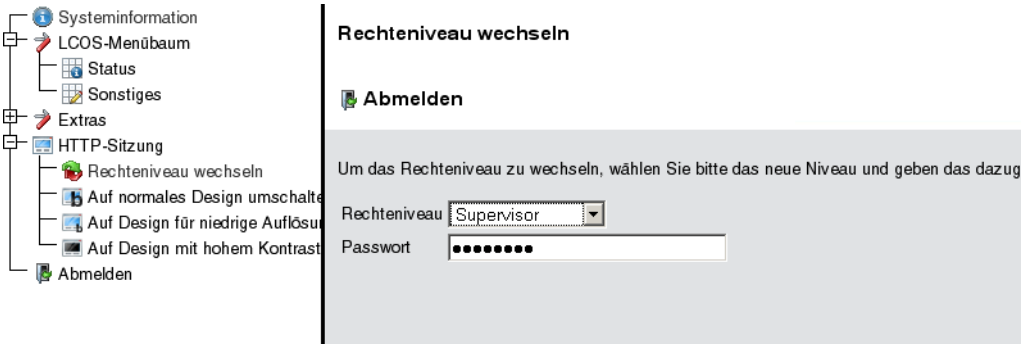
20.13.4.2 TACACS+-Anmeldung über WEBconfig

Die Anmeldung über WEBconfig an einem Gerät mit aktivierter TACACS+-Authentifizierung gelingt allen Benutzern, die im TACACS+-Server konfiguriert sind. Geben Sie beim Login über WEBconfig den Benutzernamen ein, der im TACACS+-Server konfiguriert ist, und wählen Sie den Server aus, an dem die Authentifizierung vorgenommen werden soll.



Das zugehörige Kennwort wird im nächsten Dialog abgefragt. Nach dem Login sieht der Benutzer zunächst nur eine eingeschränkte WEBconfig-Oberfläche. Wenn die Autorisierung nicht genutzt wird, haben alle Benutzer (außer der Benutzer root) unter WEBconfig zunächst nur Leserechte.

Um weitere Rechte zu erhalten, klicken Sie im linken Bildschirmbereich den Link **Rechteniveau wechseln**.



In diesem Dialog wählen Sie gewünschten Benutzerrechte und geben das passende Kennwort ein.

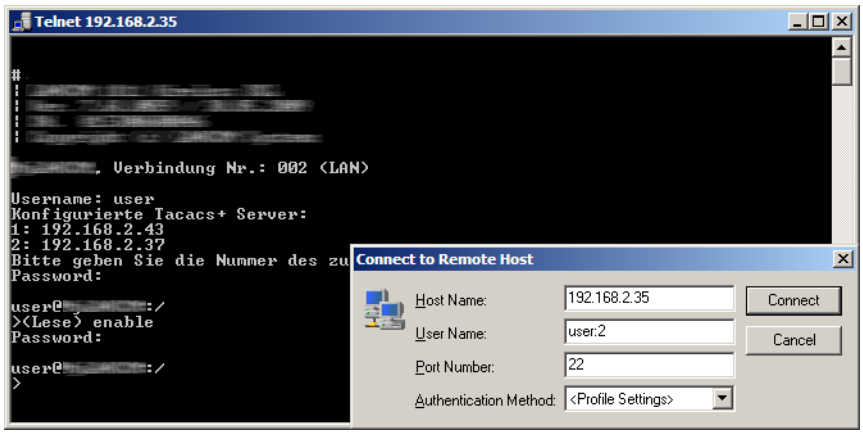
Die Kennwörter für die einzelnen Benutzerrechte werden dazu im TACACS+-Server als “enable”-Kennwörter konfiguriert.

Wenn für das Gerät neben der Authentifizierung auch die Autorisierung aktiviert ist, müssen im TACACS+-Server für die jeweiligen Benutzer die gewünschten Befehle erlaubt werden, damit der Benutzer die Konfiguration aus dem Gerät einsehen und bearbeiten kann (*Rechtezuweisung unter TACACS+* auf Seite 1718).

20.13.4.3 TACACS+-Anmeldung über Telnet oder SSH

Die Anmeldung über Telnet oder SSH an einem Gerät mit aktivierter TACACS+-Authentifizierung gelingt allen Benutzern, die im TACACS+-Server konfiguriert sind.

Geben Sie beim Login über Telnet den Benutzernamen ein, der im TACACS+-Server konfiguriert ist, und wählen Sie den Server aus, an dem die Authentifizierung vorgenommen werden soll. Beim Login über SSH geben Sie den gewünschten Server mit einem Doppelpunkt getrennt nach dem Benutzernamen ein, also entweder „user:1“ oder „user:2“.



Nach dem Login haben alle Benutzer (außer dem Benutzer root) zunächst nur Leserechte.

Um weitere Rechte zu erhalten, geben Sie den Befehl `enable` ein und geben das Kennwort ein. Die Rechte werden dann entsprechend dem konfigurierten Kennwort zugewiesen. Das enable-Kommando nimmt als Parameter die Zahlen 1-15. 1 ist das niedrigste, 15 das höchste Niveau. Ohne Parameter wird automatisch 15 angenommen.

Die Kennwörter für die einzelnen Benutzerrechte werden dazu im TACACS+-Server als „enable“-Kennwörter konfiguriert.

Wenn für das Gerät neben der Authentifizierung auch die Autorisierung aktiviert ist, müssen im TACACS+-Server für die jeweiligen Benutzer die gewünschten Befehle erlaubt werden, damit der Benutzer die Konfiguration aus dem Gerät einsehen und bearbeiten kann (*Rechtezuweisung unter TACACS+* auf Seite 1718).

20.13.5 Rechtezuweisung unter TACACS+

Die Rechte unter TACACS+ werden in bestimmten Leveln angegeben. Zur lokalen Authorisierung der Benutzer über das “enable”-Kommando unter Telnet/SSH bzw. das Rechteniveau unter WEBconfig werden die verschiedenen Admistratorenrechte von LCOS auf die TACACS+-Level abgebildet:

TACACS+-Level	LCOS-Administratorenrechte
0	No rights
1	Read-Only
3	Read-Write
5	Read-Only-Limited Admin
7	Read-Write-Limited Admin
9	Read-Only Admin
11	Read-Write Admin
15	Supervisor (Root)

20.13.6 Autorisierung von Funktionen

Wenn für das Gerät neben der Authentifizierung auch die Autorisierung aktiviert ist, müssen für die Konfiguration die entsprechenden Funktionen für den Benutzer im TACACS+-Server erlaubt sein. Tragen Sie die benötigten Werte in die Benutzerkonfiguration des TACACS+-Servers ein.

20.13.6.1 LANconfig

Befehl	Argumente	Bemerkung
readconfig	keine	Komplette Konfiguration auslesen
writeconfig	keine	Komplette Konfiguration schreiben

20.13.6.2 WEBconfig

Befehl	Argumente	Bemerkung
delRow	SNMP-ID der Tabelle	Zeile löschen
addRow	SNMP-ID der Tabelle	Zeile hinzufügen
editRow	SNMP-ID der Tabelle	Zeile bearbeiten
modifyItem	SNMP-ID des Menüeintrags	Bearbeiten eines Menüeintrags
viewTable	SNMP-ID der Tabelle	Tabelle anzeigen
viewRow	SNMP-ID der Zeile	Zeile anzeigen
setValue	SNMP-ID des Menüeintrags	Wert eines Menüeintrags setzen
listmenu	SNMP-ID des Menüs	Untermenü anzeigen
action	SNMP-ID der Aktion	Ausführen einer Aktion
reboot	keine	Gerät neu starten
$URL	keine	Anzeige eines bestimmten URL

Für den Zugriff über WEBconfig müssen alle URLs freigeschaltet werden, die während der Konfiguration an den TACACS+-Server übertragen werden. Mit der URL "config2" erlauben Sie z. B. grundsätzlich den Zugriff auf den Konfigurationszweig von LCOS über WEBconfig. Zusätzlich müssen die einzelnen Parameter freigeschaltet werden, die der Benutzer bearbeiten darf. Welche URLs WEBconfig an den TACACS+-Server übermittelt, können Sie z. B. mit dem entsprechenden Trace "trace+ tacacs" einsehen.

20.13.6.3 Telnet / SSH

Befehl	Argumente	Bemerkung
dir	SNMP-ID des Verzeichnisses	Inhalt eines Verzeichnisses anzeigen
list	SNMP-ID des Verzeichnisses	Inhalt eines Verzeichnisses anzeigen
ls	SNMP-ID des Verzeichnisses	Inhalt eines Verzeichnisses anzeigen
llong	SNMP-ID des Verzeichnisses	Inhalt eines Verzeichnisses anzeigen
del	SNMP-ID der Tabelle	Zeile löschen
delete	SNMP-ID der Tabelle	Zeile löschen
rm	SNMP-ID der Tabelle	Zeile löschen
cd	SNMP-ID des Zielverzeichnisses	Verzeichnis wechseln
add	SNMP-ID der Tabelle	Zeile hinzufügen
tab	SNMP-ID der Tabelle	Ändert die Reihenfolge der Spalten für das Hinzufügen von Werten
do	SNMP-ID der Aktion	Aktion ausführen
show	Name des Parameters	Information anzeigen
trace	Name des Parameters	Trace ausführen

Befehl	Argumente	Bemerkung
time	Name des Parameters	Zeit einstellen
feature	Name des Parameters	Funktion hinzufügen
repeat	Name des Parameters	Befehl wiederholen
readconfig	keine	Komplette Konfiguration auslesen
readstatus	keine	Status-Menü auslesen
writefiash	keine	Firmware aktualisieren
activateimage	Name des Parameters	Anderes Firmware-Image aktivieren
ping	Name des Parameters	Starte Ping
wakeup	Name des Parameters	Sende Paket zum Aufwecken
linktest	Name des Parameters	WLAN-Linktest
writeconfig	keine	Komplette Konfiguration schreiben
ll2mdetect	keine	Starte LL2M-Erkennung
ll2mexec	Name des Parameters	LL2M-Befehl ausführen
scp	Name des Parameters	Sichere Kopie
rcp	Name des Parameters	Sichere Kopie
readscript	Name des Parameters	Skript auslesen
beginscript	keine	Start Skript
endscript	keine	Stop Skript
flash	Name des Parameters	Flash-Modus ein/ausschalten

Für den Zugriff über Telnet müssen alle Parameter freigeschaltet werden, die der Benutzer bearbeiten darf. Welche Werte Telnet an den TACACS+-Server übermittelt, können Sie z. B. mit dem entsprechenden Trace "trace+ tacacs" einsehen.

Die MIB aktueller Geräte können Sie über WEBconfig herunterladen (**Extras** > **SNMP-Geräte-MIB abrufen**).

20.13.6.4 SNMP

Befehl	Argumente	Bemerkung
get	SNMP-ID des Menüeintrags	Wert auslesen
set	SNMP-ID des Menüeintrags	Wert setzen

20.13.7 TACACS+-Umgehung

20.13.7.1 Einleitung

Mit der Nutzung von TACACS+ können alle Konfigurationsschritte auf einem Netzwerkgerät einer besonderen Prüfung (Autorisierung) unterzogen werden. Gleichzeitig können über das entsprechende TACACS+-Accounting die durchgeführten Konfigurationsschritte protokolliert und so nachvollziehbar gemacht werden. Die Verwendung von TACACS+ ist u. a. in Systemen für den elektronischen Zahlungsverkehr erforderlich (PCI-Compliance).

Die strikte Überwachung der ausgeführten Konfigurationsschritte führt allerdings zu einem zusätzlichen Austauschen von Anfragen und Nachrichten mit dem oder den verwendeten TACACS+-Servern. In großen Szenarien kann die TACACS+-Kommunikation bei der Verwendung von Scripten für zentrale Konfigurationsänderungen oder bei regelmäßigen Aktionen über CRON-Befehle zu einer Überlastung der TACSACS+-Server führen.

20.13.7.2 Konfiguration

Um eine mögliche Überlastung der TACACS+-Server durch automatisierte Konfigurationsschritte zu vermeiden, können die Verwendung von CRON, die Aktionstabelle und der Einsatz von Scripten von der Autorisierung und dem Accounting über TACACS+ ausgenommen werden.

Kommandozeile: **Setup** > **TACACS+**

Umgehe-Tacacs-fuer-CRON > Skripte > Aktions-Tabelle

Hier können Sie die Umgehung der TACACS-Autorisierung und des TACACS+-Accounting für verschiedene Aktionen aktivieren bzw. deaktivieren.

Mögliche Werte:

- Aktiviert, deaktiviert.

Default:

- Deaktiviert.



Bitte beachten Sie, dass die Funktion von TACACS+ für das gesamte System über diese Optionen beeinflusst wird. Beschränken Sie die Nutzung von CRON, der Aktionstabelle und von Scripten auf jeden Fall auf einen absolut vertrauenswürdigen Kreis von Administratoren!

20.14 LLDP

Das Protokoll LLDP (Link Layer Discovery Protocol) bietet eine einfache und zuverlässige Möglichkeit für den Austausch von Informationen zwischen benachbarten Geräten im Netzwerk und für die Bestimmung der Topologie von Netzwerken. LLDP stellt durch das im Standard IEEE 802.1AB definierte Verfahren Funktionen zur Identifizierung einzelner Geräte und ganzer Netzwerkstrukturen zur Verfügung. Da das Protokoll auf Schicht 2 (Sicherungsschicht) des OSI-Schichtenmodells arbeitet und somit für die physikalische Adressierung von Geräten sorgt, ist seine Funktionalität nicht auf logische Netze wie IP-Netze begrenzt. LLDP deckt prinzipiell alle physikalisch erreichbaren Geräte eines Netzes ab.

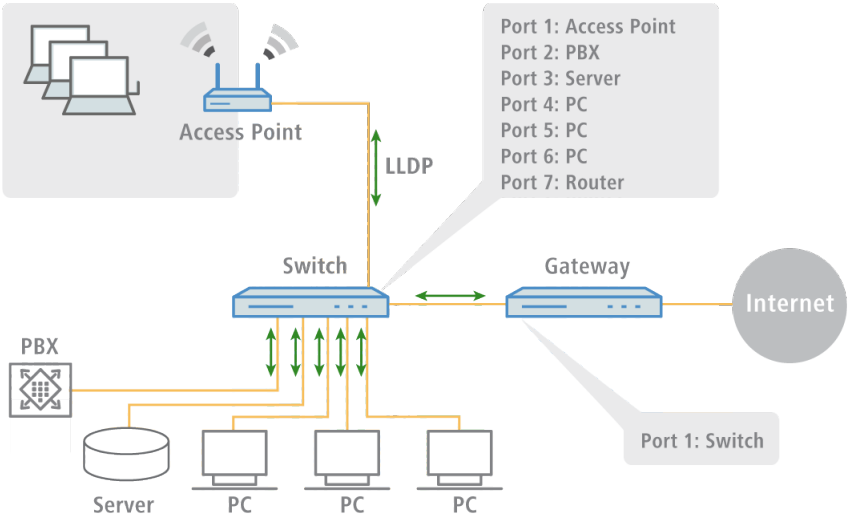
Insbesondere in komplexen Netzen bietet das herstellerunabhängige LLDP-Protokoll große Vorteile:

- Es ermöglicht die automatische Erkennung der in das Netz eingebundenen Komponenten wie Router, Switches und WLAN-Access-Points.
- Es vereinfacht die Einbindung unterschiedlichster Geräte, die den LLDP-Standard unterstützen, in ein bestehendes Netzwerk: Durch den Einsatz einer zentralen Netzwerk-Management-Software und automatisch ablaufende Prüf- und Diagnoseprozesse verringert sich der zeitliche Aufwand für Aufbau, Betrieb und Wartung eines Netzes.
- Die von den Geräten versendeten Informationen ergeben in ihrer Gesamtheit einen Überblick über die Topologie (d. h. den Aufbau und die Anordnung) des Netzes. Eine zentrale Management-Software stellt dem Administrator ein virtuelles Abbild des Netzes zur Verfügung, das sich bei Änderungen an der Topologie selbständig aktualisiert.
- Mit Hilfe einer Management-Software kann der Administrator auch komplexe Netze überwachen und auf einfache Weise verwalten. Er kann anhand der Software feststellen, welche Komponenten und Geräte zusammengeschaltet sind und auftretende Störungen problemlos lokalisieren.
- LLDP kann die Kosten für Anschaffung, Aufbau oder Umgestaltung eines Netzes verringern, da die Unternehmen durch diesen offenen Standard nicht mehr an bestimmte Hersteller gebunden sind. Sie können einzelne Netzkomponenten danach auswählen, für welche Anwendung diese jeweils am besten geeignet sind. Diese Möglichkeit war bislang nicht gegeben, wenn ein proprietäres Protokoll zum Einsatz kam.

20.14.1 Funktionsweise

LLDP funktioniert nach einem einfachen Prinzip: Auf allen Geräten mit LLDP-Unterstützung arbeitet der so genannte LLDP-Agent. Diese Software-Komponente sendet zum einen in regelmäßigen Abständen eigene Informationen an alle

Schnittstellen des Gerätes. Dies erfolgt entweder mittels Unicast oder Multicast, wobei Sie die Zieladressen je nach Bedarf konfigurieren können. Zum anderen empfängt der LLDP-Agent laufend Informationen von benachbarten Geräten. Der Versand und der Empfang der betreffenden Datenpakete erfolgt unabhängig voneinander.



Die versendeten und empfangenen Datenpakete enthalten Informationen wie den Namen und die Beschreibung des Gerätes, die Kennung und Beschreibung von Ports, die IP- oder MAC-Adresse des Gerätes, die spezifischen Fähigkeiten des Gerätes (z. B. in Bezug auf Switching und Routing), VLAN-Kennungen und herstellerspezifische Details. Hierbei definiert LLDP grundlegende Informationen, die ein Datenpaket immer enthalten muss, sowie optionale zusätzliche Informationen.

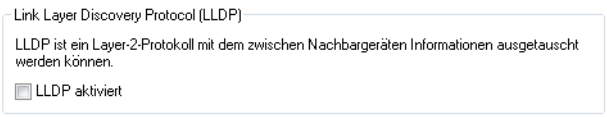
Die einzelnen Geräte legen die empfangenen Informationen lokal in einer Datenstruktur ab, der so genannten MIB (Management Information Base). Eine MIB enthält somit Daten des eigenen LLDP-Agenten und des erkannten, direkten Nachbar-Agenten.

Der Informationsaustausch sorgt für eine ständige Identifikation der Geräte innerhalb des Netzwerks, da die Geräte ihre Datenpakete im Regelfall zyklisch (d. h. in konfigurierbaren Abständen) versenden. Darüber hinaus informieren sie ihre Netz-Nachbarn aber auch dann, wenn sich Änderungen innerhalb der Geräte oder an deren Netzanbindung ergeben.

Für den eigentlichen Prozess der Geräte-Identifizierung ist ausschlaggebend, dass jeder einzelne Verbindungspunkt in der Topologie als „Media Service Access Point" (MSAP) eindeutig identifiziert ist. Ein MSAP setzt sich aus einer Gerätekennung (Chassis-ID) und einer Portkennung (Port-ID) zusammen. Die eindeutige Ermittlung bzw. Zuordnung von Geräten basiert also darauf, dass jeder MSAP in der beobachteten Netzwerk-Topologie nur einmal vorkommen darf.

Der Administrator kann die von den Geräten gemeldeten Daten dann über eine zentrale Netzwerk-Management-Software auf seinem Rechner abfragen und erfassen, wobei die Abfrage der einzelnen MIBs über das SNMP-Protokoll erfolgt. Die Management-Software dokumentiert somit die gesamte Topologie des Netzes und ermöglicht eine automatische Abbildung dieser Topologie sowie die grafische Darstellung von aktuellen Diagnosedaten.

Die Aktivierung von LLDP mittels LANconfig erfolgt unter **Schnittstellen** > **LAN**.



20.14.2 Aufbau der LLDP-Nachrichten

Der Austausch der Informationen erfolgt über spezifische Dateneinheiten, die so genannten LLDP Data Units (LLDPDU). Eine solche Dateneinheit besteht aus TLVs (Type-Length-Values), wobei jedes TLV-Feld einem bestimmten Typ entspricht und eine bestimmte Länge hat.

Gemäß LLDP-Standard IEEE 802.1AB müssen am Anfang einer LLDPU drei TLVs in der folgenden Reihenfolge stehen:

- Typ 1 = Chassis-ID
- Typ 2 = Port-ID
- Typ 3 = Time To Live

Im Anschluss an diese verbindlichen TLVs kann eine LLDPDU weitere, optionale TLVs enthalten:

- Typ 4 = Port Description
- Typ 5 = System Name
- Typ 6 = System Description
- Typ 7 = System Capabilities
- Typ 8 = Management Address

Am Ende einer LLDPDU muss dann zwingend folgende TLV stehen:

- Typ 0 = End of LLDPDU

Tabellarische Übersicht über die TLVs

TLV	Verwendung	Bezeichnung	Beispiel	Funktion
Typ 1	Erforderlich	Chassis-ID	0018.2fa6.b28c	Identifiziert das Gerät
Typ 2	Erforderlich	Port-ID	Fi-0/12	Identifiziert den Port
Typ 3	Erforderlich	Time To Live	60 sec	Signalisiert dem empfangenden Gerät, wie lange die erhaltene Information gültig sein soll
Typ 4	Optional	Port Description	GigabitEthernet0/12	Zeigt Details über den Port wie etwa die Hardware-Version an
Typ 5	Optional	System Name	PN-I/O 3	Zeigt den vom Administrator vergebenen Namen des Gerätes an
Typ 6	Optional	System Description	LCOS Software, Version 8.9.1 SE	Zeigt Details über das Gerät wie etwa die Version der Netzwerk-Software an
Typ 7	Optional	System Capabilities	Router	Zeigt die primäre Funktion sowie die Fähigkeiten des Gerätes an
Typ 8	Optional	Management Address	192.168.0.1	Zeigt die IP- oder MAC-Adresse des Gerätes an
Typ 0	Erforderlich	End of LLDPDU	----------	Signalisiert das Ende der Dateneinheit

20.14.3 Unterstützte Betriebssysteme

Grundsätzlich funktioniert LLDP auf allen gängigen Systemen, sofern hierfür LLDP-Agenten bzw. eine entsprechende Software zur Auswertung der LLDP-Pakete zur Verfügung stehen. Für Linux gibt es diverse Open-Source-Projekte wie z. B. „LLDPD“, „Open-LLDP“ (mit Bindestrich) oder „ladvd“, die einen LLDP-Agenten bereitstellen.

Das Projekt „OpenLLDP“ zielt auf eine weitere Verbreitung und Akzeptanz des LLDP-Protokolls (IEEE 802.1AB) ab. Die Software unterstützt die Übertragung und den Empfang von LLDP-Nachrichten auf den Plattformen Linux, Mac OS X, FreeBSD und NetBSD. Allerdings scheint die Weiterentwicklung derzeit zu ruhen.

Die Microsoft-Betriebssysteme Windows 7 und 10 enthalten ein proprietäres Protokoll namens LLTD (Link Layer Topology Discovery), welches im Wesentlichen die gleiche Funktionalität wie LLDP aufweist.

Will man auf Windows-Systemen LLDP installieren, kann man auf eine Shareware namens „haneWIN LLDP Agent" zurückgreifen. Mit dieser funktioniert LLDP auf allen Windows-Systemen ab Windows 2000, d. h. sowohl auf 32-Bit- wie auf 64-Bit-Systemen.

Die am weitesten verbreitete freie Software zur Auswertung und Analyse ist Wireshark. In der Grundversion ist Wireshark gratis und hat sich inzwischen als Standard etabliert. Die Software unterstützt zahlreiche Betriebssysteme und kann eine Vielzahl von Protokollen (u. a. auch LLDP) lesen und auswerten. Der Schwerpunkt der Grundversion von Wireshark liegt allerdings auf der Analyse von auftretenden Problemen innerhalb des Netzes. Benötigt man weitergehende Funktionen (wie z. B. die Visualisierung des Netzverkehrs in Form von farbigen Diagrammen), kann man kostenpflichtige Zusatzmodule erwerben.

20.15 SMS-Empfang und -Versand

Sofern Ihr Gerät über ein 3G/4G WWAN-Modul verfügt, ist Ihr Gerät ebenfalls dazu in der Lage, Kurznachrichten über den Short Message Service (SMS) zu empfangen und zu versenden.

Die SMS-Funktion dient dabei vorwiegend als benachrichtigende und funktionserweiternde Schnittstelle für die LCOS-eigenen Module sowie externe Instanzen wie Router, Management-Lösungen, Accounting-Systeme und Ähnliche. Sie haben jedoch auch als Benutzer die Möglichkeit, über die entsprechende *Funktion im LANmonitor* oder mit dem `smssend`-Kommando auf der Konsole Kurznachrichten zu verschicken. Darüber hinaus haben Sie mit LANmonitor auch die Möglichkeit, gesendete oder empfangene Nachrichten *komfortabel zu verwalten*.

Der SMS-Empfang und -Versand muss ebenfalls Vertragsgegenstand der von Ihnen verwendeten SIM-Karte sein.

20.15.1 Empfang von SMS-Nachrichten

Ihr Gerät ist dazu in der Lage, SMS-Benachrichtungen auf Basis des ETSI-Standards TS 127.005 zu empfangen bzw. abzufragen, zu speichern und auf Wunsch den Erhalt einer SMS im SYSLOG zu protokollieren. Der Eintrag ins SYSLOG erfolgt dabei als "Hinweis", um Sie über ggf. wichtige Meldungen – wie z. B. die Benachrichtigung durch eine externe Instanz – zu informieren. Eine solche Instanz kann beispielsweise das Accounting-System Ihres Providers sein:

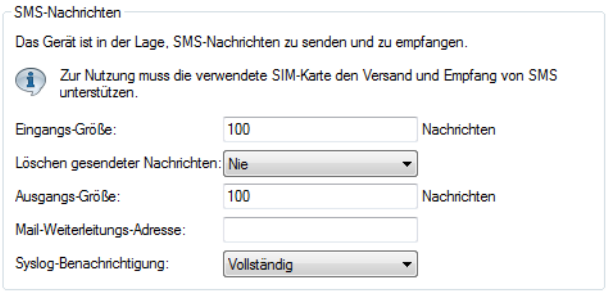
Sofern Sie mit dem Gerät eine Verbindung zum Internet über das 3G/4G WWAN-Modul herstellen und der Vertrag mit Ihrem Internet-Provider eine Volumenbegrenzung umfasst, drosselt oder stoppt Ihr Provider die Datenübertragung bei Erreichen dieser Volumengrenze (je nach Vertrag). In Ländern mit entsprechender Gesetzgebung gilt dies z. B. ebenfalls für das Erreichen bestimmter Gebührengrenzen beim Daten-Roaming. Bevor die Datenübertragung jedoch gedrosselt oder gestoppt wird, versenden viele Provider eine SMS, die Sie als Kunde über das Erreichen der Volumengrenze informiert. Mit einer enstprechenden Benachrichtigungseinstellung im Syslog und / oder per E-Mail informiert Sie das Gerät umgehend über den Empfang der SMS, sodass Sie zeitnah darauf reagieren können.

20.15.2 Basiskonfiguration des SMS-Moduls

Die nachfolgenden Schritte zeigen Ihnen, wie Sie die Basiskonfiguration des SMS-Moduls eines 3G/4G WWAN-fähigen Gerätes vornehmen.

1. Starten Sie LANconfig und öffnen Sie den Konfigurationsdialog für das Gerät.

2. Wechseln Sie in die Ansicht **Meldungen** > **SMS-Nachrichten**.



3. Geben Sie unter **Eingangs-Größe** die maximale Anzahl an Kurznachrichten an, die das Gerät im Nachrichteneingang aufbewahrt.
   Beim Überschreiten der eingestellten Anzahl wird die älteste Nachricht gelöscht. In diesem Fall erfolgt **kein** SYSLOG-Eintrag. Der Wert `0` deaktiviert das Limit, d. h. Nachrichten werden im unbegrenzten Umfang aufbewahrt.

4. Legen Sie unter **Löschen gesendeter Nachrichten** fest, wie das Gerät mit versendeten Kurznachrichten umgeht.
   - **Sofort**: Versendete Kurznachrichten werden nicht gespeichert.
   - **Nie**: Versendete Kurznachrichten werden dauerhaft gespeichert.

5. Geben Sie unter **Ausgangs-Größe** die maximale Anzahl an Kurznachrichten an, die das Gerät im Nachrichtenausgang aufbewahrt.
   Beim Überschreiten der eingestellten Anzahl wird die älteste Nachricht gelöscht. In diesem Fall erfolgt **kein** SYSLOG-Eintrag. Der Wert `0` deaktiviert das Limit, d. h. Nachrichten werden im unbegrenzten Umfang aufbewahrt.

6. Legen Sie unter **Syslog-Benachrichtigung** fest, ob und wie das Gerät eingehende Kurznachrichten im SYSLOG protokolliert.
   - **Nein**: Im SYSLOG erfolgt für eingehende Kurznachrichten kein Eintrag.
   - **Nur Absender/kein Inhalt**: Der Eingang einer Kurznachricht wird zusammen mit der Absender-Rufnummer im SYSLOG erfasst.
   - **Vollständig**: Der Eingang einer Kurznachricht wird zusammen mit der Absender-Rufnummer und dem vollständigen Nachrichtentext im SYSLOG erfasst.

7. Optional: Geben Sie unter **Mail-Weiterleitungs-Adresse** die E-Mail-Adresse an, an die das Gerät eingehende Kurznachrichten weiterleiten soll.

   Damit die E-Mail-Weiterleitung funktioniert, muss ein gültiges SMTP-Konto im Gerät konfiguriert sein.

8. Übertragen Sie die Konfiguration zurück an das Gerät.

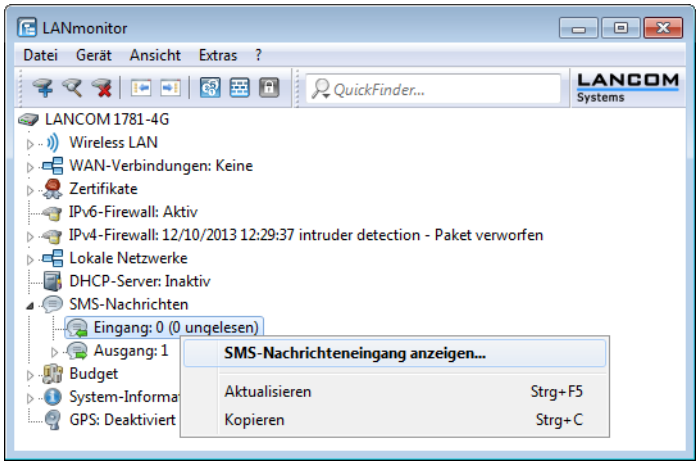
Fertig! Damit ist die Basiskonfiguration des SMS-Moduls abgeschlossen.

20.15.3 SMS-Nachrichten mit LANmonitor verwalten

Der nachfolgende Abschnitt zeigt, wie Sie auf einem 3G/4G WWAN-fähigen Gerät mit LANmonitor eingegangene oder versendete Kurznachrichten einsehen und bei Bedarf löschen.

1. Starten Sie LANmonitor und navigieren Sie im Menübaum des betreffenden Gerätes zu **SMS-Nachrichten** > **Eingang** bzw. **Ausgang**.
   Sofern im Gerät bereits Kurznachrichten vorliegen, zeigt LANmonitor direkt unter **Eingang** die letzten fünf empfangenen und unter **Ausgang** die letzten fünf gesendeten SMS an.

2. Öffnen Sie das Kontextmenü auf dem entsprechenden Eintrag und wählen Sie **SMS-Nachrichteneingang anzeigen** bzw. **SMS-Nachrichtenausgang anzeigen**.



Es öffnet sich ein neues Fenster, in dem LANmonitor alle eingegangenen bzw. versendeten Kurznachrichten und deren Status auflistet. Im **SMS-Nachrichteneingang** haben Sie die Möglichkeit, einzelne oder mehrere ausgewählte Nachrichten wahlweise zu löschen oder als gelesen/ungelesen zu markieren; der Status ist der Lesestatus (entsprechend **Neu** oder **Gelesen**). Im **SMS-Nachrichtenausgang** lassen sich die Nachrichten nur löschen; der Status ist der Sendestatus (**Ungesendet** oder **Gesendet**).

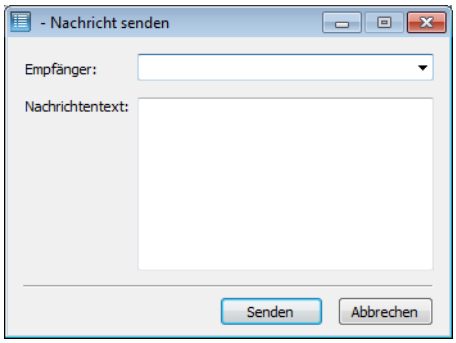
Die angezeigten Nachrichten verwalten Sie über das Kontextmenü. Um den kompletten Nachrichteneingang bzw. -ausgang zu löschen, wählen Sie in der Menüleiste unter **Nachrichten** die betreffende Aktion.

Um zwischen Nachrichteneingang und -ausgang bequem hin- und herzuwechseln, wählen Sie in der Menüleiste unter **Ansicht** die entsprechende Nachrichtenbox aus.

20.15.4 SMS-Nachrichten mit LANmonitor versenden

Der folgende Abschnitt zeigt, wie Sie mit LANmonitor Kurznachrichten über ein 3G/4G WWAN-fähiges Gerät versenden.

1. Starten Sie LANmonitor und navigieren Sie im Menübaum des betreffenden Gerätes zu **SMS-Nachrichten**.
2. Öffnen Sie das Kontextmenü auf dem Eintrag und wählen Sie **Nachricht senden**.
3. Geben Sie in dem sich öffnenden Editorfenster die Rufnummer des Empfängers und den zu versendenden Nachrichtentext ein.
   Die Anzahl der Zeichen ist dabei auf eine Kurznachricht (max. 160 Zeichen) beschränkt. Eine Übersicht der verfügbaren Zeichen finden Sie im Abschnitt *Zeichensatz für den SMS-Versand* auf Seite 1727.



4. Klicken Sie **Senden**, um die Nachricht über das geräteinterne SMS-Modul zu verschicken.

20.15.5 URL-Platzhalter für den SMS-Versand

Sie haben die Möglichkeit, das SMS-Modul in seiner Rolle als Schnittstelle auch über eine URL anzusprechen. Dazu integrieren Sie vorgegebene Platzhalter (Parameter) in die URL, was den SMS-Versand über das Gerät per HTTP(S)-Aufruf erlaubt. Somit eignen sich LANCOM Mobilfunk-Router insbesondere auch für den Einsatz als SMS-Gateway.

Der SMS-Versand eignet sich für Installationen mit einem maximalen Durchsatz von 10 SMS pro Minute.

Die Authentifizierung am Gerät erfolgt mit Ihren Zugangsdaten; deren Einbindung in die URL gibt die Credential-Schreibweise Ihres Browsers vor. Typischerweise lautet diese Schreibweise `Benutzername:Passwort@Host`.

Je nach Einsatzszenario (z. B. SMS-Gateway) empfiehlt es sich, für den Zugang einen Administrator ohne Zugriffsrechte (**Keine**) mit dem alleinigen Funktionsrecht **Senden von SMS** anzulegen.

Nicht alle Webbrowser unterstützen die Übermittlung von Zugangsdaten über die URL. Hierzu gehört u. a. der Microsoft Internet Explorer in seinen aktuellen Versionen. Weichen Sie in diesem Fall auf einen anderen Browser aus, um den SMS-Versand über die URL zu nutzen.

Der URL-Aufruf erfolgt über die Syntax:

```
(http|https)://<User>:<Password>@<Host>/sms/?<Param1>=<Value1>&…&oldauth
```

Der Parameter `oldauth` ist dabei **zwingend** erforderlich; andernfalls sendet keiner der von Ihnen verwendeten Browser die Zugangsdaten an das Gerät. Darüber hinaus sind folgende Platzhalter definiert:

`DestinationAddress`

Rufnummer, an die das Gerät die SMS schicken soll. Es gelten die gleichen Konventionen wie für normale Telefonanrufe. Geben Sie den Parameter wie folgt an:

```
&DestinationAddress=01511234567
&DestinationAddress=00491511234567
```

`Content`

Inhalt der Kurznachricht. Die Anzahl der Zeichen ist dabei auf eine Kurznachricht (max. 160 Zeichen) beschränkt. Eine Übersicht der verfügbaren Zeichen finden Sie im Abschnitt *Zeichensatz für den SMS-Versand* auf Seite 1727.

Um Leerzeichen und andere Sonderzeichen in die SMS einzubauen, müssen Sie diese in URL-kodierter Form an das Gerät übermitteln. Leerzeichen beispielsweise kodieren Sie mittels `%20` und Punkte mit `%2E`. Geben Sie den Parameter wie folgt an:

```
&Content=Dies%20ist%20eine%20Nachricht%2E
```

Mehr zu dem Thema erfahren Sie im Internet unter dem Stichwort "URL Encoding" sowie unter *www.w3schools.com*.

Manche Browser führen die URL-Kodierung automatisch durch. Generell ist jedoch zu empfehlen, Inhalte eigenständig zu kodieren, um die korrekte Umwandlung aller Zeichen sicherzustellen.

20.15.6 Zeichensatz für den SMS-Versand

Der Umfang der in einer SMS verfügbaren Zeichen (max. 160 Zeichen zu je 7 Bit = 1.120 Bit) ergibt sich aus dem GSM-Basiszeichensatz (ingesamt 128 Zeichen) sowie ausgewählten Zeichen aus dem erweiterten GSM-Zeichensatz. Mit dem erweiterten Zeichensatz lassen sich zusätzliche Zeichen darstellen; diese belegen jedoch den doppelten Speicherplatz und reduzieren die maximale Zeichenanzahl entsprechend. Zeichen, die nicht im SMS-Modul implementiert sind, ignoriert das Gerät beim Versand.

Folgende Zeichen sind im **GSM-Basiszeichensatz** definiert:

@	Δ	SP	0	¡	P	¿	p
£	_	!	1	A	Q	a	q
$	Φ	"	2	B	R	b	r
¥	Γ	#	3	C	S	c	s
è	Λ	¤	4	D	T	d	t
é	Ω	%	5	E	U	e	u
ù	Π	&	6	F	V	f	v
ì	Ψ	'	7	G	W	g	w
ò	Σ	(	8	H	X	h	x
Ç	Θ	)	9	I	Y	i	y
LF	Ξ	*	:	J	Z	j	z
Ø	ESC	+	;	K	Ä	k	ä
ø	Æ	,	<	L	Ö	l	ö
CR	æ	-	=	M	Ñ	m	ñ
Å	ß	.	>	N	Ü	n	ü
å	É	/	?	O	§	o	à

"SP" bezeichnet in der Übersicht das Leerzeichen. "LF", "CR" und "ESC" bezeichnen die Steuerzeichen für den Zeilenvorschub, den Wagenrücklauf und den Escape auf den erweiterten GSM-Zeichensatz.

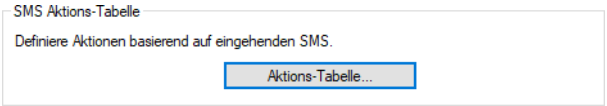
Folgende Zeichen sind aus dem **erweiterten GSM-Zeichensatz** implementiert:

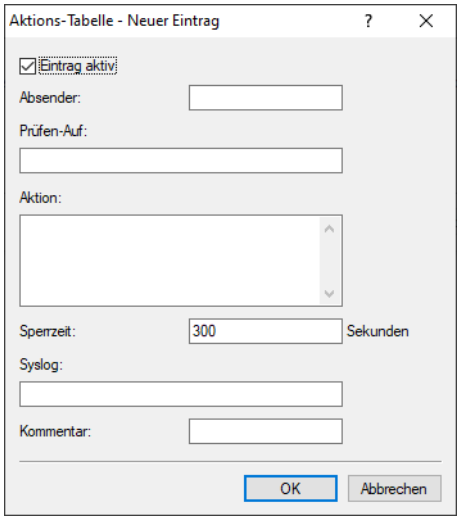
{	|	}	[	]	~	^	\	€

20.15.7 Aktionen auf eingehende SMS ausführen

Hier können Sie auf eingehende SMS mit vordefinierten Aktionen reagieren. Dadurch können Sie bei einer eingehenden SMS (z. B. Datenguthaben aufgebraucht) selber mit einer SMS an den Internetprovider reagieren und darüber neues Datenguthaben hinzubuchen.

In LANconfig konfigurieren Sie dies unter **Meldungen/Monitoring** > **SMS-Nachrichten** > **SMS Aktions-Tabelle** > **Aktions-Tabelle**.





Eintrag aktiv

Aktiviert oder Deaktiviert den Tabelleneintrag.

Absender

Absendeadresse der eingehenden SMS, auf deren Basis die folgende Aktion ausgeführt werden soll. Z. B. 7277 für die Deutsche Telekom.

Prüfen-Auf

Inhalt der eingehenden SMS, auf den geprüft werden soll. Z. B. `contains=' aufgebraucht'` im Falle eines aufgebrauchten Datenguthabens. Der Text, auf den geprüft wird, ist case-sensitiv!

Aktion

Definiert die Aktion, die nach Prüfung der Vorgaben unter **Absender** und **Prüfen-Auf** ausgeführt werden soll. Z. B. `exec:smssend -d 7277 -t "Speed"` zum Buchen eines SpeedOn im Netz der Deutschen Telekom. Mit `exec` wird ein Befehl auf der Konsole ausgeführt, in diesem Fall das Kommando `smssend`.

Die möglichen Befehle entsprechen denen der normalen Aktionstabelle, siehe *Konfiguration der Aktionstabelle*.

Sperrzeit

Definiert die Sperrzeit in Sekunden, in welcher die Aktion nicht erneut ausgeführt werden darf.

Syslog

Freies Textfeld zur Definition der Meldung, die bei Ausführung dieser Aktion in das Syslog geschrieben werden soll.

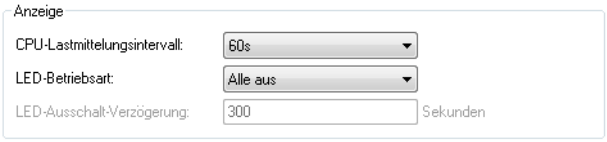
Kommentar

Freies Kommentarfeld.

20.16 Geräte-LEDs bootpersistent ausschalten

Um einen Access Point unauffällig zu betreiben, können Sie die Betriebs- und Status-LEDs am Gerät deaktivieren. Auch nach einem Neustart bleiben die LEDs ausgeschaltet. Sie können allerdings auch festlegen, dass die LEDs kurz nach einem Neustart für eine bestimmte Zeit leuchten sollen, bevor das Gerät sie deaktiviert. Das ist z. bei von WLAN-Controllern verwalteten Access Points hilfreich, um den Verbindungsaufbau zum WLAN-Controller verfolgen zu können.

Die LED-Betriebsart können Sie unter **Management** > **Erweitert** im Abschnitt **Anzeige** festlegen.



In der Auswahlliste **LED-Betriebsart** stehen drei Optionen zur Auswahl:

Normal

Die LEDs sind immer aktiviert, auch nach einem Neustart des Gerätes.

Alle aus

Die LEDs sind alle deaktiviert. Auch nach einem Neustart des Gerätes bleiben die LEDs deaktiviert.

Verzögert aus

Nach einem Neustart sind die LEDs für einen bestimmten Zeitraum aktiviert, danach schalten sie sich aus. Das ist dann hilfreich, wenn die LEDs während des Neustarts auf kritische Fehler hinweisen.

In der Betriebsart **Verzögert aus** können Sie im Feld **LED-Ausschalt-Verzögerung** die Dauer in Sekunden festlegen, nach der das Gerät die LEDs bei einem Neustart deaktivieren soll.

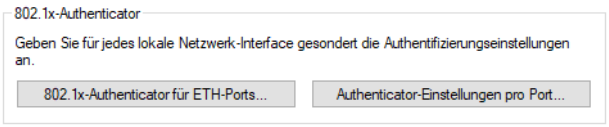
Die Funktion "LED-Test" lässt sich trotz deaktivierter LEDs ausführen.

Wenn Sie diesen Wert innerhalb der zuvor eingestellten Dauer ändern und speichern, starten Sie den Timer neu.

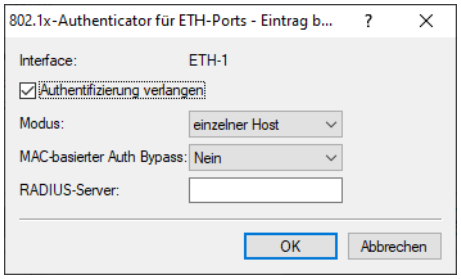
20.17 802.1X-Authenticator für Ethernet-Ports

Mittels des 802.1X-Authenticators können die an die Ethernet-Ports eines LANCOM Gerätes angeschlossenen Geräte mittels 802.1X authentifiziert werden. Dies kann dazu dienen, die Sicherheit vor ungefugtem Zugriff auf das Netzwerk auch im kabelgebundenen Bereich zu erhöhen.

In LANconfig konfigurieren Sie den 802.1X-Authenticator für Ethernet-Ports unter **Schnittstellen** > **LAN** im Abschnitt **802.1x-Authenticator**.



Die Konfiguration nehmen sie in der Tabelle **802.1x-Authenticator für ETH-Ports** vor. Das Interface wird hier jeweils vorgegeben und gibt die vorhandenen Ethernet-Ports an.



Authentifizierung verlangen

Mittels dieses Schalters legen Sie fest, ob für diesen Port eine 802.1X-Authentifizierung gefordert ist.

Modus

Mögliche Werte:

einzelner Host

Es kann an diesem Port nur ein Client die Authentifizierung durchlaufen und anschließend verwendet werden. Wenn an diesem Port ein weiterer Client mit einer eigenen MAC-Adresse erkannt wird, wird der Port in den unauthentifizierten Zustand zurück versetzt.

mehrere Hosts

Es können an diesem Port mehrere Clients (mit unterschiedlichen MAC-Adressen) verwendet werden. Die Authentifizierung muss nur einmalig durchgeführt werden. Dieser Modus bietet sich z. B. an, wenn an einem so konfigurierten Port ein WLAN Access Point betrieben wird und die Nutzdaten nicht zu einem zentralen Controller getunnelt werden. In diesem Fall würden ebenfalls Datenpakete der WLAN-Clients mit deren eigenen MAC-Adressen an dem so konfigurierten Ethernet-Port gesehen werden.

mehrere Authentifizierungen

An diesem Port können mehrere Clients eine jeweils eigene 802.1X-Authentifizierung durchlaufen.

MAC-basierter Auth-Bypass

Legt fest, ob nach dem erfolglosen Versuch, eine 802.1X-Verhandlung zu starten, die MAC-Adresse des Clients via RADIUS geprüft werden und anschließend der Port freigeschaltet werden soll. Die MAC-Adresse wird hierbei als RADIUS-Benutzername und -Passwort im Format „aabbccddeeff" übermittelt und muss auch so im RADIUS-Server hinterlegt werden.

Die MAC-Adresse ist leicht zu fälschen und bietet keinen Schutz vor böswilligen Angriffen.

In der Standardkonfiguration wird der 802.1X-Authenticator zuvor für 90 Sekunden versuchen, eine 802.1X-Verhandlung zu starten, bevor der Rückfall auf die MAC-Adress-Prüfung erfolgt. Dieser Zeitraum kann je Port durch das Ändern der Kommandozeilenparameter **Setup** > **IEEE802.1X** > **Ports** > **Max-Req** (Standard: 3 Versuche) sowie **Setup** > **IEEE802.1X** > **Ports** > **Supp-Timeout** (Standard: 30 Sekunden) angepasst werden. Alternativ kann für **MAC-basierter Auth-Bypass** der Modus „Unverzüglich" gesetzt werden. In diesem Modus wird sofort eine MAC-Adress-Prüfung gestartet, ohne einen Timeout abwarten zu müssen.

Mögliche Werte:

Nein

Die Authentifizierung über die MAC-Adresse ist nicht möglich.

Ja

Die Authentifizierung über die MAC-Adresse ist möglich.

Unverzüglich

Die Authentifizierung wird sofort über die MAC-Adresse durchgeführt.

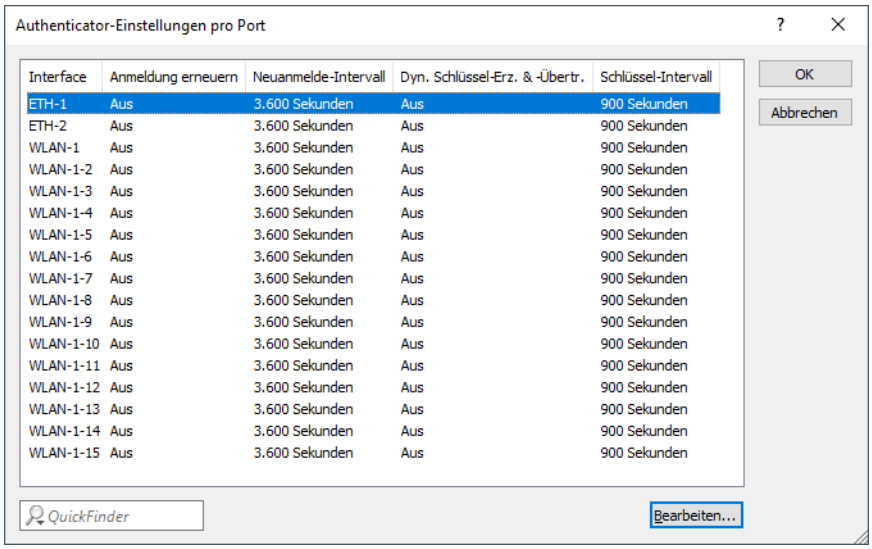
RADIUS-Server

Legt fest, welcher RADIUS-Server sowohl für 802.1X als auch für eine eventuelle MAC-Adress-Prüfung verwendet wird. Referenzieren Sie dazu einen der Einträge unter **Schnittstellen** > **802.1X** > **Radius-Server** oder legen dort ggfs. einen neuen Eintrag an.

Das Format der MAC-Adresse, die im Rahmen der MAC-Authentisierung an den RADIUS-Server übermittelt wird, ist mittels der Kommandozeilenoption **Setup** > **LAN** > **IEEE802.1X** >

Benutzername-Attribut-Format konfigurierbar. Die einzelnen Bytes der MAC-Adresse sind hier als Variablen %a bis %f repräsentiert. In der hier angegebenen Standardeinstellung werden die Bytes der MAC-Adresse nacheinander ausgegeben. Zusätzlich zu diesen Variablen können beliebige vom LCOS unterstützte Zeichen hinzugefügt werden. Ein häufig verwendetes, weiteres Format für die MAC-Adresse „aabbcc-ddeeff" (mit „-" als Trennzeichen) ließe sich dementsprechend wie folgt konfigurieren: „%a%b%c-%d%e%f"

In der Tabelle **Authenticator-Einstellungen pro Port** stellen Sie die Anmeldeinformationen für die lokalen Netzwerkinterfaces ein.



Interface

Das Interface wird hier jeweils vorgegeben und gibt die vorhandenen Ethernet- und WLAN-Zugänge an.

Anmeldung erneuern

Hier aktivieren Sie die regelmäßige Neuanmeldung. Wird eine Neuanmeldung gestartet, so bleibt der Benutzer während der Verhandlung weiterhin angemeldet.

Neuanmelde-Intervall

Standardwert für das Neuanmelde-Intervall bei regelmäßiger Neuanmeldung ist 3.600 Sekunden.

Dyn. Schlüssel erzeugen und übertragen

Hier aktivieren Sie die regelmäßige Erzeugung dynamischer WEP-Schlüssel und deren Übertragung.

Schlüssel-Intervall

Standardwert für das Schlüssel-Intervall ist 900 Sekunden.

20.18 xDSL-Schnittstelle

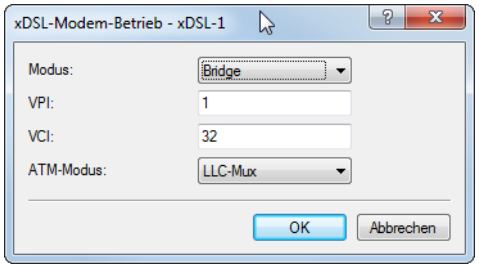
20.18.1 ADSL- / VDSL-Modem-Betrieb (Brigde-Mode)

Im Zuge der Umstellung von ISDN-Anschlüssen auf All-IP werden vorhandene ISDN-Anschlüsse ggf. in zusätzliche DSL-Anschlüsse gewandelt. Damit diese zusätzlich gewonnene Bandbreite für das gesamte Netzwerk zur Verfügung steht muss der DSL-Anschluss mit dem bereits vorhandenen Router verbunden werden. Ist der DSL-Anschluss des Gateways

bereits belegt, kann ein LANCOM VDSL-Router als reines DSL-Modem vorgeschaltet werden. Die Zugangs- und VoIP-Daten werden somit weiter im Hauptgateway hinterlegt. Somit können weitere DSL-Anschlüsse transparent in das vorhandene Szenario eingebunden werden.

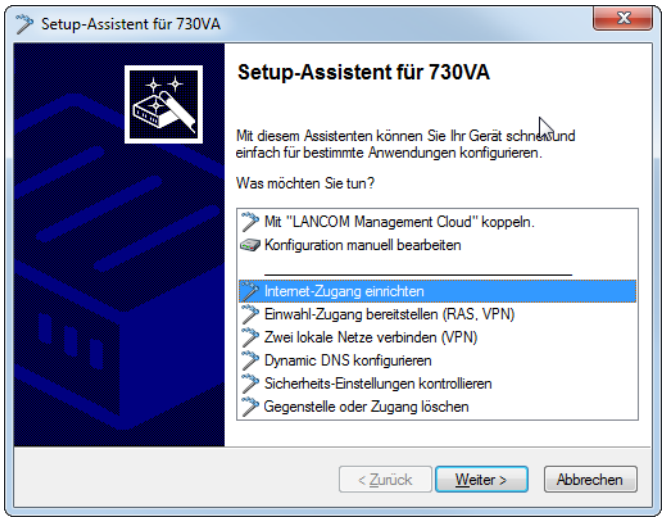
Zur Konfiguration gehen Sie folgendermaßen vor:

1. Den LANCOM Router, welcher als Modem genutzt werden soll, mit dem VDSL-Anschluss verbinden.
2. Das Hauptgateway über ein Ethernet-Kabel mit dem LANCOM Modem verbinden.
3. Unter **Schnittstellen** > **LAN** > **Port-Tabelle** das verwendete LAN und das xDSL-Interface in eine freie Bridge-Gruppe setzen.
4. In **Schnittstellen** > **WAN** > **Schnittstellen-Einstellungen** > **xDSL-Modem-Betrieb** den VDSL-Port auf Bridge-Modus konfigurieren. Bei Verwendung eines ADSL-Anschlusses müssen Sie ggf. die ATM-Parameter korrigieren (Deutsche Telekom: VPI 1, VCI 32, ATM-Modus LLC-Mux).

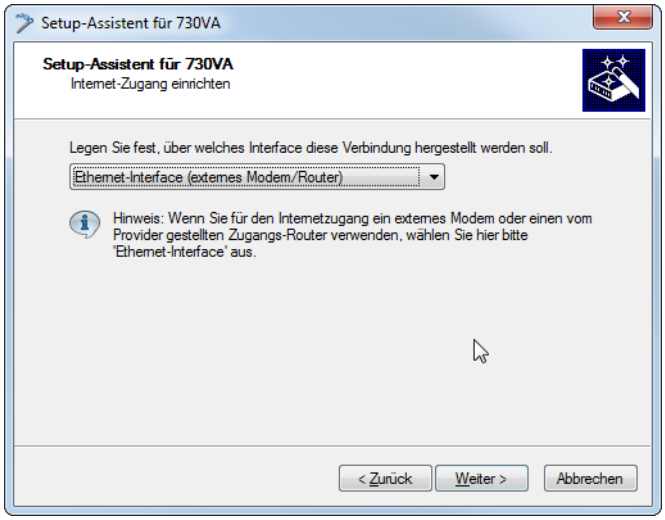


5. Den DHCP-Server unter **IPv4** > **DHCPv4** > **DHCP-Netzwerke** deaktivieren.
6. Dem Router unter **IPv4** > **Allgemein** > **IP-Netzwerke** eine Intranet-IP-Adresse aus einem nicht genutzten Bereich geben (z. B. 192.168.3.254).

   Beachten Sie, dass hierbei die oben verwendete freie Bridge-Gruppe unter **Schnittstellen-Zuordnung** ausgewählt werden muss.
7. Richten Sie auf dem Hauptgateway die Internetverbindung mittels Setup-Assistent ein:
   a. Selektieren Sie ihr Gerät in LANconfig und rufen Sie den Setup-Assistenten „Internet-Zugang einrichten“ auf.



b. Folgen sie den Anweisungen des Setup-Assistenten und wählen jeweils die für Sie passende Option aus. Im Schritt „Interface für diese Verbindung“ wählen Sie die Option **Ethernet-Interface (externes Modem/Router)**.

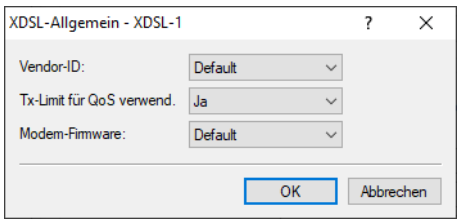


Wenn der Sync-Status des LANCOM Modems aus dem Netzwerk abrufbar sein soll, dann müssen Sie unter **Kommunikation** > **Gegenstellen** > **Gegenstellen (DSL)** die Gegenstelle „Management“ mit Haltezeit „9999“ Sekunden, Layername „IPOE“ und DSL-Port „1“ anlegen.

Legen Sie in der IP-Parameterliste unter **Kommunikation** > **Protokolle** für die Gegenstelle „Management“ eine IP-Adresse aus dem ungenutzten Bereich (z. B. 192.168.3.1/24) fest. Anschließend müssen Sie noch unter **IP-Router** > **Routing** > **IPv4-Routing-Tabelle** einen Eintrag für 192.168.3.0/24 auf Gegenstelle „Management“ mit deaktivierter IP-Maskierung anlegen. Dann kann das Modem über die IP-Adresse 192.168.3.254 erreicht und ausgelesen werden.

20.18.2 Allgemeine xDSL-Einstellungen

In dieser Tabelle finden Sie die allgemeinen Einstellungen zu xDSL.



LANconfig: **Schnittstellen** > **WAN** > **xDSL-Allgemein**

Konsole: **Setup** > **xDSL** > **Allgemein**

Interface

Fester Wert für dieses Interface: 1 für XDSL-1, 2 für XDSL-2 usw.

Herstellerkennung

Die von der deutschen Bundesnetzagentur vorgegebene Kennung für LANCOM Geräte funktioniert nicht in allen Ländern. Für diese wie z. B. die Schweiz muss die Alternativkennung ausgewählt werden.

Sync-limitiert-TX-Rate

Dieser Schalter verändert die Verwendung der Sync-Datenrate als QoS-Datenrate. Wenn aktiviert (Default), dann wird die Sync-Datenrate als QoS-Datenrate verwendet. Sonst wird die Sync-Datenrate nicht verwendet und die Schnittstelle verhält sich bezüglich der QoS-Datenrate wie eine DSL-Schnittstelle.

Modem-Firmware

Da es keine „beste" DSL-Firmware für jede Situation gibt, kann hier ggf. auf eine andere im LCOS vorhandene Modem-Firmware umgeschaltet werden.

Diese Spalte ist nur bei Geräten vorhanden, bei denen das LCOS eine alternative Modem-Firmware enthält.

20.19 GPON-Unterstützung

GPON (Gigabit Passive Optical Network) ist ein optischer Übertragungsstandard für Glasfaseranschlüsse (FTTH). LANCOM bietet hierzu GPON-SFP-Module an, die in LANCOM Routern mit SFP-Schnittstelle betrieben werden können. Die Liste der kompatiblen Geräte befindet sich im jeweiligen GPON-SFP-Datenblatt.

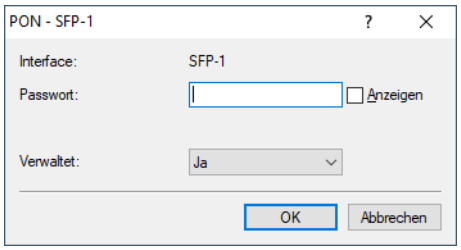
Mit einem GPON-Modul kann der LANCOM Router direkt am Glasfaseranschluss des Providers ohne separates Modem betrieben werden. Bitte kontaktieren Sie ihren Provider ob ein Betrieb ohne Modem und mit SFP-Modul unterstützt wird. In der Regel werden GPON-Modems anhand der Seriennummer und / oder mit einem GPON-Passwort authentifiziert, so dass ein Betrieb ohne Unterstützung des Providers nicht möglich ist.

In der Regel muss für den GPON-Betrieb nichts im Gerät konfiguriert werden.



LANconfig: **Interfaces** > **WAN** > **PON**

Konsole: **Setup** > **Schnittstellen** > **PON**



Interface

Wählen Sie hier das SFP-Interface aus, in dem das PON-Modul gesteckt ist, z. B. SFP-1.

Passwort

Geben Sie hier das PON-Passwort ein, falls Ihr Provider eine Authentifizierung per Passwort durchführt. Andere Begriffe für PON-Passwort sind „ONT-Installationskennung" oder „PLOAM-Passwort". Das Passwort muss aus exakt 10 (für ASCII) oder 20 Zeichen (für hexadezimale Darstellung) bestehen, ohne das führendes Präfix 0x für hexadezimale Darstellungen. Verwendet der Provider z. B. nur 14 Zeichen, so muss das Passwort durch manuelles Anhängen von Nullen (0) aufgefüllt werden. Das Passwort ist im Default leer.

Das PON-Passwort für Ihren Anschluss erhalten Sie von Ihrem Internet-Provider.

Verwaltet

Konfigurieren Sie hier, ob das Modem durch das Betriebssystem verwaltet werden soll. In diesem Fall schreibt das System das PON-Passwort (empfohlen).

20.20 ACME-Client

Ab LCOS 10.80 wird der Automatic Certificate Management Environment (ACME) Client nach *RFC 8555* für Let's Encrypt Zertifikate unterstützt. *Let's Encrypt* ist eine freie und offene Zertifizierungsstelle, die es ermöglicht, kostenfreie SSL- / TLS-Zertifikate zu beziehen. Die Zertifikate können für die WEBconfig sowie für den Public Spot verwendet werden.

Voraussetzung für die Nutzung von Let's Encrypt ist, dass das Gerät über einen öffentlich auflösbaren Domain-Namen, z. B. DynDNS, verfügt. Für eine korrekte Nutzung der Zertifikate muss die WEBconfig des Geräts über den Domain-Namen aufgerufen werden und nicht über die IP-Adresse. Bei Aufruf der WEBconfig über die IP-Adresse schlägt die Zertifikatsprüfung fehl, da Let's Encrypt-Zertifikate auf Domain-Namen und nicht auf IP-Adressen ausgestellt werden.

Bei Let's Encrypt werden Zertifikate ausgestellt, wenn ein Gerät beweisen kann, dass es den Domain-Namen unter Kontrolle hat. Dazu stellt Let's Encrypt eine sogenannte „Challenge", die das Gerät erfüllen muss. Diesen Prozess führt der ACME-Client im Gerät automatisch durch. Ebenso erneuert der ACME-Client automatisch das Zertifikat vor einer definierten Ablauffrist des Zertifikats.

In der Konfiguration muss zunächst ein Domain-Name konfiguriert werden. Das Gerät stellt dann automatisch einen Zertifikatsantrag bei Let's Encrypt und öffnet temporär z. B. den Port 443 oder 80. Daraufhin überprüft Let's Encrypt, ob das Gerät und die zuvor gestellte Challenge (z. B. Token) unter dem angegebenen Domain-Namen und Port 443 oder 80 erreichbar ist. Ist die Prüfung erfolgreich, so wird das Zertifikat ausgestellt. Das Gerät erneuert automatisch das Zertifikat bevor dieses abläuft. Das Gerät öffnet in diesem Prozess kurzzeitig den Port 80 bzw. 443 für diese Challenge und schließt diesen im zweiten Schritt auch wieder.

In folgenden Szenarien ist ein Einsatz von Let's Encrypt nicht möglich bzw. schlägt fehl:

- Das Gerät verfügt über keine öffentliche IP-Adresse
- Eine vorgeschaltete Firewall blockiert den Zugriff auf Port 443 oder 80 vom Internet aus

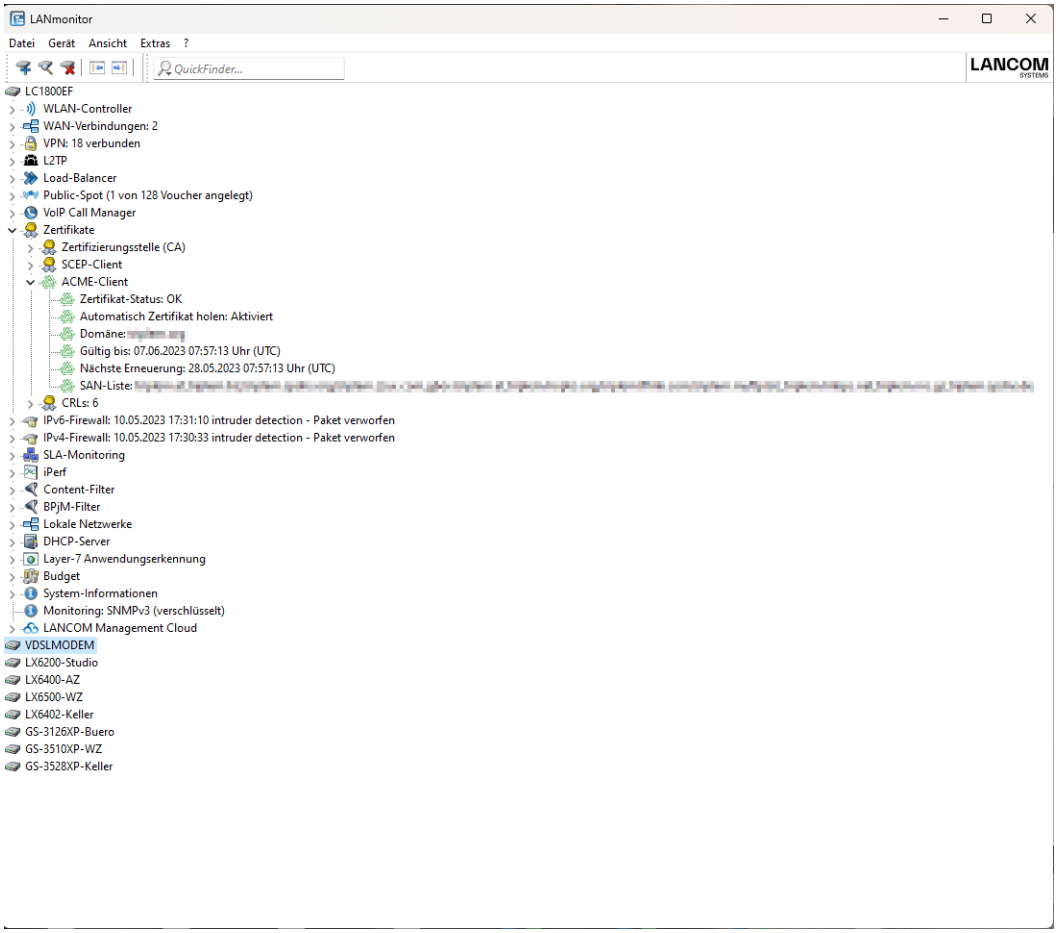
Grundsätzlich werden auch mehrere Domain-Namen im SAN-Feld (Subject Alternative Name) des Zertifikats unterstützt.

Standardmäßig wird Port 443 und das Verfahren tls-alpn-01 für die ACME-Challenge verwendet. Soll das Verfahren http-01 auf Port 80 verwendet werden, muss in der Konfiguration im LANconfig der Parameter **Allgemein** > **Admin** > **Zugriffseinstellungen** > **HTTP-Zugang von einer WAN-Schnittstelle** auf „Automatisch" eingestellt sein.

Bitte beachten Sie, dass eine Nutzung des ACME-Clients mit der Authorisierungs-Challenge tls-alpn-01 sowie ein gleichzeitiges Portforwarding mit Port 443 nicht möglich ist. Das gleiche gilt, falls der ACME-Client über die Methode http-01 verwendet werden soll für Port 80.

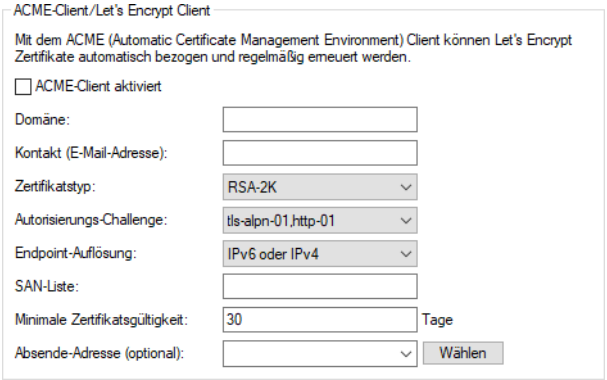
Eine manuelle Anpassung des ACME-Client auf einen beliebigen Port ist laut *RFC 8737* im Protokoll nicht möglich.

Informationen zum ACME-Client können Sie im LANmonitor sehen und mit dem Kommandozeilenbefehl `trace # acme` einen Trace starten bzw. auch wieder beenden.



20.20.1 ACME-Client konfigurieren

In LANconfig konfigurieren Sie den Automatic Certificate Management Environment (ACME) Client unter **Zertifikate** > **ACME-Client**.



ACME-Client aktiviert

Aktiviert bzw. Deaktiviert das automatische Holen und Erneuern des Zertifikats.

Domäne

DNS-Domain-Name für die das Zertifikat erstellt werden soll, z. B. „test.example.com“

Kontakt (E-Mail-Adresse)

Definiert die Kontaktinformationen für den Zertifikatsantrag, z. B. die E-Mail-Adresse „test@example.com“.

Zertifikatstyp

Definiert den Zertifikatstyp inkl. Schlüssellänge.

Mögliche Werte: RSA-2K, RSA-3K, RSA-4K, ECC-256, ECC-384

Autorisierungs-Challenge

Definiert über welche Methode die Autorisierungs-Challenge bei Let’s Encrypt durchgeführt werden soll. Mögliche Werte:

- TLS-alpn-01: Autorisierung wird über TLS und Port 443 durchgeführt
- http-01: Autorisierung wird über HTTP und Port 80 durchgeführt
- http-01,tls-alpn-01: Es wird http-01 vor TLS-alpn-01 bevorzugt
- tls-alpn-01,http-01: Es wird TLS-alpn-01 vor http-01 bevorzugt

Endpoint-Auflösung

Definiert unter welchem Protokoll der Endpunkt aufgelöst werden soll. Mögliche Werte:

- IPv4-Only
- IPv6-Only
- IPv6-Or-IPv4

SAN-Liste

Definiert welche weiteren Domain-Namen im SAN-Feld (Subject Alternative Name) des Zertifikats eingetragen werden sollen. Möglich ist eine komma-getrennte Liste von Domain-Namen (ohne Leerzeichen).

Minimale Zertifikatsgültigkeit

Minimale Anzahl von Tagen bevor das Zertifikat vor Ablauf erneuert wird. Default: 30 Tage

Absende-Adresse (optional)

Referenziert eine benamte Loopback-Adresse, die als Absender verwendet wird. Wenn das Feld leer gelassen wird, wählt der Router selbstständig eine Adresse aus.

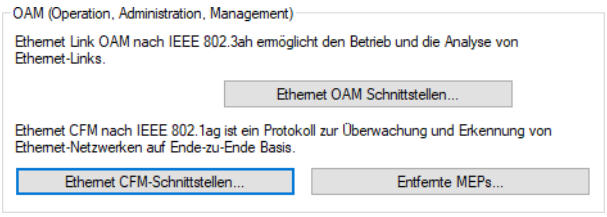
20.21 Operations, Administration und Management (OAM)

Ethernet OAM nach IEEE 802.3ah dient ISPs zur Überwachung einer Ethernet-basierten **letzten Meile**, zum Beispiel bei FTTH- oder VDSL2-Zugängen.

Hierzu werden von der aktiven Seite, die für gewöhnlich die ISP-Seite darstellt, regelmäßig OAM-Pakete (OAM Protocol Data Units – OAMPDUs) übertragen. Die passive Seite, welche für gewöhnlich die CPE-Seite darstellt, reagiert auf diese OAMPDUs und beantwortet sie. Hierdurch wird die Erreichbarkeit der Gegenseite überprüft. Dieses Verfahren wird **OAM Discovery** genannt.

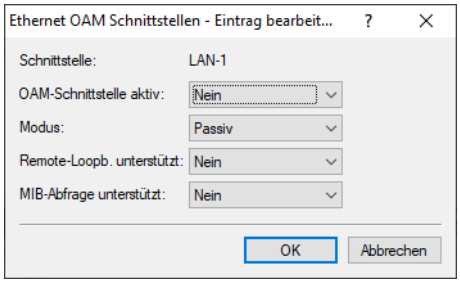
Connectivity Fault Management (CFM) nach IEEE 802.1ag / ITU-T Y.1731 ist eine Sammlung von Protokollen und Werkzeugen zur sog. OAM auf Layer 2. CFM wird verwendet zur Überwachung und Fehleranalyse in LANs, Bridges oder Ethernet-basierten WANs.

In LANconfig konfigurieren Sie OAM unter **Sonstige Dienste** > **Dienste** > **OAM (Operation, Administration, Management)**.



20.21.1 Ethernet Link OAM (IEEE 802.3ah)

In LANconfig konfigurieren Sie Ethernet OAM nach IEEE 802.3ah unter **Sonstige Dienste** > **Dienste** > **OAM (Operation, Administration, Management)** > **Ethernet OAM Schnittstellen**.



Schnittstelle

Name der Schnittstelle.

OAM-Schnittstelle aktiv

Aktiviert/deaktiviert OAM auf der jeweiligen Schnittstelle.

Modus

Legt den Modus (Aktiv/Passiv) für die jeweilige Schnittstelle fest.

Aktiv

Die passive Seite (überlicherweise die CPE-Seite) beantwortet die OAM-Pakete (OAMPDUs) des Senders.

Passiv (Default)

Die aktive Seite (üblicherweise der Internet-Provider) sendet die OAM-Pakete (OAMPDUs) an den Empfänger.

Remote-Loopback unterstützt

Definiert, ob das Geräte sich von der Gegenseite in den Loopback-Modus versetzen lassen kann. Im Loopback-Modus stellet das Gerät den Forwarding-Modus ein und sendet alle empfangenen Pakete auf der Schnittstelle zurück. Dabei wird das Paket genau so zurückgesendet wie es empfangen wurde, es werden weder MAC-Adressen noch IP-Adressen gespiegelt.

MIB-Abfrage unterstützt

Definiert, ob das Gerät erlaubt, dass die Gegenseite bestimmte Statuswerte bzw. Zähler über Pakete vom Gerät abrufen darf.

Die folgenden beiden Kommandos werden auf der CLI unterstützt:

20.21.1.1 Remote-Loopback

Mit diesem Kommando sendet das Gerät eine Loopback Control OAMPDU an die Gegenseite, so dass die Gegenseite in den Loopback-Modus versetzt wird, oder entsprechend wieder beendet wird. Im Loopback-Modus stellt das Gerät auf der Gegenseite den Forwarding-Modus auf dieser Schnittstelle ein und sendet alle empfangenen Pakete zurück. Dabei wird das Paket genau so zurückgesendet wie es empfangen wurde, es werden weder MAC-Adressen noch IP-Adressen gespiegelt.

SNMP-ID:

2.105.4

Pfad Konsole:

Setup > **OAM**

Mögliche Argumente:

-i <Schnittstelle>

Schnittstelle, auf der der Loopback-Modus gestartet oder gestoppt werden soll. Auf dieser Schnittstelle sendet das Gerät eine Nachricht, um die Gegenseite in den Loopback-Modus zu versetzen oder diesen dort zu beenden.

Mögliche Werte aus der OAM-Setup-Tabelle wie z. B. LAN-1, DSL-1, …

[-?]

Gibt eine kurze Hilfe zu den Parametern aus.

<start|stop>

Startet oder stoppt den Loopback-Modus.

20.21.1.2 Variablen-Lesen

Mit diesem Kommando sendet das Gerät eine Variable Request OAMPDU an die Gegenseite. Die Gegenseite sendet darauf den Wert der angefragten Variable auf Basis der lokalen MIB. Mit diesem Verfahren lassen sich z. B. Paketzähler der Gegenseite auslesen. Die Gegenseite muss die Funktion zum Auslesen von MIB-Variablen per OAM unterstützen.

Unterstützt werden u. A. Variablen aus IEEE 802.3.1.

Beispiel:

```
> do Variable-Read -i LAN-3 aFramesTransmittedOK

aFramesTransmittedOK = 8444
OK: Action Variable-Read done
```

SNMP-ID:

2.105.6

Pfad Konsole:

Setup > **OAM**

Mögliche Argumente:

-i <Schnittstelle>

Schnittstelle, auf der die Variable ausgelesen werden soll.

[-?]

Gibt eine kurze Hilfe zu den Parametern aus.

<Variablenname> [weitere Variablennamen]

Ein oder mehrere durch Leerzeichen getrennte Variablennamen.

20.21.2 Connectivity Fault Management (IEEE 802.1ag / ITU-T Y.1731)

Connectivity Fault Management (CFM) nach IEEE 802.1ag / ITU-T Y.1731 ist eine Sammlung von Protokollen und Werkzeugen zur sog. OAM auf Layer 2. CFM wird verwendet zur Überwachung und Fehleranalyse in LANs, Bridges oder Ethernet-basierten WANs.

Die Protokolle bieten insbesondere Providern oder Betreibern bzw. Administratoren von Ethernet-Leitungen die Möglichkeit diese Leitungen proaktiv zu überwachen oder im Fehlerfall zu analysieren.

LCOS unterstützt dabei die folgenden Funktionen:

- **Continuity Check Messages (CCM):** Es werden regelmäßige Status-Nachrichten ausgetauscht, um die Verfügbarkeit der Netzelemente zu überwachen
- **Loopback:** Es können Loopback-Nachrichten gesendet werden, die von der Gegenseite zurückgesendet werden (ethping / Layer 2). Diese Funktion ist analog zum ICMP-basierten Ping auf Layer 3. Es werden sowohl Ethernet-Unicast als auch Multicast-Adressen unterstützt.
- **Linktrace:** Es können Linktrace-Nachrichten gesendet werden, die von der Gegenseite zurückgesendet werden und von Netzelementen auf dem Pfad beantwortet werden (Layer 2). Diese Funktion ist analog zum ICMP-basierten Traceroute auf Layer 3

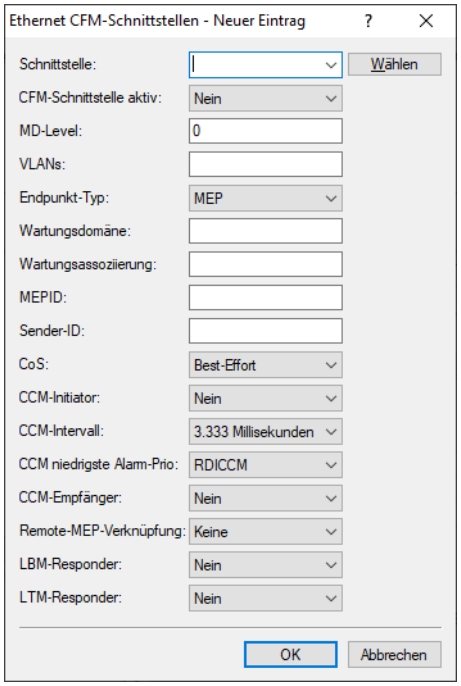
Die Funktionen CCM und Loopback / Linktrace sind unabhängig nutzbar, d. h. Loopback und Linktrace können auch ohne die Nutzung von regelmäßigen CCM-Nachrichten verwendet werden.

Darüber hinaus unterstützt LCOS die folgen Funktionen aus ITU-T Y.1731:

- Empfang und Status-Anzeige von ETH-AIS (Alarm Indication Signal)
- Empfang und Status-Anzeige von ETH-LCK (Ethernet Locked Signal)
- Empfang und Verarbeitung von ETH-RDI (Remote Defect Indication)

20.21.2.1 Ethernet CFM Schnittstellen

In LANconfig konfigurieren Sie Ethernet OAM nach IEEE 802.3ah unter **Sonstige Dienste** > **Dienste** > **OAM (Operation, Administration, Management)** > **Ethernet CFM Schnittstellen**.



Schnittstelle

Schnittstelle auf der CFM aktiviert werden soll, mögliche Werte sind LAN-Schnittstellen wie z.B. LAN-1 oder WAN-Schnittstellen wie DSL-1.

CFM-Schnittstelle aktiv

Aktiviert oder Deaktiviert CFM auf der konfigurierten Schnittstelle.

MD-Level

Definiert das Maintenance Domain Level für diese Schnittstelle.

VLANs

Definiert die VLANs auf der Schnittstelle, mit der CFM-Nachrichten empfangen und gesendet werden können. Bei leerem Wert werden alle VLANs akzeptiert. Es kann entweder ein VLAN oder eine komma-separierte Liste von VLANs konfiguriert werden.

Endpunkt-Typ

Definiert den CFM-Endpunkt-Typ. Mögliche Werte:

MEP (Maintenance Association End Point)

Der Maintenance Association End Point stellt die Grenze einer Domain dar und führt die Fehlererkennung zwischen den Domain-Grenzen durch. Der MEP erstellt und sendet CFM-Pakete.

MIP (Maintenance Intermediate Point)

Der Maintenance Intermediate Point befindet sich innerhalb der Domain und führt die Pfad- und Fehler-Erkennung innerhalb der Domain-Grenzen durch. Der MIP antwortet auf CFM-Pakete.

Wartungsdomäne

Definiert den Namen der Wartungsdomäne (Maintenance Domain (MD)).

Wartungsassoziierung

Definiert den Namen der Wartungsassoziierung (Maintenance Association (MA)).

MEPID

Definiert die Maintenance Endpoint ID des Geräts für diesen Eintrag (1-8191). Diese muss auf jedem Gerät eindeutig sein.

Sender-ID

Definiert die optionale Sender-ID in CFM-CCM-Nachrichten.

CoS

Definiert den Classs-of-Service mit dem CFM-CCM (Continuity Check Message)-Pakete markiert werden. Mögliche Werte: Best-Effort (0), Background (1), Excellent-Effort (3), Controlled-Latency (4), Video (5), Voice (6), Network-Control (7)

CCM-Initiator

Definiert, ob das Gerät regelmäßige CCM-Nachrichten (Continuity Check Message) versenden soll.

CCM-Intervall

Definiert, mit welchen Intervall CCM-Nachrichten (Continuity Check Message) von dem Gerät versendet werden sollen. CCM-Intervalle müssen zwischen Kommunikationspartnern einheitlich sein.

CCM niedrigste Alarm-Priorität

Definiert, wie schwerwiegend festgestellte Fehler mindestens sein müssen, damit der MEP das RDI-Flag (Remote Defect Indication) setzt und in CCM-Paketen propagiert. Level, in aufsteigender Schwere, sind:

RDICCM

Von mindestens einem anderen MEP wurde ein CC-Frame mit gesetztem RDI empfangen.

MACstatus (Default)

Mindestens ein anderer MEP hat einen Interface-Status ungleich 'up' gemeldet (z.B. Hardware-Problem), oder alle anderen MEPs melden einen PortStatus ungleich 'up' (z.B. Netzsegment isoliert).

RemoteCCM

Mindestens von einem konfigurierten MEP werden keine CCM-Frames empfangen.

ErrorCCM

Ein weiterer MEP verwendet die gleiche MEPID wie das lokale Gerät oder es werden CCMs von einem nicht konfigurierten MEP empfangen (falls Matching ungleich none), oder ein anderer MEP verwendet ein abweichendes CCM-Intervall.

XconCCM

Es wurden CCs von einem anderen MEP mit niedrigerem MD-Level empfangen, oder mit einer abweichenden Domain oder Association.

CCM-Empfänger

Definiert, ob das Gerät CCM-Nachrichten verarbeiten bzw. empfangen soll.

Remote MEP-Verknüpfung

Definiert, wie das Gerät die Anwesenheit von entfernten MEPs behandeln soll. Beliebige entfernte MEPs können dynamisch gelernt werden oder es kann als Fehler gewertet werden, wenn eine konfigurierte entfernte MEP nicht gefunden wurde.

Keine

Nicht konfigurierte MEPs werden in die Statustabelle aufgenommen und gehen auch in die Bedingungen RDICCM und MACstatus ein.

Ja

Nicht konfigurierte MEPs werden in die Statustabelle aufgenommen, gehen aber nicht in die Bedingungen RDICCM und MACstatus ein. Sie lösen ErrorCCM aus.

Streng

Nicht konfigurierte MEPs werden nicht in die Statustabelle aufgenommen, gehen nicht in die Bedingungen RDICCM und MACstatus ein. Sie lösen ErrorCCM aus.

LBM-Responder

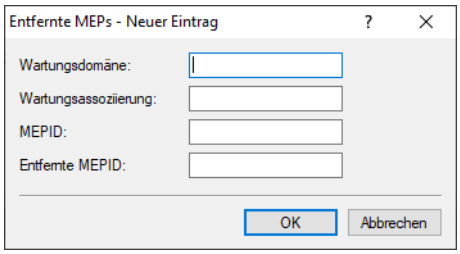
Definiert, ob das Gerät auf CFM-Loopback-Nachrichten (Ethernet-Ping) antworten soll. Die Funktion ist unabhängig vom CCM-Betriebsmodus verwendbar.

LTM-Responder

Definiert, ob das Gerät auf CFM-Linktrace-Nachrichten (Ethernet-Traceroute) antworten soll. Die Funktion ist unabhängig vom CCM-Betriebsmodus verwendbar.

20.21.2.2 Entfernte MEPs

In dieser Tabelle können optional entfernte MEPs definiert werden, die das Gerät auf der entfernten Seite erwartet. In LANconfig konfigurieren Sie diese unter **Sonstige Dienste** > **Dienste** > **OAM (Operation, Administration, Management)** > **Entfernte MEPs**.



Wartungsdomäne

Definiert den Namen der Wartungsdomäne (Maintenance Domain (MD)).

Wartungsassoziierung

Definiert den Namen der Wartungsassoziierung (Maintenance Association (MA)).

MEPID

Definiert die Maintenance Endpoint ID des Geräts für diesen Eintrag (1-8191). Diese muss auf jedem Gerät eindeutig sein.

Entfernte MEPID

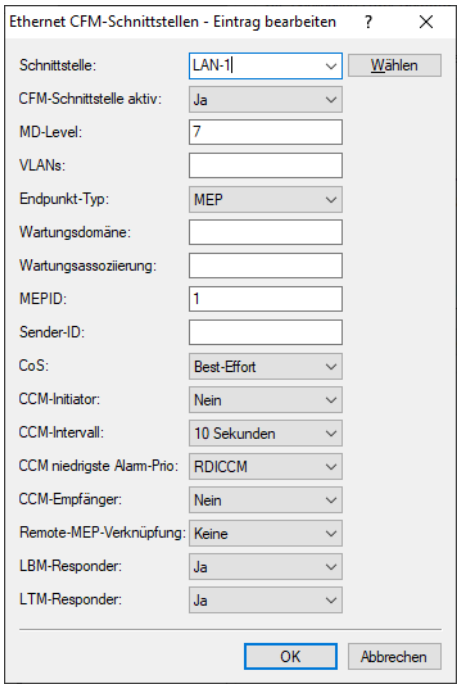
Definiert die entfernte MEPID, die für diese Konfiguration erwartet wird (1-8191). Diese muss auf jedem Gerät eindeutig sein.

20.21.2.3 Kommandos auf der Konsole

Ethping

```
ethping -i <Schnittstelle> [-?] [-c Anzahl] [-v VLAN] [-s Groesse] [-l
MD-Level] <Zieladdresse>
```

Beispiel: Um CFM-Ethernet-Ping zu verwenden ist eine minimale Konfiguration in der Tabelle Ethernet-CFM-Schnittstellen notwendig. Auf dem zweiten Gerät ist eine entsprechende Konfiguration ebenso notwendig, die MEPID muss sich allerdings unterscheiden bzw. eindeutig sein. In diesem Beispiel wird das MD-Level 7 verwendet.



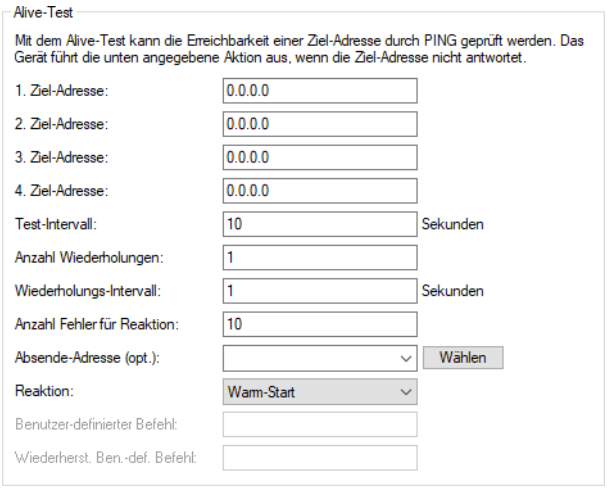

```
root@:/
> ethping -i LAN-1 -l 7 00:a0:57:9c:47:fd
    60 Byte Packet from 00:a0:57:9c:47:fd, seq.no=3109236825, time=0.130 ms
    60 Byte Packet from 00:a0:57:9c:47:fd, seq.no=3109236826, time=0.126 ms
    60 Byte Packet from 00:a0:57:9c:47:fd, seq.no=3109236827, time=0.125 ms

 ---00:a0:57:9c:47:fd ping statistic---
3 Packets transmitted, 3 Packets received, 0% loss
```

Statt den CFM-Ethernet-Ping an eine Ethernet-Unicast-MAC-Adresse zu senden, kann auch die standardisierte Multicast-Gruppe verwendet werden. Dabei ist der Aufbau der Multicast-Adresse wie folgt: 01:80:C2:00:00:3x. Dabei ist x ein Wert zwischen 0 und 7 und entspricht der Nummer des Domain Level für den MEP.

20.22 Alive-Test

Mit dem Alive-Test können Sie die Erreichbarkeit von IPv4-Adressen mittels Ping prüfen. Falls keine Antwort kommt oder nach Nichterreichbarkeit wieder erreichbar wird, dann kann das Gerät eine konfigurierbare Aktion ausführen.

In LANconfig konfigurieren Sie den Alive-Test unter **IPv4** > **Allgemein** > **Alve-Test**.



Ziel-Adresse 1-4

Bis zu vier mögliche Ziel-IPv4-Adressen, an welche das Gerät einen Ping sendet. Es muss nur eine Adresse erreichbar sein, damit der Alive-Test als erfolgreich gilt.

Test-Intervall

Das zeitliche Intervall in Sekunden, in welchem das Gerät einen Ping an die Ziel-Adressen sendet. Wenn der Ping nicht beantwortet wird, sendet das Gerät optional in definierten Abständen eine gewünschte Anzahl von Wiederholungen. Mit dieser Konfiguration bildet das Gerät „Serien" von Ping-Versuchen. Nur wenn alle diese Pings nicht beantwortet werden, wird die komplette Serie als nicht erfolgreich gewertet.

Das Produkt aus Fehler-Limit und Test-Intervall definiert die gesamte Dauer, die bis zum Neustart bzw. zur Ausführung der Aktion vergeht.

Wählen Sie das Test-Intervall größer als das Produkt aus Wiederholungs-Intervall und Anzahl Wiederholungen, damit die gewünschten Wiederholungen innerhalb des Test-Intervalls ausgeführt werden können.

Anzahl Wiederholungen

Dieser Wert gibt an, wie oft das Gerät einen nicht beantworteten Ping an die Ziel-Adresse wiederholt.

Wählen Sie diesem Wert so, dass das Produkt aus Wiederholungs-Intervall und Anzahl Wiederholungen kleiner als das gewählte Test-Intervall ist, damit die gewünschten Wiederholungen innerhalb des Test-Intervalls ausgeführt werden können.

Wiederholungs-Intervall

Dieser Wert gibt an, in welchem zeitlichen Intervall das Gerät einen nicht beantworteter Ping an die Ziel-Adresse wiederholt. Bei einem Wiederholungs-Intervall von 0 sendet das Gerät keine erneuten Versuche.

Wählen Sie diesen Wert so, dass das Produkt aus Wiederholungs-Intervall und Anzahl Wiederholungen kleiner als das gewählte Test-Intervall ist, damit die gewünschten Wiederholungen innerhalb des Test-Intervalls ausgeführt werden können.

Anzahl Fehler für Reaktion

Dieser Parameter definiert die Anzahl der aufeinander folgenden fehlerhaften Test-Serien, bevor das Gerät neu startet bzw. bevor die konfigurierte Aktion ausgeführt wird.

Das Produkt aus diesem Wert und Test-Intervall definiert die gesamte Dauer, die bis zum Neustart bzw. zur Ausführung der Aktion vergeht.

Absende-Adresse (opt.)

Weisen Sie hier eine optionale Absende-Adresse (Name eines ARF-Netzes, benannte Loopback-Adresse oder IP-Adresse) zu, die für den Alive-Test verwendet werden soll.

Reaktion

Diese Aktion führt das Gerät aus, wenn der Ping an die Ziel-Gegenstelle nicht erfolgreich war.

Kaltstart

Das Gerät führt einen Kaltstart durch.

Warmstart (Default)

Das Gerät führt einen Warmstart durch.

Benutzer-definierter Befehl

Das Gerät führt eine konfigurierbare Aktion aus. Konfigurieren Sie diesen Befehl weiter unten.

Benutzer-definierter Befehl

Tragen Sie hier die Aktion ein, die das Gerät ausführt, wenn die Ziel-Adressen nicht erreichbar ist. Als Aktion kann jeder auf der Konsole ausführbare Befehl angegeben werden.

Die hier eingestellte Aktion wird nur ausgeführt, wenn die **Reaktion** auf den Wert **Benutzer-definierter Befehl** eingestellt ist.

Wiederherstellungs-Benutzer-definierter Befehl

Als Wiederherstellungs-Aktion kann jeder auf der Konsole ausführbare Befehl angegeben werden. Dieser wird einmalig ausgeführt, wenn das Gerät vom Fehlerzustand der Nichterreichbarkeit der Zieladresse in den Fall übergeht, wo die konfigurierte Zieladresse wieder erreichbar ist.

Die hier eingestellte Aktion wird nur ausgeführt, wenn die **Reaktion** auf den Wert **Benutzer-definierter Befehl** eingestellt ist.

21 Anhang

21.1 Die CRON-Syntax

Ein CRON-Job besteht aus sechs Feldern:

```
minute    hour    day of month    month    day of week    command
```

Der Asterix '*' dient als Platzhalter für alle erlaubten Zeichen.

Einige Beispiele für das regelmäßige Ausführen eines Restart-Befehls mit CRON:

Jeden Tag um 13:30:

```
30        13        *        *        *        restart
```

Jeden Tag 30 Minuten nach jeder vollen Stunde:

```
30        *         *        *        *        restart
```

Alle 30 Minuten jeden Tag:

```
*/30      *         *        *        *        restart
```

Jeden Samstag um 20:15 Uhr:

```
15        20        *        *        6        restart
```

Der Sonntag wird wahlweise über die '0' oder die '7' ausgewählt.

Um 00:00 Uhr zum Monatsersten

```
0         0         1        *        *        restart
```