

Referenzhandbuch LCOS 7.60

- Addendum 7.70
- Addendum 7.80
- Addendum 8.00

LANCOM Systems

LANCOM Referenzhandbuch Teil 1

- Einleitung
- System-Design
- Konfiguration
- Erweitertes Management
- Diagnose
- Sicherheit

Stand: LCOS 7.6 mit Addendum 7.7 (siehe Anhang)

(letztes Update August 2009)

LANCOM Systems

© 2009 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®, Windows Vista™, Windows NT® und Microsoft® sind eingetragene Marken von Microsoft, Corp.

Das LANCOM Systems-Logo, LCOS und die Bezeichnung LANCOM sind eingetragene Marken der LANCOM Systems GmbH. Alle übrigen verwendeten Namen und Bezeichnungen können Marken oder eingetragene Marken ihrer jeweiligen Eigentümer sein.

LANCOM Systems behält sich vor, die genannten Daten ohne Ankündigung zu ändern und übernimmt keine Gewähr für technische Ungenauigkeiten und/oder Auslassungen.

Produkte von LANCOM Systems enthalten Software, die vom „OpenSSL Project" für die Verwendung im „OpenSSL Toolkit" entwickelt wurde (http://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.

Produkte von LANCOM Systems enthalten Komponenten, die als Open Source Software im Quelltext verfügbar sind und speziellen Lizenzen sowie den Urheberrechten verschiedener Autoren unterliegen. Im Besonderen enthält die Firmware Komponenten, die der GNU General Public License, Version 2 (GPL) unterliegen. Die Lizenzvereinbarung mit dem Text der GPL ist auf der LANCOM CD im Produktverzeichnis zu finden. Auf Anfrage können die Quelltexte und alle Lizenzhinweise elektronisch vom FTP-Server der LANCOM Systems GmbH bezogen werden.

LANCOM Systems GmbH

Adenauerstr. 20/B2

52146 Würselen

Deutschland

www.lancom.de

Würselen, August 2009

110650/0809

Inhalt

1 Einleitung 1 - 1

1.1 Über diese Dokumentation 1 - 1

1.2 Release-Historie 1 - 3

2 System-Design 2 - 1

2.1 Einleitung 2 - 1

3 Konfiguration 3 - 1

3.1 Mittel und Wege für die Konfiguration 3 - 1

3.2 Software zur Konfiguration 3 - 1

3.3 Geräte suchen und konfigurieren 3 - 2

3.4 Die Konfiguration mit LANconfig 3 - 2

3.4.1 LANconfig starten 3 - 2

3.4.2 Sprache der grafischen Oberfläche umschalten 3 - 4

3.4.3 Projektmanagement mit LANconfig 3 - 4

3.4.4 Benutzerspezifische Einstellungen für LANconfig 3 - 5

3.4.5 Anpassen der Symbolleiste 3 - 6

3.4.6 Automatische Sicherung der Konfiguration mit LANconfig 3 - 7

3.4.7 Verzeichnisstruktur 3 - 7

3.4.8 Bessere Übersicht in LANconfig durch mehr Spalten 3 - 8

3.4.9 Multithreading 3 - 9

3.4.10 Manuelle und automatische Suche nach Firmware-Updates 3 - 9

3.4.11 Passwortschutz für SNMP-Lesezugriff 3 - 11

3.4.12 Gerätespezifische Einstellung der Kommunikationsprotokolle 3 - 11

3.4.13 Verhalten von LANconfig beim Start von Windows 3 - 13

3.4.14 Assistent oder Konfigurationsdialog wählbar 3 - 13

3.4.15 WLAN-Konfiguration mit dem Assistenten von LANconfig 3 - 14

3.5 Gruppen-Konfiguration mit LANconfig 3 - 15

3.5.1 Anlegen einer Gruppen-Konfiguration 3 - 15

3.5.2 Gerätekonfigurationen aktualisieren 3 - 17

3.5.3 Gruppen-Konfigurationen aktualisieren 3 - 17

3.5.4 Mehrere Gruppen-Konfigurationen verwenden 3 - 17

3.5.5 Übertragen von Gerätekonfigurationen auf ähnliche Modelle 3 - 18

3.6 LANmonitor – wissen, was läuft 3 - 18

3.6.1 Erweiterte Anzeige-Optionen 3 - 18

3.6.2 Abfrage der CPU- und Speicherauslastung über SNMP 3 - 19

3.6.3 Internet-Verbindung kontrollieren 3 - 19

3.6.4 Anzeige-Funktionen im LANmonitor 3 - 20

3.6.5 Überprüfung der Verbindungsqualität mit dem LANmonitor 3 - 23

3.7 Visualisierung großer WLANs mit dem WLANmonitor 3 - 24

3.7.1 Start des LANCOM WLANmonitors 3 - 24

3.7.2 Suche nach Access Points 3 - 24

3.7.3 Access Points hinzufügen 3 - 25

3.7.4 Access Points organisieren 3 - 25

3.7.5 Rogue AP und Rogue Client Detection mit dem WLANmonitor 3 - 26

3.8 Die Konfiguration mit WEBconfig 3 - 29

3.9 Die Konfiguration mit weiteren Tools 3 - 35

3.9.1 Telnet 3 - 35

3.9.2 SNMP 3 - 39

3.9.3 Verschlüsselte Konfiguration über SSH-Zugang 3 - 39

3.9.4 SSH-Authentifizierung 3 - 40

3.9.5 ISDN-Fernkonfiguration über das DFÜ-Netzwerk 3 - 41

3.10 Abspeichern, Wiederherstellen und Erzeugen von Konfigurationsdateien 3 - 43

3.11 Neue Firmware mit LANCOM FirmSafe 3 - 44

3.11.1 So funktioniert LANCOM FirmSafe 3 - 44

3.11.2 Asymmetrisches Firmsafe 3 - 44
3.11.3 So spielen Sie eine neue Software ein 3 - 45
3.12 Dateien von einem TFTP- oder HTTP-Server direkt in das Gerät laden 3 - 47
3.12.1 TFTP 3 - 47
3.12.2 Firmware, Geräte-Konfiguration oder Script über HTTP(S) laden 3 - 47
3.12.3 Firmware, Geräte-Konfiguration oder Script über HTTP(S) oder TFTP laden 3 - 48
3.13 Wie führt man einen Gerätereset durch? 3 - 49

4 Erweitertes Management 4 -1

4.1 Scripting 4 - 1
4.1.1 Anwendungen 4 - 1
4.1.2 Funktion des Scripting 4 - 2
4.1.3 Scriptdateien erstellen 4 - 2
4.1.4 Einspielen von Konfigurations-Befehlen und Script-Dateien 4 - 4
4.1.5 Mehrere Script-Sessions parallel 4 - 6
4.1.6 Die Befehle für das Scripting 4 - 6
4.2 Rollout-Assistent 4 - 9
4.2.1 Allgemeine Einstellungen für den Rollout-Assistenten 4 - 9
4.2.2 Variablen 4 - 9
4.2.3 Vom Rollout-Assistenten auszuführende Aktionen 4 - 10
4.2.4 Aktionen zur Verwaltung des Rollout-Assistenten 4 - 11
4.3 LANCOM Layer 2 Management Protokoll (LL2M) 4 - 11
4.3.1 Einleitung 4 - 11
4.3.2 Konfiguration des LL2M-Servers 4 - 11
4.3.3 Befehle für den LL2M-Client 4 - 12
4.4 Benachrichtigungen 4 - 13
4.5 Rechteverwaltung für verschiedene Administratoren 4 - 14
4.5.1 Die Rechte für die Administratoren 4 - 15
4.5.2 Administratorenzugänge über TFTP und SNMP 4 - 16
4.5.3 Konfiguration der Benutzerrechte 4 - 16
4.5.4 Einschränkungen der Konfigurationsbefehle 4 - 18
4.5.5 TCP-Port-Tunnel 4 - 19
4.6 Benamte Loopback-Adressen 4 - 20
4.6.1 Loopback-Adressen beim ICMP Polling 4 - 21
4.6.2 Loopback-Adressen für Zeit-Server 4 - 21
4.6.3 Loopback-Adressen für SYSLOG-Clients 4 - 22

5 Diagnose 5 -1

5.1 Trace-Ausgaben – Infos für Profis 5 - 1
5.1.1 So starten Sie einen Trace 5 - 1
5.1.2 Übersicht der Schlüssel 5 - 1
5.1.3 Übersicht der Parameter 5 - 1
5.1.4 Kombinationsbefehle 5 - 2
5.1.5 Filter für Traces 5 - 2
5.1.6 Beispiele für die Traces 5 - 3
5.1.7 Traces aufzeichnen 5 - 3
5.2 Tracen mit dem LANmonitor 5 - 4
5.3 SYSLOG 5 - 10
5.3.1 Einleitung 5 - 10
5.3.2 Aufbau der SYSLOG-Nachrichten 5 - 11
5.3.3 Konfiguration von SYSLOG über LANconfig 5 - 12
5.3.4 Konfiguration von SYSLOG über Telnet oder WEBconfig 5 - 13
5.4 Der Ping-Befehl 5 - 14
5.5 Monitor-Modus am Switch 5 - 15
5.6 Kabel-Tester 5 - 16

6 Sicherheit 6 - 1

6.1 Schutz für die Konfiguration 6 - 1
6.1.1 Passwortschutz 6 - 1
6.1.2 Die Login-Sperre 6 - 2
6.1.3 Einschränkung der Zugriffsrechte auf die Konfiguration 6 - 2
6.2 Den ISDN-Einwahlzugang absichern 6 - 5
6.2.1 Die Identifikationskontrolle 6 - 5
6.2.2 Der Rückruf 6 - 5
6.3 Standort-Verifikation über ISDN oder GPS 6 - 6
6.3.1 GPS-Standort-Verifikation 6 - 6
6.3.2 ISDN-Standort-Verifikation 6 - 6
6.3.3 Konfiguration der Standort-Verifikation 6 - 6
6.4 Die Sicherheits-Checkliste 6 - 9

1 Einleitung

1.1 Über diese Dokumentation

Bestandteile der Dokumentation

Die Dokumentation Ihres Gerätes besteht aus folgenden Teilen:

- Installation Guide

  In dieser Kurzanleitung finden Sie Antworten auf die folgende Fragen:

  - Welche Software muss zur Konfiguration installiert werden?
  - Wie wird das Gerät angeschlossen?
  - Wie kann das Gerät über LANconfig, WEBconfig oder die serielle Schnittstelle erreicht werden?
  - Wie startet man die Setup-Assistenten (z.B. zur Einrichtung des Internetzugangs)?
  - Wie wird ein Gerätereset durchgeführt?
  - Wo gibt es weitere Informationen und Hilfe?

- Benutzerhandbuch

  Das Benutzerhandbuch enthält alle Informationen, die zur raschen Inbetriebnahme Ihres Gerätes notwendig sind. Außerdem finden Sie hier alle wichtigen technischen Spezifikationen.

- Handbuch TK-Anlagenfunktionen (nur bei Modelle mit VoIP-Unterstützung)

  Im Handbuch TK-Anlagenfunktionen finden Sie eine ausführliche Schritt-für-Schritt-Anleitung, um einen LANCOM VoIP Router als Telefonanlage für einen Einzelstandort in Betrieb zu nehmen. Ferner werden dort die wichtigsten Bedienhinweise für Teilnehmer und den Anschluss von Endgeräten beschrieben.

- Referenzhandbuch

  Das Referenzhandbuch ergänzt das Benutzerhandbuch und geht ausführlich auf Themen ein, die übergreifend für mehrere Modelle gelten. Dazu zählen beispielsweise:

  - Systemdesign des Betriebssystems LCOS
  - Konfiguration
  - Management
  - Diagnose
  - Sicherheit
  - Routing- und WAN-Funktionen
  - Firewall
  - Quality-of-Service (QoS)
  - Virtuelle private Netzwerke (VPN)
  - Virtuelle lokale Netzwerke (VLAN)
  - Funknetzwerke (WLAN)
  - Sprachkommunikation in Computernetzwerken mit Voice-over-IP (VoIP)
  - Backup-Lösungen
  - LANCAPI
  - weitere Server-Dienste (DHCP, DNS, Gebührenmanagement)

  Die Beschreibungen im Referenzhandbuch orientieren sich überwiegend an der Konfiguration mit LANconfig. Für jeden LANconfig-Dialog wird ausserdem zugehörige Pfad angegeben, unter dem die entsprechenden parameter bei der Konfiguration mit WEBconfig zu finden sind, z B.:

  LANconfig: Wireless LAN ▶ 802.11i/WEP ▶ WPA- / Einzel-WEP-Einstellungen

  WEBconfig: LCOS-Menübaum ▶ Setup ▶ Schnittstellen ▶ WLAN ▶ Verschluesselung

  Die Pfade für die Konfiguration über die Konsole/Telnet lassen sich daraus ableiten und werden daher nicht explizit aufgeführt. Der Telnetpfad zu den Verschlüsselungseinstellungen lautet z. B.:

  ```
  cd Setup/Schnittstellen/WLAN/Verschluesselung
  ```

- Menü-Referenz

  Die Menü-Referenz beschreibt alle Parameter von LCOS, dem Betriebssystem der LANCOM-Geräte. Diese Beschreibung unterstützt den Anwender bei der Konfiguration der Geräte mit WEBconfig bzw. über die Konsole (Telnet).

Die Parameter werden in der Menü-Referenz in der Reihenfolge der Pfade aufgeführt, wie sie bei der Konfiguration mit Webconfig erreicht werden können. Zu jedem Parameter werden neben der Beschreibung auch die möglichen Eingabewerte und die Standardbelegung wiedergegeben.

Alle Dokumente, die Ihrem Produkt nicht in ausgedruckter Form beiliegen, finden als Acrobat-Dokument (PDF-Datei) unter www.lancom.de/download oder auf der beiliegenden Produkt-CD.

LCOS, das Betriebssystem der LANCOM-Geräte

Alle LANCOM-Router und LANCOM Router Access Points setzen das gleiche Betriebssystem ein: das LCOS. Das von LANCOM Systems selbst entwickelte Betriebssystem ist von außen nicht angreifbar und bietet so eine hohe Sicherheit. Darüber hinaus steht die konsistente Verwendung von LCOS für eine komfortable und durchgängige Bedienung über alle LANCOM-Produkte. Das umfangreiche Featureset ist für alle LANCOM-Produkte (bei entsprechender Unterstützung durch die Hardware) gleich verfügbar und wird durch kostenlose, regelmäßige Software-Updates ständig weiterentwickelt.

In diesem Referenzhandbuch gelten folgende Abgrenzungen von Software, Hardware und Hersteller:

- 'LCOS' bezeichnet das geräteunabhängige Betriebssystem
- 'LANCOM' steht als Oberbegriff für alle LANCOM-Router und LANCOM Router Access Points
- 'LANCOM Systems' steht als Kurzform für den Hersteller, die LANCOM Systems GmbH

Gültigkeit

Das vorliegende Referenzhandbuch gilt für alle LANCOM-Router und LANCOM Router Access Points mit einem Firmwarestand Version 7.6 oder neuer.

Die in diesem Referenzhandbuch beschriebenen Funktionen und Einstellungen werden nicht von allen Modellen bzw. allen Firmware-Versionen unterstützt. Im Anhang befindet sich eine Tabelle, in der für die einzelnen Funktionen vermerkt ist, ab welcher Firmware-Version sie in den entsprechenden Geräte unterstützt werden ('Übersicht über die Funktionen nach Modellen und LCOS*-Versionen' → Anhang).

Die Abbildungen von Geräten sowie die Screenshots stellen immer nur Beispiele dar, die nicht unbedingt exakt dem aktuellen Firmwarestand entsprechen müssen.

Sicherheitseinstellungen

Für einen sorglosen Umgang mit Ihrem Produkt empfehlen wir Ihnen, sämtliche Sicherheitseinstellungen (z.B. Firewall, Verschlüsselung, Zugriffsschutz, Gebührensperre) vorzunehmen, die nicht bereits zum Zeitpunkt des Kaufs des Produkts aktiviert waren. Der LANconfig-Assistent 'Sicherheitseinstellungen' unterstützt Sie bei dieser Aufgabe. Weitere Informationen zu diesem Thema finden Sie auch im Kapitel 'Sicherheit' auf Seite 1.

Zusätzlich bitten wir Sie, sich auf unserer Internet-Seite www.lancom.de über technische Weiterentwicklungen und aktuelle Hinweise zu Ihrem Produkt zu informieren und ggf. neue Software-Versionen herunterzuladen.

An der Erstellung dieser Dokumentation …

… haben mehrere Mitarbeiter/innen aus verschiedenen Teilen des Unternehmens mitgewirkt, um Ihnen die bestmögliche Unterstützung bei der Nutzung Ihres LANCOM-Produktes anzubieten.

Sollten Sie einen Fehler finden, oder einfach nur Kritik oder Anregung zu dieser Dokumentation äußern wollen, senden Sie bitte eine E-Mail direkt an:

info@lancom.de

Sollten Sie zu den in diesem Handbuch besprochenen Themen noch Fragen haben oder zusätzliche Hilfe benötigen, steht Ihnen unser Internet-Server www.lancom.de rund um die Uhr zur Verfügung. Hier finden Sie im Bereich 'Support' viele Antworten auf „häufig gestellte Fragen ('FAQs')". Darüber hinaus bietet Ihnen die Wissensdatenbank einen großen Pool an Informationen. Aktuelle Treiber, Firmware, Tools und Dokumentation stehen für Sie jederzeit zum Download bereit.

Außerdem steht Ihnen der LANCOM-Support zur Verfügung. Telefonnummern und Kontaktadressen des LANCOM-Supports finden Sie in einem separaten Beileger oder auf der LANCOM Systems-Homepage.

Hinweis-Symbole	
	Sehr wichtiger Hinweis, dessen Nichtbeachtung zu Schäden führen kann.
	Wichtiger Hinweis, der beachtet werden sollte.
	Zusätzliche Informationen, deren Beachtung hilfreich sein kann aber nicht erforderlich ist.

1.2 Release-Historie



Aufgrund der begrenzten Hardwaremöglichkeiten können nicht mehr alle der älteren Modelle mit der aktuellen LCOS-Version auf die hier vorgestellten Funktionen aufgerüstet werden. Bitte informieren Sie sich in der Übersichtstabelle ('Übersicht über die Funktionen nach Modellen und LCOS*-Versionen' → Anhang), welche Funktionen von Ihrem Gerät unterstützt werden.

Erweiterungen in LCOS 7.60

- Konfiguration
  - Telnet: Erweiterte Funktionen zum Editieren der Befehle
  - Telnet: Programmierung von Funktionstasten für die Konfiguration
  - WEBconfig: Neue Weboberfläche mit umfangreichem Geräte-Status, Online-Hilfe etc.
  - Dateien von einem TFTP oder HTTP-Server direkt in das Gerät laden
  - Rechteverwaltung für verschiedene Administratoren – Administratoren ohne Trace-Rechte
  - Asymmetrisches Firmsafe
  - LANconfig: Übertragen von Gerätekonfigurationen auf ähnliche Modelle
  - LANconfig: Automatisches Anlegen von Konfigurations-Backups vor Firmware-Uploads, Konfigurationsänderung und Skriptausführung
  - LANconfig: Anpassen der Symbolleiste
  - LANconfig: Objektorientierte Konfiguration der Firewall-Regeln (siehe Firewall)
  - LL2M: LANCOM Layer 2 Management Protokoll
- Diagnose
  - LANmonitor: Speichern von Support-Dateien mit Trace-Daten, Geräte-Konfiguration, Bootlog und Sysinfo
  - LANmonitor: Automatische Sicherung der Trace-Daten
  - LANmonitor: Trace-Konfiguration mit Assistenten
  - LANmonitor: Ausgabe von Show-Kommandos
  - LANmonitor: Ausgabe von Status-Informationen und Statistiken
  - LANmonitor: SSL-verschlüsselte Telnet-Verbindung
  - SYSLOG-Anzeige in LANmonitor und WEBconfig
- WAN
  - Flexible Auswahl der PPP-Authentifizierungsprotokolle
  - Die Aktions-Tabelle
  - Unterstützung des GnuDIP-Protokolls
  - COM-Port-Forwarding, Verwendung der seriellen Schnittstellen für TCP-Verbindungen
  - Flexible Definition der WAN-RIP-Gegenstellen mit Platzhaltern
  - Schnittstellen-Tags für Gegenstellen
- VPN
  - Unbegrenzte Anzahl der VPN-Gegenstellen
  - Extended Authentication Protocol (XAUTH)
  - Backup über alternative VPN-Verbindung
  - Mehrstufige Zertifikate für SSL/TLS

- Firewall
  - □ Objektorientierte Konfiguration der Firewall-Regeln mit LANconfig
  - □ Beschränkung einer Firewall-Regel auf Backup-Verbindungen
  - □ Beschränkung einer Firewall-Regel auf die Verbindungen einer Station
  - □ Vorgabe einer maximalen Anzahl von Verbindungen
  - □ Vorgabe eines prozentualen Anteils der Bandbreite
- Voice over IP

  Angabe der folgenden Parameter für SIP-Provider- und SIP-PBX-Lines:
  - □ Lokale-Portnummer
  - □ (Re-)Registrierung
  - □ Leitungsüberwachung
  - □ Überwachungsintervall
  - □ Vertrauenswürdig
  - □ Privacy-Methode

  Angabe des folgenden Parameters für ISDN- und SIP-User:
  - □ CLIR

  Angabe der folgenden Parameter für Analog-Lines:
  - □ Caller-ID Signaling
  - □ Caller-ID Transmission Requirements
- WLAN
  - □ WLAN: Paket-Forwarding per SSID einstellbar
  - □ Mehrstufige Zertifikate für PublicSpot
  - □ DFS 2, Version 1.4: Freilassen von Kanälen für Wetter-Radar
  - □ Zentrales WLAN-Management: Interner Skript-Speicher (Skript-Management ohne HTTP-Server)
- Meldungen
  - □ SNMP-Traps: Trapversion konfigurierbar
- RADIUS
  - □ VLAN-ID in der Tabelle der RADIUS-Benutzer
  - □ Maskierung auf rufende und gerufene Station in der Tabelle der RADIUS-Benutzer
- DHCP
  - □ BOOTP: Zuweisen von unterschiedlichen IP-Adressen in Abhängigkeit vom IP-Netzwerk
- Sonstige Änderungen
  - □ Zugangslisten mit Routing-Tags

Erweiterungen in LCOS 7.50

- Änderungen bei den LANtools
  - □ 'Bessere Übersicht in LANconfig durch mehr Spalten' → Seite 4-5
  - □ 'Tracen mit dem LANmonitor' → Seite 4-11
  - □ 'WLAN-Konfiguration mit dem Assistenten von LANconfig' → Seite 4-21
  - □ 'Benutzerspezifische Einstellungen für LANconfig' → Seite 4-2
- 'RADSEC' → Seite 16-37
- 'Mehrstufige Zertifikate für SSL/TLS' → Seite 10-46
- LANCOM WLAN Controller
  - □ 'Automatische Funkfeldoptimierung mit LANCOM WLAN Controllern' → Seite 11-80
  - □ 'Zentrales Firmware- und Skript-Management' → Seite 586
- Neue Konfigurations-Assistenten
  - □ 'Rollout-Assistent' → Seite 4-9
- WLAN
  - □ 'Spezielle WLAN-Parameter für 802.11n' → Seite 41
  - □ 'Point-to-Point-Gegenstellen über Stationsnamen anbinden' → Seite 55
  - □ 'Zeiteinheit für Background-Scanning' → Seite 11-40
- GPS

- □ 'Standort-Verifikation über ISDN oder GPS' → Seite 6-6
- GPS
  - □ 'VoIP-Media-Proxy – Optimierte Verwaltung von SIP-Verbindungen' → Seite 13-49
- Weitere Funktionen
  - □ Erweiterungen für das Routing Information Protokoll 'RIP für Netzwerke getrennt einstellen' → Seite 7-8

Erweiterungen in LCOS 7.20

- 'Advanced Routing and Forwarding' → Seite 7-9
- 'Benamte Loopback-Adressen'
  - □ 'Loopback-Adressen beim ICMP Polling' → Seite 3-33
  - □ 'Loopback-Adressen für Zeit-Server' → Seite 3-33
  - □ 'Loopback-Adressen für SYSLOG-Clients' → Seite 3-34
- 'VLAN-IDs für DSL-Interfaces' → Seite 12-7
- 'VLAN Q-in-Q-Tagging' → Seite 12-3
- 'Die Roaming-Tabelle' → Seite 11-49
- 'Die Beaconing-Tabelle' → Seite 11-48
- 'DFS-Verbindungen ohne Zwangsunterbrechung' (→ Seite 11-36)
- 'Verhalten des Reset-Buttons' (→ Seite 3-49)
- 'Erweiterungen im RADIUS-Server' 'RADIUS' → Seite 16-27
- 'Zertifikatsenrollment über SCEP' → Seite 10-47
- 'Das Rapid-Spanning-Tree-Protokoll' → Seite 7-50
- 'HTTP-Tunnel' → Seite 21
- Telefonanlagenfunktion für LANCOM VoIP Router (PBX-Funktionen)
  - □ 'Anrufweiterschaltung (Verbinden und Rufumleitung)' → Seite 13-40
  - □ 'Gruppenrufe mit Ruf-Verteilung' → Seite 13-47
  - □ 'Mehrfachanmeldung (Multi-Login)' → Seite 13-49
- Änderungen bei den LANtools
  - □ '1-Click-VPN für LANCOM Advanced VPN Client' → Seite 10-13
  - □ '1-Click-VPN für Netzwerke (Site-to-Site)' → Seite 10-12
  - □ 'Zertifikate sichern und hochladen mit LANconfig' → Seite 10-36
  - □ 'Verhalten von LANconfig beim Start von Windows' → Seite 4-10
- Sonstige Dienste
  - □ 'CRON-Jobs mit Zeitverzögerung' → Seite 16-22

Erweiterungen in LCOS 6.28

- WLAN
  - □ 'Überprüfung der Verbindungsqualität mit dem LANmonitor' → Seite 4-10
- Änderungen bei den LANtools
  - □ 'Assistent oder Konfigurationsdialog wählbar' → Seite 4-12

Erweiterungen in LCOS 6.24

- WLAN
  - □ 'Background WLAN Scanning' → Seite 11-25
  - □ 'Rogue AP und Rogue Client Detection mit dem WLANmonitor' → Seite 4-39
  - □ 'Indoor-Funktion für WLAN-Kanäle' → Seite 11-26
  - □ 'Anzeige der Empfangsqualität über LEDs' → Seite 36
  - □ 'Authentifizierung nach EAP/802.1X für LANCOM Wireless Router im Client-Modus' → Seite 35
- VPN
  - □ 'Vereinfachte Netzwerkanbindung mit Zertifikaten – Proadaptives VPN' → Seite 10-44
  - □ 'Anfrage von Zertifikaten mittels CERTREQ' → Seite 10-44
  - □ 'Accounting' → Seite 16-15
  - □ 'Gemeinsamer Aufbau von Security Associations' → Seite 10-22
- VoIP

- □ 'Leitungen zum analogen Netz' → Seite 5-25
- □ 'Analog-Benutzer' → Seite 5-22
- □ 'Halten, Makeln, Verbinden' → Seite 13-12
- □ 'Übertragung von DTMF-Tönen' → Seite 13-13
- □ 'Gebühreninformationen an die internen ISDN-Busse übertragen' → Seite 13-13
- □ 'QoS-Parameter für Voice-over-IP-Anwendungen' → Seite 9-6
- □ 'SIP Traces' → Seite 13-84

■ Management
- □ 'Uhrzeitumstellung nach UTC' → Seite 16-20
- □ 'SSH-Authentifizierung' → Seite 3-40

■ LANconfig, LANmonitor, WLANmonitor
- □ 'Sprache der grafischen Oberfläche umschalten' → Seite 4-1
- □ 'Script aus Gerät downloaden' → Seite 4-3
- □ 'Gerätespezifische Einstellung der Kommunikationsprotokolle' → Seite 4-8

Erweiterungen in LCOS 6.10

- 'Certificate Revocation List - CRL' → Seite 10-45
- 'Vereinfachte Einwahl mit Zertifikaten' → Seite 10-43
- 'QoS für WLANs nach IEEE 802.11e (WMM/WME)' → Seite 9-14
- 'Erweiterte WLAN-Protokoll-Filter' → Seite 44
- 'RADIUS' → Seite 16-27
- Voice over IP
  - □ 'Unterstützung digitaler Rufe' → Seite 13-14
  - □ 'Konfiguration der ISDN-Schnittstellen' → Seite 13-52
  - □ 'LANCOM VoIP Router an einem P2P-Anschluss (Anlagenanschluss)' → Seite 13-78
  - □ 'SIP-Trunking' → Seite 13-80
  - □ 'Remote Gateway' → Seite 13-82
- 'VLAN-Tags auf Layer 2/3 im Ethernet' → Seite 12-7
- 'Betrieb von Druckern am USB-Anschluss des LANCOM' → Seite 16-38

Erweiterungen in LCOS 6.00

- 'Voice over IP (VoIP)' → Seite 13-1

Erweiterungen in LCOS 5.20

- 'Backup-Lösungen und Load-Balancing mit VRRP' → Seite 14-8
- 'PPPoE-Server' → Seite 16-23
- 'Mehrstufige Zertifikate für PublicSpots' → Seite 11-84
- 'WAN-RIP' → Seite 7-49
- 'Routing-Tags für VPN- und PPTP-Verbindungen' → Seite 7-5
- 'NAT Traversal (NAT-T)' → Seite 10-52
- 'Konfigurierbare VLAN-Protokoll-ID' → Seite 6
- 'Konfigurierbare VLAN-IDs' → Seite 12-6
- 'Vendor-Class- und User-Class-Identifier im DHCP-Client' → Seite 16-10
- 'Bandbreitenbegrenzung im WLAN' → Seite 11-85
- 'Demilitarisierte Zone (DMZ)' → Seite 7-20

Erweiterungen in LCOS 5.00

- 'Scripting' → Seite 4-1
- 'Einsatz von digitalen Zertifikaten' → Seite 10-23
- 'Adress-Anpassung' → Seite 11-42
- 'Client-Bridge-Unterstützung' → Seite 11-42
- 'DSL-Port-Mapping' → Seite 7-25
- 'Dynamisches Load-Balancing' → Seite 7-27
- 'Policy-based Routing' → Seite 7-3

- 'Monitor-Modus am Switch' → Seite 5-15
- 'Diebstahlschutz mit der ISDN-Standort-Verifikation' → Seite 134
- 'Gruppen-Konfiguration mit LANconfig' → Seite 4-22
- 'Visualisierung großer WLANs mit dem WLANmonitor' → Seite 4-38
- 'Automatische Auswahl der 5GHz-WLAN-Kanäle über DFS mit Black- und White-List' → Seite 30

Erweiterungen in LCOS 4.10

- 'Hochverfügbarkeit von Netzwerken' → Seite 14-1
- 'Betrieb eines Modems an der seriellen Schnittstelle' → Seite 7-43
- 'Der Ping-Befehl' → Seite 5-14
- 'Firmware, Geräte-Konfiguration oder Script über HTTP(S) oder TFTP laden' → Seite 3-48

Erweiterungen in LCOS 4.00

- 'Verschlüsselte Konfiguration über SSH-Zugang' → Seite 3-39
- 'VPN-Verbindungen: hohe Verfügbarkeit mit „Lastenausgleich"' → Seite 10-64
- 'Rechteverwaltung für verschiedene Administratoren' → Seite 3-26
- 'Manuelle Definition der MTU' → Seite 7-48
- 'LEPS – LANCOM Enhanced Passphrase Security' → Seite 11-24
- 'Standard-WEP-Verschlüsselung' → Seite 11-24
- 'Freies Umsetzen von TCP/IP-Ports auf maskierten Verbindungen' → Seite 7-15
- 'IEEE 802.11i für Punkt-zu-Punkt-Verbindungen im WLAN' (→ Seite 56)
- 'Multi-PPPoE' → Seite 7-23
- 'IKE Config Mode' → Seite 10-15
- 'SYSLOG' → Seite 5-10

□ Release- Historie

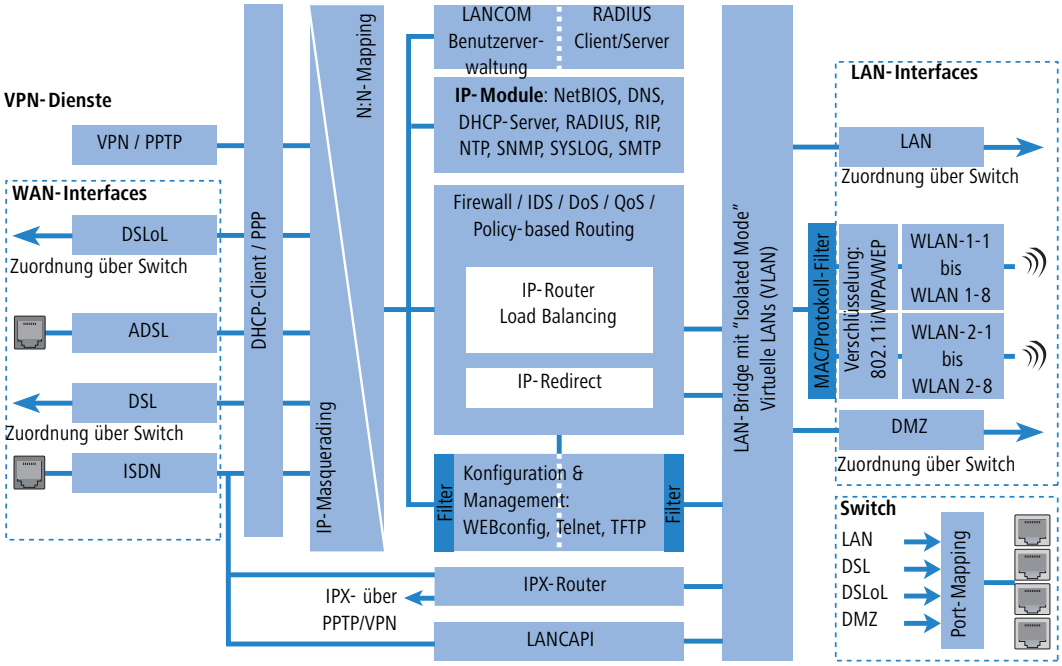
2 System- Design

2.1 Einleitung

Das LANCOM- Betriebssystem LCOS ist aus einer Vielzahl von verschiedenen Software- Modulen aufgebaut, die LANCOM- Geräte selbst verfügen über unterschiedliche Schnittstellen (Interfaces) zum WAN und zum LAN hin. Je nach Anwendung laufen die Daten auf dem Weg von einem Interface zum anderen über verschiedene Module.

Das folgende Blockschaltbild zeigt ganz abstrakt die generelle Anordnung der LANCOM- Interfaces und LCOS- Module. Die Beschreibungen der einzelnen Funktionen im weiteren Verlauf dieses Referenzhandbuchs greifen diese Darstellung jeweils auf, um die wichtigen Verbindungen der jeweiligen Anwendungen darzustellen und die daraus resultierenden Konsequenzen abzuleiten.

So kann dieses Schaubild z.B. verdeutlichen, bei welchen Datenströmen die Firewall zum Einsatz kommt oder an welcher Stelle bei einer Adressumsetzung (IP- Masquerading oder N:N- Mapping) welche Adressen gültig sind.



Hinweise zu den einzelnen Modulen und Interfaces:

- Der IP- Router sorgt für das Routing der Daten auf IP- Verbindungen zwischen den Interfaces aus LAN und WAN.
- Beim IP- Redirect werden Anfragen an ausgewählte Dienste im LAN gezielt auf bestimmte Rechner umgeleitet.
- Die Firewall (mit den Diensten "Intrusion Detection", "Denial of Service" und "Quality of Service") umschließt den IP- Router wie eine Hülle. Alle Verbindungen über den IP- Router gehen also automatisch auch durch die Firewall.
- Als Schnittstellen ins LAN stellen die LANCOM- Geräte ein separates LAN- Interface oder einen integrierten Switch mit mehreren LAN- Interfaces bereit.
- LANCOM Router Access Points bzw. LANCOM- Router mit Wireless- Modul bieten daneben zusätzlich eine oder je nach Modell auch zwei Funkschnittstellen für die Anbindung von Wireless LANs. Jede Funkschnittstelle kann je nach Modell bis zu acht verschiedene WLAN- Netzwerke aufbauen („Multi- SSID").
- Mit der DMZ- Schnittstelle kann bei einigen Modellen eine demilitarisierte Zone (DMZ) eingerichtet werden, die auch physikalisch in der LAN- Bridge von den anderen LAN- Interfaces getrennt ist.
- Die LAN- Bridge verfügt über einen Protokoll- Filter, der das Sperren von dedizierten Protokollen auf dem LAN ermöglicht. Darüber hinaus können durch den "Isolated Mode" einzelne LAN- Interfaces voneinander getrennt werden. Durch den Einsatz der VLAN- Funktionen können in der LAN- Bridge virtuelle LANs eingerichtet werden, die auf einer physikalischen Verkabelung den Betrieb von mehreren logischen Netzen erlaubt.
- Mit den verschiedenen IP- Modulen (NetBIOS, DNS, DHCP- Server, RADIUS, RIP, NTP, SNMP, SYSLOG, SMTP) können die Anwendungen über den IP- Router oder direkt über die LAN- Bridge kommunizieren.
- Die Funktionen "IP- Masquerading" und "N:N- Mapping" sorgen für die geeignete Umsetzung von IP- Adressen zwischen den privaten und dem öffentlichen IP- Bereichen oder auch zwischen mehreren privaten Netzwerken.
- Auf die Dienste für Konfiguration und Management der Geräte (WEBconfig, Telnet, TFTP) kann von LAN- und auch von WAN- Seite aus (bei entsprechender Berechtigung) direkt zugegriffen werden. Diese Dienste sind durch

Filter und Login-Sperre geschützt, es erfolgt hier jedoch **kein** Durchlauf durch die Firewall. Ein direktes "Durchgreifen" aus dem WAN in das LAN (oder umgekehrt) **über** die internen Dienste als Umweg um die Firewall ist jedoch **nicht** möglich.

- IPX-Router und LANCAPI greifen auf der WAN-Seite nur auf das ISDN-Interface zu. Beide Module sind unabhängig von der Firewall, die nur den Datenverkehr durch den IP-Router überwacht. Für IPX über VPN kann der IPX-Router zusätzlich direkt auf das PPTP/VPN-Modul zugreifen.
- Die VPN-Dienste (inklusive PPTP) erlauben das Verschlüsseln der Daten im Internet und damit den Aufbau von virtuellen privaten Netzwerken über öffentliche Datenverbindungen.
- Mit DSL, ADSL und ISDN stehen je nach Modell verschiedene WAN-Interfaces zur Verfügung.
- Das DSLoL-Interface (DSL over LAN) ist kein physikalisches WAN-Interface, sondern eher eine "virtuelle WAN-Schnittstelle". Mit der entsprechenden Einstellung im LCOS kann bei einigen Modellen ein LAN-Interface **zusätzlich** als DSL-Interface genutzt werden.

3 Konfiguration

In diesem Kapitel geben wir Ihnen 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

3.1 Mittel und Wege für die Konfiguration

LANCOM sind flexible Geräte, die verschiedene Mittel (sprich Software) und Wege (in Form von Kommunikationszugängen) für die Konfiguration unterstützen. Zunächst der Blick auf die möglichen Wege.

LANCOM-Produkte können Sie über bis zu drei verschiedene Zugänge erreichen (je nach verfügbaren Anschlüssen):

- über das angeschlossene Netzwerk (sowohl LAN als auch WAN oder WLAN – Inband)

Nicht bei allen Geräte verfügbar

- über die Konfigurations-Schnittstelle (Config-Schnittstelle) des Routers (auch Outband genannt)

Nicht bei allen Geräte verfügbar

- Fernkonfiguration über den ISDN-Anschluss oder über ein Modem (analog oder GSM, in Verbindung mit dem LANCOM Modem Adapter Kit)

Was unterscheidet nun diese drei Wege?

Zum einen die Verfügbarkeit: Die Konfiguration über Outband ist immer verfügbar. Die Inband-Konfiguration ist jedoch z.B. nicht mehr möglich, wenn das übertragende Netzwerk gestört ist. Auch die ISDN-Fernkonfiguration ist abhängig von einer ISDN-Verbindung.

Zum anderen die 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 WEBconfig (vgl. folgender Abschnitt). Die Outband-Konfiguration benötigt zusätzlich zur Konfigurationssoftware noch einen Rechner mit serieller Schnittstelle. Für die ISDN-Fernkonfiguration sind die Voraussetzungen am umfangreichsten: Neben einem ISDN-Anschluss am LANCOM wird im Konfigurations-PC ein ISDN-Adapter oder Zugriff über LANCAPI auf einen weiteren LANCOM mit ISDN-Schnittstelle benötigt.

3.2 Software zur Konfiguration

Die Situationen, in denen konfiguriert wird, unterscheiden sich – aber auch die persönlichen Ansprüche und Vorlieben der Ausführenden. LANCOM-Router verfügen daher über ein breites Angebot von Konfigurationsmöglichkeiten:

- **LANconfig** – menügeführt, übersichtlich und einfach lassen sich nahezu alle Parameter eines LANCOM einstellen. LANconfig benötigt einen Konfigurationsrechner mit Windows 98 oder höher.
- **WEBconfig** – diese Software ist fest eingebaut im Router. Auf dem Konfigurationsrechner wird nur ein Web-Browser vorausgesetzt. WEBconfig ist dadurch betriebssystemunabhängig.
- **SNMP** – geräteunabhängige Programme zum Management von IP-Netzwerken basieren üblicherweise auf dem Protokoll SNMP.
- **Terminalprogramm, Telnet** – ein LANCOM kann mit einem Terminalprogramm (z.B. HyperTerminal) oder innerhalb eines IP-Netzwerks (z. B. Telnet) konfiguriert werden.
- **TFTP** – innerhalb von IP-Netzwerken kann auch das Dateiübertragungs-Protokoll TFTP verwendet werden.

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

Konfigurations-software	LAN, WAN, WLAN (Inband)	Config-Schnitt-stelle (Outband)	ISDN-Fernkonfi-guration	Analoge Einwahl (in Verbindung mit LANCOM Modem Adapter Kit)
LANconfig	Ja	Ja	Ja	Ja
WEBconfig	Ja	Nein	Ja	Ja
SNMP	Ja	Nein	Ja	Ja
Terminalprogramm	Nein	Ja	Nein	Nein
Telnet	Ja	Nein	Nein	Nein
TFTP	Ja	Nein	Ja	Ja

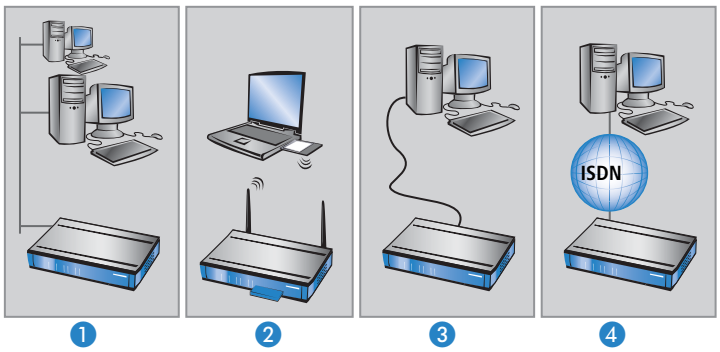
Bitte beachten Sie, dass alle Verfahren auf dieselben Konfigurationsdaten zugreifen. Wenn Sie beispielsweise in LANconfig Einstellungen ändern, hat dies auch direkte Auswirkungen auf die Werte unter WEBconfig und Telnet.

3.3 Geräte suchen und konfigurieren

Schalten Sie immer zuerst das Gerät ein, bevor Sie den Rechner zur Konfiguration starten.

Ein Router oder Access Point kann über die folgenden Wege konfiguriert werden (sofern das Modell über die entsprechende Schnittstelle verfügt):

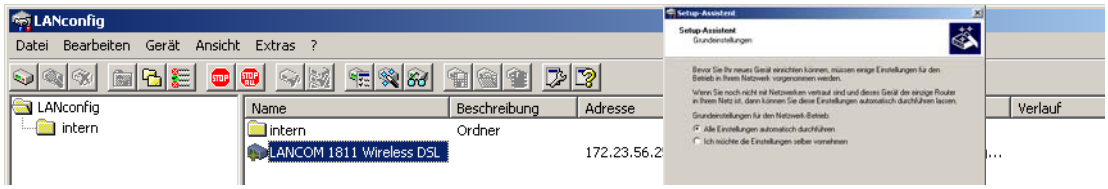
- Über das lokale Netzwerk (LAN) 1.
- Über das Funknetzwerk (WLAN) 2, wenn die WLAN-Verschlüsselung (z.B. 802.11i) in einem Gerät mit Wireless-Schnittstelle und im Konfigurationsrechner passend eingestellt bzw. deaktiviert ist.
- Über die serielle Konfigurationsschnittstelle 3.
- Über eine ISDN-Verbindung 4.



3.4 Die Konfiguration mit LANconfig

3.4.1 LANconfig starten

Rufen Sie LANconfig z.B. aus der Windows-Startleiste auf mit **Start** ▶ **Programme** ▶ **LANCOM** ▶ **LANconfig**. 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" (Windows XP) 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.

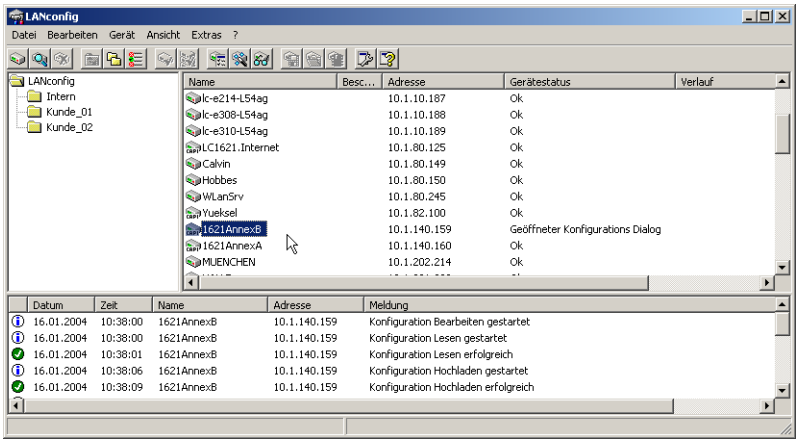
Ihr LANCOM-Gerät verfügt über eine umfangreiche eingebaute Firewall. Diese schützt Ihre Rechner auch dann, wenn keine weitere Firewall auf den Rechnern selbst – wie die „Internetverbindungsfirewall" – eingeschaltet ist.

Neue Geräte suchen



Um die Suche eines neuen Geräts manuell einzuleiten, klicken Sie auf die Schaltfläche **Suchen** oder rufen den Befehl über **Datei** ▶ **Geräte suchen** auf. LANconfig erkundigt sich dann, wo es suchen soll. Bei der Inband-Lösung reicht hier die Auswahl des lokalen Netzes, und los geht's.

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.



Der erweiterte Funktionsumfang für Profis

Für die Konfiguration der Geräte mit LANconfig stehen zwei verschiedene Darstellungsmöglichkeiten zur Auswahl:

- In der 'einfachen Darstellung' werden nur die Einstellungen angezeigt, die für übliche Anwendungsfälle benötigt werden.
- In der 'vollständigen Darstellung' werden alle verfügbaren Einstellungen angezeigt. Einige davon sollten nur von erfahrenen Benutzern verändert werden.

Wählen Sie den Darstellungsmodus im Menü **Extras** ▶ **Optionen**.



Ein Doppelklick auf den Eintrag für das markierte Gerät, der Klick auf die Schaltfläche **Konfigurieren** oder den Menüeintrag **Gerät** ▶ **Konfigurieren** liest die aktuellen Einstellungen aus dem Gerät aus und zeigt die allgemeinen Geräteinformationen an.

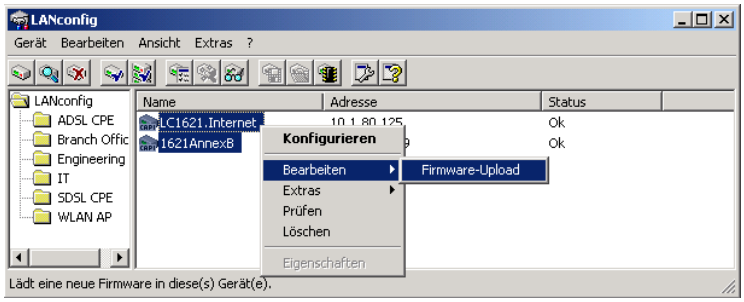
Die eingebaute Hilfe-Funktion

Die weitere Bedienung des Programms erklärt sich selbst bzw. über die Online-Hilfe. Mit einem Klick auf das Fragezeichen oben rechts in jedem Fenster bzw. mit einem rechten Mausklick auf einen unklaren Begriff können Sie die kontextsensitive Hilfe aufrufen.

Verwaltung mehrerer Geräte gleichzeitig

Mit LANconfig können mehrere Geräte gleichzeitig komfortabel (fern-) gewartet werden. Dazu einfach alle gewünschten Geräte selektieren, LANconfig führt dann alle Aktionen für alle ausgewählten Geräte nacheinander durch.

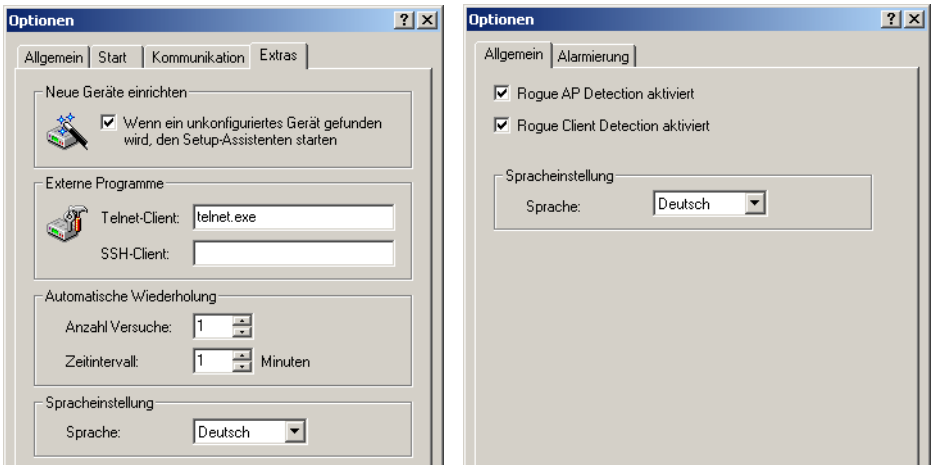
Zur bequemen Verwaltung lassen sich Geräte zu Gruppen zusammenfassen. Dazu muss die Ansicht 'Verzeichnisbaum' aktiviert sein, dann können die Geräte durch einfaches Verschieben per 'drag und drop' in die gewünschten Ordner gruppiert werden.



In der Mehrgeräte-Konfiguration zeigt LANconfig nur die für die Mehrgeräte-Konfiguration geeigneten Eingabefelder an, z.B. bei LANCOM Router Access-Points die MAC Access-Control-Liste.

3.4.2 Sprache der grafischen Oberfläche umschalten

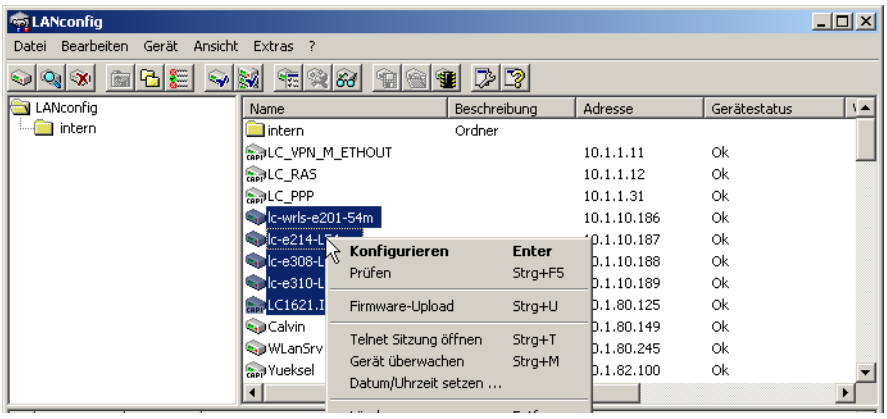
Die Sprache für die grafische Oberfläche von LANconfig, LANmonitor bzw. WLANmonitor kann wahlweise auf 'Deutsch' oder 'Englisch' eingestellt werden



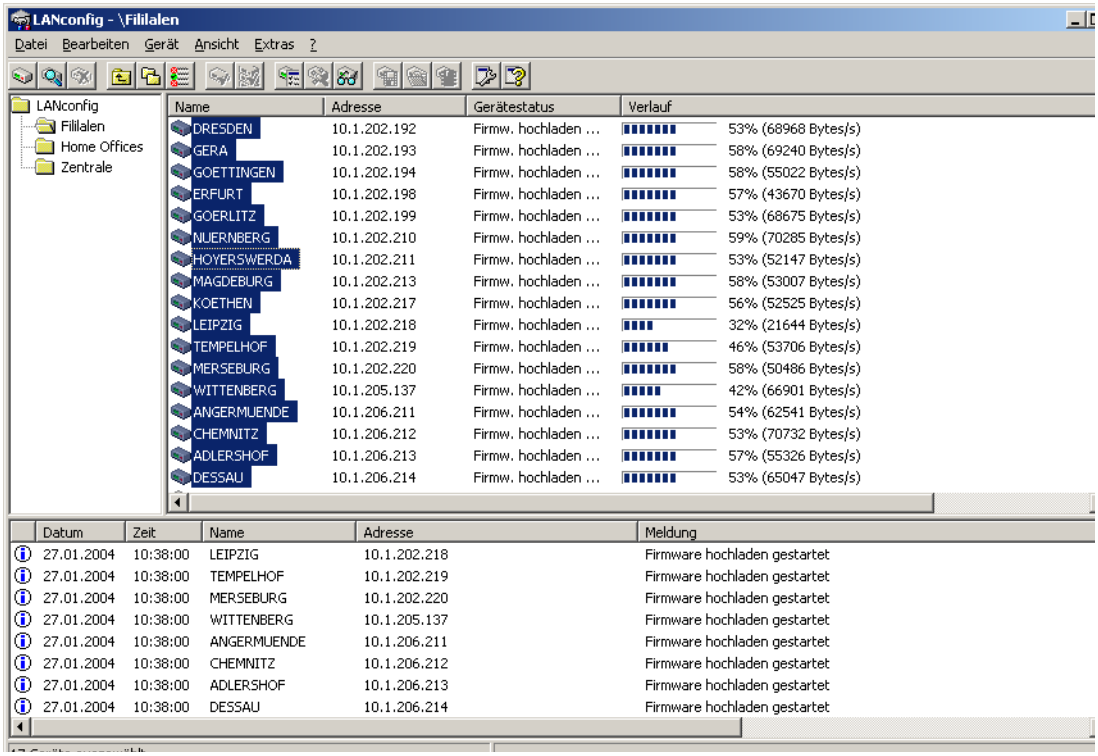
Konfigurationstool	Aufruf
LANconfig	Extras ▶ Optionen ▶ Extras
LANmonitor und WLANmonitor	Extras ▶ Optionen ▶ Allgemein

3.4.3 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.
- Firmware-Upload: Lädt eine Firmware parallel in alle ausgewählten Geräte.
- Script anwenden: Führt ein Konfigurationsscript für alle ausgewählten Geräte aus.



- Telnet-Sitzung öffnen: Öffnet mehrere "DOS-Fenster" und startet zu jedem Gerät eine separate Telnet-Verbindung
- Gerät überwachen: Öffnet die ausgewählten Geräte im LANmonitor zur Überwachung
- Datum/Uhrzeit setzen: Stellt auf allen ausgewählten Geräten die Uhrzeit gleich ein.

Beachten Sie für die Einstellung der Uhrzeit auch die Funktionen des LANCOM als NTP-Client und NTP-Server ('Zeit-Server für das lokale Netz' → Seite 16-18).

- Löschen: Löscht die ausgewählten Geräte aus der Geräteliste im LANconfig.

3.4.4 Benutzerspezifische Einstellungen für LANconfig

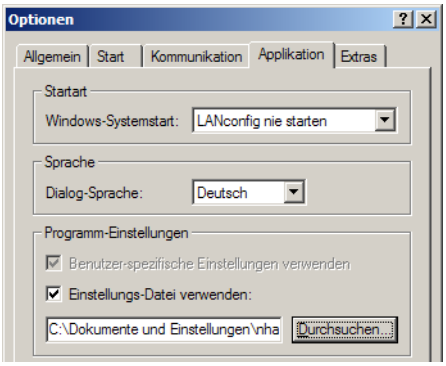
Die Progammeinstellungen von LANconfig werden beim Beenden des Programms in der Datei 'lanconf.ini' im Programmverzeichnis gespeichert. Dazu gehören z. B. die angezeigten Geräte, die Ordnerstruktur, die derzeit gewählte Sprache etc. Beim Programmstart liest LANconfig diese ini-Datei ein und stellt den vorherigen Zustand der Software wieder her. Zum Speichern der ini-Datei benötigt der angemeldete Benutzer Schreibrechte auf das Programmverzeichnis.

Alternativ zu der ini-Datei aus dem Programmverzeichnis können die Progammeinstellungen auch aus einer anderen Quelle gezogen werden. Dazu kann das Benutzerverzeichnis des aktuellen Benutzers gewählt werden oder eine beliebige lanconf.ini von einem anderen Speicherort:

- 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 z. B. die Programmeinstellungen komfortabel in eine andere LANconfig-Installation übertragen werden, oder die Programmeinstellungen können zentral an einem gemeinsamen Speicherort im Netzwerk für mehrere Benutzer angelegt werden.

Sie finden die Parameter zur Konfiguration auf folgenden Pfaden:

LANconfig: **Optionen ▶ Applikation**



- **Benutzerspezifische Einstellungen verwenden**

  Aktiviert die Verwendung der lanconf.ini aus dem aktuellen Benutzer-Verzeichnis `..Benutzer\Anwendungsdaten\LANCOM\LANconfig`.

  Wenn diese Option aktiviert ist, werden Änderungen an den Programmeinstellungen in dieser ini-Datei gespeichert.

  - □ Mögliche Werte: Ein/Aus
  - □ Default: Aus

Wenn neben dieser Option zusätzlich die Option 'Einstellungs-Datei verwenden' aktiviert ist, wird die dort gewählte Datei beim Programmstart verwendet, Änderungen an den Programmeinstellungen in der dort gewählten 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 hier gewählten ini-Datei gespeichert.

  - □ Mögliche Werte: Ein/Aus sowie Auswahl der Einstellungs-Datei
  - □ Default: Aus

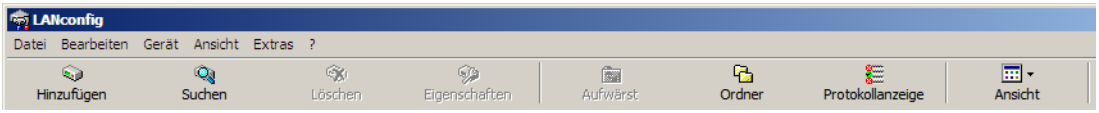
Bei der gewählten Datei muss es sich um eine gültige LANconfig-Einstellungs-Datei handeln.

Wenn keine der beiden Optionen aktiviert ist, wird die ini-Datei aus dem Programmverzeichnis verwendet.

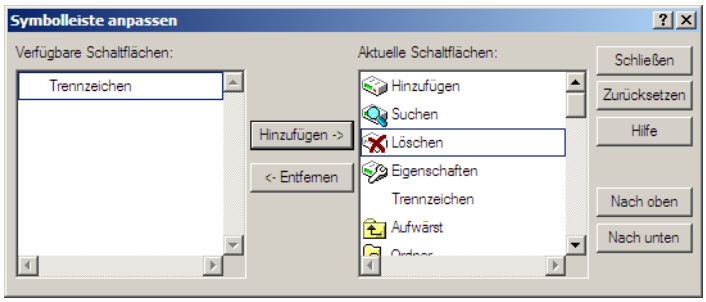
3.4.5 Anpassen der Symbolleiste

Zur benutzerdefinierten Anpassung der Symbolleiste können im LANconfig unter **Ansicht ▶ Symbolleiste** die folgenden Optionen gewählt werden:

- Schaltflächen: Blendet die Schaltflächen ein oder aus.
- Große Symbole: Zeigt eine größere Darstellung der Symbole.
- Text anzeigen: Zeigt unter den Symbolen jeweils einen Text zur Bezeichnung der Aktion.



- 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.



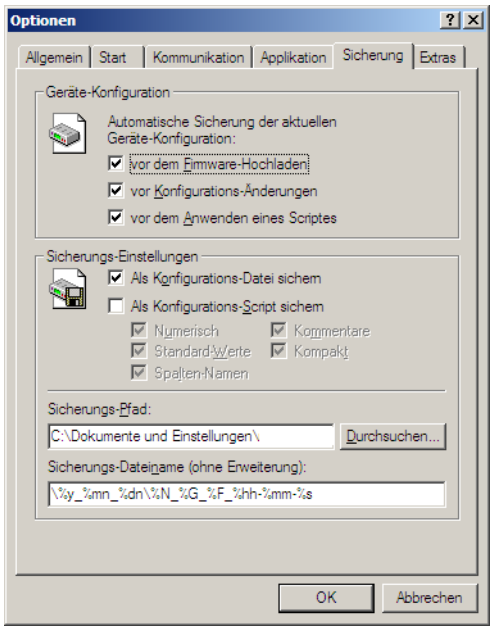
- Zurücksetzen: Setzt die Einstellungen für die Symbolleiste auf die Standardwerte zurück.

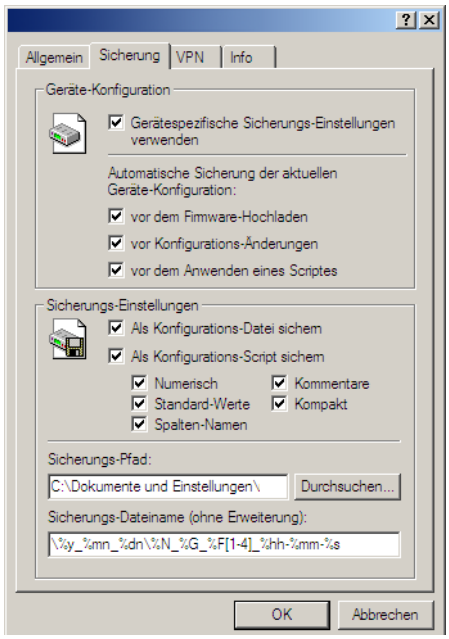
3.4.6 Automatische Sicherung der Konfiguration mit LANconfig

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 ▶ Sicherung**. Für die einzelnen Geräte können ergänzend spezielle Sicherungseinstellungen definiert werden. Klicken Sie dazu das entsprechende Gerät mit der rechten Maustaste und wählen Sie im Kontextmenü den Eintrag **Eigenschaft ▶ Sicherung**.

Wählen Sie hier folgende Optionen aus:

- Werden für dieses Gerät die globalen oder die gerätespezifischen Sicherungseinstellungen verwendet (nur im gerätespezifischen Dialog)?
- Vor welchem Ereignis die Konfiguration gespeichert werden soll (Firmware-Upload, Konfigurationsänderung und Skriptausführung).
- In welchem Format die Konfiguration gespeichert werden soll (Konfigurationsdatei, Skript ggf. mit Optionen).
- In welchem Verzeichnis die Konfiguration gespeichert werden soll.
- Wie der Dateiname der Sicherungs-Datei aufgebaut werden soll. Dabei können Platzhalter für die Geräteinformationen (IP-Adresse, Hardware-Typ etc.) und Zeitinformationen verwendet werden. Weitere Informationen zu den Platzhaltern finden Sie in der Online-Hilfe.



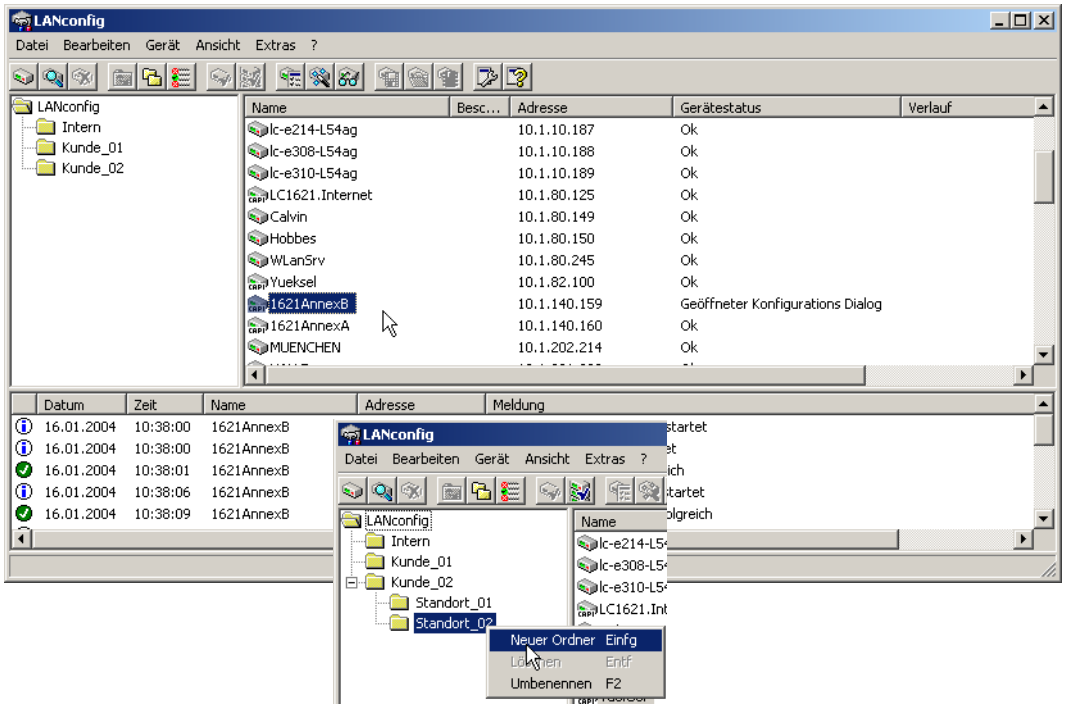


3.4.7 Verzeichnisstruktur

LANconfig erlaubt mit der Verzeichnisstruktur die übersichtliche Verwaltung einer Vielzahl von Geräten. Für jedes Projekt oder jeden Kunden kann ein eigener Ordner angelegt werden, in dem die entsprechenden Geräte organisiert werden:

- Ein neuer Ordner wird mit einem rechten Mausklick auf das übergeordnete Verzeichnis mit dem Eintrag 'Neuer Ordner' im Kontextmenü angelegt.
- Die einzelnen Geräte können dann aus der Liste der Geräte einfach mit der Maus in den entsprechenden Ordner gezogen werden. 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 insbesondere keine Auswirkung auf die Konfiguration der Geräte.



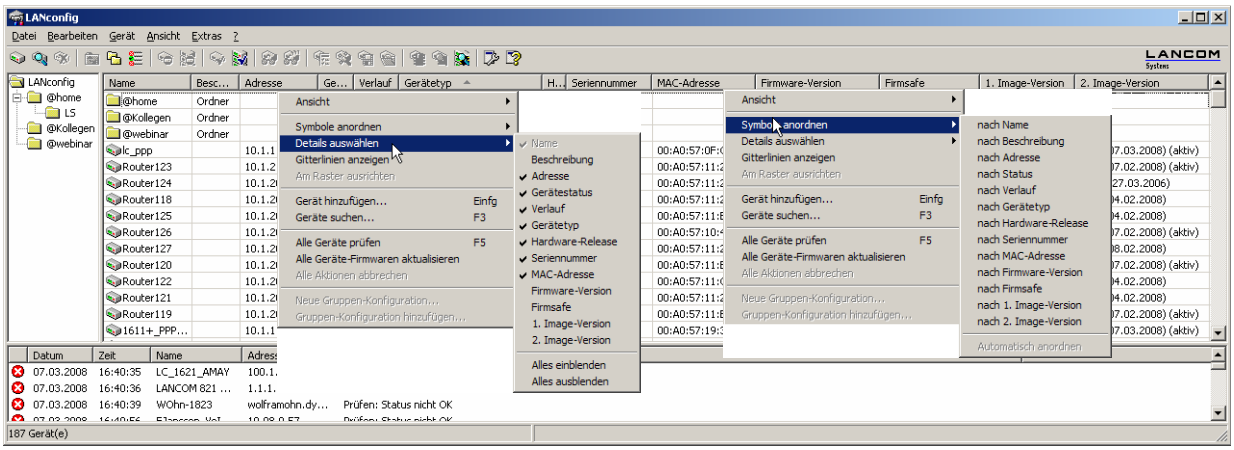
Die Ordnerstruktur am linken Rand des LANconfig-Fensters kann mit der Funktionstaste **F6** oder über das Menü **Ansicht** ▶ **Verzeichnisbaum** ein- und ausgeschaltet werden.

3.4.8 Bessere Übersicht in LANconfig durch mehr Spalten

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 **Details auswählen** die anzuzeigenden Spalten. Über den Menüpunkt **Symbole anordnen** können Sie ausserdem die gewünschte Sortierung auswählen.

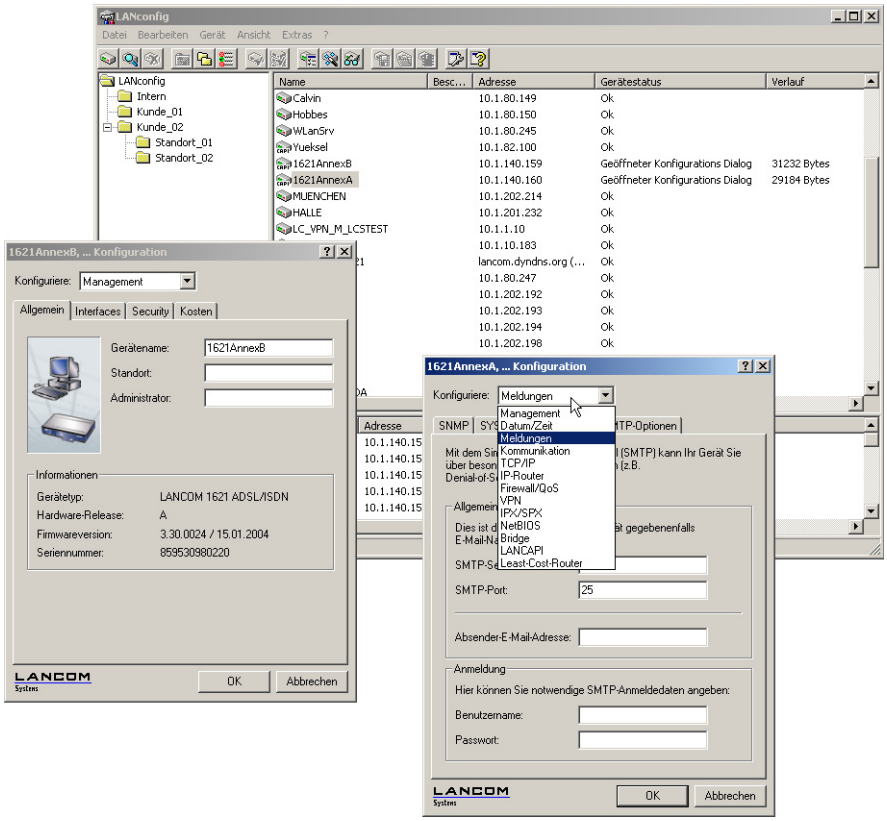
Im Einzelnen können folgende Informationen in den Spalten angezeigt werden:

- Gerätename
- Beschreibung
- Adresse
- Gerätestatus
- Verlauf
- Gerätetyp
- Hardware-Release
- Seriennummer
- MAC-Adresse
- Firmwareversion (aktive)
- Firmsafe
- 1. Image Version
- 2. Image Version



3.4.9 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 “Cut and Paste” über die Zwischenablage übertragen werden.

Beim Multithreading können sowohl 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.

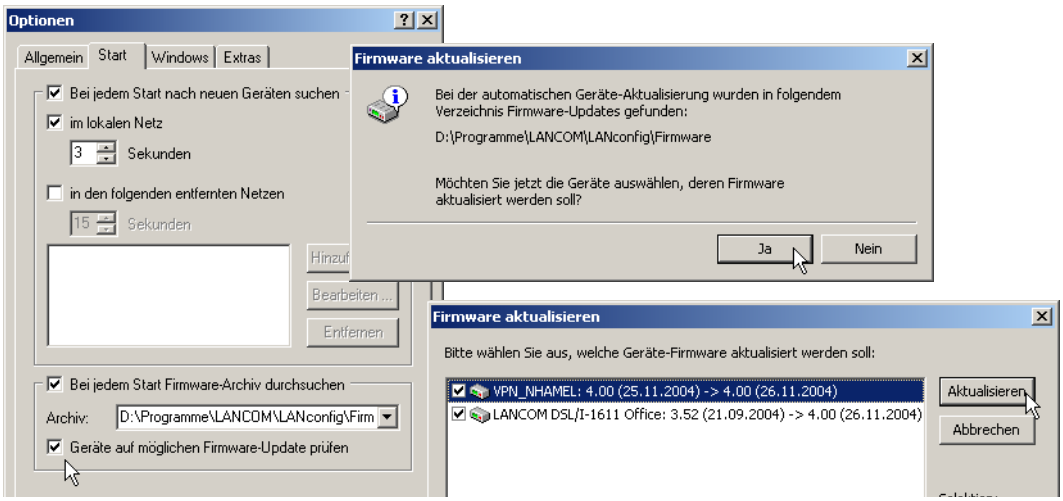
3.4.10 Manuelle und automatische Suche nach Firmware-Updates

Um das Update auf neue Firmwareversionen in den LANCOM-Geräten möglichst komfortabel zu gestalten, werden die Firmware-Dateien für die verschiedenen LANCOM-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.

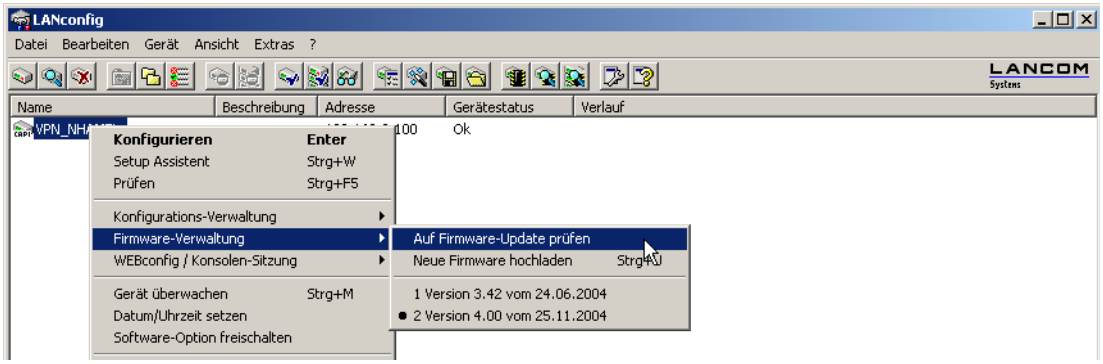
Automatische Suche nach Firmware-Updates

Das Verzeichnis, in dem LANconfig nach den Updates suchen soll, stellen Sie unter **Extras** ▶ **Optionen** ▶ **Extras** ein. Zusätzlich können Sie hier angeben, ob LANconfig nach jedem Start das Firmware-Archiv durchsuchen und die gefundenen Geräte auf mögliche Updates prüfen soll. Wenn Sie diese Optionen aktivieren, 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** ▶ **Auf Firmware-Updates prüfen**. Wenn Sie mehrere Geräte gleichzeitig updaten möchten, erscheint der Punkt **Auf Firmware-Updates prüfen** 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.

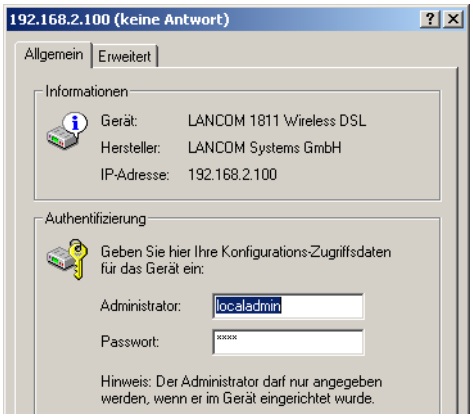


3.4.11 Passwortschutz für SNMP-Lesezugriff

Der Lesezugriff auf ein LANCOM-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.

LANmonitor

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.

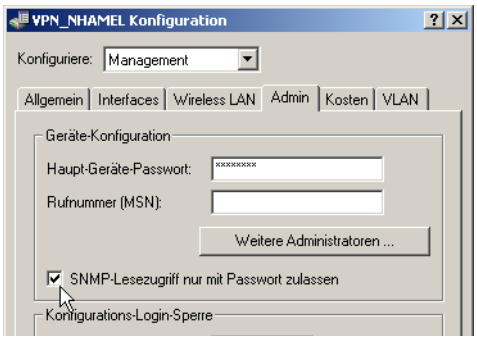


Die Zugriffsrechte im LANmonitor sind abhängig von den Rechten des Benutzers:

- Ein Supervisor hat vollen Zugriff auf die Informationen im LANmonitor und kann u.a. Aktionen ausführen wie das Trennen von Verbindungen.
- Ein lokaler Administrator hat ebenfalls vollen Zugriff auf die Informationen im LANmonitor und kann u.a. Aktionen ausführen wie das Trennen von Verbindungen.
- Ein Benutzer, der nur über Leserechte verfügt, kann die Informationen im LANmonitor ablesen, aber keine Aktionen wie das Trennen von Verbindungen ausführen.
- Ein Benutzer ohne Rechte hat keinen SNMP-Zugriff auf die Geräte-Informationen.

LANconfig

Bei der Konfiguration mit LANconfig finden Sie den Schalter für den SNMP-Lesezugriff im Konfigurationsbereich 'Management' auf der Registerkarte 'Allgemein':



WEBconfig: LCOS-Menübaum ▶ Setup ▶ Config-Modul ▶ Passw.Zwang-fuer-SNMP-lesezugriff

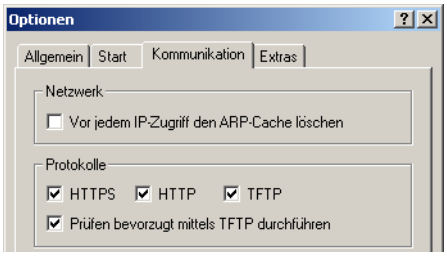
3.4.12 Gerätespezifische Einstellung der Kommunikationsprotokolle

Normalerweise werden alle Geräte-Aktionen unter LANconfig über das TFTP-Protokoll durchgeführt. Da dieses Protokoll bei der Übertragung großer Datenmengen Nachteile gegenüber anderen Protokollen hat, können alternativ auch die Protokolle HTTPS und HTTP verwendet werden.

Die Verwendung der Protokolle kann sowohl global für alle von einem LANconfig verwalteten Geräte als auch für jedes Gerät spezifisch eingestellt werden. Die globalen Einstellungen überschreiben dabei die spezifischen Einstellungen – bei den spezifischen Geräteeinstellungen kann also nur das wirksam werden, was in der globalen Konfiguration erlaubt ist.

Konfiguration der globalen Kommunikationseinstellungen

Bei der Einstellung der Kommunikationsprotokolle wird das Protokoll für das reine Prüfen des Gerätes und für andere Operationen wie z.B. einen Firmware-Upload etc. unterschieden:



LANconfig: Extras ▶ Optionen ▶ Kommunikation

- **HTTPS, HTTP, TFTP**

  Mit dieser Auswahl werden die einzelnen Protokolle für die Operationen Firmware-Upload sowie Konfigurations- und Script-Upload und -Download aktiviert. Bei diesen Operationen versucht LANconfig diese Protokolle in der Reihenfolge HTTPS, HTTP und TFTP zu verwenden. Schlägt die Übertragung nach dem gewählten Protokoll fehl, wird automatisch das nächste Protokoll versucht.

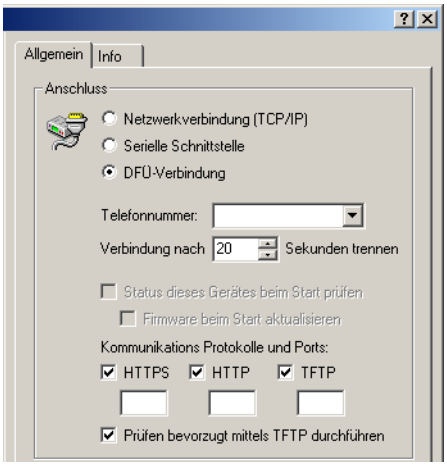
- **Prüfen bevorzugt mittels TFTP durchführen**

  Beim Prüfen der Geräte werden mit den Systeminformationen nur geringe Datenmengen übertragen. Gerade im LAN kann also die Geräteprüfung durchaus mit dem TFTP-Protokoll durchgeführt werden. Wenn diese Option aktiviert ist, wird zum Prüfen der Geräte zunächst das TFTP-Protokoll verwendet, unabhängig von den zuvor eingestellten Kommunikationsprotokollen. Schlägt die Prüfung über TFTP fehl, werden in der Reihenfolge HTTPS und HTTP versucht.

Die globalen Kommunikationseinstellungen sind den geräte-spezifischen Einstellungen übergeordnet. Auf diese Weise kann z.B. die Verwendung eines Protokolls zentral unterbunden werden.

Konfiguration der spezifischen Kommunikationseinstellungen

Zur Konfiguration der spezifischen Kommunikationseinstellungen wird der Eigenschaften-Dialog eines Gerätes über das Kontext-Menü (rechte Maustaste) geöffnet:



- **HTTPS, HTTP, TFTP**

  Auswahl der Kommunikationsprotokolle wie bei den globalen Einstellungen beschrieben.

  In den Feldern unter den Protokollen kann der zu verwendende Port eingetragen werden bei folgenden Defaultwerten:

  - HTTPS: 443
  - HTTP: 80
  - TFTP: 69

- **Prüfen bevorzugt mittels TFTP durchführen**

  Bevorzugtes Prüfen über TFTP wie bei den globalen Einstellungen beschrieben.

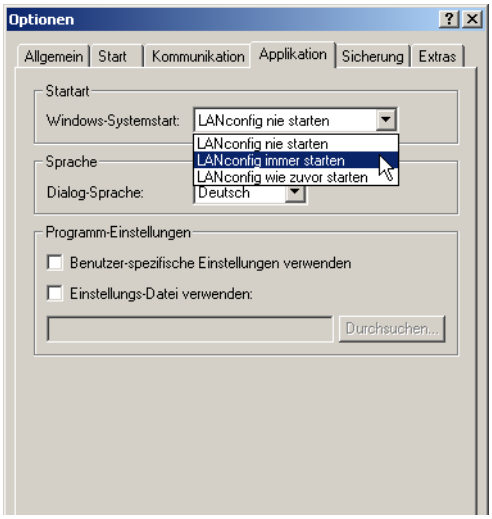
Für alle spezifischen Kommunikationseinstellungen gelten die globalen Einstellungen als übergeordnet. Ein Protokoll kann für die Operationen eines Gerätes also nur genutzt werden, wenn es auch in den globalen Einstellungen aktiviert ist.

3.4.13 Verhalten von LANconfig beim Start von Windows

LANconfig kann beim Start des Betriebssystems automatisch gestartet werden.

Konfiguration des Startverhaltens von LANconfig

Zur Konfiguration des Startverhaltens von LANconfig stehen folgende Parameter bereit:



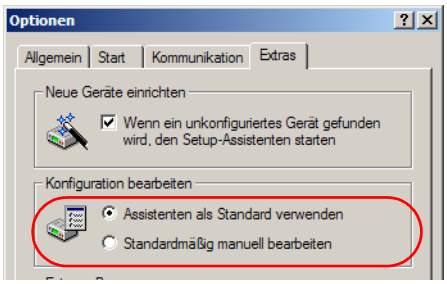
LANconfig: Optionen ▶ Extras ▶ Applikation

- **Windows-Systemstart**
  - □ LANconfig nie starten: LANconfig startet nicht automatisch mit dem Betriebssystem, sondern muss manuell gestartet werden.
  - □ LANconfig immer starten: LANconfig startet immer automatisch nach dem erfolgreichen Start des Betriebssystems.
  - □ LANconfig wie zuvor starten: LANconfig startet in dem Zustand, in dem die Anwendung beim Herunterfahren des Betriebssystems war: war LANconfig aktiv, wird es wieder gestartet, war LANconfig nicht aktiv, wird es auch nicht automatisch gestartet.

Beim Wechsel auf eine Einstellung, die ein automatisches Starten von LANconfig ermöglichen, wird ein Eintrag in der Registry des Betriebssystems vorgenommen. Persönliche Firewalls auf dem Rechner oder die Betriebssysteme selbst (Windows XP oder Windows Vista™) können diesen Eintrag ggf. als Angriff deuten und eine Warnung ausgeben bzw. den Eintrag verhindern. Um das gewünschte Startverhalten von LANconfig zu ermöglichen, können Sie diese Warnungen ignorieren bzw. die entsprechenden Aktionen zulassen.

3.4.14 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.

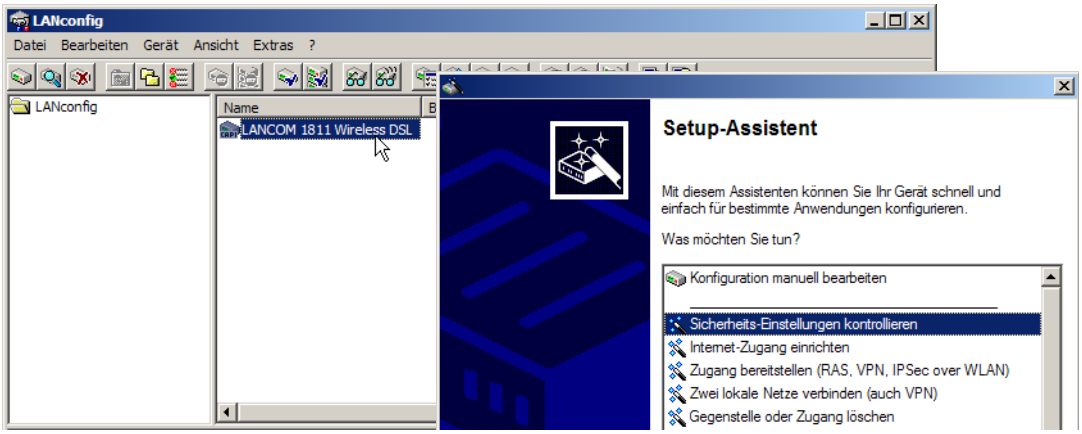


Das Standardverhalten von LANconfig kann im Dialog **Extras** ▶ **Optionen** auf der Registerkarte 'Extras' festgelegt werden.

LANconfig: Extras ▶ Optionen ▶ Extras

■ **Konfiguration bearbeiten**

□ Assistent als Standard verwenden: startet beim Doppelklick auf den Geräte-Eintrag in LANconfig den Auswahldialog für die Assistenten. Alternativ kann in diesem Dialog die Option 'Konfiguration manuell bearbeiten' gewählt werden.



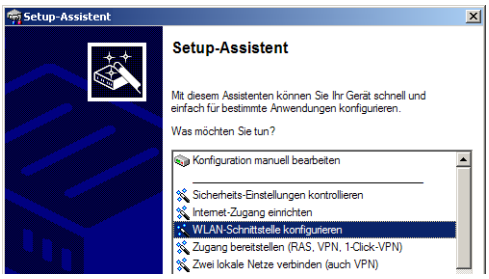
□ Standardmäßig manuell bearbeiten: startet beim Doppelklick auf den Geräte-Eintrag in LANconfig den Dialog zur manuellen Konfigurationsbearbeitung.

3.4.15 WLAN-Konfiguration mit dem Assistenten von LANconfig

Zur WLAN-Konfiguration der LANCOM Access Points stehen Ihnen komfortable Installations-Assistenten zur Verfügung.

Die Einstellungen betreffen sowohl allgemeine, übergreifende Parameter als auch die jeweiligen Einstellungen einer oder mehrerer logischer WLAN-Netzwerke (WLAN-Funkzellen oder SSIDs).

① Markieren Sie Ihren LANCOM Access Point im Auswahlfenster von LANconfig. Wählen Sie aus der Befehlsleiste den Punkt **Extras ▶ Setup Assistent**.



② Wählen Sie im Auswahlmenü den Setup-Assistenten **WLAN-Schnittstelle konfigurieren** und bestätigen Sie die Auswahl mit **Weiter**.

③ Nehmen Sie mit Hilfe des Assistenten die gewünschten Einstellungen vor wie in den folgenden Abschnitten beschrieben.

Ländereinstellungen

Der Betrieb von WLAN-Karten ist international nicht einheitlich geregelt. Die Verwendung von bestimmten Funkkanälen ist z.B. in manchen Ländern nicht erlaubt. Um den Betrieb der LANCOM Access Points auf die in dem jeweiligen Land zulässigen Parameter zu begrenzen, wird für alle physikalischen WLAN-Interfaces gemeinsam das Land eingestellt, in dem der Access Point betrieben wird.

Betriebsart der WLAN-Module

Die WLAN-Module können in verschiedenen Betriebsarten genutzt werden:

- Als Basisstation (Access Point-Modus) stellt das Gerät für die WLAN-Clients die Verbindung zu einem kabelgebundenen LAN her. Parallel dazu sind Punkt-zu-Punkt-Verbindungen möglich.
- Auch im Managed-Modus binden die Access Points WLAN-Clients in das Netzwerk ein – in dieser Betriebsart sind die Geräte allerdings Teilnehmer in einer WLAN-Infrastruktur, die von einem zentralen WLAN-Controller konfiguriert wird. In dieser Betriebsart ist keine weitere WLAN-Konfiguration erforderlich, alle WLAN-Parameter werden vom WLAN-Controller übermittelt.
- Als Client sucht das Gerät selbst die Verbindung zu einem anderen Access Point und versucht sich in einem Funknetzwerk anzumelden. In diesem Fall dient das Gerät also z.B. dazu, ein kabelgebundenes Gerät über eine Funk-

strecke an eine Basisstation anzubinden. In dieser Betriebsart sind parallele Punkt-zu-Punkt-Verbindungen **nicht** möglich.

Weitere Informationen finden Sie im Abschnitt → Client-Modus.

Bei Geräten mit zwei WLAN-Modulen kann die Betriebsart für jedes Modul separat festgelegt werden, d.h. das eine WLAN-Modul kann im Managed-Modus, ein anderes z.B. als autarker Access Point betrieben werden.

Physikalische WLAN-Einstellungen

Neben dem verwendeten Funkkanal können Sie bei den physikalischen WLAN-Einstellungen Optionen wie die Bündelung von WLAN-Paketen (TX-Burst), die Hardwarekompression oder die Nutzung von QoS nach 802.11e aktivieren. Außerdem nehmen Sie hier die Einstellungen für das Diversity-Verhalten vor.

Logische WLAN-Netzwerke

Jedes WLAN-Modul kann bis zu acht logische WLAN-Netzwerke aufspannen, in dem sich mobile WLAN-Clients anmelden können. Zur Konfiguration eines logischen WLAN-Netzwerks werden die folgenden Parameter abgefragt:

- Der Netzwerkname (SSID)
- Offenes oder geschlossenes Funk-LAN
- Verschlüsselungseinstellungen
- MAC-Filter
- Client-Bridge-Betrieb
- Filtereinstellungen

Punkt-zu-Punkt-Einstellungen

Bei der Konfiguration der P2P-Verbindungen wird neben der Betriebsart auch der Stationsname eingestellt, über den die Access Points eine Verbindung aufbauen können. Außerdem wird hier die Position als „Master" oder „Slave" festgelegt.

Neben den Einstellungen für den Access Point selbst wird auch definiert, zu welcher Gegenstelle der Access Point über die P2P-Verbindung Kontakt aufnehmen kann.

Weitere Informationen finden Sie im Abschnitt → Punkt-zu-Punkt-Verbindungen.

3.5 Gruppen-Konfiguration mit LANconfig

Bei der Verwaltung vieler Geräte ist es hilfreich, eine Auswahl an Konfigurations-Parametern gleichzeitig in eine Gruppe von Geräten einzuspielen, statt die Parameter einzeln in jedem Gerät manuell zu setzen, z.B. bei identischen Clientberechtigungen in WLAN-Access-Points. Das Importieren einer kompletten Konfigurationsdatei eines Gerätes ist insofern nicht sinnvoll, da hierbei gerätespezifische Parameter wie die IP-Adresse ebenfalls übernommen werden. Die Gruppen-Konfiguration von LANconfig ermöglicht das einfache Importieren von Teil-Konfigurationsdateien und damit das gleichzeitige Verwalten mehrerer Geräte.

Die Teil-Konfigurationsdateien mit den gemeinsamen Parametern für eine Gruppe von LANCOM-Geräten werden wie komplette Konfigurationsdateien auf der Festplatte oder einem Server gespeichert. Für die Konfiguration von ganzen Geräte-Gruppen werden unter LANconfig Verweise auf diese Teil-Konfigurationsdateien angelegt, die eine komfortable Verbindung zwischen den Geräteeinträgen in LANconfig und den Teil-Konfigurationsdateien herstellen.

Die Gruppenkonfiguration wird für LANCOM-Geräte mit einer Firmware LCOS 5.00 oder höher unterstützt.

In der LCOS-Version 5.00 werden zunächst Gruppen-Konfigurationen für WLAN-Geräte unterstützt. In späteren Firmware-Versionen werden auch andere Gruppen-Konfigurationen (z.B. für die VPN-Parameter) unterstützt. Informieren Sie sich auf der LANCOM-Webseite www.lancom.de über aktuelle Firmware-Versionen mit erweiterten Möglichkeiten der Gruppen-Konfiguration.

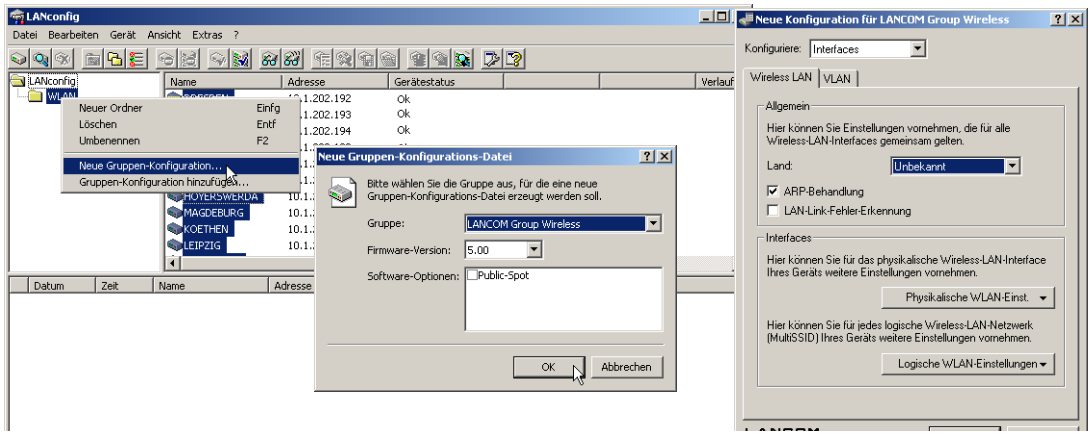
3.5.1 Anlegen einer Gruppen-Konfiguration

Voraussetzung für die Verwendung der Gruppenkonfiguration ist die Gruppierung der Geräte in Ordnern. Diese LANconfig-Ordner enthalten die Geräteeinträge, für die eine gemeinsame Teilkonfiguration sinnvoll ist sowie die Gruppen-Konfigurationen als Verweise zu den Teil-Konfigurationsdateien.

Gruppen-Konfiguration mit neuer Teil-Konfigurationsdatei

① Legen Sie einen neuen Ordner an und verschieben Sie die zu gruppierenden Geräte mit der Maus in diesen neuen Ordner.

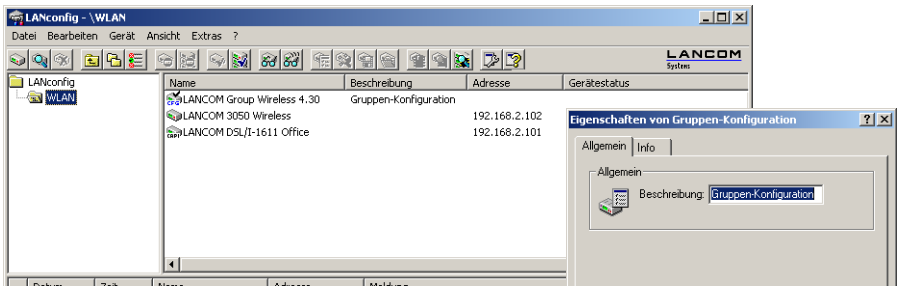
② Klicken Sie anschließend mit der rechten Maustaste auf den neuen Ordner und wählen Sie im Kontextmenü den Eintrag **Neue Gruppen-Konfiguration...**. Nach der Auswahl des Gruppen-Typs und der Firmwareversion öffnet sich der Konfigurationsdialog von LANconfig mit reduzierten Konfigurationsmöglichkeiten.



③ Stellen Sie in der Konfiguration die Parameter so ein, wie sie für die gesamte Gruppe gelten sollen. Beim Schließen des Konfigurationsdialogs fordert LANconfig Sie auf, die entsprechende Teil-Konfigurationsdatei an einem beliebigen Ort zu speichern.

Die Gruppen-Konfiguration speichert alle Parameter in eine Teil-Konfigurationsdatei. Dabei werden auch die Parameter mit den Standardwerten gespeichert, die nicht geändert wurden. Verwenden Sie die Scripting-Funktionen ('Scripting' → Seite 4-13), um nur die von der Standardeinstellung abweichenden Parameter aus dem Gerät auszulesen und ggf. auf andere Geräte zu übertragen.

④ Der Verweis zur Teil-Konfigurationsdatei erscheint in der Liste der Einträge mit der Beschreibung 'Gruppen-Konfiguration'. Der Name der Gruppen-Konfiguration kann über die Eigenschaften geändert werden. Klicken Sie dazu den Eintrag mit der rechten Maustaste und wählen Sie im Kontextmenü den Eintrag **Eigenschaften**.



Die Gruppen-Konfiguration ist ein Verweis auf die Teil-Konfigurationsdatei. Beachten Sie, dass Änderungen der Teil-Konfigurationsdatei auch Änderungen der jeweiligen Gruppen-Konfiguration zur Folge haben.

Bestehende Teil-Konfigurationsdatei verwenden

In manchen Fällen ist es sinnvoll, die mit LANconfig verwalteten Geräte anders in Ordnern zu strukturieren, als es die Gruppen-Konfiguration erfordern würde. Die Geräte in standortspezifischen Ordnern können z.B. durchaus mit den gleichen Gruppen-Konfigurationen eingestellt werden. Um nicht für jeden Ordner redundant die gleichen Teil-Konfigurationsdateien zu erstellen, können in mehreren Ordnern Verweise auf eine gemeinsame Teil-Konfigurationsdatei erstellt werden.

① Um eine vorhandene Teil-Konfigurationsdatei für eine Gruppen-Konfiguration zu verwenden, klicken Sie mit der rechten Maustaste auf den gewünschten Ordner und wählen im Kontextmenü den Eintrag **Gruppen-Konfiguration hinzufügen...**.

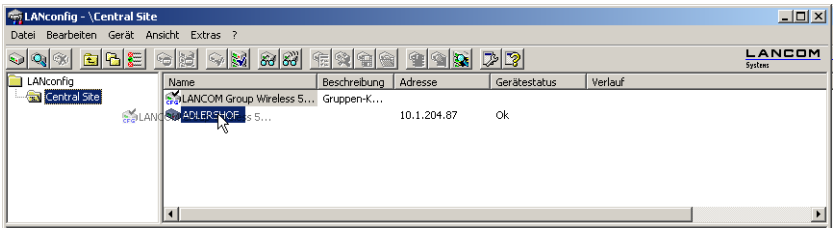
② Wählen Sie im folgenden Dialog die bereits bestehende Teil-Konfigurationsdatei aus und erstellen Sie so in dem Ordner einen Verweis auf diese Datei.

Beachten Sie, dass Änderungen der Teil-Konfigurationsdatei auch Änderungen der jeweiligen Gruppen-Konfigurationen in verschiedenen Ordnern zur Folge haben.

3.5.2 Gerätekonfigurationen 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'.



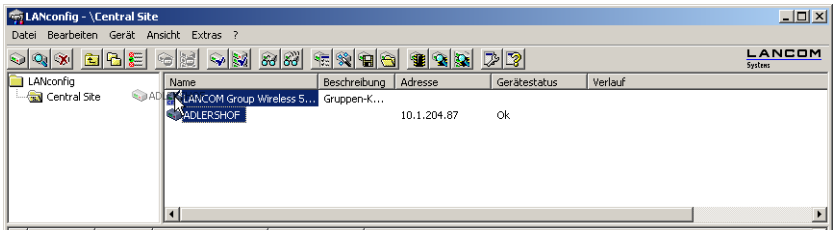
Es ist auch möglich, die Teil-Konfiguration eines Gerätes als Gruppen-Konfiguration zu verwenden. Ziehen Sie hierzu den Geräteeintrag auf den Gruppen-Konfigurationseintrag.

3.5.3 Gruppen-Konfigurationen aktualisieren

Neben dem manuellen Verändern der Parameter einer Gruppen-Konfiguration 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.

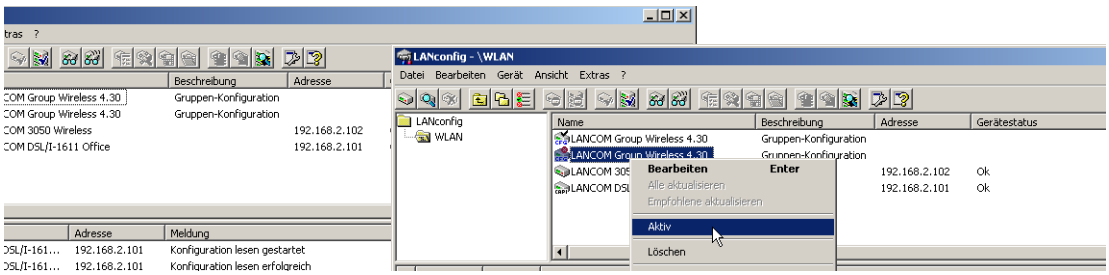
Beim folgenden Prüfen der Geräte wird LANconfig feststellen, dass die Konfigurationen der anderen Geräte im Ordner nicht mehr mit der neuen Gruppen-Konfiguration übereinstimmen und dies über den Gerätestatus entsprechend anzeigen.



3.5.4 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** 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!



3.5.5 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.

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** ▶ **Konfigurationsverwaltung** ▶ **Als Datei sichern**.

③ Trennen Sie das Ausgangsgerät vom Netzwerk, um Adresskonflikte zu vermeiden.

④ Spielen Sie die Konfiguration über **Gerät** ▶ **Konfigurationsverwaltung** ▶ **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.

3.6 LANmonitor – wissen, was läuft

Mit dem Überwachungstool LANmonitor können Sie sich unter Windows-Betriebssystemen die wichtigsten Informationen über den Status Ihrer Router auf dem Bildschirm anzeigen lassen. Und zwar den Status aller LANCOM im Netz.

Viele der internen Meldungen der Geräte werden dabei in Klartext umgewandelt, zeigen Ihnen den aktuellen Zustand des Gerätes und helfen Ihnen bei der Fehlersuche.



Erläuterungen zu den einzelnen Meldungen im LANmonitor und Hinweise zur Abhilfe finden Sie im Anhang unter 'Übersicht über die Funktionen nach Modellen und LCOS*-Versionen' → Seite 16-14.

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 zusätzlichen Gebührenlimits.



Sie können mit LANmonitor nur solche Geräte überwachen, die Sie über IP erreichen (lokal oder remote). Über die serielle Schnittstelle können Sie einen Router mit diesem Programm nicht ansprechen.

3.6.1 Erweiterte Anzeige-Optionen

Unter **Ansicht** ▶ **Anzeigen** können Sie folgende Anzeige-Optionen ein- und ausschalten:

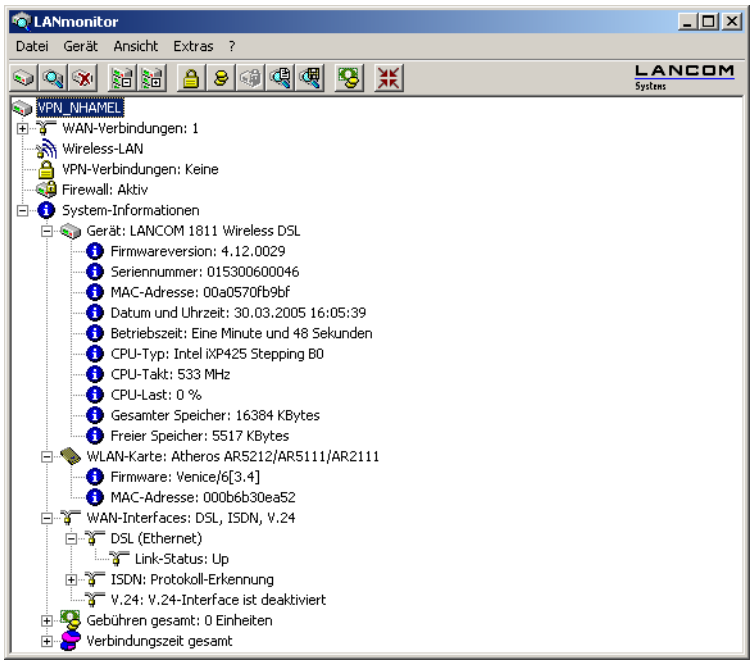
- Fehlermeldungen

- Diagnosemeldungen
- System-Informationen

Viele wichtige Details zum Status des LANCOM 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.

3.6.2 Abfrage der CPU- und Speicherauslastung über SNMP

Die CPU- und Speicherauslastung des LANCOM kann über SNMP abgefragt oder im LANmonitor angezeigt werden.



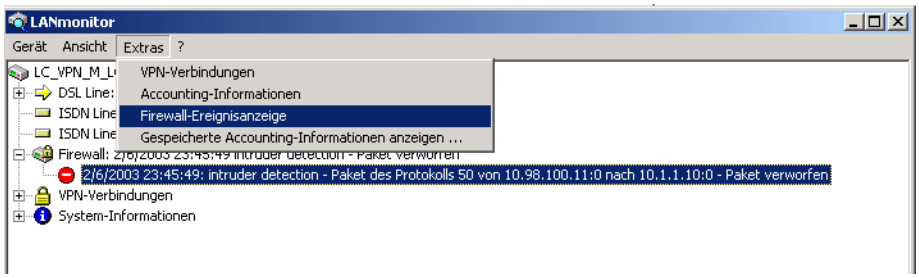
3.6.3 Internet-Verbindung kontrollieren

Als Beispiel für die Funktionen von LANmonitor zeigen wir Ihnen zuerst einmal, welche Informationen LANmonitor über den Verbindungsaufbau zu Ihrem Internet-Provider bereitstellt.

① Starten Sie LANmonitor mit **Start** ▶ **Programme** ▶ **LANCOM** ▶ **LANmonitor**. Legen Sie mit **Datei** ▶ **Gerät hinzufügen** ein neues Gerät an und geben im folgenden Fenster die IP-Adresse für den Router an, den Sie überwachen wollen. Falls die Konfiguration des Gerätes mit einem Passwort gesichert ist, geben Sie dieses gleich mit ein.

Alternativ können Sie über LANconfig das Gerät auswählen und mit **Gerät** ▶ **Gerät überwachen** die Überwachung für ein Gerät starten.

② LANmonitor legt automatisch einen neuen Eintrag in der Geräteliste an und zeigt zunächst den Zustand der Übertragungskanäle. Starten Sie Ihren Web-Browser, und geben Sie eine beliebige Webseite ein. LANmonitor zeigt nun an, wie auf einem Kanal eine Verbindung aufgebaut wird 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.

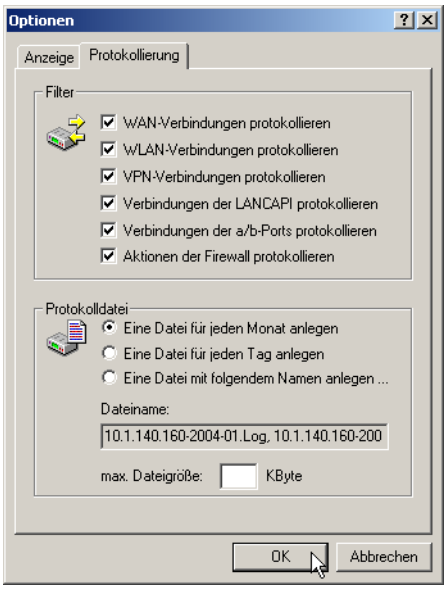


In diesem Beispiel können Sie aus den Protokoll-Informationen zum PPP ablesen, welche IP-Adresse der Provider Ihrem Router für die Dauer der Verbindung zugewiesen hat und welche Adressen für DNS- und NBNS-Server übermittelt wurden.

Unter den allgemeinen Informationen können Sie beobachten, mit welchen Übertragungsraten aktuell Daten mit dem Internet ausgetauscht werden.

③ Durch einen Klick mit der rechten Maustaste auf den aktiven Kanal können Sie die Verbindung manuell trennen. Dazu benötigen Sie ggf. das Konfigurationspasswort.

④ Wenn Sie ein Protokoll der LANmonitor-Ausgaben in Form einer Datei wünschen, starten Sie das Aktivitätsprotokoll mit **Gerät ▶ Aktivitätsprotokoll**. Öffnen Sie mit **Extras ▶ Optionen** den Dialog für die Einstellungen des Aktivitätsprotokolls.



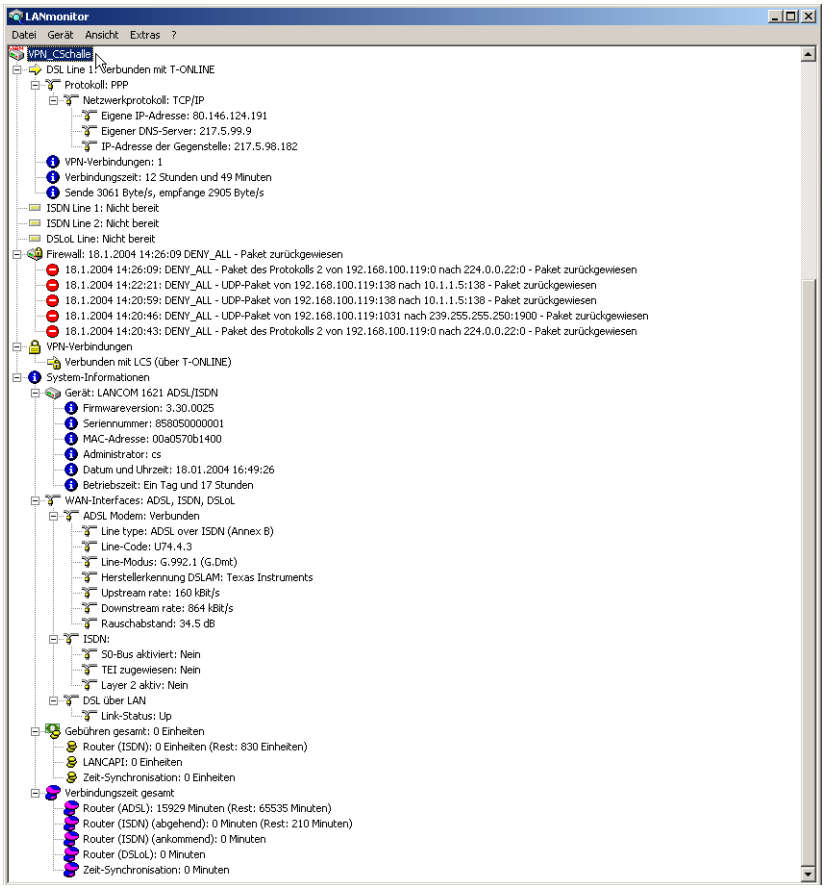
Auf der Registerkarte 'Protokollierung'. können Sie die folgenden Aktivitäten für die Protokollierung auswählen:

- WAN-Verbindungen
- WLAN-Verbindungen
- VPN-Verbindungen
- LANCAPI-Verbindungen
- a/b-Port-Verbindungen
- Firewall-Aktionen

Zusätzlich stellen Sie hier ein, ob LANmonitor täglich, monatlich oder fortlaufend eine Protokolldatei erstellt und wo diese gespeichert wird.

3.6.4 Anzeige-Funktionen im LANmonitor

LANmonitor unterstützt den Administrator von umfangreichen LANCOM-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:

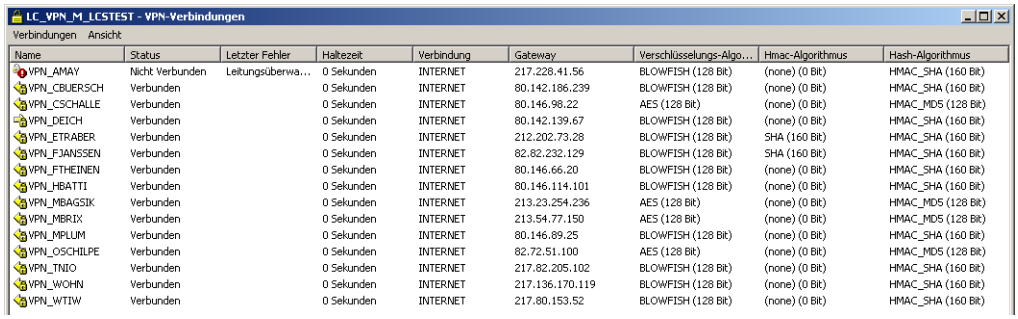


Zu den Informationen, die in der Übersicht abgelesen werden können, gehören u.a. die Details über die aktiven WAN-Verbindungen, die letzten fünf Meldungen der Firewall, die aktuellen VPN-Verbindungen, sowie die Systeminformationen mit Gebühren und Verbindungszeiten.

Mit einem rechten Mausklick auf die Geräte im LANmonitor können im Kontextmenü Listen mit weiteren Informationen aufgerufen werden:

- VPN-Verbindungen

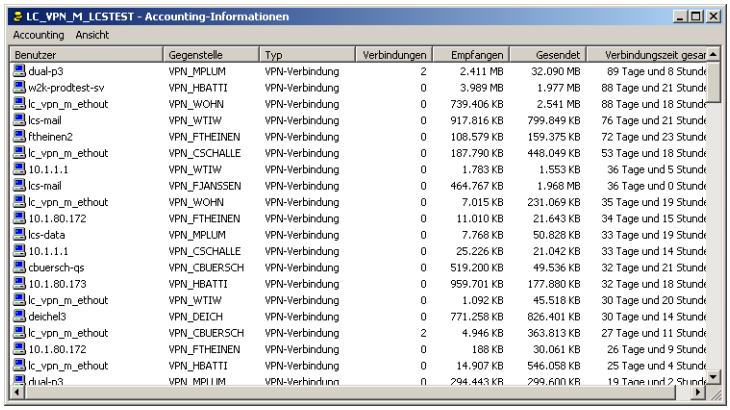
  In der Liste der VPN-Verbindungen werden die letzten 100 VPN-Verbindungen protokolliert. Dabei werden u.a. folgende Detailinformationen erfasst



Name	Status	Letzter Fehler	Haltezeit	Verbindung	Gateway	Verschlüsselungs-Algo…	Hmac-Algorithmus	Hash-Algorithmus
VPN_AMAY	Nicht Verbunden	Leitungsüberwa…	0 Sekunden	INTERNET	217.228.41.56	BLOWFISH (128 Bit)	(none) (0 Bit)	HMAC_SHA (160 Bit)
VPN_CBUERSCH	Verbunden		0 Sekunden	INTERNET	80.142.186.239	BLOWFISH (128 Bit)	(none) (0 Bit)	HMAC_SHA (160 Bit)
VPN_CSCHALLE	Verbunden		0 Sekunden	INTERNET	80.146.98.22	AES (128 Bit)	(none) (0 Bit)	HMAC_MD5 (128 Bit)
VPN_DEICH	Verbunden		0 Sekunden	INTERNET	80.142.139.67	BLOWFISH (128 Bit)	(none) (0 Bit)	HMAC_SHA (160 Bit)
VPN_ETRABER	Verbunden		0 Sekunden	INTERNET	212.202.73.28	BLOWFISH (128 Bit)	SHA (160 Bit)	HMAC_SHA (160 Bit)
VPN_FJANSSEN	Verbunden		0 Sekunden	INTERNET	82.82.232.129	BLOWFISH (128 Bit)	SHA (160 Bit)	HMAC_SHA (160 Bit)
VPN_FTHEINEN	Verbunden		0 Sekunden	INTERNET	80.146.66.20	BLOWFISH (128 Bit)	(none) (0 Bit)	HMAC_SHA (160 Bit)
VPN_HBATTI	Verbunden		0 Sekunden	INTERNET	80.146.114.101	BLOWFISH (128 Bit)	(none) (0 Bit)	HMAC_SHA (160 Bit)
VPN_MBAGSIK	Verbunden		0 Sekunden	INTERNET	213.23.254.236	AES (128 Bit)	(none) (0 Bit)	HMAC_MD5 (128 Bit)
VPN_MBRIX	Verbunden		0 Sekunden	INTERNET	213.54.77.150	AES (128 Bit)	(none) (0 Bit)	HMAC_MD5 (128 Bit)
VPN_MPLUM	Verbunden		0 Sekunden	INTERNET	80.146.89.25	BLOWFISH (128 Bit)	(none) (0 Bit)	HMAC_SHA (160 Bit)
VPN_OSCHILPE	Verbunden		0 Sekunden	INTERNET	82.72.51.100	AES (128 Bit)	(none) (0 Bit)	HMAC_MD5 (128 Bit)
VPN_TNIO	Verbunden		0 Sekunden	INTERNET	217.82.205.102	BLOWFISH (128 Bit)	(none) (0 Bit)	HMAC_SHA (160 Bit)
VPN_WOHN	Verbunden		0 Sekunden	INTERNET	217.136.170.119	BLOWFISH (128 Bit)	(none) (0 Bit)	HMAC_SHA (160 Bit)
VPN_WTIW	Verbunden		0 Sekunden	INTERNET	217.80.153.52	BLOWFISH (128 Bit)	(none) (0 Bit)	HMAC_SHA (160 Bit)

  - □ Name der Gegenstelle
  - □ aktueller Status
  - □ letzte Fehlermeldung
  - □ IP-Adresse des Gateways
  - □ Verschlüsselungsinformationen
- Accounting-Informationen

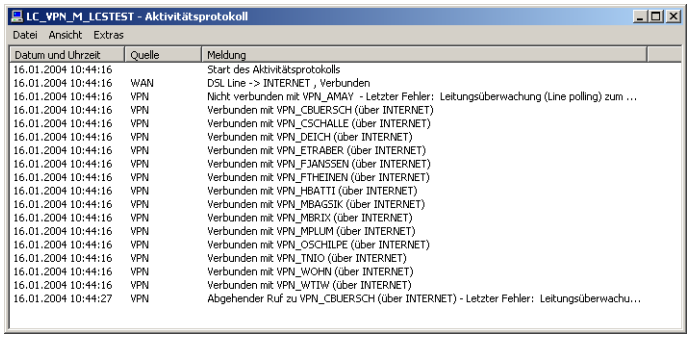
  Mit den Accounting-Informationen werden die Verbindungen der einzelnen Stationen im LAN zu den erreichbaren Gegenstellen im WAN protokolliert. Dabei werden u.a. folgende Detailinformationen erfasst:



- □ Name bzw. IP-Adresse der Station
- □ Gegenstelle, über die eine Verbindung aufgebaut wurde
- □ Typ der Verbindung, also z.B. DSL- oder VPN-Verbindung
- □ Anzahl der Verbindungen
- □ gesendetes bzw. empfangenes Datenvolumen
- □ Verbindungszeit

■ Aktivitätsprotokoll

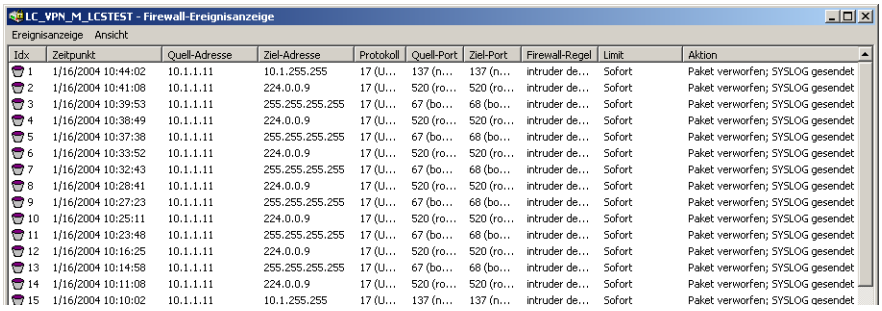
Mit dem Aktivitätsprotokoll werden die Aktivitäten auf WAN-, WLAN-, VPN-, LANCAPI- und a/b-Port-Verbindungen sowie der Firewall protokolliert. Dabei werden u.a. folgenden Detailinformationen erfasst



- □ Datum und Uhrzeit
- □ Quelle
- □ Meldung

■ Firewall-Ereignisanzeige

Mit der Firewall-Ereignisanzeige werden die letzten 100 Aktionen der Firewall protokolliert. Dabei werden u.a. folgende Detailinformationen erfasst

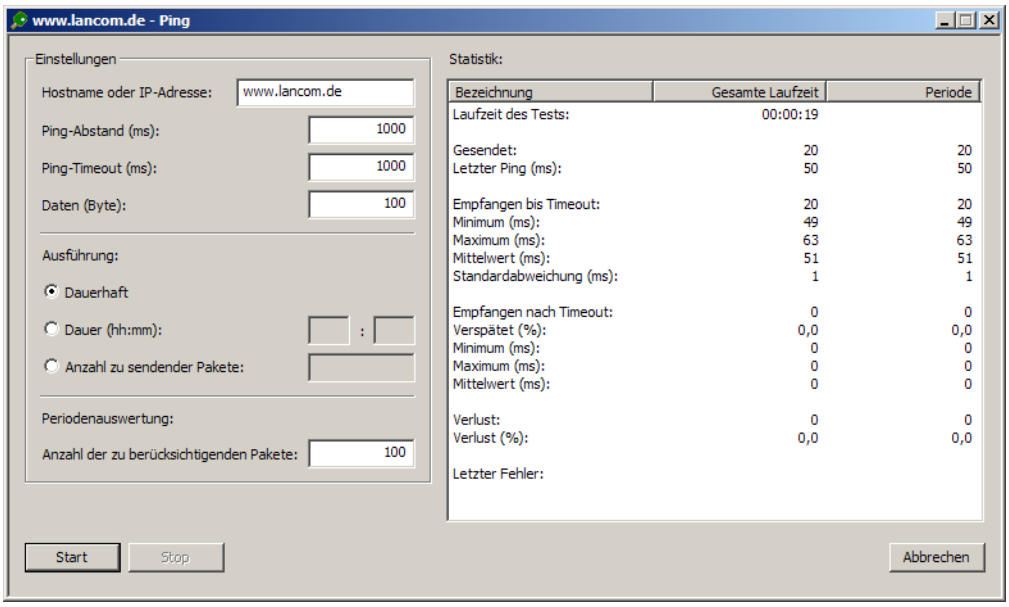


- □ Zeitpunkt
- □ Quell- und Zieladresse
- □ Protokoll mit Quell- und Ziel-Port
- □ auslösende Firewall-Regel und überschrittenes Limit
- □ ausgeführte Aktion

3.6.5 Überprüfung der Verbindungsqualität mit dem LANmonitor

Mit dem LANmonitor kann die Qualität der Verbindung zu Gegenstellen in LAN, WAN oder WLAN geprüft werden. 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 dient ein eigener Dialog, der aus dem LANmonitor heraus aufgerufen werden kann.



LANconfig: Gerät ▶ Ping ...

LANconfig: Extras ▶ Ping ... oder über Kontextmenü

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.

- **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 Paketegröße der IP-Pakete überschritten wird, werden die Pakete fragmentiert.

- **Ausführung**

  Wiederholungsmodus für den Ping-Befehl.

Auswertung

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.

Folgende Daten werden zur Auswertung angezeigt:

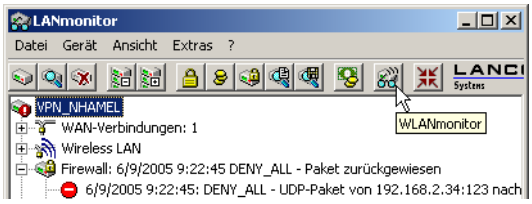
- **Laufzeit des Tests**
  - gesamte Laufzeit [Std. / Min. / Sek.]
- **Gesendet**
  - Gesamte Anzahl der gesendeten Pings
  - Laufzeit des letzten Pings [ms]
- **Empfangen bis Timeout**
  - Anzahl der Pings, die im Timeout-Zeitraum beantwortet wurden
  - Minimale Laufzeit
  - Maximale Laufzeit
  - Mittelwert
  - 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**
  - Anzahl der verlorenen Pakete
  - Anteil der verlorenen Pakete an der Gesamtzahl

3.7 Visualisierung großer WLANs mit dem WLANmonitor

Mit dem LANCOM WLANmonitor können Sie zentral den Status eines drahtlosen Netzwerkes (WLAN) überwachen. Es stehen sowohl Informationen über das gesamte Netzwerk als auch Detailinformationen zu einzelnen Access-Points und zu eingeloggten Clients zur Verfügung. Zudem bietet der LANCOM 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.

3.7.1 Start des LANCOM WLANmonitors

Der WLANmonitor ist Bestandteil des LANmonitor. Starten Sie den WLANmonitor aus dem LANmonitor über den Menüpunkt **Extras ▶ WLANmonitor**, über den entsprechenden Button in der LANmonitor-Buttonleiste oder direkt über **Start ▶ Programme ▶ LANCOM ▶ WLANmonitor**.



Alternativ kann der WLANmonitor von der Konsole aus mit dem Befehl

```
[Installationspfad]lanmon -wlan
```

gestartet werden.

3.7.2 Suche nach Access Points

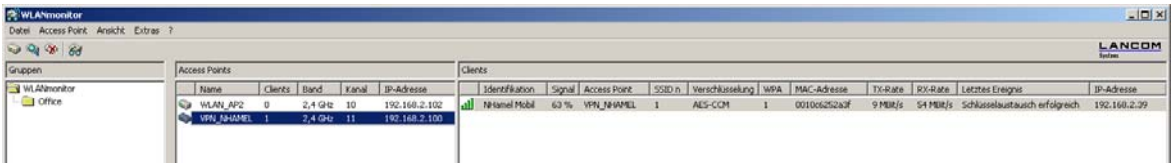
Starten Sie nach dem Start des WLANmonitors die Suche nach verfügbaren Access Points über den Menüpunkt **Datei ▶ Access-Points suchen**. In der mittleren Spalte (Access-Point-Liste) werden dann die gefundenen Access Points aufgelistet. Zusätzlich erscheinen hier die wichtigsten Basisinformationen über den Access Point:

- Name des Access Points
- Anzahl der auf ihm angemeldeten Clients
- das verwendete Frequenzband
- der verwendete Kanal
- IP-Adresse des Access Point

In der rechten Spalte (Client-Liste) werden die auf dem ausgewählten Access Point eingeloggten Clients aufgelistet. Zu jedem Client werden folgende Informationen angezeigt:

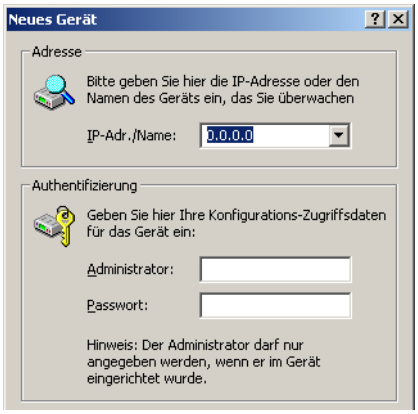
- Verbindungsqualität in Form eines Balkendiagramms
- Identifikation: Name des eingeloggten Clients, sofern dieser in der Access-Liste oder in einem RADIUS-Server eingetragen ist.

  LANconfig: **WLAN-Sicherheit ▶ Stationen ▶ Stationen**.
  Telnet: `/Setup/WLAN/Zugangsliste`
  WEBconfig: **Expertenkonfiguration ▶ Setup ▶ WLAN ▶ Zugangsliste**
- Signal: Signalstärke der Verbindung
- Access Point: Name des Access Points, auf dem der Client eingeloggt ist
- SSID: Identifikationsnummer des WLAN-Netzwerkes
- Verschlüsselung: Typ des Verschlüsselungsverfahrens der Funkverbindung
- WPA-Version (WPA-1 oder WPA-2)
- MAC-Adresse: Hardwareadresse des WLAN-Clients
- TX-Rate: Übertragungsrate beim Senden
- RX-Rate: Übertragungsrate beim Empfangen
- Letztes Ereignis, z.B. 'Authentifikation erfolgreich', 'RADIUS erfolgreich', 'Schlüsselaustausch erfolgreich'
- IP-Adresse des WLAN-Clients



3.7.3 Access Points hinzufügen

Möchten Sie einen Access Point zur Liste hinzufügen, der nicht automatisch erkannt wurde, wählen Sie den Menüpunkt **Datei ▶ Access Point hinzufügen**. Im folgenden Fenster geben Sie die IP-Adresse bzw. den Namen des Access Points und den Administratornamen sowie das zugehörige Passwort an.

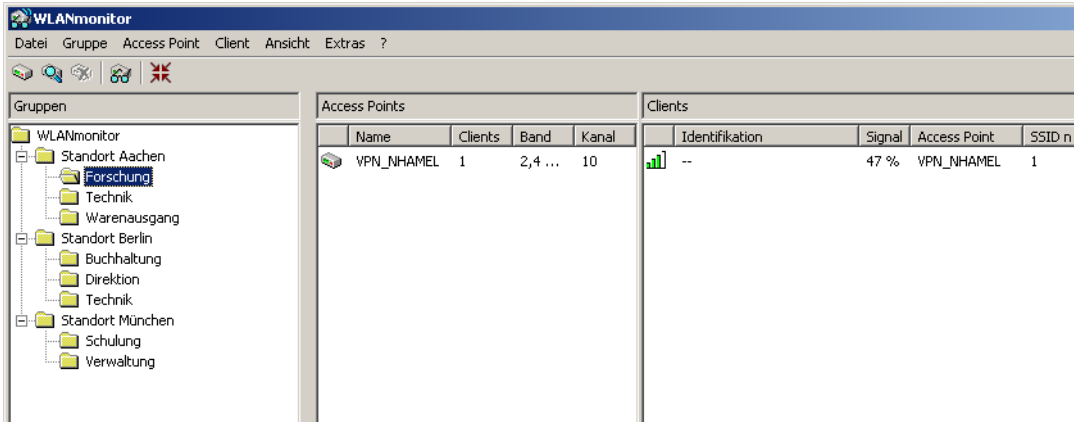


3.7.4 Access Points organisieren

Der LANCOM 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 der entsprechenden Liste 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.

3.7.5 Rogue AP und Rogue Client Detection mit dem WLANmonitor

Als Rogue bezeichnet man solche WLAN-Geräte, die unerlaubt versuchen, als Access Point oder Client Teilnehmer in einem WLAN zu werden.

- Bei Rogue Clients versuchen Rechner mit WLAN-Adapter in der Reichweite des eigenen WLAN, sich bei einem der Access Points einzubuchen, um z.B. die Internetverbindung mit zu nutzen oder Zugang zu geschützten Bereichen des Netzwerks zu erhalten.
- Rogue APs sind solche 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 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 Clients und Access Points in der Reichweite des eigenen Netzwerks eine mögliche Bedrohung und Sicherleitslücke, 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 des AirLancer Extender gespeichert. Mit der Aktivierung des Background-Scanning werden auch die benachbarten Access Points erfasst und in der Scan-Tabelle gespeichert. Mit dem WLANmonitor können diese Informationen sehr komfortabel visualisiert werden, die Access Points und Clients können dabei z.B. in Kategorien wie 'bekannt', 'unbekannt' oder 'rogue' eingeteilt werden.

Weitere Informationen finden Sie unter 'Background WLAN Scanning' → Seite 11-25.

Rogue AP Detection

Der WLANmonitor stellt alle gefundenen Access Points in vordefinierten Untergruppen von 'Rogue AP Detection' dar und zeigt dabei u.a. folgende Informationen:

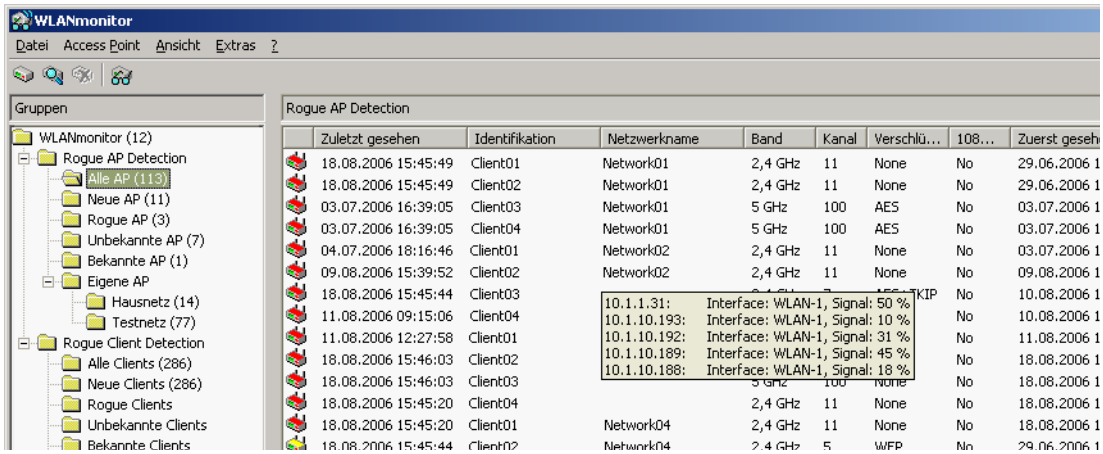
- Zeitpunkt der ersten und letzten Erkennung
- BSSID, also MAC-Adresse des AP für dieses WLAN-Netz
- Netzwerkname
- verwendete Verschlüsselung
- verwendetes Frequenzband
- verwendeter Funk-Kanal
- Verwendung des 108Mbps-Modus

Für die Nutzung der Rogue AP Detection muss im AirLancer Extender das Background Scanning aktiviert werden.

Folgende Gruppen nutzt der WLANmonitor zur Sortierung der gefundenen APs:

- Alle APs: Auflistung aller gescannter WLAN-Netze der folgenden Gruppen
- Neue APs: neue unbekannte und unkonfigurierte WLAN-Netze gelangen automatisch in diese Gruppe (die APs werden gelb dargestellt)
- Rogue APs: WLAN-Netze, die als Rogue erkannt und dringend zu beobachten sind (die APs werden rot dargestellt)
- Unbekannte APs: WLAN-Netze, bei denen weitere Untersuchungen notwendig sind (die APs werden grau dargestellt)
- Bekannte APs: WLAN-Netze, die keine Gefahr darstellen (die APs werden grau dargestellt)
- Eigene APs: neue eigene WLAN-Netze von Access Points, die der WLANmonitor beobachtet, gelangen automatisch in diese Gruppe (die APs werden grün dargestellt)

Die gefundenen WLAN-Netze können je nach Status in eine entsprechende Gruppe verschoben werden. Innerhalb der einzelnen Gruppen können über das Kontextmenü (rechte Maustaste) eigene Gruppen angelegt werden (ausgenommen der Gruppe 'Alle APs').



Wenn sich bei einem AP ein Parameter ändert, z.B. die Sicherheitseinstellung, dann wird er wieder als neu gefundener AP angezeigt.

Rogue Client Detection

Der WLANmonitor stellt alle gefundenen Clients in vordefinierten Untergruppen von 'Rogue Client Detection' dar und zeigt dabei u.a. folgende Informationen:

- Zeitpunkt der ersten und letzten Erkennung
- MAC-Adresse des Clients
- Netzwerkname

Für die Nutzung der Rogue Client Detection ist **keine** Konfiguration der AirLancer Extender erforderlich.

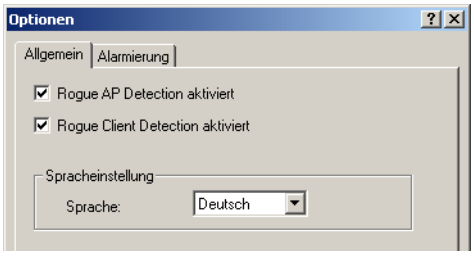
Folgende Gruppen nutzt der WLANmonitor zur Sortierung der gefundenen Clients:

- Alle Clients: Auflistung aller gesehener Clients der folgenden Gruppen (die Clients werden entsprechend der Gruppe farblich dargestellt)
- Neue Clients: neue unbekannte Clients gelangen automatisch in diese Gruppe (die Clients werden gelb dargestellt)
- Rogue Clients: Clients, die als Rogue erkannt und dringend zu beobachten sind (die Clients werden rot dargestellt)
- Unbekannte Clients: Clients, bei denen weitere Untersuchungen notwendig sind (die Clients werden grau dargestellt)
- Bekannte Clients: Clients, die keine Gefahr darstellen (die Clients werden grau dargestellt)
- Eigene Clients: neue eigene Clients, die bei Access Points assoziiert sind, die der WLANmonitor beobachtet, gelangen automatisch in diese Gruppe (die Clients werden grün dargestellt)

Die gefundenen Clients können je nach Status in eine entsprechende Gruppe verschoben werden. Innerhalb der einzelnen Gruppen können über das Kontextmenü (rechte Maustaste) eigene Gruppen angelegt werden (ausgenommen der Gruppe 'Alle Clients').

Aktivierung der Rogue AP und Rogue Client Detection

Die Nutzung der Rogue AP und Rogue Client Detection kann im WLANmonitor ein- bzw. ausgeschaltet werden.



Konfigurationstool	Aufruf
WLANmonitor	Extras ▶ Optionen ▶ Allgemein

- **Rogue AP Detection aktiviert**

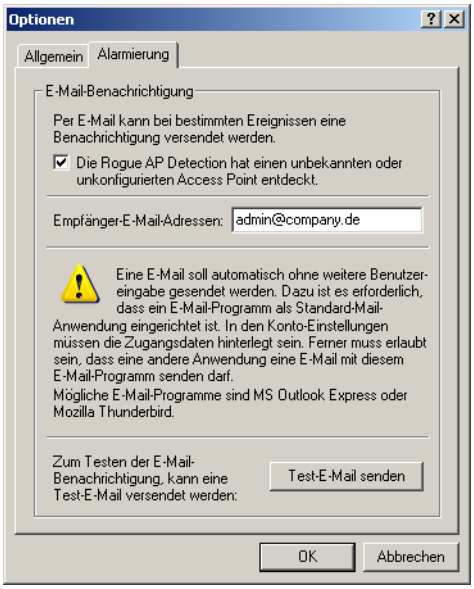
  Aktivieren Sie diese Option, wenn der WLANmonitor unbekannte oder unkonfigurierte Access Points anzeigen soll.

- **Rogue Client Detection aktiviert**

  Aktivieren Sie diese Option, wenn der WLANmonitor unbekannte oder unkonfigurierte Clients anzeigen soll.

Konfiguration Alarmierungsfunktion im WLANmonitor

Der WLANmonitor kann den Administrator automatisch per E-Mail informieren, wenn ein unbekannter oder unkonfigurierter Access Point entdeckt wird.



Konfigurationstool	Aufruf
WLANmonitor	Extras ▶ Optionen ▶ Alarmierung

- **E-Mail-Benachrichtigung**

  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 Mailclient (MS Outlook Express oder Mozilla Thunderbird) als Standard-Mail-Client eingerichtet sein, der den automatischen Mailversand 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.

3.8 Die Konfiguration mit WEBconfig

Neu mit LCOS 7.6:

■ Neues WEBconfig mit Suchfunktion, umfangreichem Geräte-Status, Online-Hilfe etc.

Sie können die Einstellungen des Gerätes über einen beliebigen Webbrowser vornehmen. Im LANCOM ist die Konfigurationssoftware WEBconfig integriert. Sie benötigen lediglich einen Webbrowser, um auf WEBconfig zuzugreifen. WEBconfig bietet ähnliche Setup-Assistenten wie LANconfig an und bietet damit optimale Voraussetzungen für eine komfortable Konfiguration des LANCOM – im Unterschied zu LANconfig aber unter allen Betriebssystemen, für die es einen Webbrowser gibt.

Sicher mit HTTPS

WEBconfig bietet zur sicheren (Fern-) Konfiguration die Möglichkeit der verschlüsselten Übertragung der Konfigurationsdaten über HTTPS.

```
https://<IP-Adresse oder Gerätename>
```



Für maximale Sicherheit sollten Sie stets die neueste Version Ihres Browsers verwenden. Unter Windows empfiehlt LANCOM Systems GmbH den aktuellen Internet Explorer.

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

Nach dem Einschalten prüfen unkonfigurierte LANCOM-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.



Wird ein LANCOM Wireless Router oder ein LANCOM Access Point von einem LANCOM WLAN Controller zentral verwaltet, dann wird beim Zuweisen der WLAN-Konfiguration auch der DHCP-Server vom Auto-Modus in den Client-Modus umgeschaltet.

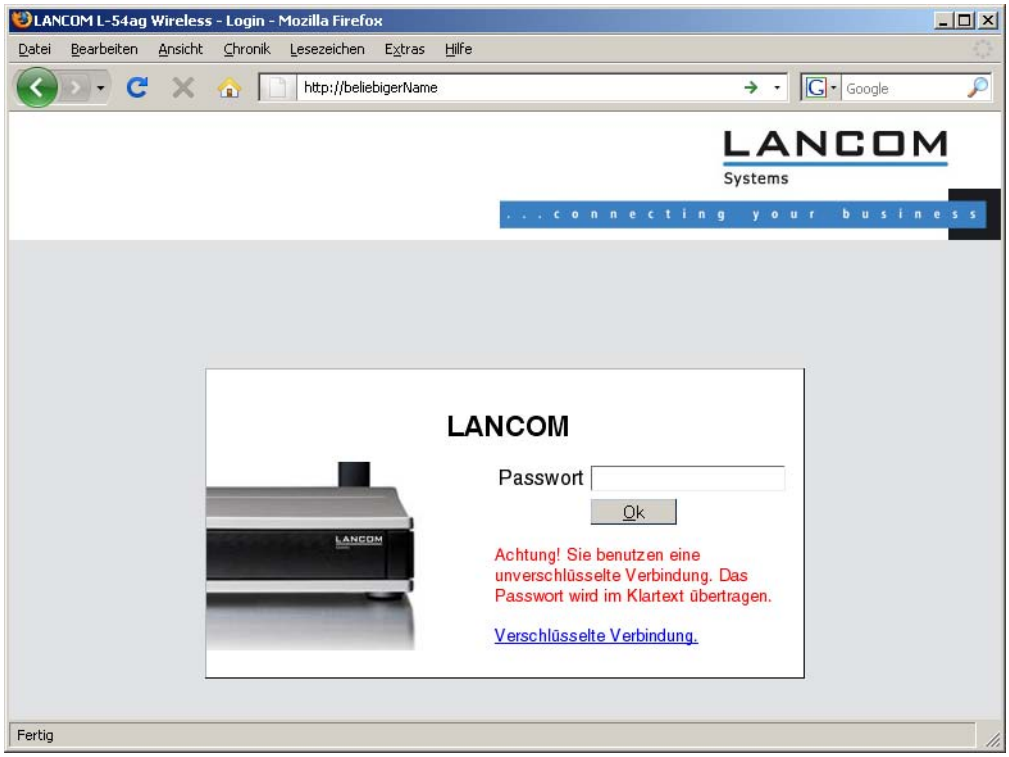
Netz ohne DHCP-Server

Nicht für zentral verwaltete LANCOM Wireless Router oder LANCOM Access Points

In einem Netz ohne DHCP-Server schalten unkonfigurierte LANCOM-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 LANCOMs einfach durch Eingabe eines beliebigen Names mittels eines Webbrowsers angesprochen und in Betrieb genommen werden.

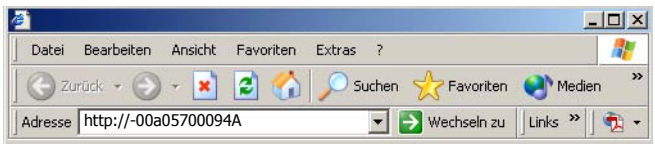


Falls der Konfigurations-Rechner seine IP-Adresse nicht vom LANCOM-DHCP-Server bezieht, ermitteln Sie die aktuelle IP-Adresse des Rechners (mit **Start** ▶ **Ausführen** ▶ **cmd** und dem Befehl **ipconfig** an der Eingabeaufforderung unter Windows 2000, Windows XP oder Windows Vista, mit **Start** ▶ **Ausführen** ▶ **cmd** und dem Befehl **winipcfg** an der Eingabeaufforderung unter Windows Me oder Windows 9x bzw. dem Befehl **ifconfig** in der Konsole unter Linux). In diesem Fall erreichen Sie das LANCOM unter der Adresse **x.x.x.254** (die "x" stehen für die ersten drei Blöcke in der IP-Adresse des Konfigurationsrechners).

Netz mit DHCP-Server

Ist im LAN ein DHCP-Server zur Zuweisung der IP-Adressen aktiv, schaltet ein unkonfiguriertes LANCOM-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 unter dem Namen "-<MAC-Adresse>" (z.B. "-00a057xxxxxx") erreicht werden.



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

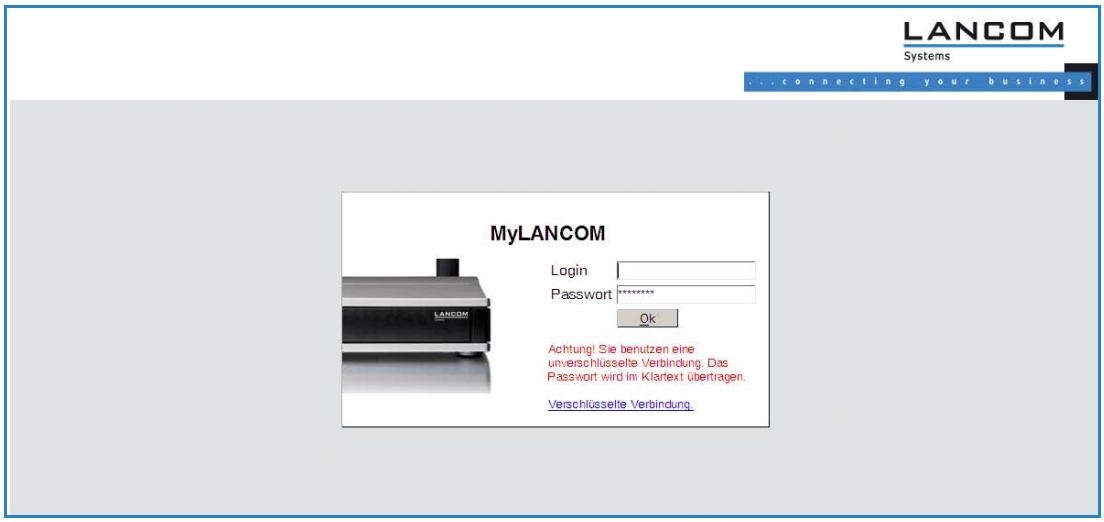
- Ist im LAN kein DNS-Server vorhanden oder ist dieser nicht mit dem DHCP-Server gekoppelt, kann das Gerät nicht über den Namen erreicht werden. In diesem Fall bleiben folgende Optionen:
  - Sie nutzen die Funktion "Geräte suchen" in LANconfig oder die Gerätesuche unter WEBconfig von einem anderen erreichbaren LANCOM.
  - Die per DHCP an das LANCOM-Gerät zugewiesene IP-Adresse über geeignete Tools ausfindig machen und das Gerät mit dieser IP-Adresse direkt erreichen.
  - Einen Rechner mit Terminalprogramm über die serielle Konfigurationsschnittstelle an das Gerät anschließen.

Login

Wenn Sie beim Zugriff auf das Gerät zur Eingabe von Benutzername und Kennwort aufgefordert werden, tragen Sie Ihre persönlichen Werte in die entsprechenden Felder der Eingabemaske ein. Achten Sie dabei auf Groß- und Kleinschreibung.

Falls Sie den allgemeinen Konfigurationszugang verwenden, tragen Sie nur das entsprechende Kennwort ein. Das Feld Benutzername bleibt in diesem Fall leer.

Der Login-Dialog bietet alternativ einen Link für eine verschlüsselte Verbindung über HTTPS. Nutzen Sie nach Möglichkeit immer die HTTPS-Verbindung mit erhöhter Sicherheit.



Setup Wizards

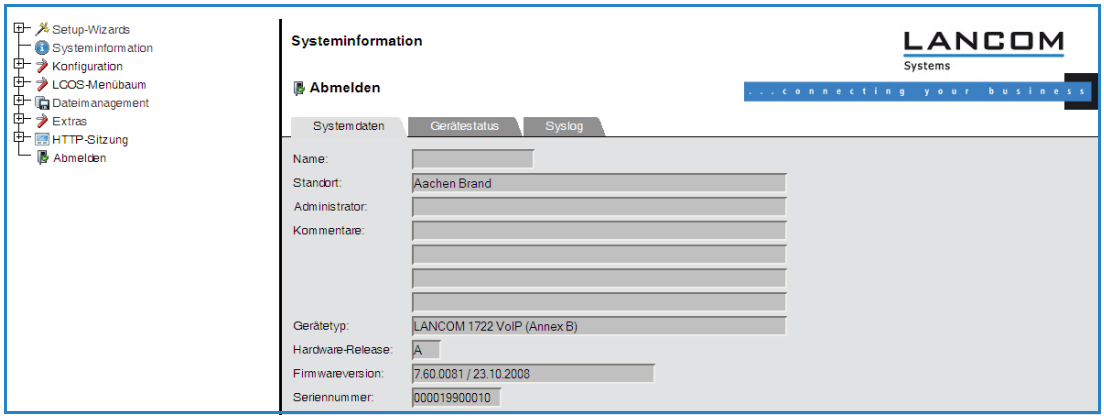
Mit den Setup-Wizards können Sie schnell und komfortabel die häufigsten Einstellungen für ein Gerät vornehmen. Wählen Sie dazu den gewünschten Assistenten aus und geben Sie auf den folgenden Seiten die benötigten Daten ein.



Die Einstellungen werden erst dann in das Gerät gespeichert, wenn Sie die Eingaben auf der letzten Seite des Assistenten bestätigen.

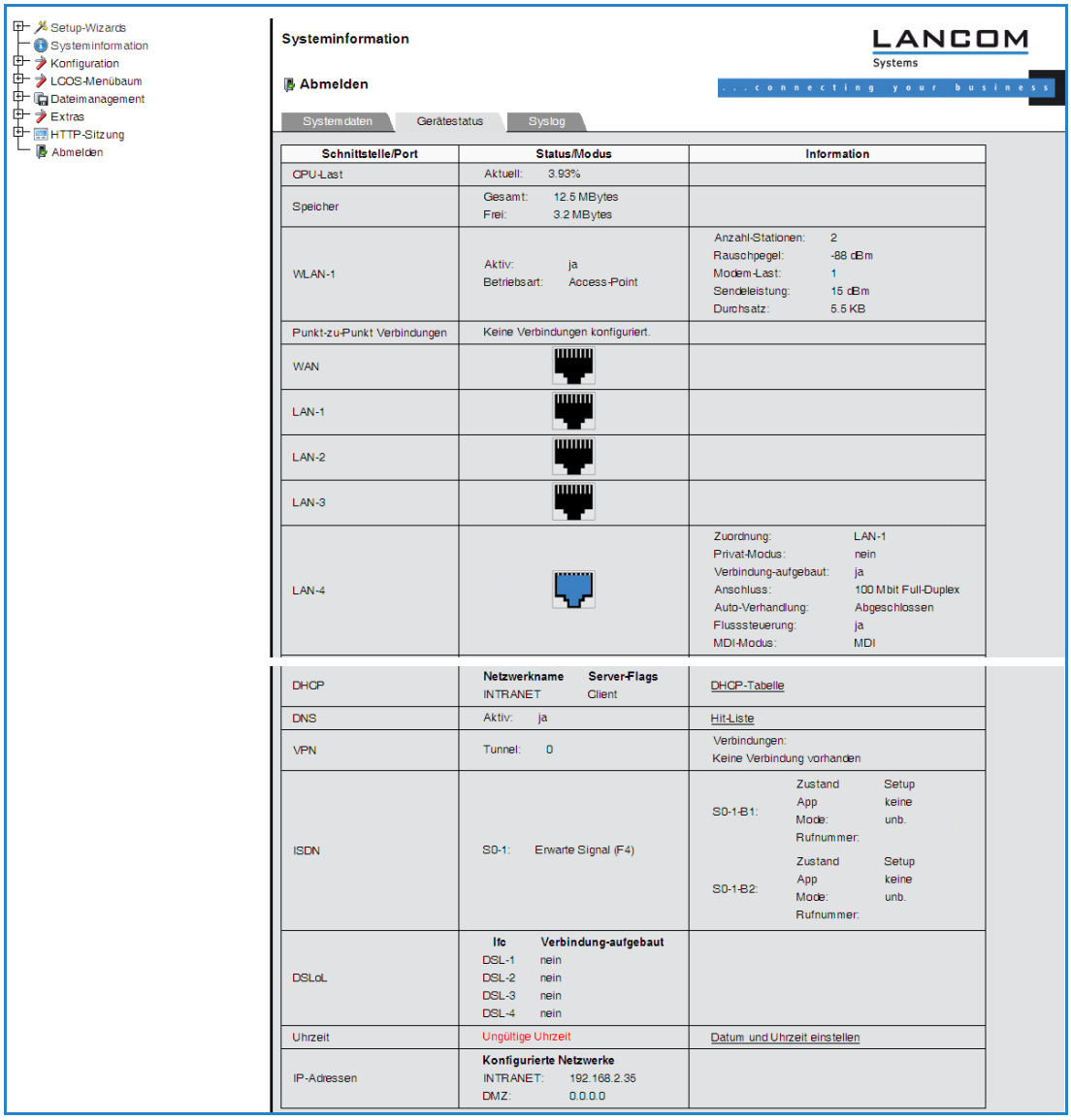
Systeminformation

Auf der Seite der Systeminformationen finden Sie auf der Registerkarte “Systemdaten” allgemeine Informationen über das Gerät, den Standort, die Firmware-Version, die Seriennummer etc.

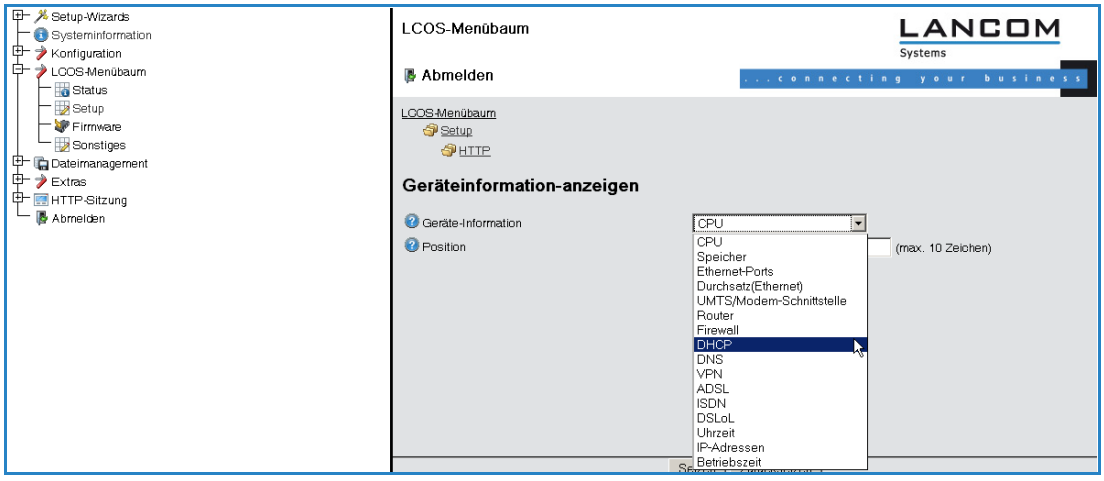


Auf der Registerkarte “Systemstatus” finden Sie umfangreiche Informationen über den aktuellen Betriebszustand des Gerätes. Dazu gehört z. B. die visuelle Darstellung der Schnittstellen mit Angabe der darauf aktiven Netzwerke. Über entsprechende Links können relevante weitere Statistiken aufgerufen werden (z. B. DHCP-Tabelle). Bei wesentlichen

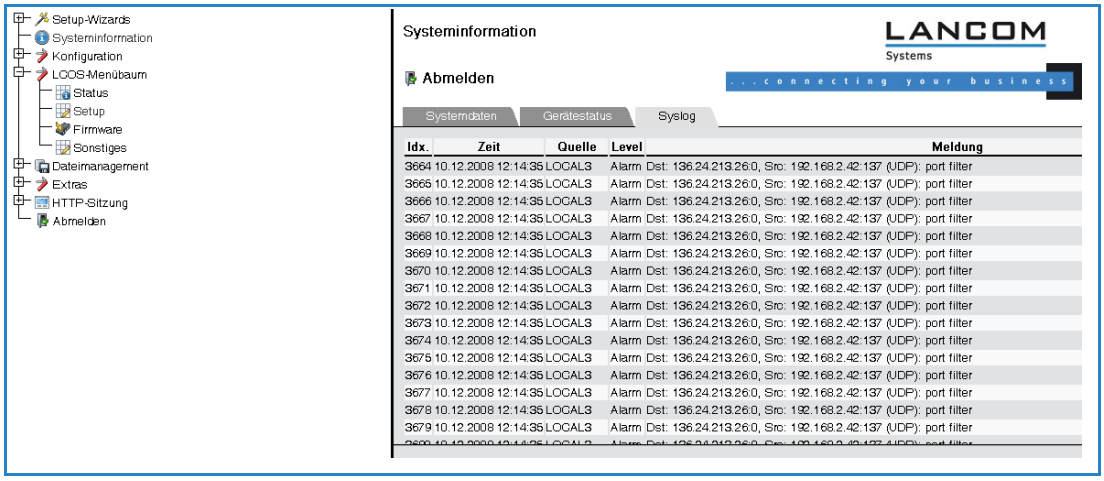
Mängeln in der Konfiguration (z. B. ungültige Zeiteinstellung) wird ein direkter Link zu den entsprechenden Konfigurationsparametern angeboten.



Den Umfang der auf dieser Seite angezeigten Informationen können Sie unter Setup/HTTP/Geräteinformation-anzeigen definieren. Dabei legen Sie über eine Indexnummer auch die Reihenfolge der Anzeige fest.



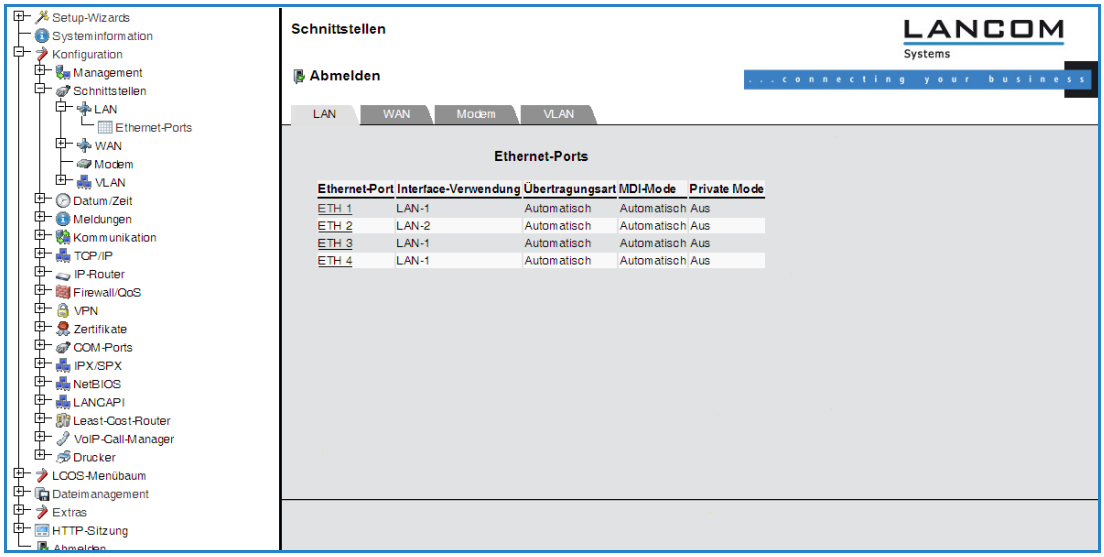
LANCOM-Geräte legen Syslog-Informationen auch im Arbeitsspeicher ab (siehe dazu Syslog). Die letzten Ereignisse können zur Diagnose auch über WEBconfig auf der Registerkarte "Systemstatus" eingesehen werden.



Konfiguration

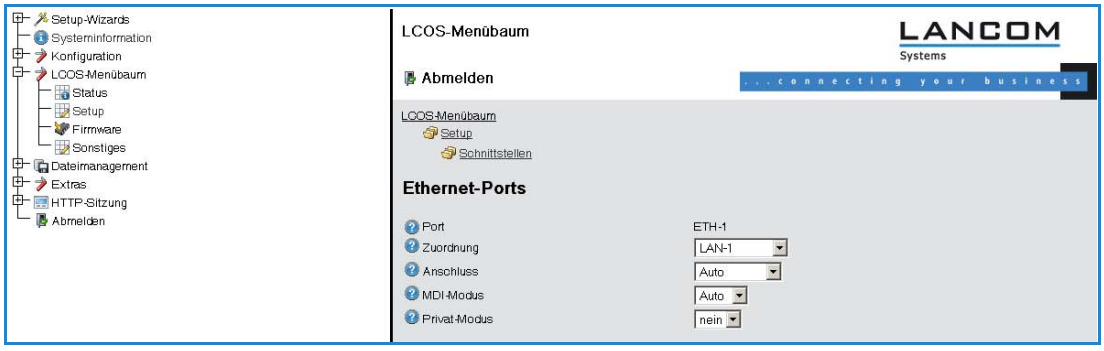
Der Menübereich "Konfiguration" bietet die Konfigurationsparameter in der gleichen Struktur an, wie Sie auch bei LANconfig verwendet wird.

Bitte beachten Sie, dass über diese Darstellung der Konfiguration nicht alle Einstellungen vorgenommen werden können.



LCOS-Menübaum

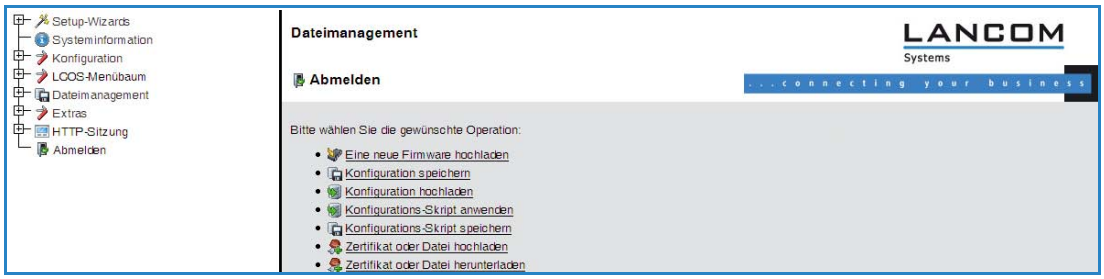
Der Menübereich "LCOS-Menübaum" bietet die Konfigurationsparameter in der gleichen Struktur an, wie Sie auch unter Telnet verwendet wird. Mit einem Klick auf das Fragezeichen können Sie für jeden Konfigurationsparameter eine Hilfe aufrufen.



Dateimanagement

Im Menübereich "Dateimanagement" finden Sie alle Aktionen, mit denen Dateien aus dem Gerät heruntergeladen oder in das Gerät hochgeladen werden:

- Eine neue Firmware hochladen
- Konfiguration speichern
- Konfiguration hochladen
- Konfigurations-Skript anwenden
- Konfigurations-Skript speichern
- Zertifikat oder Datei hochladen
- Zertifikat oder Datei herunterladen



Extras

Im Menübereich "Extras" finden Sie einige Funktionen, welche die Konfiguration der Geräte erleichtern.



Mit der Suchfunktion können Sie z. B. in den Namen aller Konfigurationsparameter suchen. Falls Sie also zu einem bestimmten Konfigurationsparameter den Namen kennen, aber nicht wissen, über welches Menü dieser Eintrag zu erreichen ist, können Sie die gewünschte Stelle im LCOS-Menü auf diese Weise schnell auffinden.

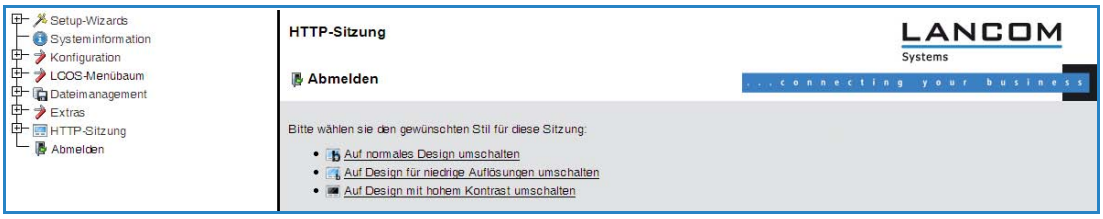


Mit der Funktion zum Suchen und Anzeigen können Sie andere LANCOM-Geräte in Ihrem Netzwerk suchen und über einen entsprechenden Link direkt auf die Konfiguration der gefundenen Geräte wechseln.



HTTP-Sitzung

Im Menübereich "HTTP-Sitzung" können Sie die Darstellung der WEBconfig-Oberfläche zur besseren Anzeige auf Ihr Ausgabegerät anpassen, z. B. die Auflösung verringern oder den Kontrast verstärken.



3.9 Die Konfiguration mit weiteren Tools

3.9.1 Telnet

Neu mit LCOS 7.6:

- Erweiterte Funktionen zum Editieren der Befehle
- Funktionstasten

Telnet-Sitzung starten

Über Telnet starten Sie die Konfiguration z.B. aus der Windows-Kommandozeile mit dem Befehl:

```
C:\>telnet 10.0.0.1
```

Telnet baut dann eine 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 und Unix 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. Die verschlüsselte Telnet-Verbindung wird dann mit dem folgenden Befehl gestartet:

```
C:\>telnet -z ssl 10.0.0.1 telnets
```

Die Sprache der Konsole auf Deutsch ändern

Der Terminalmodus steht in den Sprachen Deutsch und Englisch zur Verfügung. LANCOM Geräte werden werkseitig auf Englisch als Konsolensprache eingestellt. Im weiteren Verlauf dieser Dokumentation werden alle Konfigurationsbefehle in ihrer deutschen Form angegeben. Zur Änderung der Konsolensprache auf Deutsch verwenden Sie folgende Befehle:

WEBconfig: LCOS-Menübaum ▶ Setup ▶ Config-Module ▶ Language

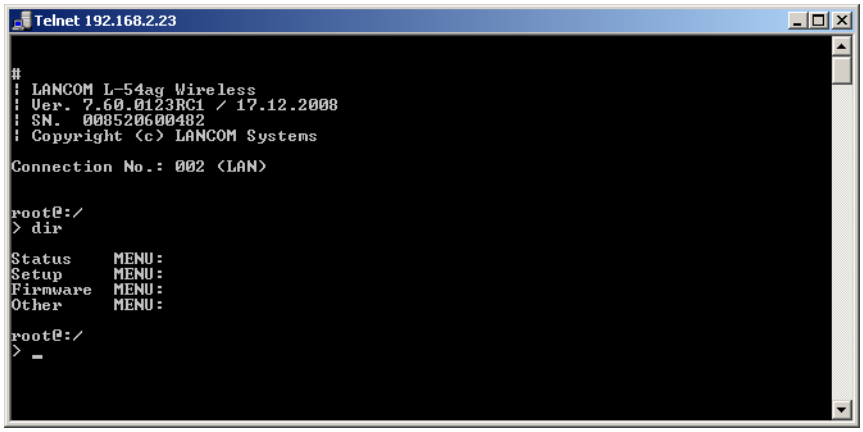
Telnet-Sitzung beenden

Um die Telnet-Sitzung zu beenden, geben Sie an der Eingabeaufforderung den Befehl `exit` ein:

```
C:\>exit
```

Die Struktur im Kommandozeilen-Interface

Das LANCOM Kommandozeilen-Interface ist stets wie folgt strukturiert:



- **Status**
  Enthält die Zustände und Statistiken aller internen Module des Gerätes
- **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

Befehle für die Kommandozeile

Das LANCOM Kommandozeilen-Interface kann mit den folgenden DOS- oder UNIX-ähnlichen Befehlen bedient werden. Die verfügbaren LCOS-Menübefehle können durch Aufrufen des HELP-Kommandos jederzeit auf der Kommandozeile angezeigt werden.

Zum Ausführen einiger Befehle sind Supervisor-Rechte erforderlich.

Befehl	Beschreibung
beginscript	Versetzt eine Konsolensitzung in den Script-Modus. In diesem Zustand werden die im Folgenden eingegebenen Befehle nicht direkt in den Konfigurations-RAM im LANCOM übertragen, sondern zunächst in den Script-Speicher des Gerätes.
cd [PFAD]	Wechselt das aktuelle Verzeichnis. Verschiedene Kurzformen werden unterstützt, z.B. "cd ../.." kann verkürzt werden zu "cd ..." etc.
del [PFAD]*	Löscht eine komplette Tabelle in dem mit `Path` angegebenen Zweig des Menübaums.
default [-r] [PFAD]	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.
dir [PFAD] list [PFAD] ls [PFAD] ll [PFAD]	Zeigt den Inhalt des aktuellen Verzeichnisses an. Der angehängte Parameter „-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.
do [PFAD] [<Parameter>]	Führt die Aktion [PATH] im aktuellen Verzeichnis aus. Zusätzliche Parameter können mit angegeben werden.
echo <ARG>...	Argument auf Konsole ausgeben
exit/quit/x	Beendet die Kommandozeilen-Sitzung
feature <code>	Freischaltung eines SW-Features mit dem angegebenen Feature-Code
flash Yes/No	Die Änderungen an der Konfiguration über die Befehle an der Kommandozeile werden standardmäßig (flash yes) direkt in den boot-resistenten Flash-Speicher der Geräte geschrieben. Wenn das Aktualisieren der Konfiguration im Flash unterdrückt wird (flash no), werden die Änderungen nur im RAM gespeichert, der beim Booten gelöscht wird.
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.
killscript	Löscht den noch nicht verarbeiteten Inhalt einer Scriptsession. Die Scriptsession wird über den Namen ausgewählt.
loadconfig	Konfiguration per TFTP-Client in das Gerät laden
loadfirmware	Firmware per TFTP-Client in das Gerät laden

Befehl	Beschreibung
loadscript	Script per TFTP-Client in das Gerät laden
passwd	Ändern des Passworts
passwd -n neues [altes]	Passwort ändern (Keine Eingabeaufforderung)
ping [IP-Adresse oder Name]	Sendet einen ICMP echo request an die angegebene IP-Adresse
readconfig	Anzeige der kompletten Konfiguration in der Geräte-Syntax
readmib	Anzeige der SNMP Management Information Base
readscript [-n] [-d] [-c] [-m] [PFAD]	Erzeugt in einer Konsolensitzung eine Textausgabe von allen Befehlen und Parametern, die für die Konfiguration des LANCOM im aktuellen Zustand benötigt werden.
repeat <INTERVAL> <Kommando>	Wiederholt das Kommando alle INTERVALL Sekunden, bis der Vorgang durch neue Eingaben beendet wird
sleep [-u] Wert[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.
stop	Beendet den PING-Befehl
set [PFAD] <Wert(e)>	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.
set [PFAD] ?	Auflistung der möglichen Eingabewerte für einen Konfigurationsparameter. Wird kein Name angegeben, so werden die möglichen Eingabewerte für alle Konfigurationsparameter im aktuellen Verzeichnis angegeben
setenv <NAME> <WERT>	Umgebungsvariable setzen
unsetenv <NAME>	Umgebungsvariable löschen
getenv <NAME>	Umgebungsvariable ausgeben (kein Zeilenvorschub)
printenv	Komplette Umgebung ausgeben
show <Optionen>	Anzeige spezieller interner Daten. show ? zeigt alle verfügbaren Informationen an, z.B. letzte Boot-Vorgänge ('bootlog'), Firewall Filterregeln ('filter'), VPN-Regeln ('VPN') und Speicherauslastung ('mem' und 'heap')
sysinfo	Anzeige der Systeminformationen (z.B. Hardware/Softwareversion etc.)
testmail	Schickt eine E-Mail. Parameter siehe 'testmail ?'
time	Zeit setzen (TT.MM.JJJJ hh:mm:ss)
trace […]	Konfiguration der Diagnose-Ausgaben.
who	Aktive Sitzungen auflisten
writeconfig	Laden einer neuen Konfigurationsfile in der Geräte-Syntax. Alle folgenden Zeilen werden als Konfigurationswerte interpretiert, solange bis zwei Leerzeilen auftreten
writeflash	Laden einer neuen Firmware-Datei (nur via TFTP)
!!	Letztes Kommando wiederholen
!<num>	Kommando <num> wiederholen
!<prefix>	Letztes mit <prefix> beginnendes Kommando wiederholen
#<blank>	Kommentar

- PFAD:
  - Pfadname für ein Menü oder einen Parameter, getrennt durch / oder \
  - .. bedeutet eine Ebene höher
  - . bedeutet aktuelle Ebene
- WERT:
  - möglicher Eingabewert
  - "" ist ein leerer Eingabewert
- NAME:
  - Sequenz von _ 0..9 A..Z
  - erstes Zeichen darf keine Ziffer sein
  - keine Unterscheidung Gross/Kleinschreibung
- 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.

- Namen, die Leerzeichen enthalten, müssen in Anführungszeichen ("") eingeschlossen werden.
- Für Aktionen und Befehle steht eine kommandospezifische Hilfefunktion zur Verfügung, indem die Funktion mit einem Fragezeichen als Parameter aufgerufen wird. Zum Beispiel zeigt der Aufruf '`ping ?`' die Optionen des eingebauten ping Kommandos an.
- Eine vollständige Auflistung der zur Verfügung stehenden Konsolen-Kommandos erhalten Sie durch die Eingabe von '`?`' auf der Kommandozeile.

Funktionen zum Editieren der Befehle

Mit den folgenden Befehlen können die Befehle auf der Kommandozeile bearbeitet werden. Die "ESC key sequences" zeigen zum Vergleich die Tastenkombinationen, die auf typischen VT100/ANSI-Terminals verwendet werden:

Funktion	Esc key sequences	Beschreibung
Pfeil nach oben	ESC [A	Springt in der Liste der letzten ausgeführten Befehle eine Position nach oben, in Richtung älterer Befehle.
Pfeil nach unten	ESC [B	Springt in der Liste der letzten ausgeführten Befehle eine Position nach unten, in Richtung neuerer Befehle.
Pfeil nach rechts	Ctrl-F ESC [C	Bewegt die Einfügemarke eine Position nach rechts.
Pfeil nach links	Ctrl-B ESC [D	Bewegt die Einfügemarke eine Position nach links.
Home oder Pos1	Ctrl-A ESC [A ESC [1~ (	Bewegt die Einfügemarke an das erste Zeichen der Zeile.
Ende	Ctrl-E ESC [F ESC OF ESC [4~	Bewegt die Einfügemarke an das letzte Zeichen der Zeile.
Einfg	ESC [ESC [2~	Schaltet um zwischen Einfügemodus und Überschreibemodus.
Entf	Ctrl-D ESC <BS> ESC [3~	Löscht das Zeichen an der aktuellen Position der Einfügemarke oder beendet die Telnet-Sitzung, wenn die Zeile leer ist.
erase	<BS><DEL>	Löscht das nächste Zeichen links neben der Einfügemarke.
erase-bol	Ctrl-U	Löscht alle Zeichen links neben der Einfügemarke.
erase-eol	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: ■ Wenn es genau eine Möglichkeit gibt, den Befehl bzw. den Pfad zu vervollständigen, so wird diese Möglichkeit in die Zeile übernommen. ■ 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. ■ 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.

Funktionstasten für die Kommandozeile

WEBconfig: Setup ▶ Config ▶ Funktionstasten

Mit den Funktionstasten haben Sie die Möglichkeit, häufig genutzte Befehlssequenzen zu speichern und an der Kommandozeile komfortabel aufzurufen. In der entsprechenden Tabelle werden den Funktionstasten F1 bis F12 die Befehle so zugeordnet, wie sie an der Kommandozeile eingegeben werden.

- **Taste**

  Bezeichnung der Funktionstaste.

  Mögliche Werte:

  □ Auswahl aus den Funktionstasten F1 bis F12.

  Default:

  □ F1

- **Abbildung**

  Beschreibung des Befehls bzw. der Tastenkombination, die bei Aufruf der Funktionstaste an der Kommandozeile ausgeführt werden soll.

  Mögliche Werte:

  □ Alle an der Kommandozeile möglichen Befehle bzw. Tastenkombinationen

Default:

□ Leer

Besondere Werte:

□ Das Caret-Zeichen ^ wird verwendet, um spezielle Steuerungsbefehle mit ASCII-Werten unterhalb von 32 abzubilden.^a

□ ^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.

3.9.2 SNMP

Das Simple Network Management Protocol (SNMP V.1 nach RFC 1157) ermöglicht die Überwachung und Konfiguration von Geräten in einem Netz von einer zentralen Instanz aus.

Es gibt eine ganze Reihe von Konfigurations- und Management-Programmen, die über SNMP laufen. Kommerzielle Beispiele sind Tivoli, OpenView von Hewlett-Packard, SunNet Manager und CiscoWorks. Daneben existieren auch zahlreiche Programme auf Freeware- und Shareware-Basis.

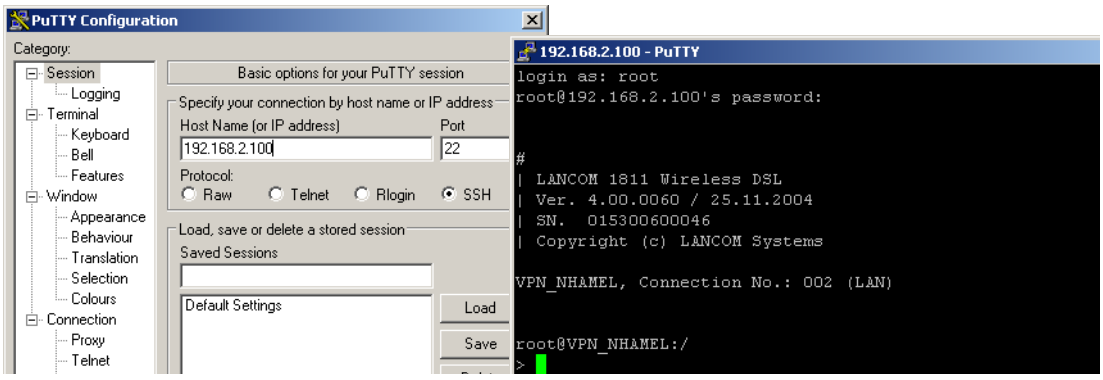
Ihr LANCOM kann die für die Verwendung in SNMP-Programmen benötigte Geräte-MIB-Datei (**M**anagement **I**nformation **B**ase) wie folgt exportieren.

WEBconfig: Extras ▶ SNMP-Geräte-MIB abrufen

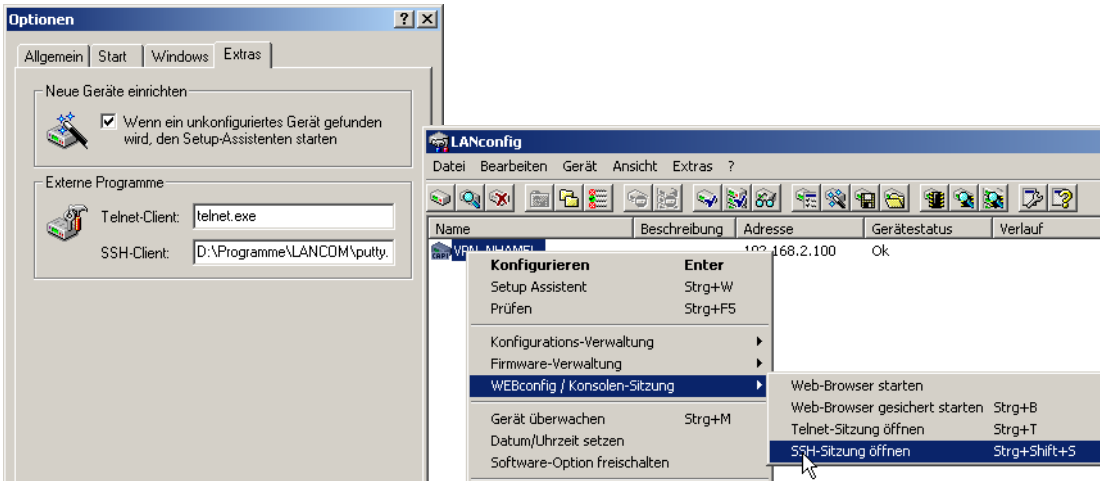
3.9.3 Verschlüsselte Konfiguration über SSH-Zugang

Neben den bisherigen Möglichkeiten, ein LANCOM über Telnet oder Terminalprogramm zu konfigurieren, gibt es ab der LCOS-Version 4.0 zusätzlich einen Zugang über SSH. Mit einem entsprechenden SSH-Client wie PuTTy können Sie so eine verschlüsselte Verbindung zum Gerät herstellen und die bei der Konfiguration übertragenen Daten so vor dem Abhören innerhalb des Netzwerks schützen.

Starten Sie z.B. PuTTy und geben Sie als Host Name die IP-Adresse des LANCOM ein. In der folgenden Eingabeaufforderung können Sie sich mit Ihren Benutzerdaten anmelden.



Alternativ können Sie im LANconfig unter **Extras** ▶ **Optionen** ▶ **Extras** Ihren SSH-Client als „externes Programm" eintragen und den SSH-Zugang dann mit einem rechten Mausklick auf das Gerät und **WEBconfig/Konsolen-Sitzung** ▶ **SSH-Sitzung öffnen** starten.



Zur Konfiguration verwenden Sie die gleichen Befehle wie über Telnet oder Terminalprogramm (‘Befehle für die Kommandozeile’ → Seite 3-36).

3.9.4 SSH-Authentifizierung

Das SSH-Protokoll erlaubt grundsätzlich zwei verschiedene Authentifizierungs-Mechanismen:

- Mit Benutzername und Kennwort
- Mit Hilfe eines öffentlichen Schlüssels (Public Key)

Beim Public-Key-Verfahren wird ein Schlüsselpaar aus privatem und öffentlichem Schlüssel verwendet – ein digitales Zertifikat. Detaillierte Informationen zu diesen Schlüsseln finden sie im VPN-Kapitel des Referenzhandbuchs im Abschnitt 'digitale Zertifikate'. Der private Teil des Schlüsselpaares wird beim Client gespeichert (häufig mit einem Kennwort geschützt), der öffentliche Teil wird in den LANCOM Router geladen.

LANCOM Router unterstützen sowohl RSA als auch DSS/DSA-Schlüssel. RSA-Schlüssel sind etwas kleiner und erlauben so einen etwas schnelleren Betrieb.

Erzeugung von Schlüsselpaaren

Die Paare aus öffentlichem und privatem Schlüssel können z.B. mit Hilfe der OpenSource-Software OpenSSH erzeugt werden. Der folgende Befehl an der Shell eines Linux-Betriebssystems erstellt ein Schlüsselpaar aus dem öffentlichen Teil '`id_rsa.pub`' und dem privaten Teil '`id_rsa`':

```
ssh-keygen -t rsa
```

Eintragen von Benutzern in den öffentlichen Schlüssel

Die öffentlichen Schlüssel werden in der folgenden Syntax erzeugt:

```
<Verschlüsselungsalgorhytmus> <öffentlicher Schlüssel> <Benutzer> [weitere Benutzer]
```

Um weitere Benutzer für den Zugang über diesen Schlüssel zu erlauben, werden die entsprechenden Benutzernamen einfach an die vorhandene Schlüsseldatei angehängt.

Installation des privaten Schlüssels beim SSH-Client

Der private Teil des Schlüssels muss beim SSH-Client installiert werden. Informieren Sie sich bitte ggf. in der Dokumentation zu Ihrem SSH-Client über die notwendigen Schritte.

Öffentlichen Schlüssel in den LANCOM Router laden

Der oder die öffentlichen Schlüssel können über WEBconfig in das Gerät geladen werden. Wählen Sie dazu auf der Startseite von WEBconfig den Eintrag **Zertifikate oder Datei hochladen**. Wählen Sie im folgenden Dialog den Eintrag 'SSH - akzeptierte öffentliche Schlüssel' aus, und wählen Sie die zuvor erstellte Datei mit den öffentlichen Schlüsseln und den Benutzern. Mit dem Befehl Upload startet die Übertragung zum LANCOM.

Die hochgeladene Datei ersetzt die Liste der bisher ggf. im Gerät vorhandenen akzeptierten Schlüssel. Alternativ können Sie auf der Startseite von WEBconfig den Eintrag **Liste erlaubter öffentlicher Schlüssel bearbeiten** wählen und die Schlüssel direkt editieren. Dabei können Sie auch einzelne Schlüssel an die bestehende Liste anhängen.

Konfiguration der Authentifizierungs-Methoden

Die zulässigen Authentifizierungs-Methoden für den SSH-Zugang können für LAN, WAN und WLAN getrennt eingestellt werden.

WEBconfig: LCOS-Menübaum ▶ Setup ▶ Config ▶ SSH-Authentisierungs-Methoden

- **Methoden**
  - Alle: Erlaubt die Authentifizierung über Kennwort und Zertifikat.
  - Passwort: Erlaubt die Authentifizierung über Kennwort.
  - Public Key: Erlaubt nur die Authentifizierung über Zertifikat.

Ablauf der Zertifikatsprüfung beim SSH-Zugang

Bei Aufbau der SSH-Verbindung erkundigt sich der Client zunächst beim LANCOM Router, 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 den LANCOM Router. Wenn der LANCOM Router in der Liste seiner öffentlichen SSH-Schlüssel einen passenden Eintrag findet, in dem der Benutzername enthalten ist, wird der Zugang über SSH erlaubt. Hat der Client keinen passenden privaten Schlüssel installiert oder auf Seiten des LANCOM Router gibt es keine Übereinstimmung mit Benutzernamen oder öffentlichem Schlüssel, kann der SSH-Client auf eine Authentifizierung mit Benutzername/Kennwort zurückfallen – sofern diese Authentifizierungs-Methode erlaubt ist.

3.9.5 ISDN-Fernkonfiguration über das DFÜ-Netzwerk

Der komplette Abschnitt zur Fernkonfiguration gilt nur für Geräte mit ISDN-Schnittstelle oder mit Modem (analog oder GSM) an der seriellen Schnittstelle (mit LANCOM Modem Adapter Kit).

Besonders einfach wird die Konfiguration von Routern an entfernten Standorten mit der Fernkonfiguration über das DFÜ-Netzwerk von Windows. Das Gerät ist nach dem Einschalten und der Verbindung mit dem ISDN-Anschluss ohne eine einzige Einstellung sofort vom Administrator zu erreichen. Damit sparen Sie bei der Konfiguration an entfernten Orten viel Zeit und Geld für die Reise oder für die Einweisung der Mitarbeiter vor Ort in die Konfiguration der Router.

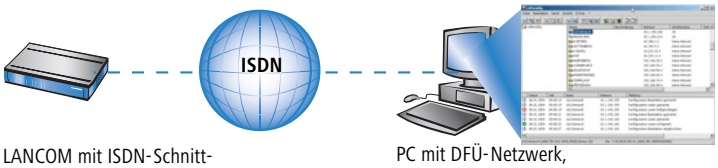
Außerdem können Sie eine spezielle Rufnummer für die Fernkonfiguration reservieren. Damit kann ein Service-Techniker immer auf den Router zugreifen, auch wenn das Gerät durch fehlerhafte Einstellungen eigentlich nicht mehr ansprechbar ist.

Das brauchen Sie für die ISDN-Fernkonfiguration

- Einen LANCOM mit ISDN-Anschluss, das von einem entfernten Standort aus konfiguriert werden soll
- Einen Konfigurations-PC mit PPP-Client (z.B. Windows DFÜ-Netzwerk) sowie ISDN-Adapter oder alternativ Zugriff über LANCAPI auf einen LANCOM mit ISDN-Anschluss
- Ein Programm für die Inband-Konfiguration, z.B. LANconfig oder Telnet

Die erste Fernverbindung mit DFÜ-Netzwerk

Für die Fernkonfiguration eines LANCOM mit LANconfig über das DFÜ-Netzwerk gehen Sie wie folgt vor:



LANCOM mit ISDN-Schnittstelle zur Konfiguration

PC mit DFÜ-Netzwerk, ISDN-Adapter (alternativ Zugriff auf LANCAPI) und LANconfig

① Wählen Sie im LANconfig **Datei ▶ Gerät hinzufügen**, aktivieren Sie die 'DFÜ-Verbindung' als Anschlusstyp und geben Sie die Rufnummer des ISDN-Anschlusses ein, an dem der LANCOM angeschlossen ist. Stellen Sie dazu ggf. die Zeit ein, nach der eine Verbindung ohne Datentransfer automatisch getrennt werden soll.

② LANconfig legt nun automatisch einen neuen Eintrag im DFÜ-Netzwerk an. Wählen Sie ein PPP-fähiges Gerät (z.B. den NDIS-WAN-Treiber aus dem Lieferumfang der LANCAPI) für die Verbindung aus, und bestätigen Sie mit **OK**.

③ Anschließend zeigt LANconfig in der Geräteliste ein neues Gerät mit dem Namen 'Unbekannt' und der Rufnummer über DFÜ als Adresse an.

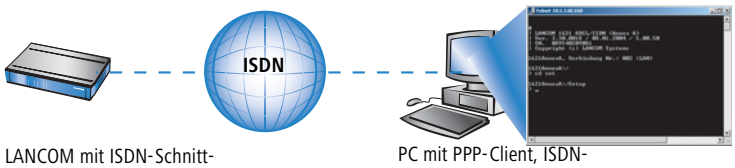
Mit dem Löschen eines Eintrags in der Geräteliste wird auch die zugehörige Verbindung im Windows-DFÜ-Netzwerk gelöscht.

④ Sie können das Gerät über die Fernverbindung nun genauso konfigurieren wie alle anderen Geräte. Hierzu baut LANconfig eine Verbindung über das DFÜ-Netzwerk auf.

Schützen Sie die Einstellungen des Geräts immer durch die Vergabe eines Passworts! Geben Sie im LANconfig im Konfigurationsbereich 'Management' auf der Registerkarte 'Security' bei der ersten Konfiguration ein Passwort ein!

Die erste Fernverbindung mit PPP-Client und Telnet

An Stelle der Fernkonfiguration mit LANconfig ist auch ein Zugriff über ISDN mit Telnet möglich. Für die Fernkonfiguration eines LANCOM mit Telnet über einen beliebigen PPP-Client gehen Sie wie folgt vor:



LANCOM mit ISDN-Schnittstelle zur Konfiguration

PC mit PPP-Client, ISDN-Adapter (alternativ Zugriff auf LANCAPI) und Telnet

① Stellen Sie mit Ihrem PPP-Client eine Verbindung zum LANCOM her, verwenden Sie dabei folgende Angaben:

- Benutzername 'ADMIN'
- Passwort wie beim LANCOM eingestellt
- eine IP-Adresse für die Verbindung, nur wenn erforderlich

② Starten Sie eine Telnet-Verbindung zum LANCOM. Verwenden Sie dazu die folgende IP-Adresse:

- '172.17.17.18', wenn Sie keine IP-Adresse für den PPP-Client festgelegt haben. Diese Adresse verwendet der LANCOM automatisch, falls nichts anderes vereinbart ist. Der Konfigurations-PC reagiert dann auf die IP '172.17.17.17'.
- Erhöhen Sie die IP-Adresse des PCs um eins, wenn Sie eine Adresse festgelegt haben. Beispiel: Sie haben für den PPP-Client die IP '10.0.200.123' festgelegt, dann hört der LANCOM auf die '10.0.200.124'. Ausnahme: Bei einer '254' am Ende der IP reagiert der Router auf die 'x.x.x.1'.

③ Sie können den LANCOM über die Fernverbindung nun genauso einstellen wie alle anderen Geräte.

Schützen Sie die Einstellungen des Geräts immer durch die Vergabe eines Passworts! Geben Sie bei einer Telnet- oder Terminalverbindung alternativ den folgenden Befehl ein:

```
passwd
```

Damit werden Sie zur Eingabe eines neuen Passworts mit Bestätigung aufgefordert.

Der Default-Layer für die Ferninbetriebnahme

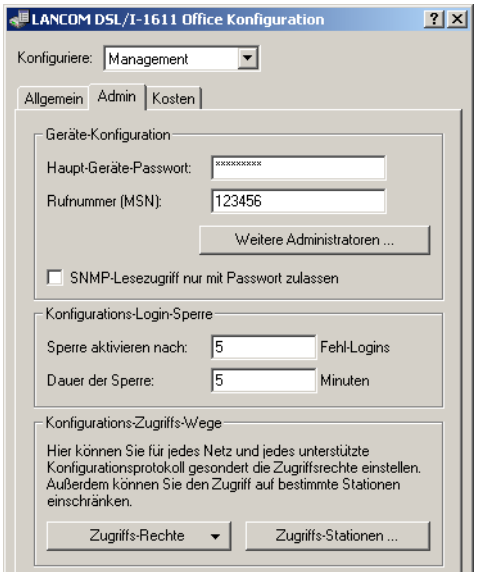
Die PPP-Verbindung von einer beliebigen ISDN-Gegenstelle zum Router gelingt natürlich nur dann, wenn das Gerät jeden Ruf mit den entsprechenden Einstellungen für den PPP-Betrieb annimmt. Im Auslieferungszustand geht das auch, da das Standard-Protokoll (Default-Layer) auf PPP eingestellt ist.

Aber vielleicht möchten Sie ja nach der ersten Konfiguration den Default-Layer z.B. für LAN-LAN-Verbindungen auf ein anderes Protokoll einstellen? Dann nimmt das Gerät die Rufe über die DFÜ-Verbindung nicht mehr mit den PPP-Einstellungen an. Abhilfe schafft hier die Vereinbarung einer speziellen Rufnummer des ISDN-Anschlusses für den Konfigurationszugriff:

Der ISDN-Administrationszugang für die Fernwartung

Empfängt das Gerät einen Ruf auf dieser Nummer, wird immer die Einstellung für PPP verwendet - unabhängig von der weiteren Konfiguration des Routers! Dabei wird nur ein spezieller Benutzername während der PPP-Verhandlung akzeptiert, der beim Verbindungsaufbau über LANconfig automatisch eingetragen wird ('ADMIN').

① Wechseln Sie im Konfigurationsbereich 'Management' auf die Registerkarte 'Admin'.



② Geben Sie als Rufnummer im Bereich 'Geräte-Konfiguration' eine Rufnummer (MSN) Ihres Anschlusses ein, die nicht für andere Zwecke verwendet wird.

Geben Sie alternativ über Telnet den folgenden Befehl ein:

```
set /setup/config-modul/Fernconfig 123456
```

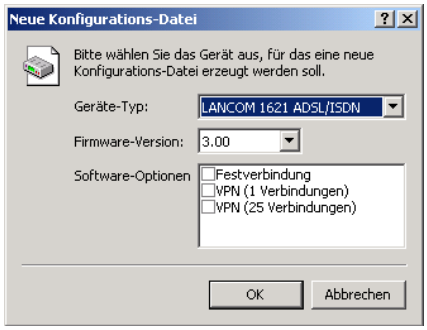
Solange keine MSN für den Konfigurations-Zugriff eingetragen ist, nimmt ein **unkonfiguriertes** LANCOM die Rufe auf alle MSNs an. Sobald die erste Änderung in der Konfiguration gespeichert ist, nimmt das Gerät nur noch die Anrufe auf der Konfigurations-MSN an!

Wenn bei der ersten Konfiguration keine Konfigurations-MSN eingetragen wird, ist die Fernkonfiguration damit ausgeschaltet und das Gerät gegen den Zugriff über die ISDN-Leitung geschützt.

3.10 Abspeichern, Wiederherstellen und Erzeugen von Konfigurationsdateien

Die aktuelle Konfiguration eines LANCOM kann als Datei abgespeichert und bei Bedarf wieder in das Gerät (oder in ein anderes Gerät desselben Typs) geladen werden.

Zusätzlich können mit LANconfig Konfigurationsdateien auch “offline” erzeugt und editiert werden - für alle unterstützten Gerätetypen, Firmware-Versionen und Software-Optionen.





Sicherheitskopien der Konfiguration

Mit dieser Funktion können Sie Sicherungskopien der Konfiguration Ihres LANCOM erstellen.

Komfortable Serienkonfiguration

Aber auch wenn Sie vor der Aufgabe stehen, mehrere gleichartige LANCOM konfigurieren zu müssen, werden Sie die Funktion des Abspeicherns und Wiederherstellens von Konfigurationen schätzen lernen. Sie können sich in diesem Fall einen großen Teil der Arbeit sparen, indem Sie in alle Geräte zunächst übereinstimmende Parameter als Grundkonfiguration einspielen und nur noch die individuellen Einstellungen an den einzelnen Geräten vornehmen.

Funktionsaufruf

LANconfig: Gerät ▶ Konfigurations-Verwaltung ▶ Als Datei sichern
LANconfig: Gerät ▶ Konfigurations-Verwaltung ▶ Aus Datei wiederherstellen

LANconfig: Bearbeiten ▶ Neue Konfigurations-Datei
LANconfig: Bearbeiten ▶ Konfigurations-Datei bearbeiten
LANconfig: Gerät ▶ Konfigurations-Verwaltung ▶ Drucken

WEBconfig: Dateimanagement ▶ Konfiguration speichern

WEBconfig: Dateimanagement ▶ Konfiguration hochladen

TFTP: tftp 10.0.0.1 get readconfig file1
TFTP: tftp 10.0.0.1 put file1 writeconfig

3.11 Neue Firmware mit LANCOM FirmSafe

Neu in LCOS 7.60:

- Asymmetrisches Firmsafe

3.11.1 So funktioniert LANCOM FirmSafe

LANCOM 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. 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 selbst entscheiden, welche Firmware nach dem Upload aktiviert werden soll:

- 'Unmittelbar': Als erste Möglichkeit können Sie die neue Firmware laden und sofort aktivieren. Folgende Situationen können dann entstehen:
  - Die neue Firmware wird erfolgreich geladen und arbeitet anschließend wie gewünscht. Dann ist alles in Ordnung.
  - Das Gerät ist nach dem Ladevorgang der neuen Firmware nicht mehr ansprechbar. Falls schon während des Uploads ein Fehler auftritt, aktiviert das Gerät automatisch wieder die bisherige Firmware und startet damit neu.

Nicht unter LANconfig

- 'Login': Um den Problemen eines fehlerhaften Uploads zu begegnen, gibt es die zweite Möglichkeit, bei der die Firmware geladen und ebenfalls sofort gestartet wird.
  - Im Unterschied zur ersten Variante wartet das Gerät anschließend für den eingestellten Firmsafe-Timeout (unter WEBconfig im Menü **Expertenkonfiguration ▶ Firmware ▶ Timeout-Firmsafe**, unter Telnet einzustellen mit 'Firmware/Timeout-Firmsafe') auf einen erfolgreichen Login über Telnet, ein Terminalprogramm oder WEBconfig. Nur wenn dieser Login erfolgt, wird die neue Firmware auch dauerhaft aktiviert.
  - Wenn das Gerät nicht mehr ansprechbar ist oder ein Login aus anderen Gründen unmöglich ist, aktiviert es automatisch wieder die bisherige Firmware und startet damit neu.
- 'Manuell': Bei der dritten Möglichkeit können Sie ebenfalls selbst eine Zeit bestimmen, in der Sie die neue Firmware testen wollen. Das Gerät startet mit der neuen Firmware und wartet in der eingestellten Zeit darauf, dass die geladene Firmware von Hand aktiviert und damit dauerhaft wirksam gemacht wird. Unter LANconfig aktivieren Sie die neue Firmware mit **Gerät ▶ Firmware-Verwaltung ▶ Im Test laufende Firmware freischalten**, unter Telnet unter 'Firmware/Firmsafe-Tabelle' mit dem Befehl 'set # active' (dabei ist # die Position der Firmware in der Firmsafe-Tabelle). Unter WEBconfig finden Sie die Firmsafe-Tabelle unter **Expertenkonfiguration ▶ Firmware**.

Den Modus für den Firmware-Upload stellen Sie unter WEBconfig im Menü **Expertenkonfiguration ▶ Firmware ▶ Modus-Firmsafe** ein, unter Telnet unter 'Firmware/Timeout-Firmsafe'. Unter LANconfig wählen Sie den Modus bei der Auswahl der neuen Firmware-Datei aus.

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 benötigen. In diesem Fall wird das asymmetrische Firmsafe verwendet.

3.11.2 Asymmetrisches Firmsafe

Durch den großen Funktionsumfang in der Firmware ist es nicht bei allen Geräten möglich, zwei vollwertige Firmwareversionen gleichzeitig zu speichern. Bei diesen Geräten wird das asymmetrische Firmsafe verwendet. Dabei enthält das Gerät immer eine vollständige Firmware sowie eine 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

Outbandschnittstelle), um eine funktionsfähige Firmware in das Gerät zu laden. Die Minimalfirmware kann nicht konfiguriert werden. Änderungen in der Konfiguration über LANconfig, WEBconfig oder Telnet werden nicht in das Gerät gespeichert.

Alle erweiterten Funktionalitäten, insbesondere die Remote Administration (auch über ISDN), 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.

Umstellung auf asymmetrisches Firmsafe

Zur Umstellung der Geräte auf das asymmetrische Firmsafe wird zunächst eine Konverter-Firmware in das Gerät geladen. 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 bleibt zur Sicherung der Erreichbarkeit im Gerät.

Firmware-Upgrade mit asymmetrischem Firmsafe

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

3.11.3 So spielen Sie eine neue Software ein

Beim Firmware-Upload (so heißt das Einspielen der Software) führen verschiedene Wege zum Ziel:

- LANconfig
- WEBconfig
- Terminalprogramm
- TFTP



Beim Firmware-Upload bleiben alle Einstellungen erhalten! Trotzdem sollten Sie sicherheitshalber die Konfiguration vorher speichern (bei LANconfig z.B. mit **Gerät** ▶ **Konfigurations-Verwaltung** ▶ **Als Datei sichern**). Neben der Konfiguration sollten Sie auch eine Version der aktuellen Firmware vor dem Upload sichern. Wenn Ihnen diese nicht mehr als Datei zur Verfügung steht, laden Sie vor dem Firmware-Upload die aktuell verwendete Version von www.lancom.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.

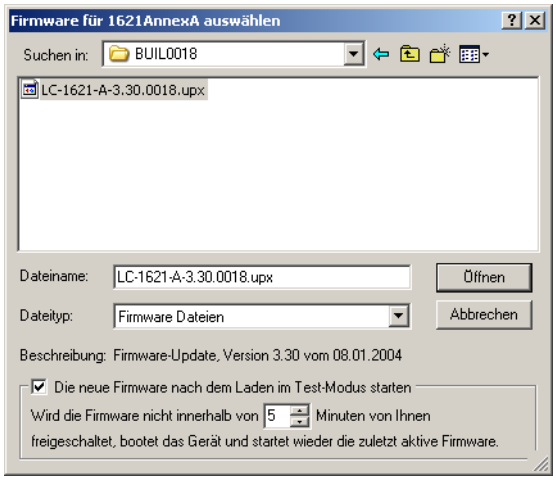
LANconfig



Beim LANconfig markieren Sie das gewünschte Gerät in der Auswahlliste und klicken auf **Gerät** ▶ **Konfigurations-Verwaltung** ▶ **Neue Firmware hochladen** oder direkt auf die Schaltfläche **Firmware-Upload**. Dann wählen Sie das Verzeichnis, in dem sich die neue Version befindet, und markieren die entsprechende Datei.

LANconfig informiert Sie dann in der Beschreibung über Versions-Nummer und Datum der Firmware und bietet den Upload an. Mit **Öffnen** ersetzen Sie die vorhandene Firmware durch die ausgewählte Version.

Wählen Sie außerdem aus, ob die Firmware sofort nach dem Laden dauerhaft aktiviert werden soll, oder stellen Sie eine Testzeit ein, in der Sie die Firmware selbst freischalten. Um anschließend die Firmware während der eingestellten Testzeit zu aktivieren, klicken Sie auf **Bearbeiten** ▶ **Firmware-Verwaltung** ▶ **Im Test laufende Firmware freischalten**.



WEBconfig

Starten Sie WEBconfig in Ihrem Web-Browser. Auf der Startseite finden Sie den Link **Eine neue Firmware hochladen**. Im nächsten Fenster können Sie die Firmware-Datei im Verzeichnissystem suchen und anschließend auf die Schaltfläche **Upload** klicken.

Terminalprogramm (z.B. Hyperterminal von Windows)

Stellen Sie bei Terminalprogrammen im Menü 'Firmware' mit dem Befehl 'set Modus-Firmsafe' zunächst ein, in welchem Modus Sie die neue Firmware laden wollen (unmittelbar, login oder manuell). Stellen Sie ggf. zusätzlich mit 'set Timeout-Firmsafe' die Zeit für den Firmwaretest ein.

Mit dem Befehl 'do Firmware-Upload' wird der Router anschließend in Empfangsbereitschaft versetzt. Starten Sie anschließend 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 Datei zum Upload aus.
- Bei Hyperterminal klicken Sie auf **Übertragung** ▶ **Datei senden**, wählen die Datei aus, stellen 'XModem' als Protokoll ein und starten mit **OK**.

Der Firmware-Upload über ein Terminalprogramm kann nur über die serielle Konfigurationsschnittstelle erfolgen.

TFTP

Auf LANCOM kann auch mit TFTP eine neue Firmware aufgespielt werden. Dazu wird der Befehl (bzw. das Ziel) **writeflash** angegeben. Um eine neue Firmware in einen LANCOM mit der IP-Adresse 10.0.0.1 zu übertragen, geben Sie z.B. unter Windows XP, Windows 2000 oder Windows NT folgenden Befehl ein:

```
tftp -i 10.0.0.1 put Lc_16xxu.282 writeflash
```

Firmwareupload über die serielle Schnittstelle mit Rücksetzen der Konfiguration

Auch über die serielle Schnittstelle kann eine Firmware in das Gerät geladen werden. Wenn Sie dabei statt des Konfigurations-Passwortes die Seriennummer verwenden, wird die Konfiguration des Gerätes wie bei einem Reset vollständig auf den Auslieferungszustand zurückgesetzt. Auf diese Weise können Sie sich wieder einen Zugang zu einem Gerät verschaffen, wenn das Konfigurationskennwort nicht mehr verfügbar ist und der Reset-Taster auf 'Ignorieren' oder 'Nur-Booten' eingestellt ist.

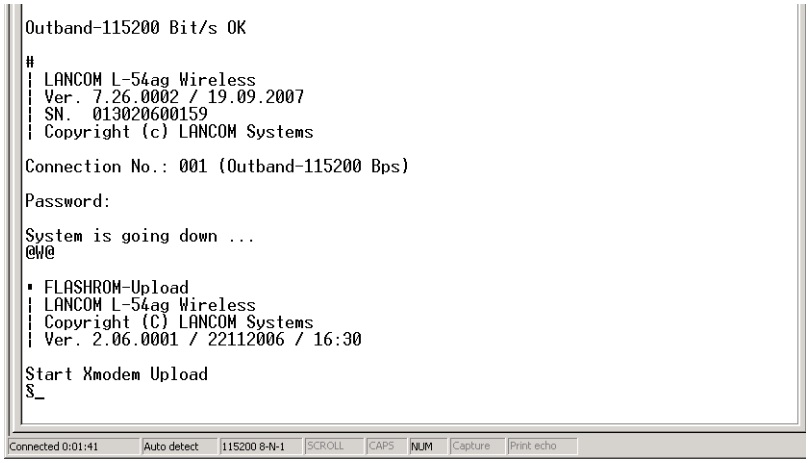
① Schliessen Sie das Gerät über das serielle Konfigurationskabel an einen Rechner an.

② Starten Sie auf diesem Rechner ein Terminal-Programm, z.B. Hyperterminal.

③ Starten Sie eine Verbindung mit den Einstellungen 115200bps, 8n1, Hardware-Handshake (RTS/CTS).

④ Drücken Sie im Begrüßungsbildschirm des Terminal-Programms die Return-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 Return.



⑥ Das Gerät erwartet nun den Firmware-Upload. Klicken Sie dazu z.B. unter Hyperterminal auf **Übertragung** ▶ **Datei senden** und wählen Sie X-Modem als Übertragungsprotokoll aus.

Bei diesem Firmware-Upload wird die Konfiguration vollständig gelöscht und auf den Auslieferungszustand zurückgesetzt! Nutzen sie diese Möglichkeit daher nur, wenn das Konfigurationskennwort nicht mehr verfügbar ist.

3.12 Dateien von einem TFTP- oder HTTP-Server direkt in das Gerät laden

Neu in LCOS 7.60:

- Angabe von Server, Pfad und Datei in URL-Schreibweise
- Laden von Dateien in das Gerät von einem HTTP(S)-Server

Bestimmte Funktionen lassen sich über Telnet nicht oder nicht befriedigend ausführen. Dazu gehören alle Funktionen, bei denen komplette Dateien übertragen werden, etwa der Upload von Firmware oder die Speicherung und Wiederherstellung von Konfigurationsdaten. In diesen Fällen wird TFTP oder HTTP(S) eingesetzt.

3.12.1 TFTP

TFTP steht unter den Windows-Betriebssystemen standardmäßig zur Verfügung. Es ermöglicht den einfachen Dateitransfer von Dateien mit anderen Geräten über das Netzwerk.

Die Syntax des TFTP-Aufrufs ist abhängig vom Betriebssystem. Unter Windows lautet die Syntax:

```
tftp -i <IP-Adresse Host> [get|put] Quelle [Ziel]
```

Bei zahlreichen TFTP-Clients ist das ASCII-Format voreingestellt. Für die Übertragung binärer Daten (z.B. Firmware) muss daher meist die binäre Übertragung explizit gewählt werden. In diesem Beispiel für Windows erreichen Sie das durch den Parameter '-i'.

Sofern das Gerät mit einem Passwort geschützt ist, müssen Username und Passwort in den TFTP-Befehl eingebaut werden. Der Filename baut sich entweder aus dem Master-Passwort und dem auszuführenden Kommando (für Supervisoren) oder aus der Kombination von Username und Passwort (für lokale Administratoren), die durch einen Doppelpunkt getrennt sind, und nachgestelltem Kommando zusammen. Ein über TFTP abgesetztes Kommando sieht daher wie folgt aus:

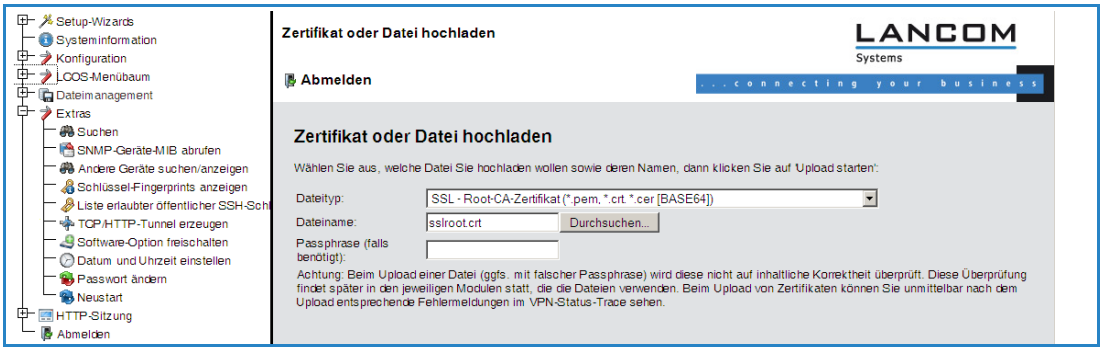
- <Master-Passwort><Kommando> bzw.
- <Username>:<Passwort>@<Kommando>

Die Rechte zur Nutzung von TFTP können für die Administratoren eingeschränkt werden, siehe auch "Rechteverwaltung für verschiedene Administratoren".

3.12.2 Firmware, Geräte-Konfiguration oder Script über HTTP(S) laden

Durch die Unterstützung von HTTP und speziell HTTPS lässt sich der Download von Firmware, Geräte-Konfiguration oder Scripts auch für automatisierte Prozesse (z.B. Self-Provisioning) auf LANCOM-Geräten nutzen, welche die Dateien über das Internet beziehen. In der Praxis ist es zumeist sehr viel leichter, einen HTTPS-Server zentral mit eindeutiger Adresse (URI) im Internet bereit zu stellen als einen TFTP-Server - ggf. lässt sich ein bestehender Webserver um diese Funktionalität erweitern.

Ein optional für den HTTPS-Server verwendetes Zertifikat wird über WEBconfig als SSL-Root-CA-Zertifikat in das Gerät hochgeladen:



3.12.3 Firmware, Geräte-Konfiguration oder Script über HTTP(S) oder TFTP laden

Neben den Möglichkeiten, eine Firmware oder eine Konfigurationsdatei über LANconfig oder WEBconfig in ein Gerät einzuspielen, kann der Upload der entsprechenden Dateien über Telnet oder SSH auch direkt von einem HTTP(S)- oder TFTP-Server erfolgen. Dieses Vorgehen kann in größeren Installationen mit regelmäßigem Update von Firmware und/oder Konfiguration die Administration der Geräte erleichtern. Über HTTP(S) bzw. TFTP können auch Scripte – z.B. mit Teilkonfigurationen – in die Geräte geladen werden.

Dazu werden die Firmware- und Konfigurationsdateien oder Scripte auf einem HTTP(S)- bzw. TFTP-Server abgelegt. Ein TFTP-Server gleicht in der Funktionsweise einem FTP-Server, verwendet allerdings zur Datenübertragung ein anderes Protokoll. Bei der Verwendung eines HTTPS-Servers kann im Gerät ein Zertifikat hinterlegt werden, mit dem die Identität des Servers geprüft wird. Von diesem Server können die Dateien mit folgenden Befehlen abgerufen werden:

- `LoadConfig`
- `LoadFirmware`
- `LoadScript`

Der Server, das Verzeichnis und die Datei können auf zwei verschiedene Arten angegeben werden:

- Bei Nutzung des TFTP-Protokolls über die Parameter -s und -f :
  - `-s <Server-IP-Adresse oder Server-Name>`
  - `-f <Dateipfad und Dateiname>`
- Für die Nutzung von TFTP oder HTTP(S) kann der Befehl in der üblichen URL-Schreibweise angegeben werden (als Protokoll wird entweder TFTP oder HTTP(S) eingetragen):
  - `Befehl Protokoll://Server/Verzeichnis/Dateiname`

  Beim Zugriff auf einen kennwortgeschützten Bereich auf einem HTTP(S)-Server werden Benutzername und Kennwort entsprechend eingetragen:
  - `Befehl Protokoll://Benutzername:Kennwort@Server/Verzeichnis/Dateiname`

  Bei der Verwendung von HTTPS kann ein Zertifikat angegeben werden, mit dem die Identität des Servers geprüft wird:
  - `-c <Name des Zertifikats>`

Im Dateinamen inklusive Pfad sind folgende Variablen erlaubt:

- %m - LAN MAC Adresse (Hexadezimal, kleine Buchstaben, ohne Trennzeichen)
- %s - Seriennummer
- %n - Gerätename
- %l - Ort ('Standort' - aus der Konfiguration)
- %d - Gerätetyp

Beispiele:

Mit dem folgenden Befehl in einer Telnet-Sitzung wird eine Firmwaredatei mit dem Namen 'LC-1811-5.00.0019.upx' aus dem Verzeichnis 'LCOS/500' vom Server mit der IP-Adresse '192.168.2.200' in das Gerät geladen:

- `LoadFirmware -s 192.168.2.200 -f LCOS/500/LC-1811-5.00.0019.upx`

Mit dem folgenden Befehl in einer Telnet-Sitzung wird ein zur MAC-Adresse passendes Script vom Server mit der IP-Adresse '192.168.2.200' in das Gerät geladen:

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

Mit dem folgenden Befehl in einer Telnet-Sitzung wird eine Firmwaredatei mit dem Namen 'LC-1811-5.00.0019.upx' aus dem Verzeichnis 'download' vom HTTPS-Server mit der IP-Adresse 'www.myserver.com' in das Gerät geladen. dabei wird die Identität des Servers mit dem Zertifikat “sslroot.crt” geprüft:

- `LoadFirmware -c sslroot.crt https://www.myserver.com/download/LC-1811-5.00.0019.upx`

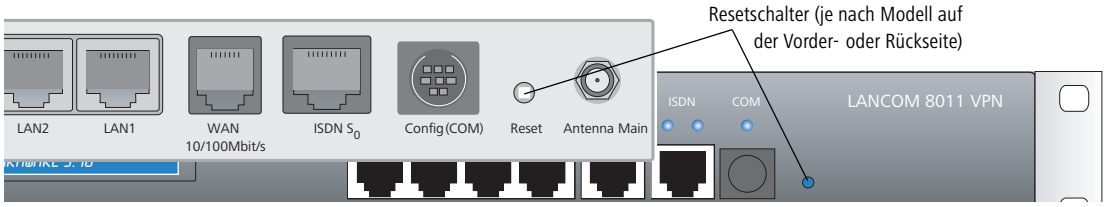
Werden die Parameter `-s` und/oder `-f` nicht angegeben, verwendet das Gerät die Standardwerte, die unter dem Pfad `/setup/config/TFTP-Client` gesetzt werden:

- `Config-Adresse`
- `Config-Dateiname`
- `Firmware-Adresse`
- `Firmware-Dateiname`

Die Nutzung dieser Standardwerte bietet sich an, wenn die aktuellen Konfigurationen und Firmware-Versionen immer unter dem gleichen Namen an der gleichen Stelle gespeichert werden. In diesem Fall können mit den einfachen Befehlen `LoadConfig` und `LoadFirmware` die jeweils gültige Dateien geladen werden.

3.13 Wie führt man einen Gerätereset durch?

Wenn Sie unabhängig von den evtl. vorhandenen Einstellungen das Gerät neu konfigurieren müssen oder keine Verbindung zur Gerätekonfiguration zustande kommt, können Sie mit einem **Reset** das Gerät in den Auslieferungszustand zurücksetzen. Dazu müssen Sie den Resetschalter betätigen, bis die LEDs des Geräts aufleuchten (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 Geräts!

Beachten Sie, dass bei einem Reset auch die im Gerät definierten WLAN-Verschlüsselungseinstellungen verloren gehen und auf den **Standard-WEP-Schlüssel** zurückgesetzt werden. Die drahtlose Konfiguration eines Geräts mit WLAN-Schnittstelle gelingt nach einem Reset nur, wenn der Standard-WEP-Schlüssel in der WLAN-Karte eingetragen ist!

Der Reset-Taster hat mit Booten (Neustart) und Reset (Rücksetzen auf Werkseinstellung) grundsätzlich zwei verschiedene Funktionen, die durch unterschiedlich lange Betätigungszeiten des Tasters 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-Taster zu lange gedrückt hält. Mit einer entsprechenden Einstellung kann das Verhalten des Reset-Tasters gesteuert werden (nur für Geräte mit serieller Konfigurationsschnittstelle):

WEBconfig: LCOS-Menübaum ▶ Setup ▶ Config

- **Reset-Taster**

  Mit dieser Option wird das Verhalten des Reset-Tasters gesteuert:

  - □ Ignorieren: Der Taster wird ignoriert.
  - □ Nur-Booten: Beim Druck auf den Taster wird nur ein Neustart ausgelöst, unabhängig von der gedrückten Dauer.

Bitte beachten Sie folgenden Hinweis: Mit der Einstellung 'Ignorieren' oder 'Nur-Booten' wird das Rücksetzen der Konfiguration auf den Auslieferungszustand durch einen Reset unmöglich gemacht. Falls für ein Gerät in diesem Zustand das Konfigurationskennwort 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 wird gelöscht. Hinweise zum Firmware-Upload über die serielle Konfigurationsschnittstelle finden Sie unter 'Firmwareupload über die serielle Schnittstelle mit Rücksetzen der Konfiguration' → Seite 3-46.

  - □ Reset-oder-Booten (Standardeinstellung): Ein kurzer Druck auf den Taster führt zum Neustart, ein Druck von 5 Sekunden oder länger führt zum Neustart mit dem Rücksetzen der Konfiguration auf den Auslieferungszustand. Alle LEDs am Gerät leuchten dauerhaft auf. Sobald der Taster freigegeben wird, startet das Gerät mit Werkseinstellungen neu.

Bei einem harten Reset startet das Gerät mit Werkseinstellungen neu, alle bisherigen Einstellungen gehen dabei verloren!

Beachten Sie, dass bei einem Reset auch die im Gerät definierten WLAN-Verschlüsselungseinstellungen verloren gehen und auf den Standard-WEP-Schlüssel zurückgesetzt werden.

4 Erweitertes Management

Die LANtools (bestehend aus LANconfig und LANmonitor) eignen sich hervorragend zum Konfigurieren und Überwachen von LANCOM-Geräten in komplexen Anwendungsszenarien. Mehrere Router und/oder Wireless Access Points können in einem Netzwerk dabei genauso von einer zentralen Stelle aus administriert werden wie Geräte in verteilten Netzwerken, z.B. bei den Kunden eines Dienstleisters.

Beim Netzwerk-Management mit den LANtools stehen u.a. folgende Funktionen im Vordergrund:

- Konfiguration der Geräte
- Konfigurationsverwaltung, also sichern und wiederherstellen der Einstellungen
- Einspielen von neuen Firmware-Versionen
- Freischalten zusätzlicher Software-Optionen
- Überwachung des Gerätestatus
- Überwachung der Verbindungen (inklusive VPN)
- Überwachung der Firewallaktionen

4.1 Scripting

In Installationen mit mehreren LANCOM-Geräten ist oft erwünscht, bestimmte Aufgaben der Konfiguration automatisiert auszuführen. Die Scripting-Funktionen im LANCOM erlauben es, ganze Sätze von Befehlen zur Konfiguration der Geräte in einer Datei – einem Script – zu speichern und in einem Vorgang in ein oder mehrere Geräte zu übertragen.

4.1.1 Anwendungen

Mit dem Scripting steht dem Anwender ein sehr mächtiges Werkzeug zur zentralen Konfiguration der LANCOM-Geräte mit vielfältigen Anwendungsmöglichkeiten zur Verfügung:

- Auslesen der Geräte-Konfiguration in einer gut lesbaren und speicherbaren Form

  Die von LANconfig erzeugten Konfigurationsdateien sind nicht zur direkten Bearbeitung mit anderen Tools vorgesehen, einen direkten Überblick über die komplette Konfiguration erhält der Anwender nur mit einem Ausdruck der Konfigurationsdatei. Mit den Scripting-Funktionen lässt sich die Konfiguration als ASCII-Text ausgeben, der z.B. als einfache Textdatei gespeichert werden kann.

- Bearbeiten der Konfiguration mit einem einfachen Texteditor

  Wenn die Offline-Konfiguration mit LANconfig nicht möglich ist oder nicht sinnvoll erscheint, kann eine mit Hilfe des Scripting erzeugte Konfigurationsdatei mit einem Texteditor bearbeitet und anschließend wieder in das Gerät zurückgespielt werden.

- Bearbeiten von Teilkonfigurationen

  Anstelle einer kompletten Konfiguration können gezielt auch nur Teile davon aus einem Gerät ausgelesen werden (z.B. die Firewall-Einstellungen). Genau wie eine Komplettkonfiguration können auch Teilkonfigurationen bearbeitet und wieder in ein oder mehrere Geräte übertragen werden. Spezielle Einstellungen eines Gerätes können auf diese Weise auch in andere Modelle oder Geräte mit einem anderen Firmware-Stand eingespielt werden.

- Automatisieren von Konfigurationsupdates

  Durch die zentrale Ablage von Konfigurationsscripten im Zusammenhang mit zeitgesteuerten LCOS-Befehlen (Cron-Jobs) können wichtige Konfigurationsteile wie z.B. die Verschlüsselungseinstellungen für ein WLAN automatisch in vielen Geräten auf dem gleichen Stand gehalten werden.

- Komfortabler Roll-Out in größeren Installationen

  Bei der Installation von mehreren Geräten an unterschiedlichen Orten kann die Konfiguration sehr leicht zentral vorbereitet werden. Die Geräte können dann dezentral von Mitarbeitern ohne Administrator-Kenntnisse über einen einzigen Befehl eingestellt werden.

- Speichern der Konfiguration in einem nicht bootresistenten Modus

  Mit den Scripting-Befehlen können die Änderungen der Konfiguration gezielt nur im RAM vorgenommen werden, die Übertragung in den bootresistenten Flash-Speicher wird verhindert. Auf diese Weise kann die Konfiguration gezielt nur bis zum nächsten Boot-Vorgang vorgehalten werden, um z.B. im Falle eines Diebstahls keine wichtigen Bestandteile der Konfiguration in fremde Hände gelangen zu lassen.

- Änderungen der Konfiguration im Testmodus

  Über den gleichen Mechanismus lässt sich die Konfiguration sehr leicht im Testmodus ändern. Dabei wird mit Hilfe eines Scriptes ein zeitverzögerter Bootvorgang ausgelöst, bis zu dessen Aktivierung die Konfiguration des Gerätes gefahrlos verstellt werden kann. Falls die Änderungen der Konfiguration nicht erfolgreich sind, wird das

Gerät nach dem Ablauf der Verzögerungszeit und dem folgenden Boot-Vorgang automatisch wieder in den vorherigen Konfigurationszustand zurückversetzt.

Mit dieser Variante lässt sich in Analogie zur FirmSafe-Funktion auch eine Art „ConfSafe" realisieren. Wird nach einem Upgrade der Firmware die Konfiguration geändert, kann nach einem späteren Downgrade zur alten Firmware-Version die Konfiguration manchmal nicht mehr editiert werden. Wird hingegen die Konfiguration nach dem Firmware-Upgrade nur im Testmodus geändert, kann durch das Downgrade und den folgenden Bootvorgang sehr leicht der ursprüngliche Zustand der Geräte bzgl. Firmware **und** Konfiguration wieder hergestellt werden.

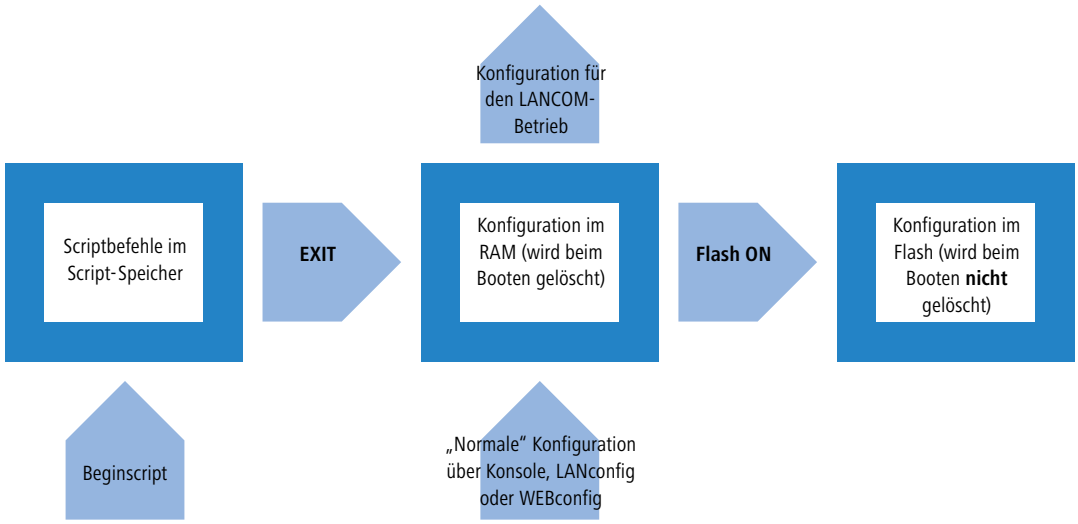
4.1.2 Funktion des Scripting

Beim Scripting wird eine Reihe von Konfigurationsbefehlen, so wie sie an der Konsole unter Telnet o.ä. eingegeben werden, gesammelt an ein LANCOM übertragen. Für diese Sammelübertragung von Konfigurationsbefehlen gibt es zwei Varianten:

- Das Gerät wird in einer Konsolensitzung mit dem Befehl `beginscript` in den Script-Modus versetzt. In diesem Zustand werden die übertragenen Befehle nicht einzeln ausgeführt, sondern zunächst in einen Zwischenspeicher (Script-Speicher) im LANCOM geschrieben. Erst durch ein weiteres Kommando (`exit`) wird die Ausführung der gespeicherten Befehle gestartet.
- Alternativ werden die Konfigurationsbefehle in einer Scriptdatei (Textdatei) offline gesammelt und editiert und dann als fertiges Script in das Gerät geladen.

Die über das Script ausgeführten Konfigurationsbefehle wirken sich zunächst nur auf die Konfiguration aus, die im RAM des Gerätes gespeichert ist. Der Flash-Modus entscheidet dann darüber, ob die Konfiguration auch im Flash geändert wird:

- Im Flash-Yes-Modus (Standard) werden die Konfigurationsbefehle auch gleichzeitig in den Flashspeicher des Gerätes geschrieben und werden damit bootresistent. Da bei der Konfiguration über die anderen Wege (Konsole ohne Script, LANconfig oder WEBconfig) der Flash-Modus immer auf ON steht, wird in diesen Varianten die Konfiguration nacheinander in den RAM-Speicher und dann direkt in den Flash geschrieben.



- Im Flash-No-Modus werden die Daten nur in den RAM geschrieben und sind damit nur bis zum nächsten Bootvorgang verfügbar.
  - □ Bei Booten holt sich das Gerät die aktuell im Flash gespeicherte Konfiguration.
  - □ Die Konfiguration aus dem RAM kann jederzeit mit dem Befehl „Flash Yes" in den Flash-Speicher übertragen werden.

Die LANCOM-Geräte verwenden für den aktiven Betrieb die Informationen, die in der RAM-Konfiguration gespeichert sind. Die im Zwischenspeicher gelagerten Scriptbefehle sind ebenso wie die Konfiguration im Flash für die aktuelle Funktionalität eines LANCOM nicht relevant.

4.1.3 Scriptdateien erstellen

Ein Script für eine LANCOM-Konfiguration liegt in Form einer normalen Textdatei vor. Sie enthält neben ggf. erforderlichen Kommentaren alle Befehle, so wie sie z.B. an der Telnet-Konsole zur Konfiguration angewendet würden. Zur Erstellung der Scriptdateien gibt es zwei verschiedene Wege:

- Das Script wird mit Hilfe eines Texteditors manuell komplett neu erstellt.
- Aus einem Gerät wird eine (Teil-)Konfiguration ausgelesen, als Scriptdatei gespeichert und dann mit dem Texteditor geeignet bearbeitet.

Beim Auslesen eines Scriptes aus einem Gerät werden standardmäßig nur die Parameter aufgeführt, die in der Konfiguration gegenüber dem Default-Zustand geändert wurden ('`readscript`' → Seite 4-6). Ein komplettes Konfigurationsscript kann mit einem speziellen Befehlszusatz ausgelesen werden ('`default`' → Seite 4-8).

Konfiguration über die Konsole auslesen

① Melden Sie sich an der Konsole mit Supervisor-Rechten an.

② Wechseln Sie ggf. in den Zweig des Konfigurationsbaumes, dessen Teilkonfiguration Sie auslesen möchten.

③ Führen Sie an der Eingabeaufforderung den Befehl `readscript` aus. Beachten Sie dazu die möglichen Befehlserweiterungen ('Die Befehle für das Scripting' → Seite 4-6).

④ Kopieren Sie die gewünschten Textpassagen über die Zwischenablage in einen Texteditor und bearbeiten Sie dort das Script wie gewünscht.

Über TFTP vom Kommandozeilen-Interface (DOS-Box)

Die Befehle zur Konfiguration können vom Kommandozeilen-Interface direkt über TFTP ausgelesen werden.

① Öffnen Sie dazu z.B. eine DOS-Box.

② Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
C:\>tftp IP-Adresse get "PASSWORDreadscript Pfad" script.lcs
```

- □ IP-Adresse ist die Adresse des Gerätes, aus dem Sie die Konfigurationsbefehle auslesen möchten
- □ PASSWORD ist das entsprechende Geräte-Passwort
- □ Pfad gibt den Zweig im Menübaum der Konfiguration an, der ausgelesen werden soll. Fehlt die Pfad-Angabe, wird die gesamte Konfiguration ausgelesen.
- □ script.lcs ist der Name der Script-Datei, unter der die Befehle im aktuellen Verzeichnis gespeichert werden.

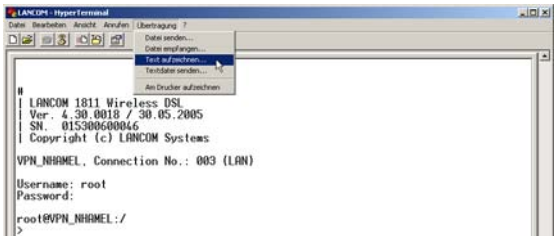
Beachten Sie, dass die Passwörter der Geräte bei der Eingabe dieses Befehls im Klartext angezeigt werden!

Über Hyperterminal

Terminalprogramme wie Hyperterminal bieten die Möglichkeit, die an der Konsole ausgegebenen Texte direkt in eine Textdatei zu speichern. Mit diesem Verfahren kann man gerade bei umfangreichen Konfigurationsdateien die manchmal unübersichtliche Übertragung über die Zwischenablage umgehen.

① Stellen Sie mit Hyperterminal eine Verbindung zu Ihrem Gerät her.

② Wählen Sie den Menüpunkt **Übertragung ▶ Textdatei aufzeichnen** und wählen Sie den gewünschten Speicherort für das Script mit dem Dateinamen aus.



③ Führen Sie an der Eingabeaufforderung den Befehl `readscript` aus. Beachten Sie dazu die möglichen Befehlserweiterungen ('Die Befehle für das Scripting' → Seite 4-6).

④ Sobald alle Teilkonfigurationen wie gewünscht aufgerufen wurden, beenden Sie die Aufzeichnung über den Menüpunkt **Übertragung ▶ Textdatei aufzeichnen ▶ Beenden**.

Die Konfigurationsbefehle liegen nun als Scriptdatei vor und können entsprechend bearbeitet werden.

Script aus Gerät downloaden

In Installationen mit mehreren LANCOM-Geräten ist oft erwünscht, bestimmte Aufgaben der Konfiguration automatisiert auszuführen. Die Scripting-Funktionen im LANCOM erlauben es, ganze Sätze von Befehlen zur Konfiguration

der Geräte in einer Datei – einem Script – zu speichern und in einem Vorgang in ein oder mehrere Geräte zu übertragen.

Neben der manuellen Erstellung eines Scripts und dem Auslesen über die Konsole können Script-Dateien auch mit Hilfe von LANconfig aus einem Gerät ausgelesen werden. Klicken Sie dazu mit der rechten Maustaste auf den entsprechenden Eintrag in der Geräte-Liste und wählen Sie im Kontext-Menü den Eintrag **Konfigurations-Verwaltung ▶ Als Script-Datei sichern**. Wählen Sie dabei folgende Optionen:

- **Sektion numerisch**

  Aktivieren Sie diese Option, wenn die Sektionen der Konfiguration im Script nicht im Klartext (z.B. `/setup/wlan/ppp`) sondern numerisch angegeben werden sollen (`/2/2/5`).

- **Standard-Werte**

  Ohne weitere Angaben werden in einem Script immer nur die Werte gesichert, die von den Default-Werten abweichen. Aktivieren sie diese Option, wenn auch die Standard-Werte mit in das Script eingetragen werden sollen.

- **Spalten-Namen**

  Ohne weitere Angaben werden in den Scripten zunächst die Felder einer Tabelle als Spaltennamen angegeben, danach werden nur die jeweiligen Werte in die Zeilen eingefügt. Aktivieren sie diese Option, wenn jeder Wert in der Tabelle explizit mit der Bezeichnung der Spalte versehen sein soll, in der er abgelegt wird.

- **Kommentare**

  Aktivieren Sie diese Option, wenn zusätzliche Kommentare in die Script-Datei aufgenommen werden sollen.

- **Kompakt formatiert**

  □ Aktivieren Sie diese Option, wenn Leerzeilen und Tabulatoren unterdrückt werden sollen.

- **Nur ausgewählte Sektionen herunterladen**

  Ohne weitere Angaben wird in einem Script immer die gesamte Geräte-Konfiguration gesichert. Abweichend davon können durch Angabe der Sektionen auch Teilkonfigurationen gesichert werden. Tragen Sie in diesem Feld die Sektionen ein, die in das Script übertragen werden sollen, z.B. `/setup/wlan`.

4.1.4 Einspielen von Konfigurations-Befehlen und Script-Dateien

Grundsätzlich können die Scriptbefehle auf zwei verschiedenen Wegen in den Zwischenspeicher des LANCOM gelangen:

- Die Befehle können an einer Konsole im Script-Modus (mit dem Befehl „beginscript“) manuell eingegeben werden. Dabei werden die Befehle direkt aus der Konsole in den Zwischenspeicher geschrieben. Nachdem alle Befehle wie gewünscht fertiggestellt sind, werden sie mit dem Befehl „exit“ abgearbeitet und in das RAM übertragen.
- Die gewünschten Befehlssequenzen können in einer Textdatei gespeichert werden. Diese Textdatei wird dann über geeignete Wege (LANconfig, Terminalprogramm, TFTP) an den Zwischenspeicher gesendet. Wenn die erforderlichen Befehle in der Datei enthalten sind, wird dann automatisch die Übertragung der Konfiguration in das RAM gestartet.

Zum Einspielen von Scriptdateien in die LANCOM-Geräte gibt es verschiedene Möglichkeiten, von denen Sie je nach verwendetem Konfigurationstool den für Sie passenden Weg auswählen können.

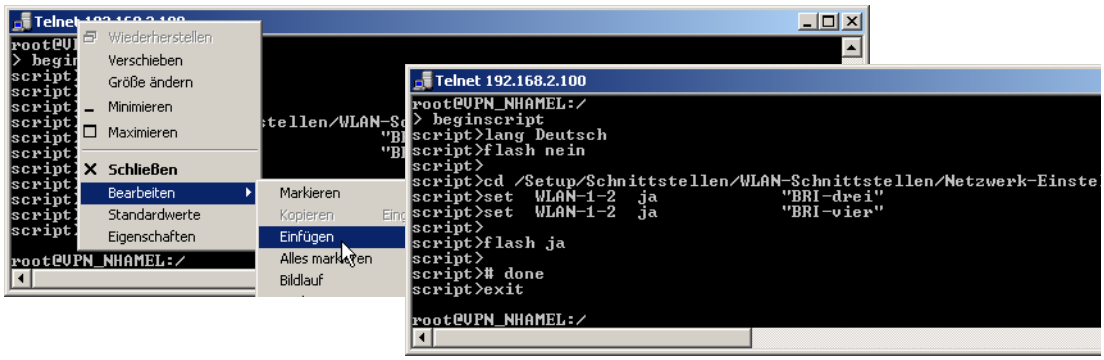
Befehlseingabe über Konsolen-Sitzung (Telnet, SSH)

In einer Konsolensitzung können Sie ein Script über die Zwischenablage in das Gerät einspielen:

① Öffnen Sie Ihr Script in einem beliebigen Texteditor und übertragen Sie die Konfigurationsbefehle in die Zwischenablage.

② Melden Sie sich an der Konsole mit Supervisor-Rechten an.

③ Starten Sie den Script-Modus mit dem Befehl `beginscript`.



④ Fügen Sie nach dem Script-Prompt (`script>`) die Befehle aus der Zwischenablage ein. Unter Telnet z.B. mit einem rechten Mausklick auf den oberen Fensterrand.

⑤ Mit dem Befehl `exit` wird die Ausführung der Konfigurationsbefehle gestartet.

Falls der Befehl `exit` schon in den kopierten Befehlen enthalten ist, wird die Ausführung der Konfiguration gleich nach dem Einfügen automatisch gestartet!

Script hochladen mit TFTP-Client

Während einer Konsolensitzung (z.B. über Telnet oder SSH) können mit Hilfe des TFTP-Befehls auch Script-Dateien von einem TFTP-Server direkt in das Gerät geladen werden.

① Melden Sie sich an der Konsole mit Supervisor-Rechten an.

② Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
>loadscript -s IP-Adresse -f script.lcs
```

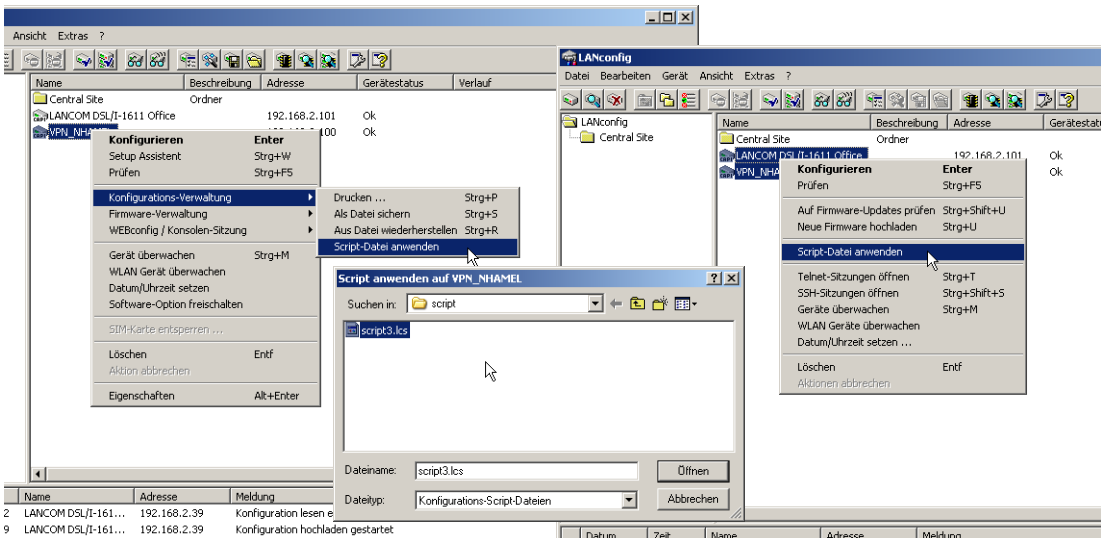
- IP-Adresse ist die Adresse des TFTP-Servers, auf dem die Script-Datei liegt
- script.lcs ist der Name der Script-Datei auf dem TFTP-Server

Script hochladen mit LANconfig

Unter LANconfig haben Sie die Möglichkeit, ein Script entweder nur auf ein Gerät oder parallel auf viele Geräte gleichzeitig anzuwenden.

① Klicken Sie mit der rechten Maustaste auf ein Gerät und wählen Sie im Kontextmenü den Eintrag **Konfigurationsverwaltung ▶ Script-Datei anwenden**. Bei mehreren markierten Geräten erscheint der Eintrag **Script-Datei anwenden** direkt im Kontextmenü.

② Wählen Sie im folgenden Dialog die gewünschte Script-Datei (*.lcs) für den Upload aus.



Der Upload des Scriptes wird automatisch gestartet. Status- und Fehlermeldungen werden entweder über LANconfig direkt ausgegeben oder können in einer Konsolensitzung mit dem Befehl `show script` eingesehen werden.

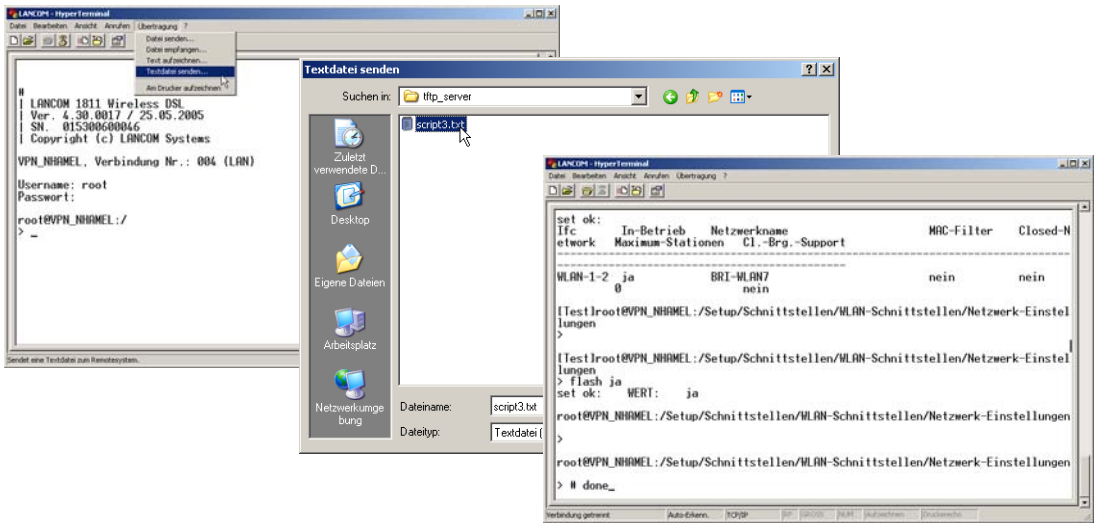
Script hochladen mit Hyperterminal

Auch über Terminalprogramme wie das mit Windows gelieferte Hyperterminal können Scripte in ein LANCOM geladen werden.

① Stellen Sie mit Hyperterminal eine Verbindung zu Ihrem Gerät her.

② Wählen Sie den Menüpunkt **Übertragung ▶ Textdatei senden**.

③ Wählen Sie die gewünschte Scriptdatei und starten Sie die Übertragung.



Nach dem erfolgreichen Beenden der Übertragung wird das Script automatisch gestartet.

4.1.5 Mehrere Script-Sessions parallel

Das LANCOM kann mehrere Script-Sessions parallel verwalten. So wie mehrere Konsolensitzungen gleichzeitig auf einem Gerät ablaufen können, können auch verschiedene Scripte gleichzeitig auf das LANCOM zugreifen. Parallele Script-Sessions machen z.B. in folgenden Szenarien Sinn:

- Mit einem Script ① wird ein zeitverzögerter Reboot des Gerätes gestartet, z.B. nach Ablauf von 30 Minuten. Mit einem zweiten Script ② wird während der Laufzeit des Gerätes die Konfiguration zu Testwecken verändert, der Flash-Modus wird dabei ausgeschaltet. Sollte das Gerät durch die Konfigurationsänderungen von Script ② nicht mehr erreichbar sein, startet Script ① das Gerät nach 30 Minuten neu und verwirft so die Änderungen in der Konfiguration.
- Bei der Anwendung von verschiedenen Scripten für Teilkonfigurationen können mehrere Scripte z.B. über Cron-Jobs automatisch gleichzeitig gestartet werden. Die einzelnen Konfigurationsaufgaben müssen dabei nicht abwarten, bis das vorhergehende Script abgearbeitet ist.

4.1.6 Die Befehle für das Scripting

- `readscript`

  Der Befehl readscript erzeugt in einer Konsolensitzung eine Textausgabe von allen Befehlen und Parametern, die für die Konfiguration des LANCOM im aktuellen Zustand benötigt werden. Im einfachsten Fall gibt das LANCOM nur die Befehle aus, mit denen von der Grundeinstellung abweichende Parameter modifiziert werden.

  Syntax: `readscript [-n] [-d] [-c] [-m] [PATH]`

Um diesen Befehl auszuführen sind Supervisor-Rechte erforderlich.

Beispiel: Der Befehl readscript führt ohne weitere Einschränkungen bei einem LANCOM, für das nur ein Internet-by-Call-Zugang über ISDN eingerichtet wurde, zu folgender Ausgabe an der Konsole:



An diesem Beispiel ist das Verhalten des Scripts zu erkennen, das mit dem Befehl `readscript` erzeugt wird.

- Zunächst werden nur die Parameter aufgeführt, die in der Konfiguration gegenüber dem Default-Zustand geändert wurden.
- Die Werte in den Tabellen und für einzelne Werte werden jeweils gelöscht (`del *`) und mit den aktuellen Werten der Konfiguration neu gesetzt (`add *`).
- Nur Tabelleneinträge oder Werte, die nicht leer sein dürfen, werden mit dem `Set`-Befehl direkt geändert.



Bei Tabellenzeilen oder Strings, die Passwörter enthalten, werden die Passwörter im Klartext ausgegeben, da diese Form auch von der Telnetoberfläche verlangt wird.

Mit dem erzeugten Script ist der Anwender in der Lage, ein LANCOM genau so zu konfigurieren wie das Ursprungsgerät.

Da die Scripte zur Anpassung der Konfiguration in manchen Fällen sehr umfangreich sind, können auch gezielt Scripte von Teilen der Konfiguration erzeugt werden. Dazu wechseln Sie z.B. zunächst in das Verzeichnis, dessen Konfiguration Sie in einem Script festhalten wollen (z.B. `cd set/ip-router/firewall` für die Firewalleinstellungen) und führen dann den `readscript`-Befehl aus. Alternativ übergeben Sie den Pfad zum gewünschten Menü direkt mit dem `readscript`-Befehl als Path-Parameter (z.B. `readscript set/ip-router/firewall`). In beiden Fällen werden nur die – im Vergleich zur Default-Konfiguration – geänderten Einstellungen der Firewall in das Script übernommen.

Mit folgenden Optionen kann der readscript-Befehl zusätzlich erweitert werden:

- `-d (default)`: Dabei werden auch die Befehle zur Modifikation derjenigen Parameter erzeugt, die den gleichen Wert wie in der Grundkonfiguration haben. Solche umfangreichen Scripte eignen sich z.B. bei der Übertragung von Konfigurationen auf Geräte eines anderen Typs oder mit einem anderen Firmwarestand, da die Grundkonfiguration in diesen Fällen abweichen kann.
- `-n (numeric)`: Mit diesem Zusatz werden die Pfade im Script nicht im Klartext, sondern numerisch anhand der SNMP-Bezeichnung ausgegeben. Auch diese Variante trägt zur Übertragbarkeit von Scripten auf andere Firmwarestände bei, da sich die Bezeichnungen der Pfade durchaus ändern können, die Positionen im SNMP-Baum jedoch üblicherweise nicht.
- `-c (comment)`: Dieser Parameter erzeugt im Zusammenspiel mit `-d` und `-n` zusätzliche Kommentare, die das Lesen der Scripte erleichtern. Für den Parameter `-d` wird jede Befehlskombination die einen Defaultwert setzt mit `# default value` gekennzeichnet. Bei `-n` wird jeder numerische Pfad mit seinem textuellen Äquivalent kommentiert.

- □ `-m (minimize)`: Mit diesem Parameter werden vorhandene Lücken aus dem Script entfernt, die Datei wird kleiner und kompakter.

■ `#`

Das Zeichen # am Zeilenbeginn – gefolgt von einem Leerzeichen – leitet einen Kommentar ein. Bis zum Zeilenende werden alle Zeichen ignoriert.



Das Leerzeichen nach dem # ist zwingend erforderlich.

■ `del *`

Dieser Befehl löscht eine komplette Tabelle in dem mit `Path` angegebenen Zweig des Menübaums.

Syntax: `del [PATH]*`

■ `default`

Mit diesem Befehl ist es möglich, einzelne Parameter, Tabellen oder ganze Menübaume in die Grundkonfiguration zurückzusetzen.

Syntax: `default [-r] [PATH]`

Dieser Befehl setzt den mit `PATH` adressierten Parameter auf den Grundzustand. Zeigt `PATH` auf einen Zweig des Menübaums, muss zwingend die option `-r` (recursive) angegeben werden.



Um diesen Befehl auszuführen sind Supervisor-Rechte erforderlich.

■ `beginscript`

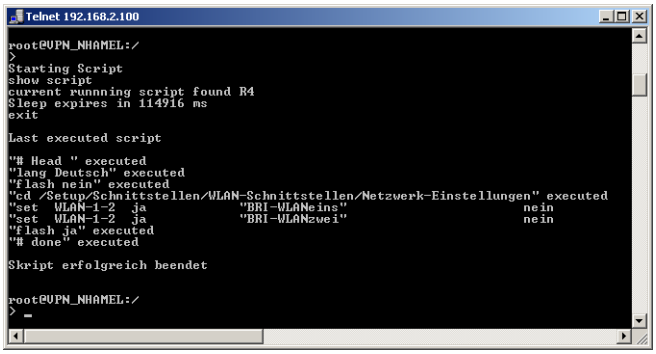
Mit dem Befehl `beginscript` wird eine Konsolensitzung in den Script-Modus versetzt. In diesem Zustand werden die im Folgenden eingegebenen Befehle nicht direkt in den Konfigurations-RAM im LANCOM übertragen, sondern zunächst in den Script-Speicher des Gerätes. Erst bei Aufruf des Befehls `exit` wird die sequenzielle Übertragung der Befehle über eine Script-Session in den Konfigurations-RAM gestartet.



Um diesen Befehl auszuführen sind Supervisor-Rechte erforderlich.

■ `show script`

Der Befehl `show script` zeigt den Inhalt des zuletzt ausgeführten Scripts und eine Übersicht über die Scripte, die aktuell noch ausgeführt werden. Die bei der Ausgabe der aktuellen Scripte angezeigten Namen können zum vorzeitigen Abbrechen der Scripte verwendet werden ('`killscript`' → Seite 4-8).





Um diesen Befehl auszuführen sind Supervisor-Rechte erforderlich.

■ `killscript`

Der Befehl `killscript` löscht den noch nicht verarbeiteten Inhalt einer Scriptsession. Die Scriptsession wird über den Namen ausgewählt ('`show script`' → Seite 4-8).



Um diesen Befehl auszuführen sind Supervisor-Rechte erforderlich.

■ `flash Yes/No`

Da beim Konfigurieren eines Gerätes mittels Script jeder add-,set- oder del-Befehl dazu führen kann, dass ein – unerwünschtes – Aktualisieren der Konfiguration im Flash erfolgt, kann das Aktualisieren im Flash abgeschaltet werden. Nach Abschluss der Konfiguration wird das Aktualisieren mit `flash Yes` wieder eingeschaltet. Änderungen in der RAM-Konfiguration werden dann ins Flash geschrieben. Der Status `flash Yes/No` wird global gespeichert.



Um diesen Befehl auszuführen sind Supervisor-Rechte erforderlich.

- `sleep`

  Mit dem Befehl sleep lässt sich die Verarbeitung der Konfigurationsbefehle um eine bestimmte Zeitspanne verzögern oder auf einen bestimmten Zeitpunkt terminieren.

  Syntax: `sleep [-u] Wert[suffix]`

  Als Suffix sind `s`, `m`, oder `h` fuer 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.

Die Sleep-Funktion ist hilfreich z.B. für einen zeitversetzten Reboot beim Testen einer geänderten Konfiguration oder für ein zeitgesteuertes Update der Firmware bei einem größeren Roll-Out von mehreren Geräten.

4.2 Rollout-Assistent

In komplexen Szenarien mit vielen LANCOM-Geräten an unterschiedlichen Standorten ist am Einsatzort manchmal kein ausgebildeter Techniker verfügbar, der die Installation und Konfiguration eines LANCOM vornehmen kann. Dabei kann ein großer Teil der Konfiguration schon in der Zentrale vorgenommen werden, vor Ort muss lediglich die Anpassung einiger weniger standortspezifischer Parameter erledigt werden. Um in diesen Fällen die abschließende Anpassung möglichst komfortabel und ohne Detailkenntnisse vornehmen zu können, kann ein spezieller Rollout-Assistent genau für die erforderlichen Schritte eingerichtet werden, der von den Mitarbeitern vor Ort einfach über einen Browser ausgeführt werden kann. Nach dem Ausführen des Rollout-Assistenten ist das Gerät dann entweder betriebsbereit oder kann weitere Teile der Konfiguration selbständig von einem zentralen Datenspeicher beziehen.

Sie finden die Parameter zur Konfiguration auf folgenden Pfaden:

WEBconfig: **Experten-Konfiguration ▶ Setup ▶ HTTP ▶ Rollout-Wizard**

4.2.1 Allgemeine Einstellungen für den Rollout-Assistenten

- **In-Betrieb**

  Schaltet den Rollout-Assistenten ein oder aus. Nach dem Einschalten wird der Assistent auf der Startseite von WEBconfig angeboten.

- **Titel**

  Name für den Rollout-Assistenten, wie er auf der Startseite von WEBconfig angezeigt wird.

4.2.2 Variablen

Maximal zehn Definitionen von Variablen mit Index, Ident, Titel, Typ, Min-Wert, Max-Wert und Vorgabewert.

- **Index**

  Index für die Variable. Die Variablen werden in der Anzeige des Rollout-Assistenten in aufsteigender Reihenfolge angezeigt.

- **Ident**

  Eindeutiger Identifier zur Kennzeichnung von Variablen, die bei der Ausführung von Aktionen referenziert werden. Die Angabe eines Identifiers ist nicht erforderlich bei Feldern, in die keine Daten vom Anwender eingetragen werden (z.B. Label).

- **Titel**

  Name der Variablen, wie er im Rollout-Assistenten von WEBconfig angezeigt wird.

■ **Typ**

Name der Variablen, wie er im Rollout-Assistenten von WEBconfig angezeigt wird.

- □ Mögliche Werte: Label, Integer, String, Passwort, Haken
- □ Label: Text zur Anzeige von weiteren Erklärungen der anderen Variablen. Min-Wert und Max-Wert haben für diese Einträge keine weitere Bedeutung.
- □ Integer: Erlaubt die Eingabe einer positiven Integer-Zahl von 0 bis 2^{32} - 1. Mit der Angabe von Min-Wert und Max-Wert kann der Eingabebereich eingeschränkt werden, außerdem kann ein Vorgabewert (Default) definiert werden. Dabei muss der Vorgabewert als Zahl innerhalb der Min- und Max-Werte eingetragen werden.
- □ String: Erlaubt die Eingabe eines Textes. Mit der Angabe von Min-Wert und Max-Wert kann die Länge des Textes eingeschränkt werden, außerdem kann ein Vorgabewert (Default) definiert werden. Dabei muss der Vorgabe-Text innerhalb der maximalen Länge liegen, längere Texte werden abgeschnitten.
- □ Passwort: Erlaubt die Eingabe eines Passwortes, welches bei der Eingabe nicht angezeigt wird. Die Eingabe des Passwortes muss wierderholt werden. Der Rollout-Asstsistent führt keine Aktionen aus, wenn die Eingabe der Passwörter nicht übereinstimmt.
- □ Haken: Einfache Option, die ein- oder ausgeschaltet sein kann. Min-Wert und Max-Wert haben für diese Einträge keine weitere Bedeutung. Haken sind standardmäßig eingeschaltet, wenn der Vorgabewert nicht leer ist.
- □ Default: Label

■ **Min-Wert**

Minimalwert der aktuellen Variablen (bei Typ Integer) bzw. minimale Anzahl der möglichen Zeichen (bei Typ String oder Passwort).

■ **Max-Wert**

Maximalwert der aktuellen Variablen (bei Typ Integer) bzw. maximale Anzahl der möglichen Zeichen (bei Typ String oder Passwort).

■ **Vorgabewert**

Vorgabewert der aktuellen Variablen.

4.2.3 Vom Rollout-Assistenten auszuführende Aktionen

Maximal 19 Definitionen von Aktionen mit Index und Aktion, die vom Rollout-Assistenten nach der Eingabe der Benutzerdaten ausgeführt werden sollen.

■ **Index**

Index für die Aktion. Die Aktionen werden bei der Ausführung des Rollout-Assistenten in aufsteigender Reihenfolge abgearbeitet.

■ **Aktion**

Aktion, die vom Rollout-Assistenten nach der Eingabe der Benutzerdaten ausgeführt werden soll.

- □ Mögliche Werte: Aktionen werden wie Cron-Befehle in der Syntax `[Protokoll:]Argument` eingetragen. Wenn kein Protokoll angegeben ist, wird 'exec:' verwendet.
- □ exec: Führt einen beliebigen Befehl aus, wie er auf der Telnet-Ebene zur Konfiguration eines LANCOM verwendet wird. Das folgende Beispiel setzt den Namen des Gerätes auf 'MyLANCOM':

  ```
  exec: set /setup/name MyLANCOM
  ```

- □ mailto: Erlaubt das Versenden einer E-Mail mit Angabe von Adressat, Betreff und Body, z. B.:

  ```
  mailto:admin@mylancom.de?subject=Rollout?body=LANCOM fertig eingerichtet
  ```



Zur Nutzung der Mail-Funktion muss in dem Gerät ein SMTP-Konto eingerichtet sein.

- □ http und https: Erlaubt das Aufrufen einer Webseite, z. B. um dort eine Aktion auszuführen:

  ```
  <http:|https:>//[user[:pass]@]hostname[:port]/...
  ```

- □ Variablen in den Aktionen: Bei der Ausführung von Aktionen können die mit dem Rollout-Assistenten definierten Variablen referenziert werden. Dazu wird der Identifier der Variable geführt von einem Prozentzeichen in die Aktion eingesetzt. Der Identifier muss dabei in geschweifte Klammern gesetzt werden, wenn weitere alphanumerische Zeichen in der Aktion enthalten sind. Das folgende Beispiel setzt den Namen des

Gerätes auf das Format 'Standort (Filiale)', wenn als Variable mit dem Identifier 'Location' der Standort des Gerätes abgefragt wird:

```
exec: set /setup/name %{Location}(Filiale)
```

Bei Variablen vom Typ Integer oder String wird der jeweilige Wert aufgrund der Benutzereingabe verwendet. Bei Variablen vom Typ Haken wird '1' (eingeschaltet) bzw. '0' (ausgeschaltet) verwendet.



Wenn der Ausdruck der Aktion Leerzeichen enthält, muss der Ausdruck in Anführungszeichen eingefasst werden.

4.2.4 Aktionen zur Verwaltung des Rollout-Assistenten

- **Variablen-Renumerieren**
- **Aktionen-Renumerieren**

  Wie schon angeführt, werden Variablen und Aktionen in der Reihenfolge Ihres Index angezeigt bzw. abgearbeitet. Manchmal muss zwischen zwei Variablen/Aktionen mit benachbartem Index ein neuer Eintrag eingeführt werden. Mit dieser Aktion können die Indizes automatisch mit einem bestimmten Abstand zwischen den Einträgen neu vergeben werden.

  Bei der Ausführung können als Argumente der Startwert und das Inkrement angegeben werden. Die Aktion nummeriert die Einträge neu, beginnend mit dem Startwert mit dem als Inkrement gewählten Abstand. Werden Startwert und Inkrement nicht angegeben, so wird für beides automatisch der Wert 10 verwendet. Ohne Argumente verwendet die Aktion daher die Indizes 10, 20, 30, 40 usw.

4.3 LANCOM Layer 2 Management Protokoll (LL2M)

Neu mit LCOS 7.6:

- LANCOM Layer 2 Management Protokoll (LL2M)

4.3.1 Einleitung

Alle Wege zur Konfiguration eines LANCOM setzen eine IP-Verbindung zwischen dem Konfigurationsrechner und dem LANCOM 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 (nicht bei allen Geräten verfügbar) 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 Atacken 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 Kommandozeile 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.

4.3.2 Konfiguration des LL2M-Servers

WEBconfig: LCOS-Menübaum/Setup/Config/LL2M

- **In-Betrieb**

  Schaltet den LL2M-Server ein oder aus. Ein aktivierter LL2M-Server kann nach dem Booten/Einschalten des Gerätes für die Dauer des Zeit-Limits von einem LL2M-Client angesprochen werden.

  Mögliche Werte:

  □ Ja, nein

  Default:

  □ Ja

■ **Zeit-Limit**

Definiert die Zeitspanne in Sekunden, in der ein aktivierter LL2M-Server nach dem Booten/Einschalten des Gerätes von einem LL2M-Client angesprochen werden kann. Nach Ablauf des Zeit-Limits wird der LL2M-Server automatisch deaktiviert.

Mögliche Werte:

□ 0 bis 4294967295

Default:

□ 0

Besondere Werte:

□ 0 deaktiviert das Zeit-Limit, in diesem Zustand bleibt der LL2MServer dauerhaft aktiv.

4.3.3 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 Telnet-Sitzung auf einem LANCOM, 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 Befehl LL2Mdetect kann mit den folgenden Parametern eingeschränkt werden.

□ -a <MAC-Adresse>: Schränkt den Befehl nur auf die Geräte mit der angegebenen MAC-Adresse ein. Die MAC-Adresse wird in der Form “00a057010203”, “00-a0-57-01-02-03” oder “00:a0:57:01:02:03” angegeben.



Wird keine MAC-Einschränkung gesetzt, geht der detect als Multicast (oder optional 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 LANCOM-MAC-Adressen.

□ -t <Geräte-Typ>: Schränkt den Befehl nur auf die Geräte des entsprechenden Hardware-Typs ein.

□ -r <Hardware-Release>: Schränkt den Befehl nur auf die Geräte des entsprechenden Hardware-Releases ein.

□ -f <Version>: Schränkt den Befehl nur auf die Geräte der entsprechenden Firmware-Version ein.

□ -s <Seriennummer>: Schränkt den Befehl nur auf die Geräte der entsprechenden Seriennummer ein.

□ -b : Versendet die LL2Mdetect-Anfrage als Broadcast und nicht als Multicast.

□ -v <VLAN-ID>: Versendet die LL2Mdetect-Anfrage nur auf dem angegebenen VLAN. Wenn keine VLAN-ID angegeben ist, wird die VLAN-ID der ersten definierten IP-Netzwerks verwendet.

Beispiel:

□ ll2mdetect -r A: Dieser Befehl versendet eine SYSINFO-Anfrage an alle Geräte mit der Hardware-Release “A”.

Die Antwort des LL2MServers enthält 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 können durch Semikolon getrennt in einem LL2M-Befehl kombiniert werden. Je nach Kommando werden Aktionen auf dem entfernten Gerät ausgeführt und die Rückmeldungen des entfernten Gerätes werden zur Anzeige an den LL2M-Client übertragen. Der Befehl LL2Mexec entspricht folgender Syntax:

□ ll2mexec <User>[:<Password>]@<MAC-Adresse>

Der Befehl LL2Mexec kann mit dem folgenden Parameter eingeschränkt werden.

- -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.

Beispiel:

- ll2mexec root@00a057010203 set name MyLANCOM: Dieser Befehl meldet den LL2M-Client als "root" auf dem LL2M-Server mit der MAC-Adresse "00a057010203" an. Das Kennwort wird in der Konsolensitzung interaktiv abgefragt. Dann setzt der LL2M-Client den Namen des entfernten Gerätes auf den Wert "MyLANCOM".

4.4 Benachrichtigungen

Für die Benachrichtigung über bestimmte Vorgänge im LANCOM stehen folgende Variablen in der Aktionstabelle zur Verfügung:

- **%a**
  WAN-IP-Adresse der WAN-Verbindung, in deren Kontext diese Aktion ausgeführt wird.
- **%H**
  Hostname der WAN-Verbindung, in deren Kontext diese Aktion ausgeführt wird.
- **%h**
  wie %h, nur Hostname in Kleinbuchstaben
- **%c**
  Verbindungsname der WAN-Verbindung, in deren Kontext diese Aktion ausgeführt wird.
- **%n**
  Gerätename
- **%s**
  Seriennummer des Geräts
- **%m**
  MAC-Adresse des Geräts (wie im Sysinfo)
- **%t**
  Uhrzeit und Datum, im Format YYYY-MM-DD hh:mm:ss

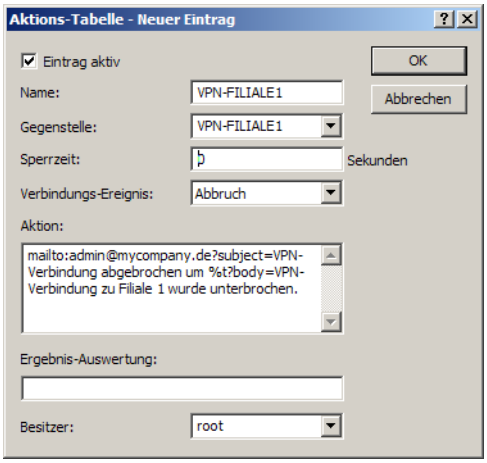
Beispiel: Information über Verbindungsabbruch als SMS auf Mobiltelefon melden

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 LANCOM 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 ein 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.

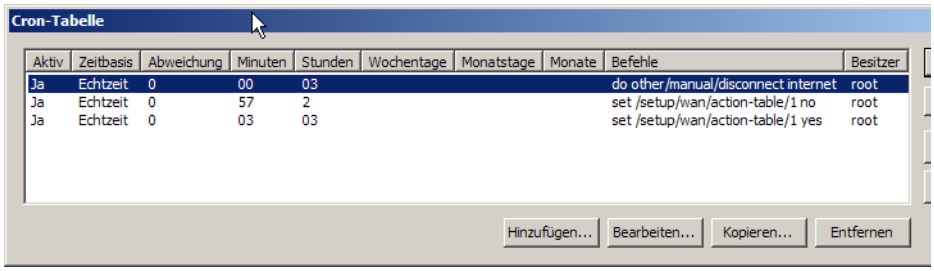
In einem komplexen Aufbau mit mehreren Filialen wird im LANCOM der Zentrale für jede Gegenstelle ein passender Eintrag angelegt. Zur Überwachung der Zentrale selbst wird eine Aktion in einem Gerät in einer der Filialen angelegt. So kann der Administrator auch dann benachrichtigt werden, wenn das VPN-Gateway der Zentrale selbst ausfällt und vielleicht keine Nachricht mehr versenden kann.

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.



4.5 Rechteverwaltung für verschiedene Administratoren

Neu in LCOS 7.60:

- Administratoren ohne Trace-Rechte

In der Konfiguration des LANCOM können mehrere Administratoren angelegt werden, die über unterschiedliche Zugriffsrechte verfügen. Für ein LANCOM können bis zu 16 verschiedene Administratoren eingerichtet werden.

Neben den in der Konfiguration angelegten Administratoren gibt es auch noch den „root"-Administrator mit dem Haupt-Geräte-Passwort. Dieser Administrator hat immer die vollen Rechte und kann auch nicht

gelöscht oder umbenannt werden. Um sich als root-Administrator anzumelden, geben Sie im Login-Fenster den Benutzernamen „root" ein oder Sie lassen dieses Feld frei.

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 der Eingabe des korrekten Benutzernamens und Passworts erscheint das Hauptmenü der WEBconfig. In diesem Menü sind nur die Punkte vorhanden, für die der Administrator Zugriffs- bzw. Funktionsberechtigungen hat.

Ist mindestens ein weiterer Administrator in der Admin-Tabelle eingerichtet, so enthält das Hauptmenü zusätzlich eine Schaltfläche **Administrator wechseln**, die es erlaubt zu einer anderen Benutzerkennung (mit ggf. anderen Rechten) zu wechseln.

4.5.1 Die Rechte für die Administratoren

Bei den Rechten für die Administratoren werden zwei Bereiche unterschieden:

- Jeder Administrator gehört zu einer bestimmten Gruppe, der global definierte Rechte zugewiesen sind.
- Jeder Administrator verfügt außerdem über „Funktionsrechte", die den persönlichen Zugriff auf bestimmte Funktionen wie z.B. die Setup-Assistenten regeln.

Administratorengruppen

Bezeichnung unter Telnet/Terminal	Bezeichnung unter LANconfig	Rechte
Supervisor	Alle	Supervisor - Mitglied in allen Gruppen
Admin-RW	Eingeschränkt	lokaler Administrator mit Lese- und Schreibzugriff
Admin-RW-Limit	Eingeschränkt ohne Trace-Rechte	lokaler Administrator mit Lese- und Schreibzugriff ohne Trace-Rechte
Admin-RO	Nur lesen	lokaler Administrator mit Lesezugriff aber ohne Schreibzugriff
Admin-RO-Limit	Nur lesen ohne Trace-Rechte	lokaler Administrator mit Lesezugriff aber ohne Schreibzugriff und ohne Trace-Rechte
kein	keine	kein Zugriff auf die Konfiguration

- Supervisor: Hat vollen Zugriff auf die Konfiguration
- lokaler Administrator mit Lese- und Schreibrechten: Ebenfalls voller Zugriff auf die Konfiguration, dabei sind jedoch die folgenden Möglichkeiten gesperrt:
  - □ Firmware in das Gerät hochladen
  - □ Konfiguration in das Gerät einspielen
  - □ Konfiguration über LANconfig



Lokale Administratoren mit Schreibrechten können auch die Admintabelle bearbeiten. Dabei kann ein lokaler Administrator jedoch nur solche Einträge bearbeiten oder anlegen, die die gleichen oder weniger Rechte haben wie er selbst. Ein lokaler Administrator kann also keinen Supervisor anlegen und sich selbst auch nicht diese Rechte einräumen.

- lokaler Administrator mit Lese- und Schreibrechten ohne Trace-Rechte: Ebenfalls voller Zugriff auf die Konfiguration, dabei sind jedoch die folgenden Möglichkeiten gesperrt:
  - □ Firmware in das Gerät hochladen
  - □ Konfiguration in das Gerät einspielen
  - □ Konfiguration über LANconfig
  - □ Trace-Ausgaben über Telnet oder LANmonitor



Lokale Administratoren mit Schreibrechten, aber ohne Trace-Rechte können keine Admistratoren mit Trace-Rechten anlegen.

- lokaler Administrator mit Leserechten: Kann die Konfiguration über Telnet oder Terminalprogramm lesen, aber keine Werte verändern. Diesen Administratoren können über die Funktionsrechte bestimmte Möglichkeiten zur Konfiguration eingeräumt werden.
- keine: Kann die Konfiguration nicht lesen. Diesen Administratoren können über die Funktionsrechte bestimmte Möglichkeiten zur Konfiguration eingeräumt werden.

Funktionsrechte

Mit den Funktionsrechten werden dem Benutzer die folgenden Möglichkeiten eingeräumt:

- Grundkonfigurations-Assistent
- Sicherheits-Assistent
- Internet-Assistent
- Assistent zur Auswahl von Internet-Providern
- RAS-Assistent
- LAN-LAN-Kopplungs-Assistent
- Uhrzeit und Datum verändern
- Nach weiteren Geräten suchen
- WLAN-Linktest
- a/b-Assistent

4.5.2 Administratorenzugänge über TFTP und SNMP

Die zusätzlichen Administratorenzugänge werden in der Regel für die Konfiguration der Geräte über Telnet, Terminalprogramme oder SSH-Zugänge genutzt. Allerdings können die zusätzlichen Administratoren auch über TFTP oder SNMP auf die Geräte zugreifen.

Zugang über LANconfig

Ein Benutzer mit Supervisorrechten kann sich bei LANconfig anmelden, wenn er im Loginfenster im Feld für das Passwort seine Benutzerdaten in der Kombination <Username>:<Passwort> eingibt.

Zugang über TFTP

Im TFTP wird der Username und das Passwort im Quell- (TFTP-Read-Request) oder Ziel-Filenamen (TFTP-Write-Request) kodiert. Der Filename baut sich entweder aus dem Master-Passwort und dem auszuführenden Kommando oder aus der Kombination von Username und Passwort, die durch einen Doppelpunkt getrennt sind, und nachgestelltem Kommando zusammen. Ein über TFTP abgesetztes Kommando sieht daher wie folgt aus:

- <Master-Passwort><Kommando> bzw.
- <Username>:<Passwort>@<Kommando>

Beispiele (das LANCOM hat die Adresse mylancom.intern, das Master-Passwort lautet 'RootPwd' und es ist der User 'LocalAdmin' mit dem Passwort 'Admin' eingerichtet):

- Konfiguration aus dem Gerät auslesen (nur für den Supervisor)

  ```
  tftp mylancom.intern GET RootPwdreadconfig mylancom.lcf
  ```

- Konfiguration in das Gerät schreiben (nur für den Supervisor)

  ```
  tftp mylancom.intern PUT mylancom.lcf RootPwdwriteconfig
  ```

- Geräte-MIB aus dem Gerät auslesen (für lokalen Administrator)

  ```
  tftp mylancom.intern GET localadmin:Admin@readmib mylancom.mib
  ```

Für die Menüs und ausführbaren Befehle gelten die gleichen Rechte-Beschränkungen wie unter Telnet.

Zugang über SNMP-Management-Systeme

Auch bei der Verwaltung von Netzwerken mit Hilfe von SNMP-Tools wie HP OpenView können über die verschiedenen Administratoren-Zugänge die Rechte gezielt gesteuert werden.

Unter SNMP werden Username und Passwort in der „Community" kodiert. Dort kann entweder die Community 'public' ausgewählt werden oder entweder das Master-Passwort oder eine Kombination von Username und Passwort, die durch einen Doppelpunkt getrennt sind, angegeben werden.

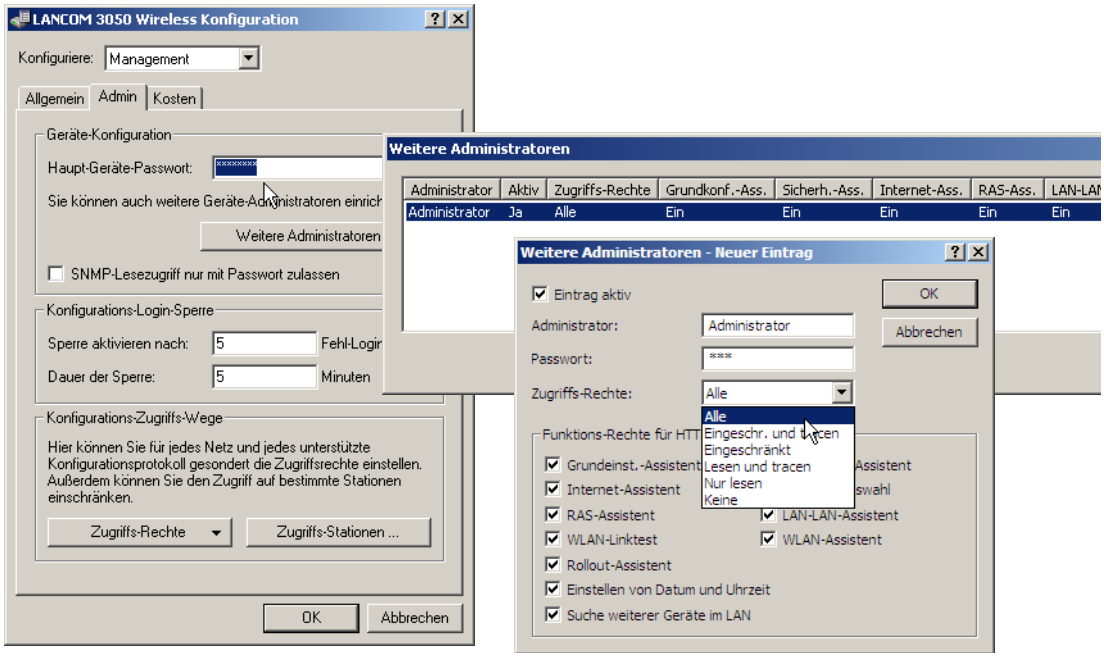
Die Community 'public' entspricht von den Rechten her einem lokalen Administrator mit Read-Only-Rechten, solange der SNMP-Lesezugriff ohne Passwort erlaubt wird. Wird dieser Zugriff verboten, so darf die Community 'public' auf keinen Menüpunkt zugreifen.

Ansonsten gelten für die Menüs die gleichen Rechte-Beschränkungen wie unter Telnet.

4.5.3 Konfiguration der Benutzerrechte

LANconfig

Bei der Konfiguration mit LANconfig finden Sie die Liste der Administratoren im Konfigurationsbereich 'Management' auf der Registerkarte 'Admin' unter der Schaltfläche **Weitere Administratoren**.



WEBconfig: LCOS-Menübaum ▶ Setup ▶ Config-Modul ▶ Admin.-Tabelle

Geben Sie hier folgende Werte ein:

- Name für den neuen Administrator mit Passwort.
- Zugriffsrechte
- Funktionsrechte

Sie können die Einträge über den Schalter 'Eintrag aktiv' vorübergehend deaktivieren, ohne sie ganz zu löschen.

Zur Darstellung der Benutzergruppen stehen die folgenden Werte zur Verfügung:

Bezeichnung	Rechte
Supervisor	Supervisor - Mitglied in allen Gruppen
Admin-RW	lokaler Administrator mit Lese- und Schreibzugriff
Admin-RW-Limit	lokaler Administrator mit Lese- und Schreibzugriff, ohne Trace-Rechte
Admin-RO	lokaler Administrator mit Lesezugriff aber ohne Schreibzugriff
Admin-RO-Limit	lokaler Administrator mit Lesezugriff aber ohne Schreibzugriff, ohne Trace-Rechte
kein	kein Zugriff auf die Konfiguration

Zur Darstellung der Funktionsrechte stehen die folgenden Hexadezimalwerte zur Verfügung:

Wert	Rechte
0x00000001	Der Benutzer darf den Grundkonfigurations-Assistenten ausführen
0x00000002	Der Benutzer darf den Sicherheits-Assistenten ausführen
0x00000004	Der Benutzer darf den Internet-Assistenten ausführen
0x00000008	Der Benutzer darf den Assistenten zur Auswahl von Internet-Providern ausführen
0x00000010	Der Benutzer darf den RAS-Assistenten ausführen
0x00000020	Der Benutzer darf den LAN-LAN-Kopplungs-Assistenten ausführen
0x00000040	Der Benutzer darf die Uhrzeit und das Datum stellen (gilt auch für Telnet und TFTP)
0x00000080	Der Benutzer darf nach weiteren Geräten suchen
0x00000100	Der Benutzer darf den WLAN-Linktest ausführen (gilt auch für Telnet)
0x00000200	Der Benutzer darf den a/b-Assistenten ausführen
0x00000400	Der Benutzer darf den WTP-Zuordnungs-Assistenten ausführen
0x00000800	Der Benutzer darf den Public-Spot-Assistenten ausführen

Wert	Rechte
0x00001000	Der Benutzer darf den WLAN-Assistenten ausführen
0x00002000	Der Benutzer darf den Rollout-Assistenten ausführen
0x00004000	Der Benutzer darf den Dynamic-DNS-Assistenten ausführen
0x00008000	Der Benutzer darf den VoIP-CallManager-Assistenten ausführen
0x00010000	Der Benutzer darf den WLC-Profil-Assistenten ausführen

Der Eintrag ergibt sich aus der jeweiligen Summe in den ersten, zweiten und dritten Spalten von rechts. Soll der Benutzer z.B. die Funktionen „Sicherheits-Assistent", „Auswahl der Internet-Provider", „RAS-Assistent", „Uhrzeit ändern" und „WLAN-Linktest" ausführen können, ergeben sich folgende Werte:

- erste Spalte von rechts: 2 (Sicherheits-Assistent) + 8 (Auswahl der Internet-Provider) = „a" (Hexadezimal)
- zweite Spalte von rechts: 1 (RAS-Assistent) + 4 (Uhrzeit ändern) = „5" (Hexadezimal)
- dritte Spalte von rechts: 1 (WLAN-Linktest) = „1" (Hexadezimal)

Für dieses Beispiel tragen Sie in die Funktionsrechte also den Wert „0000015a" ein.

Anders ausgedrückt handelt es sich hierbei um eine ODER-Verknüpfung der Hexadezimal-Werte:

Bezeichnung	Wert
Sicherheits-Assistent	0x00000002
Auswahl des Providers	0x00000008
RAS-Assistent	0x00000010
Uhrzeit ändern	0x00000040
WLAN-Linktest	0x00000100
ODER-verknüpft	0x0000015a

Beispiele:

Mit dem folgenden Befehl legen Sie einen neuen Benutzer in der Tabelle an, der als lokaler Administrator „Mueller" mit dem Passwort „BW46zG29" den Internetprovider auswählen darf. Der Benutzer wird dabei sofort aktiviert:

```
set Mueller BW46zG29 ja Admin-RW 00000008
```

Mit dem folgenden Befehl erweitern Sie die Funktionsrechte dahingehend, das Benutzer „Mueller" auch den WLAN-Link-Test ausführen kann (die Sternchen stehen für die nicht zu verändernden Werte):

```
set Mueller * * * 00000108
```

4.5.4 Einschränkungen der Konfigurationsbefehle

Die Verfügbarkeit der Befehle bei der Konfiguration der Geräte über Telnet oder Terminalprogramm hängt von den Rechten der Benutzer ab:

Befehl	Supervisor	lokaler Administrator	Bemerkung
activateimage	✔		
cfgreset	✔		
linktest	✔		Der Befehl 'linktest' kann auch ausgeführt werden, wenn der Benutzer das Funktionsrecht besitzt, einen WLAN-Linktest durchzuführen
readconfig	✔		
writeconfig	✔		
writeflash	✔		
setenv	✔	✔	
testmail	✔	✔	
time	✔	✔	Der Befehl 'time' kann auch ausgeführt werden, wenn der Benutzer das Funktionsrecht besitzt, die Systemzeit einzustellen

Befehl	Supervisor	lokaler Administrator	Bemerkung
unsetenv	✔	✔	
delete/rm	✔	✔	
readmib	✔	✔	
WLA	✔	✔	
set	✔	✔	

Alle weiteren Befehle (wie 'cd', 'ls', 'trace', etc...) dürfen von allen Benutzern verwendet werden. Um Befehle ausführen zu können, die eine Konfigurationsänderung bewirken (z.B. 'do' oder 'time'), muss der jeweilige Benutzer mindestens Schreibrechte besitzen.

Die oben aufgeführten Befehle sind nicht in allen LCOS-Versionen und nicht für alle LANCOM-Modelle verfügbar.

4.5.5 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 LAN einzuräumen. Sollten z.B. bei der Konfiguration von Netzwerkgeräten wie einem LANCOM VP-100 Fragen auftauchen, kann der jeweilige Support besser weiterhelfen, wenn er direkt auf das Gerät im LAN des Kunden zugreifen kann. Die Standardmethode für den Zugriff auf Geräte im LAN über inverses Masquerading (Port-Forwarding) erfordert jedoch in manchen Fällen eine entsprechende Konfiguration der Firewall – außerdem werden die einmal geöffneten Zugänge oft nicht wieder gelöscht und stellen damit ein Sicherheitsrisiko dar.

Als Alternative zu den dauerhaften Zugängen über festes Port-Forwarding können vorübergehende Fernwartungszugänge eingerichtet werden, die nach einer bestimmten inaktiven Zeit automatisch wieder geschlossen werden. Dazu erzeugt z.B. der Support-Mitarbeiter, der auf ein Gerät im Netzwerk des Kunden zugreifen soll, einen „TCP/HTTP-Tunnel“, über den er über TCP Port 80 Zugang zu dem entsprechenden Gerät erhält.

Dieser Zugang ist nur gültig für die IP-Adresse, von welcher der Tunnel erzeugt wurde. Der Zugriff auf das freizugebende Gerät im Netzwerk ist also nicht übertragbar!

TCP/HTTP-Tunnel konfigurieren

Zur Konfiguration der TCP/HTTP-Tunnel im LANCOM stehen folgende Parameter bereit:

WEBconfig: LCOS-Menübaum ▶ Setup ▶ HTTP

- **Max.-Tunnel-Verbindungen**

  Maximale Anzahl der gleichzeitig aktiven TCP/HTTP-Tunnel.

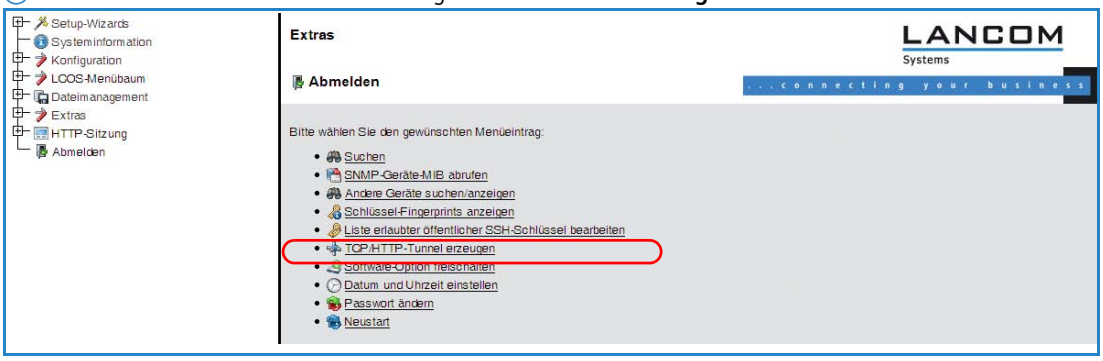
- **Tunnel-Idle-Timeout**

  Lebensdauer eines Tunnels ohne Aktivität. Nach Ablauf dieser Zeit wird der Tunnel automatisch geschlossen, wenn darüber keine Daten übertragen werden.

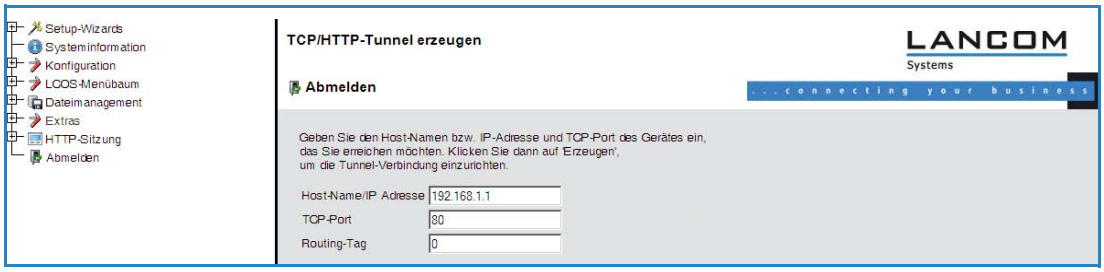
TCP/HTTP-Tunnel erzeugen

① Die HTTP-Tunnel werden auf der Startseite von WEBconfig eingerichtet. Melden Sie sich in WEBconfig auf dem LANCOM Router an, hinter dem das freizugebende Gerät erreicht werden kann. Holen Sie dazu ggf. beim zuständigen Administrator die benötigten Login-Daten ein.

② Wählen Sie im Bereich 'Extras' den Eintrag **TCP/HTTP-Tunnel erzeugen**.



③ Geben Sie den Namen bzw. die IP-Adresse des Gerätes ein, das Sie vorübergehend für den Zugriff über HTTP freischalten möchten.



④ Wählen Sie dazu einen Port aus, der für den HTTP-Tunnel verwendet werden soll und geben sie ggf. das Routing-Tag des IP-Netzwerks an, in dem sich das freizugebende Gerät befindet und bestätigen Sie die Angaben mit **Erzeugen**.

⑤ Der folgende Dialog zeigt eine Bestätigung über den neu erstellten Tunnel und bietet einen Link auf das freizugebende Gerät.



Anstelle von HTTP- oder HTTPS-Fernwartungszugängen sind Fernwartungstunnel mit beliebigen andere TCP-Diensten möglich, beispielsweise TELNET-Verbindungen (TCP-Port 23) oder SSH (TCP-Port 22).

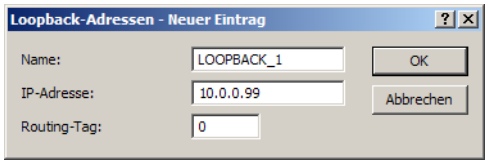
Tunnel vorzeitig löschen

Der neu erstellte HTTP-Tunnel wird automatisch nach Ablauf der Tunnel-Idle-Timeout-Zeit ohne Aktivität gelöscht. Um den Tunnel vorzeitig zu löschen, können Sie über **LCOS-Menübaum** ▶ **Status** ▶ **TCP-IP** ▶ **HTTP** die Liste der aktiven Tunnel aufrufen und die nicht mehr benötigten Tunnel gezielt löschen.

Aktive TCP-Verbindungen in diesem Tunnel werden mit dem Löschen des Tunnels **nicht** beendet, es können aber keine neuen Verbindungen mehr aufgebaut werden.

4.6 Benamte Loopback-Adressen

In einem LANCOM Router können bis zu 16 Loopback-Adressen definiert werden, unter denen das Gerät z.B. beim Management größerer Netz-Strukturen angesprochen werden kann. Um die Loopback-Adressen für bestimmte Netzwerke (z.B. im Zusammenhang mit Advanced Routing and Forwarding) zu nutzen, können den Adressen Routing-Tags zugordnet werden. Zur leichteren Identifizierung in anderen Konfigurationsteilen erhalten die Loopback-adressen außerdem einen frei wählbaren Namen:



LANconfig: TCP/IP ▶ Allgemein ▶ Loopback-Adressen

WEBconfig: LCOS-Menübaum ▶ Setup ▶ TCP-IP ▶ Loopback-Liste

- **Name**

  Frei wählbarer Name für die Loopback-Adresse.

- **Loopback-Adresse**

  Loopback-Adresse für das Gerät.

- **Routing-Tag**

  Routing-Tag der Loopback-Adresse. Loopback-Adressen mit dem Routing-Tag '0' (ungetaggt) sind in allen Netzwerken sichtbar. Loopback-Adressen mit einem anderen Routing-Tag sind nur in Netzwerken mit dem gleichen Routing-Tag sichtbar.

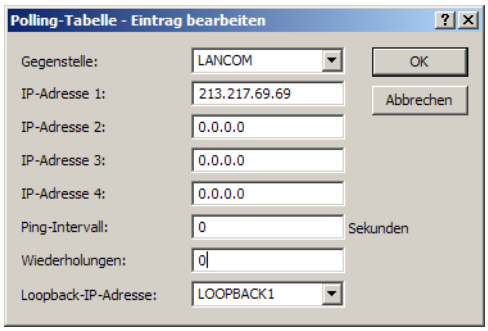
4.6.1 Loopback-Adressen beim ICMP Polling

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-Interval 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.



LANconfig: Kommunikation ▶ Gegenstellen ▶ Polling-Tabelle

WEBconfig: LCOS-Menübaum ▶ 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**

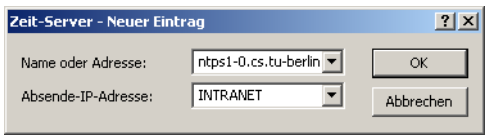
  Bleibt die Antwort auf einen Ping aus, wird die Gegenstelle in kürzeren Intervallen geprüft. Im Sekundentakt versucht das Gerät dann erneut, die Gegenstelle zu erreichen. Die Anzahl der Wiederholungen gibt an, wie oft dieser Versuch wiederholt wird. Wird hier eine „0" eingetragen, gilt der Standardwert von 5 Wiederholungen.

- **Loopback-Adresse**

  Absenderadresse, die in den Ping eingetragen wird und auf der auch die Ping-Antwort erwartet wird. Als Loopback-Adresse können eingetragen werden.

4.6.2 Loopback-Adressen für Zeit-Server

LANCOM Router können Zeitinformationen u.a. von öffentlich zugänglichen Zeit-Server im Internet (NTP-Server) beziehen. Die so ermittelte Zeit kann das LANCOM allen Stationen im lokalen Netz zur Verfügung stellen. Bei der Definition der Zeit-Server können neben den Namen oder IP-Adressen der NTP-Server, von denen der LANCOM Router die Uhrzeit abfragt, auch Loopback-Adressen angegeben werden.



LANconfig: Datum/Zeit ▶ Synchronisierung ▶ Zeit-Server

WEBconfig: LCOS-Menübaum ▶ Setup ▶ NTP ▶ RQ-Adresse

- **Name oder Adresse**

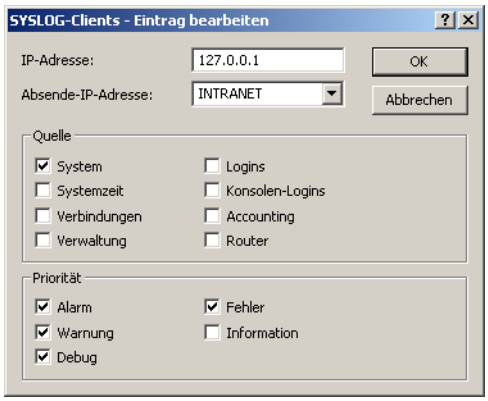
  Name oder IP-Adresse des NTP-Servers. Der LANCOM Router versucht die Server in der Reihenfolge der Einträge zu erreichen.

- **Loopback-Adresse**

  Absenderadresse, in der die NTP-Anfrage eingetragen wird und auf der auch die NTP-Antwort erwartet wird. Als Loopback-Adresse können eingetragen werden.

4.6.3 Loopback-Adressen für SYSLOG-Clients

Mit dem SYSLOG-Modul besteht die Möglichkeit, Zugriffe auf den LANCOM Router protokollieren zu lassen. Um die SYSLOG-Nachrichten empfangen zu können, werden die entsprechenden SYSLOG-Clients eingerichtet.



LANconfig: Meldungen ▶ SYSLOG ▶ SYSLOG-Clients

WEBconfig: LCOS-Menübaum ▶ Setup ▶ SYSLOG ▶ Tabelle-SYSLOG

- **IP-Adresse**

  IP-Adresse des SYSLOG-Clients.

- **Loopback-Adresse**

  Absenderadresse, die in den die SYSLOG-Meldung eingetragen wird. Auf SYSLOG-Meldungen werden keine Antworten erwartet. Als Loopback-Adresse können eingetragen werden.

- **Quelle**
  - □ System: Systemmeldungen (Bootvorgänge, Timersystem etc.)
  - □ Logins: Meldungen über Login und Logout eines Users während der PPP-Verhandlung sowie dabei auftretende Fehler
  - □ Systemzeit: Meldungen über Änderungen der Systemzeit
  - □ Konsolen-Logins: Meldungen über Konsolen-Logins (Telnet, Outband, etc), Logouts und dabei auftretende Fehler
  - □ Verbindungen: Meldungen über den Verbindungsauf- und -abbau sowie dabei auftretende Fehler (Display-Trace)
  - □ Accounting: Accounting-Informationen nach dem Abbau einer Verbindung (User, Onlinezeit, Transfervolumen)
  - □ Verwaltung: Meldungen über Konfigurationsänderungen, remote ausgeführte Kommandos etc.
  - □ Router: Regelmäßige Statistiken über die am häufigsten genutzten Dienste (nach Portnummern aufgeschlüsselt) sowie Meldungen über gefilterte Pakete, Routing-Fehler etc.
- **Priorität**
  - □ Alarm: Hierunter werden alle Meldungen zusammengefasst, die der erhöhten Aufmerksamkeit des Administrators bedürfen (allgemeine SYSLOG-Priorität: 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 (allgemeine SYSLOG-Priorität: ERROR).
  - □ Warning: Dieser Level übermittelt Fehlermeldungen, die den ordnungsgemäßen Betrieb des Geräts nicht beeinträchtigen (allgemeine SYSLOG-Priorität: WARNING).
  - □ Information: Auf diesem Level werden alle Nachrichten übermittelt, die rein informellen Charakter haben (z.B. Accounting-Informationen) (allgemeine SYSLOG-Priorität: 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 (allgemeine SYSLOG-Priorität: DEBUG).

5 Diagnose

5.1 Trace-Ausgaben – Infos für Profis

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.

5.1.1 So starten Sie einen Trace

Trace-Ausgaben starten Sie in einer Telnet-Sitzung. Stellen Sie zunächst eine Telnet-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.

5.1.2 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

5.1.3 Übersicht der Parameter



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

Dieser Parameter ...	... ruft beim Trace die folgende Anzeige hervor:
Status	Status-Meldungen der Verbindungen
Fehler	Fehler-Meldungen der Verbindungen
IPX-Router	IPX-Routing
PPP	Verhandlung des PPP-Protokolls
SAP	IPX Service Advertising Protocol
IPX-Watchdog	IPX-Watchdog-Spoofing
SPX-Watchdog	SPX-Watchdog-Spoofing
LCR	Least-Cost-Router
Script	Script-Verhandlung
IPX-RIP	IPX Routing Information Protocol
Firewall	Zeigt die Aktionen der Firewall
RIP	IP Routing Information Protocol
ARP	Address Resolution Protocol
ICMP	Internet Control Message Protocol
IP-Masquerading	Vorgänge im Masquerading-Modul
DHCP	Dynamic Host Configuration Protocol
NetBIOS	NetBIOS-Verwaltung
DNS	Domain Name Service Protocol

Dieser Parameter ...	... ruft beim Trace die folgende Anzeige hervor:
Paket-Dump	Anzeige der ersten 64 Bytes eines Pakets in hexadezimaler Darstellung
D-Kanal-Dump	Trace des D-Kanals des angeschlossenen ISDN-Busses
ATM-Cell	ATM-Paketebene
ATM-Error	ATM-Fehler
ADSL	ADSL-Verbindungsstatus
SMTP-Client	E-Mail-Verarbeitung des integrierten Mail-Clients
Mail-Client	E-Mail-Verarbeitung des integrierten Mail-Clients
SNTP	Simple Network Time Protokoll
NTP	Timeserver Trace
Connact	Meldungen aus dem Aktivitätsprotokoll ('Aktivitätsprotokoll' → Seite 4-29)
Cron	Aktivitäten der Zeitautomatik (Cron-Tabelle)
RADIUS	RADIUS-Trace
Serial	Informationen über den Zustand der seriellen Schnittstelle
USB	Informationen über den Zustand der USB-Schnittstelle
Load-Balancer	Informationen zum Load Balancing
VRRP	Informationen über das Virtual Router Redundancy Protocol
Ethernet	Informationen über die Ethernet-Schnittstellen
VLAN	Informationen über virtuelle Netzwerke
IGMP	Informationen über das Internet Group Management Protocol
WLAN	Informationen über die Aktivitäten in den Funknetzwerken
IAPP	Trace zum Inter Access Point Protocol, zeigt Informationen über das WLAN-Roaming.
DFS	Trace zur Dynamic Frequency Selection, der automatischen Kanalwahl im 5-GHz-WLAN-Band
Bridge	Informationen über die WLAN-Bridge
EAP	Trace zum EAP, dem bei WPA/802.11i und 802.1x verwendeten Protokoll zur Schlüsselaushandlung
Spgtree	Informationen zum Spanning Tree Protokoll
LANAUTH	LAN-Authentifizierung (z.B. Public Spot)
SIP-Packet	SIP-Informationen, die zwischen einem LANCOM VoIP Router und einem SIP-Provider bzw. einer übergeordneten SIP-TK-Anlage ausgetauscht werden
VPN-Status	IPSec und IKE Verhandlungen
VPN-Packet	IPSec und IKE Pakete

5.1.4 Kombinationsbefehle

Dieser Kombinations-Befehl ...	... ruft beim Trace die folgende Anzeige hervor:
All	alle Trace-Ausgaben
Display	Status- und Error-Ausgaben
Protocol	PPP- und Script-Ausgaben
TCP-IP	IP-Routing-, IP-RIP-, ICMP- und ARP-Ausgaben
IPX-SPX	IPX-Routing-, RIP-, SAP-, IPX-Wd.-, SPX-Wd.-, und NetBIOS-Ausgaben
Time	zeigt vor der eigentlichen Trace-Ausgabe auch die Systemzeit an
Source	zeigt vor der eigentlichen Trace-Ausgabe auch das Protokoll an, das die Ausgabe veranlasst hat

Die angehängten Parameter werden dabei von links nach rechts abgearbeitet. Dadurch kann ein zunächst aufgerufener Parameter anschließend auch wieder eingeschränkt werden.

5.1.5 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. Beispiel für die Verwendung der Filter finden Sie unter 'Beispiele für die Traces' → Seite 5-3.

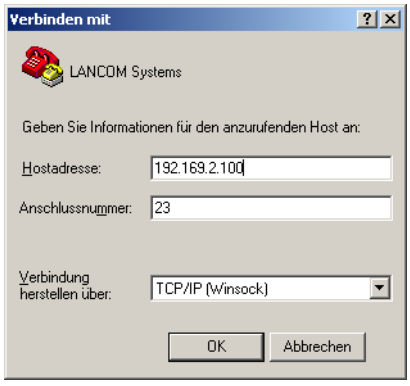
5.1.6 Beispiele für die Traces

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 + all	schaltet alle Trace-Ausgaben ein
trace - all	schaltet alle Trace-Ausgaben aus
trace + protocol display	schaltet die Ausgabe aller Verbindungsprotokolle und der Status- und Fehlermeldungen ein
trace + all - icmp	schaltet alle Trace-Ausgaben mit Ausnahme des ICMP-Protokolls ein
trace ppp	zeigt den Zustand des PPPs an
trace # ipx-rt display	schaltet die Trace-Ausgaben des IPX-Routers und der Display-Ausgaben um
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.

5.1.7 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 bitte HyperTerminal unter **Start** ▶ **Programme** ▶ **Zubehör** ▶ **Kommunikation** ▶ **Hyper Terminal**. Als Name geben Sie einen beliebigen Namen ein.



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**.

5.2 Tracen mit dem LANmonitor

Neu in LCOS 7.60:

- Speichern von Support-Dateien mit Trace-Daten, Geräte-Konfiguration, Bootlog und Sysinfo
- Automatische Sicherung der Trace-Daten
- Trace-Konfiguration mit Assistenten
- Ausgabe von Show-Kommandos
- Ausgabe von Status-Informationen und Statistiken
- SSL-verschlüsselte Telnet-Verbindung

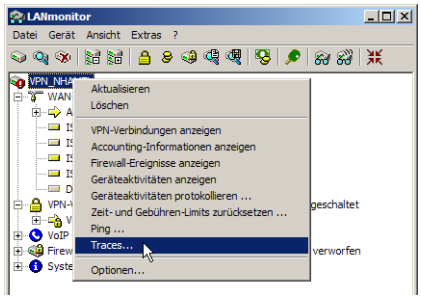
Die Abfrage von Traces kann sehr komfortabel über den LANmonitor vorgenommen werden. Klicken Sie dazu mit der rechten Maustaste auf den Geräteeintrag und wählen Sie im Kontextmenü den Eintrag **Traces**.

Zur Abfrage von Traces über den LANmonitor muss ein Telnet-Zugriff auf das Gerät erlaubt sein. Beim Starten des Trace-Dialogs versucht der LANmonitor zunächst eine SSL-verschlüsselte Telnet-Verbindung zum Gerät aufzubauen. Falls das Gerät keine SSL-Verbindungen unterstützt, wechselt der LANmonitor automatisch auf unverschlüsseltes Telnet.
Wenn der SNMP-Zugriff auf das Gerät passwortgeschützt ist, sind zudem die Zugangsdaten für einen Administrator mit Trace-Rechten erforderlich.

Einleitung

Mit der Trace-Funktion im LANmonitor können über die normalen Trace-Funktionen hinaus, wie sie von der Telnet-Oberfläche bekannt sind, weitere Funktionen genutzt werden, die eine Erstellung und Auswertung der Traces erleichtern. So kann z. B. die aktuelle Trace-Konfiguration, mit der die benötigten Trace-Befehle aktiviert werden, in einer Konfigurationsdatei gespeichert werden. Eine solche Trace-Konfiguration kann ein erfahrener Service-Techniker vorbereiten und einem weniger erfahrenen Anwender zur Verfügung stellen, der damit die gewünschte Trace-Ausgabe eines Gerätes erzeugen kann. Auch die Trace-Ergebnisse können komfortabel in einer Datei gespeichert werden und an den Techniker zur Auswertung zurückgegeben werden.

Um das Trace-Fenster für ein Gerät zu öffnen, klicken Sie im LANmonitor mit der rechten Maustaste auf den Eintrag des Gerätes und wählen im Kontext-Menü den Eintrag “Traces”.



Der LANmonitor bietet die folgenden Schaltflächen zur Bedienung des Trace-Moduls:

Öffnet eine vordefinierte Konfiguration für die Trace-Ausgabe. Damit können Sie eine Trace-Ausgabe genau so erstellen, wie Sie z. B. von einem Service-Techniker benötigt wird.

Speichert die aktuelle Trace-Konfiguration, um diese an einen Anwender weiterzugeben.

Öffnet eine Datei mit Trace-Ergebnissen zur Ansicht im Trace-Modul.

Speichert die aktuellen Trace-Ergebnisse in einer Datei.

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.



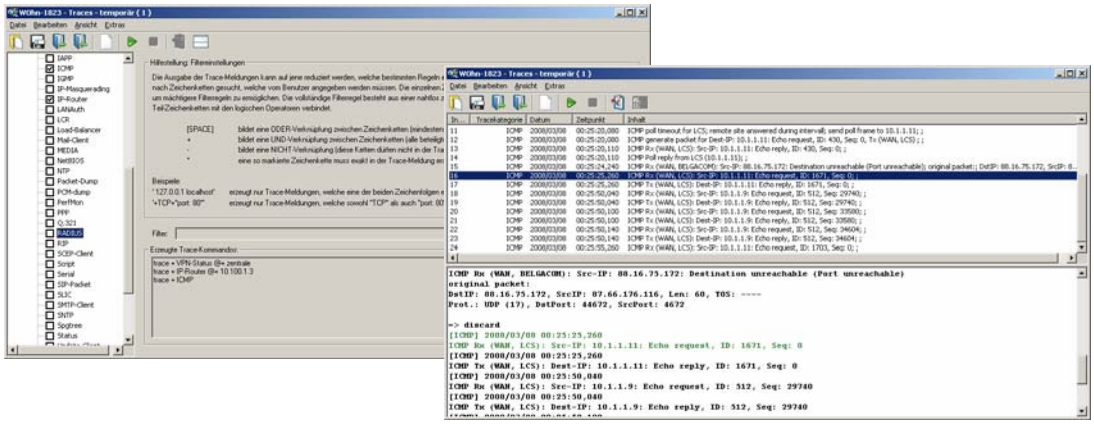
Hält die Ausgabe der Trace-Ergebnisse an.



Wechselt in den Modus zur Konfiguration der Trace-Ausgabe.



Wechselt in den Modus zur Anzeige der Trace-Ausgabe.

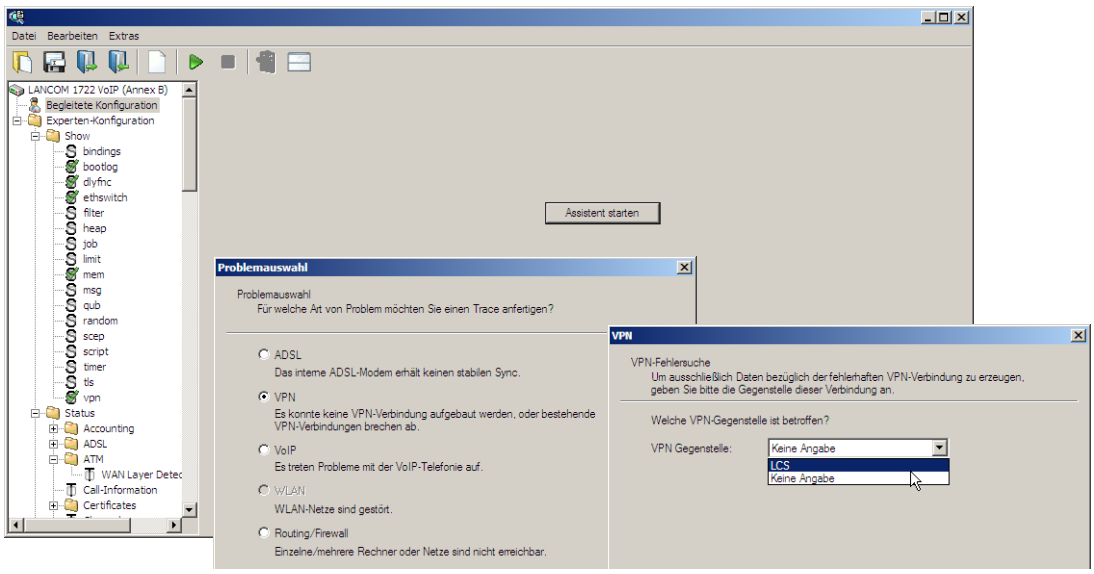


Konfiguration der Trace-Ausgaben mit dem Trace-Assistenten

Besonders einfach können die Trace-Einstellungen mit dem Assistenten vorgenommen werden. Wählen Sie dazu im linken Bereich des Trace-Dialogs die **Begleitende Konfiguration** und klicken Sie im Hauptfenster **Assistent starten**. In den folgenden Dialogen können Sie die Aufgabenstellung für den Trace auswählen (z. B. VPN) und den Trace ggf. weiter einschränken (z B. auf eine bestimmte VPN-Gegenstelle). Beim Abschluss des Assistenten wählen Sie aus, ob der Assistent die bestehende Trace-Konfiguration ersetzen oder ergänzen soll.



Beim Ersetzen der Trace-Konfiguration werden alle bisherigen Trace-Einstellungen gelöscht (mit Ausnahme des Bootlog-Traces, der automatisch enthalten ist). Speichern Sie daher ggf. vor Ausführung des Assistenten die bisherige Tracekonfiguration für eine spätere Verwendung.



Experten-Konfiguration der Trace-Ausgaben

Über die Einstellungen des Assistenten hinaus können, mit Hilfe der Experten-Konfiguration, die Traces und weitere Anzeigen genauer eingestellt werden. Die Experten-Konfiguration unterteilt sich in drei Bereiche:

- Show

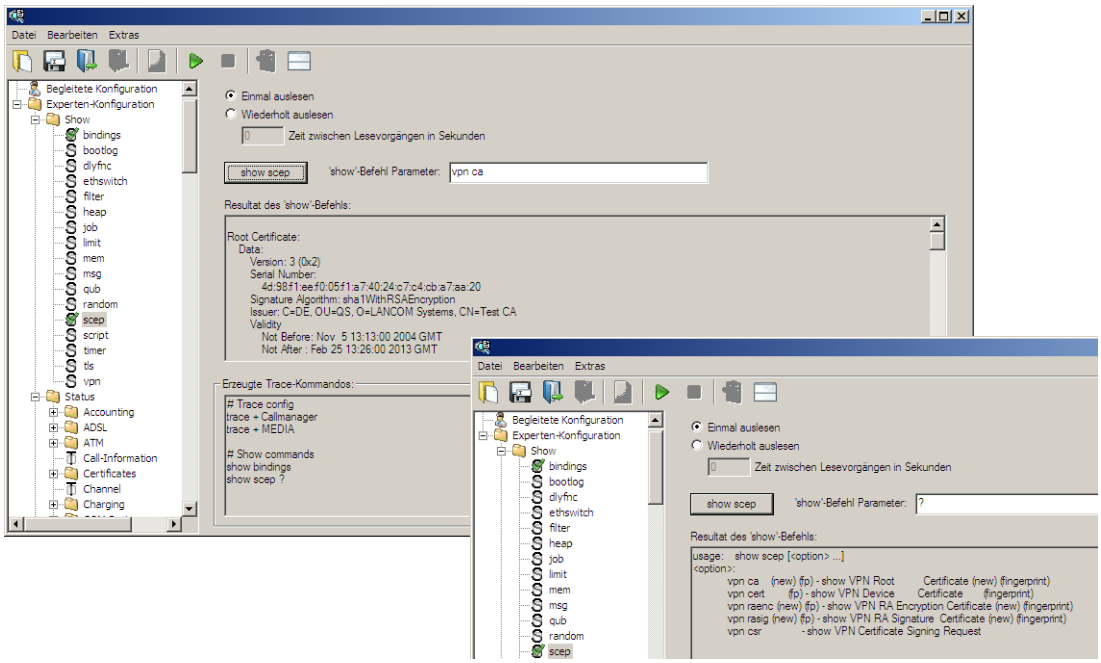
  Für jeden Gerätetyp können bestimmte Informationen mit einem Show-Kommando aufgerufen werden – üblicherweise werden die Show-Kommandos auf der Kommandozeile (Telnet) angewendet. In der Experten-Konfiguration des Traces kann der Aufruf dieser Show-Kommandos sehr bequem über die grafische Windows-Oberfläche erfolgen.

  Klicken Sie im linken Bereich des Trace-Dialogs auf den Namen eines Show-Kommandos und dann den Show-Button, um die aktuelle Ausgabe des Show-Kommandos aufzurufen. Je nach gewähltem Eintrag können bzw.

müssen noch ergänzende Parameter angegeben werden. Eine Information über diese Parameter erhalten Sie, wenn Sie in das Eingabefeld ein Fragezeichen eingeben und den Show-Button klicken.

Um die Ausgabe des Show-Kommandos in die Trace-Daten zu übernehmen, klicken Sie auf das entsprechende Kontrollkästchen vor dem Namen des Eintrags. Zu jedem aktivierten Show-Kommando kann separat eingestellt werden, ob es nur einmal beim Start des Traces ausgeführt wird oder in regelmäßigen Intervallen, die in Sekunden eingestellt werden.

Die Einstellungen der Show-Kommandos werden zusammen mit den eigentlichen Trace-Einstellungen in der Trace-Konfiguration gespeichert.



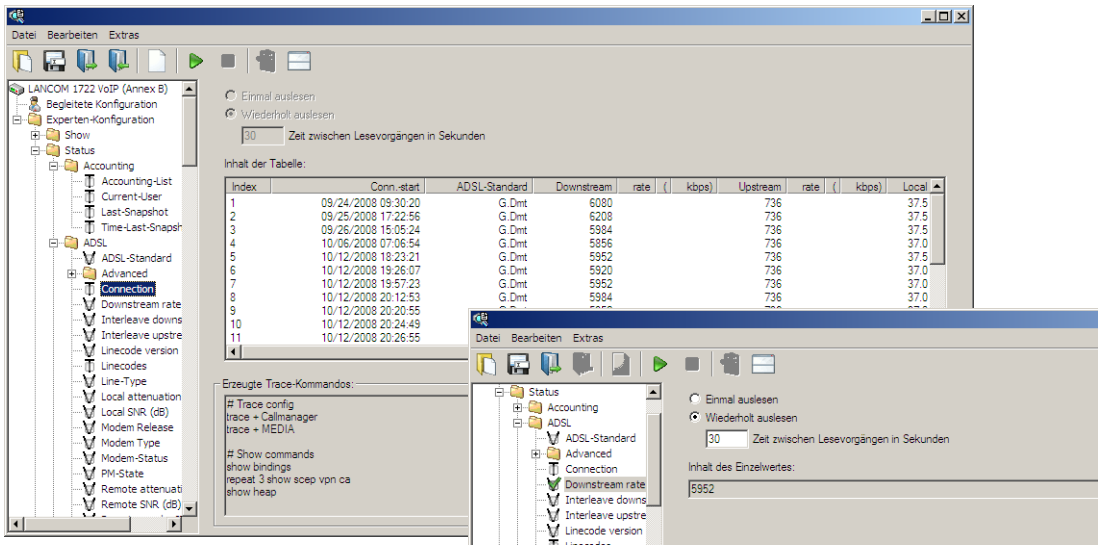
■ Status

Über die Kommandozeile (Telnet) oder über WEBconfig können umfangreiche Statusinformationen und Statistiken über ein Gerät abgefragt werden. Alle verfügbaren Status-Informationen können auch über den Trace-Dialog eingesehen werden. Tabellen und Einzelwerte werden dabei über spezielle Symbole dargestellt.

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 dem Namen des Eintrags. Zu jedem aktivierten Status-Eintrag kann separat eingestellt werden, ob er nur einmal beim Start des Traces ausgelesen wird oder in regelmäßigen Intervallen, die in Sekunden eingestellt werden.

Die Einstellungen der Status-Informationen werden zusammen mit den eigentlichen Trace-Einstellungen in der Trace-Konfiguration gespeichert. Die Status-Informationen werden zusammen mit den eigentlichen Trace-Daten gespeichert.



■ Trace-Einstellungen

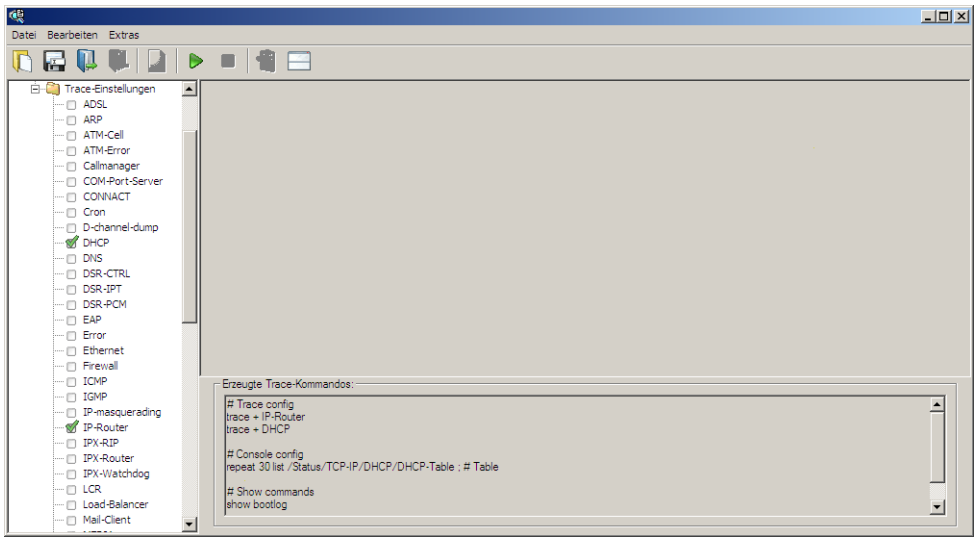
Im Bereich der Trace-Einstellungen können die Traces aktiviert werden, die für das aktuelle Gerät ausgegeben werden sollen.

Um die Ausgabe des Traces in die Trace-Daten zu übernehmen, klicken Sie auf das entsprechende Kontrollkästchen vor dem Namen des Eintrags. Zu jedem Trace können Sie einen Filter eingeben. Wenn Sie z. B. nur die IP-Traces einer bestimmten Workstation anzeigen möchten, geben Sie die entsprechende IP-Adresse als Filter des IP-Router-Traces ein.



Anzeige der Trace-Daten

Die komplette Konfiguration des Traces wird im unteren Bereich des Dialogs angezeigt: Alle aktiven Trace-, Status- und Show-Einträge werden mit den jeweiligen Filtern und Parametern dort aufgelistet.



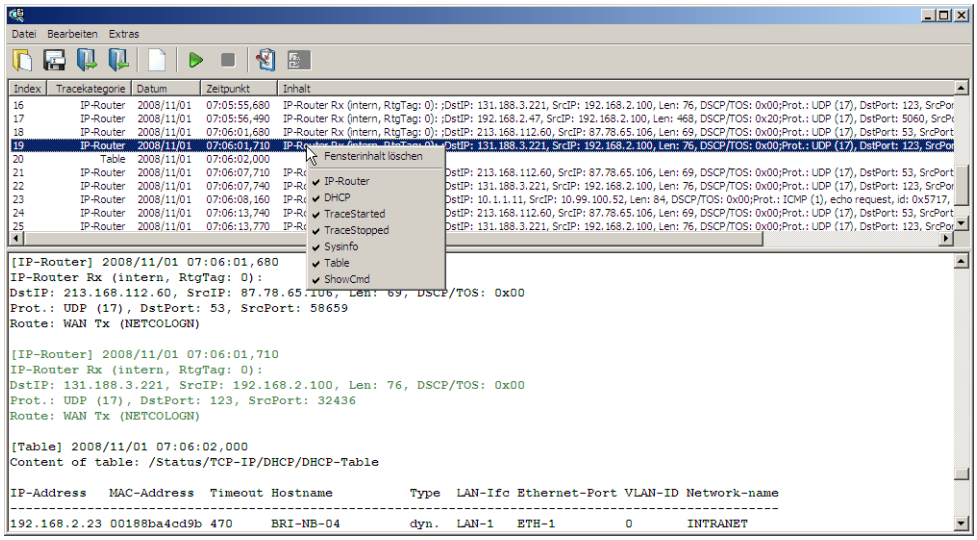
Um die Ausgabe der Trace-Daten zu starten, wechseln Sie mit dem Start-Button in den Anzeige-Modus. In dieser Ansicht werden die laufenden Trace-Ausgaben angezeigt:

- Im oberen Bereich werden die Trace-Ereignisse chronologisch aufgelistet.
- Im unteren Bereich werden die Ergebnisse der Ereignisse nacheinander aufgeführt.

Zur leichteren Navigation in langen Trace-Ausgaben können Sie im oberen Bereich auf ein Trace-Ereignis klicken, das entsprechende Ergebnis wird dann in der Liste aktiviert und in grün hervorgehoben.

Mit einem rechten Mausklick auf ein Trace-Ereignis öffnen Sie ein Kontext-Menü, in dem Sie die einzelnen Trace-Ergebnisse ein- und ausblenden können.

Die Trace-Daten werden erfasst, solange die Trace-Ausgabe aktiv ist. Um eine Überlastung des Arbeitsspeichers auf der Workstation mit dem LANmonitor zu vermeiden, werden die Trace-Daten automatisch in eine Backup-Datei gespeichert. Die zeitlichen Intervalle und die maximale Größe einer Sicherungsdatei können Sie unter **Extras** ▶ **Sonstige Einstellungen** ▶ **Tracebackup** einstellen.



Sichern und Wiederherstellen der Trace-Konfiguration

Zur späteren Wiederverwendung oder Weitergabe an einen anderen Benutzer kann die komplette Konfiguration der Trace-Ausgabe über **Datei** ▶ **Tracekonfiguration speichern** auf einen Datenträger geschrieben und später mit **Datei** ▶ **Tracekonfiguration laden** wieder geöffnet werden.

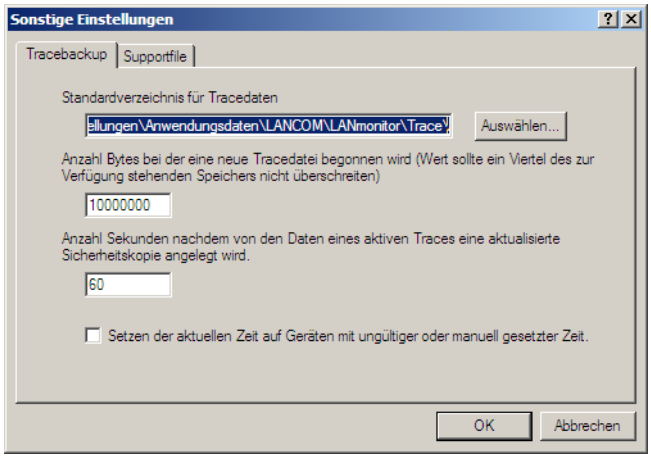
Sichern und Wiederherstellen der Trace-Daten

Auch die eigentlichen Trace-Daten können zur späteren Bearbeitung oder Weitergabe an einen anderen Benutzer über **Datei** ▶ **Tracedaten speichern** auf einen Datenträger geschrieben und später mit **Datei** ▶ **Tracedaten laden** wieder geöffnet werden.

Backup-Einstellungen für die Traces

Beim Starten eines Traces über LANmonitor wird automatisch eine Backup-Datei mit den aktuellen Trace-Daten gespeichert. Die Einstellungen für das Trace-Backup können Sie unter **Extras ▶ Sonstige Einstellungen ▶ Tracebackup** vornehmen. Stellen Sie dabei die folgenden Parameter ein:

- Verzeichnis für die Trace-Backups
- Maximale Größe einer Trace-Backup-Datei. Wenn diese Größe mit einem aktiven Trace erreicht wird, wird automatisch eine weitere Trace-Backup-Datei angelegt.
- Speicherintervall der Trace-Backup-Datei. Wenn diese Zeit erreicht ist, wird automatisch eine aktualisierte Version der Trace-Backup-Datei gespeichert. In der Trace-Backup-Datei sind also die Informationen zwischen dem letzten Backup und dem aktuellen Zeitpunkt nicht enthalten.
- Zusätzlich kann die aktuelle Zeit der Workstation mit dem LANmonitor als Zeit für den Trace gesetzt werden, z. B. wenn das getracte Gerät selbst nicht über eine gültige Zeitinformation verfügt.

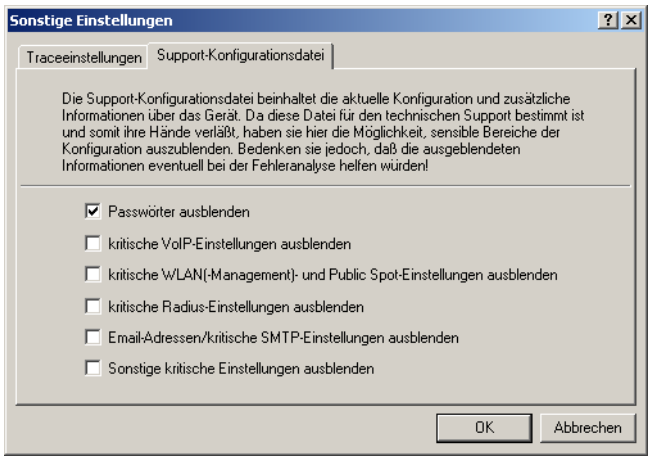


Support-Datei speichern

Mit einer Support-Datei können alle für den Support relevanten Informationen komfortabel in eine Datei geschrieben werden:

- Tracedaten wie in den aktuellen Einstellungen konfiguriert (wie mit der Funktion "Tracedaten speichern")
- aktuelle Gerätekonfiguration
- Bootlog
- Sysinfo

Beim Speichern der Gerätekonfiguration können dabei sicherheitsrelevante Informationen, die für den Support nicht von Bedeutung sind, ausgeblendet werden. Im Trace-Fenster unter **Extras ▶ Sonstige Einstellungen ▶ Supportfile** können Sie auswählen, welche Informationen nicht in der Support-Datei gespeichert werden sollen:



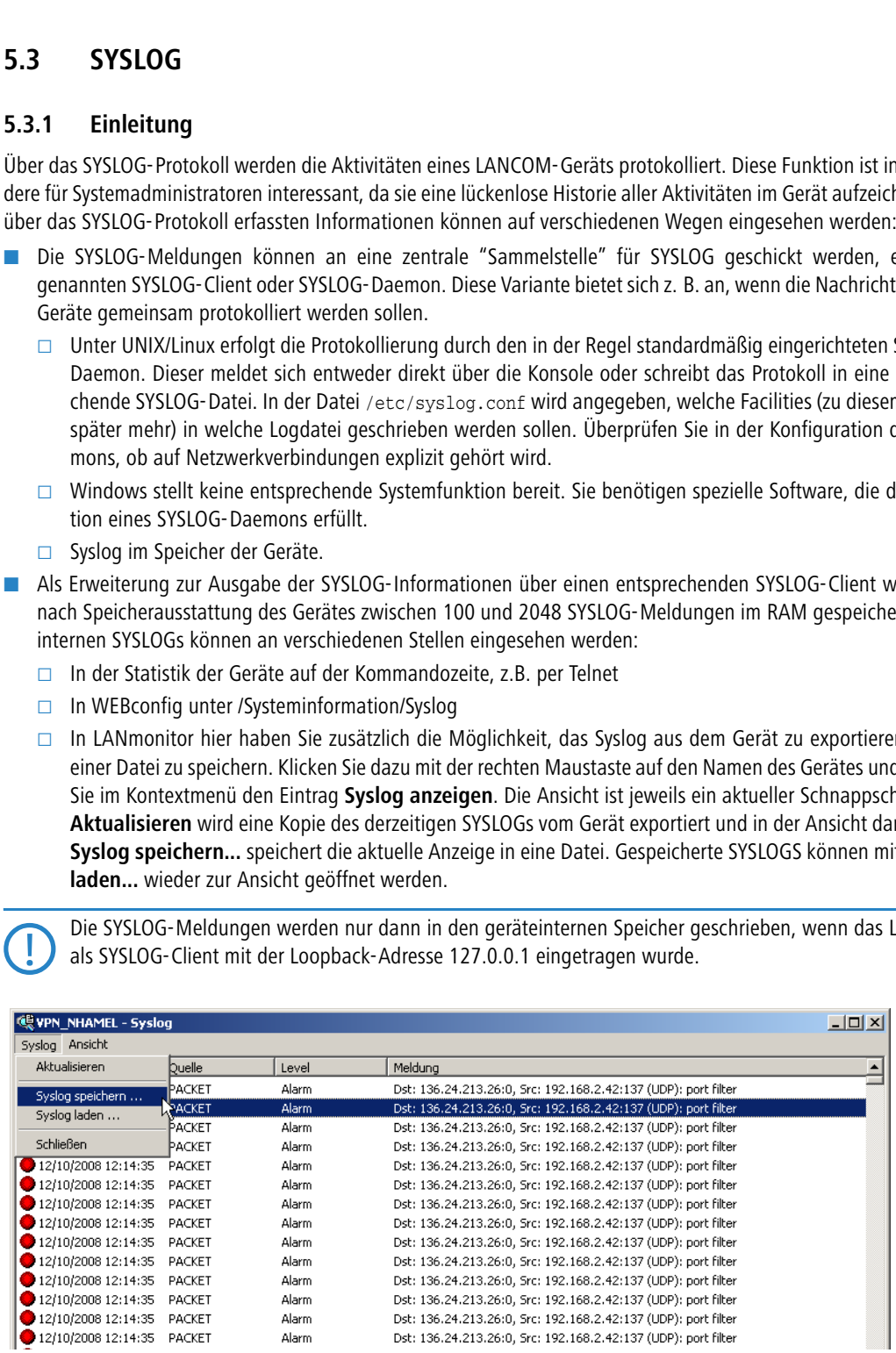
Die so erstellte Support-Datei enthält alle Informationen im Klartext. Sie können die Datei daher in einem Editor öffnen und auf ggf. noch vorhandene sensible Einträge prüfen.

5.3 SYSLOG

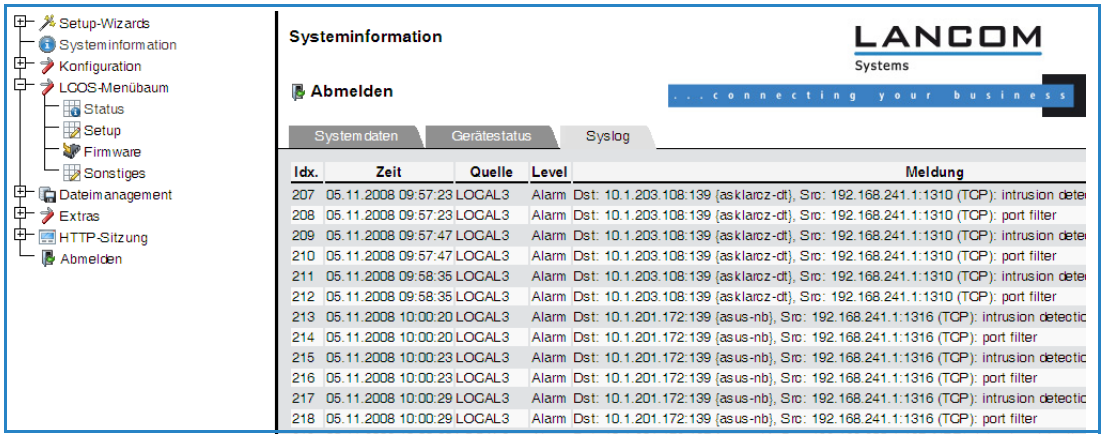
5.3.1 Einleitung

Über das SYSLOG-Protokoll werden die Aktivitäten eines LANCOM-Geräts protokolliert. Diese Funktion ist insbesondere für Systemadministratoren interessant, da sie eine lückenlose Historie aller Aktivitäten im Gerät aufzeichnet. Die über das SYSLOG-Protokoll erfassten Informationen können auf verschiedenen Wegen eingesehen werden:

- Die SYSLOG-Meldungen können an eine zentrale "Sammelstelle" für SYSLOG geschickt werden, einen so genannten SYSLOG-Client oder SYSLOG-Daemon. Diese Variante bietet sich z. B. an, wenn die Nachrichten vieler Geräte gemeinsam protokolliert werden sollen.
  - Unter UNIX/Linux erfolgt die Protokollierung durch den in der Regel standardmäßig eingerichteten SYSLOG-Daemon. Dieser meldet sich entweder direkt über die Konsole oder schreibt das Protokoll in eine entsprechende SYSLOG-Datei. In der Datei `/etc/syslog.conf` wird angegeben, welche Facilities (zu diesem Begriff später mehr) in welche Logdatei geschrieben werden sollen. Überprüfen Sie in der Konfiguration des Daemons, ob auf Netzwerkverbindungen explizit gehört wird.
  - Windows stellt keine entsprechende Systemfunktion bereit. Sie benötigen spezielle Software, die die Funktion eines SYSLOG-Daemons erfüllt.
  - Syslog im Speicher der Geräte.
- Als Erweiterung zur Ausgabe der SYSLOG-Informationen über einen entsprechenden SYSLOG-Client werden je nach Speicherausstattung des Gerätes zwischen 100 und 2048 SYSLOG-Meldungen im RAM gespeichert. Diese internen SYSLOGs können an verschiedenen Stellen eingesehen werden:
  - In der Statistik der Geräte auf der Kommandozeite, z.B. per Telnet
  - In WEBconfig unter /Systeminformation/Syslog
  - In LANmonitor hier 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.



Alternativ können Sie die aktuellen SYSLOG-Meldungen auf der Startseite von WEBconfig auf der Registerkarte SYSLOG einsehen:



5.3.2 Aufbau der SYSLOG-Nachrichten

Die SYSLOG-Nachrichten bestehen aus drei Teilen:

- Priorität
- Header
- Inhalt

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-Sufen sind im LANCOM auf fünf Stufen reduziert. Die nachfolgende Tabelle zeigt die Zuordnung zwischen dem LANCOM-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 LANCOM einstellen können. Zusätzlich gibt Ihnen die letzte Spalte der Tabelle die standardmäßige Zuordnung zwischen den internen Quellen des LANCOM und den SYSLOG-Facilities an. Diese Zuordnung kann bei Bedarf verändert werden.

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

Header

Der Header beinhalten 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.

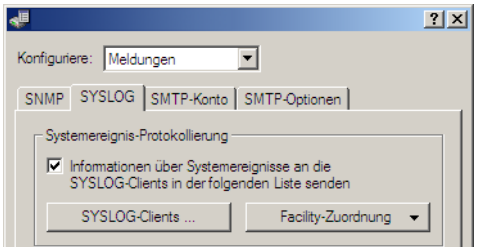
Für die Auswertung der SYSLOG-Meldungen im internen Speicher müssen die LANCOM-Geräte über eine gültige Zeitinformation verfügen.

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.

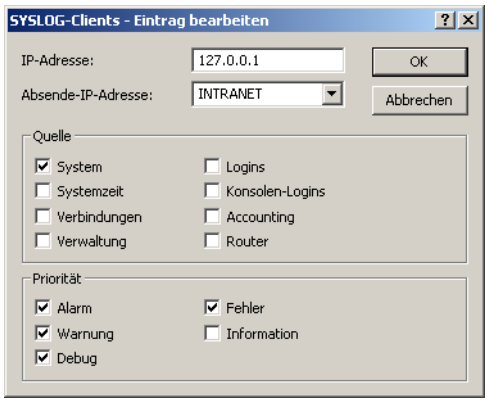
5.3.3 Konfiguration von SYSLOG über LANconfig

Die Parameter zur Konfiguration von SYSLOG finden Sie unter LANconfig im Konfigurationsbereich "Meldungen" auf der Registerkarte "SYSLOG".

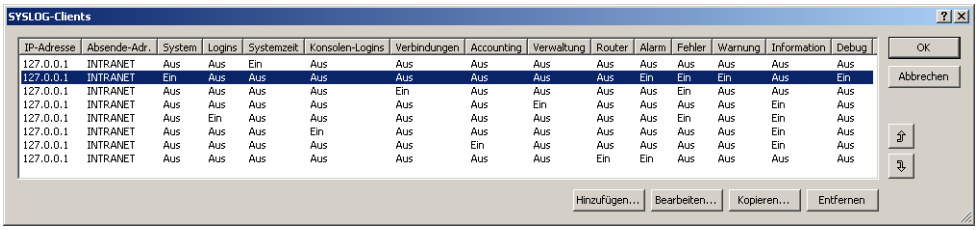


Anlegen von SYSLOG-Clients

Bei der Definition eines SYSLOG-Clients legen Sie zunächst die IP-Adresse fest, an welche die SYSLOG-Nachrichten geschickt werden sollen. Geben Sie dazu optional eine abweichende Absende-IP-Adresse an. Wählen Sie aus, welche der LANCOM-internen Quellen Nachrichten an diesen SYSLOG-Client versenden sollen. Mit der Auswahl von bestimmten Prioritäten können Sie den Umfang der Nachrichten weiter einschränken, z. B. nur auf Alarm- oder Fehlermeldungen.



Ab LCOS-Version 7.6 ist die Tabelle der SYSLOG-Clients im Auslieferungszustand mit sinnvollen Einstellungen vorbelegt, um wichtige Ereignisse für die Diagnose im internen SYSLOG-Speicher abzulegen. Der folgende Screenshot zeigt diese vordefinierten SYSLOG-Clients unter LANconfig:

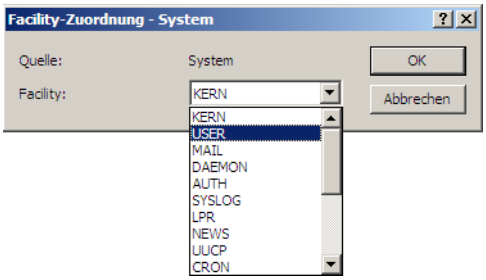


Weitere Informationen über die Bedeutung der vordefinierten SYSLOG-Clients sowie die Updatemöglichkeiten für bestehende LANCOM-Geräte finden Sie im Abschnitt "Tabelle der SYSLOG-Clients" bei der Konfiguration von SYSLOG über Telnet oder WEBconfig.

Zuordnung von LANCOM-internen Quellen zu SYSLOG-Facilities

Das SYSLOG-Protokoll verwendet bestimmte Bezeichnungen für die Quellen der Nachrichten, die so genanntne Facilities. Jede interne Quelle der LANCOM-Geräte, die eine SYSLOG-Nachricht erzeugen kann, muss daher einer SYSLOG-Facility zugeordnet sein.

Die standardmäßige Zuordnung kann bei Bedarf verändert werden. So können z. B. alle SYSLOG-Meldungen eines LANCOMs mit einer bestimmten Facility (Local7) versendet werden. Mit der entsprechenden Konfiguration des SYSLOG-Clients können so alle LANCOM-Meldungen in einer gemeinsamen Log-Datei gesammelt werden.



5.3.4 Konfiguration von SYSLOG über Telnet oder WEBconfig

Pfad: Setup/SYSLOG

- **Aktiv**

  Aktiviert den Versand von Informationen über Systemereignisse an die konfigurierten SYSLOG-Clients.

- **Port**

  Port, der für den Versand der SYSLOG-Nachichten verwendet wird.

Facility-Zuordnung

Pfad: Setup/SYSLOG/Facility-Mapper

- **Facility**

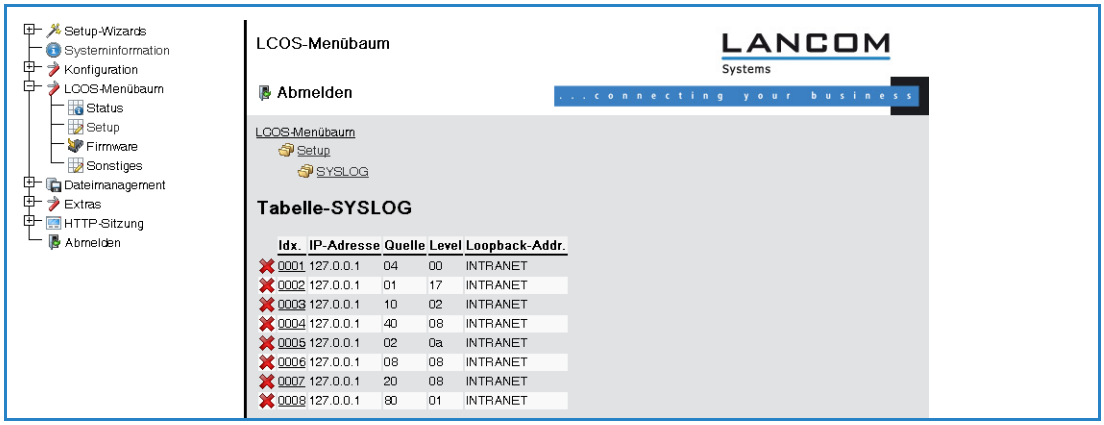
  Zuordnung der Quellen zu bestimmten Facilities.

- **Quelle**

  Zuordnung der Quellen zu bestimmten Facilities.

Tabelle der SYSLOG-Clients

Ab LCOS-Version 7.6 ist die Tabelle der SYSLOG-Clients im Auslieferungszustand mit sinnvollen Einstellungen vorbelegt, um wichtige Ereignisse für die Diagnose im internen SYSLOG-Speicher abzulegen. Der folgende Screenshot zeigt diese vordefinierten SYSLOG-Clients unter WEBconfig:



WEBconfig: LCOS-Menübaum ▶ Setup ▶ SYSLOG ▶ Tabelle-SYSLOG

Alle vordefinierten SYSLOG-Clients übertragen die Nachrichten an die IP-Adresse 127.0.0.1, also an das LANCOM selbst. Als Absende-IP-Adresse wird jeweils die IP-Adresse aus dem Netzwerk "INTRANET" verwendet. Die einzelnen Einträge haben die folgenden Funktionen:

Index	Quelle	Level	Bedeutung
0001	04	00	Systemzeit ohne Angabe eines Levels.
0002	01	17	Systemnachrichten mit dem Level Alarm, Fehler, Warnung oder Debug.
0003	10	02	Verbindungsnachrichten mit dem Level Fehler.
0004	40	08	Verwaltungsnachrichten mit dem Level Information.
0005	02	0a	Logins mit dem Level Fehler oder Information.
0006	08	08	Konsolen-Logins mit dem Level Information.
0007	20	08	Accountingnachrichten mit dem Level Information.
0008	80	01	Routernachrichten mit dem Level Alarm.

Wenn Sie ein bestehendes Gerät updaten, werden die Einstellungen für SYSLOG **nicht** auf diese Standardwerte gesetzt, sodass eventuell vorhandene Einstellungen erhalten bleiben. In diesem Fall können Sie die Einstellungen gemäß dieser Tabelle von Hand eintragen. Alternativ finden Sie in der "KnowledgeBase" im Support-Bereich der LANCOM-Webseite ein Script, mit dem Sie automatisch die vordefinierten SYSLOG-Clients einspielen können.

- **Idx.**
  Position des Eintrags in der Tabelle.
- **IP-Adresse**
  IP-Adresse des SYSLOG-Clients.
- **Quelle**
  Quelle, die zum Versenden einer Meldung führt. Jede Quelle wird durch einen bestimmten Code dargestellt.
- **Level**
  SYSLOG-Level, mit dem die Meldung verschickt wird. Jedes Level wird durch einen bestimmten Code dargestellt.
- **Loopback-Addr.**
  Hier können Sie optional eine Absendeadresse konfigurieren, die statt der ansonsten automatisch für die Zieladresse gewählten Absendeadresse verwendet wird.

5.4 Der Ping-Befehl

Das ping-Kommando an der Eingabeaufforderung einer Telnet- oder 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 der letzte Router vor dem Host mit „Network unreachable" (Netzwerk nicht erreichbar) oder „Host unreachable" (Gegenstelle nicht erreichbar).

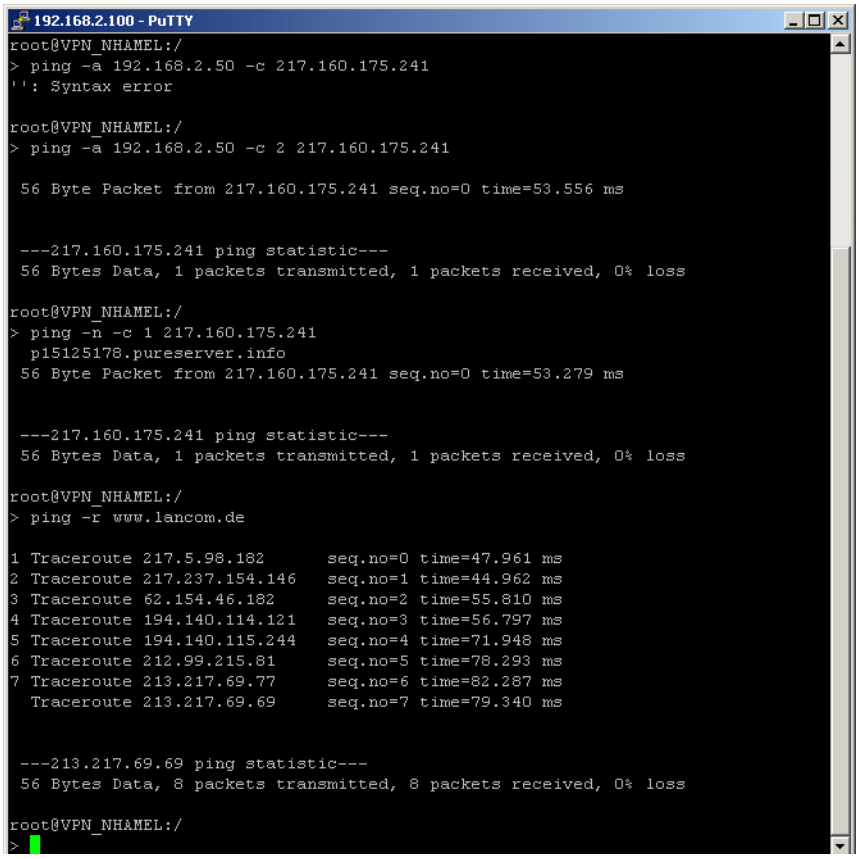
Die Syntax des Ping-Kommandos lautet wie folgt:

- `ping [-fnqr] [-s n] [-i n] [-c n] [-a a.b.c.d] Ziel-Host`

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

Parameter	Bedeutung
-a a.b.c.d	Setzt die Absenderadresse des Pings (Standard: IP-Adresse des Routers)
-a INT	Setzt die Intranet-Adresse des Routers als Absenderadresse
-a DMZ	Setzt die DMZ-Adresse des Routers als Absenderadresse
- a LBx	Setzt eine der 16 Loopback-Adressen im Lancom als Absenderadresse. Gültige Werte für x sind die Hexadezimalen Werte 0-f
-f	flood ping: Sendet große Anzahl von Ping-Signalen in kurzer Zeit. Kann z.B. zum Testen der Netzwerkbandbreite genutzt werden. ACHTUNG: flood ping kann leicht als DoS Angriff fehlinterpretiert werden.
-n	Liefert den Computernamen zu einer eingegebenen IP-Adresse zurück
-q	Ping-Kommando liefert keine Ausgaben auf der Konsole
-r	Wechselt in Traceroute-Modus: Der Weg der Datenpakete zum Zielcomputer wird mit allen Zwischenstationen angezeigt

Parameter	Bedeutung
-s n	Setze Größe der Pakete auf n Byte (max. 1472)
-i n	Zeit zwischen den einzelnen Paketen in Sekunden
-c n	Sende n Ping-Signale
Zielcomputer	Adresse oder Hostnamen des Zielcomputers
stop /<RETURN>	Die Eingabe von “stop” oder das Drücken der RETURN-Taste beenden das Ping-Kommando



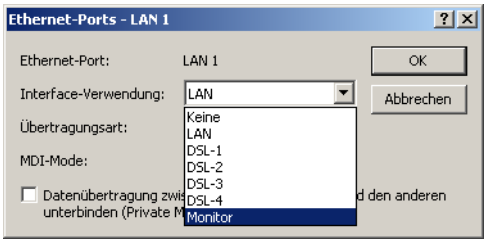
5.5 Monitor-Modus am Switch

Die über den Switch der LANCOM-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.

LANconfig

Bei der Konfiguration mit LANconfig öffnen Sie die Ethernet-Switch-Einstellungen im Konfigurationsbereich 'Interfaces' auf der Registerkarte 'LAN' mit der Schaltfläche **Ethernet-Ports**.

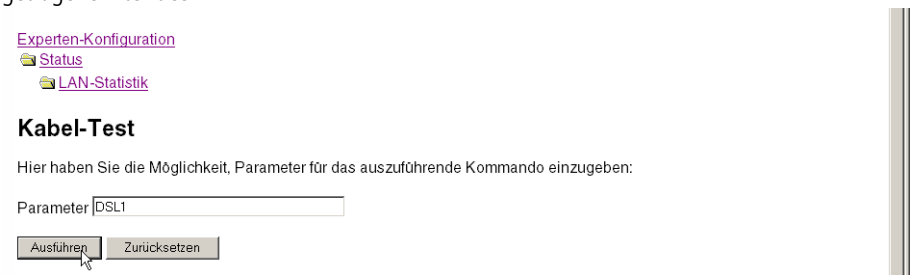


WEBconfig: LCOS-Menübaum ▶ Setup ▶ Schnittstellen ▶ Ethernet-Ports

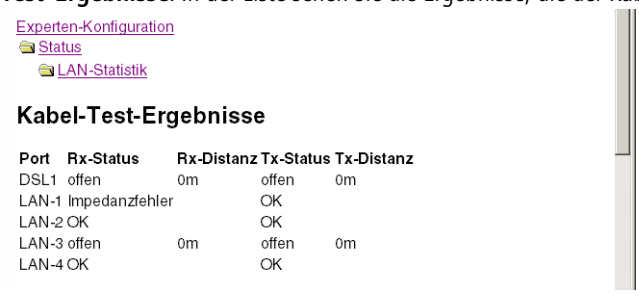
5.6 Kabel-Tester

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 LANCOM heraus die Verkabelung testen. Wechseln Sie dazu unter WEBconfig in den Menüpunkt **Expertenkonfiguration ▶ Status ▶ Ethernet-Ports ▶ 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 **Expertenkonfiguration ▶ Status ▶ Ethernet-Ports ▶ Kabel-Test-Ergebnisse**. In der Liste sehen Sie die Ergebnisse, die der Kabel-Test für die einzelnen Interfaces ergeben hat.



Als Ergebnisse können folgende Werte erscheinen:

- **OK**: Kabel richtig eingesteckt, Leitung in Ordnung.
- **offen** mit Distanz **"0m"**: kein Kabel eingesteckt oder eine Unterbrechung in weniger als ca. 10 Metern.
- **offen** mit Angabe einer konkreten Distanz: Kabel ist eingesteckt, hat jedoch in der angegebenen Entfernung einen Defekt.
- **Impedanzfehler**: Das Kabelpaar am anderen Ende ist nicht mit der korrekten Impedanz abgeschlossen.

6 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
- Absichern des ISDN-Einwahlzugangs

Zum Ende des Kapitels finden Sie die wichtigsten Sicherheitseinstellungen in Form einer Checkliste. Damit Sie ganz sicher sein können, dass Ihr LANCOM bestens abgesichert ist.

Zur Sicherheit der Daten tragen auch noch einige weitere Funktionen des LCOS bei, die in separaten Kapiteln beschrieben sind:

- 'Firewall' → Seite 8-1
- 'IP-Masquerading' → Seite 7-17
- 'Virtuelle LANs (VLANs)' → Seite 12-1

6.1 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 ein LANCOM die Möglichkeit, die Konfiguration mit verschiedenen Mitteln zu schützen.

6.1.1 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.

Hinweis: Ein nicht gesetztes Passwort wird auf allen LANCOM durch eine blinkende Power-LED signalisiert, sofern die Geräte in Betrieb genommen worden sind (lokale Intranet-Adresse vorhanden).

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 regelmäßig.**
  Passwörter sollen möglichst häufig gewechselt werden. Das ist mit Mühe verbunden, erhöht aber die Sicherheit des Passwortes beträchtlich.
- **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.

Eingabe des Passwortes

Das Feld zur Eingabe des Passworts finden Sie in LANconfig im Konfigurationsbereich 'Management' auf der Registerkarte 'Admin'. In einer Terminal- bzw. einer Telnet-Sitzung setzen oder ändern Sie das Passwort mit dem Befehl `passwd`.

LANconfig: Management ▶ Admin ▶ Passwort

WEBconfig: Extras ▶ Passwort ändern

Den SNMP-Zugang schützen

Im gleichen Zug sollten Sie auch den SNMP-Lesezugriff mit Passwort schützen. Für SNMP wird das allgemeine Konfigurations-Passwort verwendet.

LANconfig: Management ▶ Admin ▶ SNMP-Lesezugriff nur mit Passwort zulassen

WEBconfig: LCOS-Menübaum ▶ Setup ▶ SNMP ▶ Passw.Zwang-fuer-SNMP-Lesezugriff

6.1.2 Die Login-Sperre

Die Konfiguration im LANCOM 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.

Tritt auf einem Zugang die Sperre in Kraft, so sind auch alle anderen Zugänge automatisch gesperrt.

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

WEBconfig: LCOS-Menübaum ▶ Setup ▶ Config

6.1.3 Einschränkung der Zugriffsrechte auf die Konfiguration

Der Zugriff auf die internen Funktionen kann wie folgt nach Interfaces getrennt konfiguriert werden:

- ISDN-Aministrationszugang
- LAN
- Wireless LAN (WLAN)
- WAN (z.B. ISDN, DSL oder ADSL)

Bei den Netzwerk-Konfigurationszugriffen können weitere Einschränkungen vorgenommen werden, z.B. dass nur die Konfiguration von bestimmten IP-Adressen oder LANCAPI-Clients 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.

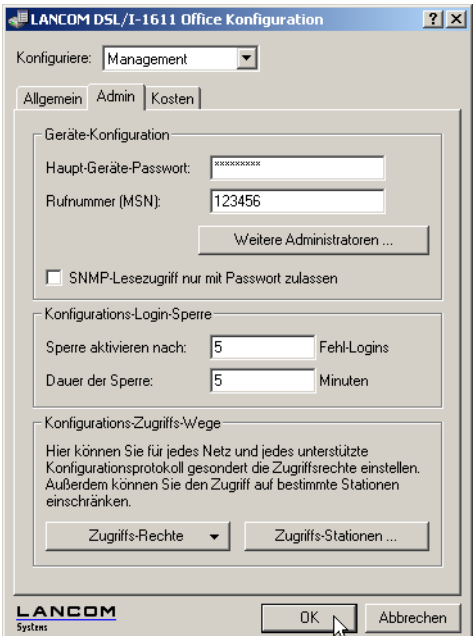
Den ISDN-Administrationszugang einschränken

Nur für Modelle mit ISDN-Schnittstelle.

Solange keine MSN für den Konfigurations-Zugriff eingetragen ist, nimmt ein **unkonfiguriertes** LANCOM die Rufe auf alle MSNs an. Sobald die erste Änderung in der Konfiguration gespeichert ist, nimmt das Gerät nur noch die Anrufe auf der Konfigurations-MSN an!

Wenn bei der ersten Konfiguration keine Konfigurations-MSN eingetragen wird, ist die Fernkonfiguration damit ausgeschaltet und das Gerät gegen den Zugriff über die ISDN-Leitung geschützt.

① Wechseln Sie im Konfigurationsbereich 'Management' auf die Registerkarte 'Admin'.



② Geben Sie als Rufnummer im Bereich 'Geräte-Konfiguration' eine Rufnummer Ihres Anschlusses ein, die nicht für andere Zwecke verwendet wird.

Geben Sie alternativ unter Telnet den folgenden Befehl ein:

```
set /setup/config/Fernconfig 123456
```

Der ISDN-Administrationszugang ist als einzige Konfigurationsmethode von den im folgenden beschriebenen Netzwerk-Zugangsbeschränkungen ausgenommen. D.h. alle auf der ADMIN-MSN eingehenden Verbindungen werden nicht über die Zugriffssteuerung von entfernten Netzen eingeschränkt.

Wenn Sie die ISDN-Fernwartung ganz abschalten wollen, lassen Sie das Feld mit der ADMIN-MSN leer.

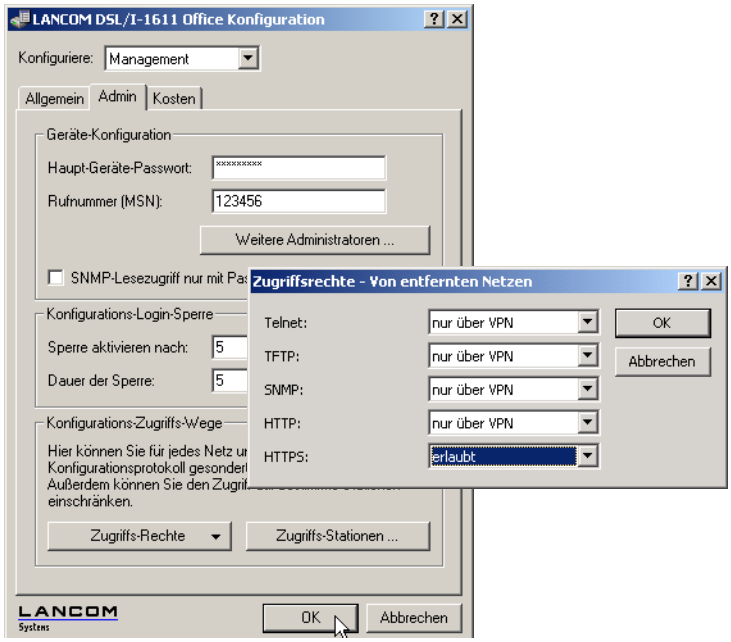
Den Netzwerk-Konfigurationszugriff einschränken

Der Zugriff auf die internen Funktionen kann - getrennt für Zugriffe aus dem lokalen Netz, aus entfernten Netzen oder aus Wireless LANs - für alle Konfigurationsdienste getrennt gesteuert werden.

Dabei kann der Konfigurationszugriff generell erlaubt oder verboten werden, als reiner Lesezugriff oder - falls Ihr Modell mit VPN ausgerüstet ist - auch nur über VPN erlaubt werden.

Konfiguration mit LANconfig

Die Konfigurationsdialoge mit den Zugriffsrechten vom lokalen oder aus entfernten Netzen werden über die Schaltfläche **Zugriffsrechte** geöffnet:



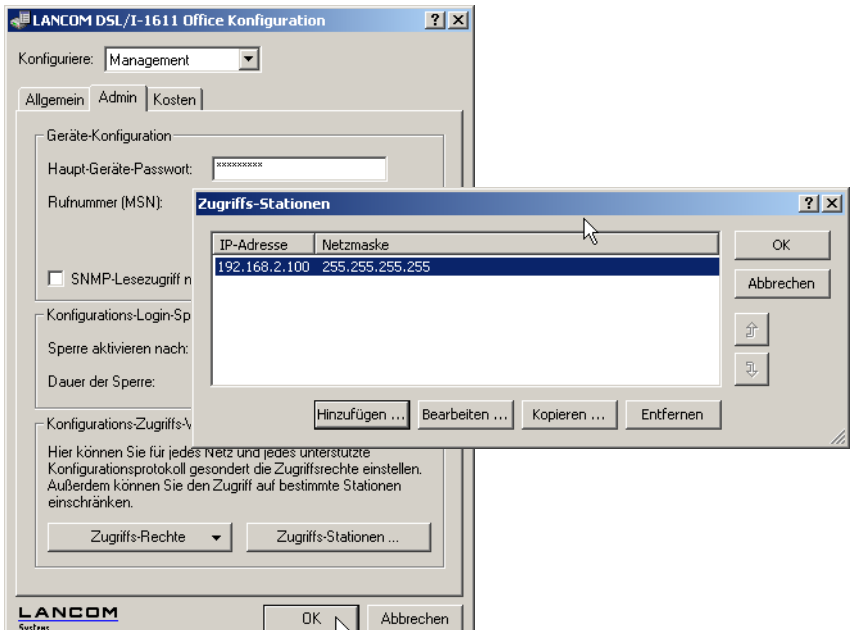
Wenn Sie den Netzwerkzugriff auf den Router über das WAN ganz sperren wollen, stellen Sie den Konfigurationszugriff von entfernten Netzen für alle Methoden auf 'nicht erlaubt'.

LANconfig: Management ▶ Admin ▶ Zugriffsrechte

WEBconfig: LCOS-Menübaum ▶ Setup ▶ Config ▶ Zugriffstabelle

Einschränkung des Netzwerk-Konfigurationszugriffs auf bestimmte IP-Adressen

Mit einer speziellen Filterliste kann der Zugriff auf die internen Funktionen der Geräte auf bestimmte IP-Adressen eingeschränkt werden. Der Konfigurationsdialog mit den Zugriffsrechten vom lokalen oder aus entfernten Netzen werden über die Schaltfläche **Zugriffs-Stationen** geöffnet:



Standardmäßig enthält diese Tabelle keine Einträge, damit kann also von Rechnern mit beliebigen IP-Adressen aus über TCP/IP ein Zugriff auf den Router 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 werden 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.

LANconfig: Management ▶ Admin ▶ Zugriffsstationen

WEBconfig: LCOS-Menübaum ▶ Setup ▶ TCP-IP ▶ Zugangs-Liste

6.2 Den ISDN-Einwahlzugang absichern

Bei einem Gerät mit ISDN-Anschluss kann sich prinzipiell jeder Teilnehmer in Ihren LANCOM einwählen. Um unerwünschte Eindringlinge zu vermeiden, müssen Sie deshalb einen besonderen Augenmerk auf die Absicherung des ISDN-Zugangs legen.

Die Absicherungsfunktionen des ISDN-Zugangs können in zwei Gruppen eingeteilt werden:

- Identifikationskontrolle
  - Zugangsschutz mit Name und Passwort
  - Zugangsschutz über die Anruferkennung
- Rückruf an festgelegte Rufnummern

6.2.1 Die Identifikationskontrolle

Zur Identifikationskontrolle kann entweder der Name der Gegenstelle oder die sogenannte Anruferkennung herangezogen werden. Die Anruferkennung ist die Telefonnummer des Anrufers, die bei ISDN normalerweise mit dem Anruf an die Gegenstelle übermittelt wird.

Welcher "Identifier" zur Erkennung des Anrufers verwendet werden soll, wird in folgender Liste eingestellt:

LANconfig: Kommunikation ▶ Ruf-Verwaltung

WEBconfig: LCOS-Menübaum ▶ Setup ▶ WAN ▶ Schutz

Zur Auswahl stehen die folgenden Möglichkeiten:

- kein Schutz: Anrufe aller Gegenstellen werden angenommen.
- nach Nummer: Es werden nur Anrufe angenommen, deren Anschlusskennungen (CLIP) in der Nummernliste eingetragen sind.
- nach geprüfter Nummer: Es werden nur Anrufe angenommen, deren Anschlusskennungen (CLIP) einerseits in der Nummernliste eingetragen sind, sowie andererseits von der Vermittlungsstelle für korrekt befunden wurden.

Die Identifizierung setzt natürlich voraus, dass die entsprechende Information vom Anrufer auch übermittelt wird.

Überprüfung des Benutzernamens und des Kennwortes

Bei einer PPP-Einwahl wird zunächst ein Benutzername (und in Verbindung mit PAP, CHAP oder MS-CHAP auch ein Passwort) beim Verbindungsaufbau an die Gegenstelle übertragen. Wählt sich ein Computer in den LANCOM ein, so fragt die verwendete Verbindungssoftware, beispielsweise das DFÜ-Netzwerk unter Windows, den zu übermittelnden Benutzernamen und das Passwort in einem Eingabefenster ab.

Baut der Router selber eine Verbindung auf, etwa zu einem Internet Service Provider, so verwendet er seinerseits Benutzername und Passwort aus der PPP-Liste. Ist dort kein Benutzername eingetragen, wird stattdessen der Gerätename verwendet.

LANconfig: Kommunikation ▶ Protokolle ▶ PPP-Liste

WEBconfig: LCOS-Menübaum ▶ Setup ▶ WAN ▶ PPP

Zur Auswahl stehen die folgenden Möglichkeiten:

Außerdem kann beim PPP-Protokoll auch der Anrufer von der Gegenstelle eine Authentifizierung verlangen. Er fordert dann die Gegenstelle zur Übermittlung eines Benutzer- bzw. Gerätenamens und eines Passwortes auf.



Die Sicherungsverfahren PAP, CHAP oder MS-CHAP wenden Sie natürlich nicht an, wenn Sie selber mit dem LANCOM z.B. einen Internet Service Provider anwählen. Sie werden den ISP wahrscheinlich nicht dazu bewegen können, eine Anfrage an ihn nach einem Passwort zu beantworten …

Überprüfung der Nummer

Beim Anruf über eine ISDN-Leitung wird in den meisten Fällen über den D-Kanal die Rufnummer des Anrufers übertragen, schon bevor eine Verbindung zustande kommt (CLI – **C**alling **L**ine **I**dentifier).

Wenn die Rufnummer in der Nummernliste vorhanden ist, kann der Zugang zum eigenen Netz gewährt werden, oder der Anrufer wird bei eingeschalteter Rückrufoption zurückgerufen. Ist ein Schutz im LANCOM über die Nummer vereinbart, werden alle Anrufe von Gegenstellen mit unbekannten Rufnummern abgelehnt.

Der Schutz mit Hilfe der Rufnummer kann mit allen B-Kanal-Protokollen (Layern) verwendet werden.

6.2.2 Der Rückruf

Eine besondere Variante des Zugriffsschutzes wird mit der Rückruffunktion erreicht: Dazu wird in der Gegenstellenliste für den gewünschten Anrufer die Option 'Rückruf' aktiviert und ggf. die Rufnummer angegeben.

LANconfig: Kommunikation ▶ Gegenstellen ▶ Gegenstellen (ISDN/seriell)

WEBconfig: LCOS-Menübaum ▶ Setup ▶ WAN ▶ Einwahl-Gegenstellen

Mit den Einstellungen in Namen- und Nummernliste können Sie das Rückrufverhalten Ihres Routers steuern:

- Der Router kann den Rückruf ablehnen.
- Er kann eine voreingestellte Rufnummer zurückrufen.
- Er kann zunächst den Namen überprüfen und dann eine voreingestellte Rufnummer zurückrufen.
- Die Rufnummer für den Rückruf kann vom Anrufer frei eingegeben werden.

Und ganz nebenbei steuern Sie über die Einstellungen die Verteilung der Kosten für die Verbindung. Ist in der Gegenstellenliste ein Rückruf 'Nach Name' vereinbart, übernimmt der rückrufende Router alle Gebühreneinheiten bis auf die, die für die Namensübermittlung benötigt wird. Ebenfalls fallen Einheiten für den Anrufer an, wenn der Anrufer nicht über CLIP (**C**alling **L**ine **I**dentifier **P**rotocol) identifiziert wird. Ist dagegen eine Identifizierung über die Rufnummer des Anrufers erlaubt und möglich, kommt der Anrufer sogar ganz ohne Kosten weg (Rückruf über den D-Kanal).

Eine besonders effektive Methode des Rückrufs ist das Fast-Call-Back-Verfahren (zum Patent angemeldet). Dieses Verfahren beschleunigt die Rückrufprozedur beträchtlich. Das Verfahren funktioniert nur dann, wenn es von beiden Gegenstellen unterstützt wird. Alle aktuellen LANCOM-Router beherrschen das Fast-Call-Back-Verfahren.

Weitere Informationen zum Rückruf finden Sie im Abschnitt 'Rückruf-Funktionen' → Seite 7-40.

6.3 Standort-Verifikation über ISDN oder 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.

6.3.1 GPS-Standort-Verifikation

Für die GPS-Standort-Verifikation 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 Standort-Verifikation wird das GPS-Modul automatisch wieder deaktiviert, sofern es nicht manuell eingeschaltet ist.

6.3.2 ISDN-Standort-Verifikation

Mit der ISDN-Standort-Verifikation können Sie den Missbrauch eines Routers verhindern: Der Router überprüft dann nach jedem Einschalten über einen ISDN-Anruf zu sich selbst, ob er am vorgesehenen Standort installiert ist. Erst wenn die Standort-Überprüfung erfolgreich ausgeführt wurde, wird das Router-Modul eingeschaltet.

Voraussetzungen für eine erfolgreiche ISDN-Standort-Verifikation:

- Das Gerät muss aus dem öffentlichen ISDN-Netz erreichbar sein.
- Während der Überprüfung mit dem Selbstanruf benötigt das Gerät zwei freie B-Kanäle. Solange nur ein freier Kanal bereitsteht, z.B. weil an einem Mehrgeräteanschluss mit zwei B-Kanälen ein Kanal zum Telefonieren verwendet wird, kann sich das Gerät nicht selbst über ISDN anrufen.

6.3.3 Konfiguration der Standort-Verifikation

LANconfig

Die Parameter für die Standort-Verifikation finden Sie im LANconfig im Konfigurationsbereich 'Management' auf der Registerkarte 'Standort'.

Auf der Registerkarte 'GPS' können Sie das GPS-Modul unabhängig von der Standort-Verifikation einschalten, um z. B. die aktuellen Standortkoordination mit LANmonitor zu überwachen.



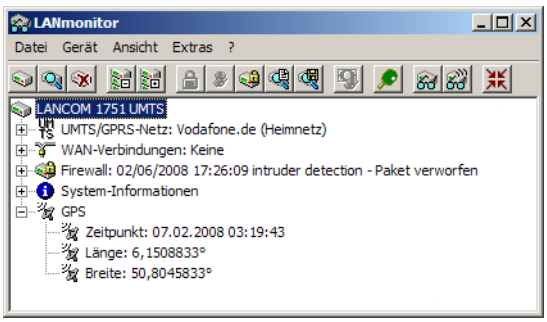
- Mit der Option 'Standort-Überprüfung einschalten' aktivieren Sie die Standort-Verifikation.
- Wählen Sie die Methode für die Standort-Überprüfung:
  - 'Selbst-Anruf' für die Überprüfung über ISDN mit einem Rückruf.
  - 'Rufweiterleitungs-Überprüfung' für die Überprüfung über ISDN durch Abfrage der Rufnummer aus der Vermittlungsstelle. Hierbei ist kein Rückruf erforderlich.
  - '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.

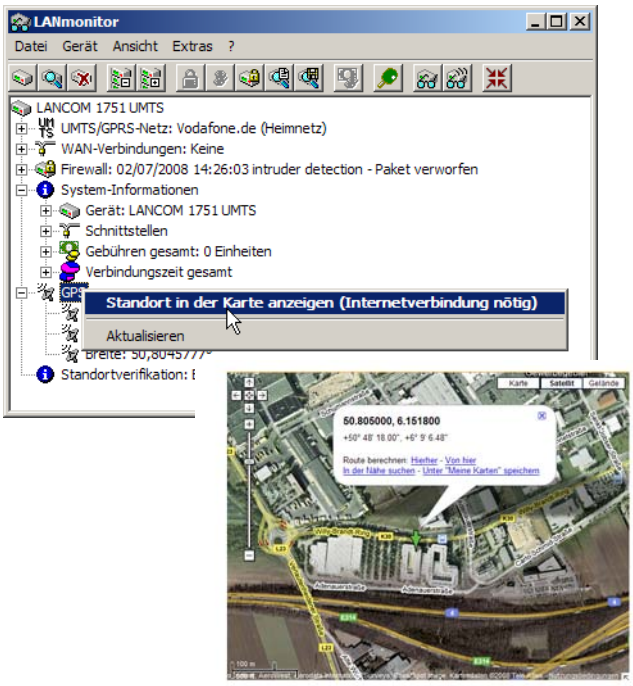
- Tragen Sie für die Standort-Überprüfung über 'Selbst-Anruf' oder 'Rufweiterleitungs-Überprüfung' als 'Ziel-Rufnummer' ein, auf welche Telefonnummer geprüft werden soll.
- Tragen Sie für die Standort-Überprüfung über GPS die Parameter für die GPS-Prüfung ein:
  - Längen- und Breitengrad
  - Abweichung von der erlaubten Position in Metern

Die Geo-Koordinaten für den aktuellen Standort kann das Gerät selbst ermitteln, indem Sie den Schalter 'Referenz-Koordinaten 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.



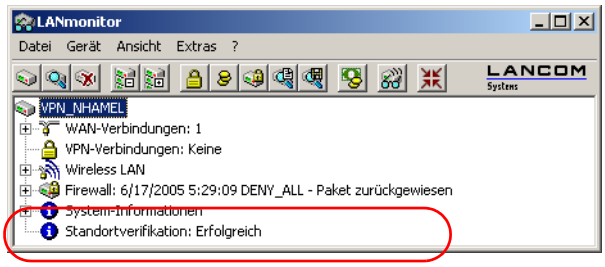
LANconfig: Kommunikation ▶ Gegenstellen ▶ Gegenstellen (ISDN/seriell)

WEBconfig: LCOS-Menübaum ▶ Setup ▶ Config ▶ Standortverifikation



Statusabfrage der Standort-Verifikation

Der Status der Standortverifikation kann über den LANmonitor eingesehen werden:



Mit WEBconfig (**Expertenkonfiguration ▶ Status ▶ Config ▶ Standortverifikation**) oder Telnet (`Status/Config/Standortverifikation`) können Sie den Status der Standort-Verifikation einsehen:



Erst wenn die Standort-Verifikation im Zustand 'Erfolgreich' ist, kann der Router Daten über die WAN-Interfaces übertragen.

- Eine Standort-Verifikation über ISDN ist dann erfolgreich, wenn die Nummer 'Erwarte-Ruf-von' mit der Nummer der 'Zuletzt-gesehener-Ruf-von' übereinstimmt. Der Anruf wird dabei nicht vom Router angenommen. Der Status zeigt außerdem an, ob der Router überhaupt einen Ruf erkannt hat.
- Eine Standort-Verifikation über GPS ist dann erfolgreich, wenn die GPS-Position gültig ist und innerhalb der zulässigen Abweichung mit der Soll-Position übereinstimmt.

6.4 Die Sicherheits-Checkliste

In der folgenden Checkliste finden Profis 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 Systems 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 Systems 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 WEP Einstellungen wählen Sie in LANconfig im Konfigurationsbereich 'WLAN-Sicherheit' auf der Registerkarte '802.11i/WEP' die Verschlüsselungseinstellungen für die logischen und physikalischen WLAN-Interfaces 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 Kontrolle der Access Control List wählen Sie in LANconfig im Konfigurationsbereich 'WLAN-Sicherheit' die Registerkarte 'Stationen'.

Mit der LANCOM Enhanced Passphrase Security (LEPS) ordnen Sie jeder MAC-Adresse in einer zusätzlichen Spalte der ACL eine individuelle Passphrase zu – eine beliebige Folge aus 4 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 WPA.

- **Haben Sie ein Kennwort für die Konfiguration vergeben?**

  Die einfachste Möglichkeit zum Schutz der Konfiguration ist die Vereinbarung eines Kennworts. Solange Sie kein Kennwort vereinbart haben, kann jeder die Konfiguration des Gerätes verändern. Das Feld zur Eingabe des Kennworts finden Sie in LANconfig im Konfigurationsbereich 'Management' auf der Registerkarte 'Security'. Es ist ins-

besondere dann unerläßlich, ein Kennwort 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 Kennwortschutz für die Konfiguration (siehe vorhergehender Abschnitt). Das Feld zur Abschaltung der Fernkonfiguration finden Sie ebenfalls in LANconfig im Konfigurationsbereich 'Management' auf der Registerkarte 'Security'. Wählen Sie hier unter 'Zugriffsrechte - von entfernten Netzen' für alle Konfigurationsarten die Option 'nicht erlaubt'.

- **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 im Konfigurationsbereich 'Management' auf der Registerkarte 'Admin'. Wählen Sie hier unter 'Zugriffsrechte - Vom Wireless LAN' für alle Konfigurationsarten die Option 'nicht erlaubt'.

- **Haben Sie die SNMP-Konfiguration mit einem Kennwort versehen?**

  Schützen Sie auch die SNMP-Konfiguration mit einem Kennwort. Das Feld zum Schutz der SNMP-Konfiguration mit einem Kennwort finden Sie ebenfalls in LANconfig im Konfigurationsbereich 'Management' auf der Registerkarte 'Security'.

- **Haben Sie die Firewall aktiviert?**

  Die Stateful-Inspection Firewall der LANCOM-Geräte sorgt dafür, dass Ihr lokales Netzwerk von außen nicht angegriffen werden kann. Die Firewall können Sie in LANconfig unter 'Firewall/Qos' auf der Registerkarte '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' auf der Registerkarte 'Regeln' zusammengefasst. Eine Anleitung dazu findet sich im Referenzhandbuch.

- **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-Tabelle finden Sie in LANconfig im Konfigurationsbereich 'IP-Router' auf der Registerkarte 'Routing'.

- **Haben Sie kritische Ports über Filter geschlossen?**

  Die Firewall-Filter des LANCOMs 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 (TCP/UDP/ICMP) gefiltert werden. Besonders komfortabel ist die Einrichtung der Filter mit Hilfe von LANconfig. Unter 'Firewall/QoS' finden Sie die Karteikarte 'Regeln', mit deren Hilfe Filterregeln definiert und verändert werden können.

- **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 Telnet oder 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 werden 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 im Konfigurationsbereich 'TCP/IP' auf der Registerkarte 'Allgemein'.

- **Lagern Sie Ihre abgespeicherte LANCOM-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. Um die IEEE-802.1x-Einstellungen zu kontrollieren oder zu aktivieren, wählen Sie in LANconfig den Konfigurationsbereich '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.

  Durch die Funktion der ISDN-Standort-Verifikation kann das Gerät nur an einem bestimmten ISDN-Anschluß betrieben werden. Nach dem Einschalten prüft das Gerät über einen Selbstanruf zu einer festgelegten Rufnummer, ob es sich noch am „richtigen" ISDN-Anschluß befindet (weitere Informationen finden Sie im Referenzhandbuch).

  Für die GPS-Standort-Verifikation 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 (weitere Informationen finden Sie im Referenzhandbuch).

  Mit der Funktion des „Autarken Weiterbetriebs" wird die Konfiguration für ein WLAN-Interface, das von einem LANCOM 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.

LANCOM Referenzhandbuch Teil 2

- Routing und WAN-Verbindungen
- Firewall
- Quality-of-Service

Stand: LCOS 7.6 mit Addendum 7.7 (siehe Anhang)

(letztes Update August 2009)

LANCOM Systems

© 2009 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®, Windows Vista™, Windows NT® und Microsoft® sind eingetragene Marken von Microsoft, Corp.

Das LANCOM Systems-Logo, LCOS und die Bezeichnung LANCOM sind eingetragene Marken der LANCOM Systems GmbH. Alle übrigen verwendeten Namen und Bezeichnungen können Marken oder eingetragene Marken ihrer jeweiligen Eigentümer sein.

LANCOM Systems behält sich vor, die genannten Daten ohne Ankündigung zu ändern und übernimmt keine Gewähr für technische Ungenauigkeiten und/oder Auslassungen.

Produkte von LANCOM Systems enthalten Software, die vom „OpenSSL Project" für die Verwendung im „OpenSSL Toolkit" entwickelt wurde (http://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.

Produkte von LANCOM Systems enthalten Komponenten, die als Open Source Software im Quelltext verfügbar sind und speziellen Lizenzen sowie den Urheberrechten verschiedener Autoren unterliegen. Im Besonderen enthält die Firmware Komponenten, die der GNU General Public License, Version 2 (GPL) unterliegen. Die Lizenzvereinbarung mit dem Text der GPL ist auf der LANCOM CD im Produktverzeichnis zu finden. Auf Anfrage können die Quelltexte und alle Lizenzhinweise elektronisch vom FTP-Server der LANCOM Systems GmbH bezogen werden.

LANCOM Systems GmbH

Adenauerstr. 20/B2

52146 Würselen

Deutschland

www.lancom.de

Würselen, August 2009

110651/0809

Inhalt

7 Routing und WAN-Verbindungen 7 -1

7.1 Allgemeines über WAN-Verbindungen 7 - 1
7.1.1 Brücken für Standard-Protokolle 7 - 1
7.1.2 Was passiert bei einer Anfrage aus dem LAN? 7 - 1

7.2 IP-Routing 7 - 2
7.2.1 Die IP-Routing-Tabelle 7 - 2
7.2.2 Policy-based Routing 7 - 3
7.2.3 Lokales Routing 7 - 5
7.2.4 Dynamisches Routing mit IP-RIP 7 - 6
7.2.5 SYN/ACK-Speedup 7 - 9

7.3 Advanced Routing and Forwarding 7 - 9
7.3.1 Einleitung 7 - 9
7.3.2 Definition von Netzwerken und Zuordnung von Interfaces 7 - 12
7.3.3 Zuweisung von logischen Interfaces zu Bridge-Gruppen 7 - 12
7.3.4 Schnittstellen-Tags für Gegenstellen 7 - 13
7.3.5 Virtuelle Router 7 - 14
7.3.6 NetBIOS-Proxy 7 - 15

7.4 Die Konfiguration von Gegenstellen 7 - 15
7.4.1 Gegenstellenliste 7 - 15
7.4.2 Layer-Liste 7 - 16

7.5 IP-Masquerading 7 - 17
7.5.1 Einfaches Masquerading 7 - 18
7.5.2 Inverses Masquerading 7 - 19

7.6 Demilitarisierte Zone (DMZ) 7 - 20
7.6.1 Zuordnung von Interfaces zur DMZ 7 - 21
7.6.2 Zuordnung der Netzwerkzonen zur DMZ 7 - 21
7.6.3 Adressprüfung bei DMZ- und Intranet-Interfaces 7 - 21
7.6.4 Unmaskierter Internet-Zugang für Server in der DMZ 7 - 22

7.7 Multi-PPPoE 7 - 23
7.7.1 Anwendungsbeispiel: Home-Office mit privatem Internetzugang 7 - 23
7.7.2 Konfiguration 7 - 23

7.8 Load-Balancing 7 - 24
7.8.1 DSL-Port-Mapping 7 - 25
7.8.2 DSL-Kanalbündelung (MLPPPoE) 7 - 27
7.8.3 Dynamisches Load-Balancing 7 - 27
7.8.4 Statisches Load-Balancing 7 - 28
7.8.5 Indirekte Bündelung für LAN-LAN-Kopplungen über PPTP 7 - 28
7.8.6 Konfiguration des Load Balancing 7 - 28

7.9 N:N-Mapping 7 - 31
7.9.1 Anwendungsbeispiele 7 - 31
7.9.2 Konfiguration 7 - 33

7.10 Verbindungsaufbau mit PPP 7 - 35
7.10.1 Das Protokoll 7 - 35
7.10.2 Alles o.k.? Leitungsüberprüfung mit LCP 7 - 37
7.10.3 Zuweisung von IP-Adressen über PPP 7 - 37
7.10.4 Einstellungen in der PPP-Liste 7 - 38
7.10.5 Die Bedeutung der DEFAULT-Gegenstelle 7 - 39
7.10.6 RADIUS-Authentifizierung von PPP-Verbindungen 7 - 39

7.11 DSL-Verbindungsaufbau mit PPTP 7 - 39

7.12 Dauerverbindung für Flatrates – Keep-alive 7 - 40

7.13 Rückruf-Funktionen 7 - 40
7.13.1 Rückruf nach Microsoft CBCP 7 - 40
7.13.2 Schneller Rückruf mit dem LANCOM-Verfahren 7 - 41
7.13.3 Rückruf nach RFC 1570 (PPP LCP Extensions) 7 - 41
7.13.4 Konfiguration der Rückruf-Funktion im Überblick 7 - 42

7.14 ISDN-Kanalbündelung mit MLPPP 7 - 42

7.15 Betrieb eines Modems an der seriellen Schnittstelle 7 - 43
7.15.1 Einleitung 7 - 43
7.15.2 Systemvoraussetzungen 7 - 44
7.15.3 Installation 7 - 44
7.15.4 Einstellen der seriellen Schnittstelle auf Modem-Betrieb 7 - 44
7.15.5 Konfiguration der Modem-Parameter 7 - 45
7.15.6 Direkte Eingabe von AT-Befehlen 7 - 46
7.15.7 Statistik 7 - 46
7.15.8 Trace-Ausgaben 7 - 47
7.15.9 Konfiguration von Gegenstellen für V.24-WAN-Schnittstellen 7 - 47
7.15.10 Konfiguration einer Backup-Verbindung auf der seriellen Schnittstelle 7 - 48
7.15.11 Kontaktbelegung des LANCOM Modem Adapter Kits 7 - 48

7.16 Manuelle Definition der MTU 7 - 48
7.16.1 Konfiguration 7 - 48
7.16.2 Statistik 7 - 49

7.17 WAN-RIP 7 - 49

7.18 Das Rapid-Spanning-Tree-Protokoll 7 - 50
7.18.1 Classic und Rapid Spanning Tree 7 - 50
7.18.2 Verbesserungen durch Rapid Spanning Tree 7 - 50
7.18.3 Konfiguration des Spanning-Tree-Protokolls 7 - 51
7.18.4 Statusmeldungen über das Spanning-Tree-Protokoll 7 - 52

7.19 Die Aktions-Tabelle 7 - 54
7.19.1 Einleitung 7 - 54
7.19.2 Aktionen für Dynamic DNS 7 - 54
7.19.3 Weitere Beispiele für Aktionen 7 - 57
7.19.4 Konfiguration 7 - 58

7.20 Verwendung der seriellen Schnittstelle im LAN 7 - 60
7.20.1 Einleitung 7 - 60
7.20.2 Betriebsarten 7 - 60
7.20.3 Konfiguration der seriellen Schnittstellen 7 - 60
7.20.4 Konfiguration des COM-Port-Servers 7 - 61
7.20.5 Konfiguration der WAN-Geräte 7 - 64
7.20.6 Status-Informationen über die seriellen Verbindungen 7 - 64
7.20.7 COM-Port-Adapter 7 - 67

8 Firewall 8 - 1

8.1 Gefährdungsanalyse 8 - 1
8.1.1 Die Gefahren 8 - 1
8.1.2 Die Wege der Täter 8 - 1
8.1.3 Die Methoden 8 - 1
8.1.4 Die Opfer 8 - 2

8.2 Was ist eine Firewall? 8 - 2
8.2.1 Die Aufgaben einer Firewall 8 - 3
8.2.2 Unterschiedliche Typen von Firewalls 8 - 3

8.3 Die Firewall im LANCOM 8 - 6
8.3.1 So prüft die Firewall im LANCOM die Datenpakete 8 - 6
8.3.2 Besondere Protokolle 8 - 8
8.3.3 Allgemeine Einstellungen der Firewall 8 - 10
8.3.4 Die Parameter der Firewall-Regeln 8 - 12
8.3.5 Die Alarmierungsfunktionen der Firewall 8 - 16
8.3.6 Strategien für die Einstellung der Firewall 8 - 18
8.3.7 Tipps zur Einstellung der Firewall 8 - 20

8.4 Konfiguration der Firewall mit LANconfig 8 - 22
8.4.1 Firewall-Assistent 8 - 22
8.4.2 Definition der Firewall-Objekte 8 - 22
8.4.3 Definition der Firewall-Regeln 8 - 24

8.5 Konfiguration der Firewall-Regeln mit WEBconfig oder Telnet 8 - 26
8.5.1 Regel-Tabelle 8 - 26
8.5.2 Objekttabelle 8 - 27
8.5.3 Aktionstabelle 8 - 27

8.6 Firewall-Diagnose 8 - 27

8.7 Grenzen der Firewall 8 - 32

8.8 Abwehr von Einbruchsversuchen: Intrusion Detection 8 - 32
8.8.1 Beispiele für Einbruchsversuche 8 - 32
8.8.2 Konfiguration des IDS 8 - 33

8.9 Schutz vor "Denial-of-Service"-Angriffen 8 - 33
8.9.1 Beispiele für Denial-of-Service-Angriffe 8 - 33
8.9.2 Konfiguration der DoS-Abwehr 8 - 35
8.9.3 Konfiguration von ping-Blocking und Stealth-Modus 8 - 36

9 Quality-of-Service 9 - 1

9.1 Wozu QoS? 9 - 1

9.2 Welche Datenpakete bevorzugen? 9 - 1
9.2.1 Was ist DiffServ? 9 - 2
9.2.2 Garantierte Mindestbandbreiten 9 - 2
9.2.3 Limitierte Maximalbandbreiten 9 - 3

9.3 Das Warteschlangenkonzept 9 - 3
9.3.1 Sendeseitige Warteschlangen 9 - 3
9.3.2 Empfangsseitige Warteschlangen 9 - 4

9.4 Reduzierung der Paketlänge 9 - 5

9.5 QoS-Parameter für Voice-over-IP-Anwendungen 9 - 6

9.6 QoS in Sende- oder Empfangsrichtung 9 - 9

9.7 QoS-Konfiguration 9 - 10
9.7.1 ToS- und DiffServ-Felder auswerten 9 - 10
9.7.2 Minimal- und Maximalbandbreiten definieren 9 - 11
9.7.3 Übertragungsraten für Interfaces festlegen 9 - 12
9.7.4 Sende- und Empfangsrichtung 9 - 13
9.7.5 Reduzierung der Paketlänge 9 - 13

9.8 QoS für WLANs nach IEEE 802.11e (WMM/WME) 9 - 14

7 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.

7.1 Allgemeines über WAN-Verbindungen

WAN-Verbindungen werden für folgende Anwendungen verwendet.

- Internet-Zugang
- LAN-LAN-Kopplung
- Remote Access

7.1.1 Brücken für Standard-Protokolle

WAN-Verbindungen unterscheiden sich von direkten Verbindungen (beispielsweise über die LANCAPI) 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).

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. Geräte mit ISDN-Schnittstelle unterstützen auf der ISDN-Schnittstelle neben IP auch IPX.

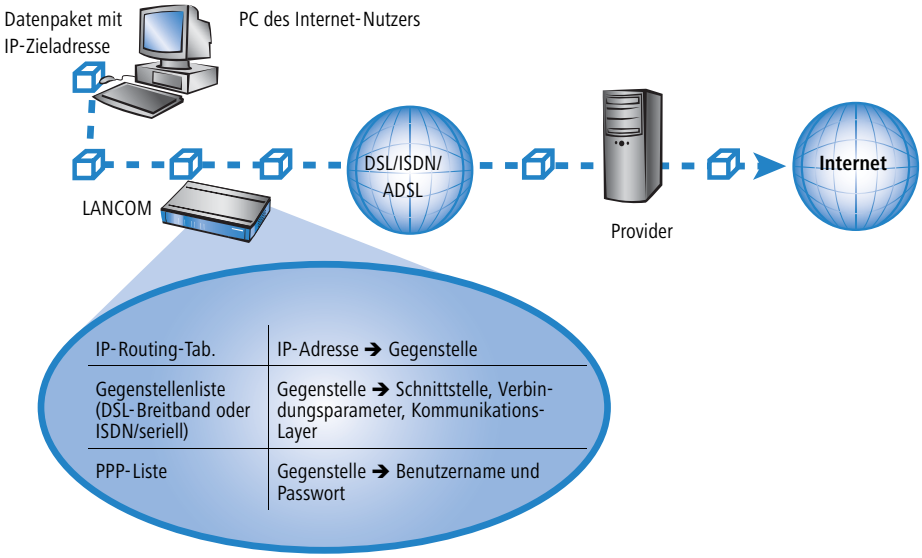
Die enge Zusammenarbeit mit den Router-Modulen

Charakteristisch für WAN-Verbindungen ist die enge Zusammenarbeit mit den Router-Modulen im LANCOM. Die Router-Module (IP und IPX) 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.

7.1.2 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 Empfän-

gers. 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, ISDN) über die der Provider angewählt wird, Protokollinformationen oder die für eine ISDN-Wählverbindung notwendige Rufnummer. 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.

7.2 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 Systems aufgebaut ist und mit welchen weiteren Funktionen das IP-Routing unterstützt wird.

7.2.1 Die IP-Routing-Tabelle

In der IP-Routing-Tabelle sagen Sie dem Router, an welche Gegenstelle (also welchen anderen Router oder Rechner) er die Daten für bestimmte IP-Adressen oder IP-Adress-Bereiche schicken soll. So ein Eintrag heißt auch „Route", weil der Weg der Datenpakete damit 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. Bei aktiviertem IP-RIP beachtet der IP-Router die statische und die dynamische Routing-Tabelle.

Außerdem sagen Sie dem Router in der IP-Routing-Tabelle, wie weit der Weg über diese Route ist, damit im Zusammenspiel mit IP-RIP bei mehreren Routen zum gleichen Ziel der günstigste ausgewählt werden kann. Die Grundeinstellung für die 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 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.

Konfiguration der Routing-Tabelle

LANconfig: IP-Router ▶ Routing ▶ Routing-Tabelle

WEBconfig: LCOS-Menübaum ▶ Setup ▶ IP-Router ▶ IP-Routing-Tabelle

Eine IP-Routing-Tabelle kann beispielsweise so aussehen:

IP-Adresse	Netzmaske	Routing-Tag	Router	Distanz	Maskierung	Aktiv
192.168.120.0	255.255.255.0	0	MAIN	2	Aus	Ja
192.168.125.0	255.255.255.0	0	NODE1	3	Aus	Ja
192.168.130.0	255.255.255.0	0	191.168.140.123	0	Aus	Ja

Was bedeuten die einzelnen Einträge in der Liste?

▶ IP-Adresse und 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. 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 ('Policy-based Routing' → Seite 7-3). Mit dem Routing-Tag „0" gilt der Routing-Eintrag für alle Pakete.

- Router

  An diese Gegenstelle 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.

  Der Name der Gegenstellen gibt an, was mit den zur IP-Adresse und Netzmaske passenden Datenpaketen geschehen soll.

  - Routen mit dem Eintrag '0.0.0.0' bezeichnen Ausschluss-Routen. Datenpakete für diese „Null-Routen" werden verworfen und nicht weitergeleitet. Damit werden z.B. die im Internet verbotenen Routen (private Adressräume, z.B. '10.0.0.0') 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.

- 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 16 (= unreachable) propagiert.
  - Eine Ausnahme bilden die Gegenstellen, die über Proxy-ARP angeschlossen sind. Diese „Proxy-Hosts" werden gar nicht propagiert.

- Maskierung

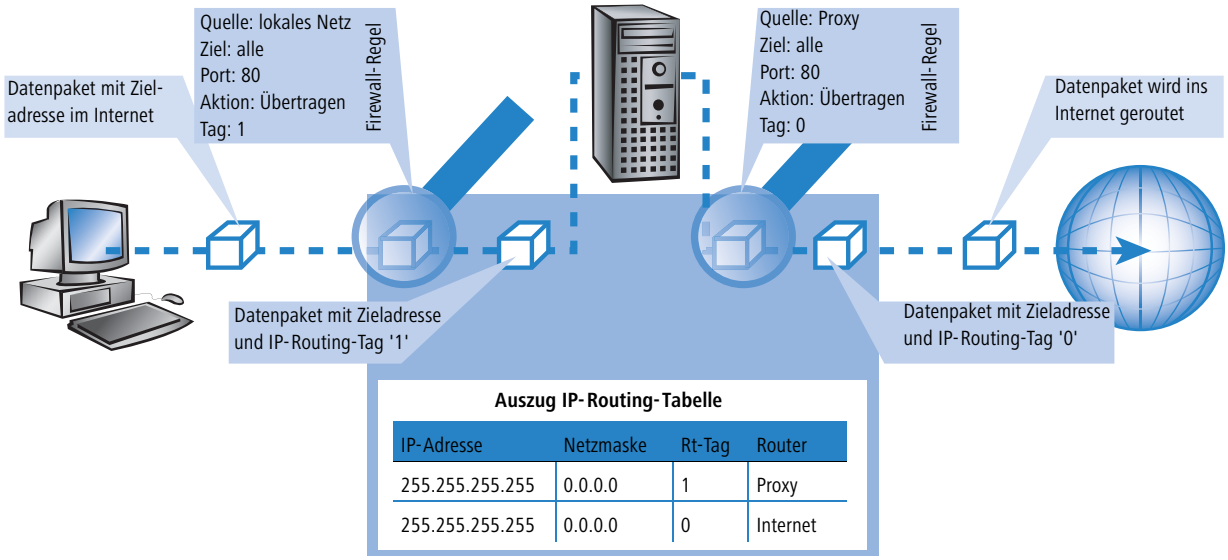
  Mit der Option 'Maskierung' in der Routing-Tabelle informieren Sie den Router darüber, welche IP-Adresse er bei der Weitergabe der Pakete verwenden soll.

  Weitere Informationen finden Sie im Abschnitt 'IP-Masquerading' → Seite 7-17.

7.2.2 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.



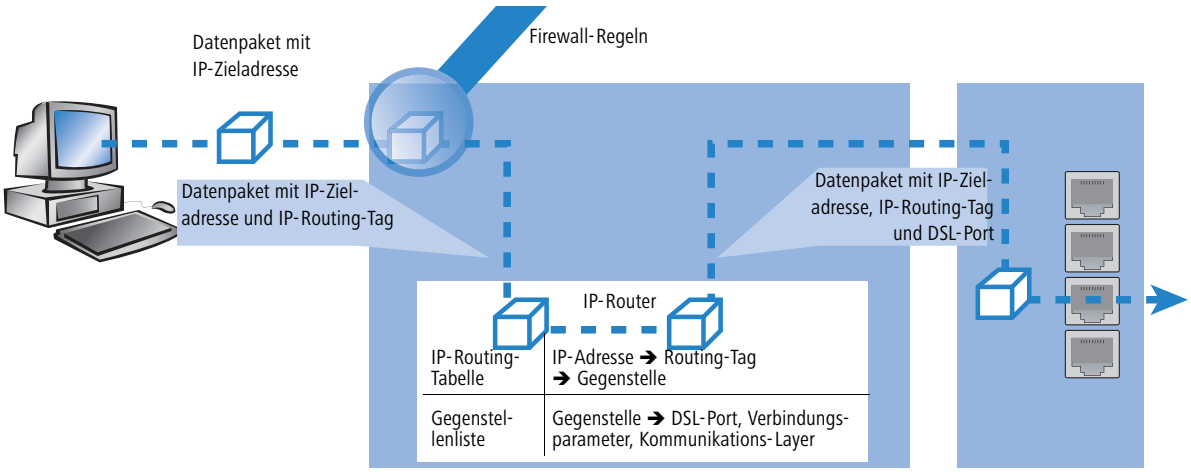
Auszug IP-Routing-Tabelle

IP-Adresse	Netzmaske	Rt-Tag	Router
255.255.255.255	0.0.0.0	1	Proxy
255.255.255.255	0.0.0.0	0	Internet

- 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 LANCOM 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.

Routing-Tags für VPN- und PPTP-Verbindungen

Routing-Tags werden im LANCOM 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	

7.2.3 Lokales Routing

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.

Wie helfen Sie dem Arbeitsplatzrechner nun weiter?

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 werden dann keine ICMP-Redirects mehr geschickt. Die Einstellung erfolgt unter:

LANconfig: IP-Router ▶ Allgemein ▶ Pakete im lokalen Netz weiterleiten

WEBconfig: LCOS-Menübaum ▶ Setup ▶ IP-Router ▶ Lok.-Routing

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.

7.2.4 Dynamisches Routing mit IP-RIP

Neben der statischen Routing-Tabelle verfügen Router von LANCOM Systems 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.

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". Dass ein Router neben der bestehenden Verbindung keine weitere aufbauen kann, liegt an einer der folgenden Ursachen:
  - □ Auf allen anderen Kanälen ist schon eine andere Verbindung hergestellt (auch über LANCAPI).
  - □ Die Y-Verbindungen für den S_0-Anschluss sind in der Interface-Tabelle ausdrücklich ausgeschlossen.
  - □ Die bestehende Verbindung benutzt alle B-Kanäle (Kanalbündelung).
  - □ Bei der bestehenden Verbindung handelt es sich um eine Festverbindung. Nur wenige ISDN-Anbieter ermöglichen es, neben einer Festverbindung auf dem ersten B-Kanal eine Wählverbindung auf dem zweiten B-Kanal aufzubauen.

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

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!

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.

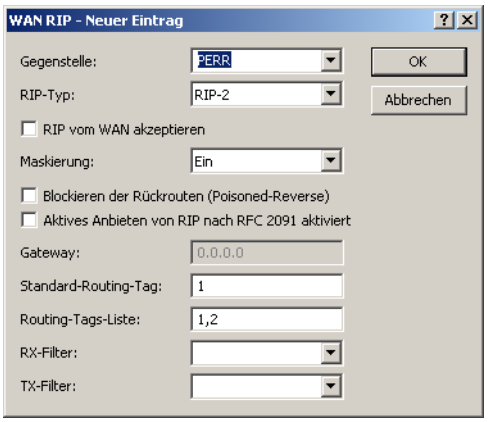
Skalierung durch IP-RIP

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.

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: IP-Router ▶ Allgemein ▶ WAN RIP



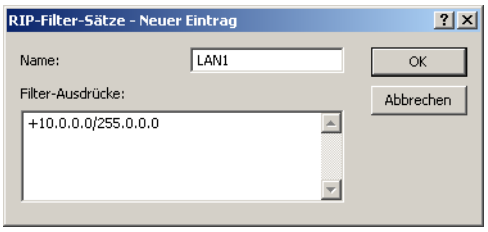
WEBconfig: Setup ▶ IP-Router ▶ RIP ▶ WAN-Tabelle

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.

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: IP-Router ▶ Allgemein ▶ RIP-Filter-Sätze

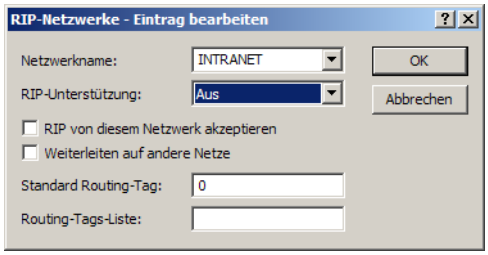


Telnet: Setup ▶ IP-Router ▶ RIP ▶ Filter

RIP für Netzwerke getrennt einstellen

Ebenso wie beim NetBIOS-Proxy ist es meistens 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: IP-Router ▶ Allgemein ▶ RIP-Netzwerke



WEBconfig: LCOS-Menübaum ▶ Setup ▶ IP-Router ▶ RIP ▶ LAN-Tabelle

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.

■ WEBconfig: **Setup ▶ IP-Router ▶ RIP ▶ Parameter**

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.

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.

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.

Statische Routen, die immer propagiert werden

Neben den dynamischen Routen propagiert ein Router über RIP auch die statisch konfigurierten Routen. Dabei sind mache 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.

WEBconfig: **Setup ▶ IP-Router ▶ IP-Routing-Tabelle**

7.2.5 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.

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

WEBconfig: LCOS-Menübaum ▶ Setup ▶ IP-Router ▶ Routing-Methode ▶ SYN/ACK-Speedup

7.3 Advanced Routing and Forwarding

7.3.1 Einleitung

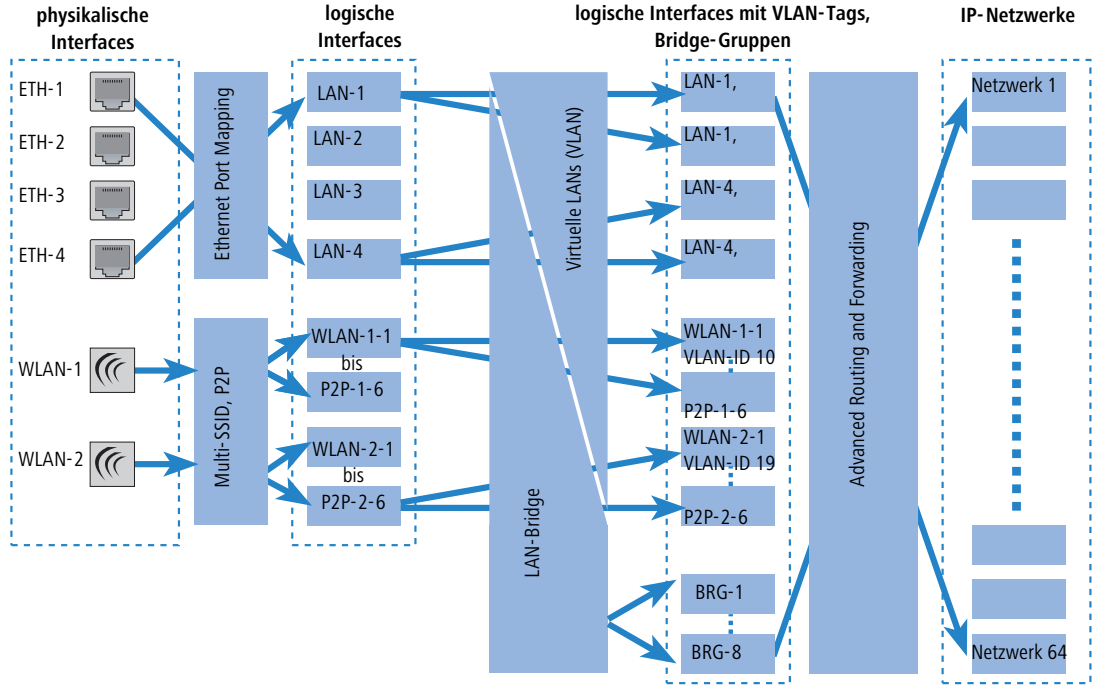
Bis zur LCOS-Version 6.30 unterstützten die LANCOM Router lediglich zwei lokale Netzwerke: das Intranet und die DMZ. In manchen Anwendungsfällen ist es jedoch wünschenwert, mehr als ein Intranet und eine DMZ mit einem LANCOM Router zu realisieren, um auf diese Weise z.B. mehreren IP-Netzen über einen zentralen Router den Zugang zum Internet zu ermöglichen. Ab der LCOS-Version 7.00 unterstützen die LANCOM Router 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 das durch das Ethernet Port Mapping, dabei werden den physikalischen ETH-1 bis z.B. ETH-4 die logischen LAN-1 bis LAN-4 zugeordnet.

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 acht WLAN-Netze und bis zu sechs 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 LANCOM Router stellen sich die VLANs also als separate Interfaces dar, aus einem einzelnen logischen Interface werden also für den LANCOM Router 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 den LANCOM Router 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 LANCOM Router betrieben werden können.

Ein Beispiel: In einem Bürogebäude sollen mehrere Firmen über einen zentralen LANCOM Router 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.

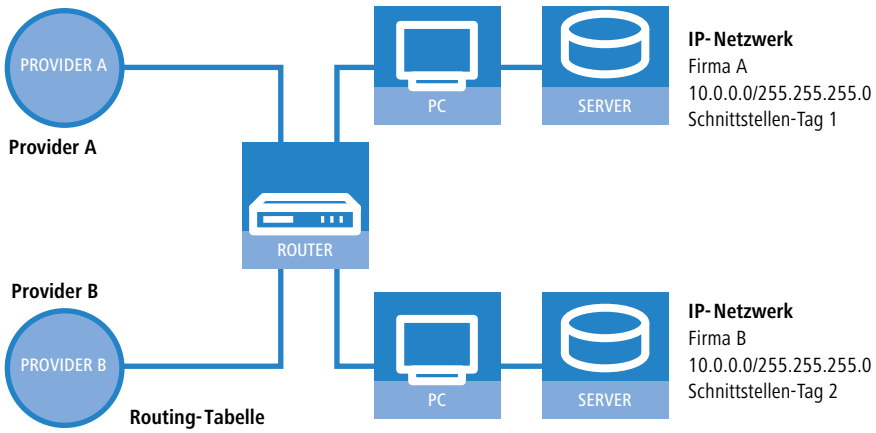
Unterschiede zwischen Routing-Tags und Schnittstellen-Tags

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

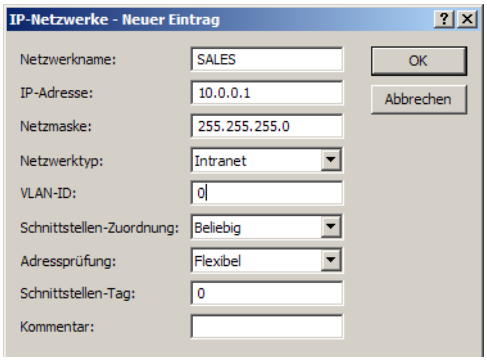
In Fällen, die keine eindeutige Zuordnung der IP-Adressen über die Schnittstellen-Tags erlauben, wird das Advanced Routing and Forwarding durch entsprechende Firewall-Regeln unterstützt. Das ist im vorgenannten Beispiel der Fall, wenn in jedem Netzwerk ein öffentlich erreichbarer Web- oder Mailserver steht, die ebenfalls die gleiche IP-Adresse verwenden.

7.3.2 Definition von Netzwerken und Zuordnung von Interfaces

Bei der Definition eines Netzwerks wird zunächst festgelegt, welcher IP-Adress-Kreis auf einem bestimmten lokalen Interface des LANCOM Router 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 (über Bridge-Gruppen oder mit der Schnittstellenzuordnung 'beliebig').

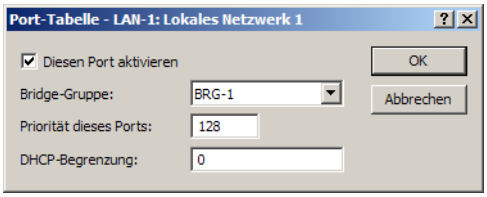
Die Netzwerke werden in einer Tabelle definiert. Neben der Definition des Adresskreises und der Interfacezuordnung wird darin auch ein eindeutiger Name für die Netzwerke festgelegt. Dieser Netzwerkname erlaubt es, die Netze in anderen Modulen (DHCP-Server, RIP, NetBIOS etc.) zu identifizieren und diese Dienste nur in bestimmten Netzen anbieten zu können.

TCP/IP ▶ Allgemein ▶ IP-Netzwerke



7.3.3 Zuweisung von logischen Interfaces zu Bridge-Gruppen

In der Port-Tabelle werden spezielle Eigenschaften der logischen Interfaces definiert.



LANconfig: Schnittstellen ▶ Spanning Tree

WEBconfig: LCOS-Menübaum ▶ Setup ▶ LAN-Bridge ▶ Port-Daten

- **Aktiv**

  Mit dieser Option wird das logische Interface aktiviert bzw. deaktiviert.

- **Bridge-Gruppe**

  Ordnet das logische Interface einer Bridge-Gruppe zu und ermöglicht so das Bridging von/zu dieser 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 LANCOM 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.

- **Priorität**

  Legt die Priorität für das logische Interface bei Verwendung des Spanning-Tree-Protokolls fest. Bei mehreren möglichen Verbindungswegen wird das Interface mit der höchsten Priorität verwendet. Kleinere Werte stehen für eine höhere Priorität. Bei gleicher Priorität wird das Interface mit den geringeren Übertragungskosten gewählt, alternativ das führende Interface in der Tabelle.

■ **DHCP-Limit**

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.

7.3.4 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:

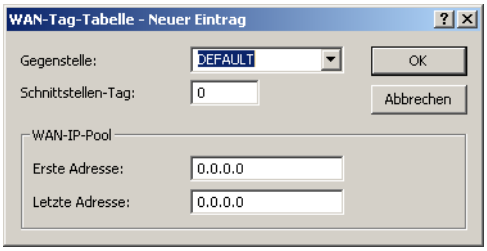
- mit Hilfe von entsprechenden Firewall-Regeln, die nur Datenpakete von bestimmten Gegenstellen, IP-Adressen oder Ports erfassen
- anhand der Routing-Tabelle
- über eine explizite Zuordnung der Tags zu den Gegenstellen.

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 bstimmt werden. Ein- und ausgehende Kommunikation kann somit einfacher bidirektional in virtuelle Router unterteilt werden.

Sowohl die über die Tag-Tabelle, als auch die anhand der Routing-Tabelle ermittelten Schnittstellen-Tags können durch einen passenden Eintrag in der Firewall überschrieben werden.

Zuweisung von Schnittstellen-Tags über die Tag-Tabelle

LANconfig: Kommukination ▶ Gegenstellen ▶ WAN-Tag-Tabelle



WEBconfig: Setup ▶ IP-Router

■ **WAN-Tag-Erzeugung**

Mit der WAN-Tag-Erzeugung wird die Quelle für die Zuordnung von Schnittstellen-Tags definiert. Neben der Zuordnung über die Firewall oder direkte Zuordnung über die Tag-Tabelle kann das Schnittstellen-Tag auch anhand Quellroute in der effektiven Routing-Tabelle gewählt werden (statische Routing-Einträge plus Routen, die über RIP gelernt wurden). Die Quell-IP und der Name der Gegenstelle, über welche die IP-Verbindung aufgebaut wurde, wird mit der Routing Information verglichen. Das Routing-Tag dieser Quellroute wird den WAN-seitig empfangenen Paketen dieser Verbindung für die weitere Verarbeitung zugewiesen. Enthält die effektive Routing-Tabelle mehrere Einträge für eine Gegenstelle mit gleichem Netzwerk, so wird das kleinste Tag verwendet.

Beispiel: Es sind folgende ARF-Netze definiert:

Netzwerk	IP-Adresse	Rtg-tag	Port
PRIVAT	192.168.1.1/24	1	LAN-1
HOMEOFFICE	192.168.10.1/24	10	LAN-2

PRIVAT soll nur das Internet nutzen, HOMEOFFICE nur einen VPN Tunnel zur Gegenstelle VPN-FIRMA. Die entsprechende effektive Routing-Tabelle sieht so aus:

IP-Adresse	IP-Netmaske	Rtg-tag	Gegenstelle	Distanz	Maskierung
192.168.10.0	255.255.255.0	10	VPN-FIRMA	0	No
255.255.255.255	0.0.0.0	1	INTERNET	0	No

□ Datenpaket kommt aus dem Netz 192.168.10.x: Tag = 10

- □ Datenpaket kommt aus dem Netz 192.168.1.x: Tag = 1
- □ Datenpaket kommt aus einem beliebigen anderen Netz: Tag = 0

Mögliche Werte:

- □ Manual: In dieser Einstellung werden die Schnittstellen-Tags ausschließlich über einen Eintrag in der Tag-Tabelle bestimmt. Die Routing-Tabelle hat keine Bedeutung für die Zuordnung der Schnittstellen-Tags.
- □ Auto: In dieser Einstellung werden die Schnittstellen-Tags zunächst über einen Eintrag in der Tag-Tabelle bestimmt. Wird dort kein passender Eintrag gefunden, so wird das Tag anhand der Routing-Tabelle ermittelt .

Sowohl die über die Tag-Tabelle, als auch die anhand der Routing-Tabelle ermittelten Schnittstellen-Tags können durch einen passenden Eintrag in der Firewall überschrieben werden.

7.3.5 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

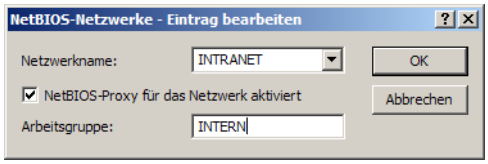
Dann lassen sich durch die Routing-Tags folgende Firewall-Regeln festlegen:

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.

7.3.6 NetBIOS-Proxy

Aus Sicherheitsgründen muss der NetBIOS-Proxy in seinem Verhalten den jeweiligen Netzwerken angepasst werden, da er z.B. üblicherweise nicht in der DMZ aktiv sein soll. Der NetBIOS-Proxy kann daher für jedes Netzwerk getrennt eingestellt werden



LANconfig: NetBIOS ▶ Allgemein ▶ NetBIOS-Netzwerke

WEBconfig: LCOS-Menübaum ▶ Setup ▶ NetBIOS ▶ Netzwerke

- **Netzwerkname**

  Name des Netzwerks, für das der NetBIOS-Proxy aktiviert werden soll.

- **NetBIOS-Proxy für das Netzwerk aktiviert**

  Diese Option gibt an, ob der NetBIOS-Proxy für das ausgewählte Netzwerk aktiviert wird oder nicht.

- **Arbeitsgruppe**

  Die Arbeitsgruppe oder Domäne, die von den Clients im Netzwerk verwendet wird. Bei mehreren Arbeitsgruppen reicht die Angabe einer Arbeitsgruppe.

In der Default-Einstellung sind sowohl 'Intranet' als auch 'DMZ' in dieser Tabelle eingetragen, dabei ist der NetBIOS-Proxy für das Intranet aktiviert und für die DMZ deaktiviert.

Sobald ein Netzwerk über ein Schnittstellen-Tag verfügt, sind von diesem Netz aus nur Namen (Hosts und Gruppen) sichtbar, die in einem Netz mit dem gleichen Tag stehen, bzw. über eine passende (mit dem selben Tag) getaggte WAN-Route erreichbar sind. Ein ungetaggtes Netz hingegen sieht alle Namen. Genauso sind alle Namen, die aus ungetaggten Netzen gelernt wurden, für alle Netze sichtbar.

Der DNS-Server berücksichtigt bei der Namensauflösung die Interface-Tags, d.h. es werden auch über DNS nur Namen aufgelöst, die aus einem Netz mit dem gleichen Tag gelernt wurden. Auch hier gilt die Sonderrolle ungetaggter Netze.

Die Arbeitsgruppe/Domäne dient dazu, beim Start des Gerätes das Netzwerk nach NetBIOS-Namen abscannen zu können. Diese ist i.A. für jedes Netz verschieden und muss daher überall angegeben werden. In Netzwerken ohne Domäne sollte hier der Name der größten Arbeitsgruppe angegeben werden.

7.4 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 bzw. IPX) 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' → Seite 7-35.

7.4.1 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 können auf folgenden Wegen aufgerufen werden:

LANconfig: Kommunikation ▶ Gegenstellen ▶ Gegenstellen (DSL)

WEBconfig: LCOS-Menübaum ▶ Setup ▶ WAN ▶ DSL-Breitband-Gegenstellen bzw. Einwahl-Gegenstellen

Für eine Gegenstelle sind folgende Parameter erforderlich:

Gegenstellen-liste	Parameter	Bedeutung
DSL-Breitband-Gegenstellen	Name	Mit diesem Namen wird die Gegenstelle in den Routermodulen identifiziert. Sobald das Routermodul 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' → Seite 7-40).
	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 AC anbietet.
	Layername	Wählen Sie den Kommunikations-Layer aus, der für diese Verbindung verwendet werden soll. Die Konfiguration dieser Layer ist im folgenden Abschnitt beschrieben.
	VPI	Virtual Path Identifier.
	VCI	Virtual Channel Identifier. Die Werte für VCI und VPI werden vom ADSL-Netzbetreiber mitgeteilt. Übliche Werte für die Kombination von VPI und VCI sind: 0/35, 0/38, 1/32, 8/35, 8/48.
Einwahl-Gegenstellen	Name	Wie in der Liste der DSL-Breitband-Gegenstellen.
	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	Wie in der Liste der DSL-Breitband-Gegenstellen.
	Haltezeit für Bündelung	Der zweite B-Kanal in einer Bündelung wird abgebaut, wenn er für die eingestellte Dauer nicht benutzt wurde.
	Layername	Wie in der Liste der DSL-Breitband-Gegenstellen.
	Automatischer Rückruf	Der automatische Rückruf ermöglicht eine sichere Verbindung und senkt die Kosten für den Anrufer. Nähere Informationen finden Sie im Abschnitt 'Rückruf-Funktionen' → Seite 7-40.

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 LANCOM 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 AC 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.

7.4.2 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

WEBconfig: LCOS-Menübaum ▶ Setup ▶ WAN ▶ Layer-Liste

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 LANCOM vorhandenen Parameter vom Funktionsumfang des Gerätes abhängen. Es kann daher sein, dass Ihr Gerät nicht alle hier beschriebenen Optionen anbietet.

Parameter	Bedeutung	
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-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.
	'AsyncPPP'	Wie 'PPP', nur wird der asynchrone Modus verwendet. PPP arbeitet also zeichenorientiert.
	'... mit Script'	Alle Optionen können wahlweise mit eigenem Script ausgeführt werden. Das Script wird in der Script-Liste angegeben.
	'DHCP'	Zuordnung der Netzwerkparameter über 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.
	'X.75LAPB'	Verbindungsaufbau nach X.75 und LAPM (Link Access Procedure Balanced).
	'PPPoE'	Kapselung der PPP-Protokollinformationen in Ethernet-Frames.
Optionen	Hier können Sie die Kompression der übertragenen Daten und die Bündelung von Kanälen aktivieren. Die gewählte Option wird nur dann wirksam, wenn sie sowohl von den verwendeten Schnittstellen als auch von den gewählten Layer-2- und Layer-3-Protokollen unterstützt wird. Weitere Informationen finden Sie im Abschnitt 'ISDN-Kanalbündelung mit MLPPP' → Seite 7-42.	
Layer-1	In diesem Feld wird der untere Teil der Sicherungsschicht (Data Link Layer) konfiguriert. Folgende Optionen stehen zur Verfügung:	
	'AAL-5'	ATM-Anpassungsschicht
	'ETH-10'	Transparentes Ethernet nach IEEE 802.3.
	'HDLC'	Sicherung und Synchronisation der Datenübertragung nach HDLC (im 7- oder 8-bit-Modus).
	'V.110'	Übertragung nach V.110 mit maximal 38.400 bit/Sekunde, z.B. für Einwahl per HSCSD-Mobiltelefon
	Modem	Modem-Übertragung (benötigt Fax-Modem-Option)

7.5 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 sein 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:

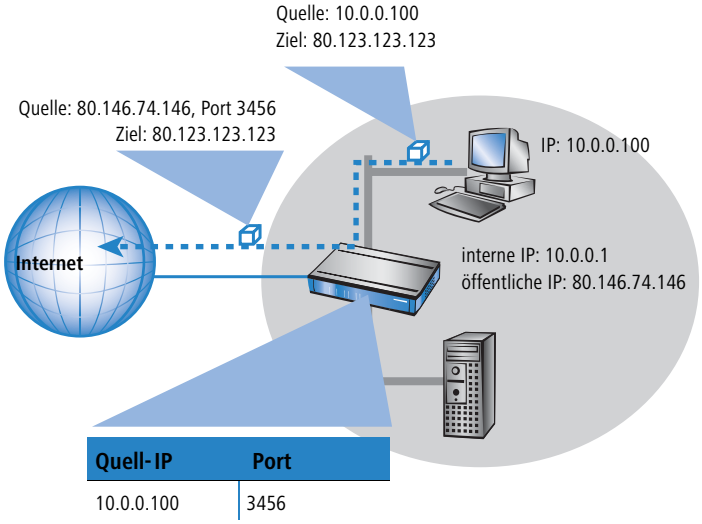
- die Intranet IP-Adresse zur Kommunikation mit den Rechnern im LAN
- die öffentliche IP-Adresse zur Kommunikation mit den Gegenstellen im Internet

Die Rechner im LAN nutzen den Router dann als Gateway und können selbst nicht erkannt werden. Der Router trennt Internet und Intranet.

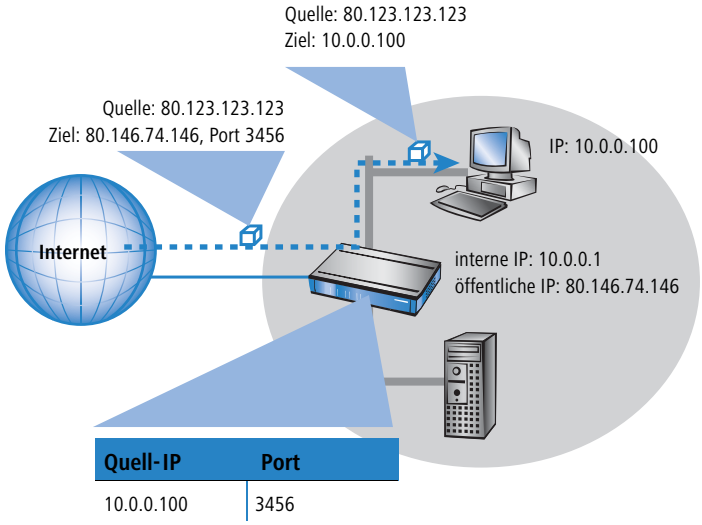
7.5.1 Einfaches Masquerading

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.



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 LANCOM unterstützten Protokollen mit Sonderbehandlung gehören:

- FTP (über die Standardports)
- H.323 (im Umfang, wie ihn Microsoft Netmeeting verwendet)
- PPTP
- IPSec
- IRC

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:

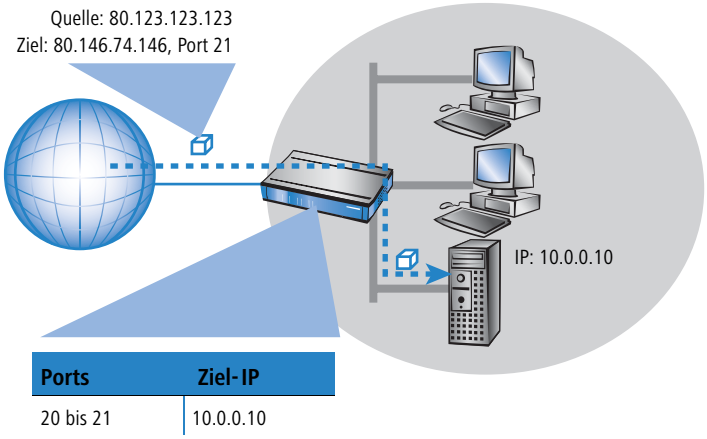
LANconfig: IP-Router ▶ Routing ▶ Routing-Tabelle

WEBconfig: LCOS-Menübaum ▶ Setup ▶ IP-Router ▶ IP-Routing-Tab

7.5.2 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 derPort-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.

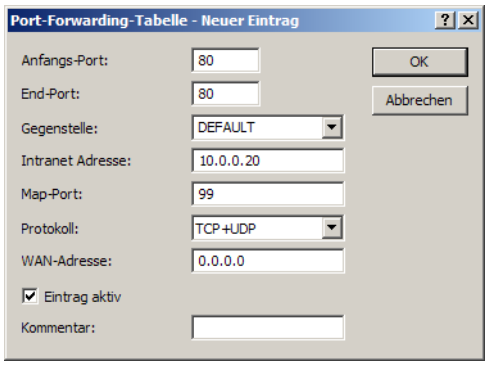
Die entsprechende Tabelle kann max. 2048 Einträge aufnehmen, also gleichzeitig 2048 Übertragungen zwischen dem maskierten und dem unmaskierten Netz ermöglichen.

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

WEBconfig: LCOS-Menübaum ▶ 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' → Seite 7-9) 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).

7.6 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.

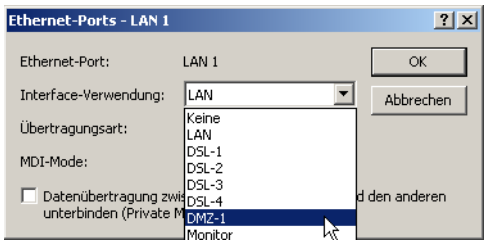
Um diesen Aufbau zu ermöglichen, muss der Datenverkehr zwischen den drei Zonen Internet, DMZ und LAN von einer Firewall geprüft werden. Diese Aufgaben der Firewall können durchaus in einem Gerät (Router) zusammengefasst werden. Dazu braucht der Router drei Interfaces, die getrennt voneinander durch die Firewall überwacht werden können:

- LAN-Interface
- WAN-Interface
- DMZ-Interface

In der Tabelle 'Übersicht über die Funktionen nach Modellen und LCOS*-Versionen' → Seite 16-14 ist aufgelistet, welche Geräte diese Funktion unterstützen.

7.6.1 Zuordnung von Interfaces zur DMZ

Zur Konfiguration der DMZ wird das entsprechende Interface als DMZ-Interface definiert.

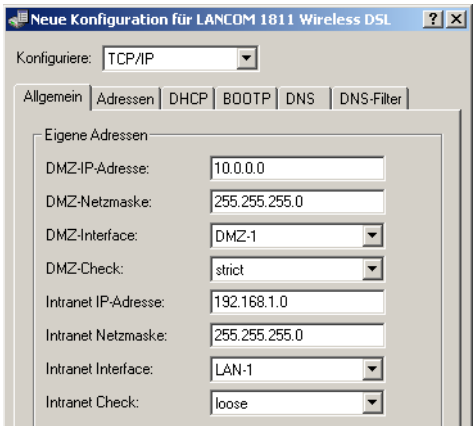


LANconfig: Interfaces ▶ LAN ▶ Ethernet-Ports

WEBconfig: LCOS-Menübaum ▶ Setup ▶ Interfaces ▶ LAN

7.6.2 Zuordnung der Netzwerkzonen zur DMZ

Die Zuordnung der verschiedenen Netzwerk-Zonen (Adresskreise) zur DMZ und zum LAN wird bei den Adresseinstellungen vorgenommen. Dabei können je nach Verfügbarkeit auch WLAN-Interfaces ausgewählt werden.



LANconfig: TCP/IP ▶ Allgemein

WEBconfig: LCOS-Menübaum ▶ Setup ▶ TCP-IP

7.6.3 Adressprüfung bei DMZ- und Intranet-Interfaces

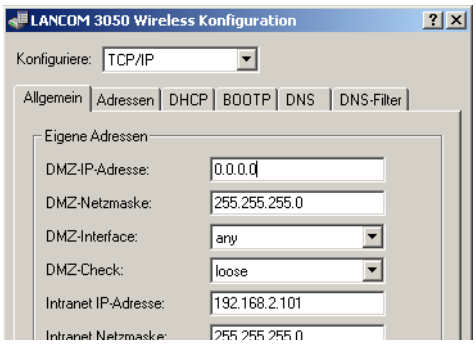
Zur besseren Abschirmung der DMZ (demilitarisierten Zone) und des Intranets gegen unerlaubte Zugriffe kann für die jeweiligen Interfaces eine zusätzliche Adressprüfung über das Intrusion Detection System (IDS) der Firewall aktiviert werden.

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 LANCOM 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'. Nur beim LANCOM 7011 VPN steht der Default auf 'strict', da bei diesem Gerät auch bisher schon eine schärfere Adressprüfung verwendet wurde.

Den Schalter zur Aktivierung von der DMZ- und Intranet-Adressprüfung finden Sie in LANconfig im Konfigurationsbereich 'TCP-IP' auf der Registerkarte 'Allgemein'.



LANconfig: TCP/IP ▶ Allgemein

WEBconfig: LCOS-Menübaum ▶ Setup ▶ TCP-IP

7.6.4 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.

Um Angriffe von 'geknackten' Servern auf das lokale Netz zu verhindern, verfügen einige LANCOM über ein dediziertes DMZ-Interface (LANCOM 7011 VPN). Alle anderen Modelle mit 4-Port-Switch (LANCOM 821 ADSL/ISDN, LANCOM 1511 DSL, LANCOM 1521 ADSL, LANCOM 1621 ADSL/ISDN, LANCOM 1711 VPN, LANCOM 1811 DSL und LANCOM 1821 ADSL) können die LAN-Ports per Hardware auf Ethernet-Ebene einzeln oder „en bloc" voneinander trennen.

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	LANCOM als Gateway für das Intranet
123.45.67.2	Gerät im lokalen Netzwerk, das unmaskierten Zugang ins Internet erhalten soll, beispielsweise ein Web-Server am DMZ-Port
123.45.67.3	Broadcast-Adresse

Alle Rechner und Geräte im Intranet haben keine öffentliche IP-Adresse und treten daher mit der IP-Adresse des LANCOM (123.45.67.1) im Internet auf.

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

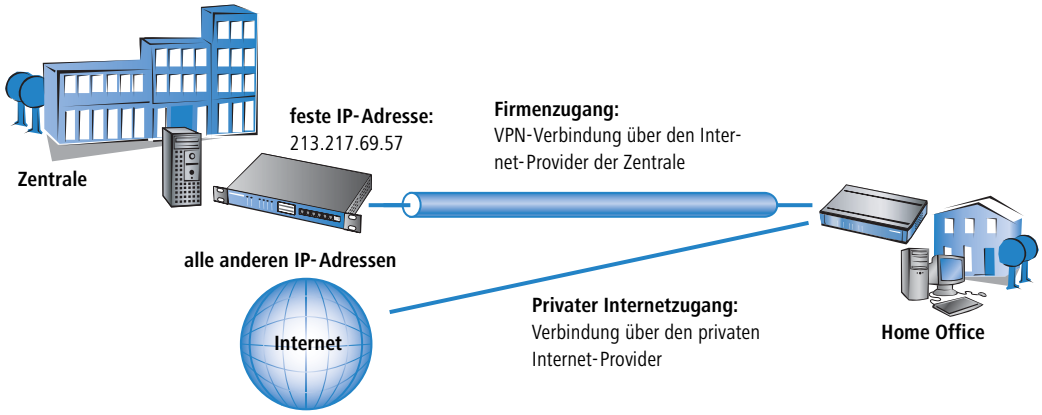
- Bei einer "Deny-All"-Strategie ('Aufbau einer expliziten "Deny-All"-Strategie' → Seite 8-20): Zugriff von "Alle Stationen im lokalen Netz" auf "123.45.67.2" erlauben

7.7 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. LANCOM-Geräte mit DSL- oder ADSL-Interface können bis zu acht verschiedene Kanäle ins WAN parallel auf dem gleichen physikalischen Interface aufbauen.

7.7.1 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.

7.7.2 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 LANCOM 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 LANCOM-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. Informationen über die Konfiguration von speziellen Benutzerrechten finden Sie in diesem Addendum unter 'Rechteverwaltung für verschiedene Administratoren' → Seite 3-26.

Sorgen Sie mit den entsprechenden Filterregeln im Bereich 'Firewall/QoS' dafür, dass der Internetverkehr nicht versehentlich über das Netzwerk der Zentrale läuft.

7.8 Load-Balancing

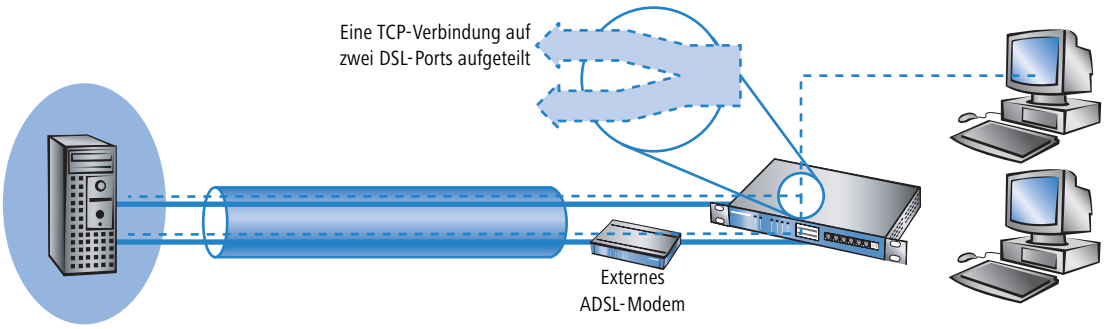
Trotz immer weiter steigender Bandbreite auf DSL-Zugängen stellen diese immer noch das Nadelöhr in der Kommunikation dar. In manchen Fällen ist es durchaus sinnvoll, mehrere DSL-Zugänge zu bündeln. Hierzu gibt es mehrere Möglichkeiten, die zum Teil vom Internet-Provider aktiv unterstützt werden müssen:

- DSL-Kanalbündelung (Multilink-PPPoE – MLPPPoE)

  Bei der direkten Bündelung ist der Anwender auf das Angebot des Carriers angewiesen, der dieses Verfahren unterstützen muss. Dem Anwender steht dabei die Summe der Bandbreiten aller gebündelter Kanäle zur Verfügung. Multilink-PPPoE kann nur zum Bündeln von PPP-Verbindungen eingesetzt werden.

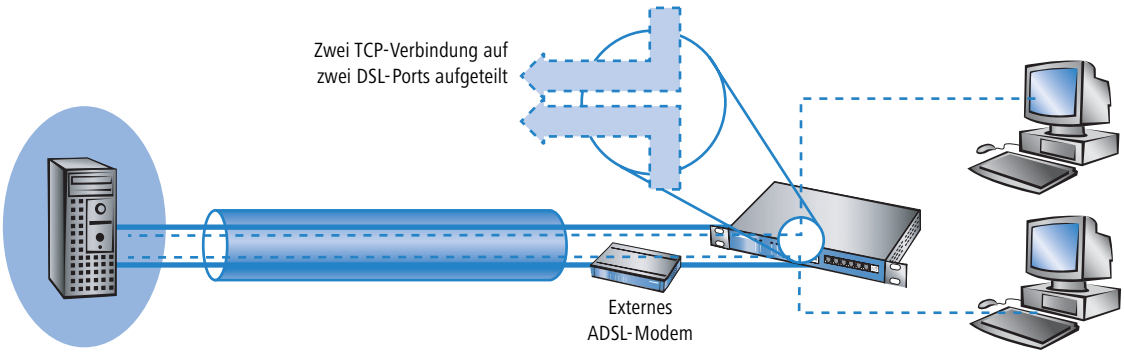
Diese Variante der Kanalbündelung stellt als Summe ein Vielfaches der kleinsten der gebündelten Kanäle zur Verfügung. Sie ist daher besonders effizient, wenn Kanäle mit gleichen Bandbreiten verbunden werden. Bei der direkten Bündelung unterschiedlicher Bandbreiten geht für die Kanäle mit hohen Datenraten effektive Bandbreite verloren.

MLPPPoE verhält sich beim Bündeln von DSL-Kanälen wie das bekannte MLPPP bei ISDN-Kanalbündelung 'ISDN-Kanalbündelung mit MLPPP' → Seite 7-42.



- Load-Balancing

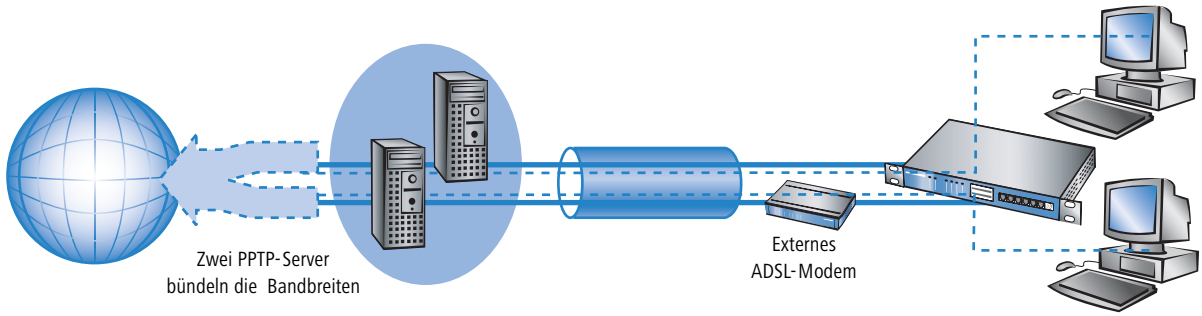
  Beim Load-Balancing werden TCP-Verbindungen dynamisch auf voneinander unabhängigen DSL-Verbindungen verteilt. Dem Anwender steht damit zwar auch die Summen-Bandbreite der gebündelten Kanäle zur Verfügung, dennoch ist jede einzelne TCP-Verbindung auf die Bandbreite des zugewiesenen DSL-Anschlusses beschränkt.



Im Gegensatz zur direkten Kanalbündelung steht beim Load-Balancing tatsächlich die Summe aller gebündelten Bandbreiten zur Verfügung. Diese Variante eignet sich daher besonders gut zum Verbinden unterschiedlicher Bandbreiten.

- 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.



7.8.1 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 LANCOM-Routers ein oder mehrere externe DSL-Modems angeschlossen.

Bitte informieren Sie sich in der Featuretabelle im Anhang (Kapitel A ab Seite 14), ob Ihr Gerät den Anschluss externer DSL-Modems unterstützt.

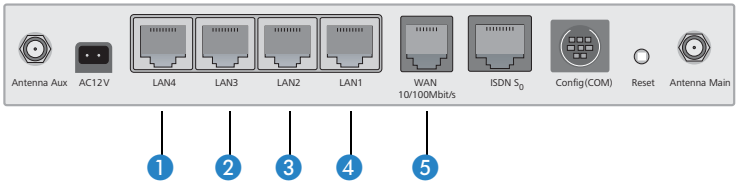
Zuordnung der Switch-Ports zu den DSL-Ports

Bei Geräten mit integriertem Switch können je nach Modell ('Übersicht über die Funktionen nach Modellen und LCOS*-Versionen' → Seite 16-14) 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 LANCOM den Port nach dem für die Verbindung gewählten Kommunikations-Layer aus.
  - □ Wenn auf Layer-1 'AAL-5' eingestellt ist, wird das ADSL-Interface ausgewählt.
  - □ 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 ADSL-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 ADSL-Interface als erstes für die Bündelung verwendet wird.



Bei Multi-PPPoE ('Multi-PPPoE' → Seite 7-23) 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.

Zuordnung der MAC-Adresse zu den DSL-Ports

Wenn ein LANCOM 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.

7.8.2 DSL-Kanalbündelung (MLPPPoE)

Um DSL-Anschlüsse zu bündeln, werden die zu verwendenen DSL-Ports in der Liste der DSL-Breitband-Gegenstellen eingetragen. Dabei wird nur die Nummer des DSL-Ports angegeben, bei mehreren Ports durch Kommata separiert (1,2,4) oder als Bereich (1-4).

Für die DSL-Kanalbündelung sind zusätzlich zwei Fälle zu unterscheiden. Diese hängen von der auf dem DSL-Anschluss verwendeten Zugangsart ab. In Deutschland wird man normalerweise nur PPPoE-Zugänge antreffen. In anderen Ländern (z.B. Österreich oder Frankreich) sich auch Zugänge möglich, die stattdessen PPTP verwenden.

- Bündelung über PPPoE

Um PPPoE-Verbindungen zu bündeln reicht es aus, die Bündelung im verwendeten Layer zu aktivieren und in der Portliste die zu verwendenden Ports zuzuweisen.

- Bündelung über PPTP

  Bei der Bündelungen von PPTP-Verbindungen ist zu beachten, dass die DSL-Modems meist auf eine feste, oft nicht editierbare, IP-Adresse (z.B. 10.0.0.138) reagieren und ggf. auch noch verlangen, dass der Router ebenfalls eine feste Adresse (ggf. 10.0.0.140) besitzt.

  In diesen Fällen wird die Kanalbündelung über das Load-Balancing realisiert. Dafür werden mehrere getrennte DSL-Verbindungen auf verschiedenen Ports eingerichtet. Alle diese Verbindungen erhalten die gleichen Einträge in der IP-Parameterliste. Eine Bündelung erfolgt dann, wenn für die physikalische Verbindung der PPTP-Gegenstelle in der Load-Balancing-Liste zusätzliche Gegenstellen definiert sind. Das PPTP fordert dann im Bündelfall vom Load-Balancer die nächste physikalische Verbindung an und baut sie dorthin auf. Dies entspricht somit der indirekten Bündelung für LAN-LAN-Kopplungen (Seite 28).

7.8.3 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.

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 min-

destens 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.

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 LANCOM 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 'Interfaces' auf der Registerkarte 'WAN' unter der Schaltfläche **Interface-Einstellungen** erforderlich (Telnet: `/Setup/Schnittstellen/DSL`, WEBconfig: **Expertenkonfiguration ▶ Setup ▶ Schnittstellen ▶ DSL**).

7.8.4 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, H.323, PPTP). Dabei akzeptiert der Server den Aufbau der Datenkanäle nur von der gleichen IP-Adresse, von der auch der Kontrollkanal aufgebaut wurde.

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.

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' → Seite 7-3.

7.8.5 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.

Hier muss noch ein Detail mit Guido geklärt werden.

7.8.6 Konfiguration des Load Balancing

Für die folgenden Konfigurationen gehen wir davon aus, dass die entsprechenden Gegenstellen mit allen Zugangsdaten bereits eingerichtet sind.

Direkte Kanalbündelung über PPPoE

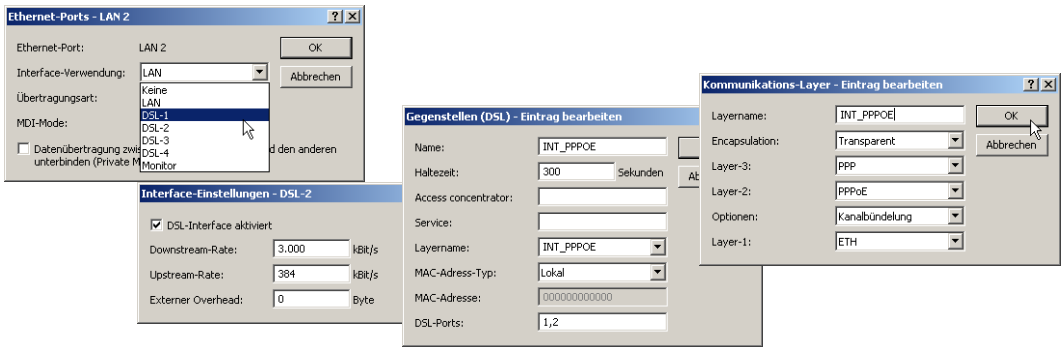
Zur Konfiguration der direkten Kanalbündelung über PPPoE gehen Sie folgendermaßen vor:

① Ordnen Sie den Ethernet-Ports die gewünschten DSL-Ports zu, in LANconfig über **Interfaces ▶ LAN ▶ Ethernet-Ports**.
Telnet: `/Setup/Schnittstellen/Ethernet-Ports`
WEBconfig: **Expertenkonfiguration ▶ Setup ▶ Schnittstellen ▶ Ethernet-Ports**

② Aktivieren Sie die zusätzlichen DSL-Interfaces in LANconfig über **Interfaces ▶ WAN ▶ Interface-Einstellungen**. Geben Sie dabei die Datenraten für Up- und Downstream an.
Telnet: `/Setup/Schnittstellen/DSL`
WEBconfig: **Expertenkonfiguration ▶ Setup ▶ Schnittstellen ▶ DSL**

③ Tragen Sie für die gewünschte Gegenstelle die zu verwendenden DSL-Ports in LANconfig über **Kommunikation ▶ Gegenstellen ▶ Gegenstellen (DSL)** ein.
Telnet: `/Setup/WAN/DSL-Breitband-Gegenstellen`
WEBconfig: **Expertenkonfiguration ▶ Setup ▶ WAN ▶ DSL-Breitband-Gegenstellen**

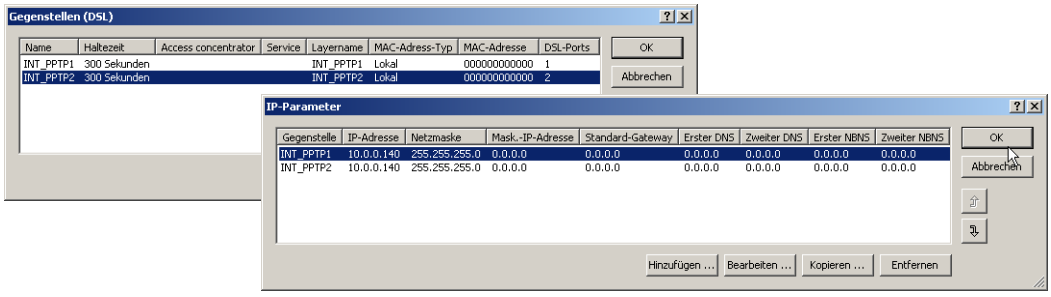
④ Aktivieren Sie für den verwendeten Layer die Kanalbündelung in LANconfig über **Kommunikation ▶ Allgemein ▶ Kommunikations-Layer**.
Telnet: `/Setup/WAN/Layer`
WEBconfig: **Expertenkonfiguration ▶ Setup ▶ WAN ▶ Layer**



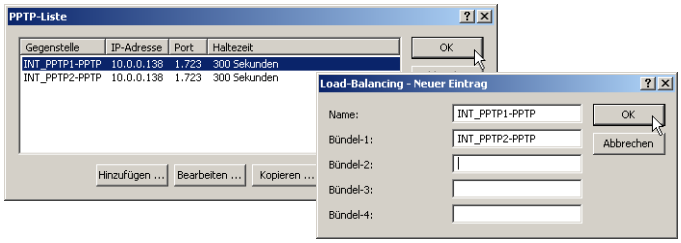
Direkte Kanalbündelung über PPTP

Zur Konfiguration der direkten Kanalbündelung über PPPoE 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.
Telnet: `/Setup/WAN/IP-Liste`
WEBconfig: **Expertenkonfiguration ▶ Setup ▶ WAN ▶ IP-Liste**



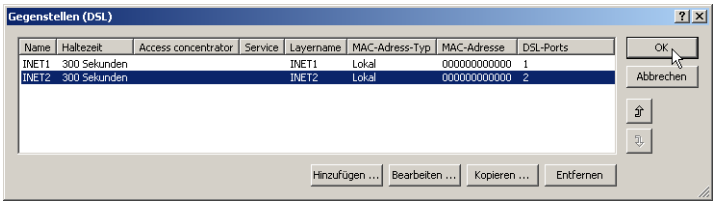
② Eine Bündelung erfolgt dann, wenn für die physikalische Verbindung der PPTP-Gegenstelle in der Load-Balancing-Liste zusätzliche Gegenstellen definiert sind. Die PPTP-Verbindung fordert dann im Bündelfall die nächste physikalische Verbindung an und baut sie dorthin auf. Tragen Sie die Bündelverbindungen in LANconfig über **IP-Router ▶ Routing ▶ Load-Balancing** ein.
Telnet: `/Setup/IP-Router/Load-Balancer`
WEBconfig: **Expertenkonfiguration ▶ Setup ▶ IP-Router ▶ Load-Balancer**



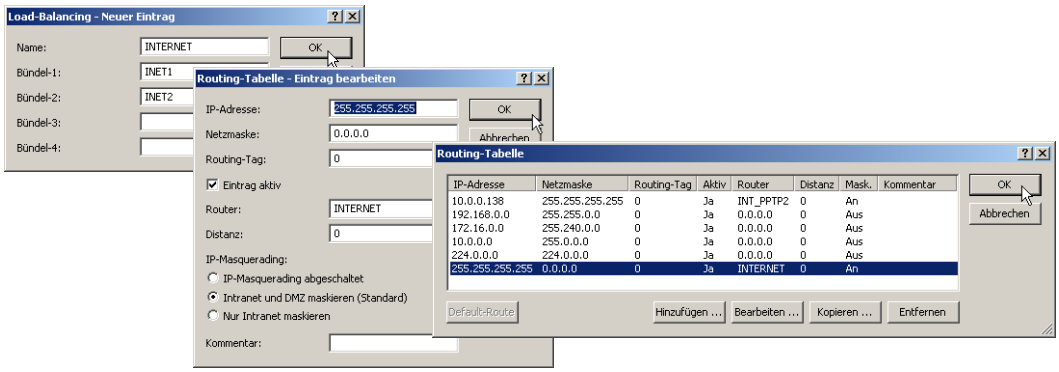
Dynamisches Load-Balancing mit mehreren DSL-Zugängen

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.
Telnet: `/Setup/WAN/DSL-Breitband-Gegenstellen`
WEBconfig: **Expertenkonfiguration ▶ Setup ▶ WAN ▶ DSL-Breitband-Gegenstellen**



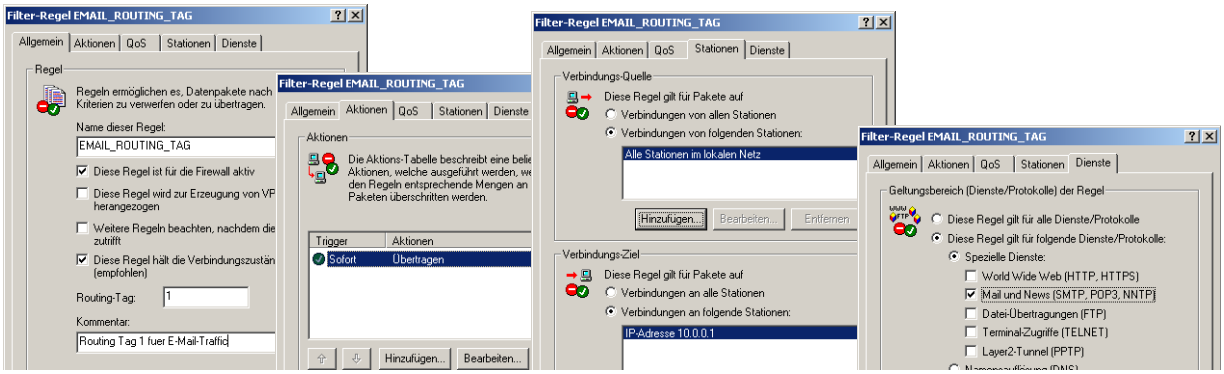
② Die beiden DSL-Gegenstellen werden dann in der Load-Balancing-Liste in LANconfig über **IP-Router ▶ Routing ▶ Load-Balancing** einer neuen, virtuellen Gegenstelle 'INTERNET' zugeordnet.
Telnet: `/Setup/IP-Router/Load-Balancer`
WEBconfig: **Expertenkonfiguration ▶ Setup ▶ IP-Router ▶ Load-Balancer**



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.
Telnet: `/Setup/IP-Router/IP-Routing-Tabelle`
WEBconfig: **Expertenkonfiguration ▶ 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.
Telnet: `/Setup/IP-Router/Firewall/Regel-Tabelle`
WEBconfig: **Expertenkonfiguration ▶ Setup ▶ IP-Router ▶ Firewall ▶ Regel-Tabelle**



7.9 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' → Seite 7-17) 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" ('Inverses Masquerading' → Seite 7-19).

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 LANCOM definiert. Dabei werden für einzelne Stationen im LAN, Teilnetze oder das gesamte LAN neue IP-Adressen festgelegt, unter denen die Stationen dann mit dem anderen Netzen in Kontakt treten können.

Bei einigen Protokollen (FTP, H.323) 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.

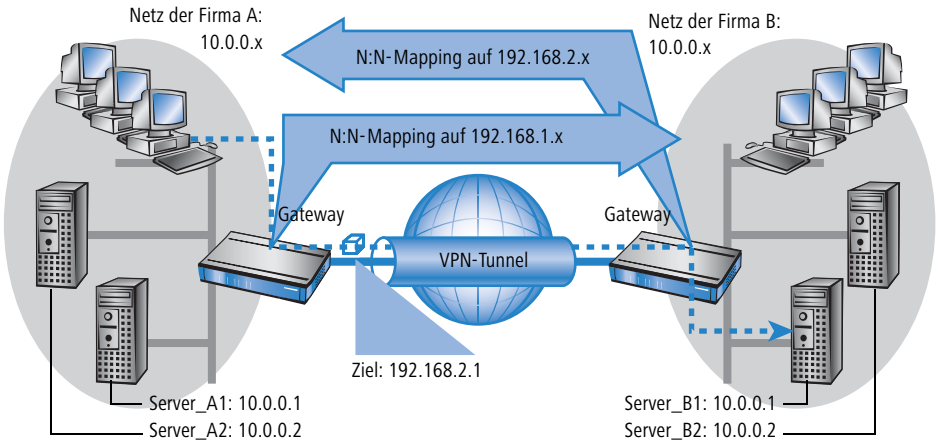
7.9.1 Anwendungsbeispiele

Im folgenden werden die folgenden typischen Anwendungen vorgestellt:

- Kopplung von privaten Netzen, die den gleichen Adressraum belegen
- Zentrale Fernüberwachung durch Dienstleister

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:

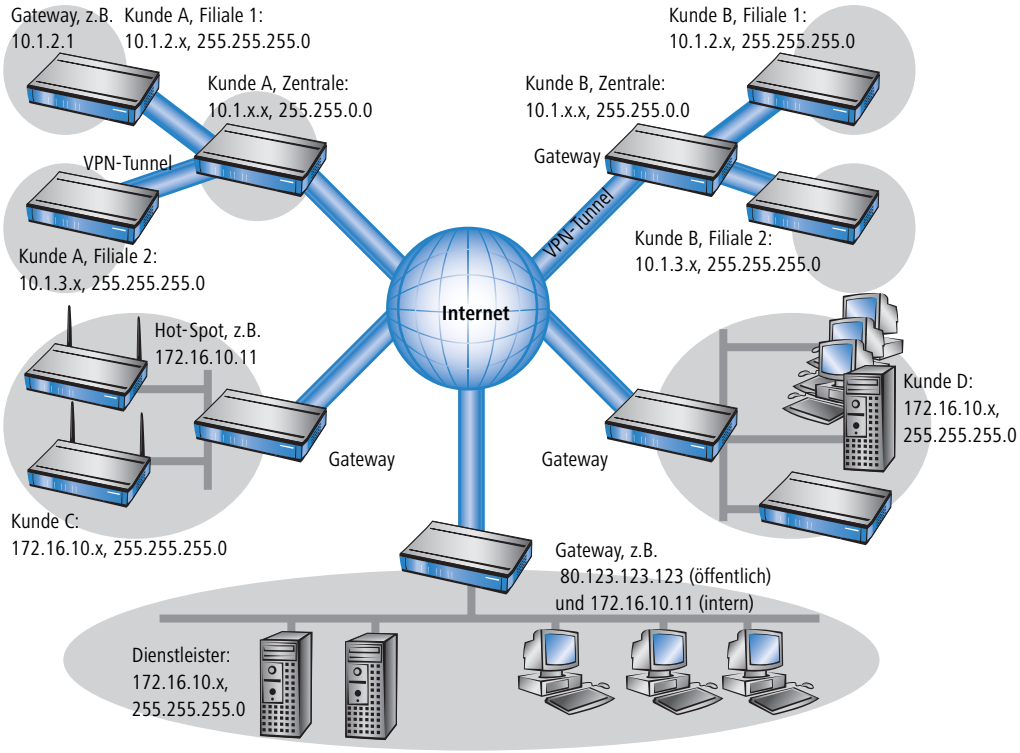


In diesem Beispiel stehen in den Netzen der Firmen A und B Server, die über einen VPN-Tunnel auf das jeweils andere Netz zugreifen wollen. Allen Stationen im LAN soll dabei der Zugang zu den Servern im remoten Netz erlaubt werden. Da beide Netze den gleichen Adresskreis nutzen, ist in dieser Konfiguration 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.

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 für ISDN-Einwahlzugänge.

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 LANCOM unterstützt werden, finden Sie im Anhang dieses Referenz-Handbuchs ('SNMP-Traps' → Seite 16-9).

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:

Loopback: dezentrales 1:1-Mapping

- 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 LANCOM ist damit nicht generell unter dieser IP-Adresse erreichbar.

Alternativ: zentrales N:N-Mapping

- 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.

7.9.2 Konfiguration

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.

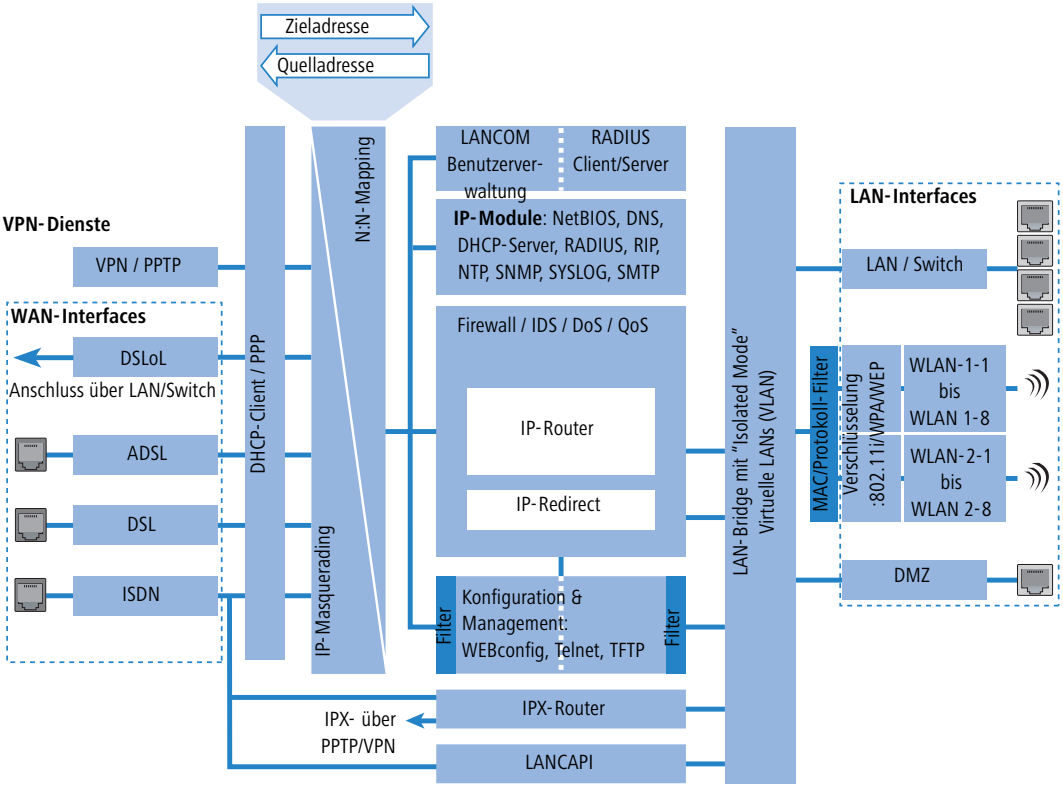
Bitte beachten Sie, dass die Funktionen des N:N-Mapping nur wirksam sind, wenn die Firewall eingeschaltet ist ('Firewall/QoS-Aktivierung' → Seite 8-10)!

Zusätzliche Konfigurationshinweise

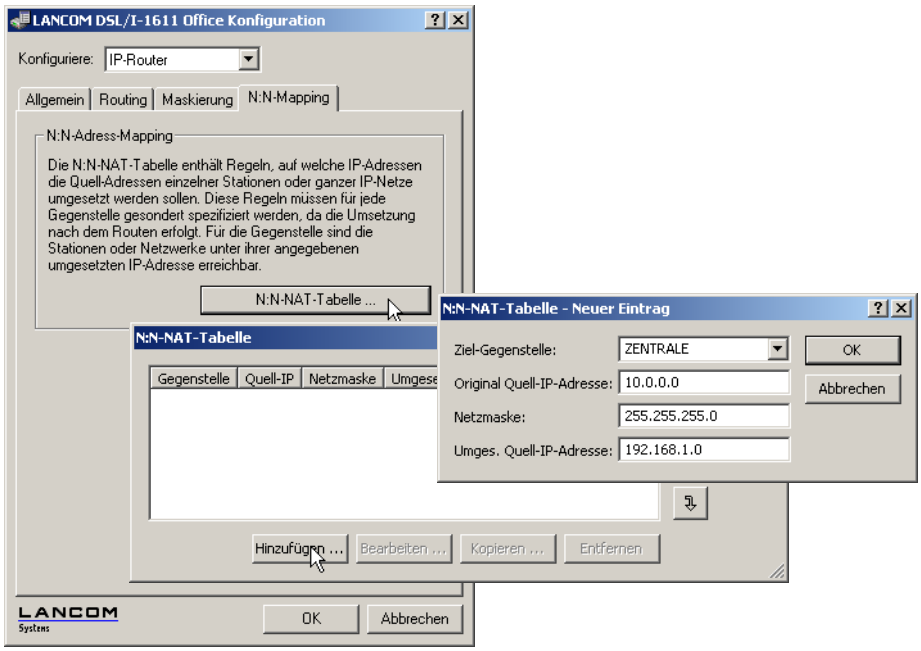
Mit dem Einrichten der Adressumleitung in der NAT-Tabelle werden die Netze und Rechner zunächst nur unter einer anderen Adresse im übergeordneten Netzverbund sichtbar. Für das einwandfreie Routing der Daten zwischen den Netzen sind aber noch einige weitere Einstellungen notwendig:

- 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 ('DNS-Forwarding' → Seite 16-11).
- 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 LANCOM 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.



Konfiguration mit den verschiedenen Tools



LANconfig: IP-Router ▶ N:N-Mapping

WEBconfig: LCOS Menübaum ▶ Setup ▶ IP-Router ▶ NAT-Tabelle

Die NAT-Tabelle präsentiert sich unter WEBconfig beim Anlegen eines neuen Eintrags folgendermaßen:



7.10 Verbindungsaufbau mit PPP

Router von LANCOM Systems 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.

7.10.1 Das Protokoll

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' → Seite 7-48).
- Überprüfung der Verbindung mit dem LCP (Link Control Protocol)
- Bündelung von mehreren ISDN- oder DSL-Kanälen (Multilink-PPP bzw. Multilink-PPPoE)

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.

Wozu wird PPP verwendet?

Das Point-to-Point Protocol wird bei folgenden Anwendungen sinnvoll eingesetzt:

- aus Kompatibilitätsgründen z.B. bei Kommunikation mit Fremdroutern
- Remote Access von entfernten Arbeitsplatzrechnern mit ISDN-Adaptern
- Internet-Access (mit der Übermittlung von Adressen)

Das im LANCOM implementierte PPP kann synchron oder asynchron sowohl über eine transparente HDLC-Verbindung als auch über eine X.75-Verbindung verwendet werden.

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 LANCOM sind die Protokolle IPCP und IPXCP implementiert.

  Nach erfolgreicher Übertragung des Passwortes können die Netzwerk-Layer IPCP und/oder IPXCP aufgebaut werden.

  Ist die Verhandlung der Parameter für mindestens eines der Netzwerk-Layer erfolgreich verlaufen, können von den Router-Modulen IP- und/oder IPX-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.

Die PPP-Verhandlung im LANCOM

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.

7.10.2 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. Streikt beispielsweise die Highspeed-Verbindung, kann als Backup eine vorhandene ISDN-Schnittstelle den Weg ins Internet bahnen.

Beim Remote Access von einzelnen Arbeitsplatzrechnern mit Windows-Betriebssystem empfehlen wir, die regelmäßigen LCP-Anfragen des LANCOM 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.

7.10.3 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 der LANCOM 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 der LANCOM die Gegenstelle beim Eintreffen des Anrufs über die Rufnummer oder den Namen identifizieren kann, d.h. die Authentifizierung erfolgreich war.

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 LANCOM anmelden muss.

  Neben der IP-Adresse werden der Gegenstelle bei dieser Konfiguration auch die Adressen der DNS- und NBNS-Server (Domain Name Server und NetBIOS 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 LANCOM 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 den LANCOM 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 der LANCOM 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 der LANCOM während der PPP-Verhandlung auch Informationen über DNS-Server beim Provider.

Im lokalen Netz ist der LANCOM 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- und NBNS-Servern. Auch Optionen wie die Kanalbündelung oder die Dauer der Verbindung werden angezeigt.

7.10.4 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.

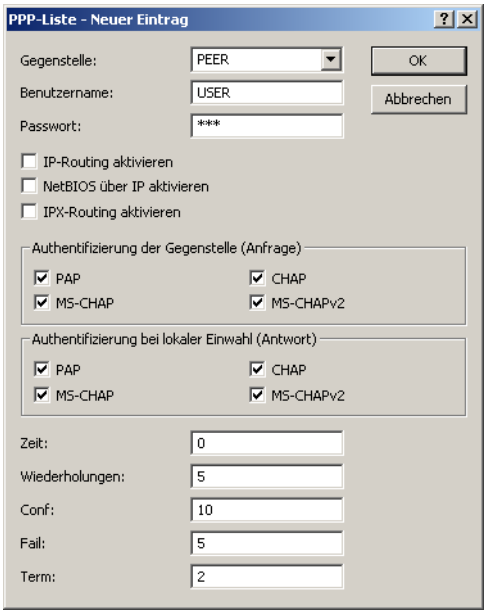
Zur Authentifizierung von Point-to-Point-Verbindungen im WAN wird häufig eines der Protokolle PAP, CHAP, MSCHAP oder MSCHAPv2 eingesetzt. Dabei haben die Protokolle untereinander eine „Hierarchie", d. h. MSCHAPv2 ist ein „höheres" Protokoll als, MSCHAP, CHAP und PAP (höhere Protokolle zeichnen sich durch 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 LANCOM 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 LANCOM 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 LANCOM wird sichergestellt, dass die PPP-Verbindung wie gewünscht zustande kommt. Dazu können ein oder mehrere Protokolle definiert werden, die zur Authentifizierung von Gegenstellen im LANCOM (eingehende Verbindungen) bzw. beim Login des LANCOM in andere Gegenstellen (ausgehende Verbindungen) akzeptiert werden.

- Das LANCOM fordert beim Aufbau eingehender Verbindungen das niedrigste der zulässigen Protokolle, lässt aber je nach Möglichkeit der Gegenstelle auch eines der höheren (im LANCOM aktivierten) Protokolle zu.
- Das LANCOM 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

WEBconfig: Setup ▶ WAN ▶ PPP

7.10.5 Die Bedeutung der DEFAULT-Gegenstelle

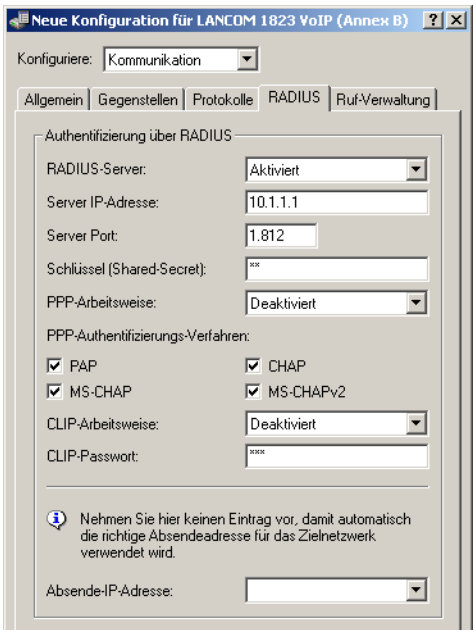
Bei der PPP-Verhandlung meldet sich die einwählende Gegenstelle mit ihrem Namen beim LANCOM an. Anhand des Namens kann das LANCOM aus der PPP-Tabelle die zulässigen Werte für die Authentifizierung entnehmen. Manchmal kann die Gegenstelle bei Verhandlungsbeginn nicht über Rufnummer (ISDN-Einwahl), IP-Adresse (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.

7.10.6 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.

WAN-RADIUS-Tabelle



LANconfig: Kommunikation ▶ RADIUS

WEBconfig: Setup ▶ WAN ▶ RADIUS

7.11 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.

Konfiguration von PPTP

Im LANCOM 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 ▶ Protokolle ▶ PPTP-Liste

WEBconfig: LCOS-Menübaum ▶ Setup ▶ WAN ▶ PPTP-Liste

Die PPTP-Konfiguration besteht aus drei 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.

7.12 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 (ICQ und ähnliche) pausenlos erreichbar sein. Es ist also wünschenswert, dass Verbindungen ununterbrochen aufrechterhalten werden.

Beim LANCOM sorgt das Keep-alive-Verfahren dafür, dass Verbindungen immer dann aufgebaut werden, wenn die Gegenstelle sie gekappt hat.

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 LANCOM 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').

7.13 Rückruf-Funktionen

LANCOM mit ISDN-Schnittstelle unterstützen einen automatischen Rückruf.

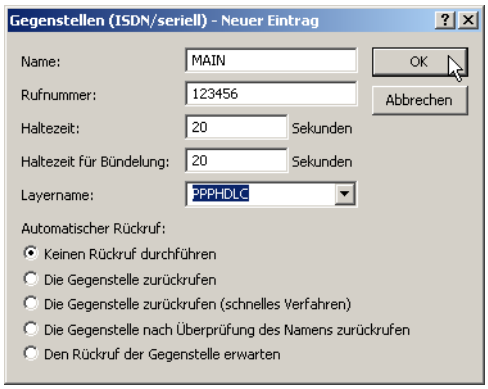
Neben dem Rückruf über den D-Kanal wird auch das von Microsoft spezifizierte CBCP (**C**allback **C**ontrol **P**rotocol) sowie der Rückruf über PPP nach RFC 1570 (PPP LCP Extensions) angeboten. Zusätzlich besteht die Möglichkeit eines besonders schnellen Rückrufs über ein von LANCOM Systems entwickeltes Verfahren. PCs mit Windows-Betriebssystem können nur über das CBCP zurückgerufen werden.

7.13.1 Rückruf nach Microsoft CBCP

Das Microsoft CBCP erlaubt verschiedene Arten, die Rückrufnummer zu bestimmen:

- Der Angerufene ruft nicht zurück.
- Der Angerufene erlaubt es dem Anrufer, die Rückrufnummer selbst anzugeben.
- Der Angerufene kennt die Rückrufnummer und ruft auch **nur** diese zurück.

Über das CBCP ist es möglich, von einem Rechner mit einem Windows-Betriebssystem eine Verbindung zum LANCOM aufzunehmen und sich von diesem zurückrufen zu lassen. Die drei möglichen Einstellungen werden über den Rückruf-Eintrag sowie den Rufnummern-Eintrag in der Gegenstellenliste ausgewählt.



Keinen Rückruf durchführen

Für diese Einstellung muss der Rückruf-Eintrag bei der Konfiguration über WEBconfig oder in der Konsole den Wert 'Aus' haben.

Rückrufnummer vom Anrufer bestimmt

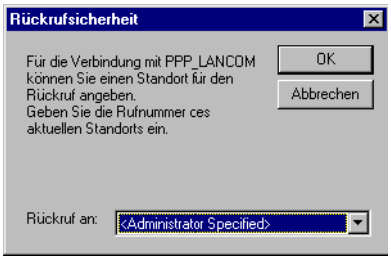
Für diese Einstellung muss der Rückruf-Eintrag auf 'Die Gegenstelle nach Überprüfung des Namens zurückrufen' stehen (bzw. in WEBconfig oder in der Konsole den Wert 'Name' haben). In der Gegenstellenliste darf **keine** Rufnummer angegeben sein.

Nach der Authentifizierung erscheint beim Anrufer in Windows ein Eingabefenster, das ihn nach der ISDN-Rufnummer des Computers fragt.

Rückrufnummer im LANCOM bestimmt

Für diese Einstellung muss der Rückruf-Eintrag auf 'Die Gegenstelle nach Überprüfung des Namens zurückrufen' stehen (bzw. in WEBconfig oder in der Konsole auf den Wert 'Name' gesetzt sein). In der Gegenstellenliste muss **eine** Rufnummer angegeben sein.

Einige Windows-Versionen (insbesondere Windows 98) fordern den Benutzer mit einem Eingabefenster auf, den Rückruf an die im LANCOM hinterlegte Rufnummer ('Administrator Specified') zu bestätigen. Andere Windows-Version informieren den Benutzer nur darüber, dass der PC auf den Rückruf vom LANCOM wartet.



Der Rückruf an einen Windows-Rechner erfolgt ca. 15 Sekunden, nachdem die erste Verbindung abgebaut wurde. Diese Zeit kann nicht verkürzt werden, da sie von Windows vorgegeben wird.

7.13.2 Schneller Rückruf mit dem LANCOM-Verfahren

Sollen zwei LANCOM miteinander kommunizieren, wobei der eine zurückgerufen wird, bietet sich der schnelle Rückruf über das LANCOM-spezifische Verfahren an.

- Der Anrufer, der gerne zurückgerufen werden möchte, stellt in der Gegenstellenliste 'Den Rückruf der Gegenstelle erwarten' ein ('Looser' bei Konfiguration über WEBconfig, Terminalprogramm oder Telnet).
- Der Rückrufer wählt 'Die Gegenstelle zurückrufen (schnelles Verfahren)' in der Gegenstellenliste und stellt die Rufnummer ein ('fast' bei Konfiguration über WEBconfig, Terminalprogramm oder Telnet).

Für den schnellen Rückruf nach LANCOM-Verfahren muss die Nummernliste für die Rufannahme auf beiden Seiten gepflegt sein.

7.13.3 Rückruf nach RFC 1570 (PPP LCP Extensions)

Der Rückruf nach 1570 ist das Standardverfahren für den Rückruf von Routern anderer Hersteller. Diese Protokollerweiterung beschreibt fünf Möglichkeiten, einen Rückruf anzufordern. Alle Versionen werden vom LANCOM akzeptiert. Es wird jedoch bei allen Varianten gleich verfahren:

Der LANCOM baut nach der Authentifizierung der Gegenstelle die Verbindung ab und ruft diese dann einige Sekunden später zurück.

Konfiguration

Für den Rückruf nach PPP wählen Sie in LANconfig die Option 'Die Gegenstelle zurückrufen' bzw. 'Auto' bei Konfiguration über WEBconfig, Terminalprogramm oder Telnet.

Für den Rückruf nach PPP muss die Nummernliste für die Rufannahme im LANCOM gepflegt sein.

7.13.4 Konfiguration der Rückruf-Funktion im Überblick

In der Gegenstellenliste stehen unter WEBconfig und Terminalprogramm/Telnet für den Rückruf-Eintrag folgende Optionen zur Verfügung:

Mit diesem Eintrag ...	... stellen Sie den Rückruf so ein:
'Aus'	Es wird nicht zurückgerufen.
'Auto' (nicht bei Windows-Betriebssystemen, s.u.)	Wenn die Gegenstelle in der Nummernliste gefunden wird, so wird diese zurückgerufen. Hierzu wird der Ruf zunächst abgelehnt und, sobald der Kanal wieder frei ist, zurückgerufen (Dauer ca. 8 Sekunden). Wird die Gegenstelle nicht in der Nummernliste gefunden, so wird sie zunächst als DEFAULT-Gegenstelle angenommen, und der Rückruf wird während der Protokollverhandlung ausgehandelt. Dabei fällt eine Gebühr von einer Einheit an.
'Name'	Bevor ein Rückruf erfolgt, wird immer eine Protokollverhandlung durchgeführt, auch wenn die Gegenstelle in der Nummernliste gefunden wurde (z.B. für Rechner mit Windows, die sich auf dem Gerät einwählen). Dabei fallen geringe Gebühren an.
'fast'	Wenn die Gegenstelle in der Nummernliste gefunden wird, wird der schnelle Rückruf durchgeführt, d.h., der LANCOM sendet ein spezielles Signal zur Gegenstelle und ruft sofort zurück, wenn der Kanal wieder frei ist. Nach ca. 2 Sekunden steht die Verbindung. Nimmt die Gegenstelle den Ruf nicht unmittelbar nach dem Signal zurück, so erfolgt zwei Sekunden später ein Rückfall auf das normale Rückrufverfahren (Dauer wieder ca. 8 Sekunden). Dieses Verfahren steht nur an DSS1-Anschlüssen zur Verfügung.
'Looser'	Benutzen Sie die Option 'Looser', wenn von der Gegenstelle ein Rückruf erwartet wird. Diese Einstellung erfüllt zwei Aufgaben gleichzeitig. Zum einen sorgt sie dafür, dass ein eigener Verbindungsaufbau zurückgenommen wird, wenn ein Ruf von der gerade angerufenen Gegenstelle hereinkommt, zum anderen wird mit dieser Einstellung die Funktion aktiviert, auf das schnelle Rückruf-Verfahren reagieren zu können. D.h., um den schnellen Rückruf nutzen zu können, muss sich der Anrufer im 'Looser'-Modus befinden, während beim Angerufenen der Rückruf auf 'LANCOM Systems' eingestellt sein muss.

Die Einstellung 'Name' bietet die höchste Sicherheit, wenn sowohl ein Eintrag in der Nummernliste als auch in der PPP-Liste konfiguriert ist. Die Einstellung 'LANCOM' ermöglicht die schnellste Rückrufmethode zwischen zwei LANCOM Systems-Routern.

Bei Windows-Gegenstellen **muss** die Einstellung 'Name' gewählt werden.

7.14 ISDN-Kanalbündelung mit MLPPP

Wenn Sie eine ISDN-Verbindung zu einer PPP-fähigen Gegenstelle aufbauen, können Sie Ihren Daten Beine machen: Sie können die Daten komprimieren und/oder mehrere B-Kanäle zur Übertragung verwenden (Kanalbündelung).

Die Verbindung mit Kanalbündelung unterscheidet sich von „normalen" Verbindungen dadurch, dass nicht nur ein, sondern mehrere B-Kanäle parallel für die Übertragung der Daten verwendet werden.

Für die Kanalbündelung wird dabei MLPPP (**M**ultilink **PPP**) verwendet. Dieses Verfahren steht natürlich nur zur Verfügung, wenn PPP als B-Kanal-Protokoll verwendet wird. MLPPP bietet sich z.B. an für den Internet-Zugang über Provider, die bei Ihren Einwahlknoten ebenfalls MLPPP-fähige Gegenstellen betreiben.

Auch für DSL-Kanäle kann eine Bündelung über MLPPPoE eingerichtet werden ('DSL-Kanalbündelung (Multilink-PPPoE – MLPPPoE)' → Seite 7-24).

Zwei Methoden der Kanalbündelung

- Statische Kanalbündelung

  Wenn eine Verbindung mit statischer Kanalbündelung aufgebaut wird, versucht der LANCOM nach dem ersten B-Kanal sofort, auch den zweiten B-Kanal aufzubauen. Gelingt dies nicht, weil z.B. dieser Kanal schon durch ein anderes Gerät oder durch eine andere Verbindung im LANCOM besetzt ist, wird dieser Aufbauversuch automatisch und regelmäßig solange wiederholt, bis auch der zweite Kanal für diese Verbindung zur Verfügung steht.

- Dynamische Kanalbündelung

  Bei einer Verbindung mit dynamischer Kanalbündelung baut der LANCOM zunächst nur einen B-Kanal auf und beginnt mit der Datenübertragung. Wenn er dann während der Verbindung feststellt, dass der Durchsatz eine Weile über einem bestimmten Schwellenwert liegt, versucht er den zweiten Kanal dazuzunehmen.

  Wenn der zweite Kanal aufgebaut ist und der Datendurchsatz wieder unter den Grenzwert zurückgeht, wartet der LANCOM noch die eingestellte B2-Haltezeit ab und schließt den Kanal dann automatisch wieder. Dabei werden die begonnenen Gebühreneinheiten ausgenutzt, sofern die Gebühreninformationen während der Verbindung übermittelt werden. Der LANCOM benutzt den zweiten B-Kanal also nur, wenn und solange er ihn auch wirklich braucht!

So stellen Sie die Kanalbündelung ein

Die Konfiguration der Kanalbündelung für eine Verbindung setzt sich aus drei Einstellungen zusammen:

① Wählen Sie für die Gegenstelle einen Kommunikations-Layer aus der Layer-Liste aus, der in den Layer-2-Optionen die Bündelung aktiviert hat. Wählen Sie unter folgenden Layer-2-Optionen:

- □ **compr.** nach dem LZS-Datenkompressionsverfahren (Stac) reduziert das Datenvolumen, wenn die Daten nicht schon vorher komprimiert waren. Dieses Verfahren wird auch von Routern anderer Hersteller und von ISDN-Adaptern unter Windows-Betriebssystemen unterstützt.
- □ **buendeln** verwendet zwei B-Kanäle für eine Verbindung.
- □ **bnd+cmpr** nutzt beides (Komprimierung und Kanalbündelung) und stellt damit die maximal mögliche Übertragungsleistung zur Verfügung.

② Erstellen Sie nun einen neuen Eintrag in der Gegenstellenliste. Achten Sie dabei auf die Haltezeiten für die Verbindung. Beachten Sie folgende Regeln:

- □ Die B1-Haltezeit sollte je nach Anwendungsfall so groß gewählt werden, dass die Verbindung nicht durch das kurzzeitige Ausbleiben von Paketen zu früh abgebaut wird. Erfahrungsgemäß sind Werte zwischen 60 und 180 Sekunden für den Beginn eine gute Basis, die man im Betrieb dann weiter anpassen kann.
- □ Die B2-Haltezeit entscheidet darüber, ob es sich um eine statische oder dynamische Kanalbündelung handelt (siehe oben). Mit einer B2-Haltezeit von '0' oder '9999' wird die Bündelung statisch, mit Werten dazwischen schaffen Sie die Möglichkeit der dynamischen Kanalbündelung. Die B2-Haltezeit definiert, wie lange der Datendurchsatz unter der Schwelle für die dynamische Kanalbündelung liegen darf, ohne dass der zweite B-Kanal automatisch abgebaut wird.

③ Legen Sie in der Router-Interface-Liste mit dem Eintrag für die Y-Verbindung fest, was geschehen soll, wenn während einer laufenden Verbindung mit Kanalbündelung der Wunsch nach einer zweiten Verbindung zu einer anderen Gegenstelle angemeldet wird.

WEBconfig: LCOS-Menübaum ▶ Setup ▶ WAN ▶ Router-Interface-Liste

- □ Y-Verbindung **Ein**: Der Router unterbricht die Bündelverbindung, um die zweite Verbindung zur anderen Gegenstelle aufzubauen. Wenn der zweite Kanal wieder frei wird, holt sich die Bündelverbindung diesen Kanal automatisch wieder zurück (bei statischer Bündelung immer, bei dynamischer nur bei Bedarf).
- □ Y-Verbindung **Aus**: Der Router hält die bestehende Bündelverbindung, die zweite Verbindung muss warten.

Bitte beachten Sie, dass bei Verwendung der Kanalbündelung die Kosten für zwei Verbindungen anfallen. Dabei sind keine weiteren Verbindungen über die LANCAPI möglich! Setzen Sie die Kanalbündelung also nur dann ein, wenn die doppelte Übertragungsleistung auch tatsächlich ausgenutzt werden kann.

7.15 Betrieb eines Modems an der seriellen Schnittstelle

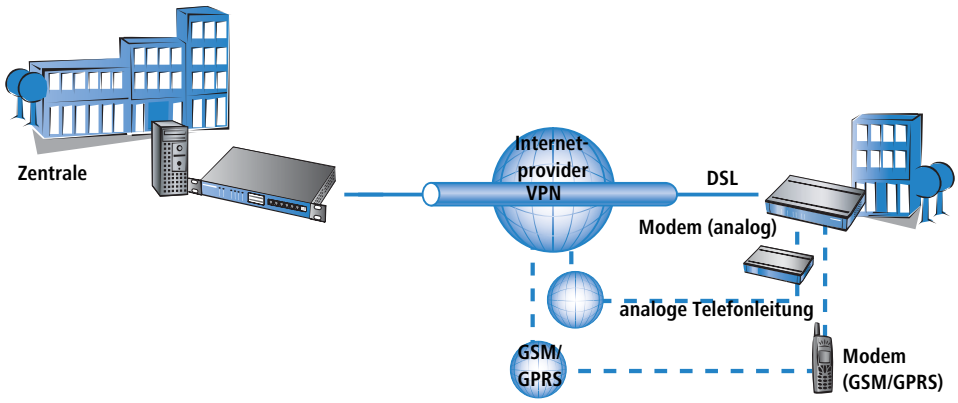
Die Ausführungen dieses Abschnittes beziehen sich nur auf Geräte mit serieller Konfigurationsschnittstelle.

7.15.1 Einleitung

International sind analoge Leitungen auch im Geschäftskundenbereich ähnlich häufig anzutreffen wie das in Deutschland dominierende ISDN. Der Betrieb von internationalen Netzwerken stellt daher besondere Anforderungen an Fernwartungsmöglichkeiten und Hochverfügbarkeit der eingesetzten Gateways und erfordert somit andere Schnittstellen als die in Deutschland in vielen Routern integrierte ISDN-Schnittstelle. Neben den normalen analogen Telefonleitungen stellt in machen Fällen das Mobilfunknetz über GSM oder GPRS die einzige Möglichkeit dar, eine Fernwartung auch ohne die Breitbandzugänge oder andere kabelgebundene Verbindungen sicherzustellen.

Um diesen Anforderungen gerecht zu werden, können die meisten LANCOM-Modelle mit serieller Schnittstelle um ein zusätzliches WAN-Interface über analoge Modems oder GSM bzw. GPRS erweitert werden. Mit einem geeignetem Modem und dem LANCOM Modem Adapter Kit stehen die folgenden Funktionen zur Verfügung:

- Internet-Zugang über Modem-Verbindung mit Nutzung aller Routerfunktionen wie Firewall, automatischer Verbindungsauf- und -Abbau etc.
- Fernwartung (z.B. Einwahl auf internationale Standorte)
- Backup-Verbindung (z.B. Hochverfügbarkeit durch GSM/GPRS Modem-Verbindung)



7.15.2 Systemvoraussetzungen

Für die Einrichtung einer zusätzlichen WAN-Schnittstelle über den seriellen Anschluss benötigen Sie:

- LANCOM mit serieller Konfigurationsschnittstelle und Unterstützung für das LANCOM Modem Adapter Kit. Für Geräte mit serieller Konfigurationsschnittstelle entnehmen Sie bitte der Tabelle 'Übersicht über die Funktionen nach Modellen und LCOS*-Versionen' → Seite 16-14, ob das jeweilige Modell den Modembetrieb an serieller Schnittstelle unterstützt.
- LANconfig, alternativ Webbrowser oder Telnet zur Konfiguration
- serielles Konfigurationskabel (im Lieferumfang des Gerätes enthalten)
- Externes Modem mit Standard AT-Kommandosatz (Hayes-kompatibel) und D-Sub9 oder D-Sub25 Anschluss
- LANCOM Modem Adapter Kit zum Anschluss des Modems über das serielle Konfigurationskabel

7.15.3 Installation

Zur Installation wird das Modem einfach über den LANCOM Modem Adapter Kit mit der seriellen Konfigurationsschnittstelle des LANCOM verbunden.

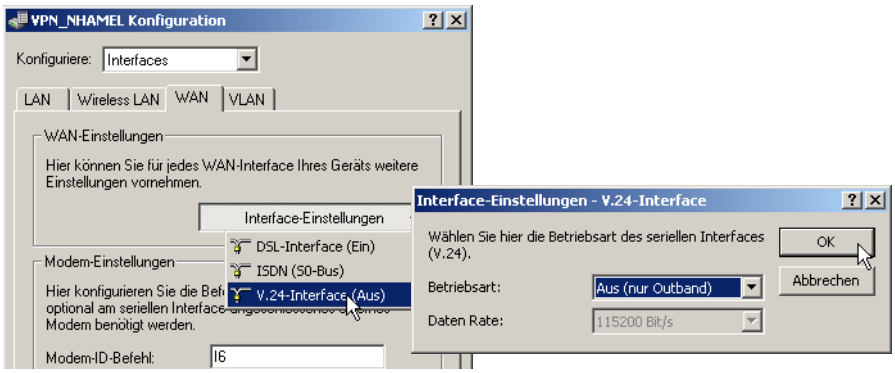
Bitte verwenden Sie ausschließlich das originale LANCOM Modem Adapter Kit! Die Kontaktbelegung beim LANCOM Modem Adapter Kit unterscheidet sich von anderen handelsüblichen Adaptern wie z.B. dem „Nullmodem-Kabel". Der Einsatz von nicht geeignetem Zubehör kann zu ernsthaften Schäden an Ihrem LANCOM oder Ihrem Modem führen. Weitere Details entnehmen Sie bitte der 'Kontaktbelegung des LANCOM Modem Adapter Kits' → Seite 7-48.

7.15.4 Einstellen der seriellen Schnittstelle auf Modem-Betrieb

Für den Betrieb der seriellen Schnittstelle können Sie die Betriebsart und die Bitrate einstellen.

- Betriebsart [Default: Outband]
  - □ Outband: In dieser Betriebsart wird die serielle Schnittstelle nur zur Konfiguration über ein Terminalprogramm verwendet.
  - □ Modem: In der Einstellung als 'Modem' versucht das Gerät, an der seriellen Schnittstelle ein Modem zu erkennen. Bei Erfolg kann das Modem als zusätzliche WAN-Schnittstelle verwendet werden. Wird jedoch ein angeschlossener Rechner mit Terminalprogramm an der seriellen Schnittstelle festgestellt, schaltet das Gerät die Schnittstelle automatisch in den Modus zur Outband-Konfiguration um.
  - □ Interlink: Direktverbindung zwischen zwei LANCOM-Geräten
- Bitrate [Default: 115.200 Bit/s.]

  Stellen Sie hier die Bitrate ein, die Ihr Modem maximal unterstützt. LANCOM-Geräte unterstützen an der seriellen Schnittstelle von 19.200 Bit/s, 38.400 Bit/s, 57.600 Bit/s bis maximal 115.200 Bit/s.



LANconfig: Interfaces ▶ WAN ▶ V.24-Schnittstelle

WEBconfig: LCOS-Menübaum ▶ Setup ▶ Schnittstellen ▶ V.24-Schnittstelle

Solange das LANCOM auf Modem-Betrieb eingestellt ist, werden bei einer Verbindung mit einem Terminalprogramm über die serielle Schnittstelle die AT-Kommandos angezeit, mit denen das LANCOM ein angeschlossenes Modem erkennen will. Drücken Sie im Terminal einige Male die Return-Taste, um die Modemerkennung zu unterbrechen und die Konfigurationssitzung zu starten.

7.15.5 Konfiguration der Modem-Parameter

Für den Betrieb eines Modems an der seriellen Schnittstelle müssen folgende Parameter eingestellt werden:

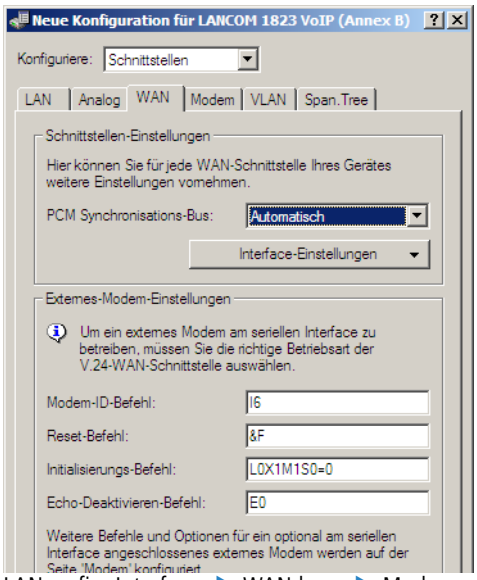
- Modem-ID-Befehl [Default: `ATI6`]
- Reset-String [Default: `AT&F`]
- Initialisierungs-String [Default: `ATL0M1X1S0=0`]
  - `L0`: Lautsprecher leise
  - `M1`: Lautsprecher an während der Aufbauphase
  - `X1`: Betrieb an einer Nebenstelle
  - `S0=0`: Rufannahme ausschalten
- Modem-Echo ausschalten [Default: `ATE0`]
- AT-Prüfzyklus-Zeit [Default: `1` in Sekunden]
- AT-Prüfzyklus-Anzahl [Default: `5`]
- Rufzahl zur Rufannahme [Default: `1`]
- Rufannahme-Initialisierungs-Befehl
- Rufannahme -Befehl [Default: `ATA`]
- Wähl-Initialisierungs-Befehl
- Wähl-Befehl [Default: `ATDT`]
- Escapesequence zum Beenden der Datenphase bzw. zur Rückkehr in die Kommandophase [Default: `+++`]
- Wartezeit nach Escapesequence [Default: `1000` in Millisekunden]
- Verbindung trennen: Zeichenfolge, die das Modem in der Datenphase als Anweisung zum Auflegen interpretiert. [Default: `ATH`]

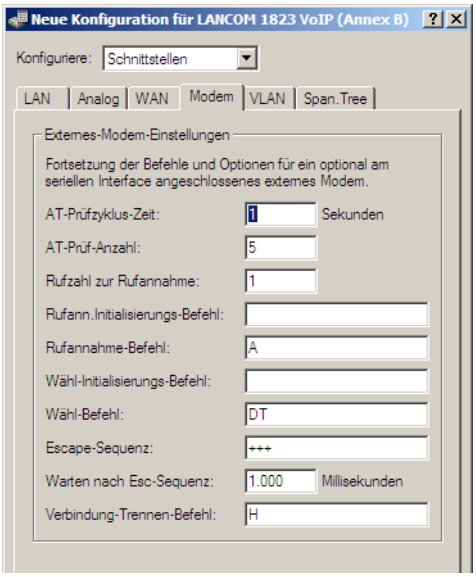
Die Modem-Parameter sind mit Werten vorbelegt, die für die meisten Modem-Typen passen – Änderungen sind daher in der Regel nicht erforderlich. Informieren Sie sich in der Dokumentation zu Ihrem Modem über evtl. abweichende Einstellungen.

GRPS-Backup-Verbindung einrichten

Wenn Sie für die Verbindung über die serielle Schnittstelle ein GRPS-fähiges Modem einsetzen, benötigen Sie den APN-Namen und die Einwahlnummer. Für T-Mobile und Vodafone ergeben sich dabei folgende Initstrings in der Konfiguration:

- T-Mobile
  - Initstring: `L0X1M1S0=0+CGDCONT=1, "IP", "internet.t-d1.de"`
  - Anwahlnummer : `*99#`
- Vodafone
  - Initstring: `L0X1M1S0=0+CGDCONT=1, "IP", "web.vodafone.de"`
  - Anwahlnummer : `*99#` oder `*99***1#`





LANconfig: Interfaces ▶ WAN bzw. ▶ Modem

WEBconfig: LCOS-Menübaum ▶ Setup ▶ Schnittstellen ▶ Modem-Parameter

Eingabe von Sonderzeichen an der Konsole

Die GPRS-Einwahl erfordert es, Initialisierungsstrings mit Anführungszeichen und Gleichheitszeichen eingeben zu können. Bestimmte Sonderzeichen können durch voranstellen eines Backslash entsprechend markiert werden:

- *
- "
- =
- Leerzeichen
- **Beispiel:** `+cgdcont\=1,\"IP\",\"internet.t-d1.de\"`

Alternativ kann die gesamte Befehlssequenz in Anführungszeichen eingeschlossen werden. Dabei müssen den inneren Anführungszeichen innerhalb der umgebenden Anführungszeichen auch Backslashes vorangestellt werden.

- **Beispiel:** `"+cgdcont=1,\"IP\",\"internet.t-d1.de\""`

7.15.6 Direkte Eingabe von AT-Befehlen

Mit dem Befehl

- `sendserial „AT..."`

können Sie bei einer aktiven Telnet-Verbindung zu einem LANCOM mit angeschlossenem Modem eine Zeichenkette direkt an das Modem übertragen. Mit dieser Funktion können Sie z.B. beliebige AT-Befehle auf dem Modem ausführen.

Das Senden von AT-Befehlen ist nur moglich, wenn sich das Modem im internen Zustand 'idle' oder 'Modem bereit' befindet. Die Rückmeldungen sind im seriellen Trace (‘Trace-Ausgaben’ → Seite 7-47) zu finden.

7.15.7 Statistik

Die Statistiken über die Aktivitäten auf der seriellen Schnittstelle finden Sie beim Zugang über Terminalprogramm oder Telnet unter:

`Status/Modem-Status`

Die Statistik zeigt den erkannten Modemtyp an und den letzten Verbindungszustand des angeschlossenen Modems, z.B. die Übertragungsrate, den verwendeten Übertragungsstandard oder die eingesetzte Fehlererkennung.

Die Statistik zeigt die folgenden Zustände:

- den Typ des angeschlossenen Modems
- den Status der letzten Verbindung, z.B. die Datenübertragungsrate, das verwendete Protokoll oder die verwendete Fehlererkennungsmethode

- den internen Zustand des Modems, z.B.:
  - Geräteerkennung
  - Schnittstelle ausgeschaltet
  - Modeminitialisierung
  - Modem bereit
  - Verbindungsaufbau
  - Modem im Übertragungsmodus

  Diese Meldungen sind hilfreich für die Fehlersuche.

7.15.8 Trace-Ausgaben

Mit dem Befehl

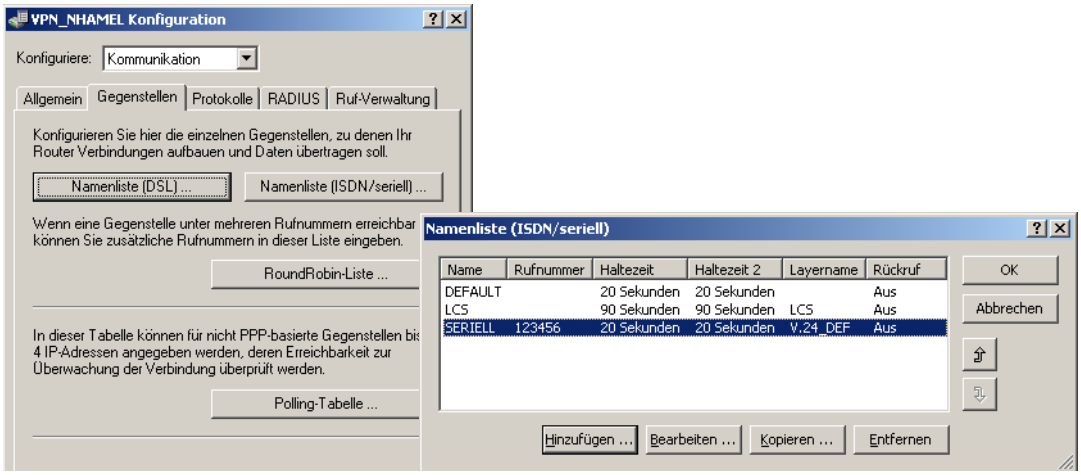
- `trace + serial`

können Sie bei einer aktiven Telnet-Verbindung zu einem LANCOM mit angeschlossenem Modem die Traceausgabe für die serielle Schnittstelle starten. Die Ausgabe zeigt alle Meldungen an, die bis zum Aufbau der Datenübertragung zwischen dem Modem und dem LANCOM ausgetauscht werden.

7.15.9 Konfiguration von Gegenstellen für V.24-WAN-Schnittstellen

Um eine Verbindung zu einer Gegenstelle über das an der seriellen Schnittstelle angeschlossene Modem aufzubauen, muss ein entsprechender Eintrag in der Gegenstellenliste (ISDN/seriell) erstellt werden. Die Gegenstellenliste (ISDN/seriell) enthält die folgenden Informationen:

- Name: Name der Gegenstelle
- Rufnummer: Rufnummer, über die die Gegenstelle erreicht werden kann. Das Feld kann leer bleiben, wenn lediglich Rufe angenommen werden sollen.
- 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 getrennt. 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.
- 2. Haltezeit: Wird ignoriert.
- Layername: Für die Verbindung über die serielle WAN-Schnittstelle wird der Layer 'V.24_DEF' ausgewählt. Der Layer ist voreingestellt und muss nicht weiter konfiguriert werden. Der Layer 'V.24_DEF' verwendet folgende Einstellungen:
  - Encapsulation: Transparent
  - Layer-3: APPP (asynchrones PPP)
  - Layer-2: Transparent
  - Optionen: keine
  - Layer-1: SERIAL (zeigt die Verwendung der seriellen Schnittstelle für Verbindungen über den Layer 'V.24_DEF' an)



Die Gegenstellenliste mit den Gegenstellen für das Modem an der seriellen Schnittstelle finden Sie auf folgenden Pfaden:

LANconfig: Kommunikation ▶ Gegenstellen ▶ Gegenstellen (ISDN/seriell)

WEBconfig: LCOS-Menübaum ▶ Setup ▶ WAN ▶ Einwahl-Gegenstellen

Wenn Sie für die serielle WAN-Schnittstelle einen Eintrag in der Gegenstellenliste erzeugt haben, kann diese Gegenstelle wie alle anderen auch für Routing und WAN-Verbindungen genutzt werden.

7.15.10 Konfiguration einer Backup-Verbindung auf der seriellen Schnittstelle

Für die Konfiguration einer Backupverbindung über ein Modem an der seriellen Schnittstelle muss zunächst ein Eintrag in der Liste der Einwahl-Gegenstellen angelegt werden, über den die gewünschte Gegenstelle erreicht werden kann. Zusätzlich werden noch folgende Einträge in der Konfiguration des LANCOM benötigt:

- Eintrag in der Backup-Tabelle

  Legen Sie in der Backup-Tabelle einen Eintrag an für die Gegenstelle, die über die Backup-Verbindung abgesichert werden soll. Dieser Gegenstelle ordnen Sie die Gegenstelle zu, die über das Modem an der seriellen Schnittstelle erreicht werden kann.

  Die Backup-Tabelle finden Sie auf folgenden Pfaden:

  LANconfig: Kommunikation ▶ Ruf-Verwaltung ▶ Backup-Tabelle

  WEBconfig: LCOS-Menübaum ▶ Setup ▶ WAN ▶ Backup-Tabelle

- Eintrag in der Polling-Tabelle

  Wenn die Erreichbarkeit für die zu sichernde Gegenstelle nicht über LCP-Polling (nur bei PPP) geprüft werden kann, legen Sie zusätzlich noch einen Eintrag in der Polling-Tabelle an. Darin ordnen Sie der Gegenstelle eine IP-Adresse zu, deren Erreichbarkeit regelmäßig mit einem Ping-Befehl geprüft wird. Als IP-Adresse wählen Sie dabei üblicherweise einen Rechner direkt am Ende der zu prüfenden Verbindung, z.B. einen DNS-Server im Netz Ihres Providers.

  Die Polling-Tabelle finden Sie auf folgenden Pfaden:

LANconfig: Kommunikation ▶ Gegenstellen ▶ Polling-Tabelle

WEBconfig: LCOS-Menübaum ▶ Setup ▶ WAN ▶ Polling-Tabelle

7.15.11 Kontaktbelegung des LANCOM Modem Adapter Kits

LANCOM-Signal	D-Sub9-Stecker	LANCOM- oder Modemsignal	D-Sub9-Stecker
TxD	3	RxD	2
RxD	2	TxD	3
RTS	7	CTS	8
CTS	8	RTS	7
DTR	4	DCD	1
DCD	1	DTR	4
GND	5	GND	5

7.16 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 LANCOM in der PPP-Verhandlung eine zulässige MTU aus, also die maximale Größe eines unfragmentierten Datenpakets. Diese MTU wird dann von Seiten des LANCOM 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.

7.16.1 Konfiguration

WEBconfig: LCOS-Menübaum ▶ Setup ▶ WAN ▶ MTU-Liste

Die Tabelle enthält folgende Einträge:

- Gerätename: Name der Gegenstelle. Es kann eine physikalische oder eine virtuelle (PPTP/VPN) Gegenstelle sein

- MTU: Auf der Verbindung zu verwendende MTU

7.16.2 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.

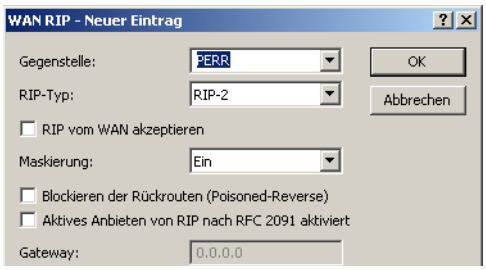
MTU-Liste und MTU-Statistik existieren nur auf Geräten mit DSL oder ADSL-Interface.

7.17 WAN-RIP

Um die über RIP gelernten Routen auch über das WAN bekannt zu machen, können die entsprechenden Gegenstellen in der WAN-RIP-Tabelle eingetragen werden. Die WAN-RIP Tabelle enthält folgende Werte:

- **Peer**: In der Spalte Peer wird der Name der Gegenstelle angegeben.
- **RIP-Type**: Die Spalte RIP-Type gibt an, mit welcher RIP-Version die lokalen Routen propagiert werden
- **RIP-Accept**: In der Spalte RIP-Accept wird angegeben, ob RIP aus dem WAN akzeptiert wird. Dazu muss gleichzeitig der RIP-Typ gesetzt sein.
- **Masquerade**: In der Spalte Masquerade wird angegeben ob und wie auf der Strecke maskiert wird. 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).
- **Dft-Rtg-Tag**: In der Spalte Dft-Rtg-Tag steht das für die WAN-Verbindung geltende „Default-Routing-Tag". Alle ungetaggten Routen werden beim Versenden im WAN mit diesem Tag getaggt.
- **Rtg-Tag-List**: In der Spalte Rtg-Tag-List steht eine kommaseparierte Liste der Tags, die auf dem Interface akzeptiert werden. Wenn diese Liste leer ist, dann werden alle Tags akzeptiert. Steht mindestens ein Tag in der Liste, dann werden nur die Tags in dieser Liste akzeptiert. Ebenso werden beim Senden von getaggten Routen auf das WAN nur Routen mit erlaubten Tags propagiert.

  Alle vom WAN gelernten Routen werden intern als ungetaggte Routen behandelt und auf das LAN mit dem Default-Tag (0) propagiert. Auf das WAN hingegen werden sie mit dem Tag propagiert, mit dem sie auch gelernt wurden.



LANconfig: IP-Router ▶ Allgemein

WEBconfig: LCOS-Menübaum ▶ Setup ▶ IP-Router ▶ RIP ▶ WAN-Sites

7.18 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.

7.18.1 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.

7.18.2 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.

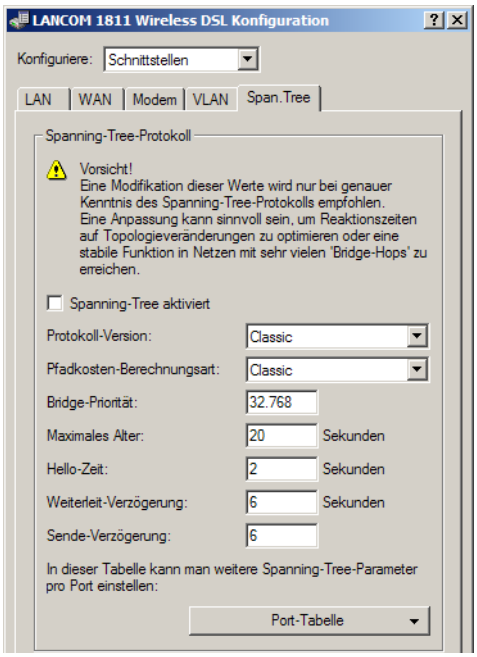
RSTP ermöglicht es dem Administrator darüber hinaus, Informationen über die Topologie des Netzwerk zu konfigurieren:

- 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 Ports 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.

7.18.3 Konfiguration des Spanning-Tree-Protokolls

Zur Konfiguration der RSTP- bzw. STP-Funktion im LANCOM stehen folgende Parameter bereit:



LANconfig: Schnittstellen ▶ Span. Tree

WEBconfig: LCOS-Menübaum ▶ Setup ▶ LAN-Bridge ▶ Spanning-Tree

Allgemeine Parameter

■ **Spanning-Tree aktiviert**

Bei ausgeschaltetem Spanning Tree verschickt ein LANCOM 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.

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

7.18.4 Statusmeldungen über das Spanning-Tree-Protokoll

Die aktuellen Werte des STP können im LAN-Bridge-Status über Telnet oder Browser eingesehen werden.

WEBconfig: LCOS-Menübaum ▶ Status ▶ LAN-Bridge ▶ Spanning-Tree

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.

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.

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.

7.19 Die Aktions-Tabelle

7.19.1 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.

7.19.2 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. "MyLANCOM.dynDNS.org").

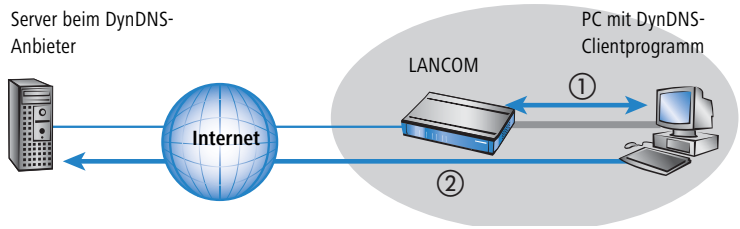
Der Vorteil liegt auf der Hand: Wenn Sie z.B. eine Fernwartung über WEBconfig/HTTP durchführen wollen, dann brauchen Sie lediglich den Dynamic DNS-Namen zu kennen. Außerdem können die DynDNS-Namen auch zum Aufbau von VPN-Verbindungnen zwischen Gegenstellen mit wechselnden IP-Adressen genutzt werden.

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 LANCOM 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.

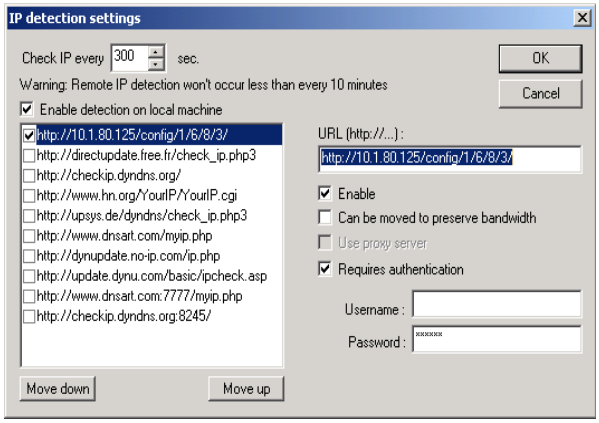
Dynamic-DNS-Client auf der Workstation

Dynamic DNS Anbieter unterstützen eine Reihe von PC-Clientprogrammen, die über verschiedene Methoden die aktuell zugewiesene IP-Adresse eines LANCOMs ermitteln können ①, und im Falle einer Änderung an den jeweiligen Dynamic DNS Server übertragen ②.



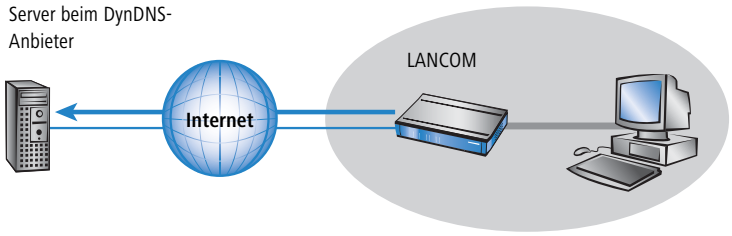
Die aktuelle WAN-seitige IP-Adresse eines LANCOMs kann unter folgender Adresse ausgelesen und dann in ein geeignetes Clientprogramm eingetragen werden:

```
http://<Adresse des LANCOM>/config/1/6/8/3/
```



Dynamic-DNS-Client im LANCOM über HTTP

Alternativ kann das LANCOM die aktuelle WAN-IP auch direkt an den DynDNS-Anbieter übertragen:

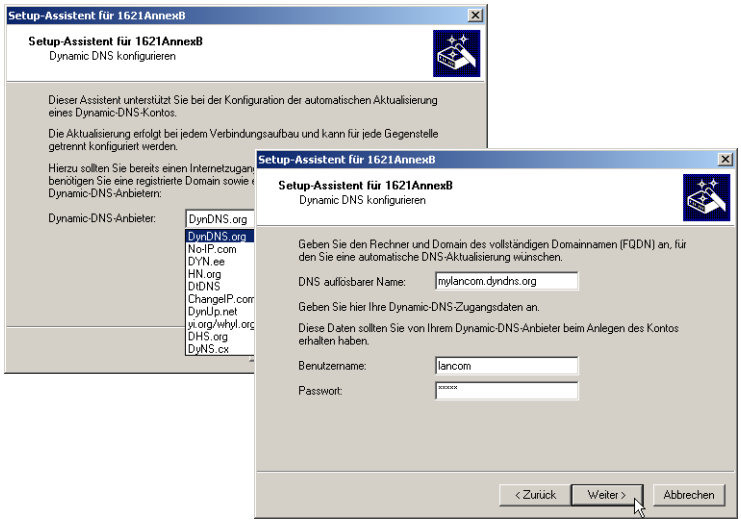


Dazu wird eine Aktion definiert, die z. B. nach jedem Verbindungsaufbau automatisch eine HTTP-Anfrage an den DynDNS-Server sendet, dabei die benötigten Informationen über das DynDNS-Konto übermittelt und so ein Update der Registrierung auslöst. Eine solche HTTP-Anfrage an den Anbieter DynDNS.org sieht 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 LANCOMs 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 anbieter-spezifische Parameter, die hier nicht näher beschrieben werden. Außerdem legt der Setup-Assistent weitere Aktionen an, mit denen das Verhalten des LANCOMs gesteuert wird für den Fall, dass die Aktualisierung nicht im ersten Durchlauf erfolgreich durchgeführt werden konnte.

Dynamic-DNS-Client im LANCOM 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 LANCOM 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 (3945 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 LANCOMs (%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 LANCOMs ausgewertet werden, um bei Bedarf weitere Aktionen einzuleiten.

7.19.3 Weitere Beispiele für Aktionen

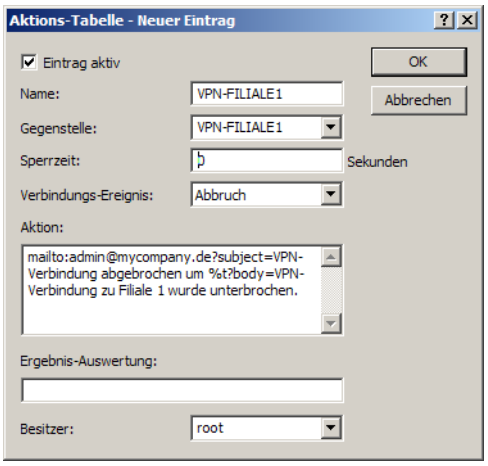
Information über Verbindungsabbruch als SMS auf Mobiltelefon melden

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 LANCOM 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.

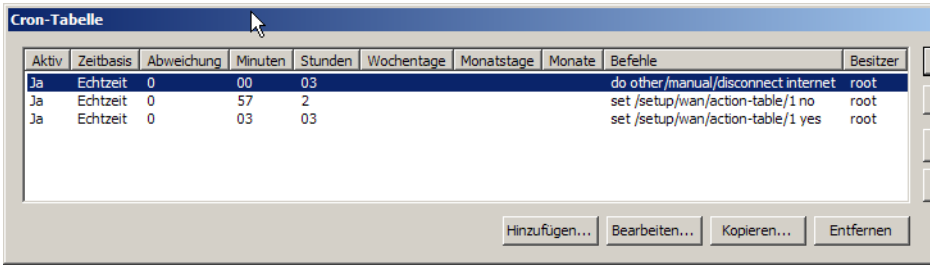
In einem komplexen Aufbau mit mehreren Filialen wird im LANCOM der Zentrale für jede Gegenstelle ein passender Eintrag angelegt. Zur Überwachung der Zentrale selbst wird eine Aktion in einem Gerät in einer der Filialen angelegt. So kann der Administrator auch dann benachrichtigt werden, wenn das VPN-Gateway der Zentrale selbst ausfällt und vielleicht keine Nachricht mehr versenden kann.

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.

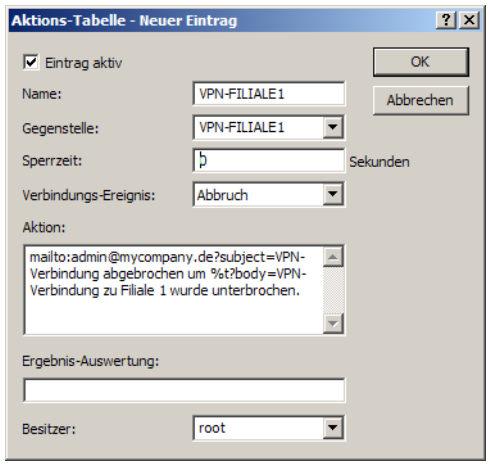


7.19.4 Konfiguration

Änderungen mit LCOS 7.6:

- "Fehler" als Bedingung für den Zustandswechsel der WAN-Verbindung
- "Aufbaufehler" als Bedingung für den Zustandswechsel der WAN-Verbindung
- Unterstützung des GnuDIP-Protokolls

In der Aktions-Tabelle können Sie Aktionen definieren, die ausgeführt werden, wenn sich am Zustand einer WAN-Verbindung etwas ändert.



LANconfig: Kommunikation ▶ Allgemein ▶ Aktions-Tabelle

WEBconfig: Setup ▶ WAN ▶ Aktions-Tabelle

- **Index**

  Der Index gibt die Position des Eintrags in der Tabelle an und muss daher eindeutig sein. Die Einträge der Aktions-Tabelle werden der Reihe nach ausgeführt, sobald der entsprechende Zustandswechsel der WAN-Verbindung eintritt. Mit dem Eintrag im Feld "Pruefen-auf" kann das Überspringen von Zeilen je nach Auswertung der Aktion ausgelöst werden. Der Index legt die Position der Einträge in der Tabelle fest (in aufsteigender Reihenfolge) und beeinflusst somit maßgeblich das Verhalten der Aktionen, wenn die Option "Pruefen-auf" verwendet wird. Über den Index kann außerdem ein Eintrag aus der Aktions-Tabelle über einen Cron-Job angesprochen werden, z. B. um einen Eintrag zu bestimmten Zeiten zu aktivieren oder zu deaktivieren.

- **Aktiv**

  Aktiviert oder deaktiviert diesen Eintrag.

- **Hostname**

  Name der Aktion. Dieser Name kann mit dem Platzhalter %h (Hostname) in den Feldern "Aktion" und "Pruefen-auf" referenziert werden.

- **Gegenstelle**

  Name der Gegenstelle, deren Zustandswechsel die in diesem Eintrag definierte Aktion auslösen soll.

- **Sperrzeit (max. 10 Zeichen)**

  Unterbricht die wiederholte Ausführung der in diesem Eintrag definierten Aktion für die eingestellte Zeit in Sekunden.

- **Bedingung**

  Die Aktion wird ausgeführt, wenn der hier eingestellte Zustandswechsel der WAN-Verbindung eintritt.

  Mögliche Werte:

  - Aufbau – Die Aktion wird ausgeführt, wenn die Verbindung erfolgreich aufgebaut wurde.

- □ Abbau – Die Aktion wird ausgeführt, wenn die Verbindung durch das Gerät selbst beendet wurde (z. B. durch eine manuelle Trennung oder den Ablauf einer Haltezeit).
- □ Ende – Die Aktion wird ausgeführt, wenn die Verbindung beendet wurde (unabhängig vom Grund für den Abbau).
- □ Fehler – Die Aktion wird ausgeführt, wenn die Verbindung beendet wurde, das Gerät selbst aber diesen Abbau nicht ausgelöst oder erwartet hat.
- □ Aufbaufehler – Die Aktion wird ausgeführt, wenn ein Verbindungsaufbau gestartet wurde, die Verbindung aber nicht erfolgreich aufgebaut werden konnte.

■ **Aktion (max. 250 Zeichen)**

Hier beschreiben Sie die Aktion, die beim Zustandswechsel der WAN-Verbindung ausgeführt werden soll. In jedem Eintrag darf nur eine Aktionen ausgeführt werden.

Mögliche Werte für die Aktionen (maximal 250 Zeichen):

- □ exec: – Mit diesem Prefix leiten Sie alle Befehle ein, wie sie an der Telnet-Konsole eingegeben würden. Sie können z. B. mit der Aktion "exec:do /o/m/d" alle bestehenden Verbindungen beenden.
- □ dnscheck: – Mit diesem Prefix leiten Sie eine DNS-Namensauflösung ein. Sie können z. B. mit der Aktion "dnscheck:myserver.dyndns.org" die IP-Adresse des angegebenen Servers ermitteln.
- □ http: – Mit diesem Prefix 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 wird in den folgenden Absätzen beschrieben.
- □ https: – Wie "http:", nur über eine verschlüsselte Verbindung.
- □ gnudip: – Mit diesem Prefix 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
  Der Zeilenumbruch dient nur der Lesbarkeit und wird nicht in die Aktion eingetragen. Die Bedeutung des Platzhalters %a wird in den folgenden Absätzen beschrieben.
- □ repeat: – Mit diesem Prefix und der Angabe einer Zeit in Sekunden werden alle Aktionen mit der Bedingung "Aufbau" wiederholt ausgeführt, sobald die Verbindung aufgebaut ist. Mit der Aktion "repeat:300" werden z. B. alle Aufbau-Aktionen alle fünf Minuten wiederholt.
- □ mailto: – Mit diesem Prefix lösen Sie den Versand einer E-Mail aus. Sie können z. B. mit der folgenden Aktion eine E-Mail an den Systemadministrator versenden, wenn eine Verbindung beendet wurde:
  mailto:admin@mycompany.de?subject=VPN-Verbindung abgebrochen um %t?body=VPN-Verbindung zu Filiale 1 wurde unterbrochen.

Mögliche Variablen zur Erweiterung der Aktionen:

- □ %a – WAN-IP-Adresse der WAN-Verbindung, in deren Kontext diese Aktion ausgeführt wird.
- □ %H – Hostname der WAN-Verbindung, in deren Kontext diese Aktion ausgeführt wird.
- □ %h – wie %h, nur Hostname in Kleinbuchstaben
- □ %c – Verbindungsname der WAN-Verbindung, in deren Kontext diese Aktion ausgeführt wird.
- □ %n – Gerätename
- □ %s – 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.

Das Ergebnis der Aktionen kann im Feld "Pruefen-auf" ausgewertet werden.

Default:

- □ leer

■ **Pruefen-auf**

Das Ergebnis der Aktion kann hier ausgewertet werden, um je nach Ergebnis eine bestimmte Anzahl von Einträge beim Abarbeiten der Aktions-Tabelle zu überspringen.

Mögliche Werte für die Aktionen (maximal 50 Zeichen):

- □ contains= – Dieses Prefix prüft, ob das Ergebnis der Aktion die definierte Zeichenkette enthält.
- □ isequal= – Dieses Prefix 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.

Mögliche Variablen zur Erweiterung der Aktionen:

- □ Wie bei der Definition der Aktion.

Beispiel:

- □ Mit einem DNS-Check wird die IP-Adresse einer Adresse der Form "myserver.dyndns.org" abgefragt. Mit der Prüfung "contains=%a?skipiftrue=2" können die beiden folgenden Einträge der Aktions-Tabelle übersprungen werden, 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 die Aktion nicht ausgeführt werden.

7.20 Verwendung der seriellen Schnittstelle im LAN

7.20.1 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 LANCOM-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 LANCOM 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.

7.20.2 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.

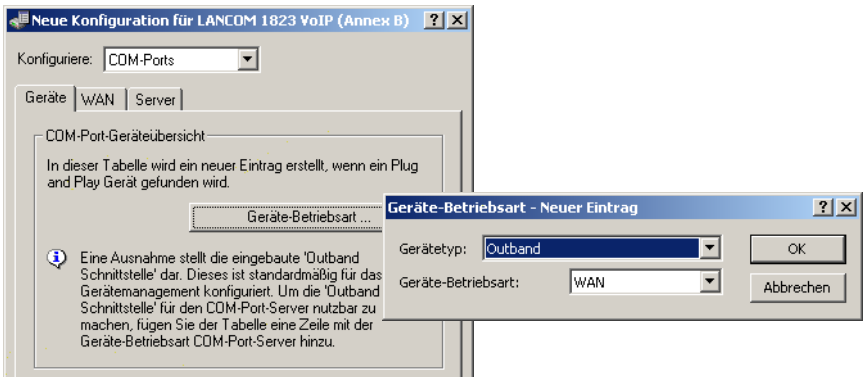
In beiden Fällen wird eine transparente Verbindung zwischen der seriellen Schnittstelle und der TCP-Verbindung hergestellt: Datenpakete, die auf der seriellen Schnittstelle empfangen werden, werden auf der TCP-Verbindung weitergeleitet und umgekehrt. Eine häufige Anwendung im Server-Modus ist die Installation 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.

7.20.3 Konfiguration der seriellen Schnittstellen

Die seriellen Schnittstellen können im LANCOM 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: COM-Ports ▶ Geräte ▶ Geräte Betriebsart



Telnet: Setup ▶ COM-Ports ▶ Geräte

- **Device-Type**

  Auswahl aus der Liste der im Gerät verfügbaren seriellen Schnittstellen.

- **Dienst**

  Aktivierung des Ports für den COM-Port-Server.

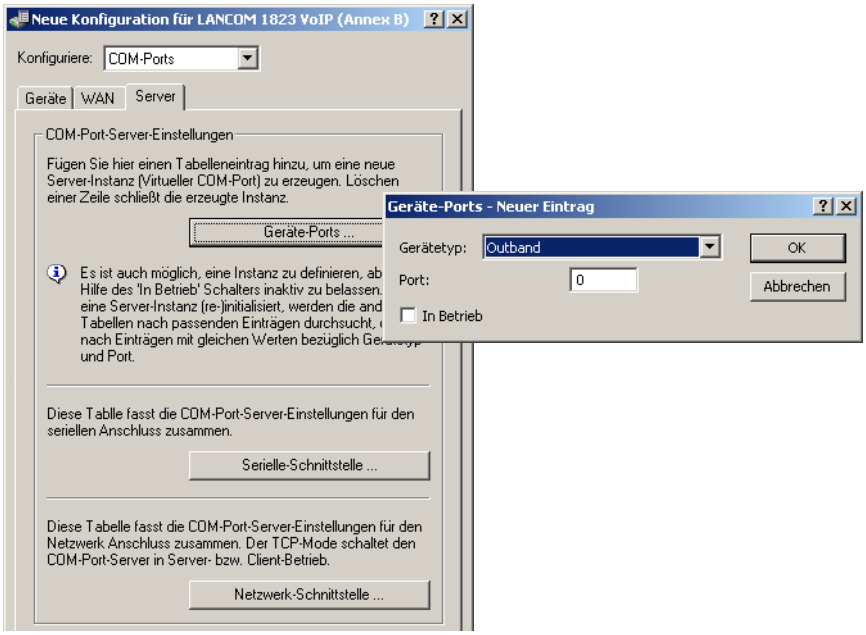
7.20.4 Konfiguration des COM-Port-Servers

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.

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 Operating 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 Device-Type und Port-Nummer durchsucht. Falls kein passender Eintrag gefunden wird, verwendet die Server-Instanz sinnvolle Default-Werte.



LANconfig: COM-Ports ▶ Server ▶ Geräte Ports

WEBconfig: Setup ▶ COM-Ports ▶ COM-Port-Server ▶ Geraete

- **Device-Type**

  Auswahl aus der Liste der im Gerät verfügbaren seriellen Schnittstellen.

- **Port-Nummer**

  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.

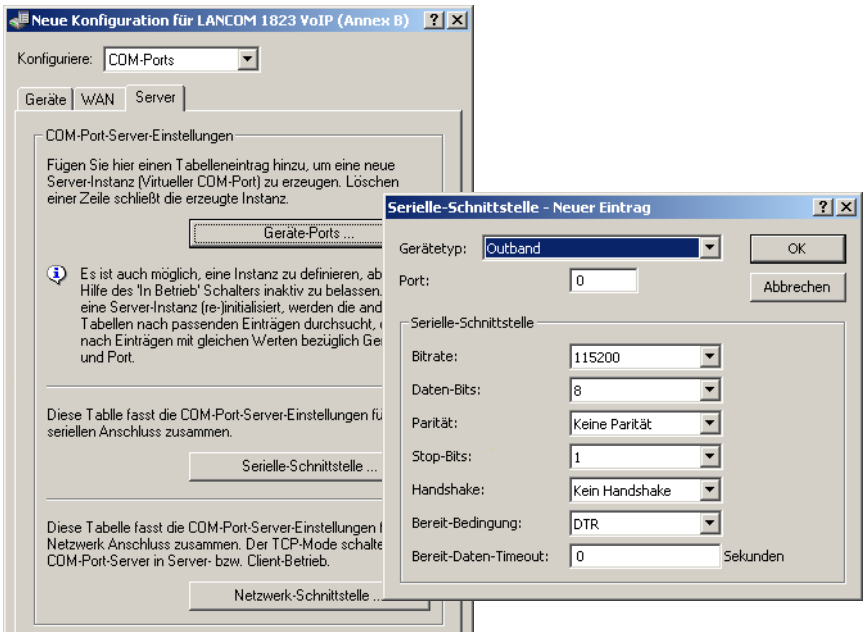
- **Operating**

  Aktiviert den COM-Port-Server auf dem gewählten Port der gewählten Schnittstelle.

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 RFC2217-Verhandlung aktiviert ist; die aktuellen Einstellungen können im Status-Menü eingesehen werden.



LANconfig: COM-Ports ▶ Server ▶ Serielle Schnittstelle

WEBconfig: Setup ▶ COM-Ports ▶ COM-Port-Server ▶ COM-Port-Einstellungen

- **Device-Type**

  Auswahl aus der Liste der im Gerät verfügbaren seriellen Schnittstellen.

- **Port-Nummer**

  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.

- **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.

■ **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".

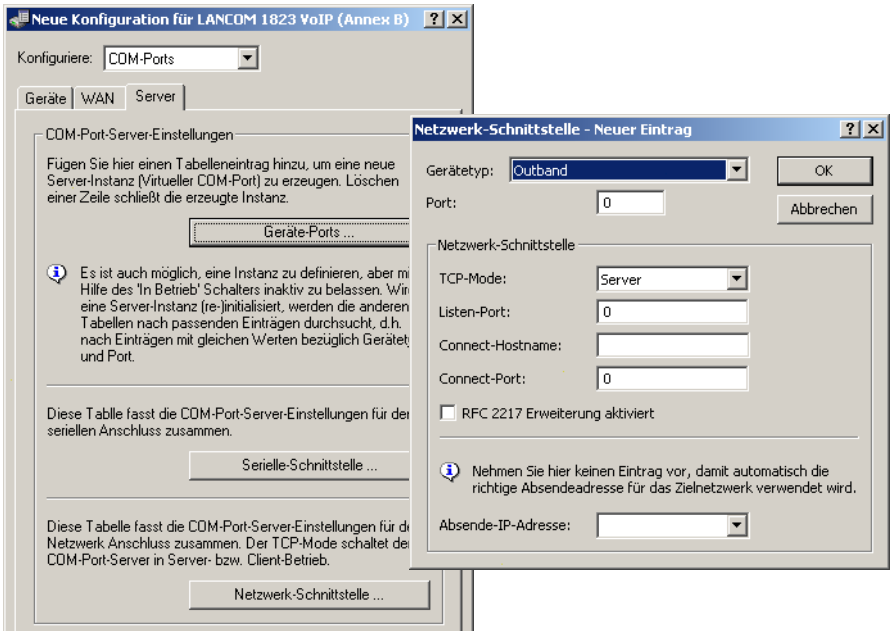
■ **Bereit-Daten-Timeout**

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.

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 RFC2217-Verhandlung aktiviert ist; die aktuellen Einstellungen können im Status-Menü eingesehen werden.



LANconfig: COM-Ports ▶ Server ▶ Netzwerk-Schnittstelle

WEBconfig: Setup ▶ COM-Ports ▶ COM-Port-Server ▶ Netzwerk-Einstellungen

■ **Device-Type**

Auswahl aus der Liste der im Gerät verfügbaren seriellen Schnittstellen.

■ **Port-Nummer**

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-Modus**

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 LANCOM die offenen Verbindungen bei einem Neustart des Gerätes.

■ **Listen-Port**

Auf diesem TCP-Port erwartet der COM-Port im TCP-Server-Modus eingehende Verbindungen.

- **Aufbau-Host-Name**

  Zu diesem Host baut der COM-Port im TCP-Client-Modus eine Verbindung auf, sobald sich der Port im Zustand "Bereit" befindet.

- **Aufbau-Port**

  Über diesen TCP-Port baut der COM-Port im TCP-Client-Modus eine Verbindung auf, sobald sich der Port im Zustand "Bereit" befindet.

- **Loopback-Adresse**

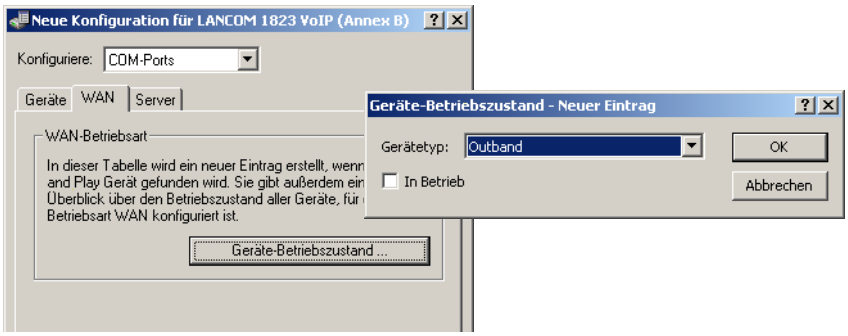
  Über diese Adresse kann der COM-Port angesprochen werden. Dies ist die eigene IP-Adresse, die als Quelladresse beim Verbindungsaufbau benutzt wird. Sie wird z.B. verwendet, um die IP-Route festzulegen, über die die Verbindung aufgebaut wird.

- **RFC2217-Erweiterungen**

  Die RFC2217-Erweiterungen können für beide TCP-Modi aktiviert werden. Wenn diese Erweiterungen eingeschaltet sind, signalisiert ein LANCOM 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 RFC2217-Erweiterungen ist auch bei nicht kompatibler Gegenstelle unkritisch, möglicherweise werden dann unerwartete Zeichen bei der Gegenstelle angezeigt. Als Nebeneffekt führt die Verwendung der RFC2217-Erweiterungen dazu, dass der Port einen regelmäßigen Alive-Check durchführt, indem Telnet-NOPs zur Gegenstelle gesendet werden.

7.20.5 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: COM-Ports ▶ WAN ▶ Geräte-Betriebszustand

WEBconfig: Setup ▶ COM-Ports ▶ WAN ▶ Geraete

- **Device-Type**

  Liste der im Gerät verfügbaren seriellen Schnittstellen.

- **Aktiv**

  Status des angeschlossenen Gerätes:

7.20.6 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.

Netzwerk-Status

Telnet: 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.

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 LANCOMs 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.

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.

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.

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.

Delete-Values

Diese Aktion löscht alle Werte in den Status-Tabellen.

7.20.7 COM-Port-Adapter

Zum Anschluss von Geräten mit seriellen Schnittstellen an ein LANCOM stehen folgende Möglichkeiten bereit:

Adapter	LANCOM-Geräte
COM-Port-Adapter	Alle mit serieller Konfigurationsschnittstelle
USB-Seriell-Adapter	Alle mit USB-Schnittstelle
CardBus-Seriell-Adapter	Alle mit CardBus-Einschub
LANCOM Modem-Adapter-Kit	Alle mit serieller Konfigurationsschnittstelle

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

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 LANCOM 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 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 Referenz-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. Im LANCOM 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' → Seite 8-32 und 'Schutz vor "Denial-of-Service"-Angriffen' → Seite 8-33.

8.2.1 Die Aufgaben einer Firewall

Prüfung der Datenpakete

Wie überwacht die Firewall den Datenverkehr? Im Prinzip arbeitet die Firewall wie ein Türwächter 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 anderen Netzwerk-Konstellationen übertragen, z.B. für den Schutz eines Subnetzes der Personalabteilung in einem Unternehmen gegen die restlichen Netzwerkbenutzer.

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.

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:

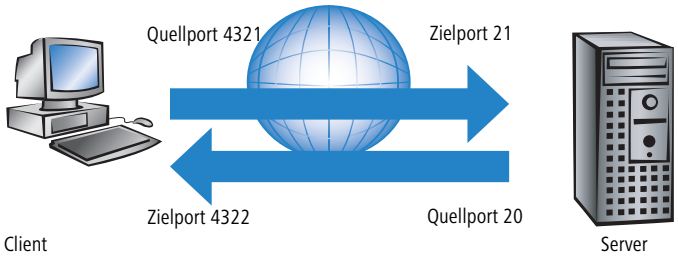
- IP-Adresse von Quelle und Ziel
- Übertragungsprotokoll (TCP, UDP oder ICMP)
- Portnummern von Quelle und Ziel
- MAC-Adresse

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 Kommunkation 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.

Stateful-Packet-Inspection

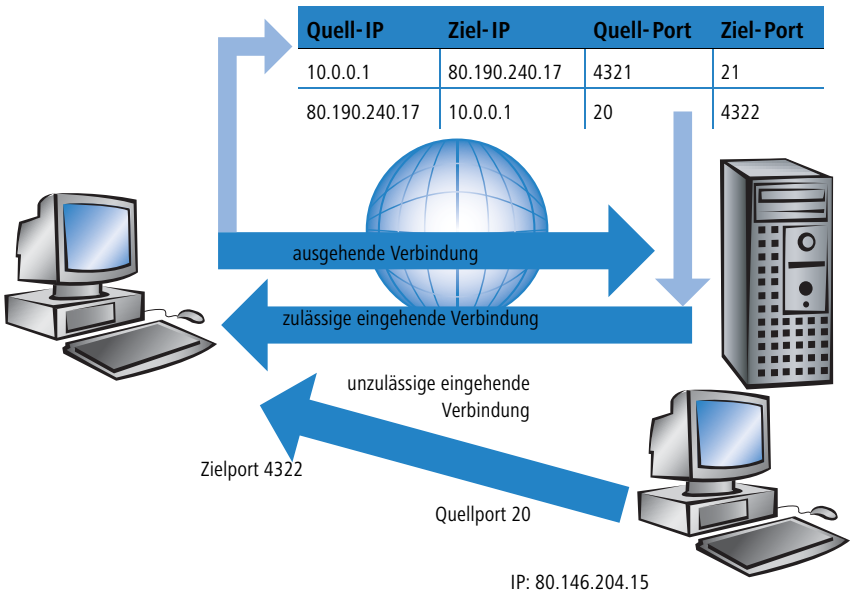
Die Stateful-Packet-Inspection (SPF) oder kurz Stateful Inspection erweitert den Ansatz der Paketfilter um eine Prüfung weiterer Verbindungsinformationen. Neben der eher statischen Tabelle mit den zugelassenen Ports und Adressbereichen wird bei dieser Variante eine dynamische Tabelle gepflegt, in die 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.

Stateful Inspection: richtungsabhängige Prüfung

Die Filter-Regeln einer Stateful-Inspection Firewall sind - anders als bei klassischen Portfilter-Firewalls - richtungsabhängig: Eine Verbindung kann immer von nur 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, H.245 und H.323 (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!

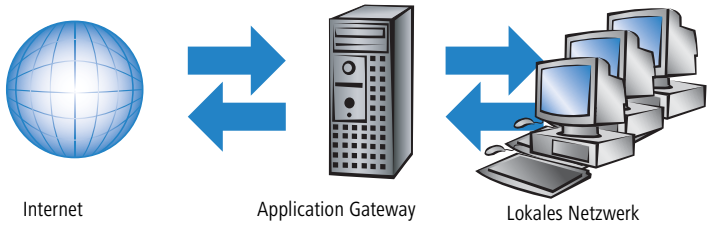
Nach der erfolgreichen Datenübertragung verschwinden die Einträge automatisch wieder aus der dynamischen Tabelle, die Ports werden also wieder geschlossen.

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.

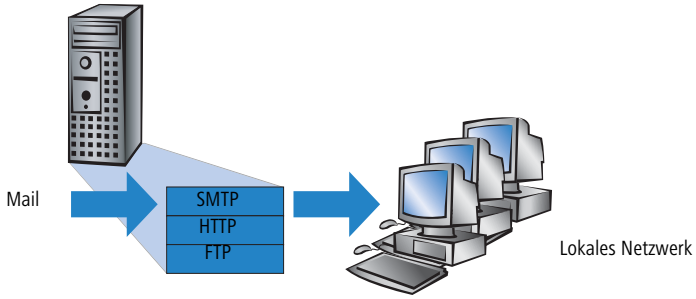
Application Gateway

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 LANCOM aufgrund der hohen Anforderungen an die Hardware nicht unterstützt.

8.3 Die Firewall im LANCOM

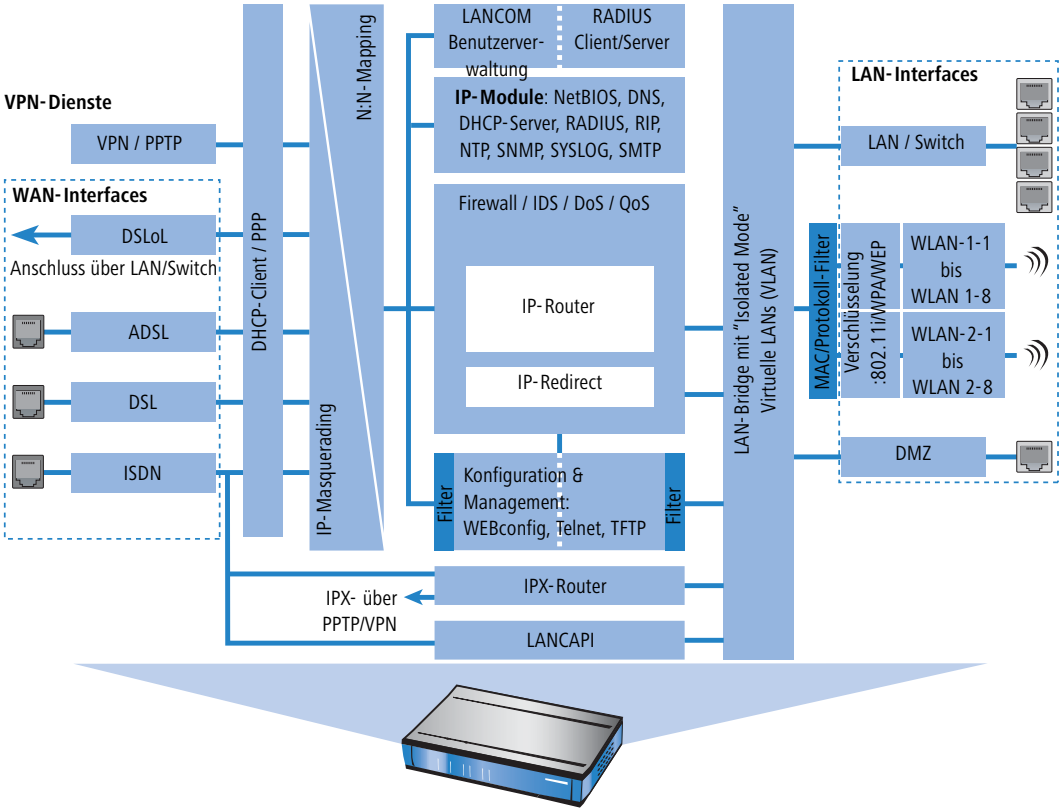
Nach den allgemeinen Erläuterungen zu den Gefahren aus dem Internet sowie den Aufgaben und Typen von Firewalls finden sich in diesem Kapitel Beschreibungen zu den speziellen Funktionen der Firewall im LANCOM und Hinweise auf die konkrete Konfiguration.

Bei LANCOM-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 LANCOM die Datenpakete

Die Firewall filtert aus dem gesamten Datenstrom, der über den IP-Router des LANCOM läuft, diejenigen Datenpakete heraus, für die eine bestimmte Behandlung vorgesehen ist.

Die Firewall prüft nur geroutete Datenpakete!



Die Firewall prüft nur die Datenpakete, die vom IP-Router im LANCOM 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 (alternativ: 'WLAN-Routing (Isolierter Modus)' → Seite 11-50). Hier wirken also auch nicht die Regeln der Firewall. Gleiches gilt für die so genannten "internen Dienste" des LANCOM 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 LANCOM.

Die Firewall im LANCOM 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

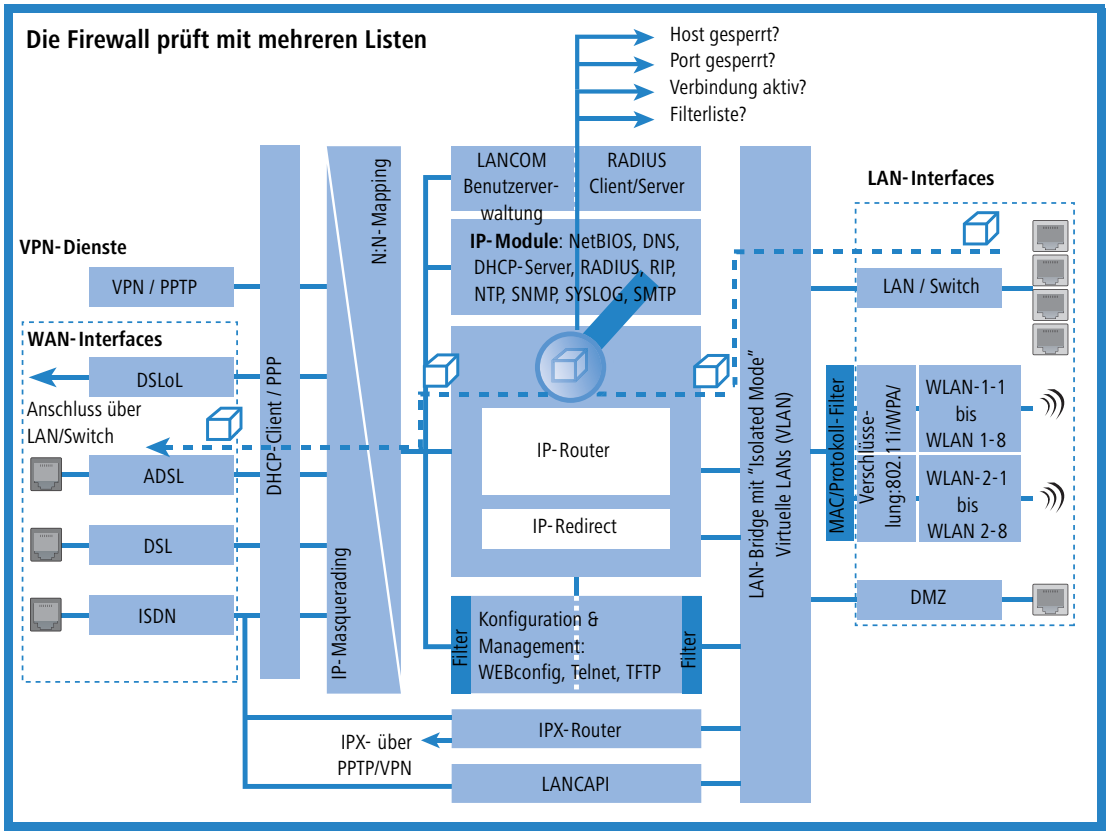
Und so setzt die Firewall die Listen ein, wenn ein Datenpaket über den IP-Router geleitet werden soll:

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/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' → Seite 8-20.

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' → Seite 8-12).

8.3.2 Besondere Protokolle

Ein wichtiger Punkt bei der Verbindungsüberwachung ist die Behandlung von Protokollen, die dynamisch Ports und / oder Adressen aushandeln, über die die weitere Kommunikation passiert. Beispiele für diese Protokolle sind FTP, H.323 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' → Seite 8-3).

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/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 senden (z.B. TFTP) 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	Ack/Data →	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 LANCOM 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.

TCP-Verbindungen

TCP-Verbindungen können nicht einfach nur durch die Prüfung der Ports nachgehalten werden. Bei einigen Protokollen wie z.B. FTP, PPTP oder H.323 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.

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.

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 (→ Seite 8-10)
- Fragmente (→ Seite 8-10)
- Sitzungswiederherstellung (→ Seite 8-10)
- Ping-Block (→ Seite 8-11)
- Stealth-Modus (→ Seite 8-11)
- Authentifizierungs-Port tarnen (→ Seite 8-12)

Firewall/QoS-Aktivierung

Mit dieser Option wird die gesamte Firewall inklusive der Quality-of-Service-Funktionen ein- bzw. ausgeschaltet.

Bitte beachten Sie, dass die Funktionen des N:N-Mapping ('N:N-Mapping' → Seite 7-31) nur wirksam sind, wenn die Firewall eingeschaltet ist!

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.

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 wie im LANCOM gehört auch die Fähigkeit, fragmentierte Pakete zu Re-assemblieren (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 re-assemblierte Paket wird dann nach den gültigen Filtereinstellungen geprüft und entsprechend behandelt.

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 erneuern.

Manchmal werden die Verbindungen gemäß den allgemeinen Aging-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 ('Advanced Routing and Forwarding' → Seite 7-9) 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

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 LANCOM die Antworten auf diese Anfragen unterdrücken.

Um dies zu erreichen, kann das LANCOM angewiesen werden, ICMP-Echo-Requests nicht mehr zu beantworten. Gleichzeitig werden auch die bei einem "traceroute" benutzten TTL-Exceeded Meldungen unterdrückt, so dass das LANCOM 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' → Seite 8-10.

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 LANCOM 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' → Seite 8-12).

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' → Seite 8-10.

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 verzögern 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 LANCOM zu sehen.

Das LANCOM 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 Newsservers (NNTP) für eine kurze Zeit (20 Sekunden) ident-Anfragen von den jeweiligen Servern abgelehnt.

Ist die Zeit abgelaufen, so wird der Port wieder versteckt.

8.3.4 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.

Informationen zur konkreten Definition der Firewall-Regeln mit den verschiedenen Konfigurationstools (LANconfig, WEBconfig oder Telnet) finden Sie im Kapitel 'Konfiguration der Firewall-Regeln' → Seite 21.

Die Komponenten einer Firewall-Regel

Eine Firewall-Regel wird zunächst bestimmt durch ihren Namen und einige weitere Optionen:

- **Ein-/Ausschalter**: Ist die Regel aktiv?
- **Priorität**: Mit welcher Priorität wird die Regel bearbeitet? (→ Seite 8-12)
- **Verknüpfung**: Sollen weitere Firewall-Regeln beachtet werden, wenn diese Regel für ein Datenpaket zutrifft? (→ Seite 8-12)
- **VPN-Regel**: Wird die Firewall-Regel auch zur Erzeugung von VPN-Regeln verwendet? (→ Seite 8-13)
- **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 ('Policy-based Routing' → Seite 7-3).

Priorität

Das LANCOM 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' → Seite 8-27 beschrieben.

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 Abtei-

lungen 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.

VPN-Regeln

Eine VPN-Regel bezieht die Informationen über Quell- und Ziel-Netz u.a. aus den Firewall-Regeln.

Mit dem Aktivieren der Option "VPN-Regel" für eine Firewall-Regel wird festgelegt, dass aus dieser Firewall-Regel eine VPN-Regel abgeleitet wird.

Bei der Verwendung von mehreren lokalen Netzwerken, siehe auch ARF, (→ Seite 7-9), muss die automatische Erzeugung der VPN-Regeln für jedes Netzwerk gezielt eingestellt werden. Zur Definition der Netzwerke mit automatischer VPN-Regel-Erzeugung wird das Schnittstellen-Tag verwendet, das für jedes Netzwerk angegeben ist. Über dieses Tag ist eine Zuordnung von lokalem Netz zur VPN-Route möglich: Jedes auf einem lokalen Interface empfangene Paket wird mit dem Schnittstellen-Tag markiert und auf eine Route mit dem selben Tag oder dem Default-Tag (0) weitergeleitet.

Für die automatische VPN-Regel-Erzeugung werden nun alle Netzwerke aufgenommen, die

- das Tag '0' haben oder
- die beiden folgenden Bedingungen erfüllen:
  - Das Netzwerk hat das gleiche Schnittstellen-Tag wie der zur VPN-Verbindung gehörende Eintrag in der IP-Routing-Tabelle (nicht zu verwechseln mit dem Routing-Tag für das remote Gateway)
  - Das Netzwerk ist vom Typ 'Intranet'



VPN-Regeln für eine DMZ müssen manuell ebenso erstellt werden wie für Netzwerke, deren Schnittstellen-Tag nicht zum Routing-Tag der VPN-Route passt.

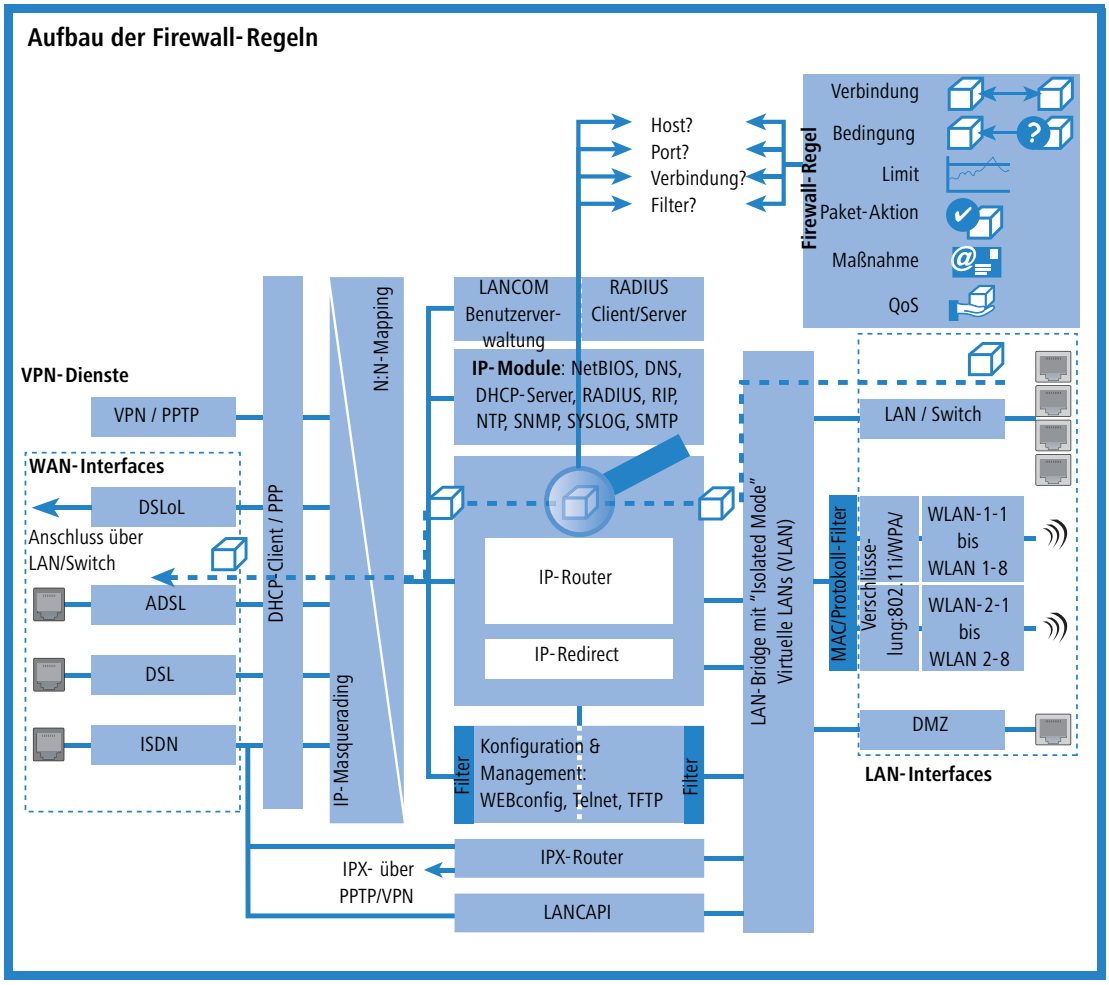
Anwendung der Firewall-Regel

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? (→ Seite 8-14)
- **Bedingung**: Ist die Wirksamkeit der Regel durch Bedingungen eingeschränkt? (→ Seite 8-15)
- **Limit (Trigger)**: Beim Erreichen welcher Schwellwerte soll die Regel anspringen? (→ Seite 8-15)
- **Paket-Aktion**: Was soll mit den Datenpaketen passieren, wenn die Bedingung erfüllt und das Limit erreicht sind? (→ Seite 8-15)
- **Sonstige Maßnahmen**: Sollen neben der Paket-Aktion noch weitere Maßnamen eingeleitet werden? (→ Seite 8-15)
- **Quality of Service (QoS)**: Werden Datenpakete bestimmter Anwendungen oder mit entsprechenden Markierungen durch die Zusicherung von speziellen Dienstgütern besonders bevorzugt? (→ Seite 8-16)

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 LANCOM die Datenpakete' → Seite 8-6 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:



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[1]-Adressen
- Bereiche von IP-Adressen
- Komplette IP-Netzwerke

Hostnamen können nur dann verwendet werden, wenn das LANCOM die Namen in IP-Adressen auflösen kann. Dafür muss das LANCOM die Namen über DHCP oder NetBIOS 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.

1. 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.

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 LANCOM schon vordefiniert, andere können je nach Bedarf zusätzlich angelegt werden.



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



Limit (Trigger)

Das Limit (oder auch Trigger) bezeichnet einen quantifizierten Schwellwert, 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 Schwellwert 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.



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 entsprechenden Nachricht über ICMP.



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-Ereignistabelle.

- **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.



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.



Weitere Informationen zu den QoS und der entsprechenden Konfiguration finden Sie im Kapitel 'Quality-of-Service' → Seite 9-1.

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 ▶ SYSLOG

WEBconfig: LCOS-Menübaum ▶ Setup ▶ Mail bzw. LCOS-Menübaum ▶ 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.

Benachrichtigung per SYSLOG

Wenn die Portfilter-Firewall ein entsprechendes Paket verwirft, wird über Syslog (siehe auch 'Einrichten des SYSLOG-Moduls' → Seite 16-23) 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 LANCOM 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;
```

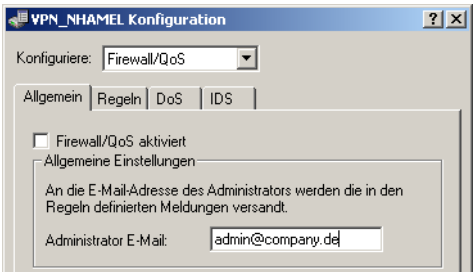
Benachrichtigung per E-Mail

Ist das E-Mail-System des LANCOM 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: LANCOM_Firewall@MyCompany.com
TO: Administrator@MyCompany.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
```

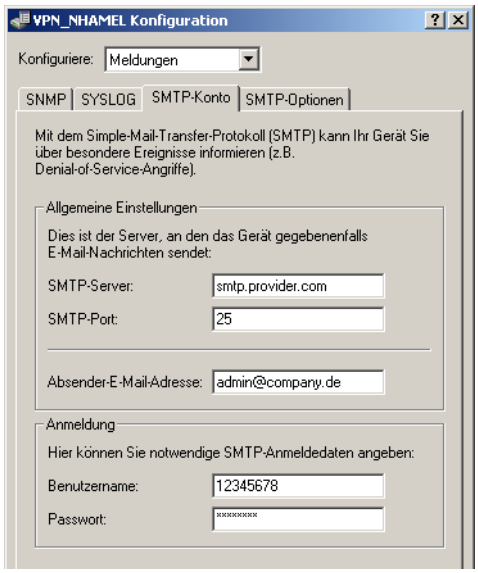
Damit der Mailversand aus dem LANCOM an den Administrator funktioniert, muss die E-Mailadresse des Empfängers richtig eingetragen sein.



LANconfig: Firewall/QoS ▶ Allgemein

WEBconfig: LCOS-Menübaum ▶ Setup ▶ IP-Router ▶ Firewall

Außerdem muss ein Mail-Postfach eingerichtet sein, über das die E-Mail verschickt werden kann.



LANconfig: Meldungen ▶ SMTP

WEBconfig: LCOS-Menübaum ▶ Setup ▶ SMTP ▶ Firewall

Benachrichtigung per SNMP-Trap

Wenn als Benachrichtigungsmethode das Versenden von SNMP-Traps aktiviert wurde (siehe auch 'SNMP' → Seite 3-39), 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 LANCOM 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.

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.

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.

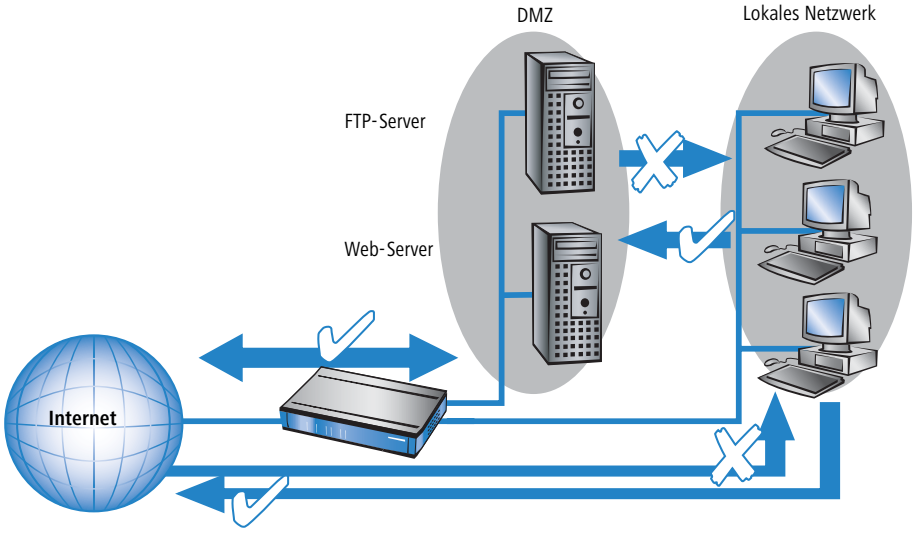
Firewall mit DMZ

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 Rech-

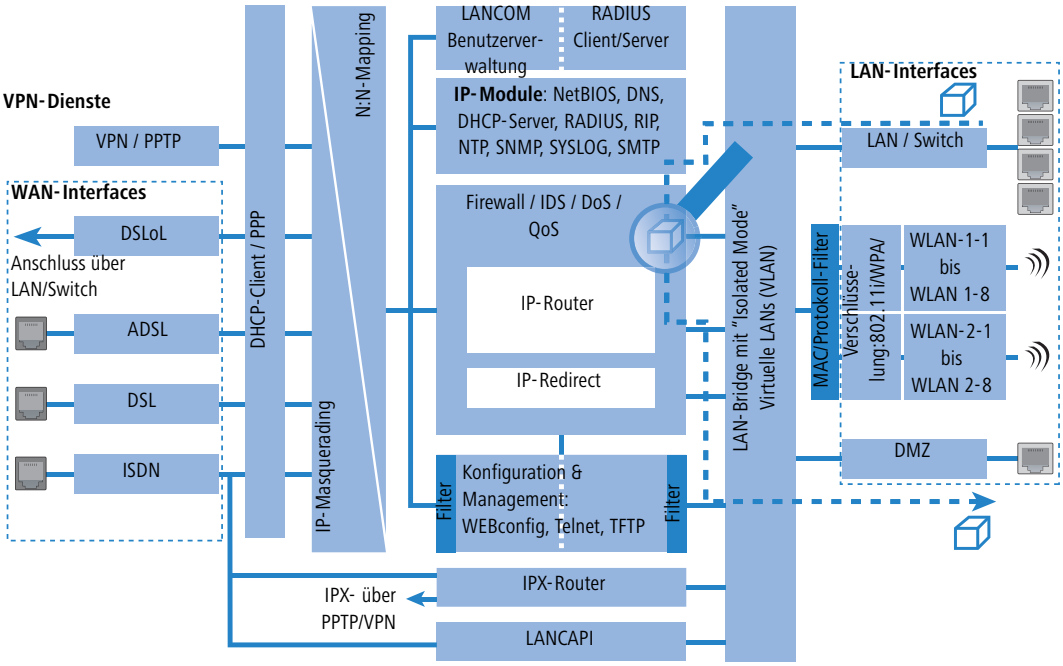
ner positioniert, auf die aus dem unsicheren Netz (Internet) direkt zugegriffen werden soll. Dazu gehören z.B. die eigenen FTP- und Web-Server.

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 LANCOM-Modelle unterstützen diesen Aufbau durch eine separate LAN-Schnittstelle, die nur für die DMZ verwendet wird. Betrachtet man den Weg der Daten durch das LANCOM, 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 LANCOM 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 LANCOM 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 LANCOM-Geräten mit integrierter oder nachträglich über Software-Option freigeschalteter VoIP-Funktion werden die für die Voice-Verbindungen benötigen Ports automatisch freigeschaltet!

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.

Das LANCOM kann durch den integrierten NetBIOS-Proxy auch für Netzwerkkopplungen diese unerwünschten Verbindungsaufbauten verhindern, indem es selbst solange eine Antwort für die betreffende Ressource vortäuscht, bis ein tatsächlicher Zugriff erfolgt.

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 LANCOM 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.

Firewall-Regeln mit Scripten übertragen

Firewall-Regeln können einfach und komfortabel mittels Scripten über Geräte- und Softwareversionen hinweg übertragen werden ('Scripting' → Seite 4-1). Explizite Beispielscripte finden sich in der LANCOM KnowledgeBase unter www.lancom.de/support.

Sofern Sie in Ihrem LAN einen Server betreiben, der über Einträge in der Servicetabelle für Zugriffe aus dem Internet freigegeben ist (siehe 'IP-Masquerading' → Seite 7-17), 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.

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.

Deny-All: Die wichtigste Regel der Firewall!

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 "vergessen" 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 LANCOM 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 und "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 LANOM (alternativ: Lokales Netzwerk)	Übertragen	DNS
DENY_ALL	Alle Stationen	Alle Stationen	Zurückweisen	ANY

■ Sofern Sie VPN-Einwahl auf ein LANCOM 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 LANCOM selbst terminiert wird (z.B. VPN-Client im lokalen Netz, oder LANCOM 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

■ Sofern Sie ISDN-Einwahl oder V.110-Einwahl (z.B. per HSCSD-Handy) gestatten, müssen Sie die betreffende Gegenstelle freischalten (siehe auch 'Die Konfiguration von Gegenstellen' → Seite 7-15):

Regel	Quelle	Ziel	Aktion	Dienst
ALLOW_DIAL_IN	Gegenstellenname	Lokales Netzwerk	Übertragen	ANY

■ 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 einen 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. 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.

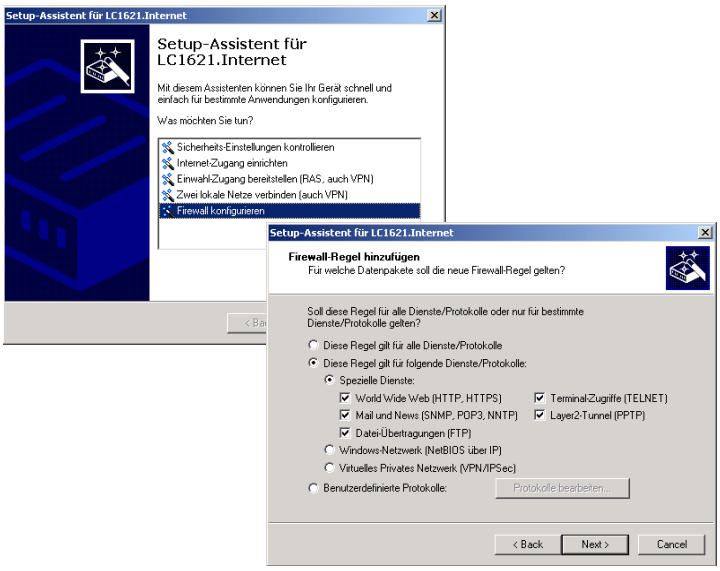


Das LANCOM nimmt beim Aufbau der Filterliste eine automatische Sortierung der Firewall-Regeln vor. Dies geschieht dadurch, dass die Regeln anhand ihres Detaillierungsgrades sortiert in die Filterliste eingetragen werden. Zunächst werden alle spezifischen Regeln beachtet, danach die allgemein (z.B. Deny-All). Prüfen Sie bei komplexen Regelwerken die Filterliste, wie im nachfolgenden Abschnitt beschrieben.

8.4 Konfiguration der Firewall mit LANconfig

8.4.1 Firewall-Assistent

Die schnellste Methode zur Konfiguration der Firewall steht mit dem Firewall-Assistenten in LANconfig zur Verfügung:

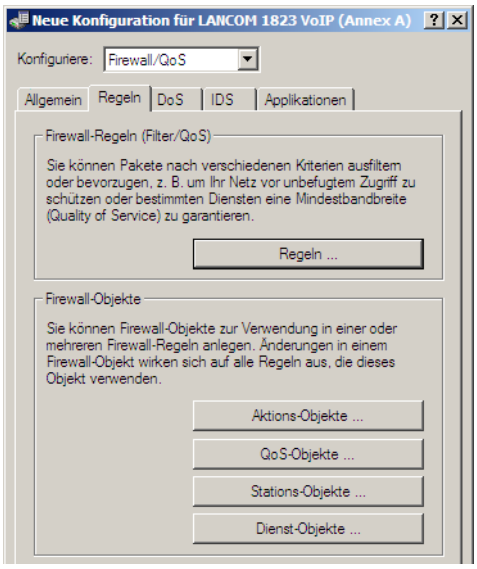


8.4.2 Definition der Firewall-Objekte

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.

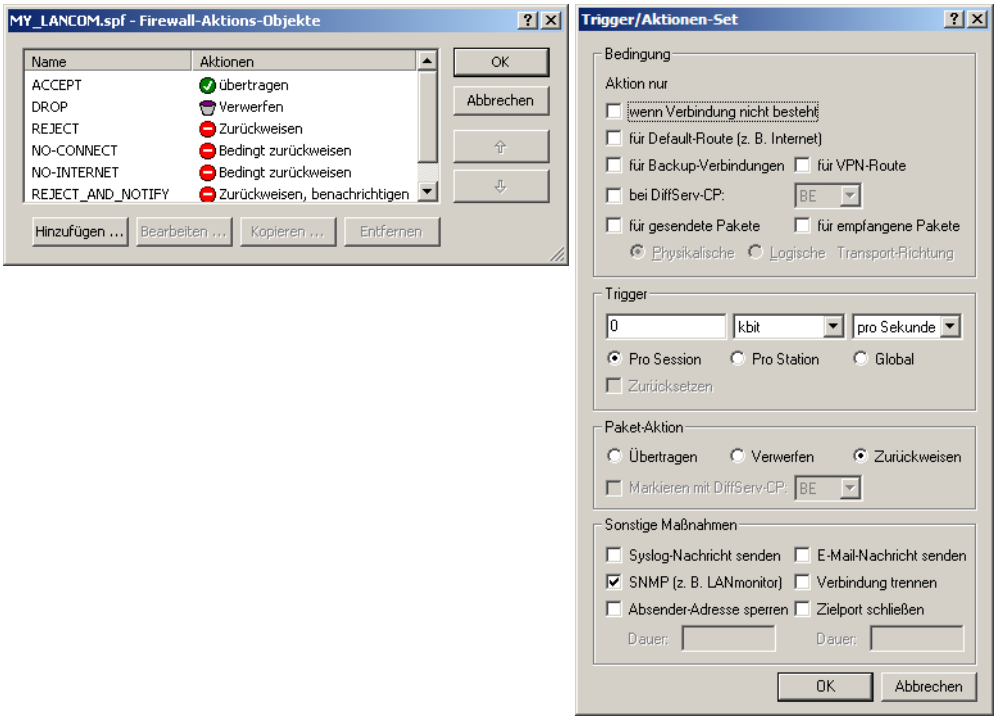
Bitte beachten Sie, dass sich eine Änderung der Firewall-Objekte auf alle Firewall-Regeln auswirkt, die dieses Objekt verwenden. Daher werden beim Ändern von Firewall-Objekten alle Firewall-Regeln angezeigt, die ebenfalls diese Objekte verwenden.

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.



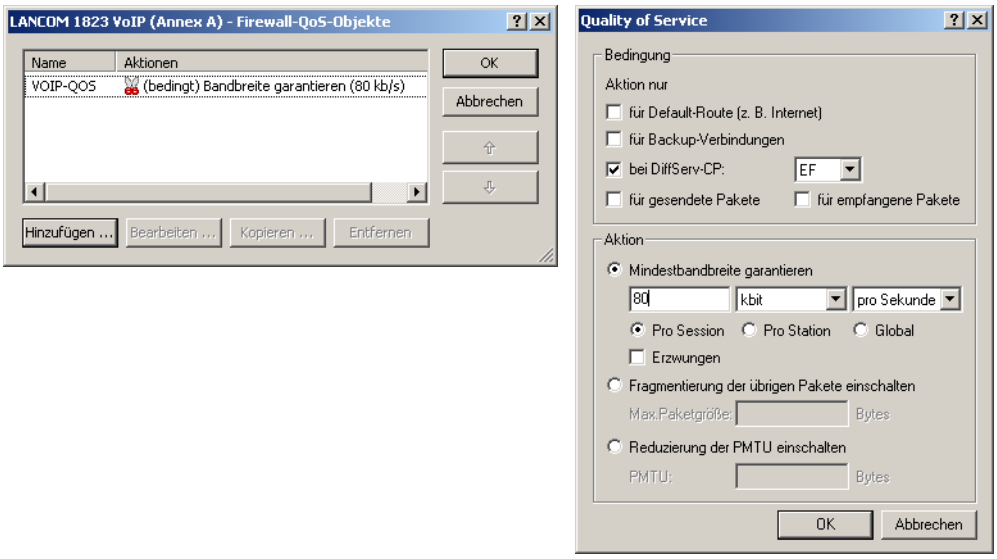
Aktions-Objekte

Hier legen Sie die Firewall-Aktion fest, bestehend aus Bedingung, Limit, Paket-Aktion und sonstigen Maßnahmen, die durch die Firewall-Regeln verwendet werden sollen.



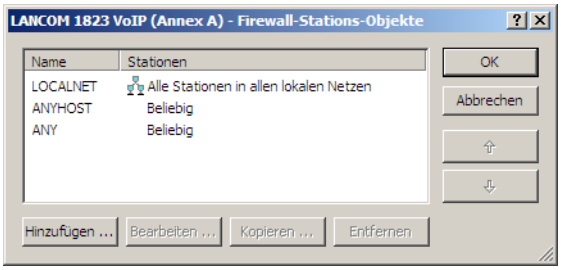
QoS-Objekte

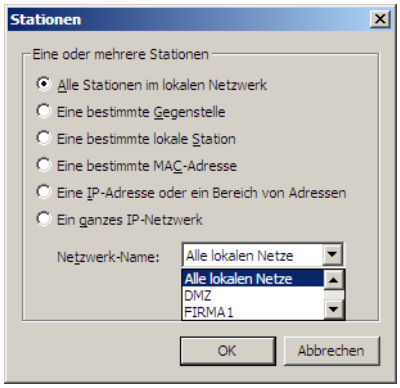
Hier können Sie die Mindestbandbreiten für die Datenpakete zur Verfügung stellen, die durch die Firewall-Regeln verwendet werden sollen.



Stations-Objekte

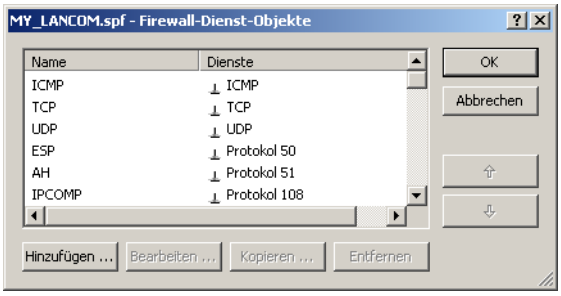
Hier werden die Stationen festgelegt, die als Absender oder Adressat der Pakete durch die Firewall-Regeln verwendet werden sollen. Die Stations-Objekte sind dabei nicht auf Quelle oder Ziel festgelegt, sondern können in den Firewall-Regeln je nach Bedarf verwendet werden. Im Zusammenhang mit ARF ('Advanced Routing and Forwarding' → Seite 7-9) ist es z. B. möglich, eine bestimtmes IP-Netzwerk als Stations-Objekt zu definieren.

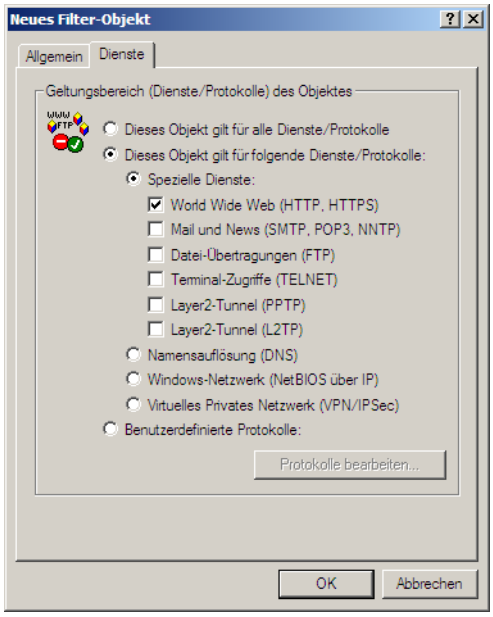




Dienst-Objekte

Hier werden die IP-Protokolle, Quell- und Zielports definiert, die durch die Firewall-Regeln verwendet werden sollen.

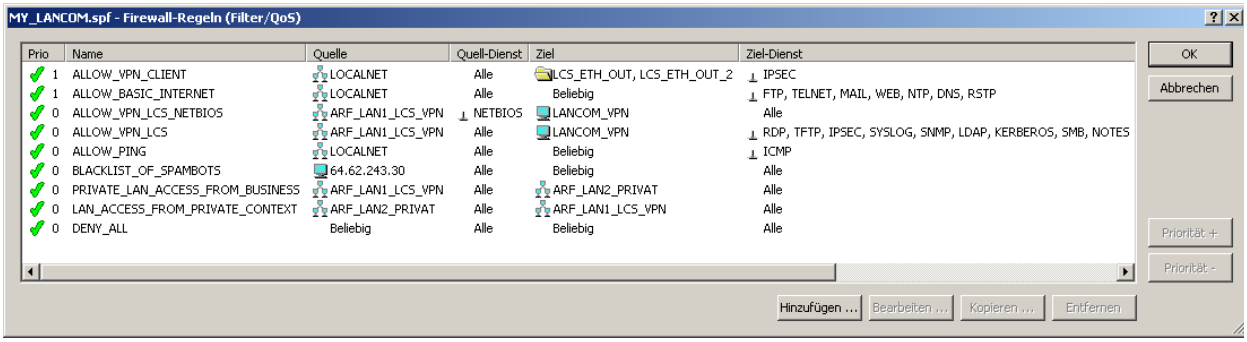




8.4.3 Definition der Firewall-Regeln

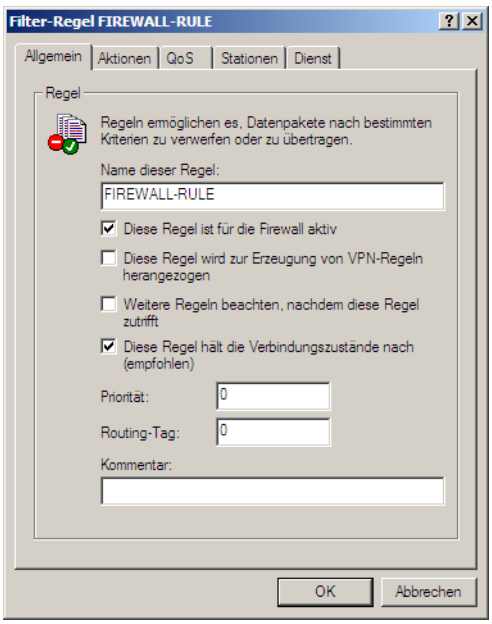
Die Firewall-Regeln werden in einer übersichtlichen Tabelle mit folgenden Informationen dargestellt:

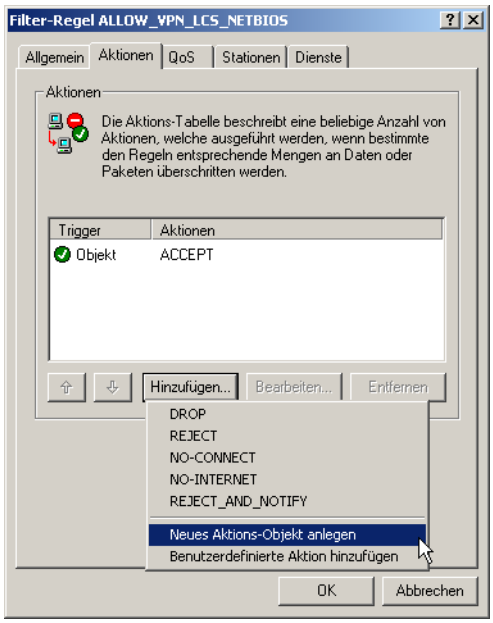
- In der Spalte äußerst links zeigen Symbole den Zustand der Firewall-Regel an:
  - Grünes Häkchen: Firewall-Regel ist aktiv.
  - Rotes Kreuzchen: Firewall-Regel ist nicht aktiv.
  - Schloss: Firewall-Regel wird zur manuellen Erzeugung von VPN-Regeln verwendet.
  - Zwei verkettete Pfeile: Wenn diese Firewall-Regel zutrifft, bitte weitere Regeln beachten.
- Name der Firewall-Regel
- Quelle
- Ziel
- Quell- und Ziel-Dienst
- Aktion/QoS
- Kommentar



Neue Firewall-Regel hinzufügen

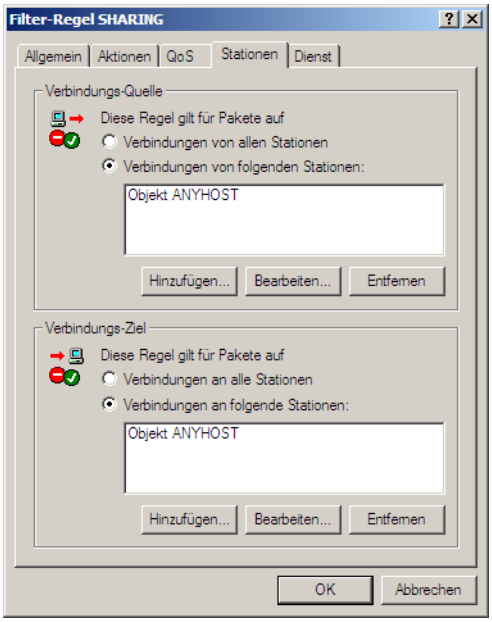
Beim Anlegen einer neuen Firewall-Regel werden zunächst die allgemeinen Daten erfasst. Auf den folgenden Registerkarten für Aktionen, QoS, Stationen oder Dienste werden die schon definierten Objekte zur direkten Verwendung angeboten. Alternativ können von dieser Stelle aus neue Objekte angelegt werden, die auch in anderen Regeln verwendet werden können oder benutzerdefinierte Einträge, die nur in der aktiven Firewall-Regel zum Einsatz kommen.

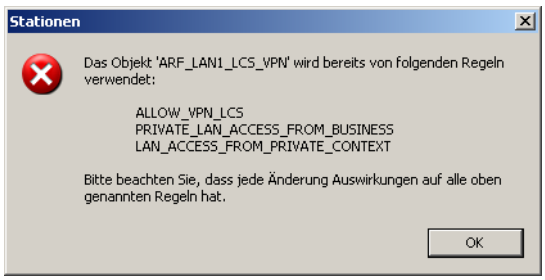




Firewall-Regel bearbeiten

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.





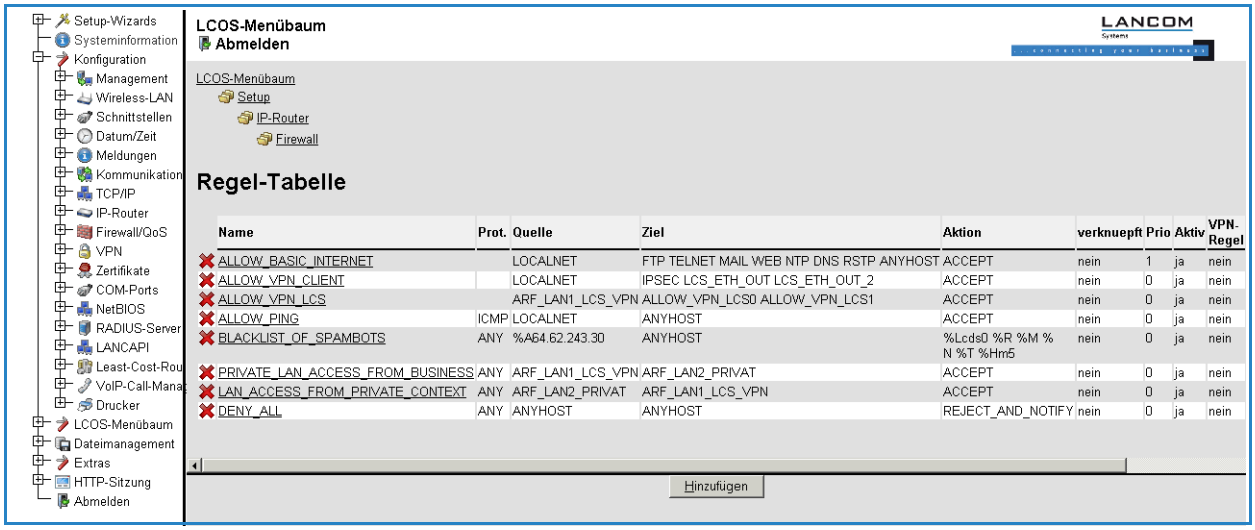
8.5 Konfiguration der Firewall-Regeln mit WEBconfig oder Telnet

8.5.1 Regel-Tabelle

■ WEBconfig: 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.

Wie in LANconfig kann auch in WEBconfig die Konfiguration der Firewall mit Hilfe von Objekten vorgenommen werden. 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 LCOS-Version 7.6 oder neuer sind automatisch die wichtigsten Objakte in der Firewall vordefiniert. Bei der Bearbeitung von älteren Konfiguration mit LANconfig werden die Standard-Objekte der Firewall automatisch ergänzt.

Zur Beschreibung der Firewall-Regeln gibt es im LCOS 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 LCOS-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 LCOS-Syntax enthalten (z.B. %P6 für TCP).

Bei der direkten Eingabe der Pegel-Parameter in der LCOS-Syntax gelten die gleichen Regeln, wie sie für Protokolle, Quelle und Ziel sowie die Firewall-Aktionen angegeben sind.

8.5.2 Objekttabelle

- WEBconfig: 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, Host-Name)
- 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

- WEBconfig: 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 (→ Seite 8-28).

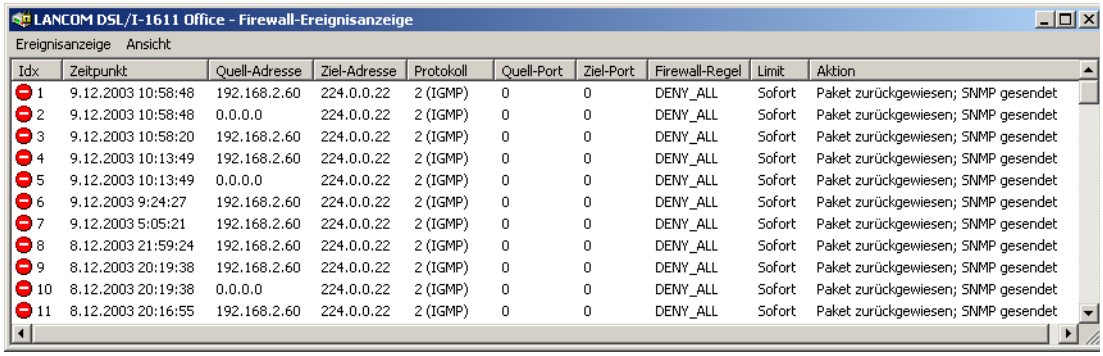
Alle in diesem Abschnitt beschriebenen Listen und Tabellen finden Sie unter folgenden Menüpunkten:

WEBconfig: LCOS-Menübaum ▶ Status ▶ IP-Router-Statistik

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	Protokoll	Quell-Port	Ziel-Port	Firewall-Regel	Limit	Aktion
1	9.12.2003 10:58:48	192.168.2.60	224.0.0.22	2 (IGMP)	0	0	DENY_ALL	Sofort	Paket zurückgewiesen; SNMP gesendet
2	9.12.2003 10:58:48	0.0.0.0	224.0.0.22	2 (IGMP)	0	0	DENY_ALL	Sofort	Paket zurückgewiesen; SNMP gesendet
3	9.12.2003 10:58:20	192.168.2.60	224.0.0.22	2 (IGMP)	0	0	DENY_ALL	Sofort	Paket zurückgewiesen; SNMP gesendet
4	9.12.2003 10:13:49	192.168.2.60	224.0.0.22	2 (IGMP)	0	0	DENY_ALL	Sofort	Paket zurückgewiesen; SNMP gesendet
5	9.12.2003 10:13:49	0.0.0.0	224.0.0.22	2 (IGMP)	0	0	DENY_ALL	Sofort	Paket zurückgewiesen; SNMP gesendet
6	9.12.2003 9:24:27	192.168.2.60	224.0.0.22	2 (IGMP)	0	0	DENY_ALL	Sofort	Paket zurückgewiesen; SNMP gesendet
7	9.12.2003 5:05:21	192.168.2.60	224.0.0.22	2 (IGMP)	0	0	DENY_ALL	Sofort	Paket zurückgewiesen; SNMP gesendet
8	8.12.2003 21:59:24	192.168.2.60	224.0.0.22	2 (IGMP)	0	0	DENY_ALL	Sofort	Paket zurückgewiesen; SNMP gesendet
9	8.12.2003 20:19:38	192.168.2.60	224.0.0.22	2 (IGMP)	0	0	DENY_ALL	Sofort	Paket zurückgewiesen; SNMP gesendet
10	8.12.2003 20:19:38	0.0.0.0	224.0.0.22	2 (IGMP)	0	0	DENY_ALL	Sofort	Paket zurückgewiesen; SNMP gesendet
11	8.12.2003 20:16:55	192.168.2.60	224.0.0.22	2 (IGMP)	0	0	DENY_ALL	Sofort	Paket zurückgewiesen; SNMP gesendet

Wird die Logging-Tabelle über WEBconfig aufgerufen, präsentiert sie sich in folgender Darstellung:

Experten-Konfiguration
Status
IP-Router-Statistik

Log-Tabelle

Idx.	System-Zeit	Quell-Adresse	Ziel-Adresse	Prot.	Quell-Port	Ziel-Port	Filterregel	Limit	Schwelle	Aktion
0001	9.12.2003 10:58:48	192.168.2.60	224.0.0.22	2	0	0	DENY_ALL	00000022	0	40000108
0002	9.12.2003 10:58:48	0.0.0.0	224.0.0.22	2	0	0	DENY_ALL	00000022	0	40000108
0003	9.12.2003 10:58:20	192.168.2.60	224.0.0.22	2	0	0	DENY_ALL	00000022	0	40000108
0004	9.12.2003 10:13:49	192.168.2.60	224.0.0.22	2	0	0	DENY_ALL	00000022	0	40000108
0005	9.12.2003 10:13:49	0.0.0.0	224.0.0.22	2	0	0	DENY_ALL	00000022	0	40000108
0006	9.12.2003 9:24:27	192.168.2.60	224.0.0.22	2	0	0	DENY_ALL	00000022	0	40000108
0007	9.12.2003 5:05:21	192.168.2.60	224.0.0.22	2	0	0	DENY_ALL	00000022	0	40000108
0008	8.12.2003 21:59:24	192.168.2.60	224.0.0.22	2	0	0	DENY_ALL	00000022	0	40000108
0009	8.12.2003 20:19:38	192.168.2.60	224.0.0.22	2	0	0	DENY_ALL	00000022	0	40000108
000a	8.12.2003 20:19:38	0.0.0.0	224.0.0.22	2	0	0	DENY_ALL	00000022	0	40000108

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-address	Quell-Adresse des gefilterten Pakets
Ziel-address	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.

Element	Bedeutung
Limit	Bitfeld, dass das überschrittene Limit beschreibt, durch welches das Paket gefiltert wurde. 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 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
Action	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 Zieladresse und -port sperren 0x20000000 Sende Syslog-Benachrichtigung 0x40000000 Sende SNMP-Trap 0x80000000 Sende E-Mail

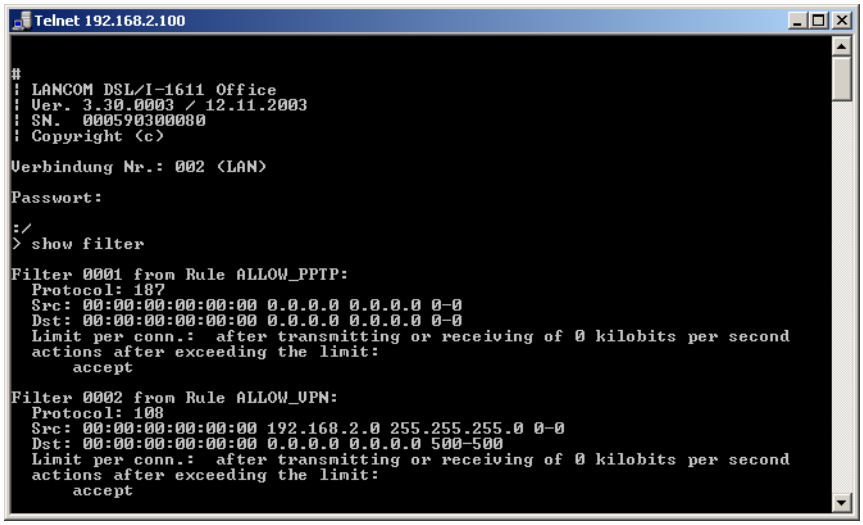
Alle Firewall-Aktionen werden ebenfalls im IP-Router-Trace angezeigt (‘So starten Sie einen Trace’ → Seite 5-1). Einige LANCOM-Modelle verfügen ferner über eine Firewall-LED, welche jedes gefilterte Paket signalisiert.

Die Filterliste

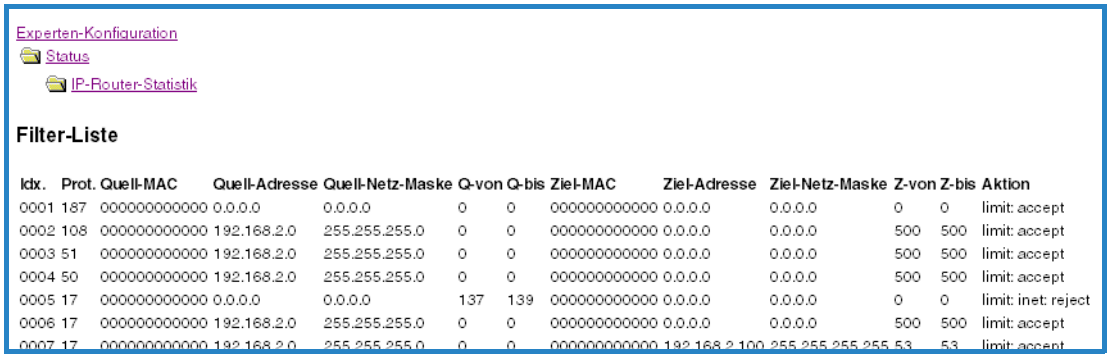
Über die Filterliste können die aus den in der Aktions-, Objekt- und Regeltabelle definierten Regeln erzeugten Filter ermittelt werden.

Bei einer manuellen Filter-Definition über Telnet oder WEBconfig wird kein Eintrag in der Filterliste angelegt, wenn die Definition Fehler in der Syntax enthält. In diesem Fall wird auch keine Fehlermeldungen ausgegeben! Wenn Sie die Filter manuell konfigurieren, sollten Sie in jedem Fall anhand der Filterliste überprüfen, ob die gewünschten Filter erzeugt wurden.

Auf Telnet-Ebene kann der Inhalt der Filterliste auch mit dem Kommando `show filter` anzeigt werden:



Unter WEBconfig hat die Filterliste den folgenden Aufbau:



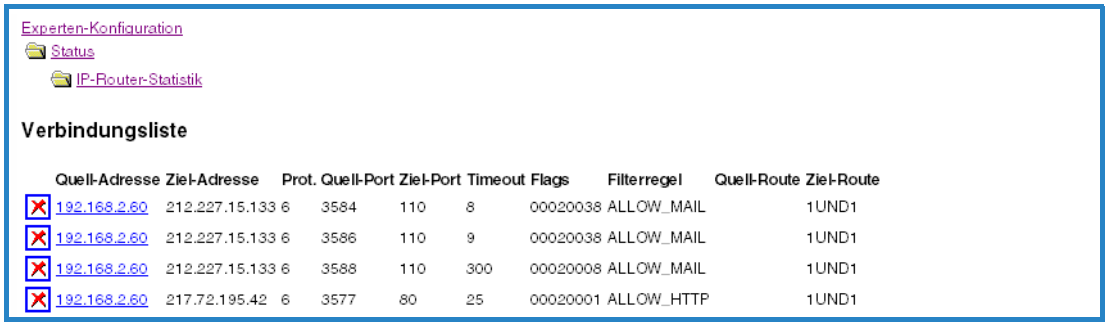
Die einzelnen Felder in der Filterliste haben folgende Bedeutung:

Eintrag	Beschreibung
Idx.	laufender Index
Prot	zu filterndes Protokoll, also z.B. 6 für TCP oder 17 für UDP
Quell-MAC	Ethernet-Quell-Adresse des zu filternden Pakets oder 000000000000, wenn der Filter für alle Pakete gelten soll
Quell-Adresse	Quell-IP-Adresse oder 0.0.0.0, wenn der Filter für alle Pakete gelten soll
Quell-Netzmaske	Quell-Netzmaske, die zusammen mit der Quell-IP-Adresse das Quell-Netz bestimmt, oder 0.0.0.0, wenn der Filter für Pakete aus allen Netzen gelten soll
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-MAC	Ethernet-Zieladresse des zu filternden Pakets oder 000000000000, wenn der Filter für alle Pakete gelten soll
Ziel-Adresse	Ziel-IP-Adresse oder 0.0.0.0, wenn der Filter für alle Pakete gelten soll
Ziel-Netzmaske	Ziel-Netzmaske, die zusammen mit der Ziel-IP-Adresse das Ziel-Netz bestimmt, oder 0.0.0.0, wenn der Filter für Pakete zu allen Netzen gelten soll
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
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, das mit einer "accept" Aktion verknüpft ist eingefügt. 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.

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
Protocol	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 (→ Seite 8-31). 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 nun die Zustände **new**, **open** und **closing** (letzteren nur, wenn die UDP-Verbindung mit einem zustandsbehafteten Steuerkanal verknüpft ist. Dies ist z.B. beim Protokoll H.323 der Fall)
Quell-Route	Name der Gegenstelle, über die das erste Paket empfangen wurde.
Ziel-Route	Name der Gegenstelle, auf die das erste Paket gesendet wird.
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

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.

Hostsperrliste

Wenn als Aktion eines Filters die Sperrung des Absenders ausgewählt wurde, so werden 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.

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 (z.B. Smurf) zu verschleiern.

Die LANCOM 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.

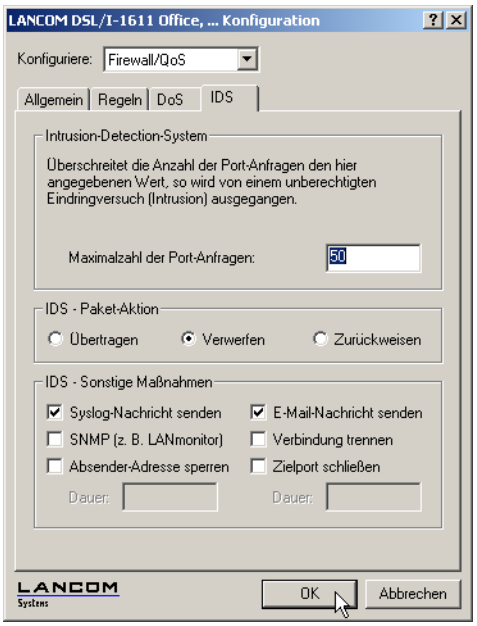
Portscan- Erkennung

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' → Seite 8-34): 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



LANconfig: Firewall/QoS ▶ IDS

WEBconfig: LCOS- Menübaum ▶ 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". LANCOM- Geräte sind mit entsprechenden Schutzmechanismen ausgestattet, die bekannte Hacker- Angriffe erkennen und die Funktionstüchtigkeit erhalten.

8.9.1 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 prinzipiellen 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.

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.

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 und 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 LANCOM das Weiterleiten von Paketen, die an die lokale Broadcastadresse gerichtet sind.

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 LANCOM ebenfalls erkannt und geblockt.

Ping of Death

Der Ping of Death gehört zu den Angriffen, die Fehler bei der Reassemblierung 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 "halb" reassemblierte 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.

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 Reassemblierung 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 reassembliert 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 "halb" reassemblierte Pakete beim Opfer.

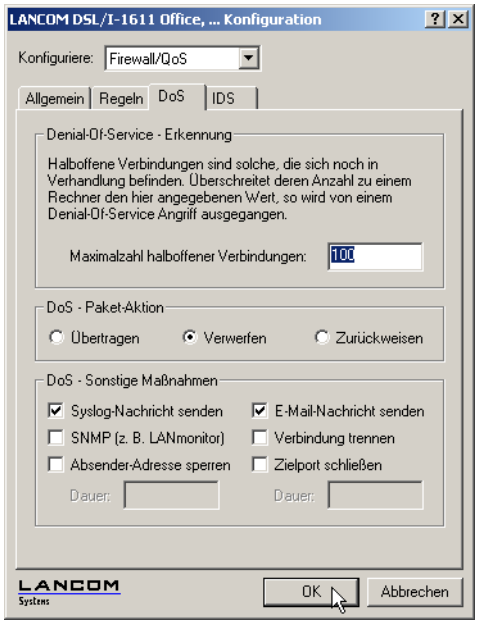
Bonk/Fragrouter

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.

8.9.2 Konfiguration der DoS-Abwehr



LANconfig: Firewall/QoS ▶ DoS

WEBconfig: LCOS-Menübaum ▶ 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 LANCOM 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.

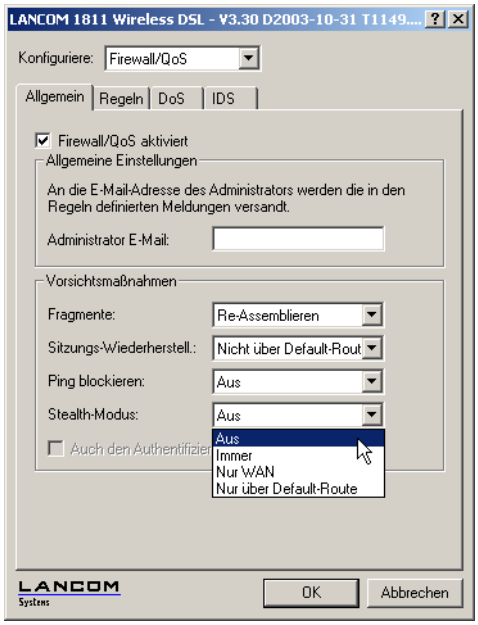
Um nicht durch fehlerhafte Konfiguration der Firewall ein Tor für DoS-Angriffe zu öffnen, wird dieser Teil zentral konfiguriert. Neben der Maximalzahl der halboffenen Verbindungen, der Paket-Aktion und den möglichen Meldemechanismen gibt es hier noch weitergehende Reaktionsmöglichkeiten:

- 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).

8.9.3 Konfiguration von ping-Blocking und Stealth-Modus



LANconfig: Firewall/QoS ▶ Allgemein

WEBconfig: LCOS-Menübaum ▶ Setup ▶ IP-Router ▶ Firewall

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 versendenen 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 LANCOM zunächst einmal erkennen, welche Datenpakete denn überhaupt bevorzugt werden sollen.

Es gibt zwei Möglichkeiten, den Bedarf für eine bevorzugte Behandlung von Datenpaketen im LANCOM 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 LANCOM 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 relativ neues Modell dar, die Priorität der Datenpakete zu signalisieren. DiffServ basiert auf dem bekannten 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.

Code-point	DSCP Bits	Dez.
CS0 (BE)	000000	0
CS1	001000	8
CS2	010000	16
CS3	011000	24
CS4	100000	32
CS5	101000	40
CS6	110000	48
CS7	111000	56

Code-point	DSCP Bits	Dez.
AF11	001010	10
AF12	001100	12
AF13	001110	14
AF21	010010	18
AF22	010100	20
AF23	010110	22
AF31	011010	26
AF32	011100	28

Code-point	DSCP Bits	Dez.
AF33	011110	30
AF41	100010	34
AF42	100100	36
AF43	100110	38
EF	101110	46

9.2.2 Garantierte Mindestbandbreiten

Hiermit geben Sie Vorfahrt für sehr wichtige Applikationen, Voice-over-IP (VoIP)-TK-Anlagen oder bestimmte Benutzergruppen.

Bei LANCOM-Geräten mit integrierter oder nachträglich über Software-Option freigeschalteter VoIP-Funktion werden die QoS-Einstellungen für SIP-Gespräche automatisch vorgenommen!

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.

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 Usern gleichzeitig und gleichberechtigt zugute kommen, setzen Sie pro Verbindung zum Server eine bestimmte Maximalbandbreite.

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 (siehe 'SYN/ACK-Speedup' → Seite 7-9)
- 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".

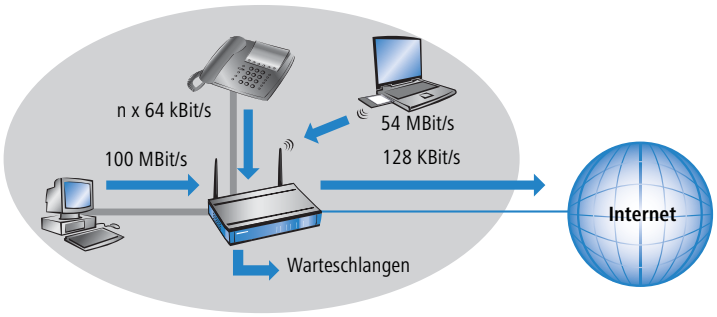
  Mit diesem Verfahren wird sichergestellt, dass priorisierte Verbindungen den restlichen Datenverkehr nicht erdrücken.
- gesicherte Queue

  Diese Warteschlange hat keine gesonderte Priorität. Jedoch werden Pakete in dieser Queue niemals verworfen (garantierte Übertragung). Hier landen folgende Datenpakete:

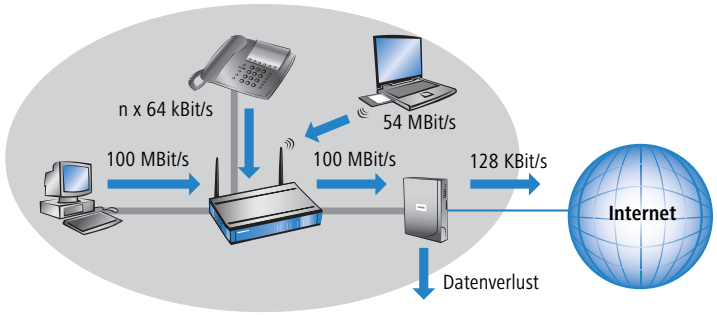
  - Pakete mit ToS "High Reliability"
  - Pakete mit DiffServ "Assured Forwarding"
- Standard-Queue

  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 LANCOM 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 LANCOM 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 LANCOM sieht die Verbindung ins Internet über das ein externes DSL-Modem wie ein Ethernet-Abschnitt aus. Auf der Strecke vom LANCOM zum DSL-Modem werden die Daten auch mit der vollen LAN-Geschwindigkeit von 10 oder 100 MBit/s übertragen. Hier bildet sich also kein natürlicher Stau, da die Ein- und Ausgangsgeschwindigkeiten gleich sind. Außerdem meldet das Ethernet zwischen LANCOM 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 LANCOM künstlich gedrosselt. Die Schnittstelle wird dabei auf die Übertragungsrate eingestellt, die für den Transport der Daten ins WAN zur Verfügung stehen. Bei einem Standard-DSL-Anschluss wird also das DSL-Interface im LANCOM auf die entsprechende Upstreamrate (128 KBit/s) eingestellt.

Bei der von den Providern angegebenen Datenraten 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 LANCOM vom DSL-Modem deutlich weniger Daten angeliefert, als eigentlich aufgrund des 10 oder 100 MBit 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, für einen Standard-DSL-Anschluss also z.B. auf eine Downstreamrate von 768 KBit/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 Bestä-

tigung 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

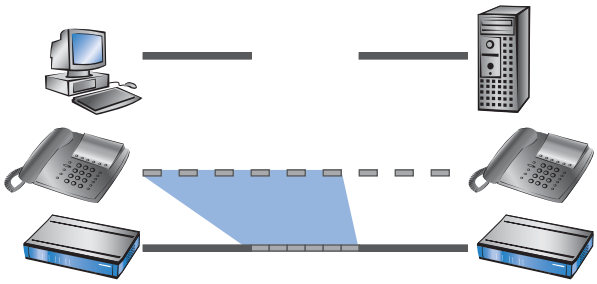
  Hier landen alle Pakete, die nicht aufgrund einer empfangsseitig aktiven QoS-Regel gesondert behandelt werden müssen. Pakete in dieser Queue werden direkt weitergeleitet bzw. bestätigt, ohne Maximalbandbreiten zu berücksichtigen.

9.4 Reduzierung der Paketlänge

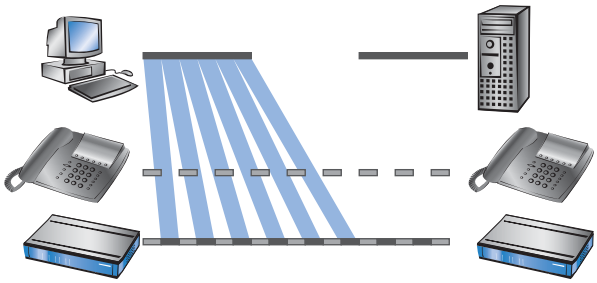
Die bevorzugte Behandlung von Datenpaketen einer wichtigen Applikation kann je nach Situation durch extrem lange Datenpakete anderer Anwendungen gefährdet werden. Das ist z.B. dann der Fall, wenn IP-Telefonie und ein FTP-Datentransfer gleichtzeitig auf der WAN-Verbindung aktiv sind.



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 LANCOM 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 möglicherweise einstellende Verzögerung nicht nachteilig aus.



Zur Beeinflussung der Paketlänge gibt es zwei verschiedene Verfahren:

- Das LANCOM 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.

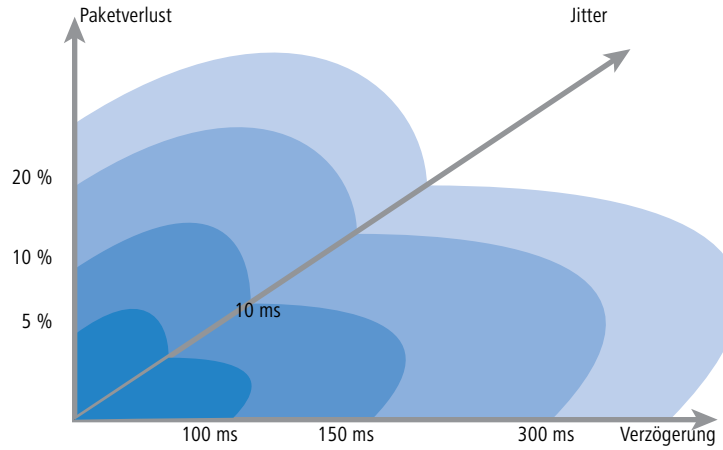
- Das LANCOM kann die zu sendenden Pakete oberhalb einer einstellbaren Maximalgröße (z.B. 256 Byte) selbst in kleinere Einheiten aufteilen. Dieses als "Fragmentieren" bezeichnete Verfahren wird jedoch nicht von allen Servern im Internet unterstützt, da die Verarbeitung von fragmentierten Paketen als 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 LANCOM-Geräten mit integrierter oder nachträglich über Software-Option freigeschalteter VoIP-Funktion werden die QoS-Einstellungen für SIP-Gespräche automatisch vorgenommen!



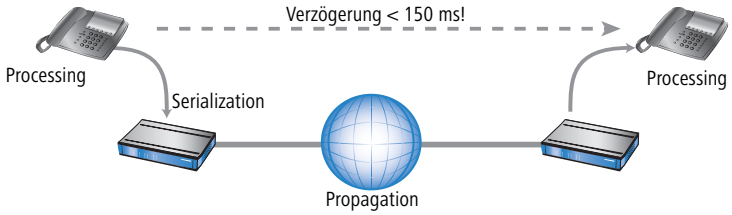
Bei einer Verzögerung von nicht mehr als 100 ms und einem Paketverlust von weniger als 5% wird die Qualität wie bei einer "normalen" Telefonverbindung empfunden, bei nicht mehr als 150 ms Verzögerung und weniger als 10% Paketverlust empfindet der Telefonteilnehmer immer noch eine sehr gute Qualität. 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 10ms.

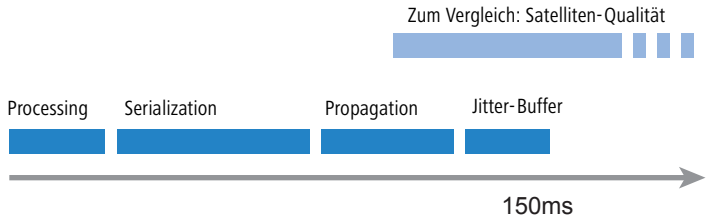
- Der Jitter kann beim Empfänger durch einen entsprechenden Puffer ausgeglichen werden. In diesem Puffer (Jitter-Buffer) werden einige Pakete zwischengespeichert und mit konstantem Abstand an den Empfänger weitergegeben. Durch diese Zwischenspeicherung können die Schwankungen in der Übertragungszeit 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).
  - 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 Pakte 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	20ms	20ms	20ms	20ms	20ms
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
G723-6,3	16	56	78	38400,0	42400,0

Ohne IPSec	Payload	IP-Payload	Ethernet/PPPoE	ATMNetto Bit/s	ATMBrutto Bit/s
Code	30ms	30ms	30ms	30ms	30ms
G711-64	240	280	302	89510,4	98834,4
G722-64	240	280	302	89510,4	98834,4
G726-40	150	190	212	63936,0	70596,0
G726-32	120	160	182	63936,0	70596,0
G726-24	90	130	152	51148,8	56476,8
G726-16	60	100	122	38361,6	42357,6
G729-8	30	70	92	38361,6	42357,6
G723-6,3	24	64	86	38361,6	42357,6

Mit IPSec	Payload	IP-Payload	IPSEC-Payload	Ethernet/PPPoE	ATMNetto Bit/s	ATMBrutto Bit/s
Code	20ms	20ms	20ms	20ms	20ms	20ms
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
G723-6,3	16	56	116	138	76800,0	84800,0

Mit IPSec	Payload	IP-Payload	IPSEC-Payload	Ethernet/PPPoE	ATMNetto Bit/s	ATMBrutto Bit/s
Code	30ms	30ms	30ms	30ms	30ms	30ms
G711-64	240	280	340	362	102297,6	112953,6
G722-64	240	280	340	362	102297,6	112953,6
G726-40	150	190	250	272	76723,2	84715,2
G726-32	120	160	220	242	76723,2	84715,2
G726-24	90	130	190	212	63936,0	70596,0
G726-16	60	100	160	182	63936,0	70596,0
G729-8	30	70	130	152	51148,8	56476,8
G723-6,3	24	64	124	146	51148,8	56476,8

- 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 LANCOM 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	32 ms	50 ms	60 ms	172 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.

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 LANCOM 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 LANCOM 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 LANCOM 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.

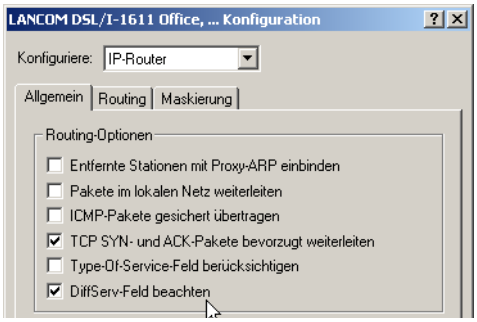
Die Unterscheidung von Sende- und Empfangsrichtung gilt nur für die Einrichtung von Maximalbandbreiten. Bei einer garantierten Mindestbandbreite sowie bei Fragmentierung und PMTU-Reduzierung gilt immer die physikalische Datenübertragung über das jeweilige Interface als Richtung!

9.7 QoS- Konfiguration

9.7.1 ToS- und DiffServ- Felder auswerten

ToS- oder DiffServ?

Wählen Sie bei der Konfiguration mit LANconfig auf der Registerkarte 'Allgemein', 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.



LANconfig: IP-Router ▶ Allgemein ▶ Routing-Optionen

WEBconfig: Setup ▶ IP-Routermodul ▶ 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:

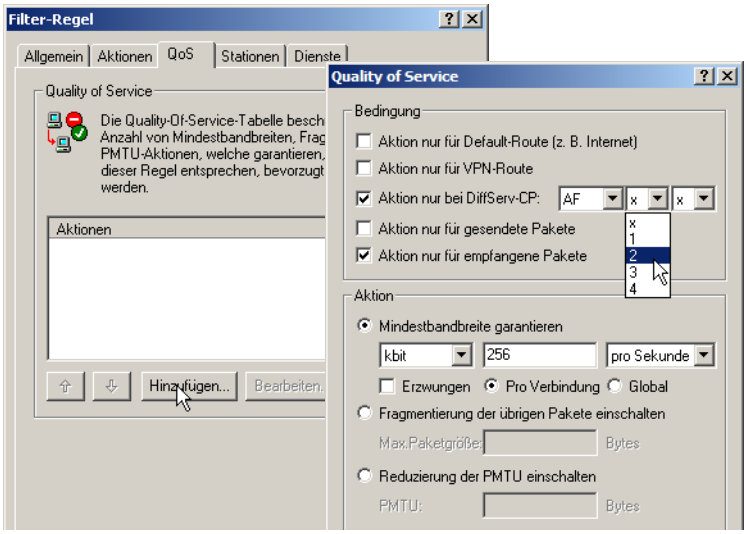
DSCP Codepoints	Übertragungsweise
CSx (inklusive CS0 = BE)	normal übertragen
AFxx	gesichert übertragen
EF	bevorzugt übertragen

DiffServ in den Firewall-Regeln

In den Firewallregeln können die Code Points aus dem DiffServ-Feld ausgewertet werden, um weitere QoS-Parameter wie Mindestbandbreiten oder PMTU-Reduzierung zu steuern.

LANconfig

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?' → Seite 9-2.

LANconfig: Firewall/QoS ▶ Regel ▶ Filter-Regel ▶ Quality of Service

WEBconfig: Setup ▶ IP-Router ▶ Firewall ▶ Regelliste

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.

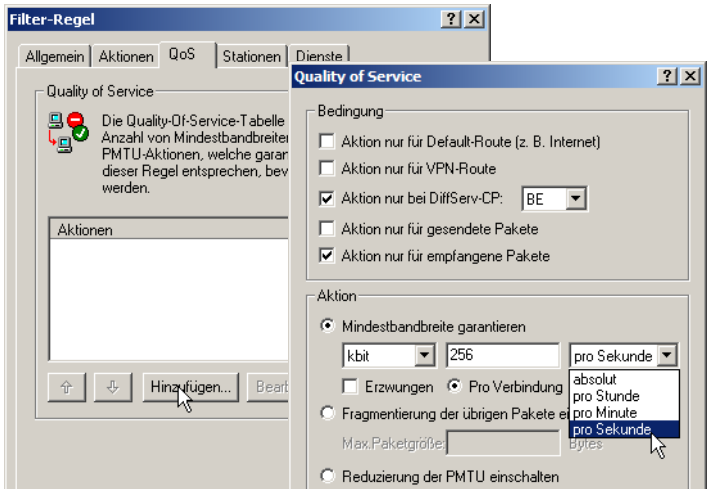


Weitere Informationen zum Definieren der Firewallregeln finden Sie im Kapitel 'Firewall' → Seite 8-1.

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.

LANconfig: Firewall/QoS ▶ Regel ▶ Filter-Regel ▶ Quality of Service

WEBconfig: Setup ▶ IP-Router ▶ Firewall ▶ Regelliste

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.

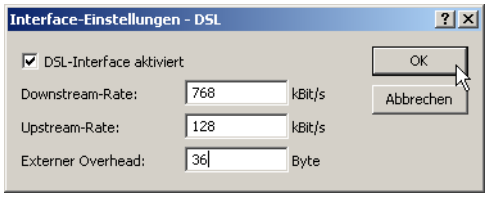
Beispiele:

- **%Qcds32**: Mindestbandbreite von 32 kBit/s für jede Verbindung
- **%Lgds256 %d**: Maximalbandbreite von 256 kBit/s für alle Verbindungen (global)

Weitere Informationen zum Definieren der Firewall-Regeln finden Sie im Kapitel 'Firewall' → Seite 8-1.

9.7.3 Übertragungsraten für Interfaces festlegen

Geräte mit eingebautem ADSL/SDSL-Modem bzw. mit ISDN-Adapter nehmen diese Einstellungen für das jeweilige Interface selbständig vor. Bei einem LANCOM-Modell mit DSL- **und** ISDN-Interface wird diese Einstellung also nur für das Ethernet-Interface vorgenommen.



- 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 3).
- 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 diese Extra-Overhead durchaus bemerkbar. Beispiele für den externen Overhead:

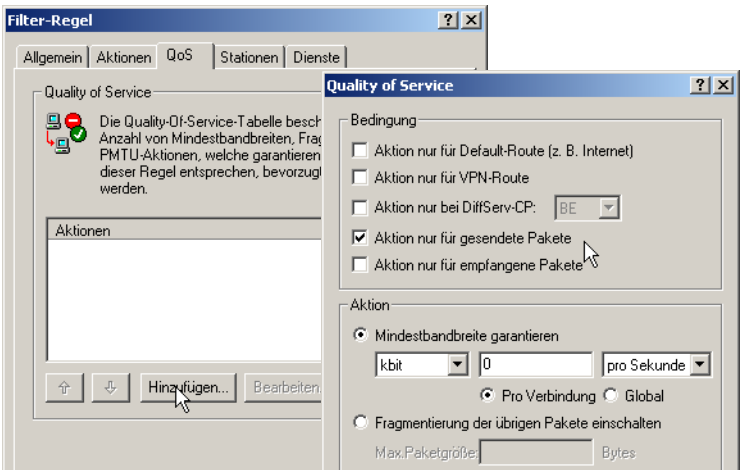
Übertragung	externer Overhead	Bemerkung
T-DSL	36 Bytes	zusätzliche Header, Verluste durch nicht vollständig genutzte ATM-Zellen
PPTP	24 Bytes	zusätzliche Header, Verluste durch nicht vollständig genutzte ATM-Zellen
IPoA (LLC)	22 Bytes	zusätzliche Header, Verluste durch nicht vollständig genutzte ATM-Zellen
IPoA (VC-MUX)	18 Bytes	zusätzliche Header, Verluste durch nicht vollständig genutzte ATM-Zellen
Kabelmodem	0	direkte Übertragung von Ethernet-Paketen

LANconfig: Schnittstellen ▶ WAN

WEBconfig: Setup ▶ Schnittstellen ▶ DSL Schnittstellen

Die Werte für die Upstream-Rate und die Downstream-Rate werden in KBit/s angegeben, die Werte für den externen Overhead in Bytes/Paket.

9.7.4 Sende- und Empfangsrichtung



Bei der Konfiguration mit WEBconfig oder Telnet wird die Bedeutung der Datenübertragungsrichtung über die Parameter "R" für receive (Empfangen), "T" für transmit (Senden) und "W" für den Bezug zum WAN-Interface eingetragen.

LANconfig: Firewall/QoS ▶ Regel ▶ Filter-Regel ▶ Quality of Service

WEBconfig: Setup ▶ IP-Router ▶ Firewall ▶ Regelliste

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:

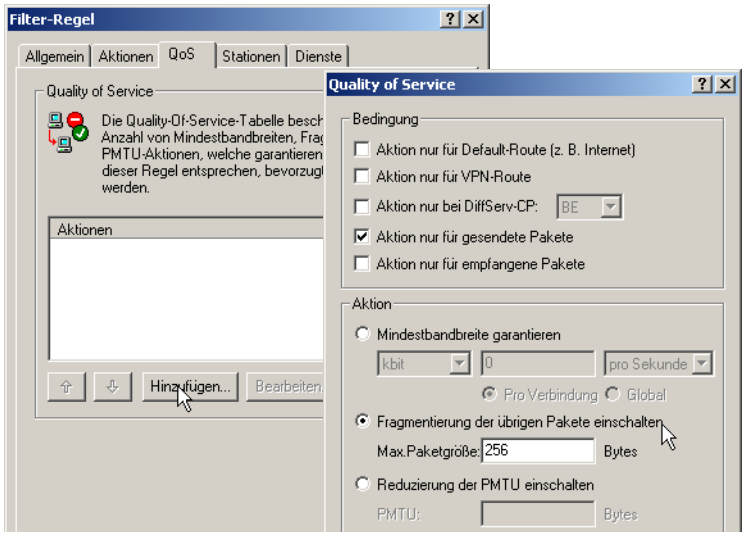
- %Lcdstw16%d

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 LANCOM-Geräten mit integrierter oder nachträglich über Software-Option freigeschalteter VoIP-Funktion können Fragmentierung und PMTU-Reduzierung separat für SIP-Gespräche eingestellt werden!



Bei der Konfiguration mit WEBconfig oder Telnet 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 eingetragen.

LANconfig: Firewall/QoS ▶ Regel ▶ Filter-Regel ▶ Quality of Service

WEBconfig: Setup ▶ IP-Router ▶ Firewall ▶ Regelliste

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 %Prt256	UDP

Diese Regel setzt die Mindestbandbreite für Senden und Empfang auf 32 KBit/s, erzwingt und verringert die PMTU beim Senden und Empfang 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 Sende- und Empfangsrichtung).

9.8 QoS für WLANs nach IEEE 802.11e (WMM/WME)

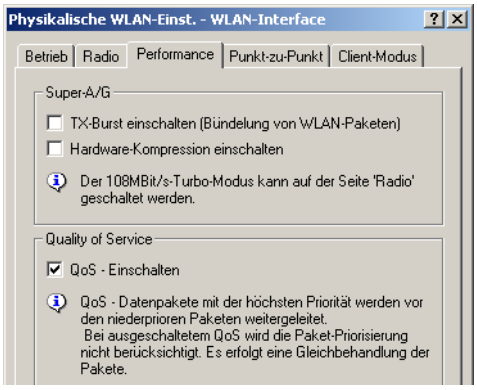
Mit der Erweiterung der 802.11-Standards um 802.11e können auch für WLAN-Übertragungen definierte Dienstgüten angeboten werden (Quality of Service). 802.11e unterstützt u.a. eine Priorisierung von bestimmten Datenpaketen. Die Erweiterung stellt damit eine wichtige Basis für die Nutzung von Voice-Anwendungen 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 LANCOM Access Point für jedes physikalische WLAN-Netzwerk getrennt aktiviert werden.



LANconfig: Wireless LAN ▶ Physikalische WLAN-Einstellungen ▶ Performance

WEBconfig: LCOS-Menübaum ▶ Setup ▶ Schnittstellen ▶ WLAN ▶ Leistung

LANCOM Referenzhandbuch Teil 3

- Virtual Private Networks - VPN

Stand: LCOS 7.6 mit Addendum 7.7 (siehe Anhang)
(letztes Update August 2009)

LANCOM
Systems

© 2009 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®, Windows Vista™, Windows NT® und Microsoft® sind eingetragene Marken von Microsoft, Corp.

Das LANCOM Systems-Logo, LCOS und die Bezeichnung LANCOM sind eingetragene Marken der LANCOM Systems GmbH. Alle übrigen verwendeten Namen und Bezeichnungen können Marken oder eingetragene Marken ihrer jeweiligen Eigentümer sein.

LANCOM Systems behält sich vor, die genannten Daten ohne Ankündigung zu ändern und übernimmt keine Gewähr für technische Ungenauigkeiten und/oder Auslassungen.

Produkte von LANCOM Systems enthalten Software, die vom „OpenSSL Project" für die Verwendung im „OpenSSL Toolkit" entwickelt wurde (http://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.

Produkte von LANCOM Systems enthalten Komponenten, die als Open Source Software im Quelltext verfügbar sind und speziellen Lizenzen sowie den Urheberrechten verschiedener Autoren unterliegen. Im Besonderen enthält die Firmware Komponenten, die der GNU General Public License, Version 2 (GPL) unterliegen. Die Lizenzvereinbarung mit dem Text der GPL ist auf der LANCOM CD im Produktverzeichnis zu finden. Auf Anfrage können die Quelltexte und alle Lizenzhinweise elektronisch vom FTP-Server der LANCOM Systems GmbH bezogen werden.

Die Firmware des LANCOM VP-100 enthält Komponenten, die als Open Source Software im Quelltext verfügbar sind und speziellen Lizenzen sowie den Urheberrechten verschiedener Autoren unterliegen. Im Besonderen enthält die Firmware Komponenten, die der GNU General Public License, Version 2 (GPL) unterliegen. Die Lizenzvereinbarung mit dem Text der GPL ist auf der LANCOM CD im Produktverzeichnis als LC-VP100-License-DE.txt zu finden. Auf Anfrage können die Quelltexte und alle Lizenzhinweise elektronisch vom FTP-Server der LANCOM Systems GmbH bezogen werden.

LANCOM Systems GmbH

Adenauerstr. 20/B2

52146 Würselen

Deutschland

www.lancom.de

Würselen, August 2009

110652/0809

Inhalt

10 Virtual Private Networks – VPN 10 - 1

10.1 Welchen Nutzen bietet VPN? 10 - 1
10.1.1 Private IP-Adressen im Internet? 10 - 2
10.1.2 Sicherheit des Datenverkehrs im Internet? 10 - 3

10.2 LANCOM VPN im Überblick 10 - 3
10.2.1 VPN Anwendungsbeispiel 10 - 3
10.2.2 Funktionen von LANCOM VPN 10 - 4

10.3 VPN-Verbindungen im Detail 10 - 5
10.3.1 LAN-LAN-Kopplung 10 - 5
10.3.2 Einwahlzugänge (Remote Access Service) 10 - 5

10.4 Was ist LANCOM Dynamic VPN? 10 - 6
10.4.1 Ein Blick auf die IP-Adressierung 10 - 6
10.4.2 So funktioniert LANCOM Dynamic VPN 10 - 7
10.4.3 Hinweise zur Dynamic VPN Lizensierung 10 - 9

10.5 Konfiguration von VPN-Verbindungen 10 - 10
10.5.1 VPN-Tunnel: Verbindungen zwischen den VPN-Gateways 10 - 11
10.5.2 VPN-Verbindungen einrichten mit den Setup-Assistenten 10 - 11
10.5.3 1-Click-VPN für Netzwerke (Site-to-Site) 10 - 12
10.5.4 1-Click-VPN für LANCOM Advanced VPN Client 10 - 13
10.5.5 VPN-Regeln einsehen 10 - 13
10.5.6 Manuelles Einrichten der VPN-Verbindungen 10 - 14
10.5.7 IKE Config Mode 10 - 15
10.5.8 VPN-Netzbeziehungen erstellen 10 - 16
10.5.9 Konfiguration mit LANconfig 10 - 17
10.5.10 Konfiguration mit WEBconfig 10 - 20
10.5.11 Gemeinsamer Aufbau von Security Associations 10 - 22
10.5.12 Diagnose der VPN-Verbindungen 10 - 23

10.6 Einsatz von digitalen Zertifikaten 10 - 23
10.6.1 Grundlagen 10 - 24
10.6.2 Vorteile von Zertifikaten 10 - 27
10.6.3 Aufbau von Zertifikaten 10 - 28
10.6.4 Sicherheit 10 - 29
10.6.5 Zertifikate beim VPN-Verbindungsaufbau 10 - 29
10.6.6 Zertifikate von Zertifikatsdiensteanbietern 10 - 30
10.6.7 Aufbau einer eigenen CA 10 - 31
10.6.8 Anfordern eines Zertifikates mit der Stand-alone Windows CA 10 - 31
10.6.9 Zertifikat in eine PKCS#12-Datei exportieren 10 - 32
10.6.10 Zertifikate mit OpenSSL erstellen 10 - 34
10.6.11 Zertifikate in das LANCOM laden 10 - 35
10.6.12 Zertifikate sichern und hochladen mit LANconfig 10 - 36
10.6.13 VPN-Verbindungen auf Zertifikatsunterstützung einstellen 10 - 36
10.6.14 Zertifikatsbasierte VPN-Verbindungen mit dem Setup-Assistenten erstellen 10 - 39
10.6.15 LANCOM Advanced VPN Client auf Zertifikatsverbindungen einstellen 10 - 42
10.6.16 Vereinfachte Einwahl mit Zertifikaten 10 - 43
10.6.17 Vereinfachte Netzwerkanbindung mit Zertifikaten – Proadaptives VPN 10 - 44
10.6.18 Anfrage von Zertifikaten mittels CERTREQ 10 - 44
10.6.19 Certificate Revocation List - CRL 10 - 45
10.6.20 Diagnose der VPN-Zertifikatsverbindungen 10 - 46

10.7 Mehrstufige Zertifikate für SSL/TLS 10 - 46
10.7.1 Einleitung 10 - 47
10.7.2 SSL/TLS mit mehrstufigen Zertifikaten 10 - 47
10.7.3 VPN mit mehrstufigen Zertifikaten 10 - 47

10.8 Zertifikatsenrollment über SCEP 10 - 47
10.8.1 SCEP-Server und SCEP-Client 10 - 48
10.8.2 Der Ablauf einer Zertifikatsverteilung 10 - 49
10.8.3 Konfiguration von SCEP 10 - 50

10.9	NAT Traversal (NAT-T)	10 - 53
10.10	Extended Authentication Protocol (XAUTH)	10 - 55
10.10.1	Einleitung	10 - 55
10.10.2	XAUTH im LCOS	10 - 56
10.10.3	Konfiguration von XAUTH	10 - 56
10.11	Backup über alternative VPN-Verbindung	10 - 57
10.11.1	Einleitung	10 - 57
10.11.2	Backup-fähige Netzstruktur	10 - 58
10.11.3	Konfiguration des VPN-Backups	10 - 60
10.12	Konkrete Verbindungsbeispiele	10 - 61
10.12.1	Statisch/statisch	10 - 62
10.12.2	Dynamisch/statisch	10 - 62
10.12.3	Statisch/dynamisch (mit LANCOM Dynamic VPN)	10 - 63
10.12.4	Dynamisch/dynamisch (mit LANCOM Dynamic VPN)	10 - 64
10.12.5	VPN-Verbindungen: hohe Verfügbarkeit mit „Lastenausgleich“	10 - 64
10.13	Wie funktioniert VPN?	10 - 66
10.13.1	IPSec – Die Basis für LANCOM VPN	10 - 66
10.13.2	Alternativen zu IPSec	10 - 67
10.14	Die Standards hinter IPSec	10 - 68
10.14.1	Module von IPSec und ihre Aufgaben	10 - 68
10.14.2	Security Associations – nummerierte Tunnel	10 - 68
10.14.3	Verschlüsselung der Pakete – das ESP-Protokoll	10 - 68
10.14.4	Die Authentifizierung – das AH-Protokoll	10 - 69
10.14.5	Management der Schlüssel – IKE	10 - 71

10 Virtual Private Networks – VPN

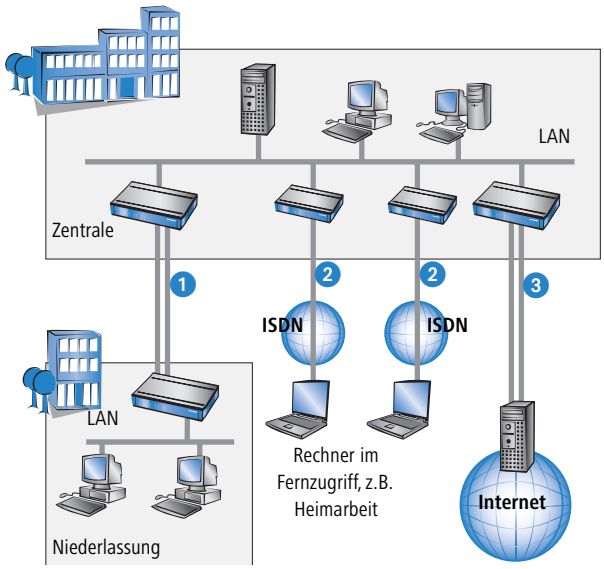
10.1 Welchen Nutzen bietet VPN?

Mit einem VPN (**V**irtual **P**rivate **N**etwork) 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.

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:

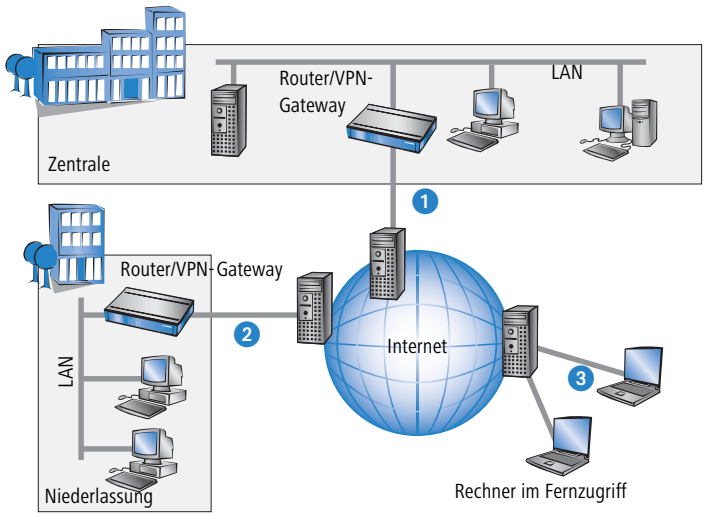
1. Eine Niederlassung ist (typischerweise über eine Standleitung) angeschlossen.
2. Rechner wählen sich über ISDN oder Modem ins zentrale Netzwerk ein (Remote Access Service – RAS).
3. Es existiert eine Verbindung ins Internet, um den Benutzern des zentralen LAN den Zugriff auf das Web und die Möglichkeit 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 (analoge Wählverbindung, ISDN, Standleitungen) entsprechende Hardware betrieben werden. Neben den Investitionskosten für diese Ausrüstung fallen auch kontinuierliche Administrations- und Wartungskosten an.

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 teueren 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 herkömmlichen 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. Aber auch herkömmliche ISDN-Verbindungen können verwendet werden.

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

10.1.1 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.

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.

10.1.2 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.

VPN – Sicherheit durch Verschlüsselung

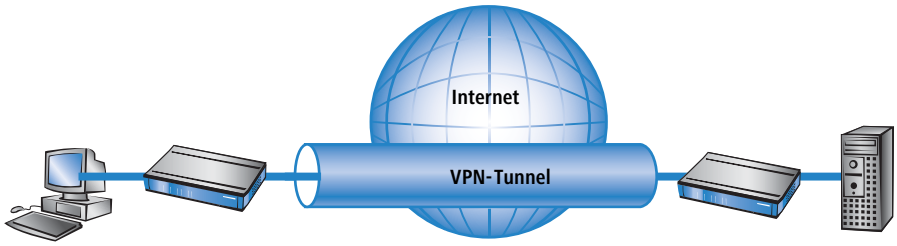
Zur Lösung dieses Sicherheitsproblems wird der Datenverkehr zwischen zwei Teilnehmern im VPN verschlüsselt. Während der Übermittlung sind die Daten für Dritte unlesbar.

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".

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.

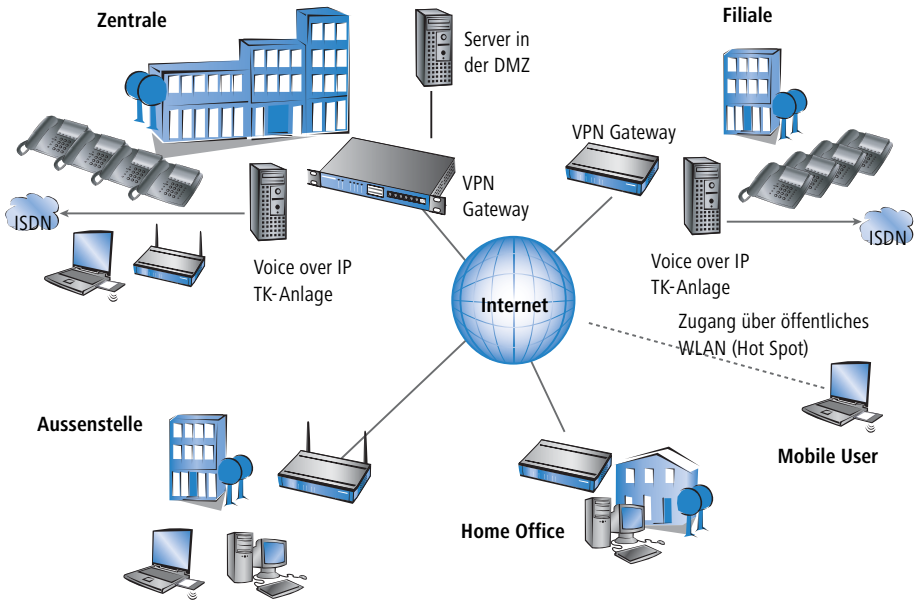


Damit ist das Ziel moderner Netzwerkstrukturen erreicht: Sichere Verbindungen über das größte und kostengünstigste aller öffentlichen IP-Netze: das Internet.

10.2 LANCOM VPN im Überblick

10.2.1 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, ggf. über ISDN oder analoge Modems
- Anbindung an Voice-over-IP-Telefonanlagen
- Anbindung von mobilen Usern, z.B. über öffentliche WLAN-Zugänge

10.2.2 Funktionen von LANCOM VPN

In diesem Abschnitt sind alle Funktionen und Eigenschaften von LANCOM VPN aufgelistet. VPN-Experten wird dieser Überblick viel sagen. Er ist sehr kompakt, verwendet allerdings eine Vielzahl komplexer Fachbegriffe. Für das Verständnis ist die Kenntnis der technischen Grundlagen von VPN notwendig. Seien Sie beruhigt: Sie können diesen Abschnitt auch bedenkenlos überspringen. Für Inbetriebnahme und Betrieb von LANCOM VPN sind die Informationen nicht erforderlich.

- VPN nach dem IPSec-Standard
- VPN-Tunnel über Festverbindung, Wählverbindung und IP-Netzwerk
- IKE Main- und Aggressive Modus
- LANCOM Dynamic VPN: Öffentliche IP-Adresse können statisch oder dynamisch sein (für den Aufbau zu Gegenstellen mit dynamischer IP-Adresse ist eine ISDN-Verbindung erforderlich)
- IPSec-Protokolle ESP, AH und IPCOMP im Transport- und Tunnelmodus
- Hash-Algorithmen:
  - HMAC-MD5-96, Hashlänge 128 Bits
  - HMAC-SHA-1-96, Hashlänge 160 Bits
- Symmetrische Verschlüsselungsverfahren
  - AES, Schlüssellänge 128, 192 und 256 Bits
  - Triple-DES, Schlüssellänge 168 Bits
  - Blowfish, Schlüssellänge 128-448 Bits
  - CAST, Schlüssellänge 128 Bits
  - DES, Schlüssellänge 56 Bits
- Kompression mit „Deflate" (ZLIB) und LZS
- IKE Config Mode
- IKE mit Preshared Keys
- IKE mit RSA-Signature und digitalen Zertifikaten (X.509)
- Schlüsselaustausch über Oakley, Diffie-Hellman-Algorithmus mit Schlüssellänge 768 Bits, 1024 Bits oder 1536 Bits (well known groups 1, 2 und 5)
- Schlüsselmanagement nach ISAKMP
- Extended Authentification Protokoll (XAUTH)

10.3 VPN-Verbindungen im Detail

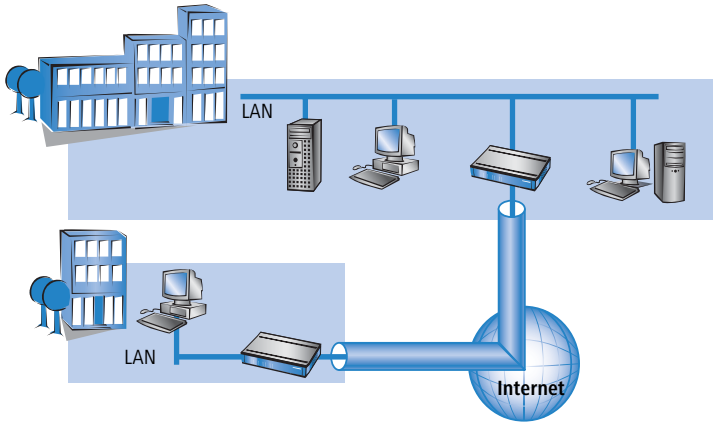
Es existieren zwei Arten von VPN-Verbindungen:

- 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).

10.3.1 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.

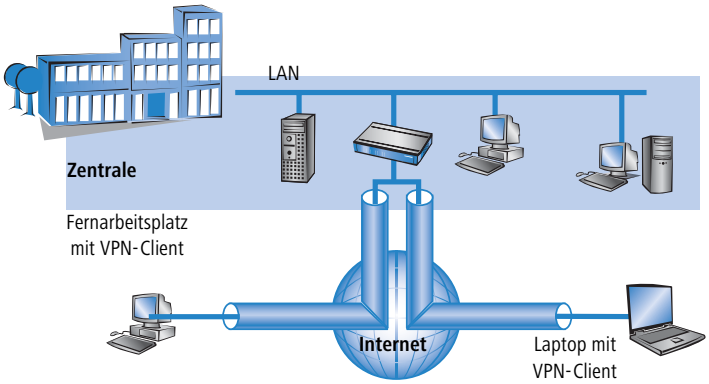
Parallele Internet-Nutzung

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.

10.3.2 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.

10.4 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.

10.4.1 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.

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.

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.

10.4.2 So funktioniert LANCOM Dynamic VPN

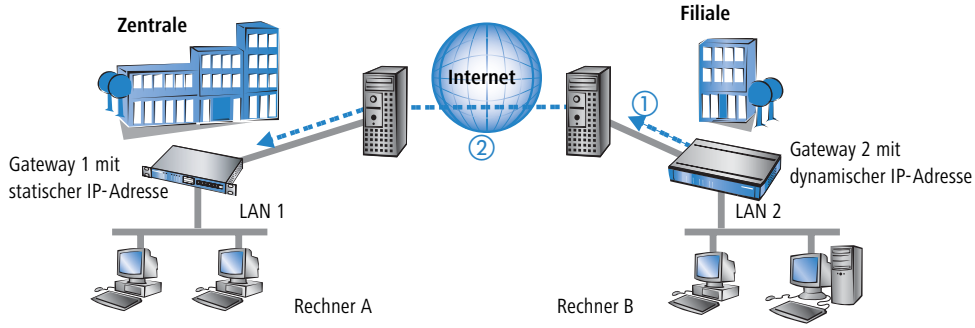
Verdeutlichen wir die Funktionsweise von LANCOM Dynamic VPN an Hand dreier Beispiele (Bezeichnungen beziehen sich auf die IP-Adressart der beiden VPN-Gateways):

- dynamisch – statisch
- statisch – dynamisch
- dynamisch – dynamisch

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.

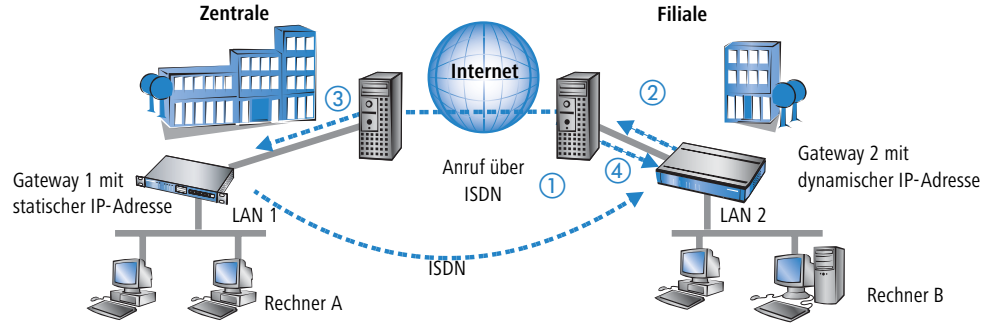
Der große Vorteil der LANCOM-Geräte bei dieser Anwendung: an Stelle des „Aggressive Mode", der normalerweise für die Einwahl von VPN-Clients in eine Zentrale verwendet wird, kommt hier der wesentlich sicherere „Main Mode" zum Einsatz. Beim Main Mode werden in der IKE-Verhandlungsphase deutlich mehr Nachrichten ausgetauscht als im Aggressive Mode.

Für diesen Verbindungsaufbau ist kein ISDN-Anschluss erforderlich. Die dynamische Seite übermittelt ihre IP-Adresse verschlüsselt über das Internet-Protokoll ICMP (alternativ auch über UDP).

Statisch – dynamisch

Möchte umgekehrt Rechner A im LAN 1 eine Verbindung zu Rechner B im LAN 2 aufbauen, z.B. um alle Außenstellen aus der Zentrale heraus fernzuwarten, dann erhält Gateway 1 die Anfrage und versucht einen VPN-Tunnel zu Gateway 2 aufzubauen. Gateway 2 verfügt nur über eine dynamische IP-Adresse und kann daher nicht direkt über das Internet angesprochen werden.

Mit Hilfe von LANCOM Dynamic VPN kann der VPN-Tunnel trotzdem aufgebaut werden. Dieser Aufbau geschieht in drei Schritten:



① Gateway 1 wählt Gateway 2 über ISDN an. Es nutzt dabei die ISDN-Möglichkeit, kostenlos seine eigene Rufnummer über den D-Kanal zu übermitteln. Gateway 2 ermittelt anhand der empfangenen Rufnummer aus den konfigurierten VPN-Gegenstellen die IP-Adresse von Gateway 1.

Für den Fall, dass Gateway 2 keine Rufnummer über den D-Kanal erhält (etwa weil das erforderliche ISDN-Leistungsmerkmal nicht zur Verfügung steht) oder eine unbekannte Rufnummer übertragen wird, nimmt Gateway 2 den Anruf entgegen, und die Geräte authentifizieren sich über den B-Kanal. Nach erfolgreicher Aushandlung übermittelt Gateway 1 seine IP-Adresse und baut den B-Kanal sofort wieder ab.

② Nun ist Gateway 2 an der Reihe: Zunächst baut es eine Verbindung zu seinem ISP auf, von dem es eine dynamische IP-Adresse zugewiesen bekommt.

③ Gateway 2 authentifiziert sich bei Gateway 1, dessen statische Adresse ihm bekannt ist.

④ Gateway 1 kennt nun die Adresse von Gateway 2 und kann den VPN-Tunnel zu Gateway 2 jetzt aufbauen.

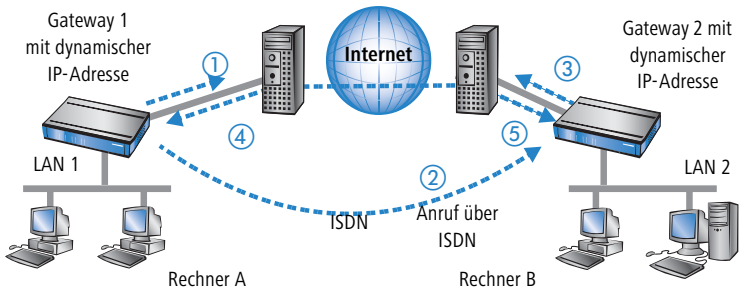
Der Vorteil der LANCOM-Geräte z.B. beim Aufbau der Verbindung aus der Zentrale zu den Filialen: Mit den Funktionen von LANCOM Dynamic VPN können auch Netzwerke ohne Flatrate erreicht werden, die also nicht „allways online" sind. Der ISDN-Anschluss ersetzt mit der bekannten MSN eine andere Adresse, z.B. eine statische IP-Adresse oder eine dynamische Adressauflösung über Dynamic-DNS-Dienste, die i.d.R. nur bei Flatrate-Anschlüssen zum Einsatz kommen.

Der beschriebene Verbindungsaufbau setzt bei beiden VPN-Gateways einen ISDN-Anschluss voraus, über den im Normalfall jedoch keine gebührenpflichtigen Verbindungen aufgebaut werden.

Beachten Sie auch die 'Hinweise zur Dynamic VPN Lizensierung' → Seite 10-9.

Dynamisch – dynamisch

Der Aufbau von VPN-Tunneln gelingt mit LANCOM Dynamic VPN auch zwischen zwei Gateways, die beide nur über dynamische IP-Adressen verfügen. Passen wir das besprochene Beispiel an, so dass diesmal auch Gateway 1 nur über eine dynamische IP-Adresse verfügt. Auch in diesem Beispiel möchte Rechner A eine Verbindung zu Rechner B aufbauen:



① Gateway 1 baut eine Verbindung zu seinem ISP auf, um eine öffentliche dynamische Adresse zu erhalten.

② Es folgt der Anruf über ISDN bei Gateway 2 zur Übermittlung dieser dynamischen Adresse. Zur Übermittlung werden drei Verfahren verwendet:

- **Als Information im LLC-Element des D-Kanals.** Über das D-Kanal-Protokoll von Euro-ISDN (DSS-1) können im sogenannten LLC-Element (**L**ower **L**ayer **C**ompatibility) beim Anruf zusätzliche Informationen an die Gegenstelle übermittelt werden. Diese Übermittlung findet vor dem Aufbau des B-Kanals statt. Die Gegenstelle lehnt nach erfolgreicher Übertragung der Adresse den Anruf ab. Eine gebührenpflichtige Verbindung über den B-Kanal kommt auf diese Weise nicht zustande. Die IP-Adresse wird aber trotzdem übertragen.

Das LLC-Element steht normalerweise im Euro-ISDN ohne besondere Anmeldung oder Freischaltung zur Verfügung. Es kann allerdings von Telefongesellschaften, einzelnen Vermittlungsstellen oder Telefonanlagen gesperrt werden. Im nationalen ISDN nach 1TR6 gibt es kein LLC-Element. Das beschriebene Verfahren funktioniert daher nicht.

- **Als Subadresse über den D-Kanal.** Funktioniert die Adressübermittlung über das LLC-Element nicht, dann versucht Gateway 1 die Adresse als sogenannte Subadresse zu übermitteln. Die Subadresse ist wie das LLC-Element ein Informationselement des D-Kanal-Protokolls und ermöglicht wie dieses die kostenlose Übermittlung kurzer Informationen. Allerdings muss hier die Telefongesellschaft das ISDN-Merkmal 'Subadressierung' (normalerweise gegen Berechnung) freischalten. Wie beim LLC-Element wird der Anruf nach

erfolgreicher Übertragung der IP-Adresse von der Gegenstelle abgelehnt und die Verbindung bleibt gebührenfrei.

- □ **Über den B-Kanal.** Scheitern beide Versuche, die IP-Adresse über den D-Kanal zu übertragen, dann muss für die Übertragung der IP-Adresse eine konventionelle Verbindung über den B-Kanal aufgebaut werden. Nach der Übertragung der IP-Adresse wird die Verbindung sofort abgebaut. Es fallen die üblichen Gebühren an.

③ Gateway 2 baut eine Verbindung zum ISP auf, der ihm eine dynamische IP-Adresse zuweist.

④ Gateway 2 authentifiziert sich bei Gateway 1 (dessen Adresse durch Schritt ② bekannt ist).

⑤ Gateway 1 kennt nun die Adresse von Gateway 2 und kann so den VPN-Tunnel zu Gateway 2 aufbauen.

Der beschriebene Verbindungsaufbau setzt bei beiden VPN-Gateways einen ISDN-Anschluss voraus.

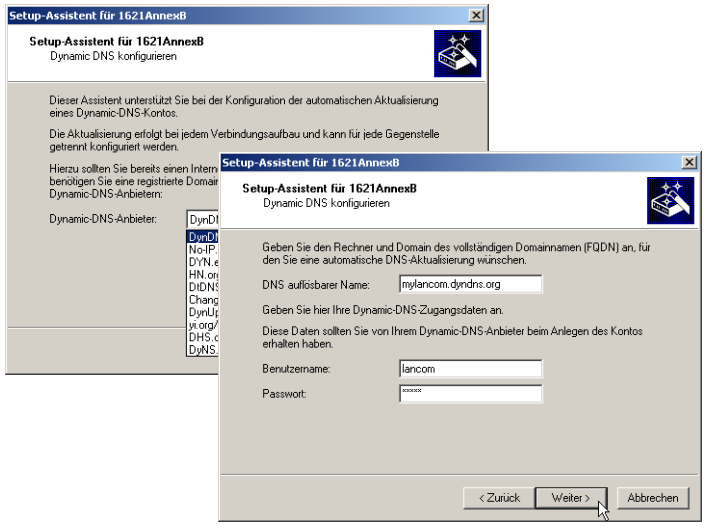
Beachten Sie auch die 'Hinweise zur Dynamic VPN Lizensierung' → Seite 10-9.

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. MyLANCOM@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 (siehe auch 'Dynamic DNS' auf Seite 14):



Aus Sicherheits- und Verfügbarkeitsgründen empfiehlt LANCOM Systems den Einsatz des Dynamic VPN Verfahrens gegenüber Dynamic DNS basierten VPN-Lösungen. Dynamic VPN basiert auf Verbindungen über das ISDN-Netz, das eine deutlich höhere Verfügbarkeit garantiert als die Erreichbarkeit eines Dynamic-DNS-Diensts im Internet.

10.4.3 Hinweise zur Dynamic VPN Lizensierung

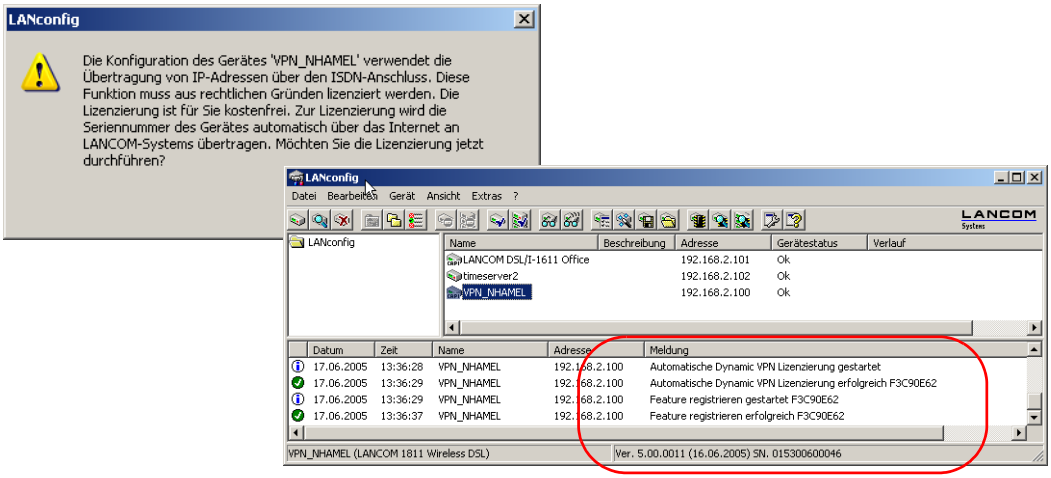
Aus patentrechtlichen Gründen muss die Verwendung der Funktion „Dynamic VPN" mit Übertragung der IP-Adressen über den ISDN-Anschluss lizensiert werden. Diese Betriebsart kommt in der Regel dann zum Einsatz, wenn Sie VPN-Kopplungen mit beidseitig dynamischen IP-Adressen nutzen und dabei keine Dynamic-DNS-Dienste verwenden. Alle anderen Betriebsarten von Dynamic VPN (also die Übermittlung der IP Adresse per ICMP, das Anklopfen bei der Gegenstelle per ISDN, um einen Rückruf herbeizuführen etc.) sind davon **nicht** betroffen.

Die Registrierung erfolgt anonym über das Internet, es werden keine Personen- oder Unternehmensspezifischen Daten übertragen.

Für die Registrierung der Dynamic-VPN-Option sind Administratorrechte auf dem Gerät erforderlich.

Registrieren über LANconfig

LANconfig erkennt beim Prüfen der Geräte z.B. direkt nach dem Programmstart automatisch, wenn ein Gerät aufgrund seiner Konfiguration registriert werden muss. Nach der Bestätigung der entsprechenden Meldung überträgt LANconfig automatisch die erforderlichen Daten des Gerätes an den Registrierungsserver von LANCOM Systems. Der Freischaltcode wird dann ebenfalls automatisch an das Gerät zurückübertragen und aktiviert. Der Vorgang kann in der Statuszeile von LANconfig beobachtet werden.



Registrieren über WEBconfig

Zur Registrierung über WEBconfig wird die Chargen- bzw. Seriennummer des zu registrierenden Produkts benötigt. Sie finden diese Informationen auf der Unterseite des Gerätes.



Beim Anmelden auf dem Gerät mit WEBconfig finden Sie im Menü Extras einen Link, der Sie zum Formular auf dem Registrierungsserver von LANCOM Systems führt. Geben Sie dort die Chargen/Seriennummer des Gerätes und Ihre E-Mailadresse an. Nach dem Absenden der Registrierungsanforderung erhalten Sie den Freischaltcode für das Gerät.

Um diesen Freischaltcode in Ihren Router zu laden, gehen Sie bitte wie folgt vor:

Melden Sie sich mit Administratorrechten unter WEBconfig auf dem entsprechenden Gerät an. Wählen Sie auf der Startseite den Eintrag **Software-Option freischalten** aus. Geben Sie auf der folgenden Seite den Freischaltcode ein und bestätigen Sie mit **Setzen**.

10.5 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.

10.5.1 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.

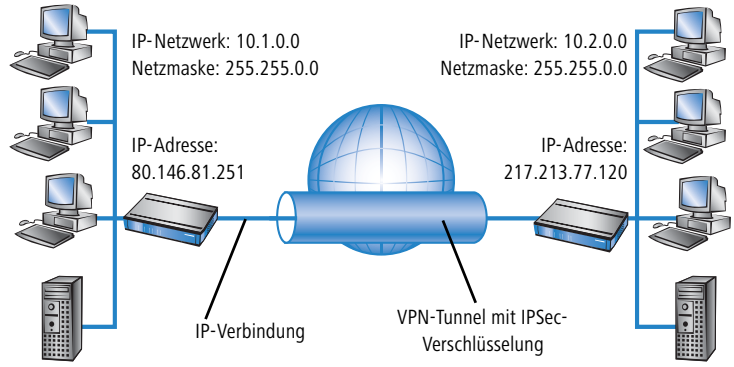
Um das gesicherte Routing der privaten IP-Adressbereiche über die Internet-Verbindung zu ermöglichen, wird zwischen den beiden LANs eine VPN-Verbindung etabliert, die auch als VPN-Tunnel bezeichnet wird.

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

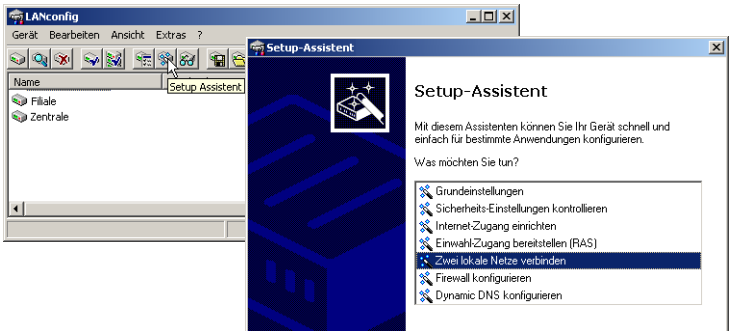


Diese Informationen sind in den so genannten VPN-Regeln enthalten.

10.5.2 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:

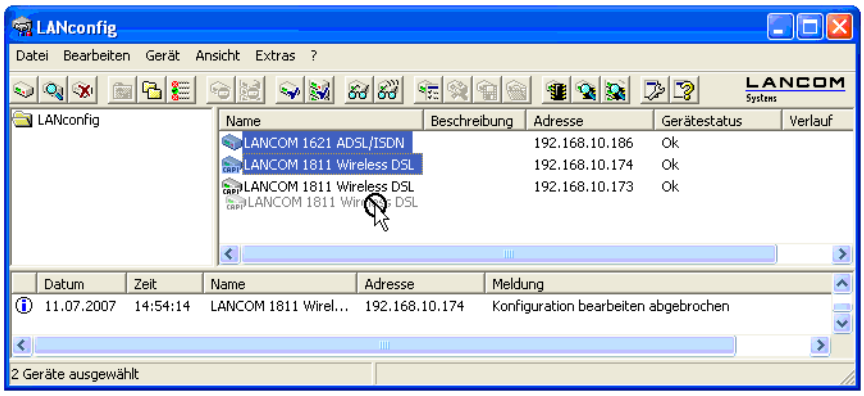
- Wenn kein Windows-Rechner mit LANconfig zur Konfiguration verwendet werden kann. In diesem Fall nehmen Sie die Einstellung der erforderlichen Parameter über WEBconfig oder die Telnet-Konsole vor.
- Wenn nicht das komplette lokale LAN (Intranet) über die VPN-Verbindung mit anderen Rechnern kommunizieren 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.

10.5.3 1-Click-VPN für Netzwerke (Site-to-Site)

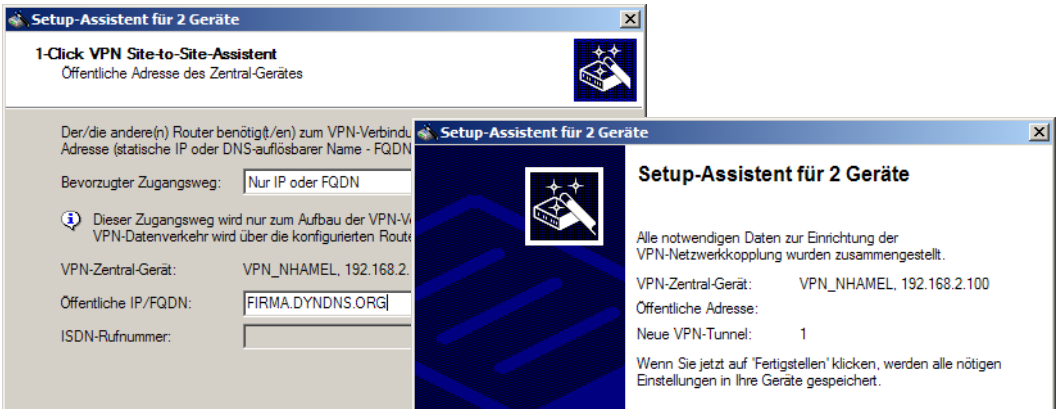
Die Einstellungen für die Kopplung von Netzwerken können sehr komfortabel über den 1-Click-VPN-Assistenten vorgenommen werden. Dabei können sogar mehrere Router gleichzeitig an ein zentrales Netzwerk gekoppelt werden.

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 oder über eine ISDN-Verbindung erfolgen soll. Geben Sie dazu die Adresse bzw. den Namen des zentralen Routers bzw. seine ISDN-Nummer 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.

10.5.4 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 LANCOM VPN Router 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.

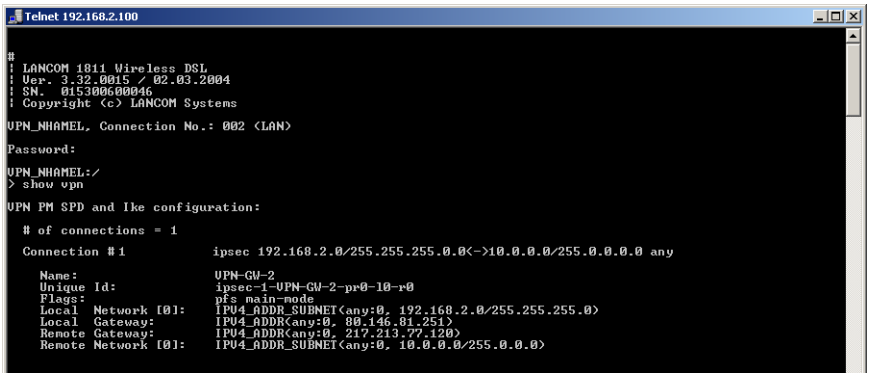
Beim Erstellen des VPN-Zugangs werden Einstellungen verwendet, die optimal auf die Verwendung im LANCOM Advanced VPN Client abgestimmt sind, darunter z.B.:

- Gateway: Sofern im LANCOM 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 LANCOM VPN Router
- Domäne: Sofern im LANCOM 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 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 LANCOM VPN Router zugewiesen.

10.5.5 VPN-Regeln einsehen

Da die VPN-Regeln stets eine Kombination von verschiedenen Informationen repräsentieren, werden diese Regeln in einem LANCOM-Gerät nicht direkt definiert, sondern aus verschiedenen Quellen zusammengestellt. Aus diesem Grund können die VPN-Regeln nicht über LANconfig oder ein anderes Konfigurations-Tool eingesehen werden.

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.

10.5.6 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 ’N:N-Mapping’ auf Seite 31 beachten.
- Bei Kopplung von Windows Netzwerken (NetBIOS/IP): Ohne WINS-Server auf beiden Seiten der VPN-Verbindung (z.B. bei der Anbindung von Home-Offices) kann das LANCOM entsprechende NetBIOS-Proxy-Funktionen übernehmen. Dazu muss das NetBIOS-Modul des LANCOM aktiviert sein, und die entsprechende VPN-Gegenstelle muss im NetBIOS-Modul als Gegenstelle eingetragen sein. Sind jedoch bei einer Standortkopplung in beiden Netzwerken eigene WINS-Server vorhanden, dann sollte das NetBIOS-Modul deaktiviert werden, so dass das LANCOM keine NetBIOS-Proxy-Funktionen mehr ausführt.

Um den NetBIOS-Proxy des LANCOM nutzen zu können muss entweder LANCOM Dynamic VPN verwendet werden, da dieses alle nötigen Adressen übermittelt, oder die IP-Adresse der Gegenstelle (hinter dem Tunnel, d.h. die dessen Intranet-Adresse) als primärer NBNS in der IP-Parameterliste (LANconfig: Kommunikation / Protokolle) eingetragen werden.

- 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“. Sollen auch Windows Netzwerke gekoppelt werden, so ist in diesem Eintrag zusätzlich NetBIOS zu aktivieren.

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 sowie je nach

Bedarf auch das Routing von "NetBIOS über IP". Die restlichen PPP-Parameter wie das Verfahren für die Überprüfung der Gegenstelle können analog zu anderen PPP-Verbindungen definiert werden.

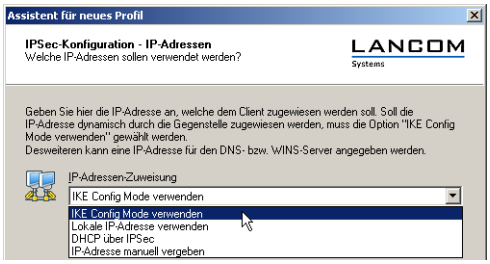
④ Die Hauptaufgabe bei der Einrichtung von VPN-Verbindungen liegt schließlich in der Definition der Netzbeziehungen: Welche IP-Adressbereiche sollen auf den beiden Seiten des VPN-Tunnels in die gesicherte Verbindung einbezogen werden?

10.5.7 IKE Config Mode

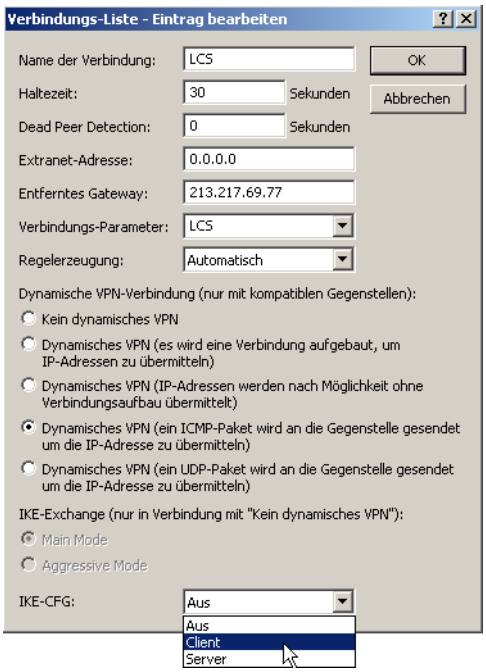
Bei der Konfiguration von VPN-Einwahlzugängen kann alternativ zur festen Vergabe der IP-Adressen für die einwählenden Gegenstellen auch ein Pool von IP-Adressen angegeben werden. In den Einträgen der Verbindungsliste wird dazu der „IKE-CFG"-Modus angegeben. Dieser kann die folgenden Werte annehmen:

- **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 ▶ Allgemein ▶ Verbindungs-Liste

WEBconfig: LCOS-Menübaum ▶ Setup ▶ VPN ▶ Name-Liste

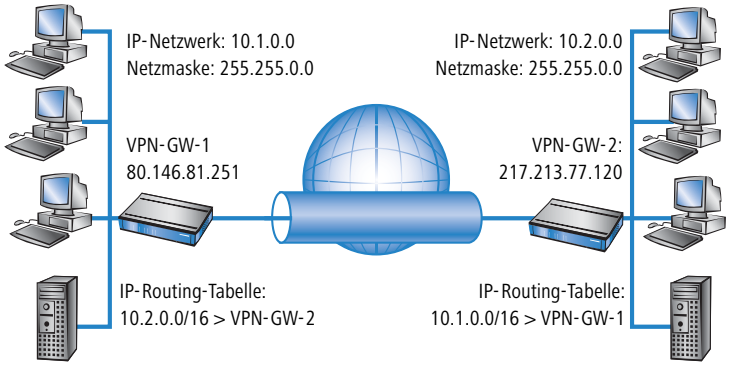
10.5.8 VPN- Netzbeziehungen erstellen

Mit der integrierten Firewall verfügen die LANCOM- Router über ein leistungsfähiges Instrument zur Definition von Quell- und Ziel- Adressbereichen, für die eine Datenübertragung (ggf. mit weiteren Einschränkungen) erlaubt bzw. verboten werden soll. Diese Funktionen werden auch für die Einrichtung der Netzbeziehungen für die VPN- Regeln verwendet.

Im einfachsten Fall kann die Firewall die VPN- Regeln automatisch erzeugen:

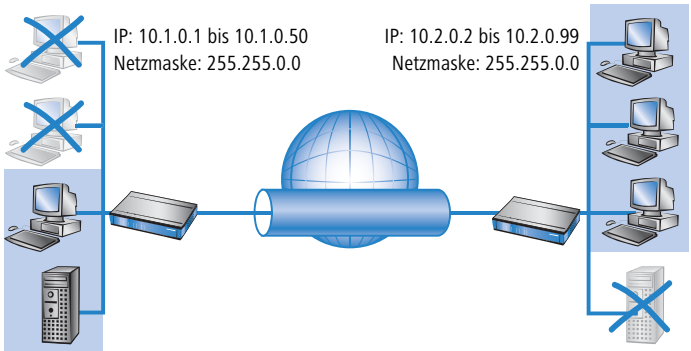
- Als Quellnetz wird dabei das lokale Intranet eingesetzt, also derjenige private IP- Adressbereich, zu dem das lokale VPN- Gateway selbst gehört.
- Als Zielnetze dienen für die automatisch erstellten VPN- Regeln die Netzbereiche aus der IP- Routing-Tabelle, für die als Router ein entferntes VPN- Gateway eingetragen ist.

Zum Aktivieren dieser automatischen Regelerzeugung reicht es aus, die entsprechende Option in der Firewall einzuschalten[1]. Bei der Kopplung von zwei einfachen lokalen Netzwerken kann die VPN- Automatik aus dem IP- Adressbereich des eigenen LANs und dem Eintrag für das entfernte LAN in der IP- Routing-Tabelle die erforderliche Netzbeziehung ableiten.



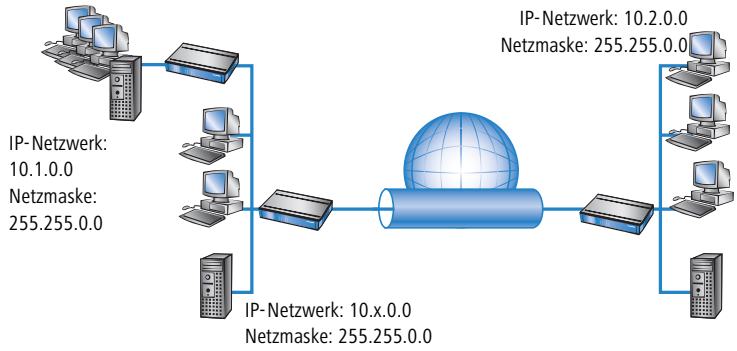
Etwas aufwändiger wird die Beschreibung der Netzbeziehungen dann, wenn die Quell- und Zielnetze nicht nur durch den jeweiligen Intranet- Adressbereich der verbundenen LANs abgebildet werden:

- Wenn nicht das gesamte lokale Intranet in die Verbindung mit dem entfernten Netz einbezogen werden soll, würde die Automatik einen zu großen IP- Adressbereich für die VPN- Verbindung freigeben.



- In vielen Netzstrukturen sind an das lokale Intranet über weitere Router noch andere Netzabschnitte mit eigenen IP- Adressbereichen angebunden. Diese Adressbereiche müssen über zusätzliche Einträge in die Netzbeziehung einbezogen werden.

1. automatisch bei Verwendung des VPN- Installationsassistenten unter LANconfig



In diesen Fällen müssen die Netzbeziehungen zur Beschreibung der Quell- und Zielnetze manuell eingetragen werden. Je nach Situation werden dabei die automatisch erzeugten VPN-Regeln erweitert, manchmal muss die VPN-Automatik ganz abgeschaltet werden, um unerwünschte Netzbeziehungen zu vermeiden.

Die erforderlichen Netzbeziehungen werden durch entsprechende Firewall-Regeln unter den folgenden Randbedingungen definiert:

- Für die Firewall-Regel muss die Option "Diese Regel wird zur Erzeugung von VPN-Regeln herangezogen" aktiviert sein.

Die Firewall-Regeln zur Erzeugung von VPN-Regeln sind auch dann aktiv, wenn die eigentliche Firewall-Funktion im LANCOM-Gerät nicht benötigt wird und ausgeschaltet ist!

- Als Firewall-Aktion muss auf jeden Fall "Übertragen" gewählt werden.
- Als Quelle und Ziel für die Verbindung können einzelne Stationen, bestimmte IP-Adressbereiche oder ganze IP-Netzwerke eingetragen werden.

Die Zielnetze müssen auf jeden Fall in der IP-Routing-Tabelle definiert sein, damit der Router in den LANCOM-Geräten die entsprechenden Datenpakete in das andere Netz weiterleiten kann. Die dort schon vorhandenen Einträge können Sie nutzen und nur ein übergeordnetes Netzwerk als Ziel eintragen. Die Schnittmenge aus dem Eintrag des Zielnetzes in der Firewall und den untergeordneten Einträgen in der IP-Routing-Tabelle fließt in die Netzbeziehungen für die VPN-Regeln ein.

Beispiel: In der IP-Routing-Tabelle sind die Zielnetze 10.2.1.0/24, 10.2.2.0/24 und 10.2.3.0/24 eingetragen, die alle über den Router VPN-GW-2 erreichbar sind. In der Firewall reicht ein Eintrag mit dem Zielnetz 10.2.0.0/16, um die drei gewünschten Subnetze in die VPN-Regeln einzubeziehen.

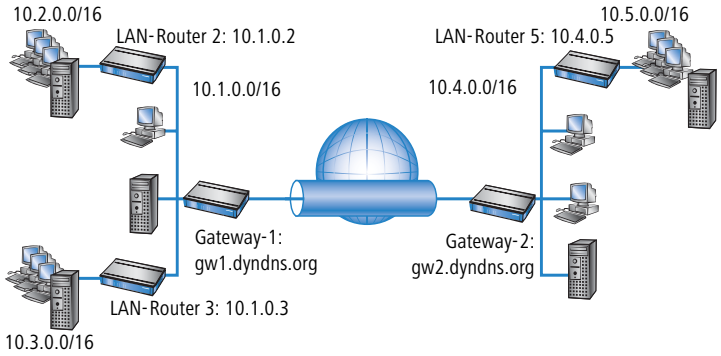
Die Quell- und Zielnetze müssen auf beiden Seiten der VPN-Verbindung übereinstimmend definiert werden. Es ist z.B. nicht möglich, einen größeren Ziel-Adressbereich auf einen kleineren Quell-Adressbereich auf der Gegenseite abzubilden. Maßgebend sind dabei die in den VPN-Regeln gültigen IP-Adressbereiche, nicht die in den Firewall-Regeln eingetragenen Netze. Diese können aufgrund der Schnittmengenbildung durchaus von den Netzbeziehungen in den VPN-Regeln abweichen.

- Je nach Bedarf kann die VPN-Verbindung zusätzlich auf bestimmte Dienste oder Protokolle eingeschränkt werden. So kann die VPN-Verbindung z.B. nur auf die Nutzung für ein Windows-Netzwerk reduziert werden.

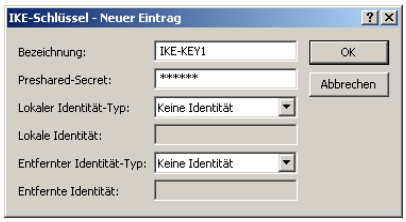
Verwenden Sie für diese Einschränkungen eigene Regeln, die nur für die Firewall gelten und nicht zur Erzeugung von VPN-Regeln herangezogen werden. Kombinierte Firewall/VPN-Regeln können sehr leicht komplex und schwer überschaubar werden.

10.5.9 Konfiguration mit LANconfig

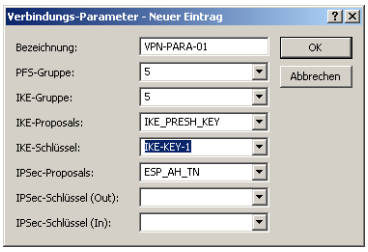
Dieser Anschnitt zeigt die Konfiguration einer LAN-LAN-Kopplung mit zusätzlichen Subnetzen mit Hilfe von LANconfig. In diesem Abschnitt wird das VPN-Gateway 1 konfiguriert, die Einstellung von Gateway 2 wird anschließend mit Hilfe von WEBconfig demonstriert.



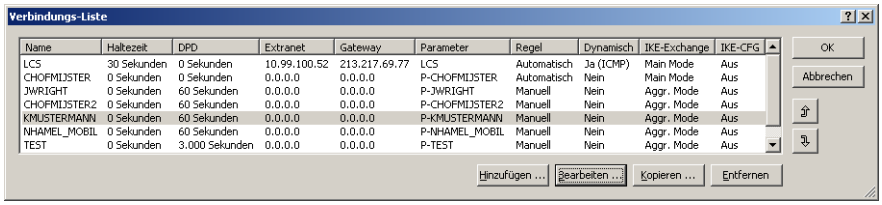
① Legen Sie im Konfigurationsbereich VPN auf der Registerkarte „IKE-Auth." einen neuen IKE-Schlüssel für die Verbindung an:



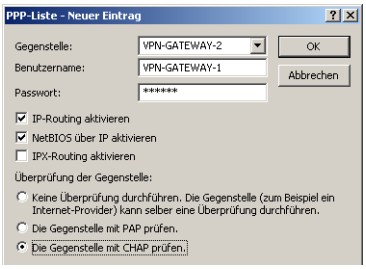
② Erstellen Sie auf der Registerkarte „Allgemein" einen neuen Eintrag in der Liste der Verbindungsparameter. Wählen Sie dabei den zuvor erstellten IKE-Schlüssel aus. PFS- und IKE-Gruppe können Sie ebenso wie IKE- und IPSec-Proposals aus den vorbereiteten Möglichkeiten wählen.



③ Erstellen Sie dann einen neuen Eintrag in der Verbindungs-Liste mit dem Namen des entfernten Gateways als „Name der Verbindung". Für LANCOM Dynamic VPN Verbindungen muss der Eintrag „Entferntes Gateway" leer bleiben. Andernfalls tragen Sie hier die öffentliche Adresse der Gegenstelle ein: entweder die feste IP-Adresse oder den DNS-auflösbaren Namen.

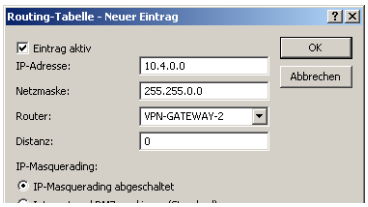


④ Bei Nutzung von LANCOM Dynamic VPN: Wechseln Sie in den Konfigurationsbereich „Kommunikation". Erstellen Sie auf der Registerkarte „Protokolle" in der PPP-Liste einen neuen Eintrag. Wählen Sie als Gegenstelle das entfernte VPN-Gateway aus, tragen Sie als Benutzernamen denjenigen VPN-Verbindungsnamen ein, mit dem das entfernte VPN-Gateway das lokale Gerät erreichen soll, und geben Sie ein geeignetes, auf beiden Seiten identisches Passwort ein, welches aus Sicherheitsgründen nicht identisch mit dem verwendeteten Pre-Shared Key sein sollte.



Aktivieren Sie auf jeden Fall das „IP-Routing" und je nach Bedarf „NetBIOS über IP" (→ Seite 10-14).

⑤ Wechseln Sie in den Konfigurationsbereich „IP-Router". Erstellen Sie auf der Registerkarte „Routing" einen neuen Eintrag in der Routingtabelle für jeden Netzbereich, der im entfernten und im lokalen LAN erreicht werden soll. Verwenden Sie dabei jeweils als Router das entfernte VPN-Gateway und schalten Sie das IP-Masquerading aus.



Für das „VPN-Gateway-1" sind die folgenden Einträge erforderlich, damit die entfernten Netzabschnitte erreicht werden:

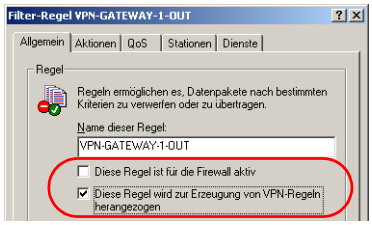
IP-Adresse	Netzmaske	Router	IP-Masquerading
10.4.0.0	255.255.0.0	VPN-Gateway-2	Nein
10.5.0.0	255.255.0.0	VPN-Gateway-2	Nein

Für die an das eigene LAN angebundenen Teilnetze wird als Router die IP-Adresse des jeweiligen LAN-Routers eingetragen:

IP-Adresse	Netzmaske	Router	IP-Masquerading
10.2.0.0	255.255.0.0	10.1.0.2	Nein
10.3.0.0	255.255.0.0	10.1.0.3	Nein

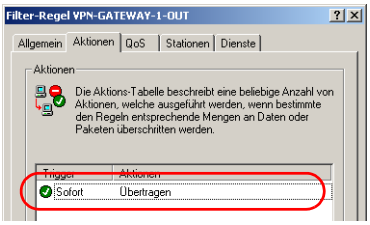
Mit diesen Einträgen ist das VPN-Gateway 1 in der Lage, auch die aus dem entfernten Netz eintreffen Pakete für die angebundenen Netzabschnitte richtig weiterzuleiten.

⑥ Wechseln Sie in den Konfigurationsbereich „Firewall/QoS". Erstellen Sie auf der Registerkarte „Regeln" eine neue Firewall-Regel mit dem Namen „VPN-GATEWAY-1-OUT" und aktivieren Sie für diese Regel die Option „Diese Regel wird für die Erzeugung von VPN-Regeln herangezogen". Damit legen Sie fest, dass die in dieser Regel beschriebenen IP-Netzwerke für die Bildung von VPN-Netzbeziehungen verwendet werden.

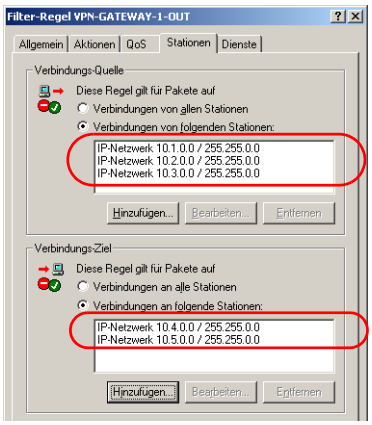


Die Firewall-Regeln zum Erzeugen von VPN-Netzbeziehungen mit Angabe der Tunnelendpunkte (IP-Quell- und Ziel-Adressen) sollten auf jeden Fall von Firewall-Regeln zum Filtern (z.B. der zu übertragenden bzw. der zu sperrenden Protokolle) getrennt werden. Die Verknüpfung dieser beiden Aspekte kann zu einer hohen Anzahl der intern verwalteten VPN-Beziehungen und damit zu Performanceverlusten in den VPN-Tunneln führen.

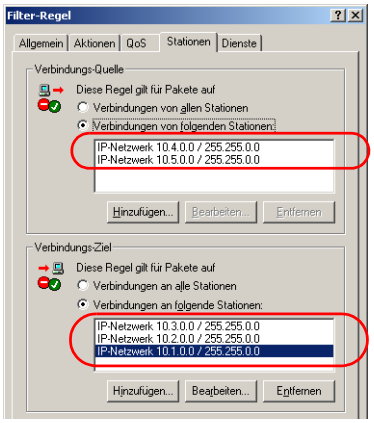
⑦ Auf der Registerkarte „Aktionen" dieser Firewall-Regel stellen Sie als Paketaktion „Übertragen" ein.



⑧ Auf der Registerkarte „Stationen" dieser Firewall-Regel stellen Sie für die ausgehende Datenübertragung als Quelle die Teilnetze auf der lokalen Seite ein, als Ziel alle Teilnetze auf der entfernten Seite.



⑨ Für die eingehende Datenübertragung erstellen Sie eine Firewall-Regel unter dem Namen „VPN-GATEWAY-1-IN" mit den gleichen Parametern wie die vorherige Regel. Nur bei den Stationen sind hier die Quell- und Zielnetze vertauscht:



10.5.10 Konfiguration mit WEBconfig

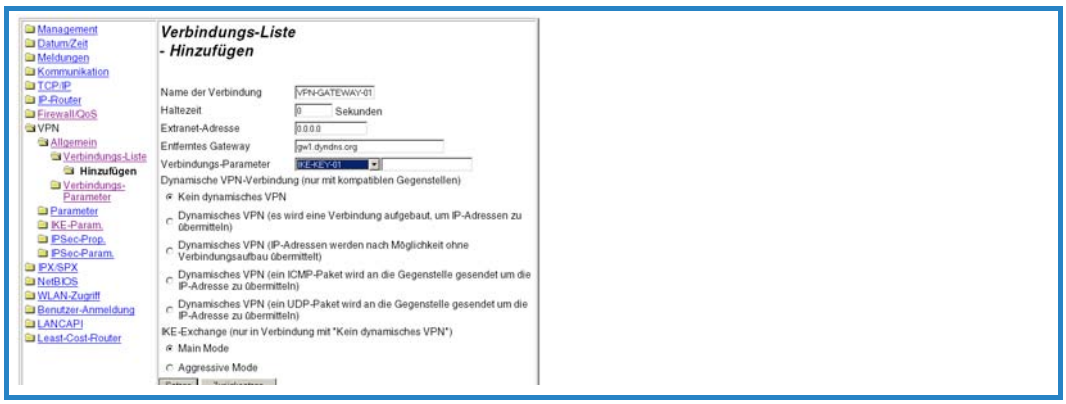
① Legen Sie unter **Konfiguration ▶ VPN ▶ IKE-Param. ▶ IKE-Schlüssel** einen neuen IKE-Schlüssel für die Verbindung an:



② Erstellen Sie unter **Konfiguration ▶ VPN ▶ Allgemein ▶ Verbindungsparameter** einen neuen „VPN-Layer" für die Verbindungsparameter. Wählen Sie dabei den zuvor erstellten IKE-Schlüssel aus.



③ Erstellen Sie unter **Konfiguration ▶ VPN ▶ Verbindungsliste** einen neuen Eintrag mit dem Namen des entfernten Gateways als „Name". Als „Entferntes Gateway" tragen Sie die öffentliche Adresse der Gegenstelle ein: entweder die feste IP-Adresse oder den DNS-auflösbaren Namen.



④ Bei Nutzung von LANCOM Dynamic VPN: Erstellen Sie unter **Konfiguration ▶ Setup ▶ WAN ▶ PPP** einen neuen Eintrag.
Wählen Sie als Gegenstelle das entfernte VPN-Gateway aus, tragen Sie als Benutzernamen denjenigen VPN-Verbindungsnamen ein, mit dem das entfernte VPN-Gateway das lokale Gerät erreichen soll, und geben Sie geeignetes, auf beiden Seiten identisches Passwort ein.



Aktivieren Sie auf jeden Fall das „IP-Routing" und je nach Bedarf „NetBIOS über IP" (→ Seite 10-14).

⑤ Erstellen Sie unter **Konfiguration ▶ Setup ▶ IP-Router ▶ IP-Routing-Tabelle** einen neuen Eintrag für jeden Netzbereich, der im entfernten und im lokalen LAN erreicht werden soll. Verwenden Sie dabei jeweils als Router das entfernte VPN-Gateway und schalten Sie das IP-Masquerading aus.



Für das „VPN-Gateway-2" sind die folgenden Einträge erforderlich, damit die entfernten Netzabschnitte erreicht werden:

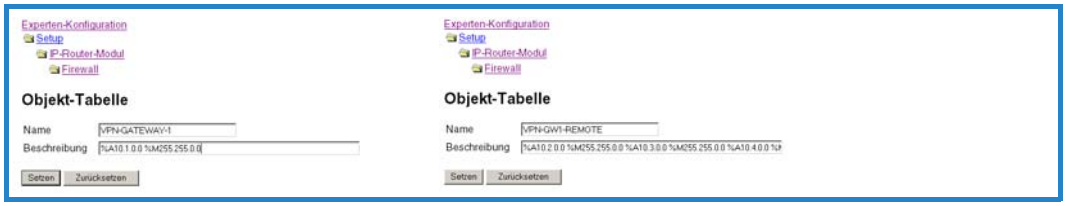
IP-Adresse	Netzmaske	Router	IP-Masquerading
10.1.0.0	255.255.0.0	VPN-Gateway-1	Nein
10.2.0.0	255.255.0.0	VPN-Gateway-1	Nein
10.3.0.0	255.255.0.0	VPN-Gateway-1	Nein

Für die an das eigene LAN angebundenen Teilnetze wird als Router die IP-Adresse des jeweiligen LAN-Routers eingetragen:

IP-Adresse	Netzmaske	Router	IP-Masquerading
10.5.0.0	255.255.0.0	10.4.0.5	Nein

Mit diesen Einträgen ist das VPN-Gateway 2 in der Lage, auch die aus dem entfernten Netz eintreffenden Pakete für die angebundenen Netzabschnitte richtig weiterzuleiten.

⑥ Erstellen Sie unter **Konfiguration ▶ Firewall/QoS ▶ Objekt-Tabelle** jeweils einen Eintrag für die Netzbereiche, die bei der VPN-Verbindung mit „VPN-GATEWAY-1" als Quelle oder Ziel verwendet werden sollen („VPN-GW1-LOCAL" und „VPN-GW1-REMOTE"). Geben Sie dabei die Netzbereiche z.B. in der Form „%A10.1.0.0 %M255.255.0.0" ein.



⑦ Erstellen Sie unter **Konfiguration ▶ Firewall/QoS ▶ Regel-Tabelle** eine neue Firewall-Regel mit dem Namen „VPN-GW1-OUT". Verwenden Sie dabei die Objekte „VPN-GW1-LOCAL" und „VPN-GW1-REMOTE", die Protokolle „ANY" und die Aktion „ACCEPT". Aktivieren Sie die Option „VPN-Regel", damit die in dieser Regel beschriebenen IP-Netzwerke für die Bildung von VPN-Netzbeziehungen verwendet werden.



In der Regel empfiehlt sich die Trennung von Regeln, mit denen die VPN-Netzbeziehungen gebildet werden, und den Firewall-Regeln, die Auswirkungen z.B. auf die bei der Kommunikation zugelassenen Dienste haben.

⑧ Für die eingehende Datenübertragung erstellen Sie eine Firewall-Regel unter dem Namen „VPN-GW1-IN" mit den gleichen Parametern wie die vorherige Regel. Nur bei den Stationen sind hier die Quell- und Zielnetze vertauscht:



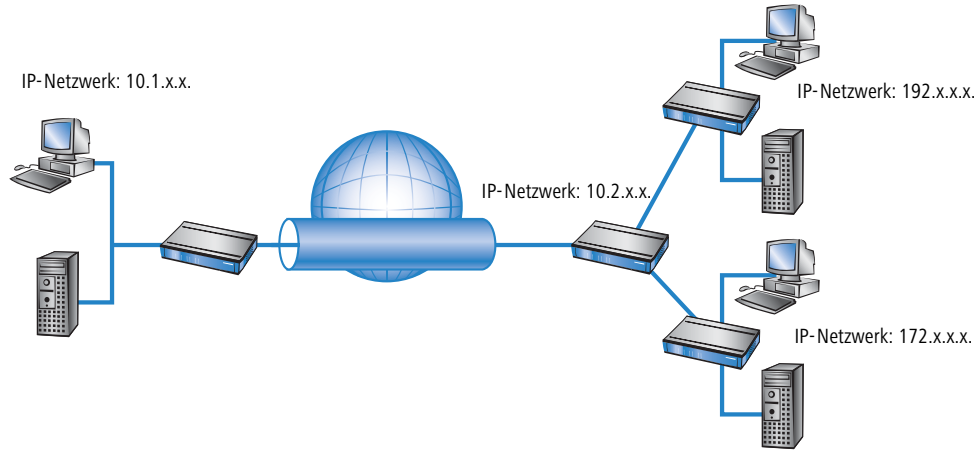
10.5.11 Gemeinsamer Aufbau von Security Associations

Die Basis für den Aufbau eines VPN-Tunnels zwischen zwei Netzwerken stellen die „Security Associations" (SAs) dar. In einer SA sind u.a. folgende Parameter definiert:

- IP-Adressen von Quell- und Zielnetzwerk
- Verfahren zur Verschlüsselung, Integritätsprüfung und Authentifizierung
- Schlüssel für die Verbindung
- Gültigkeitsdauer der verwendeten Schlüssel

Die Security Associations werden durch automatisch oder manuell erzeugte VPN-Regeln definiert (siehe auch 'VPN-Netzbeziehungen erstellen' → Seite 10-16 im Referenzhandbuch).

Der Aufbau der Security Associations wird normalerweise durch ein IP-Paket angestossen, das vom Quell- ins Zielnetz übertragen werden soll. Im Fall von Keep-Alive-Verbindungen ist dies ein ICMP-Paket, daß durch einen Eintrag in der Polling-Tabelle an die Gegenstelle verschickt wird.



In komplexen Netzwerk-Szenarien kommt es vor, dass zwischen zwei VPN-Gateways mehrere Netzbeziehungen definiert sind. Wird nun ein einzelnes IP-Paket übertragen, dann werden auch nur die SAs für genau diese eine, auf dieses Paket passende Netzbeziehung aufgebaut. Zum Aufbau der anderen SAs werden wiederum zu den anderen Netzbeziehungen passende IP-Pakete benötigt.

Der Aufbau von SAs aufgrund von Datenpaketen benötigt zum einen Zeit und zum anderen führt es zu Paketverlusten, solange die SAs noch nicht installiert sind. Aber gerade das ist – insbesondere bei Keep-Alive Verbindungen – oft nicht gewünscht. Stattdessen sollen **alle** SAs **sofort** aufgebaut werden, die zu den in der Gegenstelle definierten Netzbeziehungen passen. Da aber das Aushandeln aller SAs gerade in komplexen Szenarien viel CPU-Leistung benötigt, kann das Verhalten über den Parameter „SA-Aufbau-gemeinsam" festgelegt werden.

- **SA-Aufbau-gemeinsam**
  - □ Ja: Alle im Gerät definierten SAs werden aufgebaut.
  - □ Nein [Default]: Nur die explizit durch ein zu übertragenes Paket angesprochene SA wird aufgebaut.
  - □ nur-bei-KeepAlive: Alle definierten SAs werden aufgebaut, für deren Gegenstelle in der VPN-Verbindungsliste eine Haltezeit von '9999' eingestellt ist (Keep Alive).

  WEBconfig: LCOS-Menübaum ▶ Setup ▶ VPN

Die Voreinstellung für den ausschließlichen Aufbau von explizit angesprochenen SAs reicht in den meisten Fällen aus, insbesondere wenn nur automatisch erzeugte VPN-Regeln verwendet werden.

Die aktuell vorhandenen SAs können unter /Status/VPN eingesehen werden.

10.5.12 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 Telnet-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.

10.6 Einsatz von digitalen Zertifikaten

Die Sicherheit der Kommunikation über VPN erfüllt im Kern drei Anforderungen:

- **Vertraulichkeit**: Die übertragenen Daten können von keinem Unbefugten gelesen werden (über Verschlüsselung).
- **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.

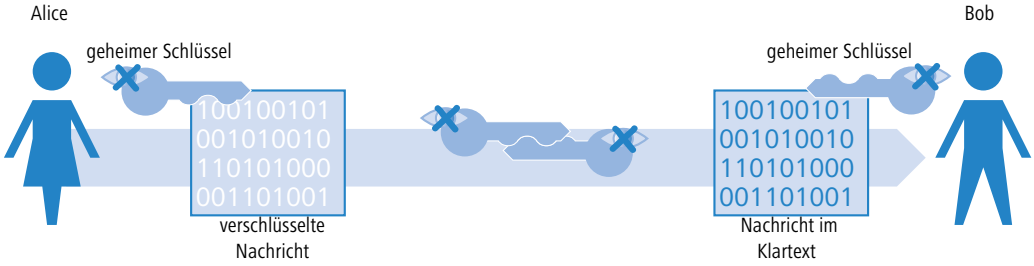
10.6.1 Grundlagen

Verschlüsselungsverfahren kann man in zwei Kategorien einteilen: Die symmetrische und die asymmetrische Verschlüsselung.

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:

- 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.
- 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.

Das Verfahren der asymmetrischen Verschlüsselung

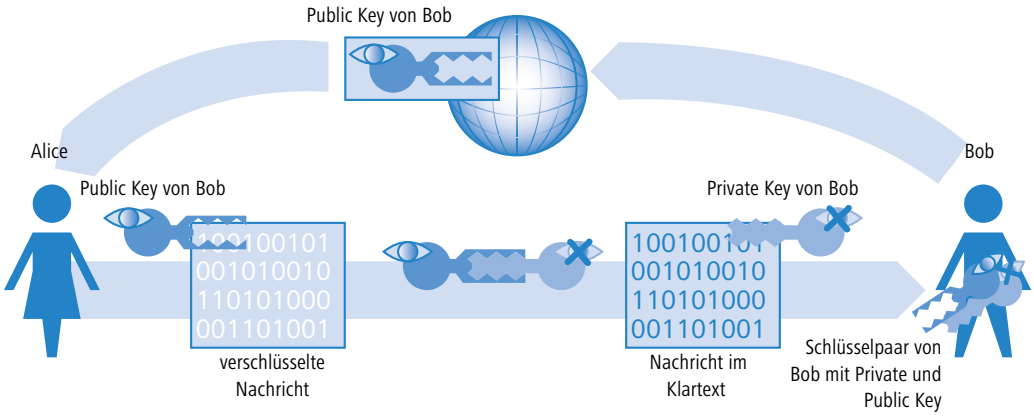
Als grundlegend neuer Ansatz wurde in den 1970er Jahren die asymmetrische Verschlüsselung entwickelt. Diese Variante setzt nicht mehr auf einen Schlüssel, der auf beiden Seiten bekannt und dabei geheim ist, sondern auf ein Schlüsselpaar:

- 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:

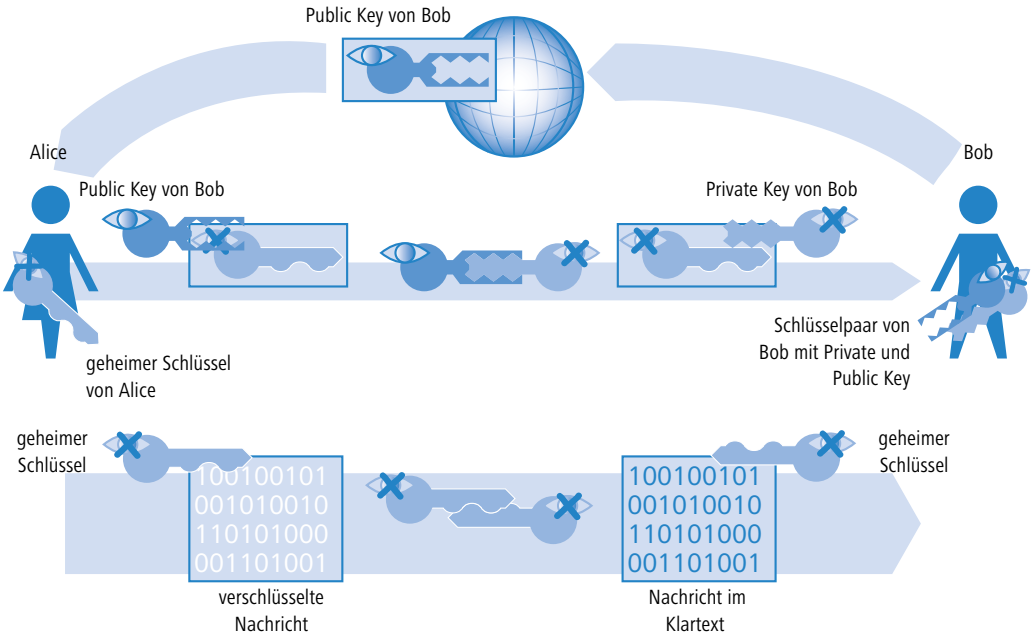
- Es wird nicht für jede Kommunikationsbeziehung ein Schlüsselpaar benötigt, sondern nur für jeden Teilnehmer. Bei 1000 Teilnehmern benötigt jeder nur sein eigenes Schlüsselpaar, von dem er den Public Key öffentlich zur Verfügung stellt. Anstelle der 500.000 geheimen Schlüssel werden beim Public Key-Verfahren 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.

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 gehei-

men Schlüssels zu schützen. Die eigentlichen Nutzdaten der Verbindung werden anschließend mit den schnelleren symmetrischen Verfahren verschlüsselt.



- Bob erstellt im ersten Schritt sein Schlüsselpaar und stellt den Public Key öffentlich bereit.
- 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.
- Nur Bob kann den geheimen Schlüssel nun wieder mit Hilfe seines Private Keys **ent**schlüsseln.
- Alice und Bob verwenden dann den geheimen Schlüssel zum **Ver**- und **Ent**schlüsseln der deutlich größeren Nutzdaten-Volumina.

Public-Key-Infrastructure

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.

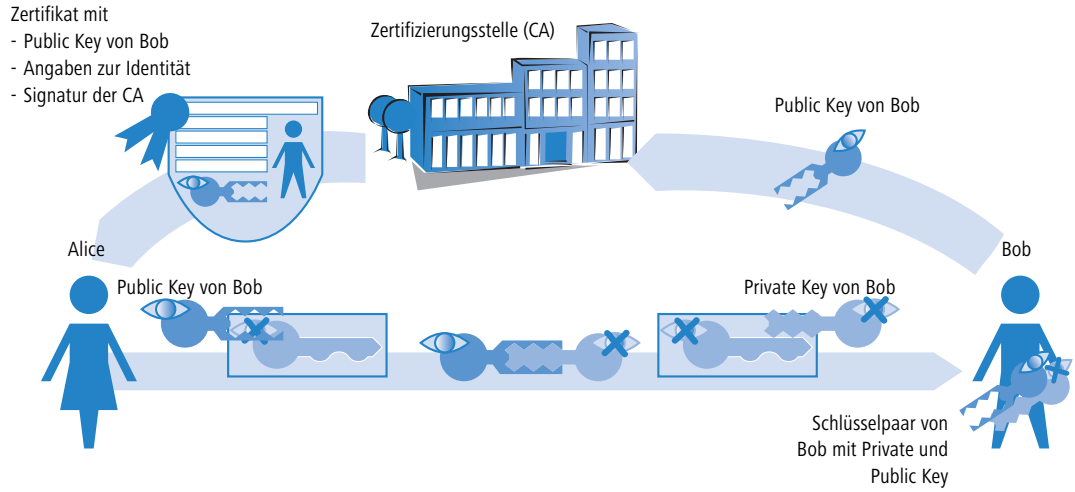
Um dieses Vertrauen zu sichern, können die verwendeten Schlüsselpaare der asymmetrischen Verschlüsselung von öffentlich anerkannten, vertrauenswürdigen Stellen bestätigt werden. So ist z.B. in Deutschland die Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen die oberste 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:

- Auch die CA verfügt über ein Schlüsselpaar aus Private und Public Key. Als vertrauenswürdige Stelle kann ihr eigenes Schlüsselpaar als zuverlässig angesehen werden.
- 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.
- 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.

10.6.2 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 oder Notebooks wird verhindert.

Den Vorteilen von Zertifikaten steht allerdings der höhere Aufwand für die Einführung und Pflege einer Public Key Infrastructure (PKI) gegenüber.

10.6.3 Aufbau von Zertifikaten

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. Die derzeit (06/2005) aktuelle Version ist 'v3'.
- 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, Email-Adresse, Nationalität etc.
- Subject: Daten zur Identifizierung des Eigentümers des Zertifikates, z.B. Name, Institution, Email-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.

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.

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
```

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 PCKS#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 -----`

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.

10.6.4 Sicherheit

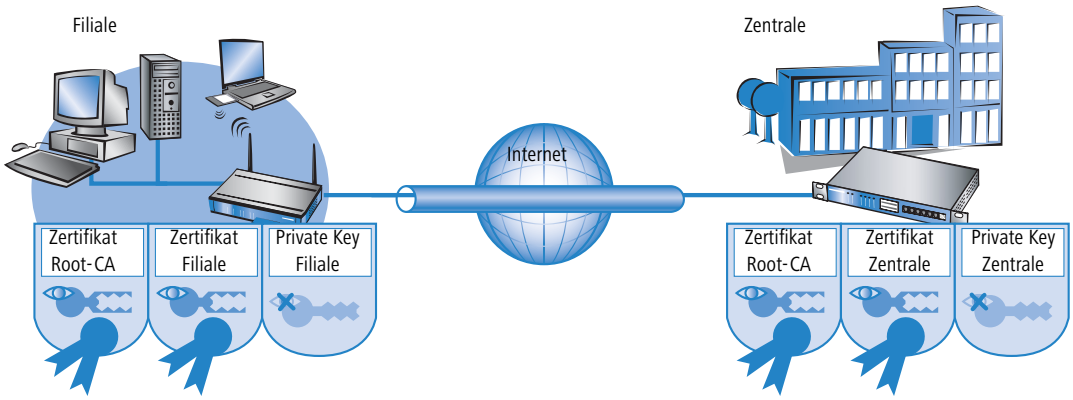
Auch beim Umgang mit Zertifikaten sind bestimmte Sicherheitsaspekte zu beachten:

- 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.

10.6.5 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 müs-

sen auf beiden Seiten der Verbindung (z.B. Anbindung einer Filiale an das Netzwerk der Zentrale über LANCOM-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) und nur während dieser Verbindung berechnen können.
- 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.

10.6.6 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.

10.6.7 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 2003 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.

10.6.8 Anfordern eines Zertifikates mit der Stand-alone Windows CA

Für die Verwendung in einem LANCOM leistet eine Kombination aus PKCS#12-Datei mit Root-Zertifikat, eigenem Geräte Zertifikat und Public Key des Gerätes die besten Dienste.

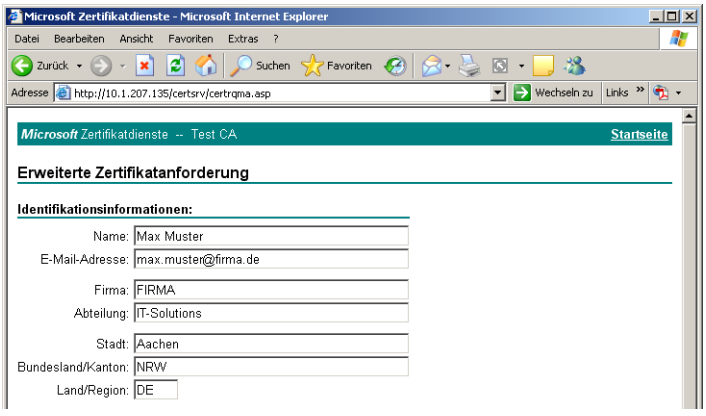
① Rufen Sie in Ihrem Browser die Startseite des Microsoft Zertifikatsdienstes auf.

② Wählen Sie als Zertifikatstyp die 'erweiterte Zertifikatanforderung'.

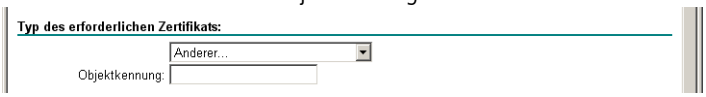
③ Wählen Sie im nächsten Schritt die Option 'Eine Anforderung an diese Zertifikatsstelle erstellen und einreichen'.

Nur wenn das Root-Zertifikat schon in einer separaten Datei vorliegt, wählen Sie hier die Option 'BASE64'.

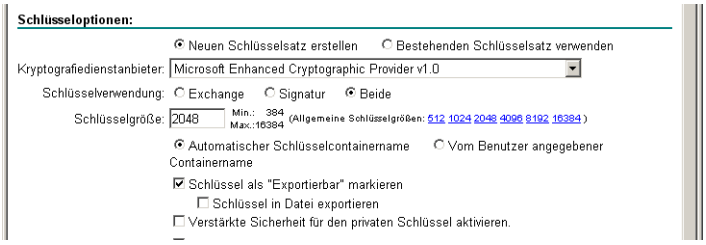
④ Im nächsten Schritt werden die Daten zur Identifikation eingetragen.



⑤ Wählen Sie im gleichen Dialog als Typ des Zertifikats die Option 'Anderer...' und löschen Sie den daraufhin erscheinenden Wert für die 'Objektkennung'.



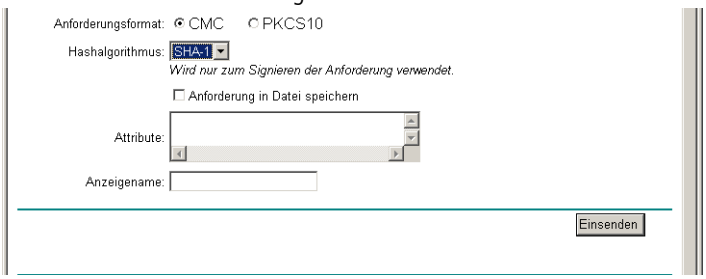
⑥ Markieren Sie die 'Automatische Schlüsselerstellung'. Damit werden Public und Private Key für den aktuellen Benutzer automatisch von der CA erstellt.



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, die für die Weiterverarbeitung in einem LANCOM 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.

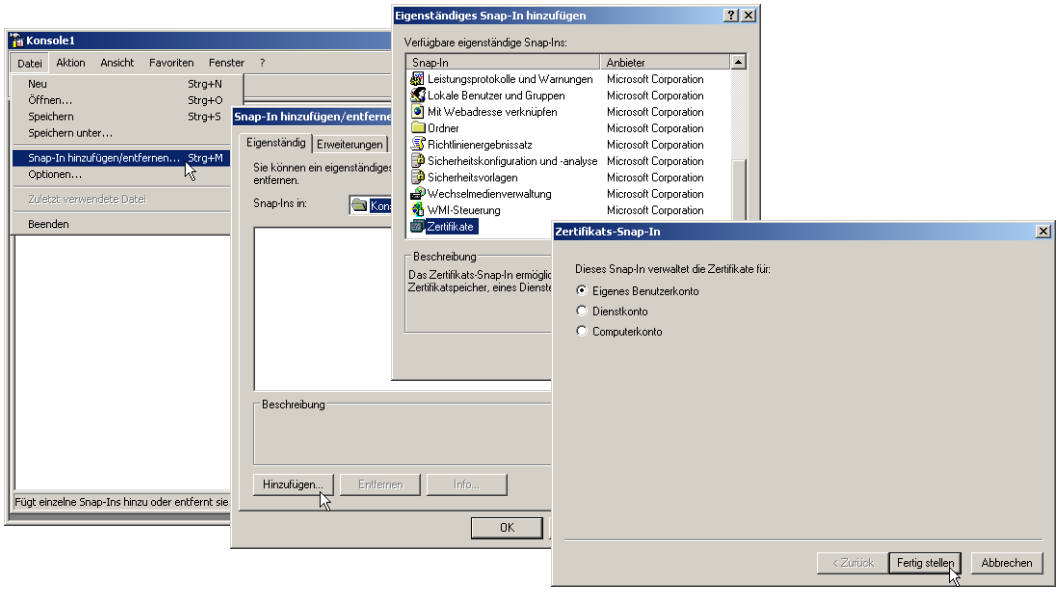
Sie können die Zertifikate nur auf dem gleichen Rechner installieren, mit dem Sie die Anforderung eingereicht haben.

10.6.9 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 LANCOM. Um zu einem Zertifikat in Dateiform zu gelangen, müssen Sie es zunächst exportieren.

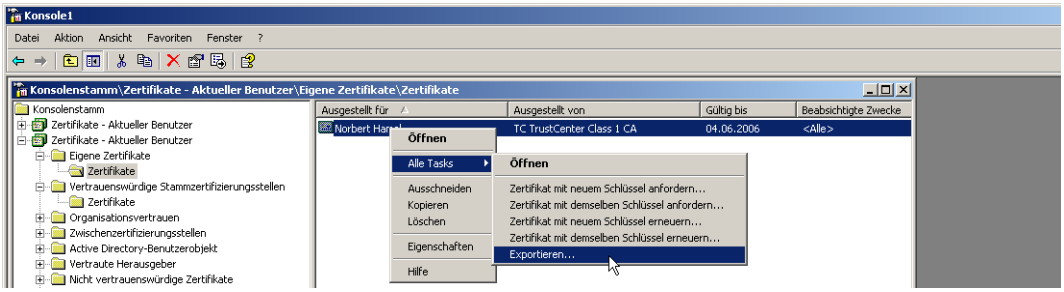
Export über den Windows-Konsolenstamm

① Öffnen Sie dazu die Management-Konsole über den Befehl `mmc` an der Eingabeaufforderung und wählen Sie den Menüpunkt **Datei ▶ Snap-In hinzufügen/entfernen**.

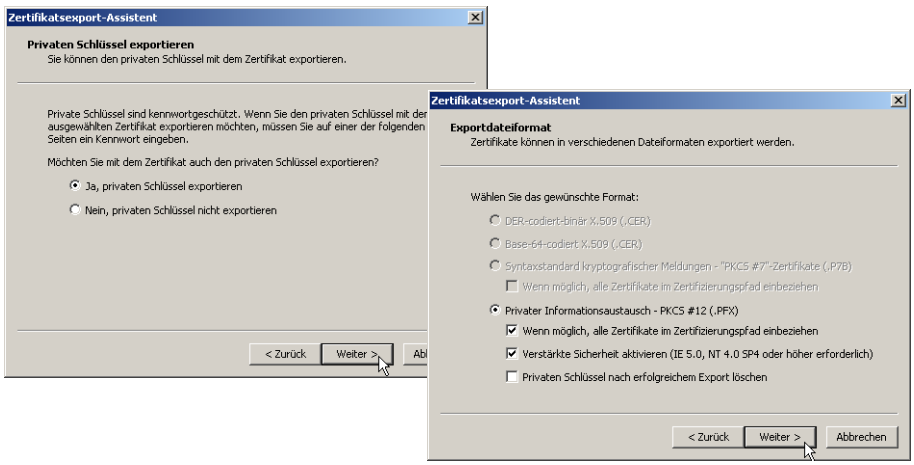


② Klicken Sie auf **Hinzufügen...** und wählen Sie den Eintrag 'Zertifikate'. Bestätigen Sie mit **Hinzufügen**, markieren Sie anschließend 'Eigenes Benutzerkonto' und klicken Sie auf **Fertig stellen**.

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 Tasks ▶ 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 'alle Zertifikate in den Zertifizierungspfad mit 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 LANCOM wieder benötigen.

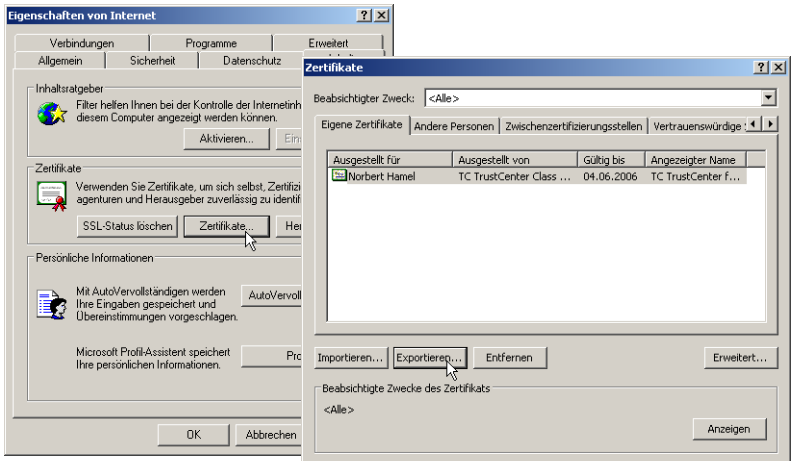
Für das Kennwort werden je nach Umgebung auch die synonymen Begriffe „Passwort“ oder „PIN“ verwendet.

Export über die Systemsteuerung

Alternativ können Sie die auf dem System installierten Zertifikate über die Systemsteuerung öffnen.

① Wählen Sie dazu **Start** ▶ **Systemsteuerung** ▶ **Internetoptionen** und dort auf der Registerkarte 'Inhalte' die Schaltfläche **Zertifikate**.

② Wählen Sie das gewünschte Zertifikat aus und klicken Sie auf **Exportieren**.



Der folgende Zertifikatsexportassistent verhält sich genau so wie unter 'Export über den Windows-Konsolenstamm' → Seite 10-33 beschrieben.

10.6.10 Zertifikate mit OpenSSL erstellen

Mit OpenSSL steht eine weitere Möglichkeit zur Verfügung, eigene Zertifikate zu erstellen und Zertifikats-Verbindungen zu testen. OpenSSL ist als OpenSource-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.

OpenSSL installieren

① Laden Sie eine aktuelle OpenSSL-Version von http://www.slproweb.com/products/Win32OpenSSL.html.

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`.

Zertifikat für Root-CA ausstellen

① Erstellen Sie einen Schlüssel für die CA mit dem Befehl:

```
genrsa -des3 -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.

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 ('Zertifikate in das LANCOM laden' → Seite 10-35).

10.6.11 Zertifikate in das LANCOM laden

Für den zertifikatgesicherten VPN-Verbindungsaufbau müssen in einem LANCOM 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 **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 **Expertenkonfiguration ▶ Status ▶ Datei-System ▶ Inhalt** eingesehen werden.



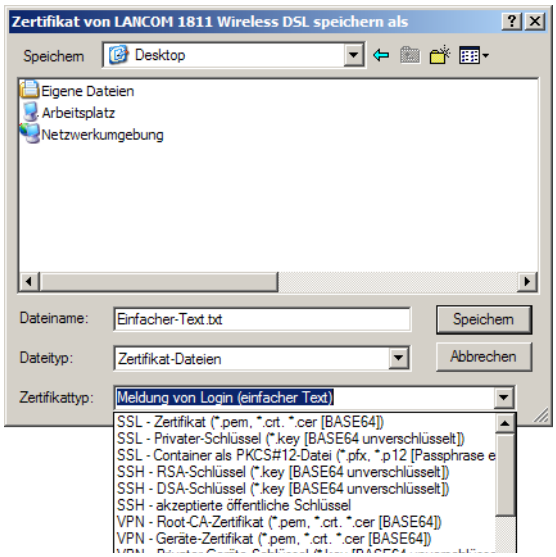
Eine kombinierte PKCS#12-Datei wird beim Upload automatisch in die benötigten Teile zerlegt.

10.6.12 Zertifikate sichern und hochladen mit LANconfig

In einem LANCOM 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 ▶ Zertifikat als Datei sichern** bzw. **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 Kennwort (Passphrase) notwendig.

10.6.13 VPN-Verbindungen auf Zertifikatsunterstützung einstellen

VPN-Verbindungen mit Zertifikatsunterstützung können nur aufgebaut werden, wenn das LANCOM 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.

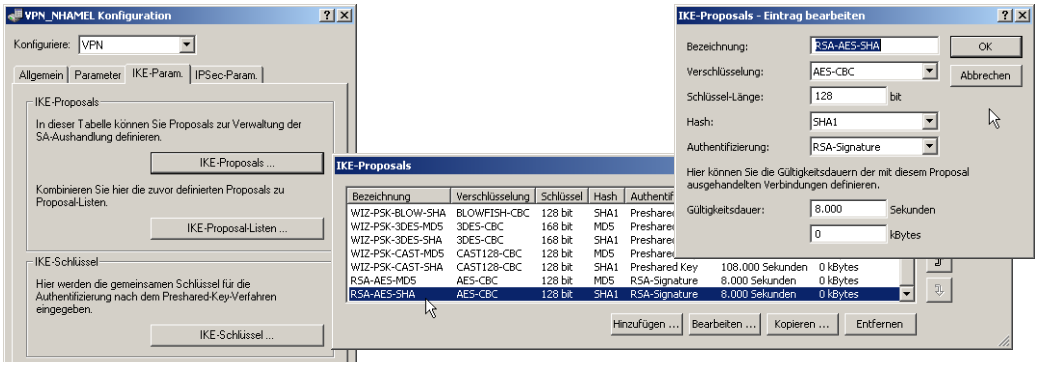
Um VPN-Verbindungen auf die Unterstützung von Zertifikaten einzustellen, müssen verschiedene Teile der Konfiguration entsprechend vorbereitet werden:

- 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!

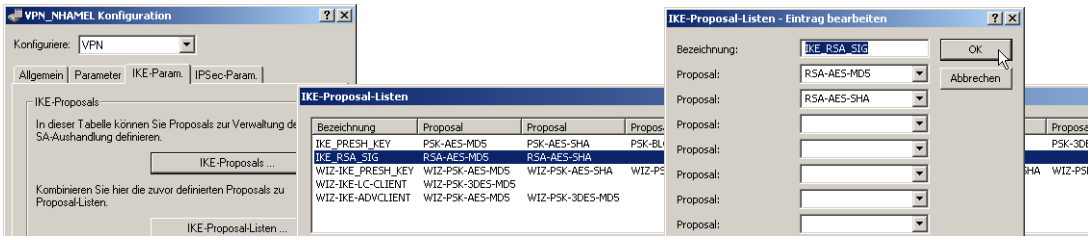
① In den Listen der Proposals werden zwei neue Proposals mit den exakten Bezeichnung 'RSA-AES-MD5' und 'RSA-AES-SHA' benötigt, die beide als Verschlüsselung 'AES-CBC' und als Authentifizierungsmodus 'RSA-Signature' verwenden und sich nur im Hash-Verfahren (MD5 bzw. SHA1) unterscheiden.



LANconfig: VPN ▶ IKE-Param. ▶ IKE-Proposals

WEBconfig: LCOS-Menübaum ▶ Setup ▶ VPN ▶ Proposals ▶ IKE

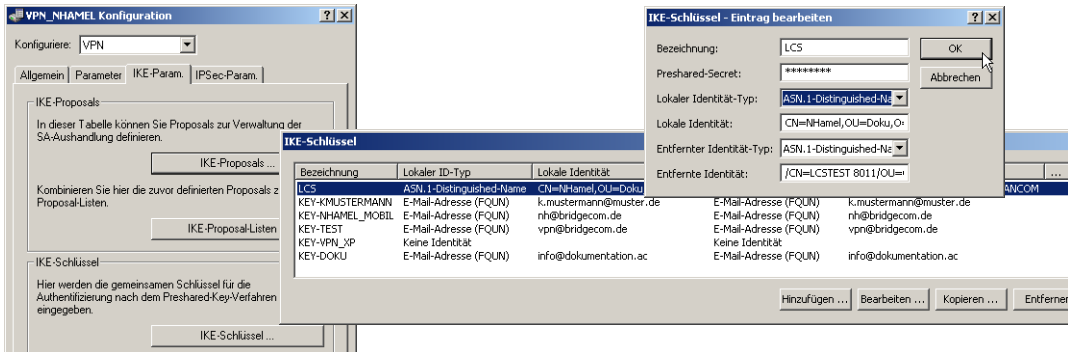
② In den Proposal-Listen wird eine neue Liste benötigt mit der exakten Bezeichnung 'IKE_RSA_SIG', in der die beiden neuen Proposals 'RSA-AES-MD5' und 'RSA-AES-SHA' aufgeführt sind.



LANconfig: VPN ▶ IKE-Param. ▶ IKE-Proposallisten

WEBconfig: LCOS-Menübaum ▶ Setup ▶ VPN ▶ Proposals ▶ IKE-Proposal-Listen

③ In der Liste der IKE-Schlüssel müssen für alle Zertifikats-Verbindungen die entsprechenden Identitäten eingestellt werden.



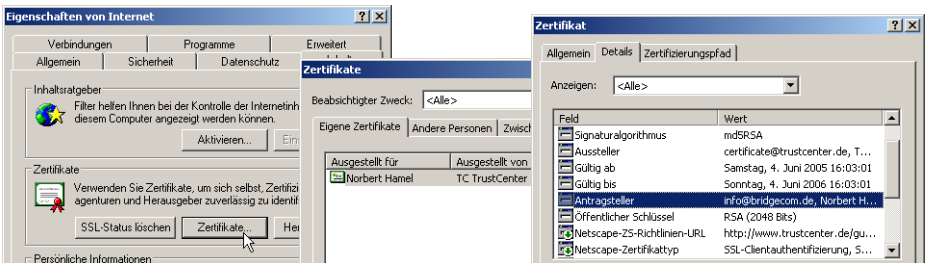
LANconfig: VPN ▶ IKE-Param. ▶ IKE-Schlüssel

WEBconfig: LCOS-Menübaum ▶ Setup ▶ VPN ▶ Proposals ▶ IKE-Keys

- 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. Wählen Sie dazu **Start ▶ Systemsteuerung ▶ Internetoptionen** und dort auf der Registerkarte 'Inhalte' die Schaltfläche **Zertifikate**.

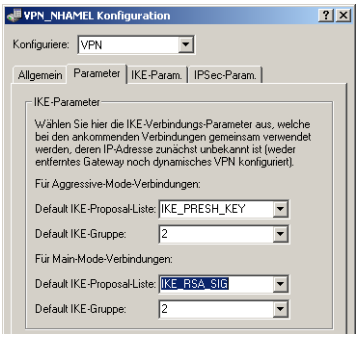
  Öffnen Sie das gewünschte Zertifikat und wählen Sie auf der Registerkarte 'Details' den entsprechenden Wert aus. Für den Antragsteller finden Sie hier z.B. die benötigten ASN.1 Distinguished Names mit den zugehörigen Kurzzeichen. Die in den Zertifikaten von oben nach unten aufgeführten Werte müssen in 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“.

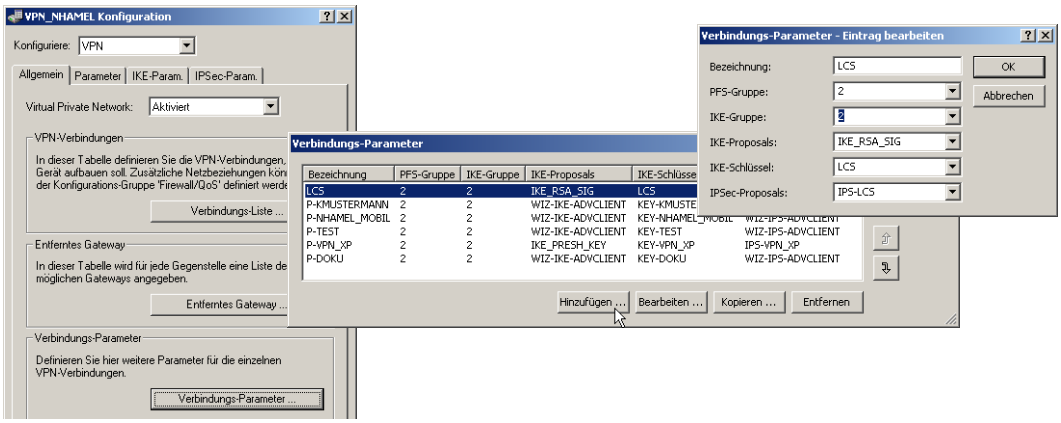
④ In den IKE-Verbindungs-Parametern müssen die Default-IKE-Proposal-Listen für eingehende Aggressive-Mode- und Main-Mode-Verbindungen auf die Proposal-Liste 'IKE_RSA_SIG' eingestellt sein. Beachten Sie außerdem die Einstellung der Default-IKE-Gruppe, die im nächsten Schritt ggf. angepasst werden muss.



LANconfig: VPN ▶ Parameter

WEBconfig: LCOS-Menübaum ▶ Setup ▶ VPN

⑤ 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.



LANconfig: VPN ▶ Allgemein ▶ Verbindungs-Parameter

WEBconfig: LCOS-Menübaum ▶ Setup ▶ VPN ▶ VPN-Layer

10.6.14 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 LANCOM über die korrekte Uhrzeit verfügt und die entsprechenden Zertifikate in das Gerät geladen wurden (‘Zertifikate in das LANCOM laden’ → Seite 10-35).

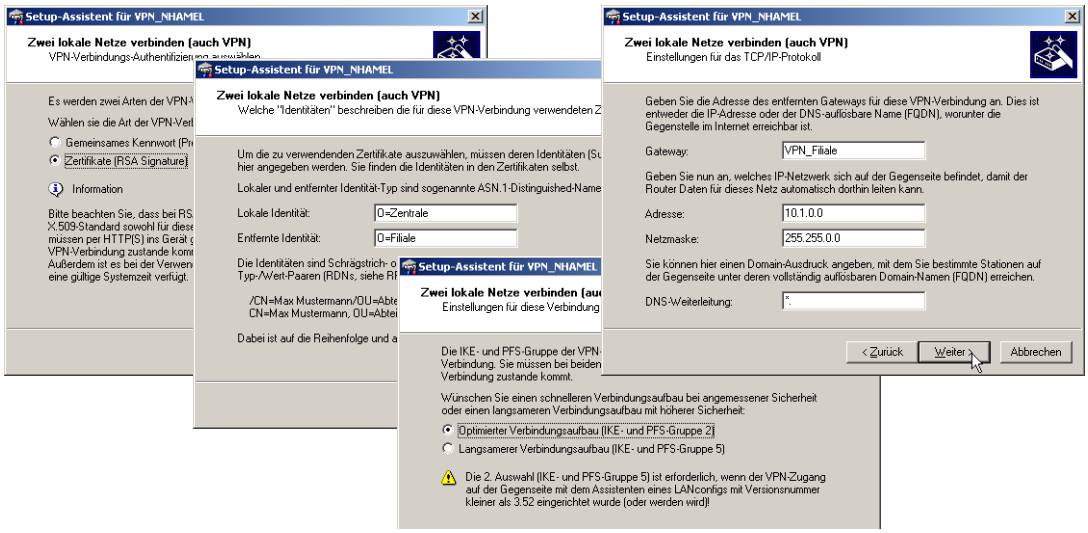
LAN-Kopplungen

① Wählen Sie den Assistenten 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 Telnetbefehl `show vpn cert` zeigt die Inhalte des Geräte-Zertifikates in einem LANCOM, u.a. dabei die eingetragenen Relative Distinguished Names (RDN) unter „Subject“. Die Relative Distinguished Names werden in dieser Darstellung bis LCOS 6.00 in umgekehrter Reihenfolge, ab LCOS 6.10 in der üblichen Reihenfolge angezeigt!



③ Wählen Sie nach Möglichkeit den optimierten Verbindungsaufbau mit IKE- und PFS-Gruppe 2. Wählen Sie nur dann die Gruppe 5 für IKE und PFS, wenn dies von der Gegenstelle verlangt wird. Dies ist z.B. dann der Fall, wenn die VPN-Gegenstelle mit LANconfig 3.52 oder kleiner konfiguriert wird.

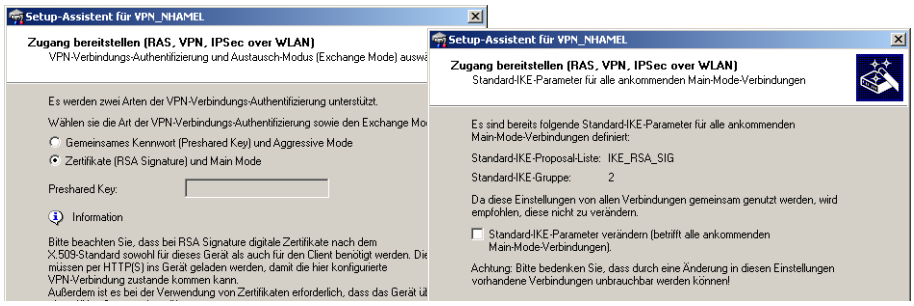
④ Tragen Sie den Namen der VPN-Gegenstelle, die IP-Adresse und die Netzmaske des entfernten Netzes sowie die ggf. verwendeten Domain für die DNS-Weiterleitung ein. Aktivieren Sie je nach Bedarf die „Extranet"-Funktion und das „NetBIOS-Routing".

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 LANCOM 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.

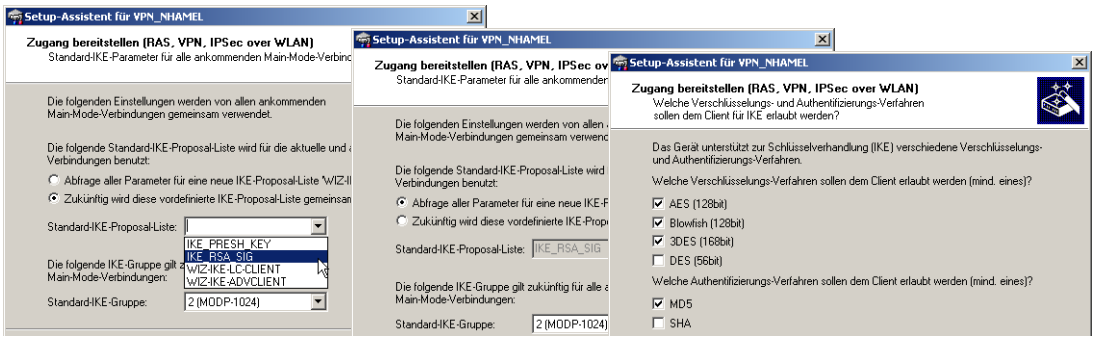
① Wählen Sie den Assistenten zum Bereitstellen von Zugängen über VPN. Wählen Sie dann im entsprechenden Dialog die VPN-Verbindungsauthentifizierung über Zertifikate (RSA-Signature). Als „Exchange Mode" wird dabei automatisch der Main Mode verwendet.



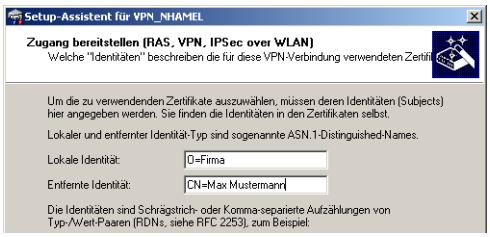
Nur bei benutzerdefiniertem VPN-Client

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.



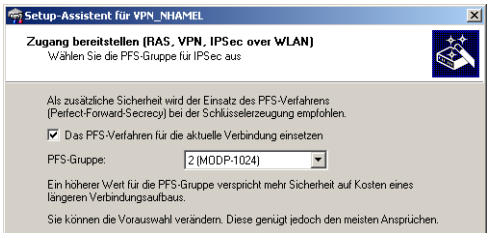
④ Tragen Sie die Identitäten aus dem lokalen und entfernten Geräte-Zertifikat ein. Übernehmen Sie dabei die vollständigen Angaben aus den jeweiligen Zertifikaten in der richtigen Reihenfolge: die in den Zertifikaten unter Windows von oben nach unten aufgeführten ASN.1-Distinguished Names werden in LANconfig von links nach rechts eingetragen.



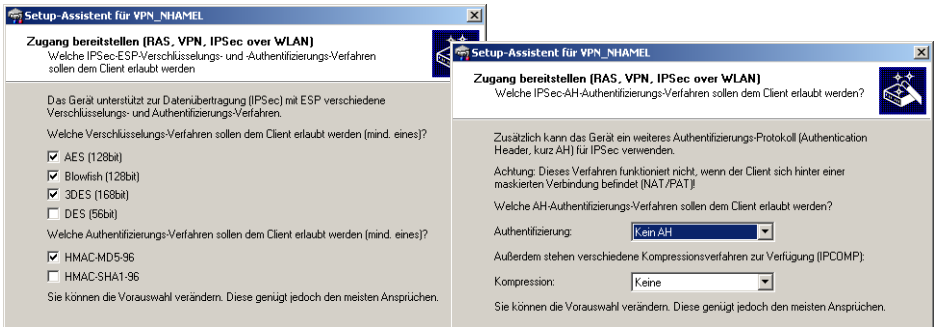
Die Anzeige von Zertifikaten unter Microsoft Windows zeigt für manche Werte ältere Kurzformen an, beispielweise 'S' anstelle von 'ST' für 'stateOrProvinceName' (Bundesland) oder 'G' anstelle von 'GN' für 'givenName' (Vorname). Verwenden Sie hier ausschließlich die aktuellen Kurzformen 'ST' und 'GN'.

Der Telnetbefehl `show vpn cert` zeigt die Inhalte des Geräte-Zertifikates in einem LANCOM, u.a. dabei die eingetragenen Relative Distinguished Names (RDN) unter „Subject". Die Relative Distinguished Names werden in dieser Darstellung bis LCOS 6.00 in umgekehrter Reihenfolge, ab LCOS 6.10 in der üblichen Reihenfolge angezeigt!

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. Aktivieren Sie je nach Bedarf das „NetBIOS-Routing".

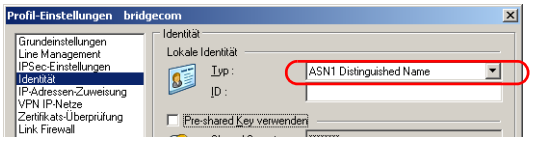
10.6.15 LANCOM Advanced VPN Client auf Zertifikatsverbindungen einstellen

Bei der Einwahl mit dem LANCOM Advanced VPN Client in einen LANCOM-Router müssen die entsprechenden Profil-Einstellungen an die Verwendung von Zertifikaten angepasst werden.

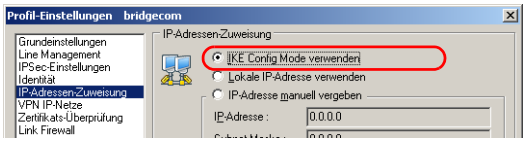
① Stellen Sie in den IPSec-Einstellungen des Profils die IKE-Richtlinie auf 'RSA-Signatur' um.



② Stellen Sie die Identität auf 'ASN1 Distinguished Names' um. Die 'Identität' kann frei bleiben, da diese Information aus dem Zertifikat ausgelesen wird.



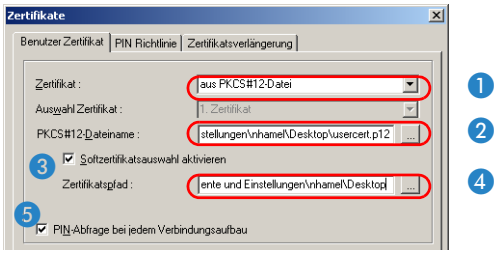
③ Verwenden Sie bei der IP-Adress-Zuweisung den 'IKE Config Mode'.



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.



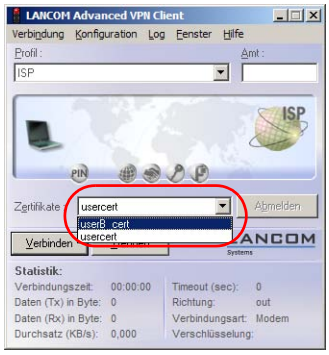
⑤ Nachdem Sie das geänderte Verbindungsprofil gespeichert haben, öffnen Sie über den Menüpunkt **Konfiguration ▶ Zertifikate** die Einstellungen für die Benutzerzertifikate.



- □ Wählen Sie als Zertifikatetyp die 'PKCS#12-Datei aus ❶ und geben Sie die gewünschte Zertifikatsdatei an ❷.
- □ Wenn Sie mit verschiedenen Zertifikaten arbeiten möchten, aktivieren Sie die Option 'Softzertifikatsauswahl' ❸ und geben den Pfad zum Ordner an, in dem die Zertifikatsdateien abgelegt sind ❹.
- □ Wählen Sie aus, ob die PIN (das Kennwort) für das Zertifikat bei jedem Verbindungsaufbau abgefragt werden soll ❺. 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.



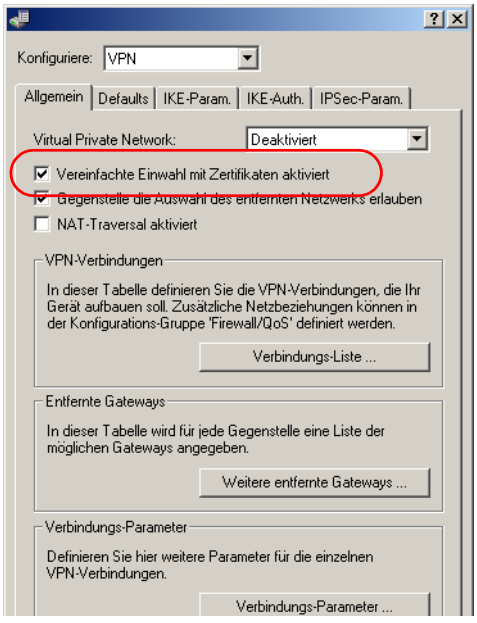
10.6.16 Vereinfachte Einwahl mit Zertifikaten

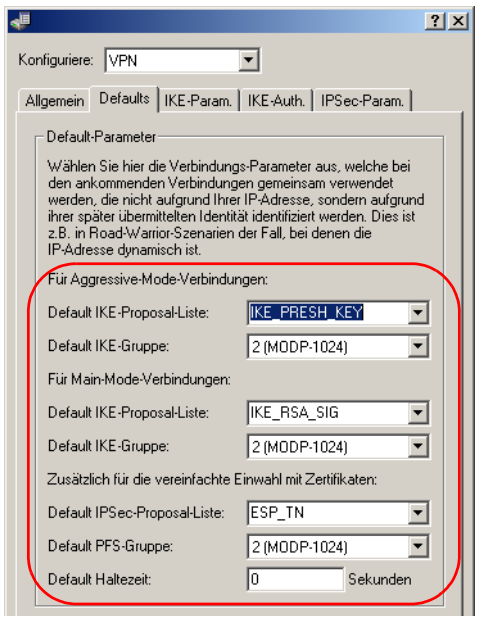
Bei der Einwahl von Rechnern mit wechselnden IP-Adressen ist zu Beginn der IKE-Verhandlung (Phase 1) die Identität der Gegenstelle noch nicht bekannt, zur Kommunikation werden Defaultwerte für IKE-Proposal-Listen und IKE-Proposal-Gruppen verwendet. Während der Verhandlung wird die Identität übermittelt, 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 aktiviert. Die Default-Parameter können bei Bedarf verändert werden.





LANconfig: VPN ▶ Allgemein und VPN ▶ Allgemein ▶ Defaults

WEBconfig: LCOS-Menübaum ▶ Setup ▶ VPN

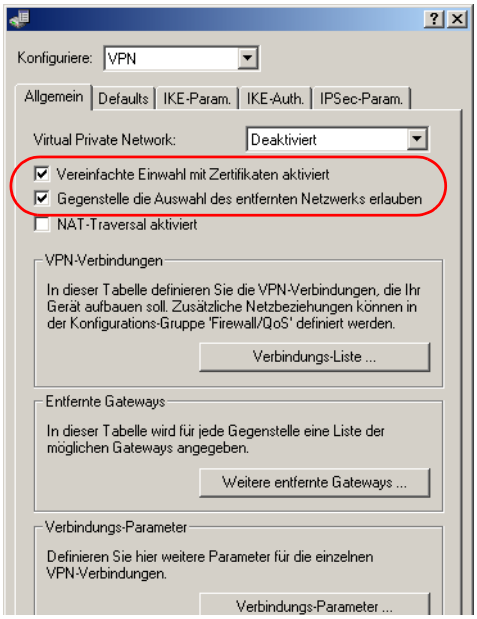
Durch das Aktivieren der vereinfachten Zertifikate-Einwahl können sich **alle** Clients mit einem gültigen Zertifikat, das vom Herausgeber des im Gerät befindlichen Root-Zertifikats signiert ist, in das entsprechende Netzwerk einwählen. Es ist keine weitere Konfiguration des Routers erforderlich! Unerwünschte Einwahlen können ausschließlich über das Sperren der Zertifikate und die Verwendung einer CRL verhindert werden.

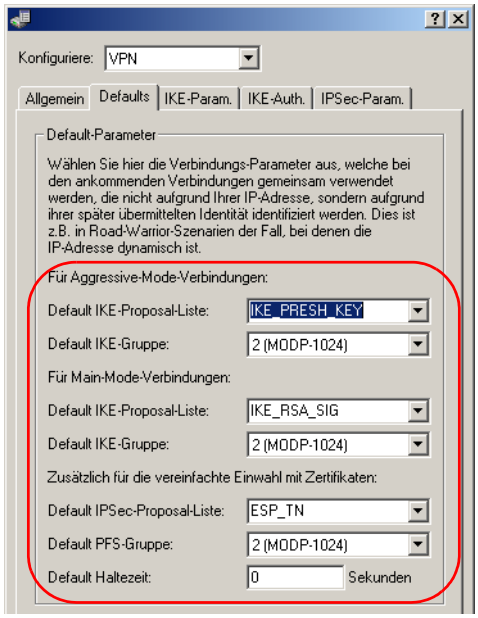
10.6.17 Vereinfachte Netzwerkanbindung mit Zertifikaten – Proadaptives VPN

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 LANCOM 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 LANCOM Router in der Zentrale akzeptiert das vorgeschlagene Netzwerk, wenn die Option 'Gegenstelle 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.





LANconfig: VPN ▶ Allgemein und VPN ▶ Allgemein ▶ Defaults

WEBconfig: LCOS-Menübaum ▶ Setup ▶ VPN

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 LANCOM Router beschränkt, die Certification Revocation Lists (CRL) unterstützen.

10.6.18 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 LANCOM VPN Router beim Verbindungsaufbau einen entsprechenden CERTREQ, der den Herausgeber des im LANCOM gespeicherten Root-Zertifikates enthält.

10.6.19 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.

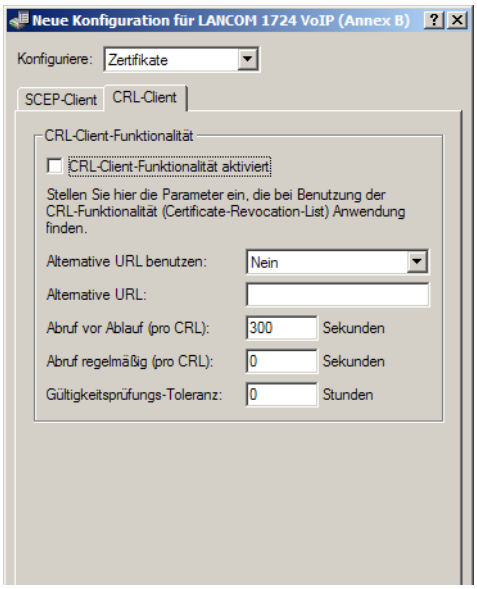
Da sich das Zertifikat selbst beim Mitarbeiter befindet und nicht verändert werden kann, wird eine Zertifikatsperrliste verwendet. In einer solchen Zertifikatsperrliste (Certificate Revocation List – CRL), wie sie z.B. von der Microsoft CA oder von OpenSSL unterstützt werden, sind die ungültigen Zertifikate 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 LANCOM 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.

Konfiguration der CRL-Funktion

Bei der Konfiguration der CRL-Funktion werden neben dem Pfad der CRL zusätzliche Parameter wie das Update-Intervall angegeben.



LANconfig: Zertifikate ▶ CRL-Client

WEBconfig: LCOS-Menübaum ▶ Setup ▶ Zertifikate ▶ CRLs

- **CRL-Funktionalität [Default: Aus]**
  - □ Aktiviert: Bei Prüfung eines Zertifikats wird die CRL (falls vorhanden) ebenfalls herangezogen.

Wenn diese Option aktiviert ist und keine gültige CRL gefunden werden kann, weil z.B. der Server nicht erreichbar ist, werden alle Verbindungen abgelehnt und bestehende Verbindungen unterbrochen.

- **Alternative URL benutzen [Default: Nein]**
  - □ Nein: Es wird nur die im Root-Zertifikat angegebene URL verwendet.
  - □ Ja, immer: Die alternative URL wird immer benutzt, auch wenn im Root-Zertifikat eine URL eingetragen ist.
  - □ Ja, alternativ: Die alternative URL wird nur benutzt, wenn im Root-Zertifikat keine URL eingetragen ist.
- **Alternative URL**
  - □ Diese URL kann (alternativ) benutzt werden, um eine CRL abzuholen.

- **Abruf vor Ablauf [Default: 300 Sekunden]**

  Der Zeitpunkt vor dem Ablauf der CRL, ab dem versucht wird, eine neue CRL zu laden. Dieser Wert wird um einen Zufallskomponente erhöht, um gehäufte Anfragen an den Server zu vermeiden. Be Erreichen dieses Zeitpunkts wird ein evtl. aktiviertes regelmäßiges Update angehalten.

Wenn die CRL im ersten Versuch nicht geladen werden kann, werden in kurzen Zeitabständen neue Versuche gestartet.

- **Abruf regelmäßig [Default: 0 Sekunden]**

  Die Länge des Zeitraums, nach dessen Ablauf periodisch versucht wird, eine neue CRL zu erhalten. Hiermit können eventuell außer der Reihe veröffentlichte CRLs frühzeitig heruntergeladen werden. Mit einem Eintrag von '0' wird das regelmäßige Abrufen ausgeschaltet.

Wenn die CRL bei regelmäßigen Update nicht geladen werden kann, werden keine Versuche bis zum nächsten regelmäßigen Termin gestartet.

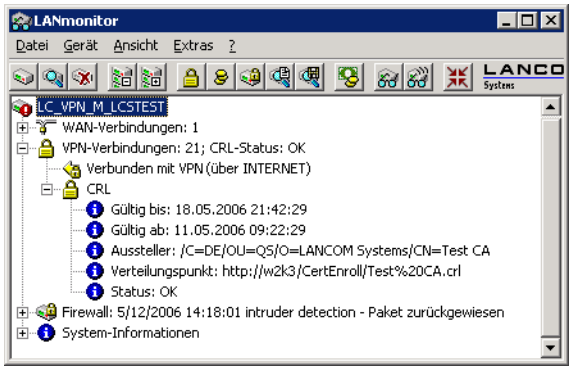
- **Gültigkeitstoleranz**

  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.

Anzeige des CRL-Status im LANmonitor

Informationen über die Gültigkeitsdauer und den Herausgeber der aktuellen CRL im LANCOM können im LANmonitor eingesehen werden.



10.6.20 Diagnose der VPN-Zertifikatsverbindungen

Die folgenden Befehle an der LANCOM-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 LCOS 6.00 in umgekehrter Reihenfolge, ab LCOS 6.10 in der üblichen Reihenfolge angezeigt!

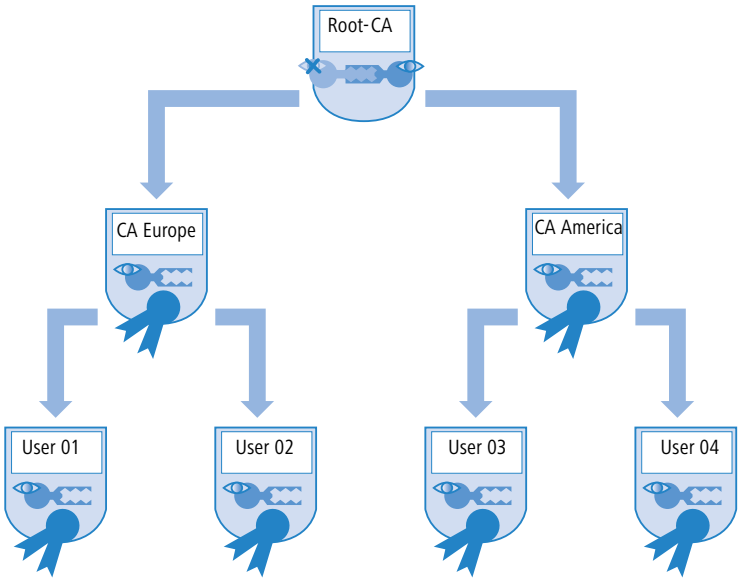
10.7 Mehrstufige Zertifikate für SSL/TLS

Neu mit LCOS 7.6:

- Mehrstufige Zertifikate für SSL/TLS

10.7.1 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.

10.7.2 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 LANCOM senden. Die Zertifikatskette wird im LANCOM auf Gültigkeit geprüft.

10.7.3 VPN mit mehrstufigen Zertifikaten

Für den zertifikatsbasierten Aufbau von VPN-Verbindungen werden im Dateisystem des LANCOM 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 LANCOM entpackt – die restlichen Zertifikat 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 LANCOM 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.

10.8 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 LANCOM 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 LANCOM 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 LANCOM VPN Router über SCEP automatisiert von einer zentralen Stelle abrufen.

10.8.1 SCEP-Server und SCEP-Client

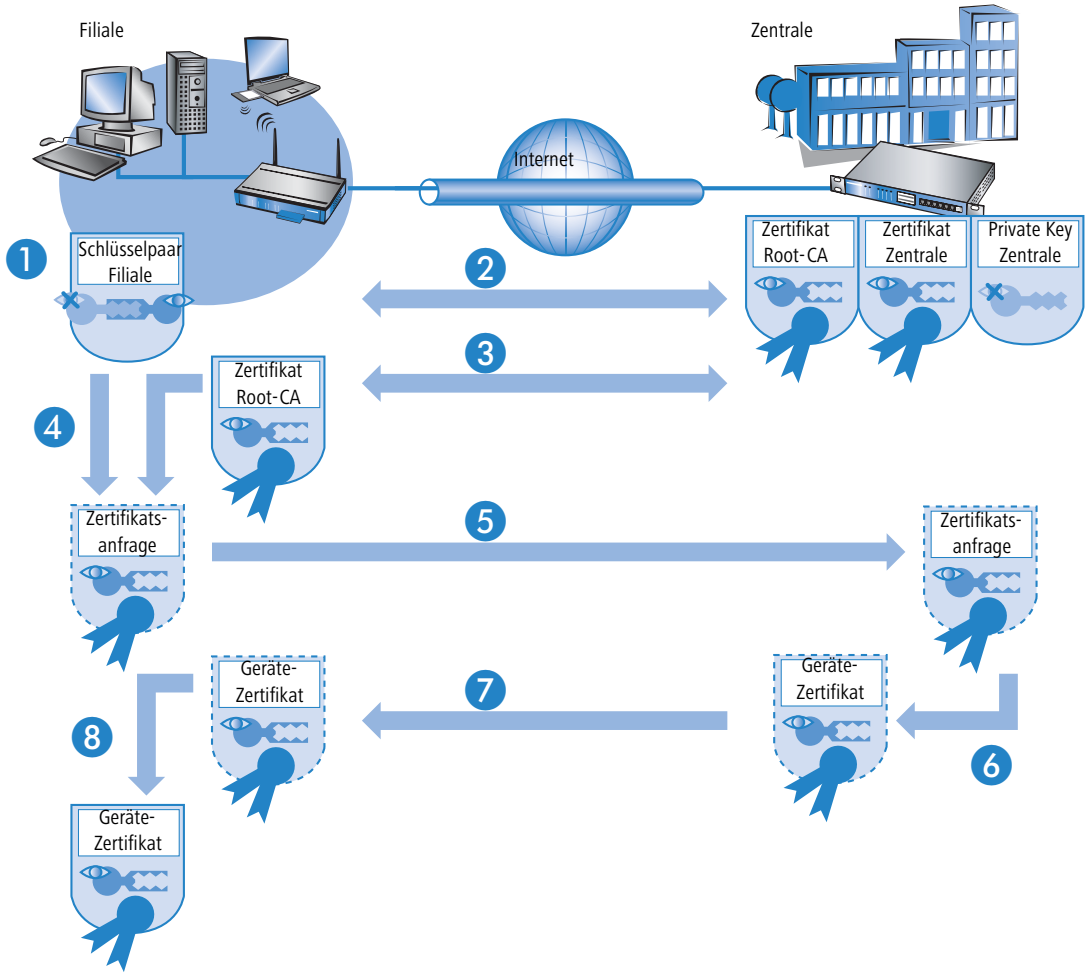
Die Bereitstellung und Verwaltung der Zertifikate wird von einem SCEP-Server vorgenommen, der neben der Funktion einer üblichen Certification Authority (CA) um die SCEP-Funktionalität erweitert ist. Dieser Server kann z.B. als Windows 2003 Server CA mit einem speziellen Plug-In (der mscep.dll) realisiert 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-Geräte auf (also die LANCOM VPN Router), 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 LANCOM VPN Router dabei vor allem gültige Systemzertifikate (Gerätezertifikate). Die anderen ggf. genutzten Zertifikate werden nur für den SCEP-Vorgang benötigt.

10.8.2 Der Ablauf einer Zertifikatsverteilung

Im Überblick verläuft die Verteilung von Zertifikaten über SCEP nach folgendem Schema ab:



① Schlüsselpaar im LANCOM VPN Router erzeugen.

Im LANCOM 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 (LANCOM 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 LANCOM 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 LANCOM 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

10.8.3 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.

WEBconfig: LCOS-Menübaum ▶ Setup ▶ Zertifikate ▶ SCEP-Client

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

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 LANCOM Router 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.

Konfiguration der CAs

■ **Name**

Konfigurationsname der CA.

■ **URL**

URL der CA.

■ **DN**

Distinguished Name des Gerätes. 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.

■ **Enc-Alg**

Mit diesem Algorithmus wird die Nutzlast des Zertifikatsantrags verschlüsselt.

- □ Mögliche Werte: DES, 3-DES, Blowfish.
- □ Default: DES.

■ **Identifier**

CA-Identifier (wird von manchen Webservern benötigt, um die CA zuordnen zu können).

■ **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: Ja, Nein.
- □ Default: Nein.

■ **CA-Signaturalgorithmus**

Mit diesem Algorithmus wird der Zertifikatsantrag signiert.

- □ Mögliche Werte: MD5, SHA1.
- □ Default: MD5.

■ **CA-Fingerprintalgorithmus**

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, der sich bei Verwendung des Algorithmus ergibt.

- □ Mögliche Werte: Aus, MD5, SHA1.
- □ Default: Aus.

■ **CA-Fingerprint**

Anhand der hier eingetragenen Prüfsumme (Fingerprint) kann die Authentizität des erhaltenen CA-Zertifikats überprüft werden (entsprechend des eingestellten CA-Fingerprintalgorithmus).

■ **Verwendung**

Gibt den Verwendungszweck der eingetragenen CA an. Die hier eingetragene CA wird dann nur für den entsprechenden Verwendungszweck abgefragt.

- □ Mögliche Werte: VPN, WLAN-Controller, Allgemein
- □ Besondere Werte: Allgemein. Wenn eine allgemeine CA vorhanden ist, lässt sich keine weitere konfigurieren, da sonst die Wahl der CA nicht eindeutig ist.

Konfiguration der Systemzertifikate

- **Name**

  Konfigurationsname des Zertifikats.

- **CADN**

  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.

- **Subject**

  Distinguished Name des Subjects des Antragstellers.

- **ChallengePwd**

  Kennwort (für das automatische Ausstellen der Geräte-Zertifikate auf dem SCEP-Server).

- **SubjectAltName**

  Weitere Angaben zum Requester, z.B. Domain oder IP-Adresse.

- **KeyUsage**

  Beliebige kommaseparierte Kombination aus:

  - □ digitalSignature
  - □ nonRepudiation
  - □ keyEncipherment
  - □ dataEncipherment
  - □ keyAgreement
  - □ keyCertSign
  - □ cRLSign
  - □ encipherOnly
  - □ decipherOnly
  - □ critical (möglich aber nicht empfohlen)

- **Extended Key Usage**

  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

- **Systemzertifikate-Schlüssellänge**

  Länge der Schlüssel, die für das Gerät selbst erzeugt werden.

- **Verwendung**

  Gibt den Verwendungszweck der eingetragenen Zertifikate an. Die hier eingetragenen Zertifikate werden dann nur für den entsprechenden Verwendungszweck abgefragt.

10.9 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 ausge-

henden 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 in den letzten Jahren sehr 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 UMTS-Mobilfunknetze auf, bei denen die Server des Netzbetreibers die Adress-Umsetzung in Verbindung mit IPSec-basierten VPNs nicht unterstützen.

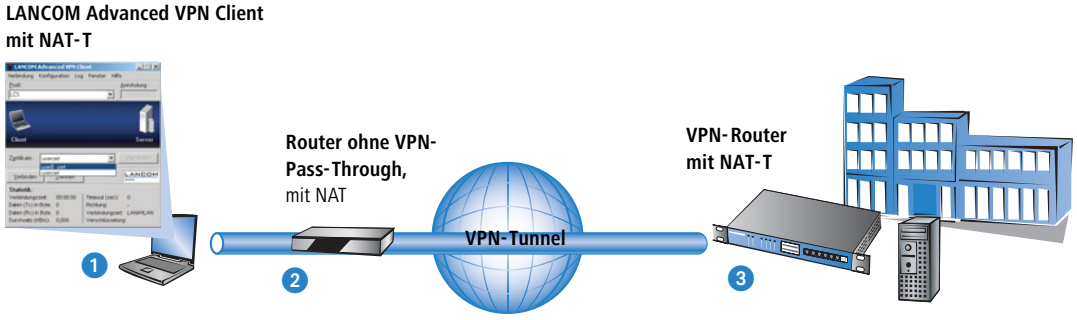
Um auch in diesen Fällen eine VPN-Verbindung erfolgreich aufbauen zu können, steht mit NAT-T (NAT Traversal) ein Verfahren bereit, die beschriebenen Probleme bei der Behandlung von Datenpaketen mit geänderten Adressen zu überwinden.

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:

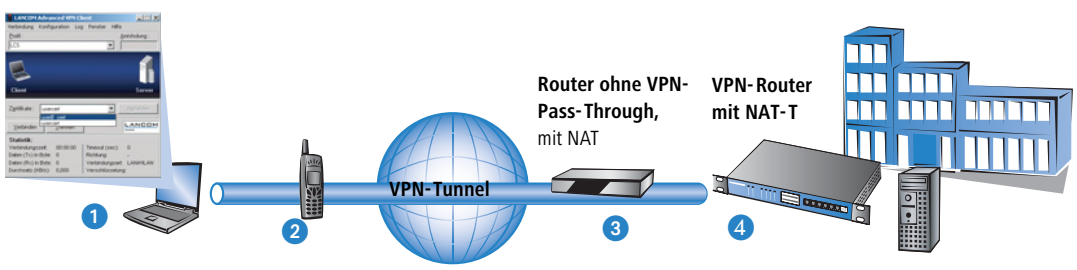
- Ein Aussendienstmitarbeiter wählt sich mit einem LANCOM Advanced VPN Client über einen Router **ohne** „VPN-Pass-Through"-Unterstützung (d.h. IPSec Maskierung), aber **mit** Network Address Translation in den VPN-Router seiner Firma ein.



  - □ 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.

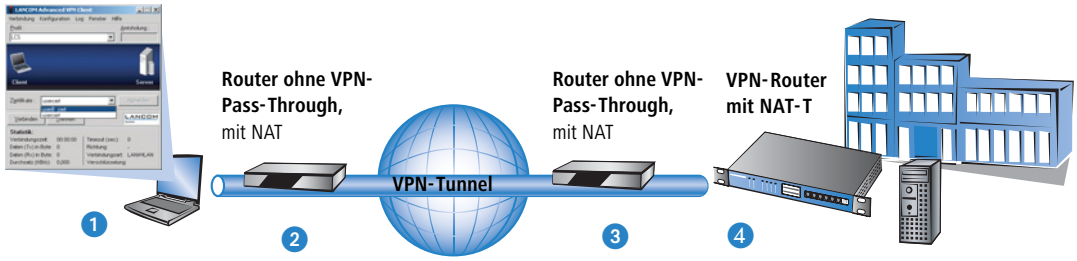
    In diesem Router wird kein NAT-T benötigt, hier müssen jedoch die Ports 500 und 4500 in der Firewall freigeschaltet sein, um die NAT-T-Kommunikation der beiden Tunnelendpunkte zu ermöglichen.

- 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.



- □ 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 der 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.

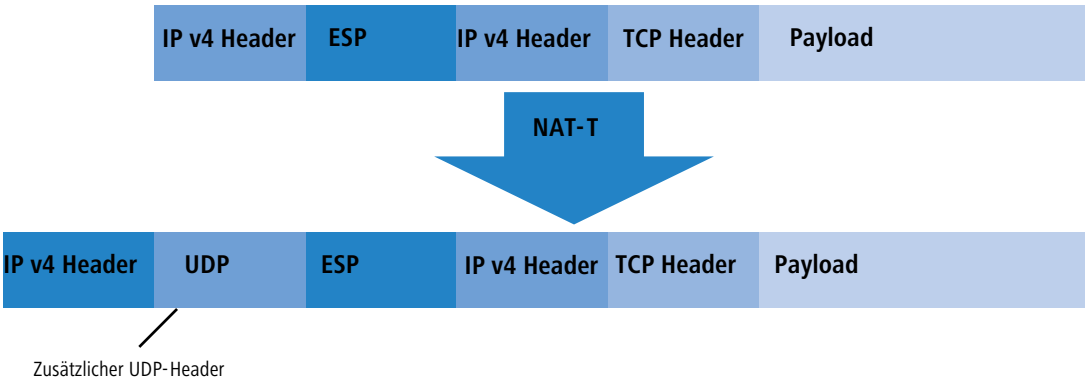
② Im zweiten Schritt wird dann geprüft, ob auf der Strecke zwischen den beiden Tunnelendpunkten eine Adressumsetzung nach NAT stattfindet und an welcher Stelle der Verbindung sich die NAT-Geräte befinden.

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.

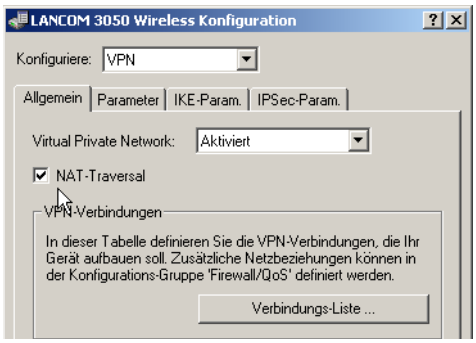
Achten Sie darauf, dass neben dem UDP-Port 500 auch der UDP-Port 4500 bei Verwendung von NAT-T in der Firewall freigeschaltet ist, wenn das LANCOM als NAT-Router zwischen den VPN-Endpunkten fungiert! Bei Verwendung des Firewall-Assistenten in LANconfig wird dieser Port automatisch freigeschaltet.

Sofern die VPN-Verbindungen erstmals auf Geräten mit einer LCOS-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.



LANconfig: VPN ▶ Allgemein

WEBconfig: LCOS-Menübaum ▶ Setup ▶ VPN ▶ NAT-T-Operating

10.10 Extended Authentication Protocol (XAUTH)

10.10.1 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).

10.10.2 XAUTH im LCOS

Im LANCOM 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:

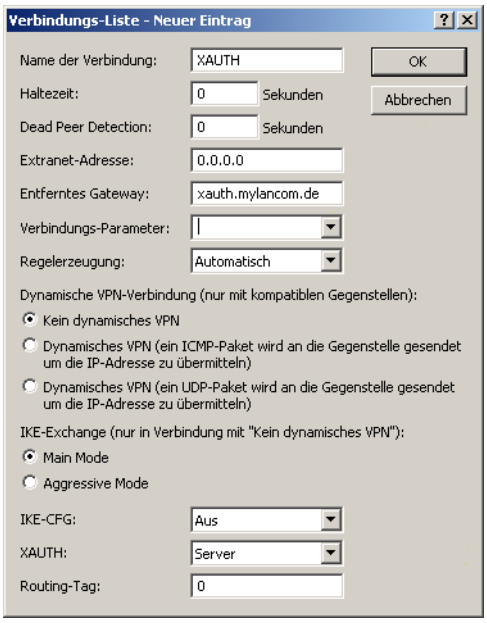
XAUTH-Betriebsart	Server	Client
XAUTH-Benutzername	Gegenstelle aus der PPP-Tabelle. Es wird dabei der Eintrag aus der PPP-Tabelle gewählt, bei dem die PPP-Gegenstelle dem übermittelten XAUTH-Benutzernamen entspricht. Die PPP-Gegenstelle muss dabei auch der verwendeten VPN-Gegenstelle entsprechen.	Benutzername 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.

Da in der LCOS-Version 7.60 in der Betriebsart als XAUTH-Server der übermittelte XAUTH-Benutzername dem Namen der VPN-Gegenstelle entsprechen muss, kann für jede VPN-Gegenstelle nur ein Benutzer über XAUTH authentifiziert werden. Eine Authentifizierung über einen RADIUS-Server ist in LCOS 7.60 nicht vorgesehen.

10.10.3 Konfiguration von XAUTH

Die Verwendung des XAUTH-Protokolls wird für jede VPN-Gegenstelle separat vorgenommen. Dabei wird lediglich der XAUTH-Betriebsmodus festgelegt.

LANconfig: VPN ▶ Allgemein ▶ Verbindungs-Liste



WEBconfig: 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: Bei der Verbindung zu dieser Gegenstelle wird keine XAUTH-Authentifizierung durchgeführt.

Default:

- □ Aus

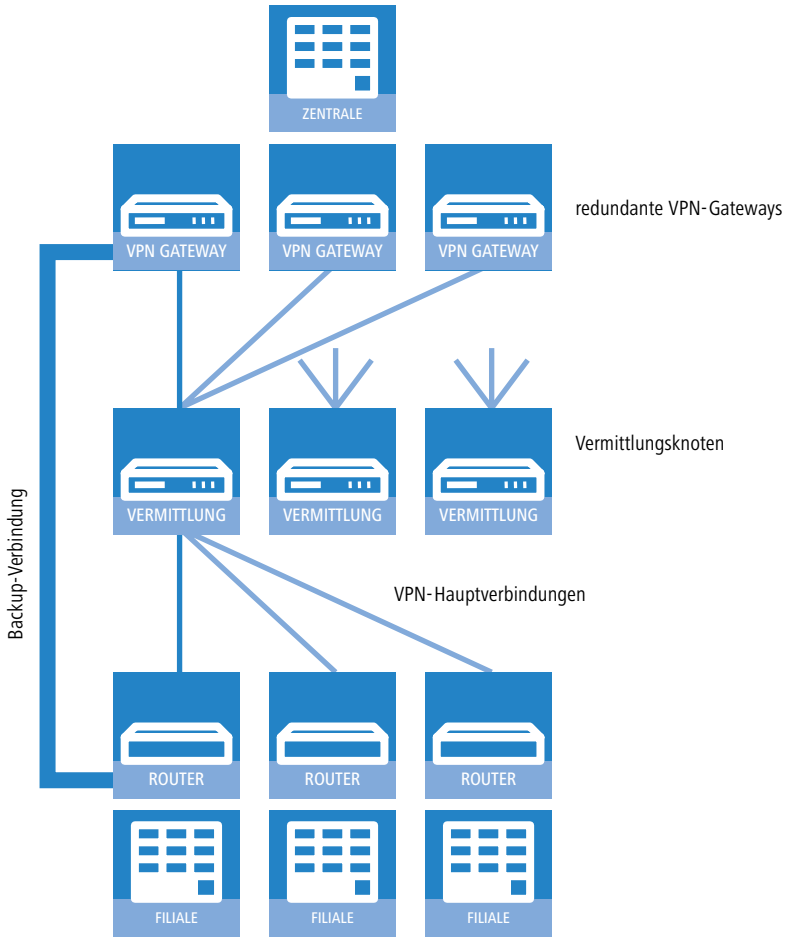
Wenn die XAUTH-Authentifizierung für eine VPN-Gegenstelle aktiviert ist, muss die Option IKE-CFG auf den gleichen Wert eingestellt werden.

10.11 Backup über alternative VPN-Verbindung

10.11.1 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 ISDN-Verbindung, die aus Kostengründen und wegen der 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.

10.11.2 Backup-fähige Netzstruktur

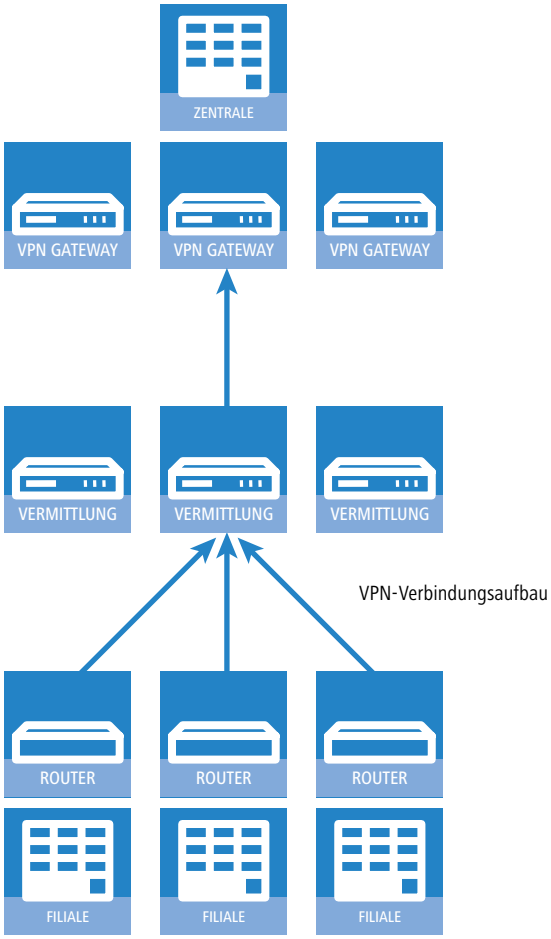
Um auch für diese Anwendungen ein funktionsfähiges Backup aufbauen zu können, müssen die in den folgenden Abschnitten beschriebenen Aspekte erfüllt sein.

Grundvorraussetzungen

Grundvoraussetzung für die hier beschriebene Backup-Funktion ist die Einrichtung einer "Dynamic VPN"-Verbindung zwischen Filialen und Vermittlungsknoten sowie die Aktivierung der Funktionen "vereinfachten Einwahl mit Zertifikaten" und "Gegenstelle die Auswahl des entfernten Netzes erlauben" in den VPN-Gateways der Zentrale.

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.

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

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 "vereinfachten 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 "vereinfachten 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.

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. Wenn die nächste Backupverbindung eine ISDN-Verbindung ist, dann wird sie ganz normal aufgebaut, d. h. es müssen keine IPSec-Regeln umkonfiguriert werden.

Bei einem ISDN-Backup in der Zentrale muss eine Kopplung der Backup-Verbindung und den normalen VPN-Verbindungen zu den anderen Filialen verhindert werden, da über die VPN-Hauptverbindungen ja nicht nur der Datenverkehr zur Filiale im Backup-Fall läuft, sondern auch der zu den Vermittlungsknoten und allen anderen Filialen. Um diese Kopplung zu verhindern, stehen zwei Möglichkeiten zur Auswahl:

- In die ISDN-Backupverbindung wird eine sehr hohe Distanz für das Netz der Filiale eingetragen. So kann diese Route von den über VPN automatisch übermittelten Routen überschrieben werden.
- Alternativ können die Routen über WAN-RIP gesteuert werden. Dazu wird für jeden B-Kanal eine ISDN-Verbindung mit WAN-RIP-Unterstützung eingerichtet.

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.

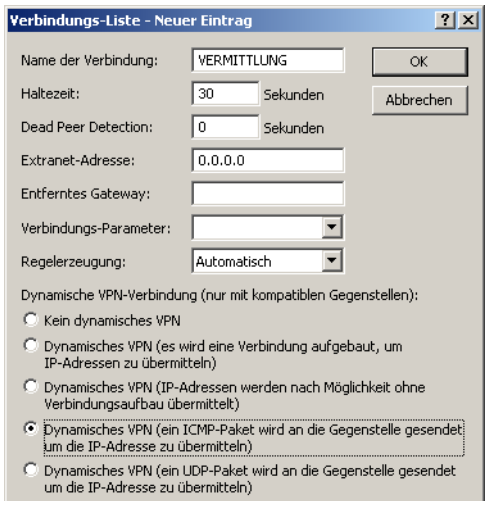
Um das zu verhindern, wird zunächst eine "Dynamic VPN"-Verhandlung mit der Gegenstelle der Hauptverbindung durchgeführt. Verläuft diese Verhandlung erfolgreich, kann die Hauptverbindung wieder aufgebaut werden. Dazu wird zunächst die Backup-Verbindung getrennt und zusätzlich der Backup-Status zurückgesetzt. 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.

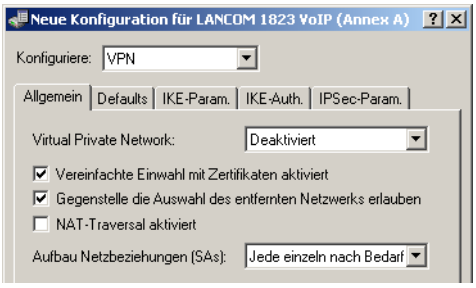
10.11.3 Konfiguration des VPN-Backups

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".
  - □ Das Backup wird wie beim ISDN-Backup in der Backup-Tabelle konfiguriert.
  - □ 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.

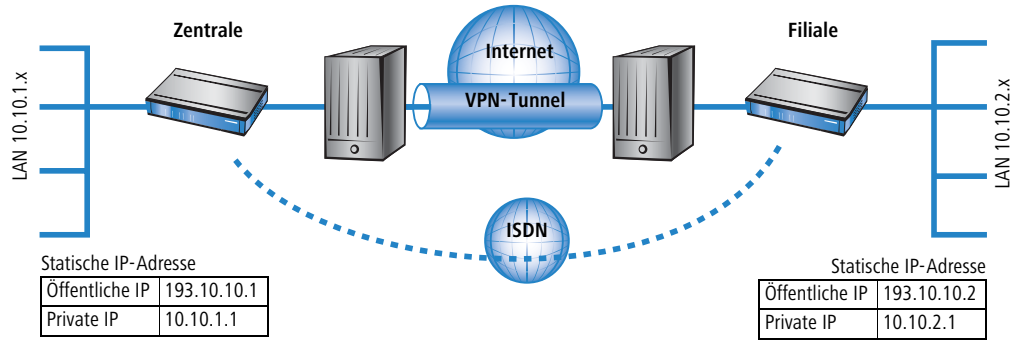
10.12 Konkrete Verbindungsbeispiele

In diesem Kapitel werden die vier möglichen VPN-Verbindungstypen an Hand konkreter Beispiele veranschaulicht. Die vier Verbindungsarten werden nach der IP-Adressart der beiden VPN-Gateways kategorisiert:

- statisch/statisch
- dynamisch/statisch (die dynamische Seite initiiert die Verbindung)
- statisch/dynamisch (die statische Seite initiiert die Verbindung)
- dynamisch/dynamisch

Zu jeder dieser vier VPN-Verbindungsarten gibt es einen eigenen Abschnitt mit einer Aufführung aller notwendigen Konfigurationsangaben in Form der bereits bekannten Tabelle.

10.12.1 Statisch/statisch

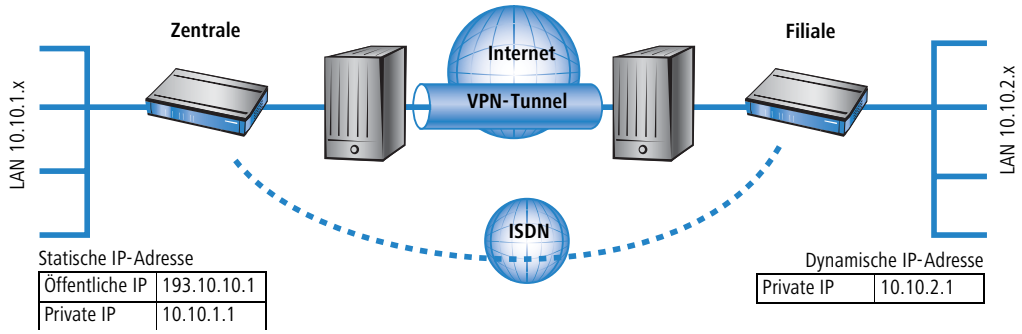


Zwischen den beiden LANCOM **Zentrale** und **Filiale** wird eine VPN-Verbindung aufgebaut. Beide Gateways verfügen über statische IP-Adressen. Beide Seiten können den Verbindungsaufbau initiieren.

Angabe	Zentrale		Filiale
Typ der eigenen IP-Adresse	statisch		statisch
Typ IP-Adresse der Gegenstelle	statisch		statisch
Name des eigenen Gerätes	Zentrale		Filiale
Name der Gegenstelle	Filiale		Zentrale
Shared Secret für Verschlüsselung	geheim	↔	geheim

Angabe	Zentrale		Filiale
IP-Adresse der Gegenseite	193.10.10.2		193.10.10.1
IP-Netzadresse des entfernten Netzes	10.10.2.0		10.10.1.0
Netzmaske des entfernten Netzes	255.255.255.0		255.255.255.0

10.12.2 Dynamisch/statisch



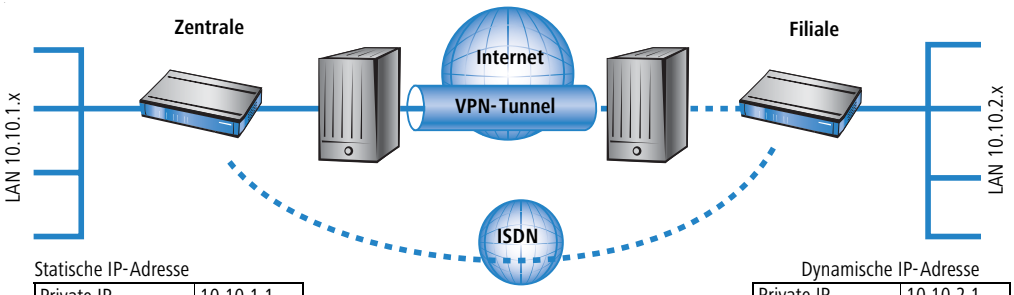
Das VPN-Gateway **Filiale** baut eine VPN-Verbindung zum Gateway **Zentrale** auf. **Filiale** verfügt über eine dynamische IP-Adresse (die ihm bei der Internet-Einwahl von seinem Internet-Anbieter zugewiesen wurde), **Zentrale** hingegen über eine statische. Während des Verbindungsaufbaus überträgt **Filiale** seine aktuelle IP-Adresse an **Zentrale** (standardmäßig über ICMP, alternativ auch über UDP Port 87).

Angabe	Zentrale		Filiale
Typ der eigenen IP-Adresse	statisch	⇄	dynamisch
Typ IP-Adresse der Gegenstelle	dynamisch		statisch
Name des eigenen Gerätes	Zentrale	⇄	Filiale
Name der Gegenstelle	Filiale		Zentrale
Kennwort zur sicheren Übertragung der IP-Adresse	vertraulich	↔	vertraulich
Shared Secret für Verschlüsselung	geheim	↔	geheim
IP-Adresse der Gegenseite	–		193.10.10.1
IP-Netzadresse des entfernten Netzes	10.10.2.0		10.10.1.0
Netzmaske des entfernten Netzes	255.255.255.0		255.255.255.0

Für diesen Verbindungsaufbau ist kein ISDN-Anschluss erforderlich. Die dynamische Seite übermittelt ihre IP-Adresse verschlüsselt über das Internet-Protokoll ICMP (alternativ auch über UDP).

10.12.3 Statisch/dynamisch (mit LANCOM Dynamic VPN)

In diesem Fall initiiert (im Gegensatz zur dynamisch/statischen Verbindung) die statische Seite den Aufbau der VPN-Verbindung.



Das VPN-Gateway **Zentrale** baut eine VPN-Verbindung zu **Filiale** auf. **Zentrale** verfügt über eine statische IP-Adresse, **Filiale** über eine dynamische.

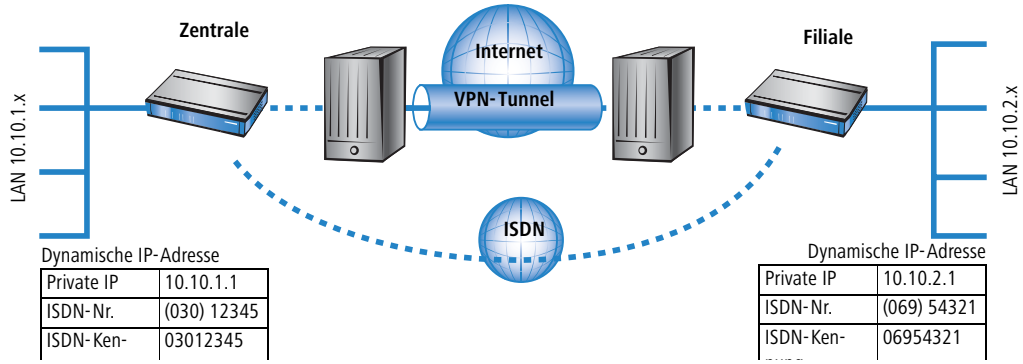
Die Angaben zur ISDN-Verbindung werden für die Übertragung der IP-Adresse verwendet und nicht für den eigentlichen Verbindungsaufbau ins Internet. Die Internetverbindung wird mit dem Internet-Zugangs-Assistenten konfiguriert.

Alternativ kann diese Anwendung mit Hilfe von Dynamic-DNS gelöst werden. Dabei wird als Pendant zur statischen IP-Adresse in der Zentrale auf der Seite der Filiale ein dynamischer DNS-Name verwendet, der die Zuordnung zur gerade aktuellen dynamischen IP-Adresse erlaubt. Weitere Informationen dazu finden Sie unter 'Dynamische IP-Adressen und DynDNS' → Seite 10-9.

Angabe	Zentrale		Filiale
Typ der eigenen IP-Adresse	statisch		dynamisch
Typ IP-Adresse der Gegenstelle	dynamisch		statisch
Name des eigenen Gerätes	Zentrale		Filiale
Name der Gegenstelle	Filiale		Zentrale
ISDN-Rufnummer Gegenstelle	06954321		03012345
ISDN-Anruferkennung Gegenstelle	06954321		03012345
Kennwort zur sicheren Übertragung der IP-Adresse	vertraulich	↔	vertraulich
Shared Secret für Verschlüsselung	geheim	↔	geheim
IP-Adresse der Gegenseite			193.10.10.1
IP-Netzadresse des entfernten Netzes	10.10.2.0		10.10.1.0
Netzmaske des entfernten Netzes	255.255.255.0		255.255.255.0

Der beschriebene Verbindungsaufbau setzt bei beiden VPN-Gateways einen ISDN-Anschluss voraus, über den im Normalfall jedoch keine gebührenpflichtigen Verbindungen aufgebaut werden.

10.12.4 Dynamisch/dynamisch (mit LANCOM Dynamic VPN)



Zwischen den beiden LANCOM **Zentrale** und **Filiale** wird eine VPN-Verbindung aufgebaut. Beide Seiten haben dynamische IP-Adressen. Beide Seiten können den Verbindungsaufbau initiieren.

Die Angaben zur ISDN-Verbindung werden für die Übertragung der IP-Adresse verwendet und nicht für den eigentlichen Verbindungsaufbau ins Internet. Die Internetverbindung wird mit dem Internet-Zugangs-Assistenten konfiguriert.

Alternativ kann diese Anwendung mit Hilfe von Dynamic-DNS gelöst werden. Dabei wird an Stelle einer statischen IP-Adresse ein dynamischer DNS-Name verwendet, der die Zuordnung zur gerade aktuellen dynamischen IP-Adresse erlaubt. Weitere Informationen dazu finden Sie unter 'Dynamische IP-Adressen und DynDNS' → Seite 10-9.

Angabe	Zentrale		Filiale
Typ der eigenen IP-Adresse	dynamisch		dynamisch
Typ IP-Adresse der Gegenstelle	dynamisch		dynamisch
Name des eigenen Gerätes	Zentrale		Filiale
Name der Gegenstelle	Filiale		Zentrale

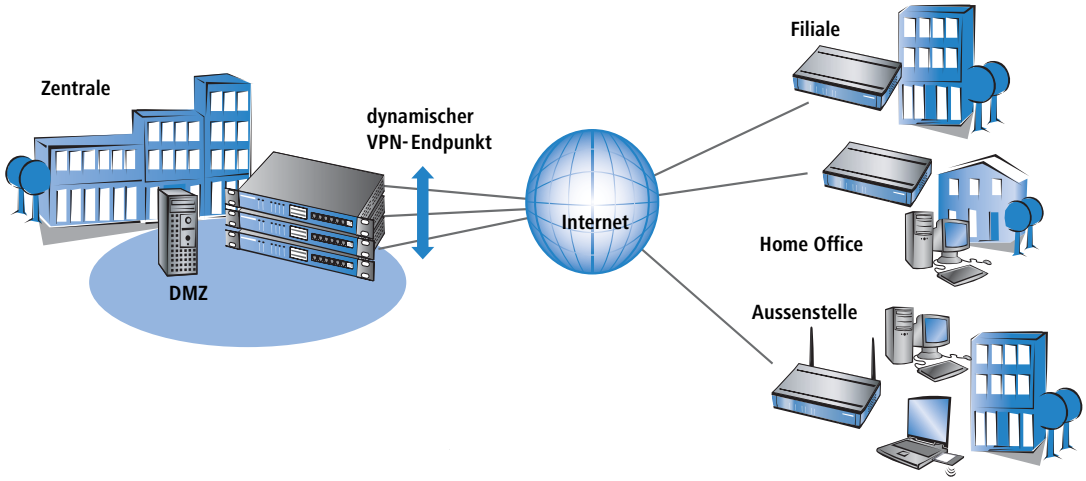
Angabe	Zentrale		Filiale
ISDN-Rufnummer Gegenstelle	06954321		03012345
ISDN-Anruferkennung Gegenstelle	06954321		03012345
Kennwort zur sicheren Übertragung der IP-Adresse	vertraulich	◄►	vertraulich
Shared Secret für Verschlüsselung	geheim	◄►	geheim
IP-Netzadresse des entfernten Netzes	10.10.2.0		10.10.1.0
Netzmaske des entfernten Netzes	255.255.255.0		255.255.255.0

Der beschriebene Verbindungsaufbau setzt bei beiden VPN-Gateways einen ISDN-Anschluss voraus.

10.12.5 VPN-Verbindungen: hohe Verfügbarkeit mit „Lastenausgleich"

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 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 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").

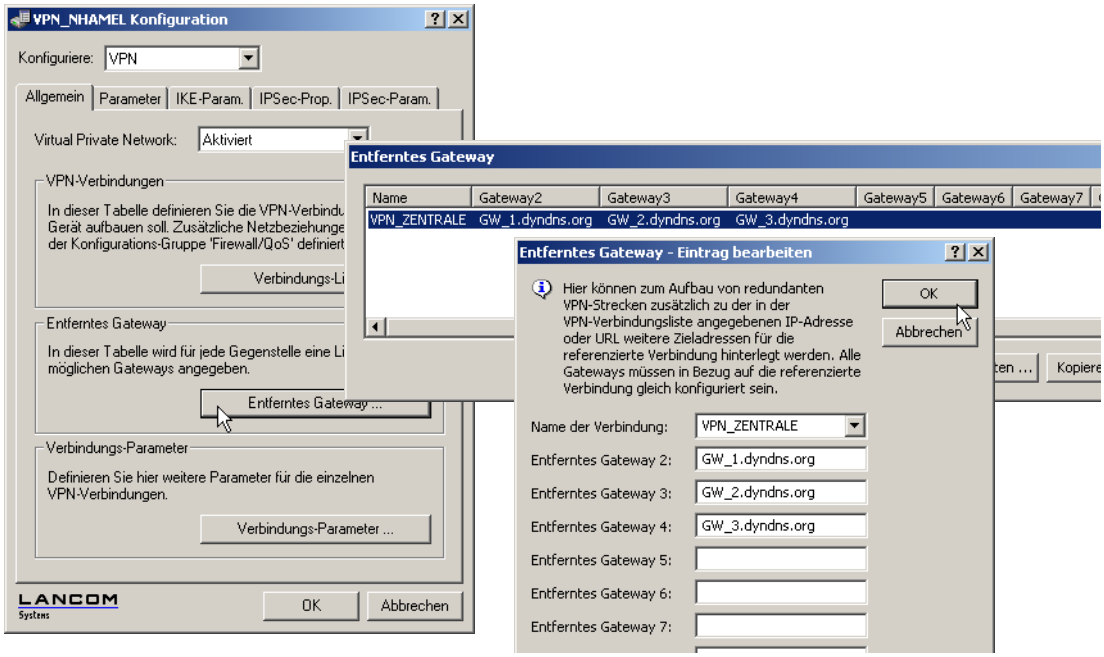
Konfiguration

Bei der Konfiguration tragen Sie in der Liste der „Remote Gateways" zusätzliche Ziele für eine VPN-Verbindung ein. Die Liste besteht aus den folgenden Einträgen:

- Name: Name der Gegenstelle aus der VPN-Verbindungsliste, das „Ziel" der VPN-Verbindung.
- Gateway 2 bis Gateway 9: Adresse der alternativen Gateways, als IP-Adresse oder auflösbarer DNS-Name.
- Anfang: In welcher Reihenfolge sollen die Einträge versucht werden. Zur Auswahl stehen:
  - Zuletzt benutzter: Wählt den Eintrag, zu dem zuletzt erfolgreich eine VPN-Verbindung hergestellt werden konnte.
  - Erster: 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.

Der Eintrag für das Gateway in der VPN-Verbindungsliste kann frei bleiben, wenn alle möglichen Gateways in der Liste der „Remote Gateways" eingetragen sind.



LANconfig: VPN ▶ Allgemein ▶ Entferntes Gateway

WEBconfig: LCOS-Menübaum ▶ Setup ▶ Config ▶ Remote-Gateway-Liste

Zur Definition der Strategie, nach der die konfigurierten Remote-Gateway-Adressen verwendet werden, stehen folgende Möglichkeiten zur Verfügung:

- `zuletzt-verwendetem`
- `erstem`
- `zufaelligem`

Beispiel:

Mit dem folgenden Befehl legen Sie drei Gateways als Ziel in der Zentrale fest, die zufällig ausgewählt werden:

```
set VPN_ZENTRALE 213.217.69.75  213.217.69.76  213.217.69.77 * * * * * zufaelligem
```

10.13 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 LANCOM VPN durch die Verwendung des weitverbreiteten IPSec-Standards.

10.13.1 IPSec – Die Basis für LANCOM 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. LANCOM VPN basiert auf IPSec.

IPSec steht für „**IP Sec**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 selber 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.

Sicherheit im IP-Gewand

IPSec ist (nahezu) vollständig innerhalb in 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.

10.13.2 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.

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 und IPX.

Ein wesentlicher Nachteil der beschriebenen Protokolle ist die fehlende Sicherheit auf Paketebene. Außerdem wurden die Protokolle speziell für Einwahlverbindungen entwickelt.

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. Zumeist sind sie aber auch deutlich komplexer.

Alle diese Layer-2-Protokolle erlauben nur Ende-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.

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.

10.14 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.

10.14.1 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

10.14.2 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: AH oder ESP (zu diesen Protokollen in den folgenden Abschnitten mehr).

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. Werden AH und ESP verwendet, so sind ebenfalls zwei separate SAs notwendig, also jeweils zwei für jede Kommunikationsrichtung.

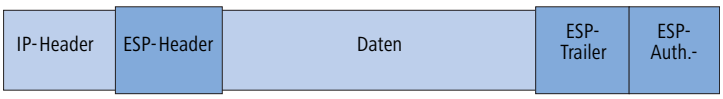
Die SAs werden im IPSec-Gerät in einer internen Datenbank verwaltet, in der auch die erweiterten Verbindungsparameter abgelegt werden. Zu diesen Parametern gehören beispielsweise die verwendeten Algorithmen und Schlüssel.

10.14.3 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 auch ESP inzwischen über einen wirksamen Schutz gegen Wiedereinspielung von Paketen. ESP bietet damit alle Funktionen von AH an.

Arbeitsweise von ESP

Der Aufbau von ESP ist komplizierter als der von AH. Auch ESP fügt einen Header hinter den IP-Header ein, zusätzlich allerdings auch noch einen eigenen Trailer und einen Block mit ESP-Authentifizierungsdaten.



Transport- und Tunnel-Modus

ESP kann (wie AH auch) 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.

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-amerikanischer 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.

- **DES – Data Encryption Standard**
  DES wurde Anfang der 70er Jahre von IBM für die NSA (National Security Agency) entwickelt und war jahrelang weltweiter Verschlüsselungsstandard. Die Schlüssellänge dieses symmetrischen Verfahrens beträgt 56 Bits. Es gilt heute aufgrund der geringen Schlüssellänge als unsicher und wurde vom NIST im Jahr 2000 durch den AES (Rijndael-Algorithmus) ersetzt. Er sollte nicht mehr verwendet werden.

- **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 sehr sicher. Triple-DES arbeitet allerdings langsamer als andere Verfahren.

- **Blowfish**
  Die Entwicklung des prominenten Kryptografen Bruce Schneier verschlüsselt symmetrisch. Blowfish erreicht einen hervorragenden Datendurchsatz und gilt als sehr sicher.

- **CAST** (nach den Autoren **C**arlisle **A**dams und **S**tafford **T**avares)
  Ist ein symmetrisches Verfahren mit einer Schlüssellänge von 128 Bits. CAST ermöglicht eine variable Änderung von Teilen des Algorithmus' zur Laufzeit.

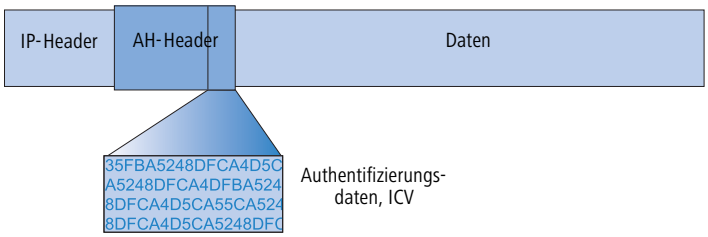


Die Verschlüsselung kann unter LANconfig in der Expertenkonfiguration angepasst werden. Eingriffe dieser Art sind in der Regel nur dann erforderlich, wenn VPN-Verbindungen zwischen Geräten unterschiedlicher Hersteller aufgebaut werden sollen. Standardmäßig bieten LANCOM-Gateways die Verschlüsselung entweder nach AES (128-bit), Blowfish (128-bit) oder Triple-DES (168-bit) an.

10.14.4 Die Authentifizierung – das AH-Protokoll

Das AH-Protokoll (**A**uthentification **H**eader) gewährleistet die Integrität und Authentizität der Daten. Häufig wird die Integrität als Bestandteil der Authentizität betrachtet. Wir betrachten im Folgenden die Integrität als separates Problem, das von AH gelöst wird. Neben Integrität und Authentizität bietet AH auch einen wirksamen Schutz gegen Wiedereinspielen empfangener Pakete (Replay Protection).

IP-Paketen fügt AH einen eigenen Header direkt hinter dem ursprünglichen IP-Header hinzu. Wichtigster Bestandteil dieses AH-Headers ist ein Feld mit Authentifizierungsdaten (Authentication Data), häufig auch als **I**ntegrity **C**heck **V**alue (ICV) bezeichnet.



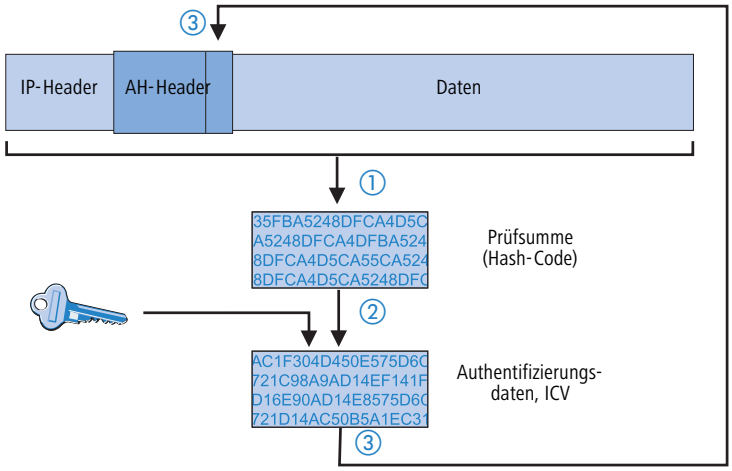
Der Ablauf von AH im Sender

Im Sender der Pakete läuft die Erstellung der Authentication Data in 3 Schritten ab.

① Aus dem Gesamtpaket wird eine Prüfsumme mittels Hash-Algorithmen errechnet.

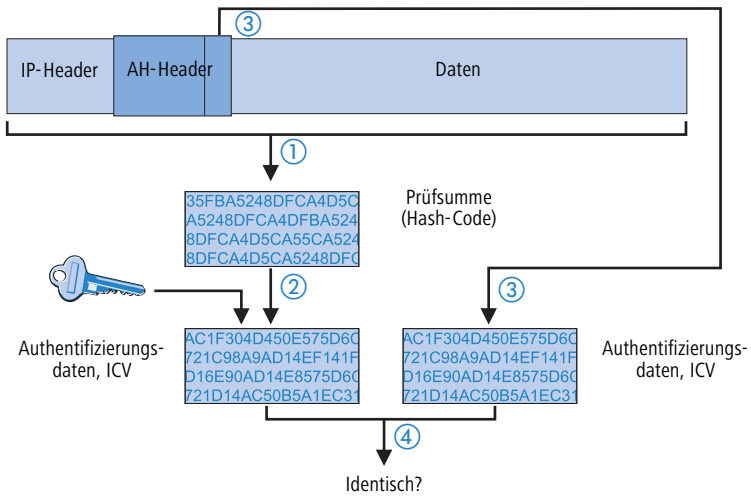
② Diese Prüfsumme wird zusammen mit einem dem Sender und Empfänger bekannten Schlüssel erneut durch einen Hash-Algorithmus geschickt.

③ Es ergeben sich die gesuchten Authentifizierungsdaten, die im AH-Header abgelegt werden.



Prüfung von Integrität und Authentizität im Empfänger

Beim Empfänger läuft das AH-Protokoll sehr ähnlich ab. Auch der Empfänger berechnet zunächst mit seinem Schlüssel die Authentifizierungsdaten für das empfangene Paket. Beim Vergleich mit dem übermittelten ICV des Paketes stellt sich heraus, ob Integrität und Authentizität des Paketes gegeben sind oder nicht.



Bildung der Prüfsumme für den Integritäts-Check

Um die Integrität, also die Korrektheit der transferierten Pakete zu gewährleisten, versieht AH beim Versand jedes Paket mit einer Prüfsumme. Beim Empfänger prüft AH, ob die Prüfsumme zum Inhalt des Paketes passt. Ist das nicht der Fall, dann wurde es entweder falsch übertragen oder bewusst verändert. Solche Pakete werden sofort verworfen und gelangen nicht mehr auf höhere Protokollebenen.

Zur Errechnung der Prüfsumme stehen verschiedene sogenannte Hash-Algorithmen zur Verfügung. Hash-Algorithmen zeichnen sich dadurch aus, dass das Ergebnis (der Hash-Code) charakteristisch für die Eingangsdaten ist („Fingerabdruck"), ohne dass umgekehrt vom Hash-Code auf die Eingangsdaten geschlossen werden könnte. Außerdem haben bei einem hochwertigen Hash-Algorithmus kleinste Änderungen des Eingangswertes einen völlig unterschiedlichen Hash-Code zur Folge. So werden systematische Analysen mehrerer Hash-Codes erschwert.

LANCOM VPN unterstützt die beiden gängigsten Hash-Algorithmen: MD5 und SHA-1. Beide Methoden arbeiten übrigens ohne Schlüssel, d.h. alleine auf der Basis fester Algorithmen. Schlüssel kommen erst in einem späteren Schritt von AH ins Spiel: bei der endgültigen Berechnung der Authentification Data. Die Integritäts-Prüfsumme ist nur ein notwendiges Zwischenergebnis auf dem Weg dorthin.

Berechnung der Authentifizierungsdaten

Im zweiten Schritt bildet AH einen neuen Hash-Code aus der Prüfsumme und einem Schlüssel, die endgültigen Authentifizierungsdaten. Auch für diesen Prozess gibt es unter IPSec verschiedene Standards zur Auswahl. LANCOM VPN unterstützt HMAC (**H**ash-based **M**essage **A**uthentication **C**ode). Als Hash-Algorithmen stehen die Hash-Funktionen MD5 und SHA-1 zur Verfügung. Die HMAC-Versionen heißen entsprechend HMAC-MD5-96 und HMAC-SHA-1-96.

Jetzt wird deutlich, dass AH das Paket selber unverschlüsselt lässt. Lediglich die Prüfsumme des Paketes und der eigene Schlüssel werden gemeinsam zum ICV, den Authentifizierungsdaten, chiffriert und dem Paket als Prüfkriterium beigelegt.

Replay Protection – Schutz vor wiederholten Paketen

AH kennzeichnet zusätzlich zur Beschriftung mit dem ICV jedes Paket auch mit einer eindeutigen, fortlaufenden Nummer (Sequence Number). Dadurch kann der Empfänger solche Pakete erkennen, die von einem Dritten aufgenommen wurden und nun wiederholt gesendet werden. Diese Art von Angriffen wird als „Packet Replay" bezeichnet.

Mit AH ist keine Maskierung von IPSec-Tunneln möglich, sofern nicht zusätzliche Maßnahmen wie NAT-Traversal oder ein äußeres Layer-2-Tunneling (z.B. PPPT/L2TP) nochmals einen „veränderbaren" äußeren IP-Header bereitstellen.

10.14.5 Management der Schlüssel – IKE

Das **I**nternet **K**ey **E**xchange Protocol (IKE) ist ein Protokoll, in dem Unterprotokolle zum Aufbau der SAs und für das Schlüsselmanagement eingebunden werden können.

Innerhalb von IKE werden in LANCOM VPN zwei Unterprotokolle verwendet: Oakley für die Authentifizierung der Partner und den Schlüsselaustausch sowie ISAKMP für die Verwaltung der SAs.

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.

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 'Lifetime' in der erweiterten Konfiguration von LANconfig kontrolliert werden.

LANCOM Referenzhandbuch Teil 4

- Wireless LAN - WLAN
- Virtuelle LANs (VLANs)

Stand: LCOS 7.6 mit Addendum 7.7 (siehe Anhang)

(letztes Update August 2009)

LANCOM Systems

© 2009 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®, Windows Vista™, Windows NT® und Microsoft® sind eingetragene Marken von Microsoft, Corp.

Das LANCOM Systems-Logo, LCOS und die Bezeichnung LANCOM sind eingetragene Marken der LANCOM Systems GmbH. Alle übrigen verwendeten Namen und Bezeichnungen können Marken oder eingetragene Marken ihrer jeweiligen Eigentümer sein.

LANCOM Systems behält sich vor, die genannten Daten ohne Ankündigung zu ändern und übernimmt keine Gewähr für technische Ungenauigkeiten und/oder Auslassungen.

Produkte von LANCOM Systems enthalten Software, die vom „OpenSSL Project" für die Verwendung im „OpenSSL Toolkit" entwickelt wurde (http://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.

Produkte von LANCOM Systems enthalten Komponenten, die als Open Source Software im Quelltext verfügbar sind und speziellen Lizenzen sowie den Urheberrechten verschiedener Autoren unterliegen. Im Besonderen enthält die Firmware Komponenten, die der GNU General Public License, Version 2 (GPL) unterliegen. Die Lizenzvereinbarung mit dem Text der GPL ist auf der LANCOM CD im Produktverzeichnis zu finden. Auf Anfrage können die Quelltexte und alle Lizenzhinweise elektronisch vom FTP-Server der LANCOM Systems GmbH bezogen werden.

Die Firmware des LANCOM VP-100 enthält Komponenten, die als Open Source Software im Quelltext verfügbar sind und speziellen Lizenzen sowie den Urheberrechten verschiedener Autoren unterliegen. Im Besonderen enthält die Firmware Komponenten, die der GNU General Public License, Version 2 (GPL) unterliegen. Die Lizenzvereinbarung mit dem Text der GPL ist auf der LANCOM CD im Produktverzeichnis als LC-VP100-License-DE.txt zu finden. Auf Anfrage können die Quelltexte und alle Lizenzhinweise elektronisch vom FTP-Server der LANCOM Systems GmbH bezogen werden.

LANCOM Systems GmbH

Adenauerstr. 20/B2

52146 Würselen

Deutschland

www.lancom.de

Würselen, August 2009

110653/0809

Inhalt

11 Wireless LAN – WLAN 11 - 5

11.1 Einleitung 11 - 5

11.2 Anwendungsszenarien 11 - 5
- 11.2.1 Infrastruktur-Modus 11 - 6
- 11.2.2 Hotspot oder Gastzugang 11 - 6
- 11.2.3 Managed-Modus 11 - 6
- 11.2.4 WLAN-Bridge (Point-to-Point) 11 - 7
- 11.2.5 WLAN-Bridge im Relais-Betrieb 11 - 8
- 11.2.6 WLAN-Bridge zum Access Point – managed und unmanaged gemischt 11 - 8
- 11.2.7 Wireless Distribution System (Point-to-Multipoint) 11 - 8
- 11.2.8 Client-Modus 11 - 9
- 11.2.9 Client-Modus bei bewegten Objekten im Industriebereich 11 - 9

11.3 WLAN-Standards 11 - 10
- 11.3.1 IEEE 802.11n 11 - 11
- 11.3.2 IEEE 802.11a: 54 MBit/s 11 - 17
- 11.3.3 IEEE 802.11h – ETSI 301 893 11 - 17
- 11.3.4 IEEE 802.11g: 54 MBit/s 11 - 19
- 11.3.5 IEEE 802.11b: 11 MBit/s 11 - 19

11.4 WLAN-Sicherheit 11 - 19
- 11.4.1 Grundbegriffe 11 - 19
- 11.4.2 IEEE 802.11i / WPA2 11 - 20
- 11.4.3 TKIP und WPA 11 - 23
- 11.4.4 WEP 11 - 23
- 11.4.5 LEPS – LANCOM Enhanced Passphrase Security 11 - 24
- 11.4.6 Standard-WEP-Verschlüsselung 11 - 24
- 11.4.7 Background WLAN Scanning 11 - 25

11.5 Konfiguration der WLAN-Parameter 11 - 26
- 11.5.1 Allgemeine WLAN-Einstellungen 11 - 26
- 11.5.2 WLAN-Sicherheit 11 - 27
- 11.5.3 Auswahl der im WLAN zulässigen Stationen 11 - 31
- 11.5.4 Verschlüsselungs-Einstellungen 11 - 32
- 11.5.5 Die physikalischen WLAN-Schnittstellen 11 - 35
- 11.5.6 Die Punkt-zu-Punkt-Partner 11 - 43
- 11.5.7 Die logischen WLAN-Schnittstellen 11 - 44
- 11.5.8 IEEE 802.1x/EAP 11 - 47
- 11.5.9 Experten-WLAN-Einstellugnen 11 - 48
- 11.5.10 WLAN-Routing (Isolierter Modus) 11 - 50

11.6 Konfiguration des Client-Modus 11 - 50
- 11.6.1 Client-Einstellungen 11 - 51
- 11.6.2 SSID des verfügbaren Netzwerke einstellen 11 - 51
- 11.6.3 Verschlüsselungseinstellungen 11 - 51
- 11.6.4 Roaming 11 - 52

11.7 Konfiguration der Punkt-zu-Punkt-Verbindungen 11 - 53
- 11.7.1 Geometrische Auslegung von Outdoor-Funknetz-Strecken 11 - 54
- 11.7.2 Ausrichten der Antennen für den P2P-Betrieb 11 - 56
- 11.7.3 Vermessung von Funkstrecken 11 - 58
- 11.7.4 Punkt-zu-Punkt-Betriebsart aktivieren 11 - 58
- 11.7.5 Konfiguration der P2P-Verbindungen 11 - 58
- 11.7.6 Access Points im Relais-Betrieb 11 - 60
- 11.7.7 Sicherheit von Punkt-zu-Punkt-Verbindungen 11 - 60

11.8 Zentrales WLAN-Management 11 - 61
- 11.8.1 Der CAPWAP-Standard 11 - 62
- 11.8.2 Die Smart-Controller-Technologie 11 - 62
- 11.8.3 Kommunikation zwischen Access Point und WLAN-Controller 11 - 64
- 11.8.4 Zero-Touch-Management 11 - 65
- 11.8.5 Split-Management 11 - 65
- 11.8.6 Allgemeine Einstellungen 11 - 65

11.8.7 Profile 11 - 66
11.8.8 Liste der Access Points 11 - 68
11.8.9 Stationstabelle (ACL-Tabelle) 11 - 70
11.8.10 Optionen für den WLAN-Controller 11 - 70
11.8.11 Neue Access Points manuell in die WLAN-Struktur aufnehmen 11 - 71
11.8.12 Access Points manuell aus der WLAN-Struktur entfernen 11 - 72
11.8.13 Vererbung von Parametern 11 - 73
11.8.14 Sicherung der Zertifikate 11 - 73
11.8.15 Sichern und Wiederherstellen weiterer Dateien der SCEP-CA 11 - 75
11.8.16 Load-Balancing zwischen den WLAN-Controllern 11 - 76
11.8.17 Dynamische VLAN-Zuweisung 11 - 76
11.8.18 Prüfung der WLAN-Clients über RADIUS (MAC-Filter) 11 - 77
11.8.19 Access Point deaktivieren oder dauerhaft aus der WLAN-Struktur entfernen 11 - 78
11.8.20 Anzeigen und Aktionen im LANmonitor 11 - 79
11.8.21 Konfiguration der Access Points 11 - 79
11.8.22 Automatische Funkfeldoptimierung mit LANCOM WLAN Controllern 11 - 80

11.9 Zentrales Firmware- und Skript-Management 11 - 81

11.10 Mehrstufige Zertifikate für PublicSpots 11 - 84

11.11 DFS 2: Freilassen von Kanälen für Wetter-Radar 11 - 85

11.12 Bandbreitenbegrenzung im WLAN 11 - 85
11.12.1 Einstellung als Access Point 11 - 85
11.12.2 Einstellung als Client 11 - 86

12 Virtuelle LANs (VLANs) 12 - 1

12.1 Was ist ein Virtuelles LAN? 12 - 1

12.2 So funktioniert ein VLAN 12 - 1
12.2.1 Frame-Tagging 12 - 2
12.2.2 Umsetzung in den Schnittstellen des LANs 12 - 2
12.2.3 VLAN Q-in-Q-Tagging 12 - 3
12.2.4 Anwendungsbeispiele 12 - 3

12.3 Konfiguration von VLANs 12 - 4
12.3.1 VLAN und ARF 12 - 4
12.3.2 VLAN und WLAN-Controller 12 - 4
12.3.3 Allgemeine Einstellungen 12 - 5
12.3.4 Die Netzwerktabelle 12 - 5
12.3.5 Die Porttabelle 12 - 6

12.4 Konfigurierbare VLAN-IDs 12 - 6
12.4.1 VLAN-IDs für WLAN-Clients 12 - 6
12.4.2 VLAN-IDs für DSL-Interfaces 12 - 7
12.4.3 VLAN-IDs für DSLoL-Interfaces 12 - 7

12.5 VLAN-Tags auf Layer 2/3 im Ethernet 12 - 7
12.5.1 Einleitung 12 - 7
12.5.2 Konfiguration des VLAN-Taggings auf Layer 2/3 12 - 8

11 Wireless LAN – WLAN

11.1 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 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 LANCOM Access Points 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 ADSL, DSL und/oder ISDN. 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.

LANCOM Wireless Router und LANCOM Access Points können entweder als autarke Access Points 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 gesteuert wird (Betriebsart „Managed-Modus").

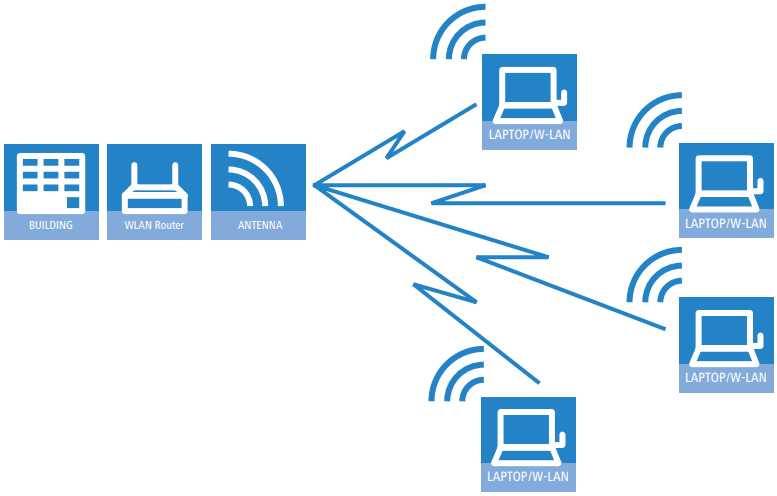
11.2 Anwendungsszenarien

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 Access Points (Infrastruktur-Modus)
- Hotspot oder Gastzugang
- Verbinden zweier LANs über eine Funkstrecke (Point-to-Point-Modus)
- Relaisfunktion zur Verbindung von Netzwerken über mehrere Access Points
- Anbindung von Geräten mit Ethernet-Schnittstelle über einen Access Point (Client-Modus)
- Zentrale Verwaltung durch einen LANCOM WLAN Controller (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 Access Point (Ad-hoc-Modus)

11.2.1 Infrastruktur-Modus

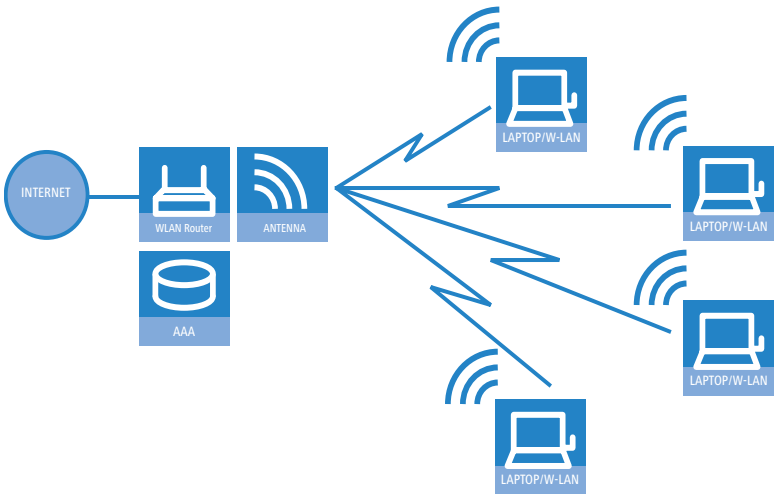
Im Infrastruktur-Modus verbinden sich die WLAN-Clients mit einem zentralen Vermittlungspunkt, dem Access Point. Der Access Point spannt eine oder mehrere Funkzellen (WLAN-Netzwerke) auf, regelt die Zugangsrechte der WLAN-Clients zu diesen Funkzellen, die Kommunikation der Clients untereinander und den 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 Access Points einen gemeinsamen Zugang für WLAN-Clients anbieten. Je nach Bedarf können die Clients zwischen den verschiedenen Access Points 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".



11.2.2 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 Access Points 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 Access Point 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.



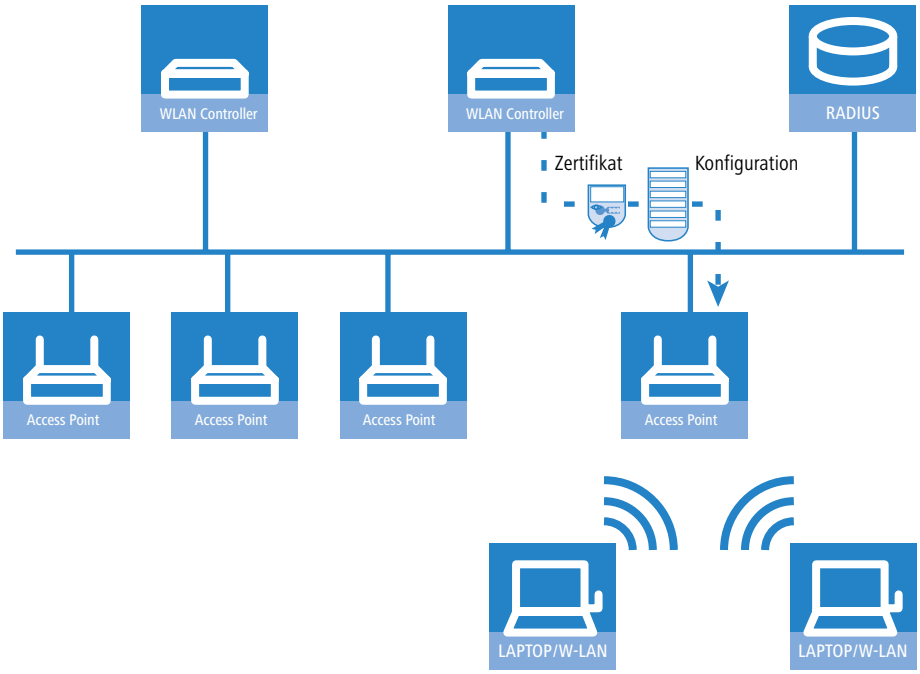
11.2.3 Managed-Modus

Der weit verbreitete Einsatz von Wireless Access Points und Wireless Routern hat zu einem deutlich komfortableren und flexibleren Zugang zu Netzwerken in Firmen, Universitäten und anderen Organisationen geführt. Mit einem zen-

tralen WLAN-Management wird die Konfiguration der Access Points im Managed-Modus nicht mehr in den Geräten selbst vorgenommen, sondern in einer zentralen Instanz, dem WLAN-Controller.

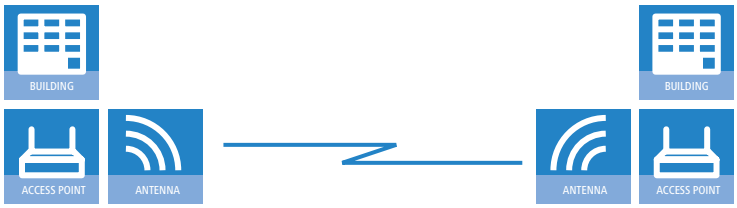
Der WLAN-Controller authentifiziert die Access Points und überträgt den zugelassenen Geräten ein Zertifikat und eine passende Konfiguration. Dadurch kann die Konfiguration des WLANs komfortabel von einer zentralen Stelle übernommen werden und die Konfigurationsänderungen wirken sich zeitgleich auf alle Access Points 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.

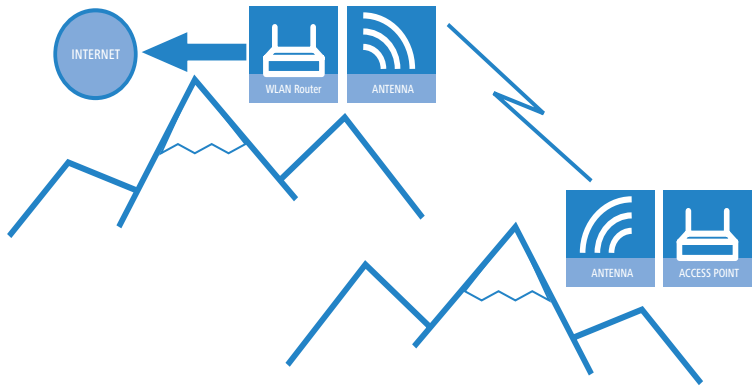


11.2.4 WLAN-Bridge (Point-to-Point)

Während es sich bei den bisher vorgestellten Anwendungsszenarien immer um die Anbindung von mehreren WLAN-Clients an einen Access Point handelt (Point-to-Multipoint), spielen die WLAN-Systeme gerade im Outdoor-Bereich ihre Stärken auch und vor allem bei der Verbindung von zwei Access Points aus (Point-to-Point). Mit der Einrichtung einer Funkstrecke zwischen zwei Access Points kann z. B. ein Produktionsgebäude auf einem weitläufigen Unternehmensgelände sehr einfach in das Netzwerk eingebunden werden.



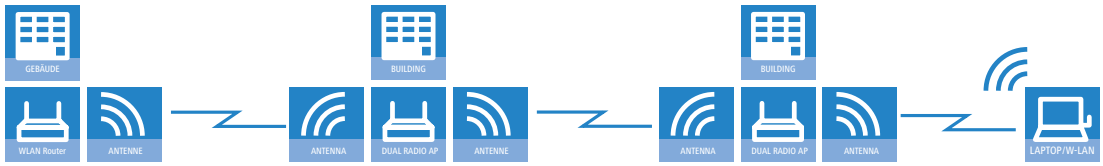
Mit einer Punkt-zu-Punkt-Verbindung kann aber z. B. auch in schwierigem Gelände (z. B. in den Bergen oder auf einer Insel) ein Internetzugang an Orten bereitgestellt werden, an denen eine Verkabelung zu aufwendig wäre. Bei direkter Sichtbeziehungen zwischen den beiden Access Points können mit diesen Funkstrecken Distanzen von mehreren Kilometern überbrückt werden.



11.2.5 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 Access Points über die tatsächliche Reichweite hinausgeht oder wenn Hindernisse zwischen den Access Points die direkte Funkübertragung stören oder verhindern.

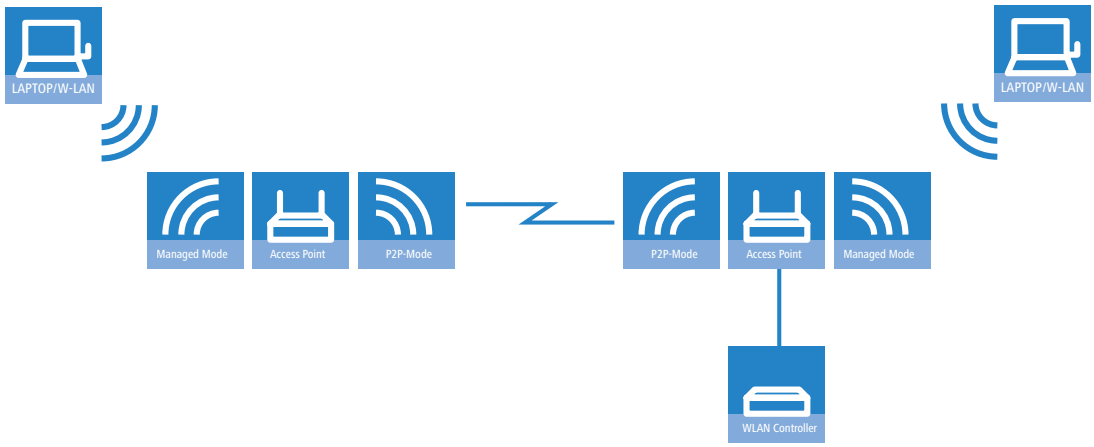
In solchen Fällen kann durch eine Verkettung von mehreren Access Points mit jeweils zwei WLAN-Modulen eine Verbindung zwischen den beiden Endpunkten hergestellt werden. Da die Access Points an den Zwischenstationen in der Regel nur als Schaltstelle dienen, nennt man diese Betriebsart der Access Points auch „Relais-Modus".



Obwohl LANCOM Access Points 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.

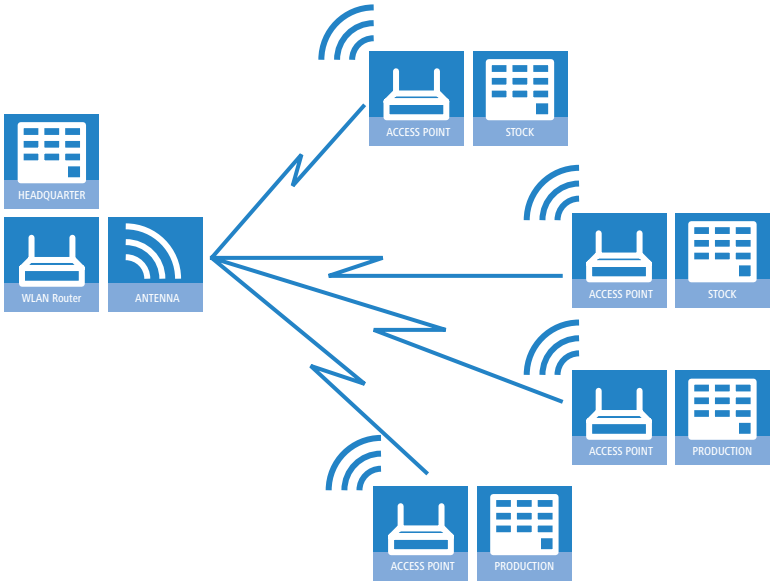
11.2.6 WLAN-Bridge zum Access Point – managed und unmanaged gemischt

Die von einem zentralen WLAN-Controller verwalteten Access Points werden in der Regel direkt mit dem kabelgebundenen Ethernet verbunden. Wenn das nicht möglich ist, können die managed Access Points 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 Access Point betrieben, dieses WLAN-Modul bezieht seine Konfiguration immer zentral vom WLAN-Controller. Das andere WLAN-Modul wird dabei fest als WLAN-Bridge konfiguriert.



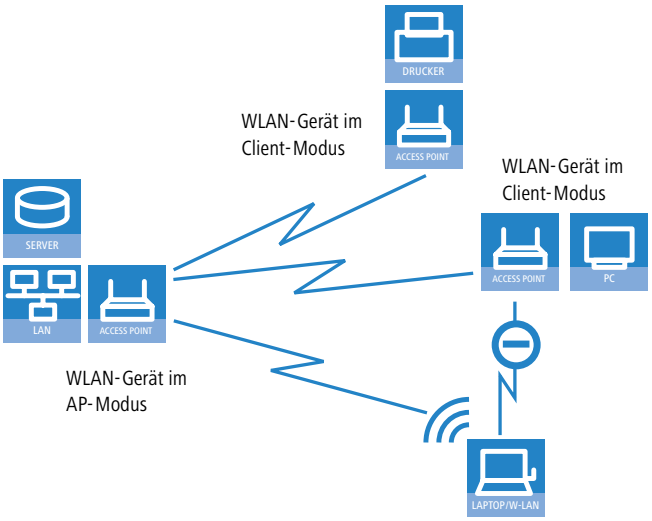
11.2.7 Wireless Distribution System (Point-to-Multipoint)

Eine besondere Variante der Funkstrecken ist die Anbindung von mehreren verteilten Access Points 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 Access Point oder Wireless Router wird dabei als „Master" konfiguriert, die WDS-Gegenstellen als „Slave".



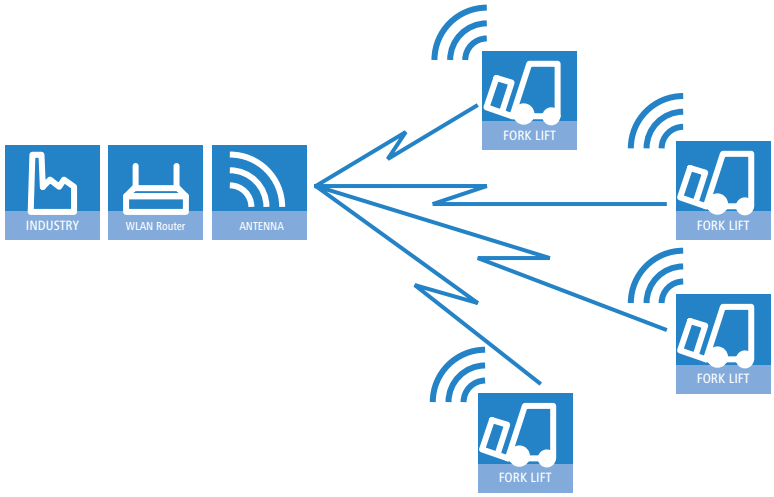
11.2.8 Client-Modus

Zur Anbindung von einzelnen Geräten mit einer Ethernet-Schnittstelle in ein WLAN können LANCOM Access Points in den sogenannten Client-Modus versetzt werden, in dem sie sich wie ein herkömmlicher WLAN-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 WLAN einzubinden.



11.2.9 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.



11.3 WLAN-Standards

IEEE 802.11

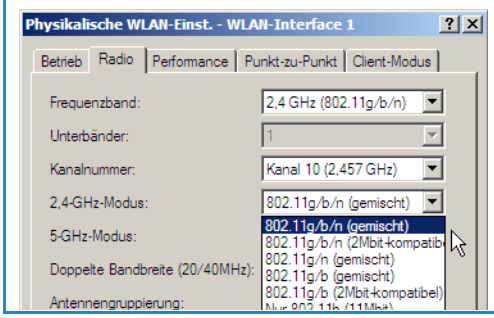
LANCOM WLAN-Geräte arbeiten nach dem IEEE-Standard 802.11. Diese Standard-Familie stellt eine Erweiterung der bereits vorhandenen IEEE-Normen für LANs dar, von denen IEEE 802.3 für Ethernet die bekannteste ist. Innerhalb der IEEE 802.11 Familie gibt es verschiedene Standards für die Funkübertragung in unterschiedlichen Frequenzbereichen und mit unterschiedlichen Geschwindigkeiten. LANCOM Access Points und AirLancer Client Adapter unterstützen je nach Ausführung unterschiedliche Standards:

- IEEE 802.11n mit bis zu 300 MBit/s Übertragungsrate im 5 GHz oder 2,4 GHz Frequenzband, mit neuen Mechanismen wie zum Beispiel die Nutzung von MIMO, 40-MHz-Kanälen, Packet Aggregation und Block Acknowledgement.
- IEEE 802.11a mit bis zu 54 MBit/s Übertragungsrate im 5 GHz Frequenzband, bis zu 108 MBit/s mit Turbo-Modus (Ergänzung zum Standard).
- IEEE 802.11g mit bis zu 54 MBit/s Übertragungsrate im 2,4 GHz Frequenzband, bis zu 108 MBit/s mit Turbo-Modus (Ergänzung zum Standard).
- Auch wenn aktuelle WLAN-Adapter in der Regel nach 802.11a/g/n betrieben werden, untertsützen LANCOM Access Points aus Gründen der Kompatibilität zu älteren WLAN-Adaptern auch den Standard IEEE 802.11b mit bis zu 11 MBit/s Übertragungsrate im 2,4 GHz Frequenzband.

Durch die Einhaltung der IEEE-Standards arbeiten die LANCOM WLAN-Geräte problemlos und zuverlässig auch mit Geräten anderer Hersteller zusammen. Ihr LANCOM Access Point unterstützt je nach Modell die Standards IEEE 802.11g (abwärtskompatibel zu IEEE 802.11b) und/oder IEEE 802.11a sowie IEEE 802.11n Draft 2.0.

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 ein anderes Frequenzband nutzen. Da die Standards im 2,4 GHz-Band IEEE 802.11b/g/n abwärtskompatibel zu einander sind, ist der gleichzeitige Betrieb dieser Standards auf einem WLAN-Modul mit Geschwindigkeitseinbußen möglich.

Übertragungsraten im Kompatibilitätsmodus



Bitte beachten Sie, dass die erreichten Datenübertragungsraten bei IEEE 802.11b/g/n-Geräten vom verwendeten 2,4-GHz-Modus abhängen. Werden die langsameren Stationen in einem Funknetzwerk mit eingeschaltetem Kompatibilitätsmodus aktiv, sinkt die tatsächliche Übertragungsrate ab.

Bitte beachten Sie, dass nicht alle Frequenzen in jedem Land erlaubt sind! Eine Tabelle mit den Frequenzen und die Zulassungsvorschriften finden Sie im Anhang des Handbuchs zum jeweiligen Gerät.

11.3.1 IEEE 802.11n

Mit einer Reihe von technologischen Veränderungen erlaubt 802.11n, die Performance von WLAN-Systemen im 5 GHz oder 2,4 GHz Frequenzband etwa um das Fünffache zu steigern. Die Änderungen sind zwar noch nicht offiziell von der IEEE beschlossen, aber die Auswirkungen des absehbaren Technologiesprungs sind so faszinierend, dass die Industrie bereits vor der Verabschiedung des Standards entsprechende WLAN-Geräte auf den Markt bringt. Der aktuelle Stand der Diskussion wird als so genannter „Draft 2.0" definiert, auf den sich die aktuell im Markt verfügbaren Geräte beziehen.

Wenn in diesem Dokument von „802.11n" die Rede ist, wird daher immer der aktuelle Draft 2.0 gemeint, es handelt sich nicht um einen verabschiedeten IEEE-Standard.

Einige der Verbesserungen beziehen sich auf den Physical Layer (PHY), der die Übertragung der einzelnen Bits auf dem physikalischen Medium beschreibt – wobei in diesem Fall die Luft das physikalische Medium darstellt. Andere Erweiterungen beziehen sich auf den MAC-Layer (MAC), der u. a. den Zugriff auf das Übertragungsmedium regelt. Beide Bereiche werden im Folgenden separat betrachtet.

Vorteile von 802.11n

Zu den Vorteilen der neuen Technologie gehören unter anderem die folgenden Aspekte:

- **Höherer effektiver Datendurchsatz**

  Der 802.11n Draft 2.0 beinhaltet zahlreiche neue Mechanismen um die verfügbare Bandbreite signifikant zu erhöhen. Bei den aktuellen WLAN-Standards nach 802.11a/g sind physikalische Datenraten (Brutto-Datenraten) von bis zu 54 Mbit/s möglich, netto werden ca. 22 Mbit/s erreicht. Netzwerke nach 802.11n erzielen **derzeit** einen Brutto-Datendurchsatz von bis zu 300 Mbit/s (netto in der Praxis ca. 120 bis 130 Mbit/s) – prinzipiell definiert der Standard bis zu 600 Mbit/s mit vier Datenströmen. Die maximal realisierbaren Geschwindigkeiten überschreiten zum ersten Mal den Fast-Ethernet-Standard mit 100 Mbit/s in einem kabelgebundenen Netzwerk, was aktuell an den meisten Arbeitsplätzen den Standard darstellt.

- **Bessere und zuverlässigere Funkabdeckung**

  Die neuen Technologien bei 802.11n steigern nicht nur den Datendurchsatz, sondern bringen gleichzeitig Verbesserungen in der Reichweite und reduzieren die Funklöcher bei vorhandenen a/b/g Installationen.

  Das Ergebnis sind bessere Signalabdeckung und höhere Stabilität, die insbesondere für Anwender im professionellen Umfeld eine deutliche Verbesserung bei der Nutzung des drahtlosen Netzwerkes bieten.

- **Höhere Reichweite**

  Mit der Entfernung des Empfängers vom Sender nimmt im Allgemeinen der Datendurchsatz ab. Durch den insgesamt verbesserten Datendurchsatz erzielen WLAN-Netze nach 802.11n auch eine höhere Reichweite, da in einer bestimmten Entfernung vom Access Point ein wesentlich stärkeres Funksignal empfangen wird als in 802.11a/b/g-Netzen.

Kompatibilität mit anderen Standards

Der 802.11n Standard ist rückwärts-kompatibel mit bisherigen Standards (IEEE 802.11a/b/g). Einige Vorteile der neuen Technologie sind jedoch nur verfügbar, wenn neben den Access Points auch die WLAN-Clients 802.11n-kompatibel sind.

Um die Co-Existenz von WLAN-Clients nach 802.11a/b/g zu ermöglichen (die im Sprachgebrauch von 802.11n als „Legacy-Clients" bezeichnet werden), bieten die 802.11n-Access Points besondere Mechanismen für den gemischten Betrieb an, in denen die Performance-Steigerungen gegenüber 802.11a/b/g geringer ausfallen. Nur in reinen 802.11n-Umgebungen wird der „Greenfield-Modus" verwendet, der alle Vorteile der neuen Technologien ausnutzen kann. Im Greenfield-Modus unterstützen sowohl Access Points als auch WLAN-Clients den 802.11n-Draft und die Access Points lehnen Verbindungen von Legacy Clients ab.

Der physikalische Layer

Der physikalische Layer beschreibt, wie die Daten umgewandelt werden müssen, damit sie als Folge von einzelnen Bits über das physikalische Medium übertragen werden können. Bei einem WLAN-Gerät werden dazu die beiden folgenden Schritte vollzogen:

- Modulation der digitalen Daten auf analoge Trägersignale
- Modulation der Trägersignale auf ein Funksignal im gewählten Frequenzband, bei WLAN entweder 2,4 oder 5 GHz.

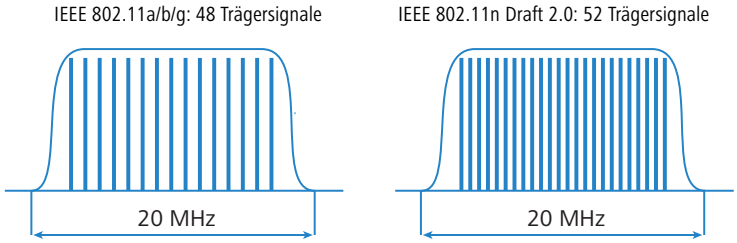
Die zweite der beiden Modulationen läuft bei IEEE 802.11n genau so ab wie bei den bisherigen WLAN-Standards und ist daher keine weitere Betrachtung wert. Für die Modulation der digitalen Daten auf analoge Trägersignale ergeben sich durch 802.11n jedoch zahlreiche Änderungen.

Technische Aspekte von 802.11n

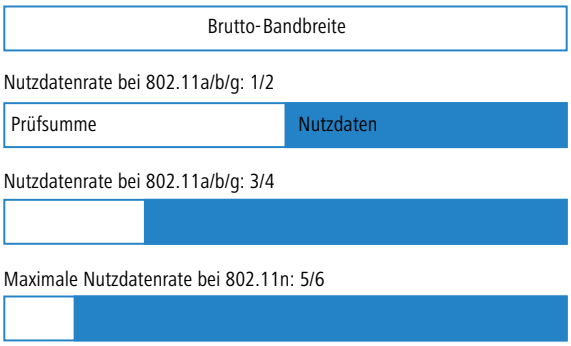
Verbesserte OFDM- Modulation (MIMO- OFDM)

802.11n nutzt wie auch 802.11a/g das OFDM-Verfahren (Orthogonal Frequency Division Multiplex) als Modulationstechnik. Dabei wird das Datensignal nicht nur auf ein einzelnes, sondern parallel auf mehrere Trägersignale moduliert. Der Datendurchsatz, der mit dem OFDM-Verfahren zu erzielen ist, hängt u. a. von folgenden Parametern ab:

- Anzahl der Trägersignale: Während bei 802.11a/g 48 Trägersignale verwendet werden, nutzt 802.11n maximal 52 Trägersignale.



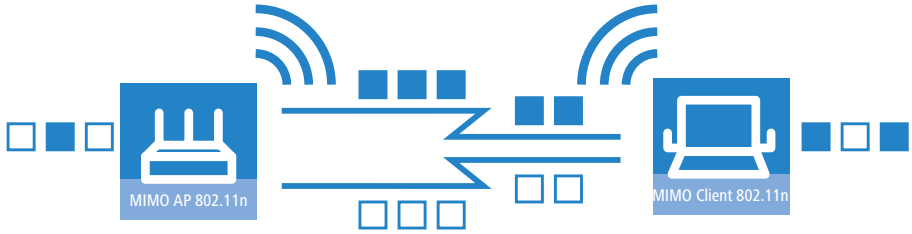
- Nutzdatenrate: Die Übertragung der Daten über die Luft ist grundsätzlich nicht zuverlässig. Schon leichte Störungen im WLAN-System können zu Fehlern in der Datenübertragung führen. Um diese Fehler auszugleichen, werden sogenannte Prüfsummen verwendet, die einen Teil der verfügbaren Bandbreite beanspruchen. Die Nutzdatenrate gibt das Verhältnis der theoretisch verfügbaren Bandbreite zu den tatsächlichen Nutzdaten an. 802.11a/g können mit Nutzdatenraten von 1/2 oder 3/4 arbeiten, 802.11n kann bis zu 5/6 der theoretisch verfügbaren Bandbreite für die Nutzdaten verwenden.



Mit diesen beiden Maßnahmen steigt die nutzbare Bandbreite von maximal 54 Mbit/s bei 802.11a/g auf 65 Mbit/s bei 802.11n. Diese Steigerung ist noch nicht spektakulär, sie wird jedoch durch die noch folgenden Maßnahmen weiter verbessert.

Die MIMO-Technologie

MIMO (Multiple Input Multiple Output) ist die wichtigste neue Technologie in 802.11n. MIMO benutzt mehrere Sender und mehrere Empfänger, um bis zu vier parallele Datenströme auf dem gleichen Übertragungskanal zu übertragen (derzeit werden nur zwei parallele Datenströme realisiert). Das Resultat ist eine Steigerung des Datendurchsatzes und Verbesserung des Funkabdeckung.

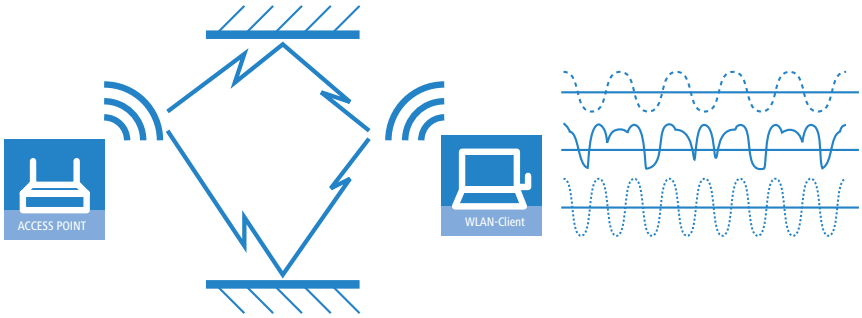


Die Daten werden also z. B. beim Access Point in zwei Gruppen aufgeteilt, die jeweils über separate Antennen, aber gleichzeitig zum WLAN-Client gesendet werden. Mit dem Einsatz von zwei Sende- und Empfangsantennen kann also der Datendurchsatz verdoppelt werden.

Wie aber können auf einem Kanal mehrere Signale gleichzeitig übertragen werden, was bei den bisherigen WLAN-Anwendungen immer für unmöglich gehalten wurde?

Betrachten wir dazu die Datenübertragung in „normalen" WLAN-Netzen: Die Antenne eines Access Points sendet Daten je nach Antennentyp in mehrere Richtungen gleichzeitig. Die elektromagnetischen Wellen werden an vielen

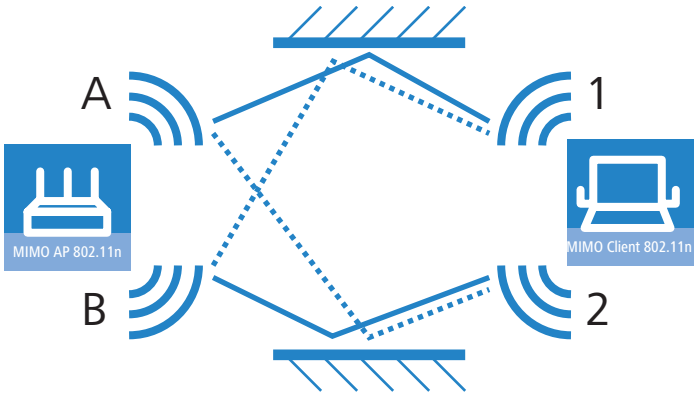
Flächen in der Umgebung reflektiert, sodass ein ausgesendetes Signal auf vielen unterschiedlichen Wegen die Antennen des WLAN-Clients erreicht – man spricht auch von „Mehrwegeausbreitung". Jeder dieser Wege ist unterschiedlich lang, sodass die einzelnen Signale mit einer gewissen Zeitverzögerung den Client erreichen.



Die zeitverzögerten Signale überlagern sich beim WLAN-Client so, dass aus diesen Interferenzen eine deutliche Verschlechterung des Signals resultiert. Aus diesem Grund werden in den bisherigen WLAN-Netzwerken die direkten Sichtbeziehungen zwischen Sender und Empfänger (englisch: Line of Sight – LOS) angestrebt, um den Einfluss der Reflexionen zu reduzieren.

Die MIMO-Technologie wandelt diese Schwäche der WLAN-Übertragung in einen Vorteil, der eine enorme Steigerung des Datendurchsatzes ermöglicht. Wie schon angemerkt ist es eigentlich unmöglich, zur gleichen Zeit auf dem gleichen Kanal unterschiedliche Signale zu übertragen, da der Empfänger diese Signale nicht auseinanderhalten kann. MIMO nutzt die Reflexionen der elektromagnetischen Wellen, um mit dem räumlichen Aspekt ein drittes Kriterium zur Identifizierung der Signale zu gewinnen.

Ein von einem Sender A ausgestrahltes und vom Empfänger 1 empfangenes Signal legt einen anderen Weg zurück als ein Signal von Sender B zu Empfänger 2 – beide Signale erfahren auf dem Weg andere Reflexionen und Polarisationsänderungen, haben also einen charakteristischen Weg hinter sich. Zu Beginn der Datenübertragung wird dieser charakteristische Weg in einer Trainingsphase mit normierten Daten aufgezeichnet. In der Folgezeit kann aus den empfangenen Daten zurückgerechnet werden, zu welchem Datenstrom die Signale gehören. Der Empfänger kann also selbst entscheiden, welches der anliegenden Signale verarbeitet wird und vermeidet so die Verluste durch die Interferenzen der ungeeigneten Signale.



MIMO ermöglicht also die gleichzeitige Übertragung mehrerer Signale auf einem geteilten Medium wie der Luft. Die einzelnen Sender und Empfänger müssen dazu jeweils einen räumlichen Mindestabstand einhalten, der allerdings nur wenige Zentimeter beträgt. Dieser Abstand schlägt sich in unterschiedlichen Reflexionen bzw. Signalwegen nieder, die zur Trennung der Signale verwendet werden können.

Generell sieht MIMO bis zu vier parallele Datenströme vor, die auch als „Spatial Streams" bezeichnet werden. In der aktuellen Chipsatz-Generation werden jedoch nur zwei parallele Datenströme realisiert, da die Trennung der Datenströme anhand der charakteristischen Wegeinformationen sehr rechenintensiv ist und daher relativ viel Zeit und Strom benötigt. Gerade Letzteres ist aber besonders bei WLAN-Systemen eher unerwünscht, da oft eine Unabhängigkeit vom Stromnetz auf der Seite der WLAN-Clients bzw. eine PoE-Versorgung der Access Points angestrebt wird.

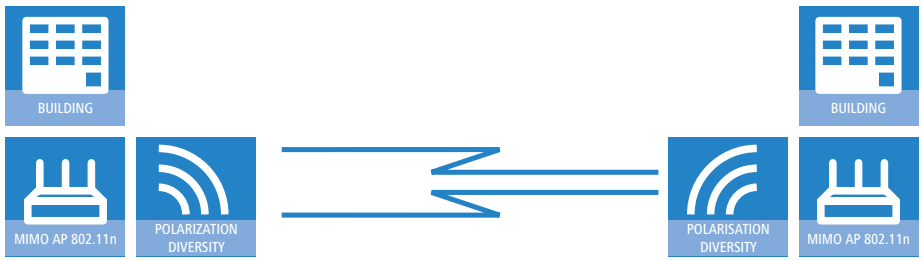
Auch wenn das Ziel von vier Spatialströmen derzeit nicht erreicht wird, führt die Verwendung von zwei separaten Datenverbindungen zu einer Verdoppelung des Datendurchsatzes, was einen wirklichen Technologiesprung im Bereich der WLAN-Systeme darstellt. Zusammen mit den Verbesserungen in der OFDM-Modulation steigt der erreichbare Datendurchsatz damit auf maximal 130 Mbit/s.

Mit der Kurzbezeichnung „Sender x Empfänger" wird die tatsächliche Anzahl der Sender- und Empfänger-Antennen wiedergegeben. Ein 3x3-MIMO beschreibt also drei Sender- und drei Empfänger-Antennen. Die Anzahl der Antennen ist jedoch nicht gleichbedeutend mit der Anzahl der Datenströme: Die verfügbaren Antennen begrenzen nur die

maximale Anzahl der Spatial Streams. Der Grund für den Einsatz von mehr Antennen als für die Übertragung der Datenströme eigentlich notwendig sind, liegt in der Zuordnung der Signale über den charakteristischen Weg: Mit einem dritten Signal werden zusätzliche räumliche Informationen übertragen. Sollten sich die Daten aus den beiden ersten Signalen einmal nicht eindeutig zuordnen lassen, kann die Berechnung mithilfe des dritten Signals dennoch gelingen. Die Verwendung von zusätzlichen Antennen trägt also nicht zur Steigerung des Datendurchsatzes bei, resultiert aber in einer gleichmäßigeren und besseren Abdeckung für die Clients.

MIMO im Outdoor- Einsatz

Bei Outdoor-Anwendungen von 802.11n können die natürlichen Reflexionen nicht genutzt werden, da die Signalübertragung üblicherweise auf direktem Weg zwischen den entsprechend ausgerichteten Antennen stattfindet. Um auch hier zwei Datenströme parallel übertragen zu können, werden spezielle Antennen verwendet, die gezielt zwei um 90° gedrehte Polarisationsrichtungen verwenden. Bei diesen sogenannten „Dual-Slant-Antennen" handelt es sich also eigentlich um zwei Antennen in einem gemeinsamen Gehäuse. Da ein drittes Signal hier keine zusätzliche Sicherheit bringen würde, werden bei Outdoor-Anwendungen üblicherweise genau so viele Antennen (bzw. Polarisationsrichtungen) eingesetzt, wie Datenströme übertragen werden.

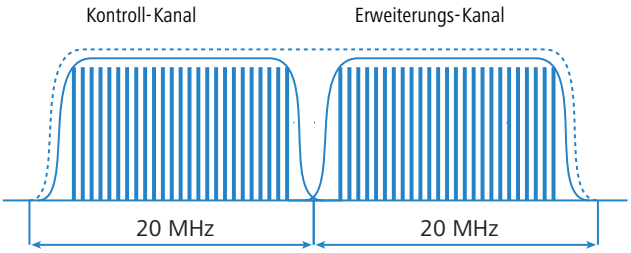


40 MHz- Kanäle

Bei den Ausführungen zur OFDM-Modulation wurde bereits beschrieben, dass der Datendurchsatz mit zunehmender Anzahl von Trägersignalen steigt, weil so mehrere Signale gleichzeitig übertragen werden können. Wenn in einem Kanal mit einer Bandbreite von 20 MHz nicht mehr als 48 (802.11a/g) bzw. 52 (802.11n) Trägersignale genutzt werden können, liegt es nahe, einen zweiten Kanal mit weiteren Trägersignalen zu verwenden.

Bereits in der Vergangenheit wurde diese Technik von einigen Herstellern (u. a. LANCOM Systems) eingesetzt und als „Turbo-Modus" bezeichnet, der Datenraten von bis zu 108 Mbit/s ermöglicht. Der Turbo-Modus ist zwar nicht Bestandteil der offiziellen IEEE-Standards, wird aber z. B. auf Point-to-Point-Verbindungen häufig eingesetzt, weil dabei die Kompatibilität zu anderen Herstellern eine eher untergeordnete Rolle spielt.

Der Erfolg hat der zugrunde liegenden Technik aber dazu verholfen, in die Entwicklung von 802.11n einzufließen. Der IEEE 802.11n Draft 2.0 verwendet den zweiten Übertragungskanal allerdings in einer Art und Weise, dass die Kompatibilität zu Geräten nach IEEE 802.11a/g erhalten bleibt. 802.11n überträgt die Daten über zwei direkt benachbarte Kanäle. Einer davon übernimmt die Aufgabe des Kontroll-Kanals, über den u. a. die gesamte Verwaltung der Datenübertragung abgewickelt wird. Durch diese Konzentration der Basisaufgaben auf den Kontroll-Kanal können auch Geräte angebunden werden, die nur Übertragungen mit 20 MHz unterstützen. Der zweite Kanal fungiert als Erweiterungs-Kanal, der nur dann zum Zuge kommt, wenn die Gegenstelle auch 40 MHz-Übertragungen unterstützt. Die Nutzung des zweiten Kanals bleibt dabei optional, Sender und Empfänger können während der Übertragung dynamisch entscheiden, ob einer oder beide Kanäle verwendet werden sollen.



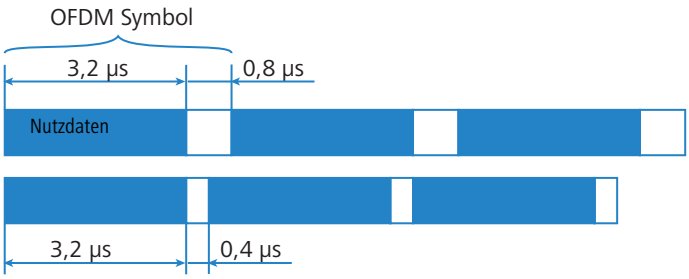
Da die 40 MHz-Implementation im 802.11n-Draft durch die Aufteilung in Kontroll- und Erweiterungskanal etwas effizienter geregelt ist als im bisherigen Turbo-Modus, können statt der doppelten Anzahl sogar noch ein paar zusätzliche Trägersignale gewonnen werden (in Summe 108). So steigt der maximale Datendurchsatz damit bei Nutzung der verbesserten OFDM-Modulation und zwei parallelen Datenströmen auf maximal 270 Mbit/s.

Short Guard Interval

Die letzte Verbesserung des 802.11n-Draft bezieht sich auf die Verbesserung der zeitlichen Abläufe in der Datenübertragung. Ein Signal zur Datenübertragung in einem WLAN-System wird nicht nur zu einem diskreten Zeitpunkt ausgestrahlt, sondern es wird für eine bestimmte Sendezeit konstant „in der Luft gehalten". Um Störungen auf der Empfangsseite zu verhindern, wird nach dem Ablauf der Sendezeit eine kleine Pause eingelegt, bevor die Übertra-

gung des nächsten Signals beginnt. Die gesamte Dauer aus Sendezeit und Pause wird in der WLAN-Terminologie als „Symbol" bezeichnet, die Pause selbst ist als „Guard Interval" bekannt.

Bei IEEE 802.11a/g wird ein Symbol mit einer Länge von 4 µs genutzt: Nach einer Übertragung von 3,2 µs und einer Pause von 0,8 µs wechselt die auf dem Trägersignal übertragene Information. 802.11n reduziert die Pause zwischen den Übertragungen auf das sogenannte „Short Guard Interval" von nur noch 0,4 µs.



Durch die Übertragung der Datenmenge in kürzeren Intervallen steigt der maximale Datendurchsatz damit bei Nutzung der verbesserten OFDM-Modulation, zwei parallelen Datenströmen und Übertragung mit 40 MHz auf maximal 300 Mbit/s.

Optimierung des Netto-Datendurchsatzes

Die bisher beschriebenen Verfahren haben zum Ziel, den physikalisch möglichen Datendurchsatz zu verbessern. Mit den im Folgenden beschriebenen Verfahren optimieren 802.11n-Netzwerke auch den Durchsatz, der netto zu erzielen ist – also den Durchsatz für die tatsächlichen Nutzdaten.

- **Frame-Aggregation**

Jedes Datenpaket enthält neben den eigentlichen Nutzdaten auch Verwaltungsinformationen, die für den reibungslosen Datenaustausch wichtig sind. Mit der Frame-Aggregation werden mehrere Datenpakete (Frames) zu einem größeren Paket zusammengefasst. Als Folge davon müssen die Verwaltungsinformationen nur einmal für das gesammelte Paket angegeben werden, der Anteil der Nutzdaten am gesamten Datenvolumen steigt.

- **Block Acknowledgement**

Jedes Datenpaket wird nach dem Empfang sofort bestätigt. Der Sender wird so informiert, dass das Paket richtig übertragen wurde und nicht wiederholt werden muss. Dieses Prinzip gilt auch für die aggregierten Frames bei 802.11n.

Aus einem solchen aggregierten Frame können aber unter Umständen einige Pakete erfolgreich zugestellt werden, andere jedoch nicht. Um nicht unnötig einen ganzen aggegierten Frame erneut zustellen zu müssen, aus dem vielleicht nur ein Paket **nicht** zugestellt wurde, wird für jedes einzelne WLAN-Paket aus einem aggregierten Frame eine separate Bestätigung erstellt. Diese Bestätigungen werden wieder zu einem Block zusammengefasst und gemeinsam an den Sender zurückgemeldet (Block Acknowledgement). Der Sender erhält eine Information über den Empfangsstatus von jedem einzelnen WLAN-Paket und kann so bei Bedarf auch gezielt nur die nicht erfolgreichen Pakete erneut übertragen.

Der MAC-Layer

- **Frame-Aggregation**

Die Verbesserungen im Physical Layer durch die neuen Technologien mit 802.11n beschreiben zunächst nur den theoretisch möglichen Datendurchsatz des physikalischen Mediums. Der tatsächlich für Nutzdaten verfügbare Teil dieser theoretischen Bandbreite wird jedoch durch zwei Aspekte geschmälert:

- Jedes Datenpaket im WLAN-System enthält neben den eigentlichen Nutzdaten weitere Informationen, z. B. die Präambel und die MAC-Adress-Information.
- Beim tatsächlichen Zugriff auf das Übertragungsmedium gehen durch die Verwaltungsvorgänge Zeit verloren. So muss der Sender vor der Übertragung eines jeden Datenpakets (Frame) mit den anderen vorhandenen Sendern die Zugriffsberechtigung aushandeln; durch Kollisionen von Datenpaketen und andere Vorgänge entstehen weitere Verzögerungen.

Dieser als „Overhead" bezeichnete Verlust kann reduziert werden, wenn mehrere Datenpakete zu einem größeren Frame zusammengefasst und gemeinsam übertragen werden. Dabei werden Informationen wie die Präambel nur einmal für alle zusammengefassten Datenpakete übertragen und Verzögerungen durch die Zugriffsregelung auf das Übertragungsmedium werden erst in größeren Abständen nötig.

Der Einsatz dieses als Frame-Aggregation bezeichneten Verfahrens unterliegt aber gewissen Einschränkungen:

- Damit auch Informationen wie die MAC-Adressen nur einmal für den aggregierten Frame übertragen werden müssen, können nur solche Datenpakete zusammengefasst werden, die an die gleiche Adresse gerichtet sind.

- Alle Datenpakete, die zu einem größeren Frame aggregiert werden sollen, müssen zum Zeitpunkt der Aggregation beim Sender anliegen – in der Folge müssen einige Datenpakete möglicherweise warten, bis ausreichend andere Pakete für das gleiche Ziel vorhanden sind, mit denen sie aggregiert werden können. Dieser Aspekt stellt für zeitkritische Übertragungen wie Voice over IP möglicherweise eine wichtige Einschränkung dar.
- **Block Acknowledgement**

Jedes Datenpaket, das an einen bestimmten Adressaten gerichtet ist (also keine Broadcast- oder Multicast-Pakete), wird nach dem Empfang sofort bestätigt. Der Sender wird so informiert, dass das Paket richtig übertragen wurde und nicht wiederholt werden muss. Dieses Prinzip gilt auch für die aggregierten Frames bei 802.11n.

Für die Frame-Aggregation werden zwei verschiedene Verfahren eingesetzt, die hier nicht näher erläutert werden, die sich allerdings bei der Bestätigung der aggregierten Frames unterscheiden:

- Bei der Mac Service Data Units Aggregation (MSDUA) werden mehrere Ethernet-Pakete zu einem gemeinsamen WLAN-Paket zusammengefasst. Dieses Paket wird nur einmal als Block bestätigt und gilt somit für alle aggregierten Pakete. Bleibt die Bestätigung aus, wird der gesamte Block erneut zugestellt.
- Bei der Mac Protocol Data Units Aggregation (MPDUA) werden einzelne WLAN-Pakete zu einem gemeinsamen, größeren WLAN-Paket zusammengefasst. Hier wird jedes einzelne WLAN-Paket bestätigt, die Bestätigungen werden wieder zusammengefasst und als Block übertragen. Der Sender erhält hier jedoch anders als bei MSDUA eine Information über den Empfangsstatus von jedem einzelnen WLAN-Paket und kann so bei Bedarf auch gezielt nur die nicht erfolgreichen Pakete erneut übertragen.

Resultierender Datendurchsatz

Der gesamte Datendurchsatz in einem 802.11n-Netzwerk wird von der Nutzung der vorher beschriebenen Techniken bestimmt. Eine eindeutige Kombination aus Modulationsverfahren, Nutzdatenrate und Anzahl der Spatial Streams wird als Modulation Coding Scheme (MCS) bezeichnet. Der Datendurchsatz hängt weiter davon ab, ob das kurze Guard-Intervall und die Kanalbündelung auf 40 MHz genutzt werden.

802.11n verwendet den Begriff „Datendurchsatz" anstelle von „Datenrate" bei älteren WLAN-Standards, weil die Datenrate keine ausreichende Beschreibung mehr ist. Die folgende Tabelle zeigt den maximalen Brutto-Datendurchsatz bei Nutzung von kurzem Guard-Intervall mit 40 MHz-Kanälen.

Der Netto-Datendurchsatz – also die Menge an tatsächlich übertragenen IP-Paketen – erreicht für einen 802.11n-Datenstrom bis zu 90 Mbit/s, bei zwei Spatial Streams entsprechend bis zu 180 Mbit/s. Der in der Praxis zu beobachtende Netto-Datendurchsatz liegt Stand Anfang 2008 meist im Bereich zwischen 80 und 130 Mbit/s, was am individuellen Reifegrad der Hardware- und Software-Optimierung sowie an der Chipsatz-Abstimmung zwischen verschiedenen Herstellern liegt.

Datenströme	Modulation	Nutzdatenrate	Datendurchsatz (GI=0,4 µs, 40 MHz)
1	BPSK	1/2	15
1	QPSK	1/2	30
1	QPSK	3/4	45
1	16QAM	1/2	60
1	16QAM	3/4	90
1	64QAM	1/2	120
1	64QAM	3/4	135
1	64QAM	5/6	150
2	BPSK	1/2	30
2	QPSK	1/2	60
2	QPSK	3/4	90
2	16QAM	1/2	120
2	16QAM	3/4	180
2	64QAM	1/2	240
2	64QAM	3/4	270
2	64QAM	5/6	300

11.3.2 IEEE 802.11a: 54 MBit/s

IEEE 802.11a sieht den Betrieb von Funk-LANs im 5 GHz Frequenzband (5,15 GHz bis 5,75 GHz) mit bis zu 54 MBit/s maximaler Übertragungsrate vor. Der tatsächliche Durchsatz ist allerdings abhängig von der Entfernung, beziehungsweise von der Qualität der Verbindung. Bei zunehmender Entfernung und abnehmender Verbindungsqualität sinkt die Übertragungsgeschwindigkeit auf 48 MBit/s, danach auf 36 MBit/s usw. bis auf minimal 6 MBit/s. Die Reichweite der Übertragung beträgt im Freien bis zu 125 m, in Gebäuden typischerweise bis zu 25 m. Der IEEE 802.11a Standard verwendet OFDM (**O**rthogonal **F**requency **D**ivision **M**ultiplexing) als Modulationsverfahren.

OFDM

Bei OFDM handelt es sich um ein Modulationsverfahren, das mehrere unabhängige Trägerfrequenzen für die Übertragung des Datensignals verwendet und diese Trägerfrequenzen mit einer verringerten Übertragungsrate moduliert. Das OFDM Modulationsverfahren ist dabei insbesondere sehr unempfindlich gegen Echos und andere Beeinträchtigungen und ermöglicht hohe Übertragungsraten.

Turbo-Modus

Im 'Turbo-Modus' können LANCOM Router Basis-Stationen zwei Funkkanäle gleichzeitig nutzen und damit die Übertragungsrate auf maximal 108 MBit/s steigern. Der Turbo-Modus kann in Verbindung mit dem IEEE 802.11a-Standard genutzt werden zwischen LANCOM Basis-Stationen und AirLancer Funknetzwerkkarten. Diese Steigerung der Übertragungsrate muss in der Basisstation entsprechend eingeschaltet werden und kann zu einer Reduzierung der Sendeleistung und damit der Reichweite der Funkverbindung führen.

11.3.3 IEEE 802.11h – ETSI 301 893

Im November 2002 wurde das 5 GHz-Band in Deutschland für die private Nutzung freigegeben und machte den Weg frei für deutlich schnellere WLAN-Verbindungen nach dem schon länger verfügbaren IEEE 802.11a-Standard. Der breitere Einsatz von 5 GHz-WLANs wurde dabei jedoch durch den ausschließlichen Einsatz in geschlossenen Räumen und die Übertragung mit relativ geringen Sendeleistungen beschränkt.

Mit der Erweiterung 802.11h wurde im September 2003 die private Nutzung des 5 GHz-Bandes schließlich auch außerhalb geschlossener Räume ermöglicht. Dabei wurden zum Schutz der militärischen Anwendungen im 5 GHz-Band die Verfahren DFS (Dynamic Frequency Selection) und TPC (Transmission Power Control) vorgeschrieben. Allerdings können bei Nutzung von DFS und TPC mit maximal 1000 mW deutliche höhere Sendeleistungen als in allen anderen bis dahin gültigen Standards erzielen.

ETSI-Standards

Die ETSI verabschiedete schon 1996 den ersten Standard zur Regelung von Datenfernübertragungen unter dem Namen Hiperlan (High Performance Radio Local Area Networks). Die erste Fassung (Hiperlan Typ1) war für den Einsatz im Frequenzbereich von 5,15 bis 5,30 GHz mit einer Übertragungsrate von 20 MBit/s vorgesehen. Da sich in der Industrie keine Hersteller für Produkte nach diesem Standard fanden, blieb Hiperlan zunächst ohne praktische Bedeutung.

Mit der im Jahre 2000 vorgestellten neuen Fassung des Hiperlan Typ 2 stellt die ETSI eine WLAN-Lösung vor, die wie IEEE 802.11a im 5 GHz-Band arbeitet und eine Bruttodatenrate von ebenfalls 54 MBit/s anbietet. Die Überlagerung der verwendeten Frequenzen und das ebenfalls wie bei 802.11a verwendete OFDM-Modulationsverfahren machen jedoch eine Anpassung der Standards zwischen IEEE und ETSI notwendig, um Störungen der Systeme untereinander zu vermeiden.

Europäische Harmonisierung

Um die Nutzung des 5GHz-Bandes in Europa zu vereinheitlichen, hat die Europäische Kommission am 11.07.2005 den Standard ETSI 301 893 erlassen. Die Mitgliedsländer der EU sind verpflichtet, diese bis zum 31.10.2005 umzusetzen.

Anstelle der in den 802.11a/h-Standards beschriebenen drei Unterbändern (5150 - 5350 MHz, 5470 - 5725 MHz und 5725 - 5875 MHz für UK) regelt die Norm ETSI 301 893 die drei folgenden Bereiche mit unterschiedlichen Vorschriften:

- 5150 - 5250 MHz
- 5250 - 5350 MHz
- 5470 - 5725 MHz

Der Kern der Richtlinie sind Vorkehrungen zur Vermeidung von Störungen mit anderen Systemen, die das gleiche Frequenzband verwenden. Hierunter fallen z.B. Radaranlagen, die als „Primäranwendungen" gelten. Die „Sekundäranwendungen" wie WLAN müssen die Frequenz wechseln, sobald ein Konflikt festgestellt wird.

- Dynamic Frequency Selection – DFS

  Zur Priorisierung der Primäranwendungen wird das Verfahren der dynamischen Frequenzwahl (DFS) vorgeschrieben. DFS geht zunächst davon aus, dass kein Kanal im entsprechenden Frequenzband verfügbar ist. Das WLAN-Gerät wählt beim Start zufällig einen Kanal aus und führt einen sogenannten Channel availability Check (CAC)

durch. Dabei wird **vor** dem Senden auf einem Kanal für 60 Sekunden (Channel Observation Time, COT) geprüft, ob ein anderes Gerät auf diesem Kanal bereits arbeitet und der Kanal somit belegt ist. Ist das der Fall, so wird ein weiterer Kanal mit CAC geprüft. Andernfalls kann das WLAN-Gerät den Sendebetrieb aufnehmen.

Auch während des Betriebes wird überprüft, ob eine Primäranwendung wie z.B. ein Radargerät diesen Kanal benutzt. Dabei wird ausgenutzt, dass Radare häufig nach dem Rotationsverfahren arbeiten, bei dem ein eng gebündelter Richtfunkstrahl durch eine rotierende Antenne ausgestrahlt wird. Durch die Rotation der Antenne nimmt ein entfernter Empfänger das Radar-Signal als einen kurzen Impuls (Radar-Peak) wahr. Empfängt ein Gerät einen solchen Radar-Peak, so stellt es zunächst den Sendebetrieb ein und überwacht den Kanal auf weitere Impulse. Treten während der COT weitere Radar Peaks auf, wird automatisch ein neuer Kanal gewählt.

Vorgeschrieben ist, dass eine solche Überprüfung alle 24 Stunden stattfinden muss. Daher ist eine Unterbrechung der Datenübertragung für 60 Sekunden unvermeidlich.

DFS ist für die Frequenzbereiche von 5250 - 5350 MHz und von 5470 - 5725 MHz fest vorgeschrieben. Für den Frequenzbereich von 5150 - 5250 MHz ist es optional einsetzbar.

- Transmission Power Control – TPC

  Für eine Verminderung der funktechnischen Störungen soll eine dynamische Anpassung der Sendeleistung sorgen.

  Die dynamische Anpassung der Sendeleistung erleichtert die gemeinsame Nutzung der Frequenzbänder 5250-5350 MHz und 5470 - 5725 MHz mit Sattelitendiensten. TPC soll eine durchschnittliche Abschwächung der Sendeleistung gegenüber der max. zulässigen Sendeleistung von mindestens drei dB bewirken. Dazu ermittelt TPC die minimal notwendige Sendeleistung, um die Verbindung zum Partner (z.B. einem Access Point) aufrecht zu erhalten. Verzichtet man innerhalb dieser Frequenzbänder auf TPC, so verringert sich die höchstzulässige mittlere EIRP und die entsprechende maximale geforderter TPC-Regelbereich um 3 dB. Im Frequenzbereich von 5150-5250 MHz gilt diese Einschränkung nicht.

  Im Betrieb ohne DFS und TPC sind nur maximal 30 mW EIRP erlaubt. Unter Verwendung von DFS und TPC sind maximal 200 mW (bei 5150 bis 5350 MHz) bzw. 1000 mW EIRP bei (5470 bis 5725 MHz) als Sendeleistung erlaubt (zum Vergleich: 100 mW bei 802.11 b/g, 2,4 GHz, DFS und TPC sind hier nicht nötig). Die höhere maximale Sendeleistung gleicht nicht nur die höhere Dämpfung der Luft für die 5 GHz-Funkwellen aus, sondern ermöglicht sogar deutlich größere Reichweiten als im 2,4 GHz-Bereich möglich sind.

Unterschiede zu USA und Asien

In den USA und in Asien werden vom europäischen Standard abweichende Frequenzbänder und maximale Signalstärken verwendet.

In den USA werden für Funknetze im 5 GHz-Band drei je 100 MHz breite Unterbänder verwendet. Das „Lower Band" reicht von 5150 - 5250 MHz, das „Middle Band" von 5250 - 5350 MHz und das „Upper Band" von 5725 - 5825 MHz. Im Lower Band ist eine maximale mittlere EIRP von 50 mW, im Middle Band von 250 mW sowie im Upper Band von 1 W zugelassen.

In Japan ist die Nutzung des 5 GHz-Bandes bisher nur sehr eingeschränkt möglich: hier ist nur das untere Band von 5150 - 5250 MHz für die private Nutzung freigegeben.

Nutzbare Kanäle im 5 GHz-Band

Im nutzbaren Frequenzraum von 5,13 bis 5,875 GHz stehen die folgenden Kanäle in Europa zur Verfügung, unterteilt in Frequenzbereiche, für die unterschiedliche Nutzungsbedingungen gelten können:

- 5150 - 5250 MHz (Kanäle 36, 40, 44 und 48)
- 5250 - 5350 MHz (Kanäle 52, 56, 60 und 64)
- 5470 - 5725 MHz (Kanäle 100, 104, 108, 112, 116, 132, 136 und 140)
- 5755 - 5875 MHz
  - Kanäle 151, 155, 159, 163, 167: In Deutschland nur mit DFS und nur für kommerzielle Nutzung freigegeben (BFWA).
  - Kanäle 149, 153, 157, 161, 165: Für den FCC-Betrieb in den USA ohne DFS freigegeben.

In der folgenden Übersicht sehen Sie, welche Kanäle in den verschiedenen Regionen verwendet werden dürfen:



* Hinweis: Bitte beachten Sie, dass die Frequenzbereiche und Funkkanäle aus Band 3 je nach Land bestimmten Restriktionen unterworfen sind (z.B. in Deutschland nur für öffentliche „Broadband Fixed Wireless Access" Kommunikationsdienstleister zugelassen).

Frequenzbereiche für Indoor-/Outdoor-Verwendung im 5 GHz-Band

Der Einsatz der in ETSI 301 893 beschriebenen Verfahren zur Reduzierung der gegenseitigen Störungen im 5 GHz-Band TPC und DFS ist nicht für alle Einsatzbereiche vorgeschrieben. Die folgende Tabelle gibt Aufschluss über die zulässige Verwendung und die zugehörigen Sendeleistungen innerhalb der EU:

Frequenz (GHz)	Sendeleistung (mW/dBm)	Verwendung	DFS	TPC
5,15-5,25	200/23	Indoor		
5,15-5,35	200/23	Indoor	✔	✔
5,470-5,725	1000/30	Indoor/Outdoor	✔	✔
5,755-5,875	4000/36	Outdoor (BFWA)	✔	✔

Beim Einsatz in anderen Ländern können ggf. andere Vorschriften gelten. Bitte informieren Sie sich über die aktuellen Funkregelungen des Landes, in dem Sie ein Funk-LAN-Gerät in Betrieb nehmen wollen, und stellen Sie in den WLAN-Einstellungen unbedingt das Land ein, in dem Sie das Gerät betreiben.

11.3.4 IEEE 802.11g: 54 MBit/s

Der IEEE 802.11g Standard arbeitet ebenfalls mit bis zu 54 MBit/s Übertragungsrate im 2,4 GHz ISM-Frequenzband. Im Gegensatz zu IEEE 802.11b wird jedoch bei IEEE 802.11g die OFDM Modulation verwendet wie schon bei IEEE 802.11a. IEEE 802.11g enthält einen besonderen Kompatibilitätsmodus der eine Abwärtskompatibilität zu dem weit verbreiteten IEEE 802.11b Standard gewährleistet. Wird dieser Kompatibilitätsmodus verwendet, so ist jedoch mit Geschwindigkeitseinbussen bei der Datenübertragung zu rechnen. IEEE 802.11g ist wegen der unterschiedlichen Frequenzbänder nicht kompatibel zu IEEE 802.11a. Die Reichweiten von IEEE 802.11g Produkten sind vergleichbar mit denen von IEEE 802.11b Produkten.

Turbo-Modus

Auch im 802.11g-Standard kann mit dem 'Turbo-Modus' durch die parallele Nutzung von zwei Funkkanälen die Übertragungsrate auf maximal 108 MBit/s gesteigert werden. Da im 2,4 GHz-Band jedoch weniger Kanäle als im 5 GHz-Band genutzt werden können, schränkt die Verwendung des Turbo-Modus hier die Kanalwahl deutlich ein.

11.3.5 IEEE 802.11b: 11 MBit/s

IEEE 802.11b sieht den Betrieb von lokalen Funk-LANs im ISM-Frequenzband vor (**I**ndustrial, **S**cientific, **M**edical: 2.4 bis 2.483 GHz). Die maximale Bandbreite der Datenübertragung beträgt bis zu 11 MBit/s. Der tatsächliche Durchsatz ist allerdings abhängig von der Entfernung, beziehungsweise von der Qualität der Verbindung. Bei zunehmender Entfernung und abnehmender Verbindungsqualität sinkt die Übertragungsgeschwindigkeit auf 5,5 MBit/s, danach auf 2 und schließlich auf 1 MBit/s. Die Reichweite der Übertragung beträgt im Freien bis zu 150 m, in Gebäuden typischerweise bis zu 30 m. IEEE 802.11b ist wegen der unterschiedlichen Frequenzbänder nicht kompatibel zu IEEE 802.11a.

DSSS

Zur Abschirmung gegen Störungen durch andere Sender, die gegebenenfalls das gleiche Frequenzband verwenden, wird im 2,4 GHz Frequenzband für IEEE 802.11b das DSSS-Verfahren verwendet (**D**irect **S**equence **S**pread **S**pectrum). Normalerweise benutzt ein Sender nur einen sehr schmalen Bereich des verfügbaren Frequenzbandes zur Übertragung. Wird genau dieser Bereich auch von einem weiteren Sender verwendet, kommt es zu Störungen in der Übertragung. Beim DSSS-Verfahren nutzt der Sender einen breiteren Teil des möglichen Frequenzbandes und wird so unempfindlicher gegen schmalbandige Störungen.

11.4 WLAN-Sicherheit

11.4.1 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.

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 Access Point verbindet, und nicht mit einem von unbefugten Dritten eingeschmuggelten Access Point mit dem gleichen Netzwerk-Namen. So eine Authentifizierung kann z.B. durch Zertifikate oder Passwörter gewährleistet werden.

Authentizität

Authentizität: Nachweis der Urheberschaft von Daten und der Echtheit des Datenmaterials; die Durchführung eines solchen Nachweises bezeichnet man als Authentifizierung

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.

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. DES, AES, RC4 oder Blowfish. 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 Pre-Shared-Keys 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.

11.4.2 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 stellt den derzeit höchsten sicherheitsstandard für WLANs dar, da es zum einem die Authentifizierung und Autorisierung der Benutzer über IEEE 802.1X erlaubt und 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.

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 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. Abbildung 2 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.

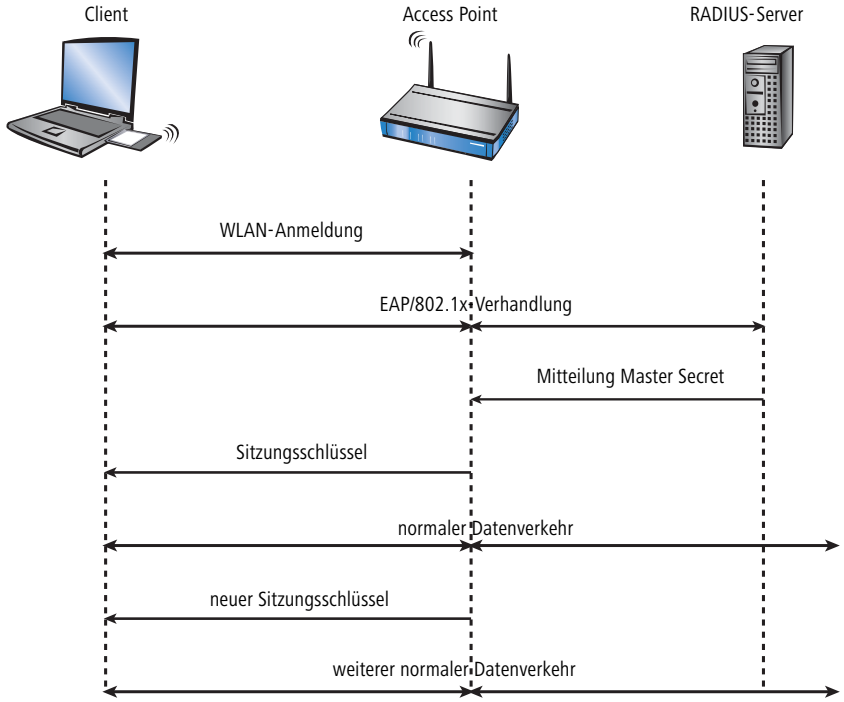


Abbildung 2: Schematischer Ablauf einer WLAN-Sitzung mit EAP/802.1x

In der ersten Phase meldet sich der Client wie gewohnt beim Access Point an und erreicht einen Zustand, in dem er bei früher verwendeten WEP jetzt über den Access Point 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 Access Points 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 Access Point packt diese Pakete in RADIUS-Anfragen um und reicht sie an den Authentifizierungs-Server weiter. Umgekehrt wandelt der Access Point darauf vom RADIUS-Server kommende Antworten wieder in EAP-Pakete um und reicht sie an den Client weiter.

Der Access Point 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 Access Point 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" Access Points lassen sich so erkennen.

Es gibt eine ganze Reihe von Authentifizierungsverfahren, die in diesem Tunnel angewendet werden können. Ein gängiges (und seit Windows XP unterstütztes) 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 Access Point eingebunden wird. Dazu schickt der RADIUS-Server das sogenannte 'Master Secret', einen während der Verhandlung berechneten Sitzungsschlüssel, zum Access Point. Das LAN hinter dem Access Point wird in diesem Szenario als sicher betrachtet, von daher kann diese Übertragung im Klartext erfolgen.

Mit diesem Sitzungsschlüssel übernimmt der Access Point 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 Access Point und genau diesem Client benutzt wird. Ältere WEP-Hardware verwendet meistens nur Gruppenschlüssel, den der Access Point für die Kommunikation mit mehreren Clients benutzt.

Der besondere Vorteil dieses Verfahrens ist es, dass der Access Point über den EAP-Tunnel die Schlüssel regelmäßig wechsel 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.

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.

TKIP

TKIP steht für **T**emporal **K**ey **I**ntegrity **P**rotocol. Wie der Name nahelegt, handelt es sich dabei 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.

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.

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.

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 Access Points 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 Access Point deutlich länger dauern.

Als erste Maßnahme wurde deshalb das sogenannte PMK-Caching eingeführt. Das PMK dient nach einer 802.1x-Authentifizierung zwischen Client und Access Point als Basis für die Schlüsselverhandlung. In VoIP-Umgebungen ist es denkbar, dass ein Anwender sich zwischen einer relativ kleinen Zahl von Access Points hin- und herbewegt. Dabei wird es vorkommen, dass ein Client wieder zu einem Access Point 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 Access Point 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 Access Point erkennen und einen neuen Access Point selektieren, während er noch Verbindung zum alten Access Point hat.

In diesem Fall hat er die Möglichkeit, die 802.1x-Verhandlung über den alten Access Point mit dem neuen Access Point zu führen, was wiederum die 'Totzeit' um die Zeit der 802.1x-Verhandlung verkürzt.

11.4.3 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 WiFi-Alliance der 'Standard' Wifi Protected Access (WPA) definiert. WPA setzt auf die folgenden Änderungen:

- TKIP und Michael als Ersatz für WEP
- Ein standardisiertes Handshake-Verfahren zwischen Client und Access Point 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 Access Point 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 allzuviele 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 Access Point brechen dann für eine Minute den Datentransfer ab und handeln danach TKIP- und Michael-Schlüssel neu aus.

Verhandlung des Verschlüsselungsverfahrens

Da die ursprüngliche WEP-Definition feste Schlüssellänge von 40 Bit vorschrieb, musste bei der Anmeldung eines Clients an einem Access Point 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 Access Point über das zu verwendende Verschlüsselungs- und Authentifizierungsverfahren verständigen können. Dabei werden folgenden Informationen bereitgestellt:

- Eine Liste von Verschlüsselungsverfahren, die der Access Point 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 im Moment 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 Access Point kommunizieren, andere Clients jedoch über AES.

11.4.4 WEP

WEP ist eine Abkürzung für **W**ired **E**quivalent **P**rivacy. 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 Access Points weiterhin dieses Verschlüsselungsverfahren. LANCOM Systems empfiehlt jedoch ausdrücklich, nach Möglichkeit eine bessere Absicherung der WLANs (z. B. nach IEEE 802.1x/WPA2) zu verwenden.

11.4.5 LEPS – LANCOM Enhanced Passphrase Security

LEPS behebt die Unsicherheit von globalen Passphrases

Mit den modernen Verschlüsselungsverfahren WPA und IEEE 802.11i kann der Datenverkehr im WLAN deutlich besser als mit WEP gegen unerwünschte „Lauschangriffe" geschützt werden. Die Verwendung einer Passphrase als zentraler Schlüssel ist sehr einfach zu handhaben, ein RADIUS-Server wie in 802.1x-Installationen wird nicht benötigt.

Dennoch birgt die Verwendung der abhörsicheren Verfahren WPA und IEEE 802.11i 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 (**L**ANCOM **E**nhanced **P**assphrase **S**ecurity) hat LANCOM Systems ein effizientes Verfahren entwickelt, das die einfache Konfigurierbarkeit von IEEE 802.11i mit Passphrase nutzt und dabei die möglichen Unsicherheiten bei der Nutzung einer globalen Passphrase vermeidet.

Bei LEPS 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 und die anschließende Verschlüsselung per IEEE 802.11i oder WPA.

Da Passphrase und MAC-Adresse verknüpft sind, ist auch das Spoofing der MAC-Adressen wirkungslos – LEPS schließt damit auch einen möglichen Angriffspunkt gegen die ACL aus. Wenn als Verschlüsselungsart WPA oder 802.11i 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 kann sowohl lokal im Gerät genutzt werden als auch mit Hilfe eines RADIUS-Servers zentral verwaltet werden. LEPS funktioniert mit sämtlichen am Markt befindlichen WLAN-Client-Adaptern, ohne dass dort eine Änderung stattfinden muss. Da LEPS ausschließlich im Access Point konfiguriert wird, ist jederzeit die volle Kompatibilität zu Fremdprodukten gegeben.



Ein weiterer Sicherheitsaspekt: Mit LEPS können auch einzelne Point-to-Point-Strecken (P2P) mit einer individuellen Passphrase abgesichert werden. Wenn bei einer P2P-Installation ein Access Point entwendet wird und dadurch Passphrase und MAC-Adresse bekannt werden, sind alle anderen per LEPS abgesicherten WLAN-Strecken weiterhin sicher, insbesondere wenn die ACL auf einem RADIUS-Server abgelegt ist.

Konfiguration

Bei der Konfiguration von LEPS wird lediglich jeder MAC-Adresse eines im WLAN zugelassenen Clients eine eigene Passphrase zugeordnet. Dazu wird der MAC-Filter positiv eingestellt, d.h. die Daten von den hier eingetragenen WLAN-Clients werden übertragen.



Verwenden Sie als Passphrase zufällige Zeichenketten von mindestens 32 Zeichen Länge.

11.4.6 Standard-WEP-Verschlüsselung

Ab Werk ist für jeden unkonfigurierten LANCOM Wireless Router standardmäßig eine WEP128-Verschlüsselung aktiviert. Diese Verschlüsselung dient nur der Erst-Konfiguration von über das WLAN.

LANCOM Access Points sind im Auslieferungszustand auf den „Managed Modus" eingestellt, die WLAN-Module sind dabei ausgeschaltet. Eine Erst-Konfiguration von LANCOM Access Points ist über WLAN daher nicht möglich. Für WLAN-Interfaces, die von einem LANCOM WLAN Controller verwaltet werden, wird die WEP-Verschlüsselung durch die zentralen Verschlüsselungseinstellungen in den Profilen des WLAN Controllers überschrieben.

Der Schlüssel der Standard-WEP-Verschlüsselung setzt sich aus dem Anfangsbuchstaben „L" gefolgt von der LAN-MAC-Adresse des Access Points in ASCII-Schreibsweise zusammen. Die LAN-MAC-Adressen der LANCOM-Geräte beginnen immer mit der Zeichenfolge „00A057". Sie finden die LAN-MAC-Adresse auf einem Aufkleber auf der

Unterseite des Gerätes. Verwenden Sie **nur** die als „MAC-Address“ gekennzeichnete Nummer, die mit „00A057“ beginnt. Bei den anderen ggf. angegebenen Nummern handelt es sich **nicht** um die LAN-MAC-Adresse!



Für ein Gerät mit der LAN-MAC-Adresse „00A0570FB9BF“ lautet der Standard-WEP-Schlüssel also „L00A0570FB9BF“. Dieser Schlüssel wird in den 'Einzel-WEP-Einstellungen' des Gerätes für jedes logische WLAN-Netzwerk als 'Schlüssel 1' eingetragen.

Um mit einem WLAN-Adapter eine Verbindung zu einem neuen LANCOM Access Point herzustellen, muss in dem WLAN-Adapter die WEP128-Verschlüsselung aktiviert und der 13-stellige Standard-WEP-Schlüssel eingetragen werden.

Ändern Sie die WLAN-Verschlüsselung nach der ersten Anmeldung auf WPA2/802.11i, um eine sichere Verbindung zu gewährleisten.

Beachten Sie, dass bei einem Reset auch die im Gerät definierten WLAN-Verschlüsselungseinstellungen verloren gehen und auf diesen Standard-WEP-Schlüssel zurückgesetzt werden. Der WLAN-Zugang gelingt nach dem Reset nur, wenn der Standard-WEP-Schlüssel im WLAN-Client eingetragen ist!

11.4.7 Background WLAN Scanning

Zur Erkennung anderer Access Points in der eigenen Funkreichweite können LANCOM Wireless Router aktiv alle verfügbaren Kanälen prüfen (so wie das ein WLAN-Client machen würde, der nach verfügbaren Access Points sucht). Wenn dort ein anderer Access Point aktiv ist, werden die entsprechenden Informationen in der Scan-Tabelle gespeichert. Da diese Aufzeichnung im Hintergrund neben der „normalen“ Funktätigkeit der Access Points 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

Rogue AP Detection

Als Rogue bezeichnet man solche WLAN-Geräte, die unerlaubt versuchen, als Access Point oder Client Teilnehmer in einem WLAN zu werden. Rogue APs sind solche 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 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 Access Points 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.

Schnelles Roaming im Client-Modus

Das Verfahren des Background-Scanning kann aber auch mit anderen Zielen als der Rogue AP Detection verwendet werden. Ein LANCOM Access Point im Client-Modus, der sich selbst bei einem anderen Access Point anmeldet, kann in einer mobilen Installation auch das Roaming-Verfahren nutzen. Dies ist z.B. dann der Fall, wenn der LANCOM Access Point in einer Industrieanwendung auf einem Gabelstapler befestigt ist, der sich durch mehrere Hallen mit separaten Access Points bewegt. Normalerweise würde der WLAN-Client sich nur dann bei einem anderen Access Point einbuchen, wenn er die Verbindung zu dem bisherigen Access Point vollständig verloren hat. Mit der Funktion des Background-Scanning kann der LANCOM Access Point im Client-Modus schon vorher Informationen über andere verfügbare Access Points sammeln. Die Umschaltung auf einen anderen Access Point erfolgt dann nicht erst, wenn die bisherige Verbindung vollständig verloren wurde, sondern wenn ein anderer Access Point in Reichweite über ein stärkeres Signal verfügt.

Auswertung des Background-Scans

Die Informationen über die gefundenen Access Points können in der Statistik des LANCOM Access Point eingesehen werden. Sehr komfortabel stellt der WLANmonitor die Scan-Ergebnisse dar und bietet darüber hinaus zusätzliche Funktionen wie das Gruppieren der Access Points oder die automatische Benachrichtigung per E-Mail beim Auftauchen neuer WLAN-Geräte.



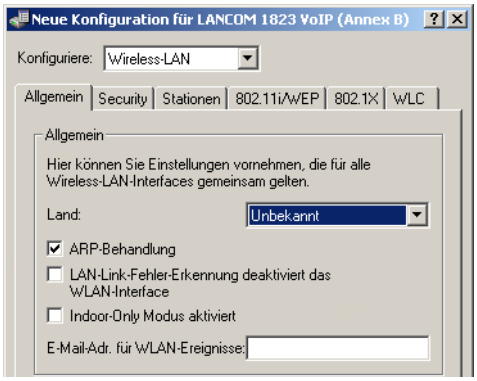
Weitere Informationen finden Sie unter 'Rogue AP und Rogue Client Detection mit dem WLANmonitor' → Seite 4-39.

11.5 Konfiguration der WLAN-Parameter

Die Einstellungen für die Funknetzwerke können an verschiedenen Stellen in der Konfiguration vorgenommen werden:

- Manche Parameter betreffen die physikalische WLAN-Schnittstellen. Einige LANCOM-Modelle verfügen über eine WLAN-Schnittstelle (Single Radio Access Point), andere Modelle haben ein zweites WLAN-Modul integriert (Dual Radio Access Point). 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 (Access Point 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.

11.5.1 Allgemeine WLAN-Einstellungen



LANconfig: Wireless-LAN ▶ Allgemein

WEBconfig: LCOS-Menübaum ▶ Setup ▶ WLAN

- **Ländereinstellung**

  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 LANCOM Access Points auf die in dem jeweiligen Land zulässigen Parameter zu begrenzen, wird für alle physikalischen WLAN-Interfaces gemeinsam das Land eingestellt, in dem der Access Point 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 Access Point diese Aufgabe und beantwortet die ARP Anfragen an Stelle der Stationen im Stromsparmodus.

- **Link-Fehler-Erkennung**

  Die 'Link-Fehler-Erkennung' schaltet das WLAN-Modul ab, wenn der Access Point keine Verbindung zum LAN mehr hat.

- **Indoor-Funktion für WLAN-Kanäle**

  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 LANCOM Wireless Router 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 LANCOM Wireless Router 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 Access Point betrieben wird.

Die Aktivierung der Indoor-Only-Funktion ist nur erlaubt, wenn sich der Access Point sowie alle verbundenen Clients in einem geschlossenen Raum befinden.

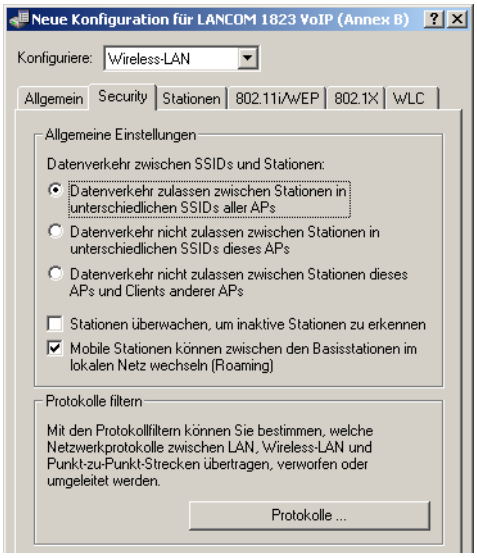
■ **Mail-Adresse**

An diese E-Mail-Adresse werden Informationen über die Ereignisse im WLAN versendet.

11.5.2 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. Außerdem werden hier die Schlüssel für die jeweilige Verschlüsselung im WLAN eingestellt.

Allgemeine Einstellungen



LANconfig: Wireless-LAN ▶ Security

■ **Datenverkehr zwischen SSIDs und Stationen**

Je nach Anwendungsfall ist es gewünscht oder eben auch nicht erwünscht, dass die an einem Access Point 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 allem 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 Access Point 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.

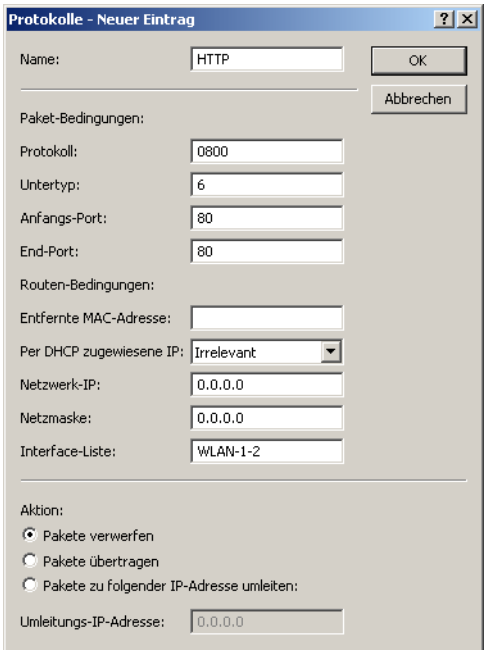
■ **Mobile Stationen können zwischen den Basisstationen im lokalen Netz wechseln (Roaming)**

Neben der Kommunikation der Clients untereinander kann hier auch eingestellt werden, ob die benachbarten Access Points beim Roaming Informationen über das IAPP austauschen. Das Inter Access Point Protocol (IAPP) ist ein Protokoll zur Kommunikation zwischen Access Points. Der “abgebende Access Point” bekommt so die

Nachricht, dass ein bei ihm eingebuchter WLAN-Client nun zu einem anderen Access Point wechselt und kann den Client sofort aus seiner Liste entfernen.

Protokoll-Filter

Mit dem Protokoll-Filter können Sie die Behandlung von bestimmten Datenpaketen bei der Übertragung 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: Wireless LAN ▶ Security ▶ Protokolle

WEBconfig: LCOS-Menübaum ▶ 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** und **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.
- **DHCP-Source-MAC**: Aktivierung des DHCP-Adress-Tracking.
  - **Ja**: Die Regel trifft zu, wenn die Quell-MAC-Adresse des Pakets in der Tabelle unter `Status > LAN-Bridge-Statistiken > DHCP-Tabelle` 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. Weitere Informationen finden Sie unter 'DHCP-Adress-Tracking' → Seite 55.

- **IP-Netzwerk** und **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.

- **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, für die Datenpakete ausgeführt wird, die mit dieser Regel erfasst werden:
- **Umleite-IP-Adresse**: Ziel-IP-Adresse für die Aktion 'Umleiten'

  Bei einem Redirect wird die Ziel-IP-Adresse der Pakete durch die hier eingetragene Umleite-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	Umleite-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.

Ablauf der Filterprüfung

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 Pakete die zur Prüfung benötigten Informationen ausgelesen:

- □ DHCP-Source-MAC
- □ Ziel-MAC-Adresse des Paketes
- □ Protokoll, z.B. IPv4, IPX, 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.

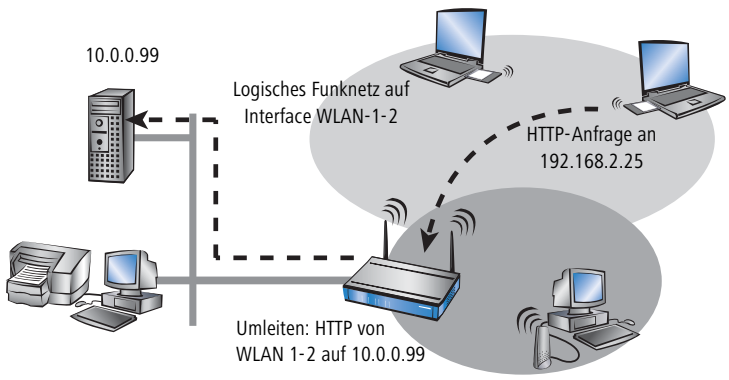
Redirect-Funktion

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 Umleite-IP-Adresse ersetzt, die Ziel-MAC-Adresse des Pakets wird durch die per ARP ermittelte, zur Umleite-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 Access Point, sondern wechseln den Access Point 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.

DHCP-Adress-Tracking

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.

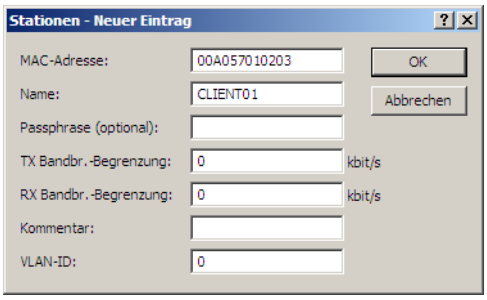
11.5.3 Auswahl der im WLAN zulässigen Stationen

Access Control List

Mit der **A**ccess **C**ontrol **L**ist (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-LAN-Adapter.

Bei der zentralen Verwaltung der LANCOM Wireless Router und LANCOM Access Point über einen LANCOM WLAN Controller finden Sie die Stationstabelle im Konfigurationsbereich 'WLAN-Controller' auf der Registerkarte 'Stationen' unter der Schaltfläche **Stationen**.

Kontrollieren Sie, ob die Einstellung 'Daten von den aufgeführten Stationen übertragen, alle anderen Stationen ausfiltern' aktiviert ist. Fügen Sie neue Stationen die an Ihren Funk-Netzwerk teilnehmen sollen ggf. über den Schalter 'Stationen' hinzu.



LANconfig: Wireless LAN ▶ Stationen ▶ Stationen

WEBconfig: LCOS-Menübaum ▶ Setup ▶ WLAN ▶ Zugangs-Liste

- **MAC-Adresse**
  MAC-Adresse des WLAN-Clients, für den dieser Eintrag gilt.
- **Name**
  Name für den WLAN-Client für eine leichtere Zuordnung, z.B. zu den Mitarbeitern.
- **Passphrase**
  Passphrase für den WLAN-Client in Netzwerken mit 802.11i/WPA/AES-PSK.

- **TX Bandbreitenbegrenzung**
  Erlaubte Bandbreite für den WLAN-Client. Siehe auch 'Bandbreitenbegrenzung im WLAN' → Seite 11-85
- **RX Bandbreitenbegrenzung**
  Erlaubte Bandbreite für den WLAN-Client. Siehe auch 'Bandbreitenbegrenzung im WLAN' → Seite 11-85
- **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).

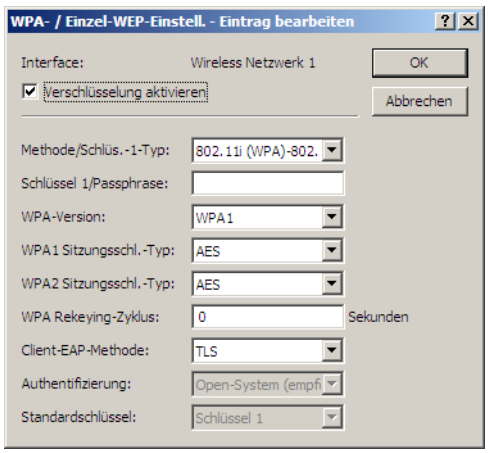
11.5.4 Verschlüsselungs-Einstellungen

Die Access Points 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 (wie den 54-MBit-AirLancer-Clients und den 54-MBit-LANCOM-Access-Points) 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 aktuellen 802.11i/WPA-Methoden eingesetzt werden sollten.

Weitere Informationen zum 802.11i- und WPA-Standard finden Sie unter 'Entwicklung der WLAN-Sicherheit' → Seite 12.

WPA- und Einzel-WEP-Einstellungen



LANconfig: Wireless LAN ▶ 802.11i/WEP ▶ WPA- / Einzel-WEP-Einstellungen

WEBconfig: LCOS-Menübaum ▶ Setup ▶ Schnittstellen ▶ WLAN ▶ Verschluesselung

- **Methode/Schlüssel-1-Typ**
  Stellen Sie hier das zu verwendende Verschlüsselungsverfahren ein.
  - □ 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 die Option '802.11i (WPA)-802.1x'. 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 ist nur zu empfehlen, wenn die verwendete Hardware der WLAN-Clients die modernen Verfahren nicht unterstützt.

- □ 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.

■ **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 'Regeln für die Eingabe von WEP-Schlüsseln' → Seite 11-34.

■ **WPA-Version**

WPA-Version die der Access Point den WLAN-Clients zur Verschlüsselung anbietet.

- □ WPA1: Nur WPA1
- □ WPA2: Nur WPA1
- □ WPA1/2: Sowohl WPA1 als auch WPA2 in einer SSID (Funkzelle)

■ **WPA 1 Sitzungs-Schlüssel-Typ**

Wenn als Verschlüsselungsmethode '802.11i (WPA)-PSK' eingestellt wurde, kann hier das Verfahren zur Generierung des Sitzungs- bzw. Gruppenschlüssels für WPA 1ausgewählt 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.

■ **WPA 2 Sitzungs-Schlüssel-Typ**

Verfahren zur Generierung des Sitzungs- bzw. Gruppenschlüssels für WPA 2.

■ **WPA Rekeying-Zyklus**

Ein 48 Bit langer Initialization Vector (IV) erschwert die Berechnung des WPA-Schlüssels für Angreifer. Die Wiederholung des aus IV und WPA-Schlüssel bestehenden echten Schlüssels würde erst nach 16 Millionen Paketen erfolgen. In stark genutzten WLANs also erst nach einigen Stunden. Um die Wiederholung des echten Schlüssels zu verhindern, sieht WPA eine automatische Neuaushandlung des Schlüssels in regelmäßigen Abständen vor. Damit wird der Wiederholung des echten Schlüssels vorgegriffen.

Geben Sie hier einen Wert in Sekunden an, nachdem der Schlüssel neu ausgehandelt wird.

In der Standardeinstellung ist der Wert auf '0' eingestellt, so dass keine vorzeitige Aushandlung des Schlüssels erfolgt.

■ **Client-EAP-Methode**

LANCOM Access Points in der Betriebsart als WLAN-Client können sich über EAP/802.1X bei einem anderen Access Point 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 LANCOM Access Point 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.

■ **Authentifizierung**

Wenn als Verschlüsselungsmethode eine WEP-Verschlüsselung eingestellt wurde, stehen zwei verschiedene Verfahren für die Authentifizierung der WLAN-Clients zur Verfügung:

- □ Beim 'OpenSystem'-Verfahren wird komplett auf eine Authentifizierung verzichtet. Die Datenpakete müssen von Beginn an richtig verschlüsselt übertragen werden, um von der Basisstation akzeptiert zu werden.
- □ Beim 'SharedKey'-Verfahren wird das erste Datenpakte unverschlüsselt übertragen und muss vom Client richtig verschlüsselt zurückgesendet werden. Bei diesem Verfahren steht einem potenziellen Angreifer mindestens ein Datenpaket unverschlüsselt zur Verfügung.

■ **Standardschlüssel**

Wenn als Verschlüsselungsmethode eine WEP-Verschlüsselung eingestellt wurde, kann der Access Point für jedes logische WLAN-Interface aus vier verschiedenen WEP-Schlüsseln wählen:

- □ Drei WEP-Schlüssel für das physikalische Interface
- □ Ein zusätzlicher WEP-Schlüssel speziell für jedes logische WLAN-Interface

Bei den Einzel-WEP-Einstellungen wird der zusätzliche Schlüssel für jedes logische WLAN-Interface eingestellt (siehe 'Schlüssel-1/Passphrase'). Wählen Sie außerdem aus, welcher der vier eingestellten Schlüssel aktuell für die Verschlüsselung der Daten verwendet werden soll (Standardschlüssel). Mit dieser Einstellung können Sie den Schlüssel häufiger wechseln, um die Abhörsicherheit zusätzlich zu steigern.

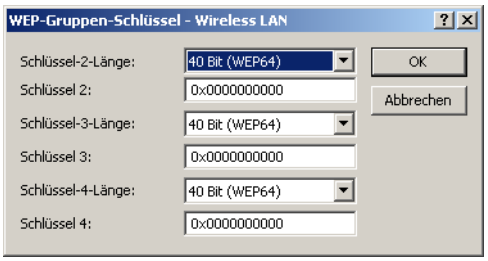
Die Regeln für die Eingabe der Schlüssel finden Sie bei der Beschreibung der WEP-Gruppenschlüssel 'Regeln für die Eingabe von WEP-Schlüsseln' → Seite 11-34.

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 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.

Die Regeln für die Eingabe der Schlüssel finden Sie bei der Beschreibung der WEP-Gruppenschlüssel 'Regeln für die Eingabe von WEP-Schlüsseln' → Seite 11-34.



LANconfig: Wireless LAN ▶ 802.11i/WEP ▶ WEP-Gruppen-Schlüssel

WEBconfig: LCOS-Menübaum ▶ 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

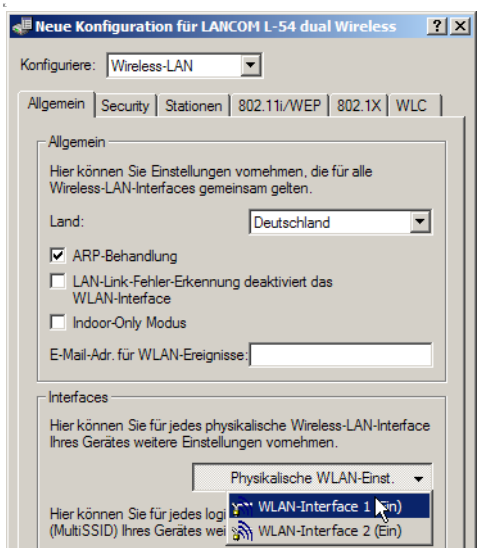
Der ASCII-Zeichensatz umfasst die Zeichen '0' bis'9', 'a' bis 'z', 'A' bis 'Z' sowie die folgenden Sonderzeichen:
! " # $ % & ´ () * + , - ./ : ; < = > ? @ [\ ] ^ _ ' { | } ~

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.

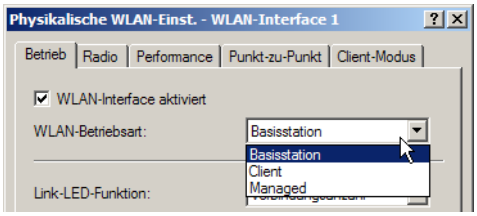
Wählen Sie die Länge und das Format (ASCII oder HEX) der Schlüssel immer nach den Möglichkeiten der Funknetzwerkkarten aus, die sich in Ihrem WLAN anmelden sollen. Wenn Sie im Access Point eine Verschlüsselung nach WEP 152 eingestellt haben, können manche Clients sich nicht mehr in diesem WLAN anmelden, weil sie die entsprechende Schlüssellänge nicht unterstützen.

11.5.5 Die physikalischen WLAN-Schnittstellen

Neben den allgemeinen WLAN-Parametern gelten eine Reihe von Einstellungen für jedes WLAN-Modul des Access Points speziell.



Betriebseinstellungen



LANconfig: Wireless LAN ▶ Allgemein ▶ Physikalische WLAN-Einstellungen ▶ Betrieb

WEBconfig: LCOS-Menübaum ▶ Setup ▶ Schnittstellen ▶ WLAN ▶ Betriebs-Einstellungen

■ **WLAN-Betriebsart**

LANCOM Access Points können grundsätzlich in verschiedenen Betriebsarten arbeiten:

- □ Als Basisstation (Access Point) stellt es für die WLAN-Clients die Verbindung zu einem kabelgebundenen LAN her.
- □ Als Client sucht das Gerät selbst die Verbindung zu einem anderen Access Point 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.
- □ Als Managed-Access Point sucht das Gerät einen zentralen WLAN-Controller, von dem es eine Konfiguration beziehen kann.

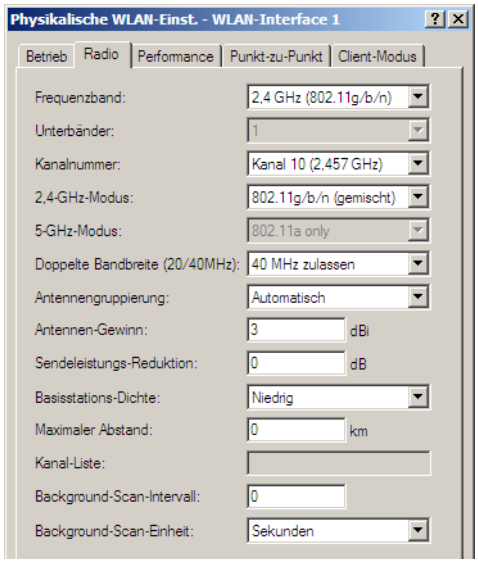
Wenn das WLAN-Interface nicht benötigt wird, kann es vollständig deaktiviert werden.

■ **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.

- □ Verbindungsanzahl: In dieser Betriebsart zeigt die LED mit einem „inversen Blitzen" die Anzahl der WLAN-Clients an, die bei dem Access Point als Client eingebucht sind. Nach der Anzahl der Blitzer für jeden Client erfolgt eine kurze Pause. Wählen Sie diese Betriebsart dann, wenn Sie den LANCOM Wireless Router im Access-Point-Modus betreiben.
- □ Client-Signalstärke: In dieser Betriebsart zeigt die LED die Signalstärke des Access Points an, bei dem ein LANCOM Access Point selbst als Client eingebucht ist. Je schneller die LED blinkt, umso besser ist das Signal. Wählen Sie diese Betriebsart nur, wenn Sie den LANCOM Access Point im Client-Modus betreiben.
- □ P2P1- bis P2P6-Signalstärke: In dieser Betriebsart zeigt die LED die Signalstärke des jeweiligen P2P-Partners, mit dem ein LANCOM Access Point eine P2P-Strecke bildet. Je schneller die LED blinkt, umso besser ist das Signal.

Radio-Einstellungen



LANconfig: Wireless LAN ▶ Allgemein ▶ Physikalische WLAN-Einstellungen ▶ Radio

WEBconfig: LCOS-Menübaum ▶ Setup ▶ Schnittstellen ▶ WLAN ▶ Radio-Einstellungen

■ **Frequenzband, Unterband**

Mit der Auswahl des Frequenzbandes auf der Registerkarte 'Radio' bei den Einstellungen für die physikalischen Interfaces legen Sie fest, ob das WLAN-Modul im 2,4 GHz- oder im 5 GHz-Band arbeitet (siehe auch 'Standardisierte Funkübertragung nach IEEE' → Seite 6), 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 zur automatischen Kanalsuche vorgeschrieben. Mit der Wahl des Unterbands wird damit auch der Bereich der Funkkanäle festgelegt, die für die automatische Kanalauswahl verwendet werden kann.

Beim DFS-Verfahren (Dynamic Frequency Selection) wird automatisch eine freie Frequenz gewählt, z. B. um das Stören von Radaranlagen zu verhindern und um die WLAN-Geräte möglichst gleichmäßig über das ganze Frequenzband zu verteilen. Nach dem Einschalten oder Booten wählt das Gerät aus den (z.B. aufgrund der Ländereinstellungen) verfügbaren Kanälen einen zufälligen Kanal aus und prüft, ob auf diesem Kanal ein Radarsignal gefunden wird und ob auf diesem Kanal schon ein anderes Wireless LAN arbeitet. Dieser Scan-Vorgang wird solange wiederholt, bis ein radarfreier Kanal mit möglichst wenig anderen Netzwerken gefunden wurde. 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 LANCOM den Scanvorgang **vor** die Auswahl eine 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 kann das WLAN-Gerät einen Kanal aus einer Liste der radarfreien Kanäle mit der geringsten Anzahl an anderen Netzwerken auswählen (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 Access Point dauerhaft den Kanal, der beim ersten Scan als Betriebskanal gewählt wurde. Die Verbindungen können beliebig lange auf dem vom DFS-Algorithmus gewählten Kanal bestehen blei-

ben, bis entweder ein Radarsignal erkannt wird oder die Funkzelle neu gestartet wird (z.B. bedingt durch Umkonfigurieren des Geräts, Firmware-Upload oder einen Neustart).

Wann ist ein erneuter 60-Sekunden-Scanvorgang wieder 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 de Access Points. In diesem Fall verfügt der Access Point 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 Kanalwechsel notwendig. Die Einträge in der Whitelist sind aus der Datenbank „herausgealtert", der Access Point 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 ein-minütigen Unterbrechungg des WLAN-Betriebs.

Damit der 60-Sekunden-Scanvorgang nicht zur unpassenden Zeit ausgelöst wird, können Sie unter WEBconfig oder Telnet im Menü `/Setup/Schnittstellen/WLAN/Radio-Einstellungen` die gewünschten Zeitpunkte für den Scanvorgang einstellen, zu denen das Löschen der Datenbank erzwungen wird. Für die Definition der Stunde können die Möglichkeiten der cron-Befehle genutzt werden, z.B. '1,6,13' für einen DFS-Scan immer um 1 Uhr, um 6 und um 13 Uhr oder '0-23/4' für einen DFS-Scan in der Zeit von 0 bis 23 Uhr alle vier Stunden. Voraussetzung für das Erzwingen des DFS-Scans ist eine korrekte Systemzeit im Gerät.

Mit der Version 1.4.1 der Richtlinie 301 893 hat die ETSI neue Vorschriften für den Betrieb von 5 GHz-WLANs veröffentlicht. Im Zusammenhang mit den WLAN-Modulen, die in LANCOM Wireless Routern und LANCOM Access Points verwendet werden, spricht man bei dieser Richtlinie auch von DFS 2.

Die Richtlinie fordert verschärfte Radar-Erkennungsmuster für den Betrieb der 5 GHz-WLANs. Die Vorschrift gilt für alle Geräte, die nach dem 01.04.2008 in Verkehr gebracht werden. Geräte, die schon vor diesem Datum in Verkehr gebracht worden sind, müssen diese nicht erfüllen. Insbesondere müssen Geräte mit älternen WLAN-Chips (Zwei- oder Drei-Chip-Module) diese Richtlinie nicht erfüllen und müssen somit auch nicht nachgerüstet werden.

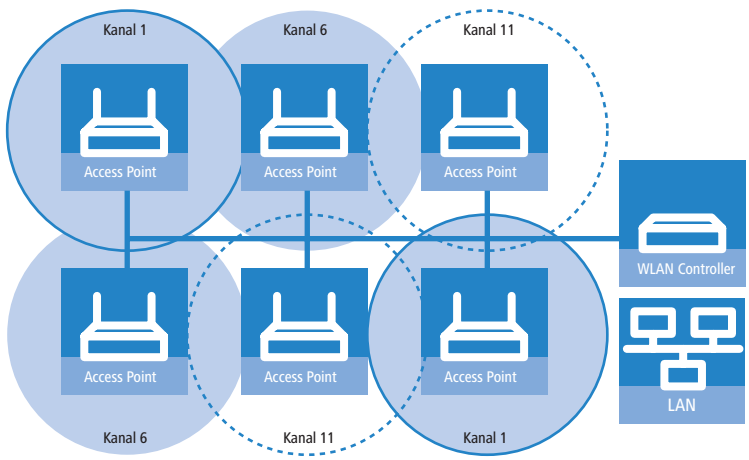
LANCOM Systems bietet mit LCOS 7.30 (für die aktuellen Wireless Router und Access Points) sowie 7.52 (für LANCOM Wireless L-310agn und LANCOM Wireless L-305agn) Firmware-Versionen an, die DFS 2 unterstützen. Dabei werden in der Firmware andere Schwellwerte für die Radar-Muster-Erkennung definiert als beim bisherigen DFS.

Grundsätzlich ist der Betreiber des WLANs zuständig für die Einhaltung der neuen ETSI-Regelungen. LANCOM Systems empfiehlt daher den zeitnahen Umstieg auf eine Firmware-Version mit DFS 2-Unterstützung.

■ Kanalnummer

Mit dem Funkkanal wird ein Teil des theoretisch denkbaren Frequenzbandes für die Datenübertragung im Funknetz ausgewählt.

Im 2,4 GHz-Band müssen zwei getrennte Funknetze mindestens drei Kanäle auseinander liegen, um Störungen zu vermeiden.



■ 2,4 GHz- Modus

Im 2,4 GHz- Band gibt es drei verschiedene Funk- Standards: IEEE 802.11b, IEEE 802.11g und IEEE 802.11n. Wenn als Frequenzband das 2,4 GHz- Band ausgewählt ist, kann zusätzlich der Kompatibilitätsmodus eingestellt werden.

Bitte beachten Sie, dass sich Clients, die nur einen langsameren Standard unterstützen, sich ggf. nicht mehr in Ihrem WLAN anmelden können, wenn Sie den Kompatibilitätsmodus auf einen hohen Wert einstellen.

Um eine möglichst hohe Übertragungsgeschwindigkeit zu erreichen, gleichzeitig aber auch langsamere Clients nicht auszuschließen, bietet sich der 802.11gbn- Kompatibilitätsmodus an. In diesem Modus arbeitet das WLAN- Modul im Access Point grundsätzlich nach dem schnelleren Standard, fällt aber auf den langsameren Modus zurück, wenn sich entsprechende Clients im WLAN anmelden.

802.11n ist prinzipiell abwärtskompatibel zu den vorhergehenden WLAN- Standards IEEE 802.11b/g, dabei werden jedoch nicht alle 802.11n- Funktionen unterstützt.

Im 2,4 GHz- Band können Sie den Betrieb nach 802.1b/g/n entweder ausschließlich oder in verschiedenen Mischformen zulassen. Bei der Unterstützung von 802.11b können sie zusätzlich auswählen, ob hier nur der 11 MBit- Modus oder auch der ältere 2 MBit- Modus unterstützt werden sollen.

Die Kompatibilität geht immer zu Lasten der Performance. Erlauben Sie daher nur die Betriebsarten, die aufgrund der vorhandenen WLAN- Clients unbedingt erforderlich sind.

■ 5 GHz- Modus

Wenn Sie gleichzeitig zwei benachbarte, freie Kanäle für die Funkübertragung nutzen, können Sie die Übertragungsgeschwindigkeit auf bis zu 108 MBit/s steigern. Wenn Sie die Basisstation in den 108Mbit/Sekunde-Turbo- Modus schalten, können nur noch diejenigen WLAN- Clients eine Verbindung zu dieser Basisstation aufnehmen, welche ebenfalls im 108Mbit/Sekunde-Turbo- Modus betrieben werden.

Auch im 5 GHz- Band können Sie neben dem Greenfield- Modus (nur 802.11n) den mit 802.11a gemischten Betrieb zulassen. Befinden sich in einem Netzwerk nur 802.11n- Geräte, so sollte der Greenfield- Modus gewählt werden, denn dieser garantiert höchst mögliche Datendurchsatzraten.

Nur 802.11n

■ Doppelte Bandbreite (20/40 MHz)

Normalerweise nutzt das WLAN- Modul einen Frequenzbereich von 20 MHz, in dem die zu übertragenen Daten auf die Trägersignale aufmoduliert werden. 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.

Nur 802.11n

■ Antennengruppierung

LANCOM Access Points mit 802.11- 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 Access- Point- 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 Antennen an den Anschluss 1 angeschlossen, die Anschlüsse 2 und 3 werden deaktiviert.

□ Mit der Einstellung 'Auto' 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 zweiten Antenne entweder Anschluss 2 oder Anschluss 3 gewählt werden.

Die softwareseitige Konfiguration des Gerätes muss dabei mit dem Anschluss der Antennenkabel übereinstimmen.

Nur 802.11abg

■ **Diversity-Einstellungen**

Die Diversity-Einstellungen legen fest, welche Antennen zum Senden bzw. zum Empfangen verwendet werden:

□ 'Nur auf der primären Antenne senden' (Rx-Diversity): In dieser Standardeinstellung wird über die am Main-Anschluss des Access Points angeschlossene Antenne gesendet. Zum Empfangen (RX) wird die Antennen ausgewählt, die den besten Empfang hat (an Main oder AUX).

□ 'Automatisch die beste Antenne zum Senden selektieren' (Tx- und Rx-Diversity): Wird die Diversity-Funktion auch auf das Senden angewendet (TX), wird auch zum Senden die Antenne mit dem stärksten Signal ausgewählt.

□ 'Auf der primären Antennen Senden und auf der sekundären empfangen' (kein Diversity): Hierbei wird nur die Main-Antenne zum Senden verwendet, zum Empfangen bevorzugt die Antenne den AUX-Anschluss. Mit dieser Variante können Antennen mit sehr hohen Leistungen zum Empfangen eingesetzt werden, die aus rechtlichen Gründen nicht zum Senden verwendet werden dürfen.

■ **Antennen-Gewinn, Sendeleistungs-Reduktion**

Wenn Antennen mit einer höheren Sendeleistung eingesetzt werden, als in dem jeweiligen Land zulässig, ist eine Dämpfung der Leistung auf den zulässigen Wert erforderlich.

□ In das Feld 'Antennen-Gewinn' wird der Gewinn der Antenne abzüglich der tatsächlichen Kabeldämpfung eingetragen. Bei einer AirLancer Extender O-18a-Antenne mit einem Gewinn von 18dBi wird bei einer Kabellänge von 4m Länge mit einer Dämpfung 1dB/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.

□ Im Gegensatz dazu reduziert der Eintrag im Feld 'Sendeleistungs-Reduktion' die Leistung immer statisch um den dort eingetragenen Wert, ohne Berücksichtigung der anderen Parameter. Siehe dazu auch 'Geometrische Auslegung von Outdoor-Funknetz-Strecken' → Seite 65.

Durch die Sendeleistungsreduktion 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.

■ **Basisstations-Dichte**

Mit zunehmender Dichte von Access Points überlagern sich die Empfangsbereiche der Antennen. Die Information über die 'Basisstations-Dichte' wird in den Beacons mitgeteilt und von älteren Agere-Clients ausgewertet.

■ **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 Datenpakete bei der drahtlosen Kommunikation zugestanden werden soll.

■ **Background-Scan-Intervall**

Wird hier ein Wert angegeben, so sucht der LANCOM Wireless Router innerhalb dieses Intervalls zyklisch die aktuell ungenutzten Frequenzen des aktiven Bandes nach erreichbaren Access Points ab.

□ Für LANCOM Wireless Router im Access-Point-Modus wird die Background-Scan-Funktion üblicherweise zur Rogue AP Detection eingesetzt. Das Scan-Intervall sollte hier der Zeitspanne angepasst werden, innerhalb derer unbefugte Access Points erkannt werden sollen, z.B. 1 Stunde.

- □ Für LANCOM Wireless Router 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.

■ **Zeiteinheit für Background-Scanning**

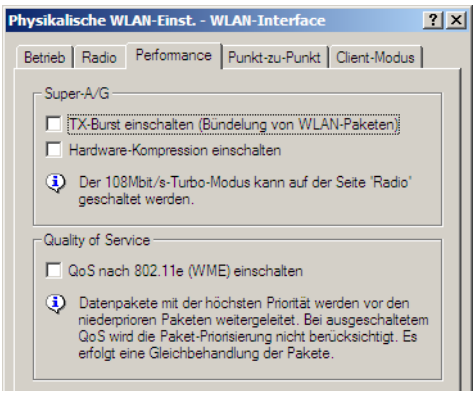
Das Background-Scan-Intervall gibt an, in welchen zeitlichen Abständen ein Wireless Router oder Access Point nach fremden WLAN-Netzen in Reichweite sucht.

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 Access Point-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 20s = 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 LANCOM Wireless Router im Client-Modus noch weiter verbessert werden.

Performance



LANconfig: Wireless LAN ▶ Allgemein ▶ Physikalische WLAN-Einstellungen ▶ Performance

WEBconfig: LCOS-Menübaum ▶ Setup ▶ Schnittstellen ▶ WLAN ▶ Leistung

■ **TX-Burst**

Erlaubt/Verbietet das Paket-Bursting, was den Durchsatz erhöht, jedoch die Fairness auf dem Medium verschlechtert.

■ **Hardware-Kompression**

Erlaubt oder verbietet eine Hardwarekompression von Paketen.

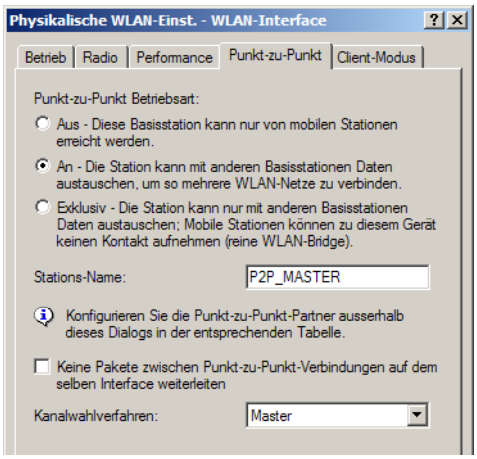
■ **QoS nach 802.11e**

Mit der Erweiterung der 802.11-Standards um 802.11e können auch für WLAN-Übertragungen definierte Dienst-güten angeboten werden (Quality of Service). 802.11e unterstützt u.a. eine Priorisierung von bestimmten Datenpa-keten. Die Erweiterung stellt damit eine wichtige Basis für die Nutzung von Voice-Anwendungen im WLAN dar (Voiceoder 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 Steuerung der Prioritäten die VLAN-Tags bzw. die DiffServ-Felder von IP-Paketen, wennkeine VLAN-Tags vorhanden sind. Die Verzögerungszeiten (Jitter) bleiben mit weniger als zwei Millisekunden ineinem Bereich, der vom menschlichen Gehör nicht wahrgenommen wird. Zur Steuerung des Zugriffs auf das Über-tragungsmedium 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 den802.11e-Standard bzw. WMM unterstützen und die Anwendungen die Datenpakete mit den entsprechen-den Prioritäten kennzeichnen.

Punkt-zu-Punkt-Verbindungen

Access Points können nicht nur mit mobilen Clients kommunizieren, sie können auch Daten von einer Basisstation zur anderen übertragen.



LANconfig: Wireless LAN ▶ Allgemein ▶ Physikalische WLAN-Einstellungen ▶ Punkt-zu-Punkt

WEBconfig: LCOS-Menübaum ▶ Setup ▶ Schnittstellen ▶ WLAN ▶ Interpoint-Einstellungen

- **Punkt-zu-Punkt-Betriebsart**
  - 'Aus': Die Basisstation kann nur mit mobilen Clients kommunizieren
  - 'An': Die Basisstation kann mit anderen Basistationen und mit mobilen Clients kommunizieren
  - 'Exklusiv': Die Basisstation kann nur mit anderen Basistationen kommunizieren
- **Stations-Name**

  Geben Sie hier einen im WLAN eindeutigen Namen für diese physikalische WLAN-Schnittstelle ein. Dieser Name kann auf anderen WLAN-Geraten genutzt werden, um diese Basisstation über Punkt-zu-Punkt anzubinden.

  Sie können dieses Feld frei lassen, wenn das Gerät nur eine WLAN-Schnittstelle hat und bereits ein im WLAN eindeutiger Geräte-Name konfiguriert ist oder die übrigen Basisstation diese Schnittstelle über die MAC-Adresse des WLAN-Adapters identifizieren.
- **Keine Pakete zwischen Punkt-zu-Punkt-Verbindungen auf dem selben interface weiterleiten**

  Erlaubt oder verbietet die Übertragung von Paketen zwischen P2P-Links auf der gleichen WLAN-Schnittstelle.
- **Kanalwahlverfahren**

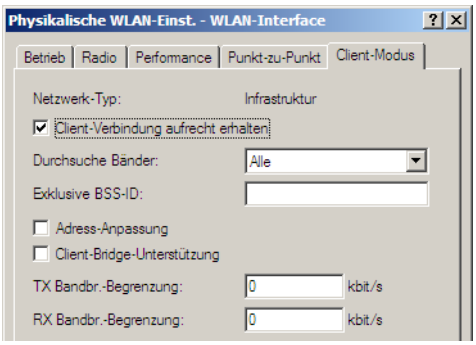
  Bei der automatischen Suche nach einem freien WLAN-Kanal kann es im 5 GHz-Band zu gleichzeitigen Sendeversuchen mehrerer Access Points kommen, die sich in der Folge gegenseitig nicht finden. Diese Pattsituationen kann mit dem geeigneten „Kanalwahlverfahren" verhindert werden.

  Es ist daher empfehlenswert, im 5 GHz-Band jeweils einen zentralen Access Point 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.
  - Master: Dieser Access Point übernimmt die Führung bei der Auswahl eines freien WLAN-Kanals.
  - Slave: Alle anderen Access Points suchen solange nach dem freien Kanal, bis sie einen sendenden Master gefunden haben.

In diesem Bereich werden nur die allgemeinen P2P-Parameter definiert – die konkreten Verbindungen zu den entfernten WLAN-Gegenstellen werden unter folgenden Pfaden definiert:
LANconfig: Wireless LAN ▶ Allgemein ▶ Punkt-zu-Punkt-Partner
WEBconfig: Setup ▶ Schnittstellen ▶ WLAN Interpoint-Gegenstellen

Client-Modus

Wenn das LANCOM Router-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

WEBconfig: LCOS-Menübaum ▶ 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**

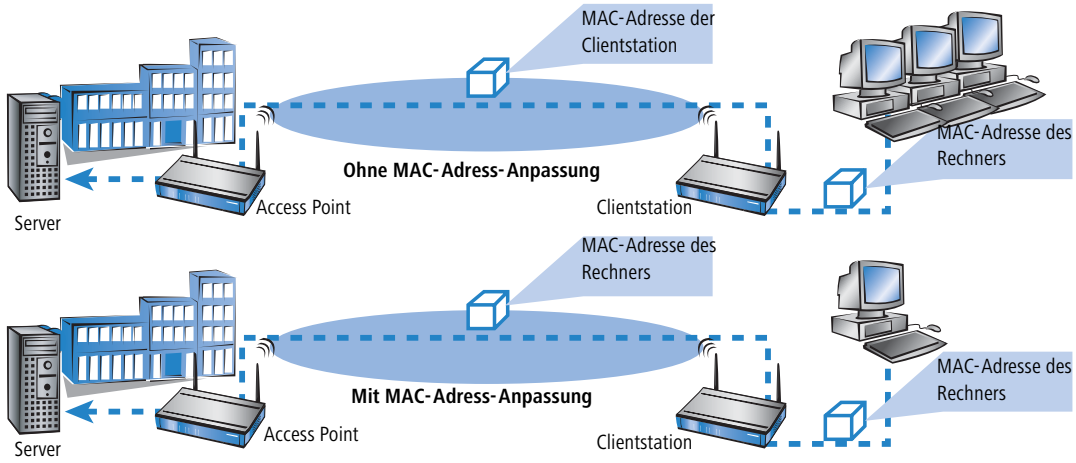
Legen Sie hier fest, ob die Clientstation nur das 2,4 GHz-, nur das 5 GHz-Band oder alle verfügbaren Bänder absuchen soll, um eine Basisstation zu finden.

■ **Bevorzugte BSS-ID**

Wenn sich die Clientstation nur bei einem bestimmten Access Point einbuchen soll, können Sie hier die MAC-Adresse des WLAN-Moduls aus diesem Access Point 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 Access-Point 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.

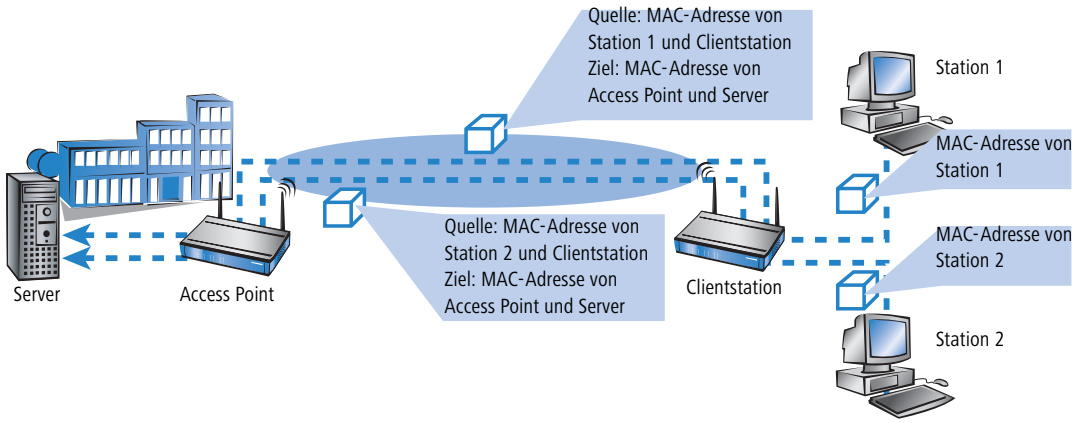


In manchen Installationen ist es jedoch gewünscht, dass die MAC-Adresse eines Rechners und nicht die der Clientstation an den Access Point übertragen wird. Mit der Option 'Adress-Anpassung' wird das Ersetzen der MAC-Adresse durch die Clientstation unterbunden, die Datenpakete werden mit der originalen MAC-Adresse übertragen – der Access Point übernimmt im WLAN die MAC-Adresse des Clients.

Die Adress-Anpassung funktioniert nur, wenn an die Clientstation nur **ein** Rechner angeschlossen ist!

■ **Client-Bridge-Unterstützung**

Während mit der Adress-Anpassung ('Adress-Anpassung' → Seite 11-42) nur die MAC-Adresse eines **einzigen** angeschlossenen Gerätes für den Access Point sichtbar gemacht werden kann, werden über die Client-Bridge-Unterstützung alle MAC-Adressen der Stationen im LAN hinter der Clientstationen transparent an den Access Point übertragen.



Dazu werden in dieser Betriebsart nicht die beim Client-Modus üblichen drei MAC-Adressen verwendet (in diesem Beispiel für Server, Access Point und Clientstation), sondern wie bei Punkt-zu-Punkt-Verbindungen vier Adressen (zusätzlich die MAC-Adresse der Station im LAN der Clientstation). Die volltransparente Anbindung eines LANs an der Clientstation ermöglicht die gezielte Übertragung der Datenpakete im WLAN und damit Funktionen wie TFTP-Downloads, die über einen Broadcast angestossen werden.

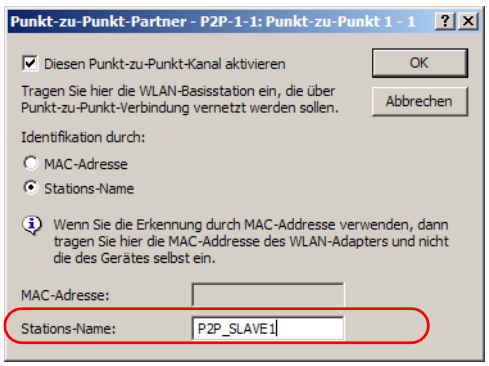
Der Client-Bridge-Modus hat folgende Vorteile gegenüber den anderen Verfahren:

- Gegenüber dem „normalen" Client-Modus entfällt die Adress-Übersetzung (Maskierung) in der Clientstation.
- Gegenüber den Punkt-zu-Punkt-Verbindungen entfällt die manchmal unerwünschte feste Eintragung der MAC-Adressen oder Stationsnamen. Darüber hinaus können mit dem Client-Bridge-Modus mehr als sechs Verbindungen (Einschränkung bei P2P) eingerichtet werden.
- Die Client-Station kann Roamen, was bei Point-to-Point nicht möglich ist (gilt sowohl für den Client-Bridge-Modus wie auch für den einfachen Client-Modus).

Der Client-Bridge-Modus kann ausschließlich zwischen zwei LANCOM-Geräten verwendet werden. Die Verwendung des Client-Bridge-Modus muss in den Einstellungen für das logische Netzwerk des Access Points ebenfalls aktiviert werden.

11.5.6 Die Punkt-zu-Punkt-Partner

Für jedes WLAN-Modul können bis zu sechs Punkt-zu-Punkt-Verbindungen aktiviert werden.



LANconfig: Wireless LAN ▶ Allgemein ▶ Punkt-zu-Punkt-Partner

WEBconfig: Setup ▶ Schnittstellen ▶ WLAN Interpoint-Gegenstellen

- **Identifikation durch**

  Wählen Sie hier aus, anhand welchen Merkmals die P2P-Gegenstelle identifiziert werden soll.

- **MAC-Adresse**

  MAC-Adresse der P2P-Gegenstelle.

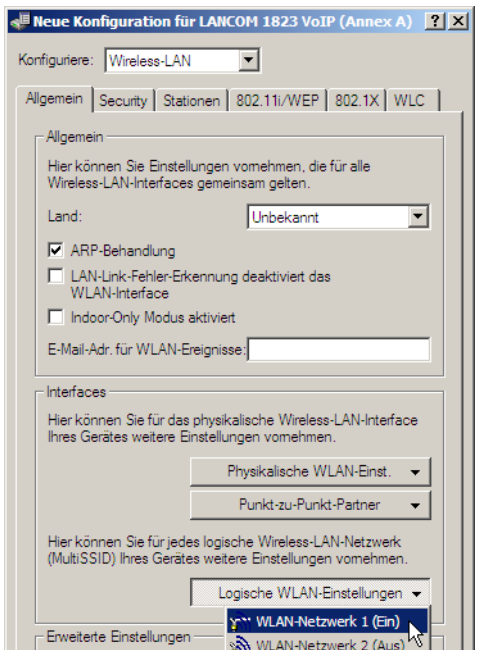
- **Stations-Name**

  Stations-Name der P2P-Gegenstelle.

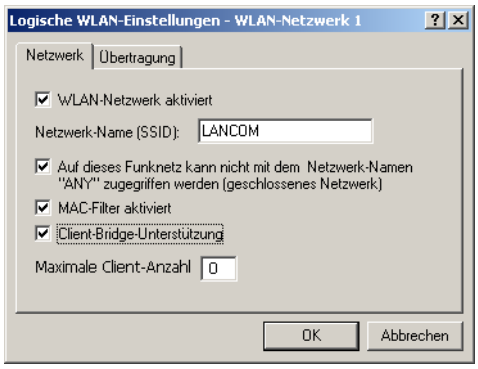
Wenn Sie die Erkennung durch MAC-Addresse verwenden, dann tragen Sie hier die MAC-Addresse des WLAN-Adapters und nicht die des Gerätes selbst ein.

11.5.7 Die logischen WLAN-Schnittstellen

Jede physikalische WLAN-Schnittstelle kann bis zu acht verschiedene logische Funknetzwerke aufspannen (Multi-SSID). Für jedes dieser Funknetze können bestimmte Parameter speziell definiert werden, ohne dass zusätzliche Access Points benötigt werden.



Netzwerkeinstellungen



LANconfig: Wireless LAN ▶ Allgemein ▶ Logische WLAN-Einstellungen ▶ Netzwerk

WEBconfig: LCOS-Menübaum ▶ Setup ▶ Schnittstellen ▶ WLAN ▶ Netzwerk

- **WLAN-Netzwerk aktivieren**

  Mit diesem Schalter kann das logische WLAN separat ein- oder ausgeschaltet werden.

- **Netzwerk-Name (SSID)**

  Stellen Sie für jedes benötigte logische Funknetzwerk eine eindeutige SSID (den Netzwerknamen) ein. Nur solche Netzwerkkarten, 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 Angabe der SSID kontaktiert werden. Durch das Unterdrücken der SSIDs in den Broadcasts 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 das Unterdrücken der SSID-Broadcasts ein, wenn Sie verhindern möchten, dass sich WLAN-Clients ohne Angabe der SSID in Ihrem Funknetzwerk anmelden.

- **MAC-Filter aktiviert**

  In der MAC-Filterliste (**Wireless-LAN ▶ Stationen ▶ Stationen**) werden die MAC-Adressen der Clients hinterlegt, die sich bei einem Access Point einbuchen dürfen. Mit dem Schalter 'MAC-Filter aktiviert' kann die Verwendung der MAC-Filterliste gezielt für einzelne logische Netzwerke ausgeschaltet werden.

Die Verwendung der MAC-Filterliste ist auf jeden Fall erforderlich für logische Netzwerke, in denen sich die Clients mit einer individuellen Passphrase über LEPS anmelden. Die bei LEPS verwendete Passphrase wird ebenfalls in der MAC-Filterliste eingetragen. Für die Anmeldung mit einer individuellen Passphrase wird daher immer die MAC-Filterliste beachtet, auch wenn diese Option hier deaktiviert ist.

- **Maximale Client-Anzahl**

  Legen Sie hier die maximale Anzahl der Clients fest, die sich bei diesem Access Point einbuchen dürfen. Weitere Clients, die sich über diese Anzahl hinaus anmelden wollen, werden abgelehnt.

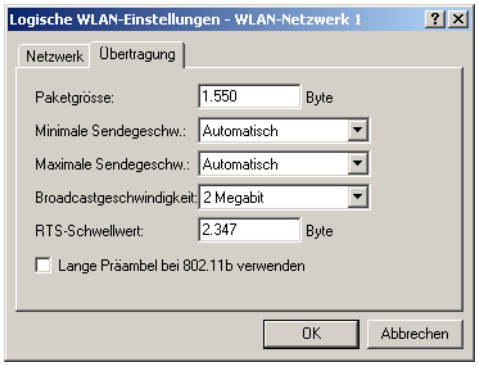
- **Client-Bridge-Unterstützung**

  Aktivieren Sie diese Option für einen Access Point, wenn Sie im WLAN-Client-Modus für eine Clientstation die Client-Bridge-Unterstützung aktiviert haben ('Client-Bridge-Unterstützung' → Seite 11-42).

Der Client-Bridge-Modus kann ausschließlich zwischen zwei LANCOM-Geräten verwendet werden.

Einstellungen für die Übertragung

Die Details für die Datenübertragung auf dem logischen Interface stellen Sie auf der Registerkarte 'Übertragung' ein.



LANconfig: Wireless LAN ▶ Allgemein ▶ Logische WLAN-Einstellungen ▶ Übertragung

WEBconfig: LCOS-Menübaum ▶ Setup ▶ Schnittstellen ▶ WLAN ▶ Uebertragung

- **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 Access Point handelt mit den angeschlossenen WLAN-Clients die Geschwindigkeit für die Datenübertragung normalerweise fortlaufend dynamisch aus. Dabei passt der Access Point die Übertragungsgeschwindigkeit an die Empfangslage an. Alternativ können Sie hier die minimalen und maximalen Übertragungsgeschwindigkeiten fest vorgeben, wenn Sie die dynamische Geschwindigkeitsanpassung verhindern wollen.

Nur 802.11n

- **Modulation Coding Scheme (MCS)**

  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 „Datenrate" bei älteren WLAN-Standards, weil die Rate keine eindeutige Beschreibung mehr ist.

MCS-Index	Datenströme	Modulation	Coding-Rate	Datendurchsatz (GI=0,4 µs, 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

MCS-Index	Datenströme	Modulation	Coding-Rate	Datendurchsatz (GI=0,4 µs, 40 MHz)
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 µs mit Nutzung des 40 MHz-Kanals).

■ **Broadcastgeschwindigkeit**

Die eingestellte Broadcastgeschwindgkeit 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.

Nur 802.11n

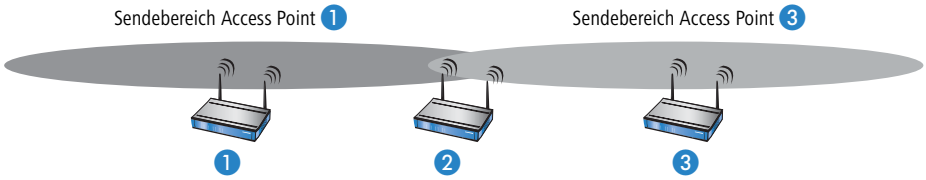
■ **Anzahl Spatial-Streams**

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.

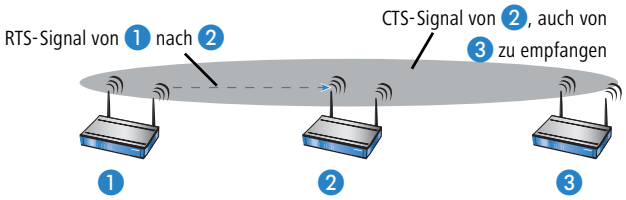
Mit der Einstellung 'Auto' werden alle Spatial-Streams genutzt, die von dem jeweiligen WLAN-Modul unterstützt werden.

■ **RTS-Schwellwert**

Mit dem RTS-Schwellwert wird das Phänomen der „Hidden-Station" vermieden.



Dabei sind drei Access Points 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 ausgestrahle 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-Pakete 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-Schwellwert 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-Schwellwert muss auch in den WLAN-Clients entsprechend den Möglichkeiten des Treibers bzw. des Betriebssystems eingestellt werden.

■ **Lange Präambel bei 802.11b**

Normalerweise handeln die Clients im 802.11b-Modus die Länge der zu verwendenden Präambel mit dem Access Point selbst aus. Stellen Sie hier die „lange Präambel" nur dann fest ein, wenn die Clients diese feste Einstellung verlangen.

Nur 802.11n

■ **Kurzes Guard-Intervall**

Mit dieser Option wird die Sendepause zwischen zwei Signalen von 0,8 µs (Standard) auf 0,4 µs (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.

Nur 802.11n

■ **Frame-Aggregation**

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.

Nur mit WEBconfig

■ **Hard-Retries**

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.

Nur mit WEBconfig

■ **Soft-Retries**

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.

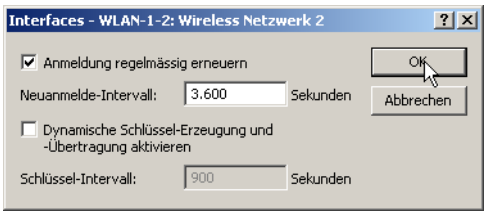
Der Vorteil von Soft-Retries auf Kosten von Hard-Retries ist, dass aufgrund des Raten-Adaptionalgorithmus die nächste Serie von Hard-Retries direkt mit einer niedrigeren Rate beginnt.

11.5.8 IEEE 802.1x/EAP

Der internationale Industrie-Standard IEEE 802.1x und das **E**xtensible **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.

Diese Technologie ermöglicht außerdem den gesicherten Versand und den regelmäßigen automatischen Wechsel von WEP Schlüsseln. Auf diese Weise verbessert IEEE 802.1x die Sicherungswirkung von WPA2.

Ab Windows XP ist die IEEE-802.1x-Technologie bereits fest integriert. Für andere Betriebssysteme existiert Client-Software.



LANconfig: Wireless LAN ▶ Allgemein ▶ 802.1X

WEBconfig: LCOS-Menübaum ▶ 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. Ein typischer Standardwert fiir das Neuanmelde-Intervall ist 3.600 Sekunden.

■ **Neuanmelde-Intervall**

Intervall für die regelmäßige Neuanmeldung.

■ **Dynamische Schlüssel-Erzeugung und Übertragung aktivieren**

Hier aktivieren Sie die regelmäßige Erzeugung dynamischer WEP-Schlüssel und deren Übertragung.

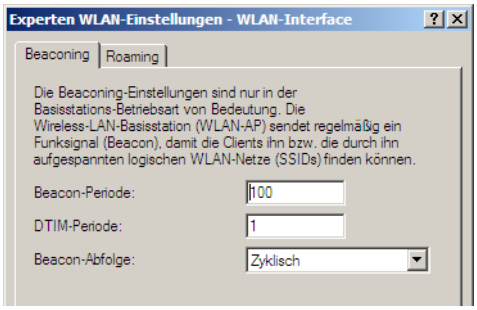
■ **Schlüssel-Intervall**

Intervall für die regelmäßige Erzeugung der Schlüssel.

11.5.9 Experten-WLAN-Einstellugnen

Die Beaconing-Tabelle

Die Einstellungen in der Beaconing-Tabelle beeinflussen, wie die im AP-Modus vom Access Point 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 ▶ Experten-WLAN-Einstellugnen ▶ Beaconing

WEBconfig: LCOS-Menübaum ▶ Setup ▶ Schnittstellen ▶ WLAN ▶ Beaconing

■ **Beacon-Periode**

Dieser Wert gibt den zeitlichen Abstand in Kµs an, in dem Beacons verschickt werden (1 Kµs entspricht 1024 Mikrosekunden und stellt eine Recheneinheit des 802.11-Standard dar – 1 Kµs wird auch als Timer Unit TU bezeichnet). Niedrigere Werte ergebenen kleinere Beacon-Timeout-Zeiten auf dem Client und erlauben damit ein schnelleres Roaming beim Access Point-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 Beacon zu den verschiedenen WLAN-Netzen versendet werden. Wenn z.B. drei logische WLAN-Netze aktiv sind und die Beacon-Periode 100 Kµs beträgt, so werden alle 100 Kµs die Beacons für die drei WLANs verschickt. Je nach Beacon-Abfolge werden die Beacons zu folgenden Zeitpunkten versendet:

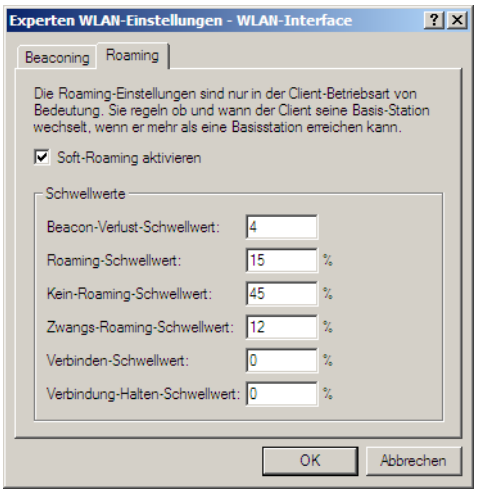
- □ zyklisch: In diesem Modus beginnt der Access Point beim ersten Beacon-Versand (0 Kµs) mit WLAN-1, gefolgt von WLAN-2 und WLAN-3. Beim zweiten Beacon-Versand (100 Kµs) wird zuerst WLAN-2 versendet, dann WLAN-3 und erst dann kommt wieder WLAN-1 an die Reihe. Beim dritten Beacon-Versand (200 Kµs) entsprechend 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 Kµs wird nur WLAN-1 verschickt, nach 33,3 Kµs kommt WLAN-2, nach 66,6 Kµs WLAN-3 – mit Beginn einer neuen Beacon-Periode startet der Versand wieder mit WLAN-1.
- □ einfach-Burst: In diesem Modus verschickt der Access Point die Beacons für die definierten WLAN-Netze immer in der gleichen Abfolge. Beim ersten Beacon-Versand (0 Kµs) mit WLAN-1, WLAN-2 und WLAN-3, beim zweiten Versand nach dem gleichen Muster und so weiter.
- □ Default: zyklisch

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 Access Point. Die zyklische Aussendung stellt sich als guter Kompromiss dar, weil hier jedes Netz einmal als erstes ausgesendet wird.

Die Roaming-Tabelle

Zur genauen Steuerung, wie sich ein LANCOM Wireless Router in der Betriebsart 'Client' beim Roaming verhält, dienen verschiedene Schwellwerte in der Roaming Tabelle.



LANconfig: Wireless LAN ▶ Experten-WLAN-Einstellugnen ▶ Roaming

WEBconfig: LCOS-Menübaum ▶ Setup ▶ Schnittstellen ▶ WLAN ▶ Roaming

- **Soft-Roaming**

  Diese Option ermöglicht dem Client, anhand verfügbarer Scan-Informationen ein Roaming zu einem stärkeren Access Point durchzuführen (Soft-Roaming). Roaming aufgrund eines Verbindungsverlustes (Hard-Roaming) bleibt davon natürlich unbeeinflusst. Die eingestellten Roaming-Schwellwerte haben nur eine Funktion, wenn Soft-Roaming aktiviert ist.

- **Beacon-Empfangs-Schwellwert**

  Der Beacon-Empfangs-Schwellwert gibt an, wieviele Beacons des Access Points 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 Access Point 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 Access Points besser sein muss, damit der Client auf den anderen Access Point 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 Access Point als so gut betrachtet wird, dass auf keinen Fall auf einen anderen Access Point gewechselt wird.

- **Zwangs-Roaming-Schwellwert**

  Dieser Schwellwert gibt die Feldstärke in Prozent an, ab welcher der aktuelle Access Point als so schlecht betrachtet wird, dass auf jeden Fall auf einen anderen, besseren Access Point gewechselt wird.

- **Verbindungs-Schwellwert**

  Dieser Schwellwert gibt die Feldstärke in Prozent an, die ein Access Point mindestens aufweisen muss, damit ein Client einen Versuch zum Einbuchen bei diesem Access Point startet.

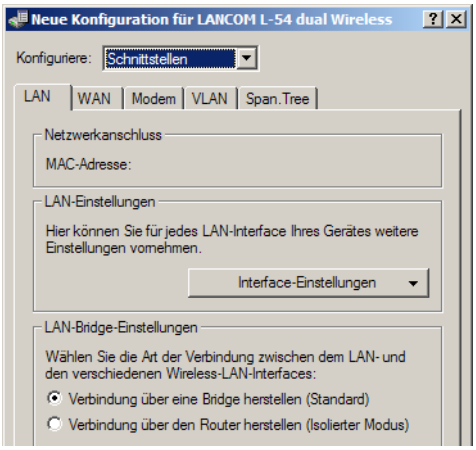
■ **Verbindung- Halten- Schwellwert**

Dieser Schwellwert gibt die Feldstärke in Prozent an, die der aktuelle Access Point mindestens aufweisen muss, damit die Verbindung nicht als abgerissen betrachtet wird.

11.5.10 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).

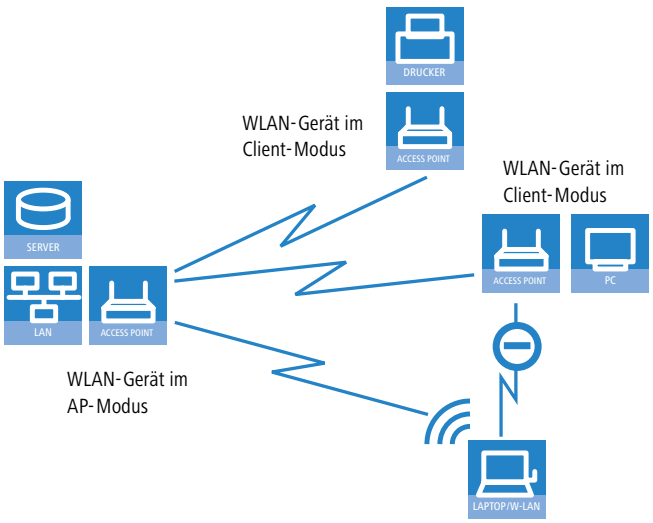


LANconfig: Wireless LAN ▶ Schnittstellen ▶ LAN

WEBconfig: LCOS- Menübaum ▶ Setup ▶ LAN- Bridge ▶ Isolierter- Modus

11.6 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.

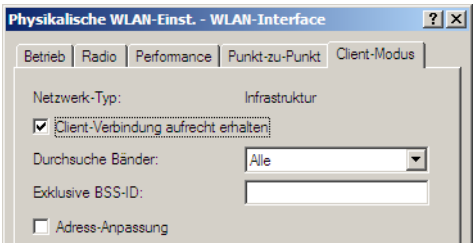


Bei einem WLAN- Gerät im AP- Modus können sich weitere WLAN- Clients anmelden, bei einem WLAN- Gerät im Client- Modus jedoch nicht.

11.6.1 Client- Einstellungen

Für LANCOM Access Points und LANCOM Wireless Router im Client- Modus können auf der Registerkarte 'Client- Modus' bei den Einstellungen für die physikalischen Interfaces weitere Einstellungen bzgl. des Verhaltens als Client vorgenommen werden.

Die Konfiguration der Client- Einstellungen kann auch mit dem WLAN- Assistenten von LANconfig erfolgen.



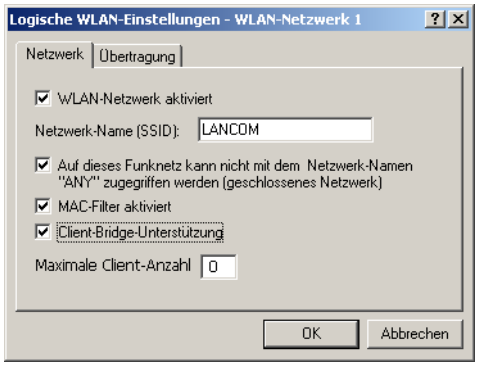
① Zum Bearbeiten der Einstellungen für den Client- Modus wechseln Sie unter LANconfig bei den physikalischen WLAN- Einstellungen für das gewünschte WLAN- Interface auf die Registerkarte 'Client- Modus'.

② Stellen Sie unter 'Durchsuchte Bänder' ein, ob die Clientstation nur das 2,4 GHz- , nur das 5 GHz- Band oder alle verfügbaren Bänder absuchen soll, um eine Basisstation zu finden.

11.6.2 SSID des verfügbaren Netzwerke einstellen

In den WLAN- Clients muss die SSID desNetzwerks eingetragen werden, zu denen sich die Clientstationen verbinden sollen.

① Zum Eintragen der SSID wechseln Sie unter LANconfig im Konfigurationsbereich 'Wireless LAN' auf die Registerkarte 'Allgemein'. Im Abschnitt 'Interfaces' wählen Sie aus der Liste der logischen WLAN- Einstellungen das **erste** WLAN- Interface aus.

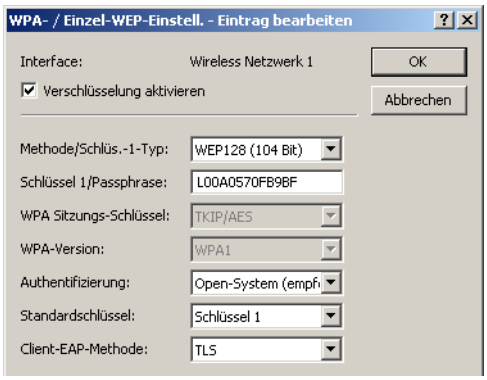


② Aktivieren Sie das WLAN- Netzwerk und tragen Sie die SSID des Netzwerks ein, bei dem sich die Clientstation einbuchen soll.

11.6.3 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 im Konfigurationsbereich 'Wireless LAN' auf die Registerkarte '802.11i/WEP'. Im Abschnitt 'WPA- / Einzel- WEP- Einstellungen' wählen Sie aus der Liste der logischen WLAN- Einstellungen das **erste** WLAN- Interface aus



② Aktivieren Sie die Verschlüsselung und passen Sie die Verschlüsselungsmethode an die Einstellungen des Access Points an.

③ LANCOM Access Point und LANCOM Wireless Router in der Betriebsart als WLAN-Client können sich über EAP/802.1X bei einem anderen Access Point authentifizieren. Wählen Sie dazu hier die gewünschte Client-EAP-Methode aus. Beachten Sie, dass die gewählte Client-EAP-Methode zu den Einstellungen des Access Points passen muss, bei dem sich das Gerät einbuchen will.

Je nach gewählter EAP-Methode müssen im Gerät die ensprechenden Zertifikate hinterlegt werden:

- Für TTLS und PEAP nur das EAP/TLS-Root-Zertifikat, als Schlüssel wird dabei die Kombination Benutzername:Kennwort eintragen.
- 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.

11.6.4 Roaming

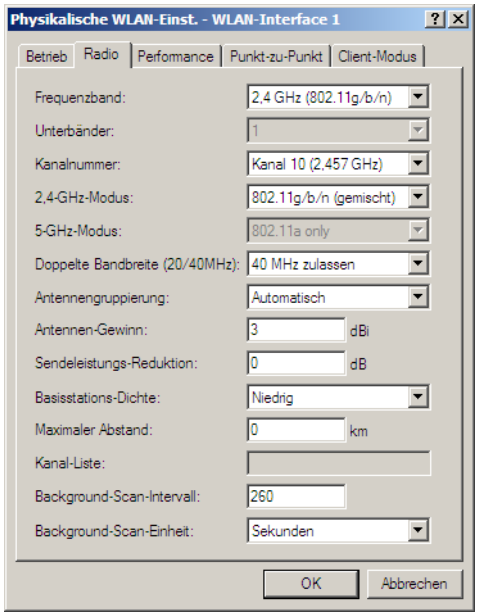
Mit Roaming bezeichnet man den Übergang eines WLAN-Clients zu einem anderen Access Point, wenn er keine Verbindung zum bisherigen Access Point mehr aufrecht erhalten kann. Um das Roaming zu ermöglichen, muss sich mindestens ein weiterer Access Point in der Reichweite des Clients befinden, der ein Netzwerk mit der gleichen SSID und den passenden Radio- und Verschlüsselungs-Einstellungen anbietet.

Normalerweise würde der WLAN-Client sich nur dann bei einem anderen Access Point einbuchen, wenn er die Verbindung zu dem bisherigen Access Point vollständig verloren hat (Hard-Roaming). Das Soft-Roaming ermöglicht dem Client hingegen, anhand verfügbarer Scan-Informationen ein Roaming zu einem stärkeren Access Point durchzuführen. Mit der Funktion des Background-Scanning kann der LANCOM Wireless Router im Client-Modus schon vor Verbindungsverlust Informationen über andere verfügbare Access Points sammeln. Die Umschaltung auf einen anderen Access Point erfolgt dann nicht erst, wenn die bisherige Verbindung vollständig verloren wurde, sondern wenn ein anderer Access Point in Reichweite über ein stärkeres Signal verfügt.

① Zum Aktivieren des Soft-Roaming wechseln Sie unter WEBconfig oder Telnet in den Bereich Setup > Schnittstellen > WLAN > Roaming und wählen dort das physikalische WLAN-Interface.

② Schalten sie das Soft-Roaming ein und stellen sie ggf. die weiteren Parameter wie die Schwellwerte und Signalpegel ein.

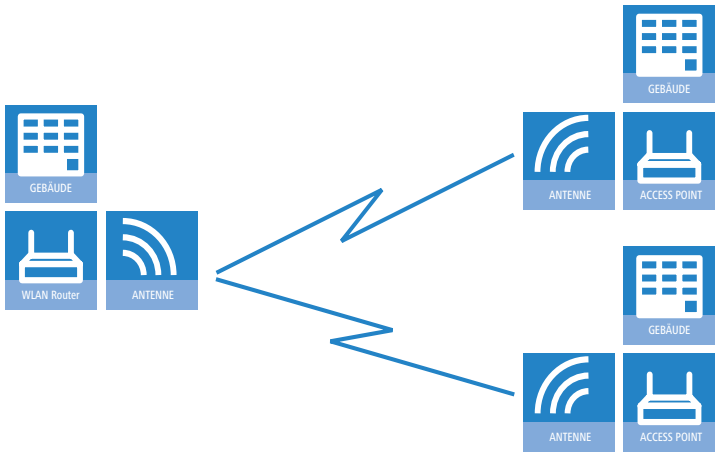
③ Zur Konfiguration des Background-Scanning wechseln Sie unter LANconfig bei den physikalischen WLAN-Einstellungen für das gewünschte WLAN-Interface auf die Registerkarte 'Radio'.



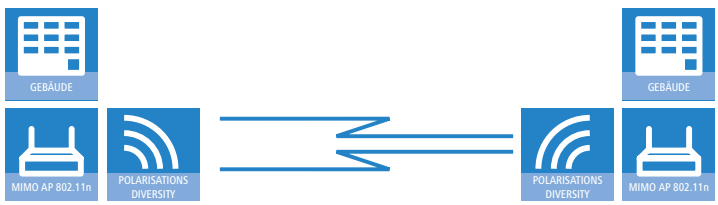
④ Tragen Sie als Background-Scan-Intervall die Zeit ein, in welcher der LANCOM Wireless Router zyklisch die aktuell ungenutzten Frequenzen des aktiven Bandes nach erreichbaren Access Points absucht. Um ein schnelles Roaming zu erzielen, wird die Scan-Zeit auf z.B. 260 Sekunden (2,4 GHz) bzw. 720 Sekunden (5 GHz) eingestellt.

11.7 Konfiguration der Punkt-zu-Punkt-Verbindungen

LANCOM Access Points 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 Access Points 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.



Je nachdem, welcher WLAN-Standard und welche WLAN-Antenne verwendet wird, können folgende Werte für den Datendurchsatz erzielt werden:

Access Point	Antenne	Datendurchsatz	Entfernung
802.11n Indoor AP	Richtantenne mit 9° Öffnungswinkel, Blitzschutz, 10m Kabel	Brutto 240Mbit/s	1km
802.11n Indoor AP	Richtantenne mit 9° Öffnungswinkel, Blitzschutz, 10m Kabel	Brutto 15Mbit/s	8,9km
802.11n Outdoor AP	Richtantenne mit 9° Öffnungswinkel, Blitzschutz, 2m Kabel	Brutto 240Mbit/s	2,1km
802.11n Outdoor AP	Richtantenne mit 9° Öffnungswinkel, Blitzschutz, 2m Kabel	Brutto 15Mbit/s	18km
802.11a Indoor AP	Richtantenne mit 9° Öffnungswinkel, Blitzschutz, 10m Kabel	Brutto 54Mbit/s	0,4km
802.11a Indoor AP	Richtantenne mit 9° Öffnungswinkel, Blitzschutz, 10m Kabel	Brutto 6Mbit/s	6km
802.11a Outdoor AP	Richtantenne mit 9° Öffnungswinkel, Blitzschutz, 2m Kabel	Brutto 54Mbit/s	1,3km
802.11a Outdoor AP	Richtantenne mit 9° Öffnungswinkel, Blitzschutz, 2m Kabel	Brutto 6Mbit/s	13km
802.11g Indoor AP	Richtantenne mit 30° Öffnungswinkel, Blitzschutz, 10m Kabel	Brutto 54Mbit/s	0,08km
802.11g Indoor AP	Richtantenne mit 30° Öffnungswinkel, Blitzschutz, 10m Kabel	Brutto 6Mbit/s	1km
802.11g Outdoor AP	Richtantenne mit 30° Öffnungswinkel, Blitzschutz, 2m Kabel	Brutto 54Mbit/s	0,28km
802.11g Outdoor AP	Richtantenne mit 30° Öffnungswinkel, Blitzschutz, 2m Kabel	Brutto 6Mbit/s	2,5km

Mit hochoptimierten Funkbrücken nach IEEE 802.11n können also auch über große Entferungen hohe Übertragungsraten erzielt werden.

Dieses Kapitel stellt die Grundlagen zur Auslegung von Point-to-Point-Strecken vor und gibt Hinweise zur Ausrichtung der Antennen.

11.7.1 Geometrische Auslegung von Outdoor-Funknetz-Strecken

Bei der Auslegung der Funkstrecken sind im Wesentlichen folgende Fragen zu beantworten:

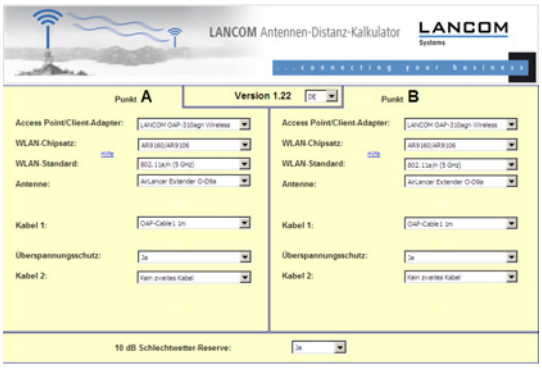
- Welche Antennen müssen für die gewünschte Anwendung eingesetzt werden?
- Wie müssen die Antennen positioniert werden, um eine einwandfreie Verbindung herzustellen?
- Welche Leistungen müssen die eingesetzten Antennen aufweisen, um einen ausreichenden Datendurchsatz innerhalb der gesetzlichen Grenzen zu gewährleisten?

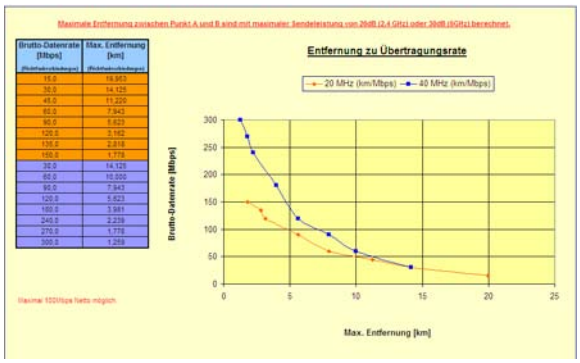
Auswahl der Antennen mit dem LANCOM Antennen-Kalkulator

Zur Berechnung der Ausgangsleistungen in den Access Points sowie der erreichbaren Distanzen und Datenraten können Sie den LANCOM Antennen-Kalkulator verwenden, den Sie zum Download auf unserer Webseite unter www.lancom.de finden.

Nach Auswahl der verwendeten Komponenten (Access Points, Antennen, Blitzschutz und Kabel) berechnet der Kalkulator neben Datenraten und Distanzen auch den Antennen-Gewinn, der in den Access Points 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.



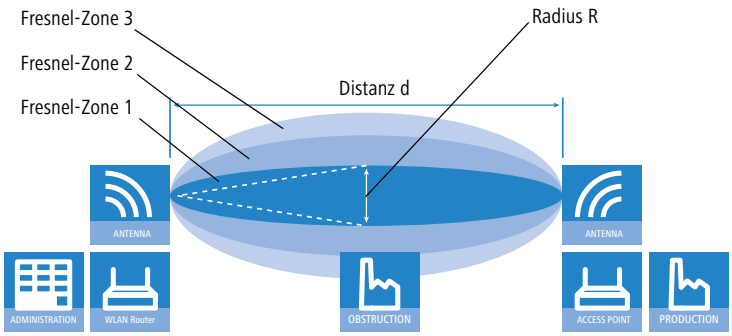


Positionierung der Antennen

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.

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 Systems ansonsten keine Garantie für Schäden an den LANCOM- und AirLancer-Komponenten übernehmen kann!

Informationen zur Installation von WLAN-Systemen im Outdoor-Einsatz finden Sie im 'LANCOM Outdoor Wireless Guide'.



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.

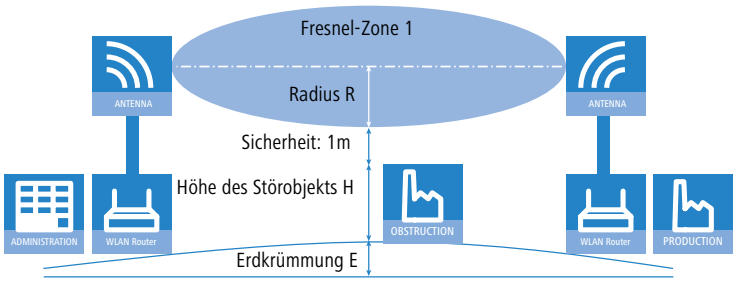
Der Radius (R) der Fresnel-Zone 1 berechnet sich bei gegebener Wellenlänge der Strahlung (λ) und der Distanz zwischen Sender und Empfänger (d) nach folgender Formel:

$R = 0{,}5 * \sqrt{(\lambda * d)}$

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)

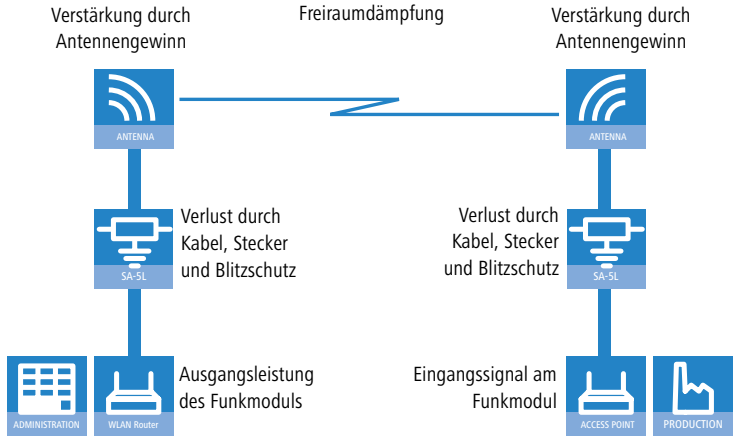
Die Höhe der Erdkrümmung (E) ergibt sich bei einer Distanz (d) zu E = d² * 0,0147 – bei einer Distanz von 8 km also immerhin schon fast 1m!

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**.

Antennen-Leistungen

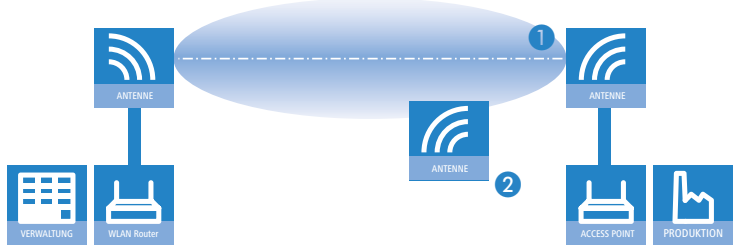
Die Leistungen der eingesetzten Antennen müssen so ausgelegt sein, dass eine ausreichende Datenübertragungsrate erreicht wird. Auf der anderen Seite dürfen die länderspezifischen gesetzlichen Vorgaben für die maximal abgestrahlten Leistungen nicht überschritten werden.

Die Berechnung der effektiven Leistungen führt dabei vom Funkmodul im sendenden Access Point bis zum Funkmodul im empfangenden Access Point. Dazwischen liegen dämpfende Elemente wie die Kabel, Steckverbindungen oder einfach die übertragende Luft und verstärkende Elemente wie die externen Antennen.



11.7.2 Ausrichten der Antennen für den P2P-Betrieb

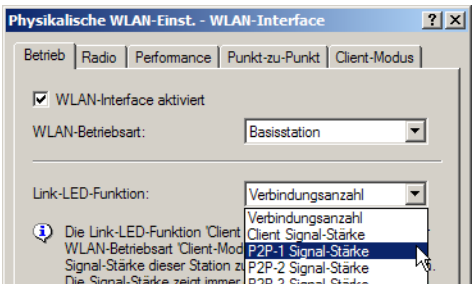
Beim Aufbau von P2P-Strecken kommt der genauen Ausrichtung der Antennen eine große Bedeutung zu. Je besser die empfangende Antenne in der „Ideallinie" der sendenden Antenne liegt, desto besser ist die tatsächliche Leistung und damit die nutzbare Bandbreite (1). Liegt die empfangende Antenne jedoch deutlich neben dem idealen Bereich, sind erhebliche Leistungsverluste zu erwarten (2).



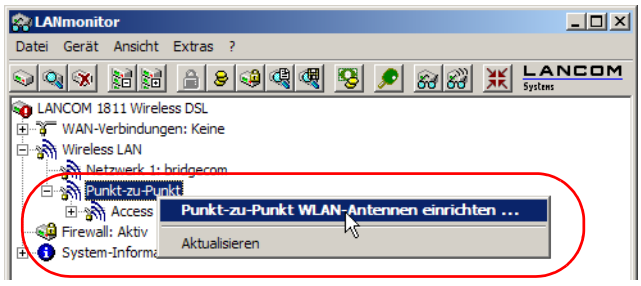
Weitere Informationen zur geometrischen Auslegung von Funkstrecken und zur Ausrichtung der Antennen mit Hilfe der LANCOM-Software finden Sie im LCOS-Referenzhandbuch.

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 ...'

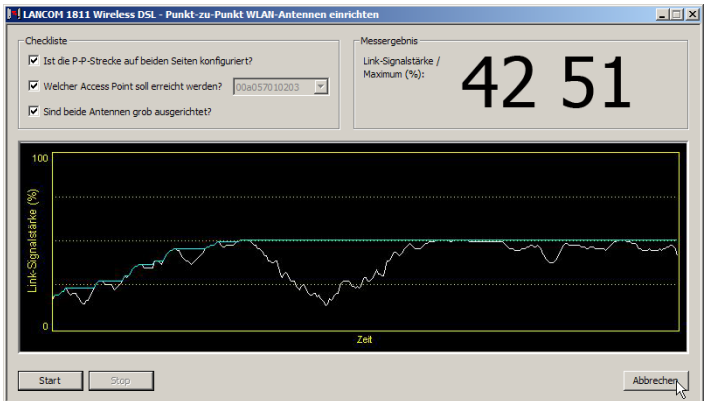


Der Eintrag 'Punkt-zu-Punkt' ist im LANmonitor nur sichtbar, wenn in dem überwachten Gerät mindestens eine Basisstation als Gegenstelle für eine P2P-Verbindung eingerichtet ist (LANconfig: **Wireless LAN ▶ Allgemein ▶ Physikalische WLAN-Einstellungen ▶ Punkt-zu-Punkt**).

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 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 erzielen.

11.7.3 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 Techpaper „Performance von P2P-Verbindungen im Outdoor-Bereich" als Download auf www.lancom.de.

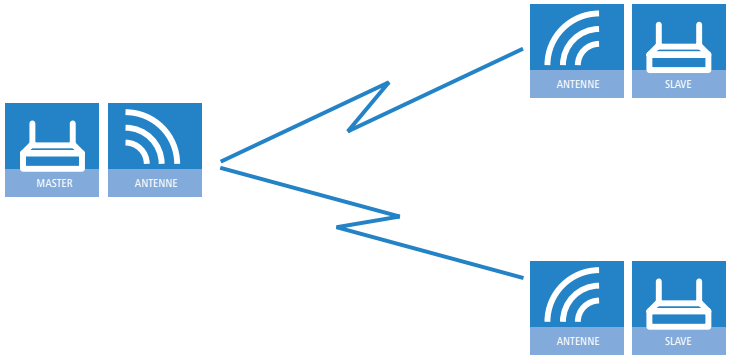
11.7.4 Punkt-zu-Punkt-Betriebsart aktivieren

Das Verhalten eines Access Points beim Datenaustausch mit anderen Access Points wird in der „Punkt-zu-Punkt-Betriebsart" festgelegt:

- **Aus:** Der Access Point kann nur mit mobilen Clients kommunizieren
- **An:** Der Access Point kann mit anderen Basis-Stationen und mit mobilen Clients kommunizieren
- **Exklusiv:** Der Access Point 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 Access Points kommen, die sich in der Folge gegenseitig nicht finden. Diese Pattsituationen kann mit dem geeigneten „Kanalwahlverfahren" verhindert werden:

- **Master:** Dieser Access Point übernimmt die Führung bei der Auswahl eines freien WLAN-Kanals.
- **Slave:** Alle anderen Access Points suchen solange nach dem freien Kanal, bis sie einen sendenden Master gefunden haben.



Es ist daher empfehlenswert, im 5 GHz-Band jeweils einen zentralen Access Point 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).

11.7.5 Konfiguration der P2P-Verbindungen

Bei der Konfiguration der Punkt-zu-Punkt-Verbindungen werden neben der Punkt-zu-Punkt-Betriebsart und dem Kanalwahlverfahren die MAC-Adressen oder die Stationsnamen der Gegenstellen eingetragen.

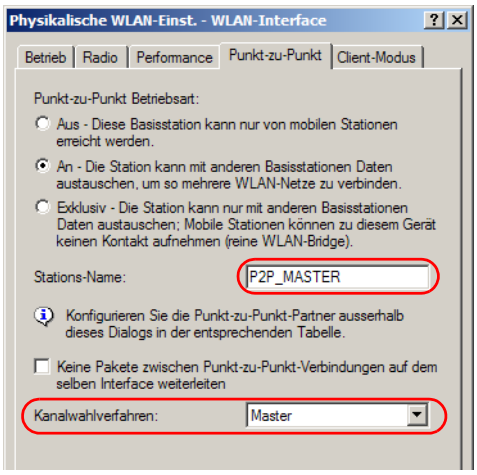
Bei der Konfiguration mit LANconfig finden Sie die Einstellungen für die P2P-Verbindungen im Konfigurationsbereich 'Interfaces' auf der Registerkarte 'Wireless LAN'.

Die Konfiguration der P2P-Verbindungen kann auch mit dem WLAN-Assistenten von LANconfig erfolgen.

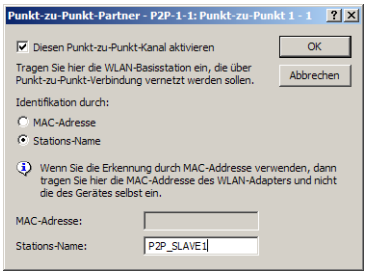
① Öffnen Sie mit der Schaltfläche **Physikalische WLAN-Einst.** die Optionen für das entsprechende WLAN-Interface und wechseln Sie dort auf die Registerkarte 'Punkt-zu-Punkt'.

② Aktivieren Sie hier die geeignete Punkt-zu-Punkt-Betriebsart und stellen Sie als Kanalwahlverfahren entweder 'Master' oder 'Slave' ein. Wenn die Gegenstellen der P2P-Verbindungen über den Stationsnamen identifiziert werden sollen, tragen Sie einen eindeutigen Namen für diese WLAN-Station ein.

Bei Modellen mit mehreren WLAN-Modulen kann der Stationsname für jede physikalische WLAN-Schnittstelle separat eingetragen werden.

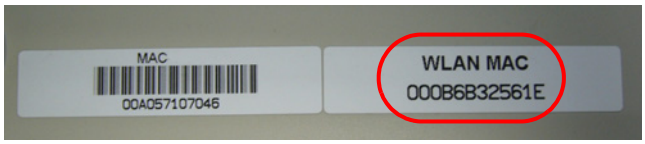


③ Schließen Sie die physikalischen WLAN-Einstellungen und öffnen Sie die Liste der **Punkt-zu-Punkt-Partner**. Tragen Sie zu jeder der maximal sechs P2P-Verbindungen entweder die jeweiligen MAC-Adressen der WLAN-Karte auf der Gegenseite ein oder den Namen der entsprechenden WLAN-Station (je nach Wahl der Identifizierung).



Bitte beachten Sie, hier nur die MAC-Adressen der WLAN-Karten auf der anderen Seite der Verbindung einzutragen! Nicht die eigenen MAC-Adressen und nicht die MAC-Adressen von anderen Interfaces, die möglicherweise in den Basisstationen vorhanden sind.

Sie finden die WLAN-MAC-Adresse auf einem Aufkleber, der unterhalb des jeweiligen Antennenanschlusses 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!



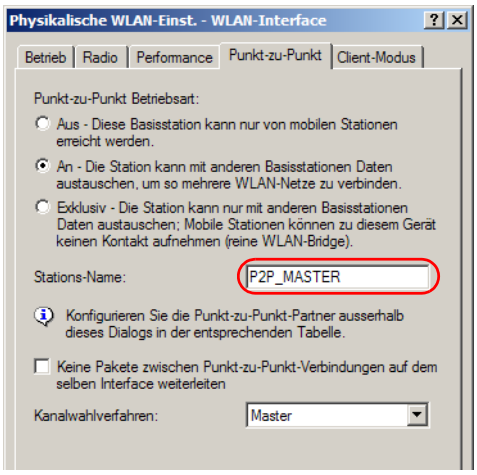
Point-to-Point-Gegenstellen über Stationsnamen anbinden

Bei der Konfiguration der Punkt-zu-Punkt-Verbindungen kann alternativ zu den MAC-Adressen auch der Stationsnamen der Gegenstellen verwendet werden.

Der Stationsname wird zunächst in den Punkt-zu-Punkt-Einstellungen der Wireless Router oder Access Points definiert.

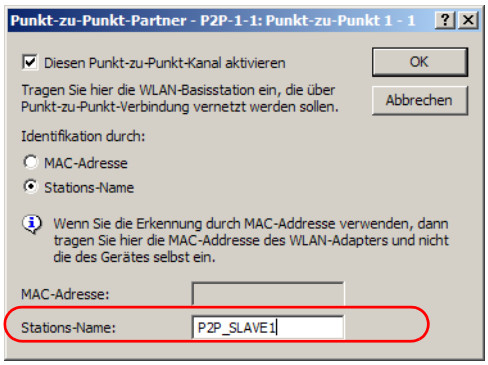
- LANconfig: **Wireless LAN ▶ Allgemein ▶ Physikalische WLAN-Einst. ▶ Punkt-zu-Punkt**
- WEBconfig: **Setup ▶ Schnittstellen ▶ WLAN Interpoint-Einstellungen**

Bei Modellen mit mehreren WLAN-Modulen kann der Stationsname für jede physikalische WLAN-Schnittstelle separat eingetragen werden.



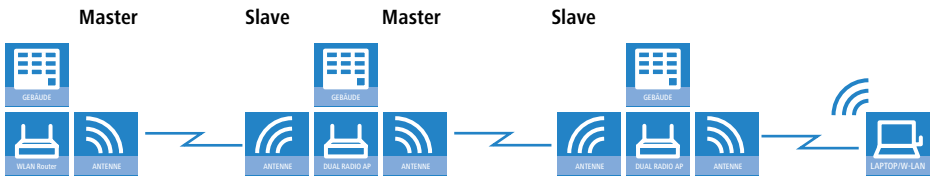
Bei der Konfiguration der Punkt-zu-Punkt-Verbindungn wird dann die Identifikation durch Stationsnamen gewählt, dazu wird der Name der entsprechenden Station eingetragen.

- LANconfig: **Wireless LAN ▶ Allgemein ▶ Punkt-zu-Punkt-Partner**
- WEBconfig: **Setup ▶ Schnittstellen ▶ WLAN Interpoint-Gegenstellen**



11.7.6 Access Points im Relais-Betrieb

Access Points 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.

11.7.7 Sicherheit von Punkt-zu-Punkt-Verbindungen

Mit IEEE 802.11i kann auch die Sicherheit auf Punkt-zu-Punkt-Verbindungen im WLAN deutlich verbessert werden. 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 (LEPS).

Verschlüsselung mit 802.11i/WPA

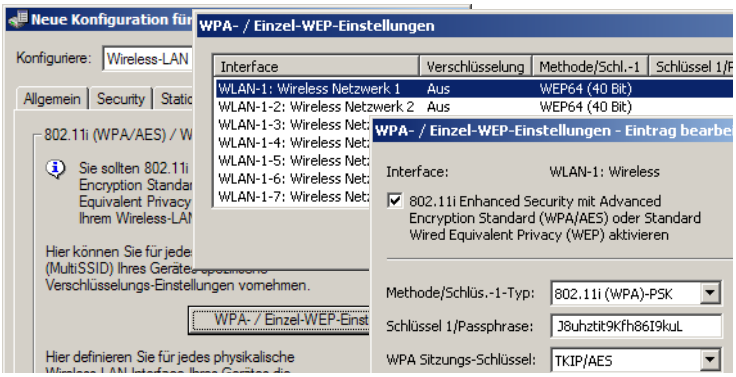
Zum Aktivieren der 802.11i-Verschlüsselung auf einer korrekt konfigurierten P2P-Verbindung passen Sie die Einstellungen für das erste logische WLAN-Netzwerk im verwendeten WLAN-Interface an (also WLAN-1, wenn Sie das erste WLAN-Modul für die P2P-Verbindung nutzen , WLAN-2 wenn Sie das zweite WLAN-Modul z.B. bei einem Access Point mit zwei WLAN-Modulen nutzen).

- Aktivieren Sie die 802.11i-Verschlüsselung.
- Wählen Sie als Methode '802.11i (WPA)-PSK' aus.
- Geben Sie die verwendete Passphrase ein.

Verwenden Sie als Passphrase zufällige Zeichenketten von mindestens 32 Zeichen Länge.

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 Access Point diese Informationen an die Gegenseite, um sich dort anzumelden.

Bei der Konfiguration mit LANconfig finden Sie die Verschlüsselungs-Einstellungen im Konfigurationsbereich 'Wireless-LAN' auf der Registerkarte '802.11i/WEP'.

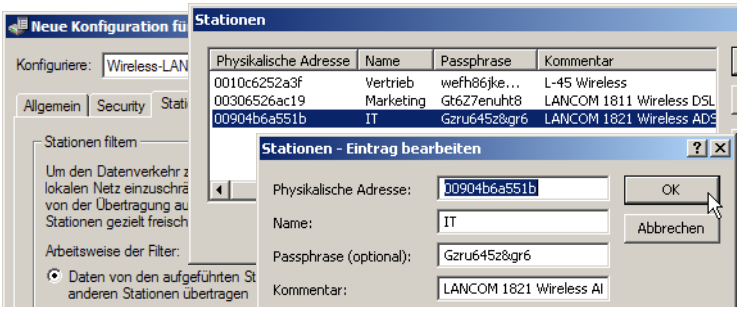


LEPS für P2P-Verbindungen

Einen weiteren Sicherheitsgewinn erzielen Sie durch die zusätzliche Verwendung der LANCOM Enhanced Passphrase Security (LEPS), also der Verknüpfung der MAC-Adresse mit der Passphrase.

Mit LEPS können einzelne Punkt-zu-Punkt-Strecken (P2P) mit einer individuellen Passphrase abgesichert werden. Wenn bei einer P2P-Installation ein Access Point entwendet wird und dadurch Passphrase und MAC-Adresse bekannt werden, sind alle anderen per LEPS 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.



11.8 Zentrales WLAN-Management

Der weit verbreitete Einsatz von Wireless Access Points 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 Wireless Access Points benötigen eine Konfiguration und ein entsprechendes Monitoring zur Erkennung von unerwünschten WLAN-Clients etc. Die Administration der Access Points 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 Access Points 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 Access Points notwendig, um Frequenzüberlagerungen zu vermeiden und die Netzwerkperformance zu optimieren.
- Access Points 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 Access Points mit dem LAN verbunden werden und so die geltenden Sicherheitsrichtlinien umgehen.

Mit einem zentralen WLAN-Management werden diese Probleme gelöst. Die Konfiguration der Access Points wird dabei nicht mehr in den Geräten selbst vorgenommen, sondern in einer zentralen Instanz, dem WLAN-Controller. Der WLAN-Controller authentifiziert die Access Points 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 Access Points aus. Da die vom WLAN-Controller zugewiesene Konfiguration in den Access Points 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" ('Autarker Weiterbetrieb' → Seite 11-67) wird die Konfiguration für eine definierte Zeit optional im Flash gespeichert (in einem Bereich, der nicht mit LANconfig oder anderen Tools auszulesen ist).

11.8.1 Der CAPWAP-Standard

Mit dem CAPWAP-Protokoll (Control And Provisioning of Wireless Access Points) stellt die IETF (Internet Engineering Task Force) einen Draft-Standard für das zentrale Management großer WLAN-Strukturen vor.

CAPWAP verwendet zwei Kanäle für die Datenübertragung:

- Kontrollkanal, verschlüsselt mit DTLS. Über diesen Kanal werden die Verwaltungsinformationen zwischen dem WLAN-Controller und dem Access Point ausgetauscht.



Das Datagram Transport Layer Security (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.

- Datenkanal, optional ebenfalls verschlüsselt mit DTLS. Über diesen Kanal werden die Nutzdaten aus dem WLAN vom Access Point über den WLAN-Controller ins LAN übertragen – gekapselt in das CAPWAP-Protokoll.

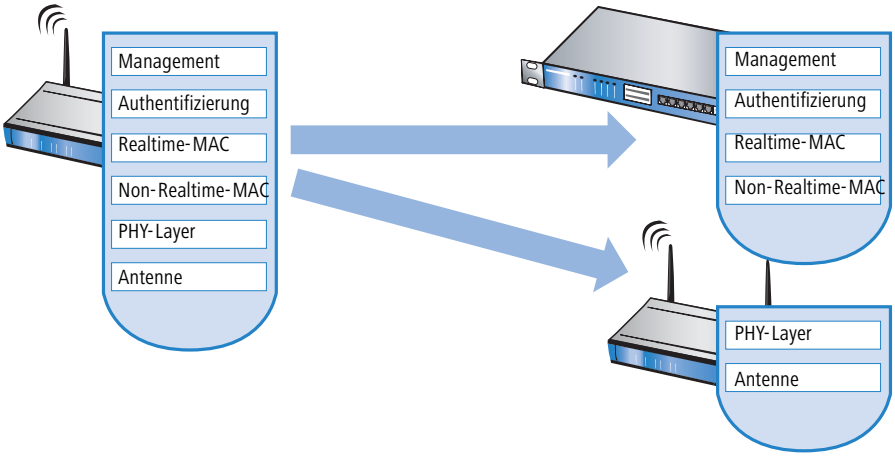
11.8.2 Die Smart-Controller-Technologie

In einer dezentralen WLAN-Struktur mit autonomen Access Points (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 Access Points enthalten. Mit dem zentralen WLAN-Management werden diese Aufgaben auf zwei verschiedene Geräte aufgeteilt:

- Der zentrale WLAN-Controller übernimmt die Verwaltungsaufgaben.
- Die verteilten Access Points 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).

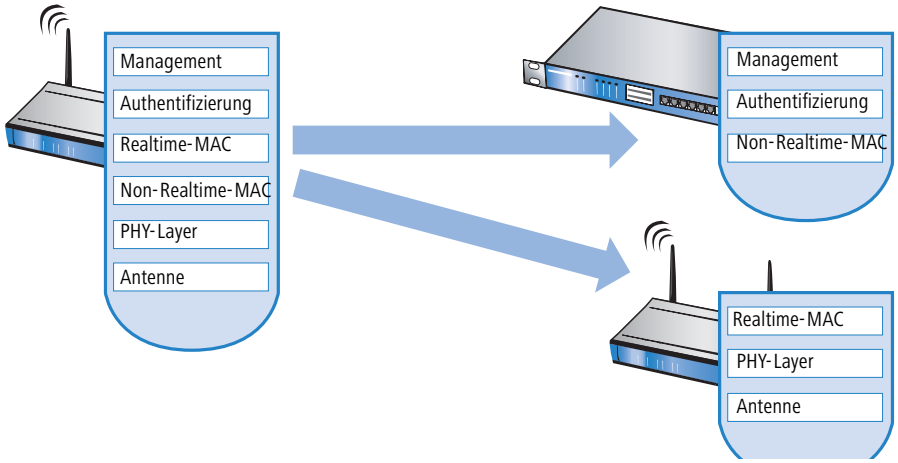
CAPWAP beschreibt drei unterschiedliche Szenarien für die Verlagerung von WLAN-Funktionen in den zentralen WLAN-Controller.

- Remote-MAC: Hier werden alle WLAN-Funktionen vom Access Point an den WLAN-Controller übertragen. Die Access Points dienen hier nur als „verlängerte Antennen" ohne eigene Intelligenz.

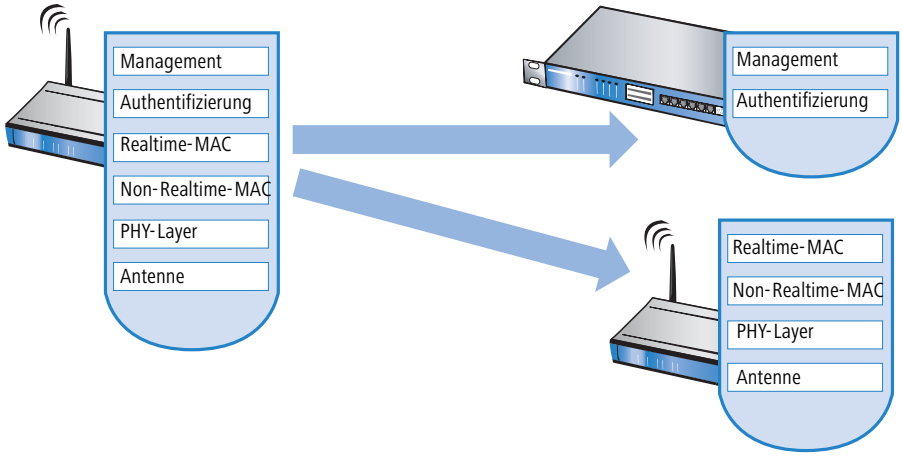


- Split-MAC: Bei dieser Variante wird nur ein Teil der WLAN-Funktionen an den WLAN-Controller übertragen. Üblicherweise werden die zeitkritischen Anwendungen (Realtime-Applikationen) weiterhin auf dem Access Point

abgearbeitet, die nicht zeitkritischen Anwendungen (Non-Realtime-Applikationen) werden über den zentralen WLAN-Controller abgewickelt.



- Local-Mac: Die dritte Möglichkeit sieht eine vollständige Verwaltung und Überwachung des WLAN-Datenverkehrs direkt in den Access Points vor. Zwischen dem Access Point und dem WLAN-Controller werden lediglich Nachrichten zur Sicherung einer einheitlichen Konfiguration der Access Points und zum Management des Netzwerks ausgetauscht.



Die Smart-Controller-Technologie von LANCOM Systems setzt das Local-MAC-Verfahren ein. Durch die Reduzierung der zentralisierten Aufgaben bieten die WLAN-Strukturen eine optimale Skalierbarkeit. Gleichzeitig wird der WLAN-Controller 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 WLAN-Controller laufen. In Local-MAC-Architekturen können die Daten jedoch alternativ auch direkt von den Access Points in das LAN ausgekoppelt werden, sodass eine hochperformante Datenübertragung ermöglicht wird. WLAN-Controller von LANCOM eignen sich daher auch für WLANs nach dem Draft Standard IEEE 802.11n mit deutlich höheren Bandbreiten als in den bisher bekannten WLANs. 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.

CAPWAP-Tunneling und Layer-3-Roaming

In einer späteren LCOS-Version unterstützen die LANCOM WLAN Controller auch die Übertragung der Nutzdaten durch einen CAPWAP-Tunnel.

- Auf diese Weise können z.B. ausgewählte Applikationen wie VoIP über den zentralen WLAN-Controller geleitet werden. Beim Wechsel der WLAN-Clients in eine andere Funkzelle bleibt so die zugrundeliegende IP-Verbindung ohne Unterbrechung, da sie fortlaufend vom zentralen WLAN-Controller 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 WLAN-Controller verwaltet werden.

11.8.3 Kommunikation zwischen Access Point und WLAN-Controller

Ab der Firmware-Version LCOS 7.20 unterscheiden sich LANCOM Access Points (z. B. LANCOM L-54ag) und LANCOM Wireless Router (z. B. LANCOM 1811 Wireless) bzgl. der Einstellung der WLAN-Module im Auslieferungszustand. In den folgenden Beschreibungen wird meistens der übergreifende Begriff „Access Point" verwendet.

Die Kommunikation zwischen einem Access Point und dem WLAN-Controller wird immer vom Access Point aus eingeleitet. Die Geräte suchen in folgenden Fällen nach einem WLAN-Controller, der ihnen eine Konfiguration zuweisen kann:

- Ein LANCOM Access Point befindet sich im Auslieferungszustand und ist noch nicht konfiguriert. In diesem Zustand sind die WLAN-Module ausgeschaltet, der Access Point sucht im LAN nach einem WLAN-Controller.
- Ein LANCOM Access Point ist bereits konfiguriert, für mindestens ein WLAN-Modul ist manuell die Betriebsart auf 'Managed' eingestellt ('Konfiguration der Access Points' → Seite 11-79). Der Access Point sucht für das oder die entsprechenden WLAN-Module im LAN nach einem WLAN-Controller.
- Ein LANCOM Wireless Router ist bereits konfiguriert, für mindestens ein WLAN-Modul ist manuell die Betriebsart auf 'Managed' eingestellt. Der Wireless Router sucht für das oder die entsprechenden WLAN-Module im LAN nach einem WLAN-Controller.

Der Access Point sendet zu Beginn der Kommunikation eine „Discovery Request Message", um die verfügbaren WLAN-Controller zu ermitteln. Dieser Request wird grundsätzlich als Broadcast versendet. Da in manchen Strukturen ein potenzieller WLAN-Controller aber nicht über Broadcast zu erreichen ist, können auch spezielle Adressen von weiteren WLAN-Controllers in die Konfiguration der Access Points eingetragen werden.

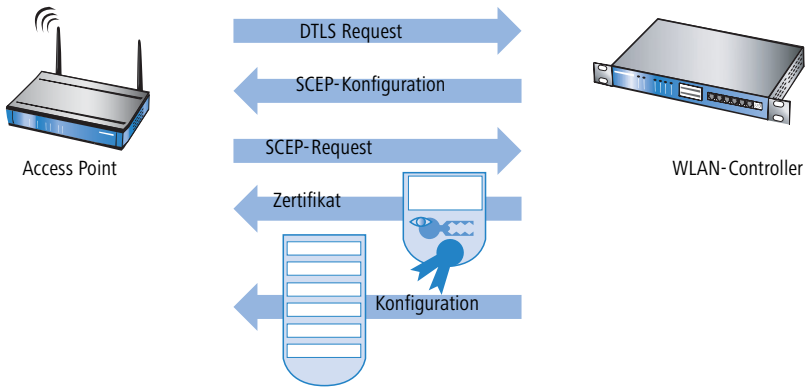
Außerdem können auch DNS-Namen von WLAN-Controllern aufgelöst werden. Alle Access Points mit LCOS 7.22 oder höher haben den Standardnamen 'WLC-Address' bereits konfiguriert, sodass ein DNS-Server diesen Namen zu einem LANCOM WLAN Controller auflösen kann. Gleiches gilt auch für die über DHCP gelernten DHCP-Suffixe. Somit können auch WLAN-Controller erreicht werden, die nicht im gleichen Netz stehen, ohne die Access Points konfigurieren zu müssen.

Aus den verfügbaren WLAN-Controllern wählt der Access Point den Besten aus und fragt bei diesem nach dem Aufbau der DTLS-Verbindung an. Der „beste" WLAN-Controller ist für den Access Point derjenige mit der geringsten Auslastung, also dem kleinsten Verhältnis von gemanagten Access Points zu den maximal möglichen Access Points. Bei zwei oder mehreren gleich „guten" WLAN-Controllern wählt der Access Point den im Netzwerk nächsten, also den mit der geringsten Antwortzeit.

Der WLAN-Controller ermittelt daraufhin mit einer internen Zufallszahl einen eindeutigen und sicheren Sitzungsschlüssel, mit dem er die Verbindung zum Access Point schützt. Die CA im WLAN-Controller stellt dem Access Point Zertifikat mittels SCEP aus. Das Zertifikat ist mit einem Kennwort für einmalige Verwendung als „Challenge" gesichert, der Access Point kann sich mit diesem Zertifikat gegenüber dem WLAN-Controller für die Abholung des Zertifikats authentifizieren.

Über die gesicherte DTLS-Verbindung wird dem Access Point die Konfiguration für den integrierten SCEP-Client mitgeteilt – der Access Point kann dann über SCEP sein Zertifikat bei der SCEP-CA abholen. Anschließend wird die dem Access Point zugewiesene Konfiguration übertragen.

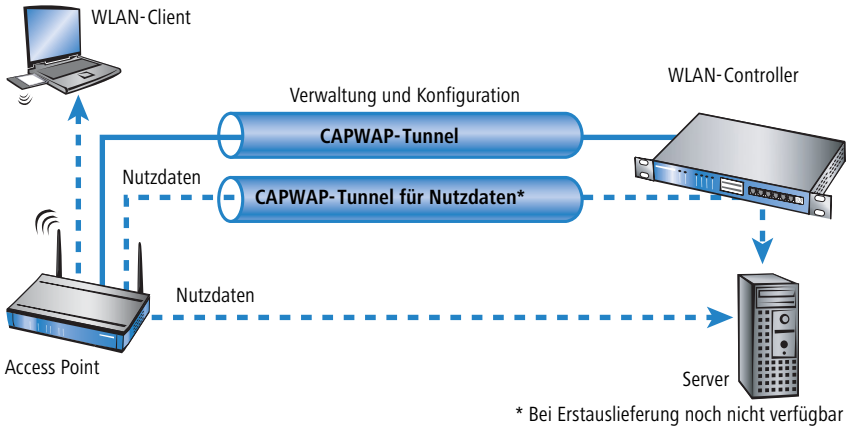
SCEP steht für Simple Certificate Encryption Protocol, CA für Certification Authority.



Sowohl Authentifizierung als auch Konfiguration können entweder automatisch vorgenommen werden oder nur bei passendem Eintrag der MAC-Adresse des Access Point in der AP-Tabelle des WLAN-Controller. Sofern bei dem

Access Point 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 Access Point direkt in das LAN ausgekoppelt und z. B. an den Server übertragen.



11.8.4 Zero-Touch-Management

Mit der Möglichkeit, den anfragenden Access Points Zertifikat und Konfigurationen automatisch zuweisen zu lassen, realisieren die LANCOM WLAN Controller ein echtes „Zero-Touch-Management". Neue Access Points müssen nur noch mit dem LAN verbunden werden, es sind keine weiteren Konfigurationsschritte 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.

11.8.5 Split-Management

LANCOM Access Points können ihren WLAN-Controller auch in entfernten Netzen suchen – eine einfache IP-Verbindung z. B. über eine VPN-Strecke reicht aus. Da die WLAN-Controller nur den WLAN-Teil der Konfiguration im Access Point beeinflussen, können alle anderen Funktionen separat verwaltet werden. Durch diese Aufteilung der Konfigurationsaufgaben können LANCOM WLAN Controller ideal für den Aufbau einer firmenweiten WLAN-Infrastruktur in der Zentrale inklusive aller angeschlossenen Niederlassungen und Home-Offices eingesetzt werden.

11.8.6 Allgemeine Einstellungen

Die meisten Parameter zur Konfiguration der LANCOM 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.

In diesem Bereich nehmen sie die Basiseinstellungen für Ihren WLAN-Controller vor.

- **Automatische Annahme neuer APs (Auto-Accept)**

  Ermöglicht dem WLAN-Controller, allen neuen Access Points eine Konfiguration zuzuweisen, auch wenn diese nicht über ein gültiges Zertifikat verfügen.

  Ermöglicht dem WLAN-Controller, allen neuen Access Points **ohne** gültiges Zertifikat ein solches Zertifikat zuzuweisen. Dazu muss eine der beiden Bedingungen erfüllt sein:

  - □ Für den Access Point 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 WLAN-Controller, allen neuen Access Points (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 LANCOM WLAN Controller alle im LAN gefundenen Access Points im Managed-Modus automatisch in die von ihm verwaltete WLAN-Struktur aufnehmen (bis zur maximalen Anzahl der auf einem WLAN-Controller verwalteten Access Points). Per Default aufgenommene Access Points werden auch in die MAC-Liste aufgenommen.

Mit dieser Option können möglicherweise auch unbeabsichtigte Access Points 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 Access Points abdecken:

Auto-Accept	Default-Konfiguration	Geeignet für
Ein	Ein	Rollout-Phase: Verwenden Sie diese Kombination nur dann, wenn **keine Access Points 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 Access Points 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 Access Points ohne Zustimmung der Administratoren in die WLAN-Struktur aufgenommen.

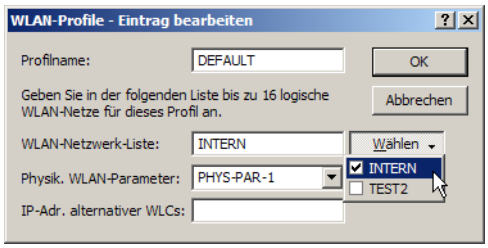
11.8.7 Profile

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.

WLAN-Profile

In den WLAN-Profilen werden die Einstellungen zusammengefasst, die den Access Points zugewiesen werden. Die Zuordnung der WLAN-Profile zu den Access Points erfolgt in der AP-Tabelle.

Für jedes WLAN-Profil können Sie die folgenden Parameter definieren:



LANconfig: WLAN-Controller ▶ Profile ▶ WLAN-Profile

WEBconfig: LCOS-Menübaum ▶ Setup ▶ WLAN-Management ▶ AP-Konfiguration ▶ Gesamtprofile

- **Profil-Name**

  Name des Profils, unter dem die Einstellungen gespeichert werden.

- **WLAN-Netzwerk-Liste**

  Liste der logischen WLAN-Netzwerke, die über dieses Profil zugewiesen werden.

Die Access Points nutzen aus dieser Liste nur die ersten acht Einträge, die mit der eigenen Hardware kompatibel sind. Somit können in einem Profil z. B. jeweils acht WLAN-Netzwerke für reinen 2,4 GHz-Betrieb und acht für reinen 5 GHz-Betrieb definiert werden. Für jeden LANCOM Access Point – sowohl Modelle mit 2,4 GHz- als auch die mit 5 GHz-Unterstützung – stehen damit die maximal möglichen acht logischen WLAN-Netzwerke zur Verfügung.

- **Physikalische WLAN-Parameter**

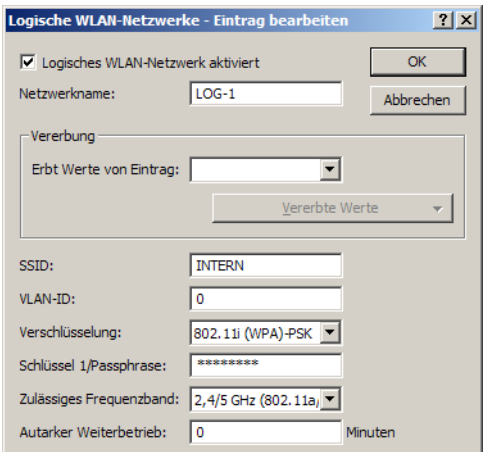
  Ein Satz von physikalischen Parametern, mit denen die WLAN-Module der Access Points arbeiten sollen.

- **IP-Adresse alternativer WLAN-Controller**

  Liste der WLAN-Controller, bei denen der Access Point eine Verbindung versuchen soll. Der Access Point leitet die Suche nach einem WLAN-Controller über einen Broadcast ein. Wenn nicht alle WLAN-Controller über einen solchen Broadcast erreicht werden können (WLAN-Controller steht z. B. in einem anderen Netz), dann ist die Angabe von alternativen WLAN-Controllern sinnvoll.

Logische WLAN-Netzwerke

Hier werden die logischen WLAN-Netzwerke eingestellt, die den Access Points zugewiesen werden. Für jedes logische WLAN-Netzwerk können Sie die folgenden Parameter definieren:



LANconfig: WLAN-Controller ▶ Profile ▶ Logische WLAN-Netzwerke

WEBconfig: LCOS-Menübaum ▶ Setup ▶ WLAN-Management ▶ AP-Konfiguration ▶ Netzwerkprofile

■ **Netzwerkname**

Name des logischen WLAN-Netzwerks, unter dem die Einstellungen gespeichert werden. Dieser Name wird nur für die interne Verwaltung der logischen Netze verwendet.

■ **Vererbung**

Auswahl eines schon definierten logischen WLAN-Netzwerks, von dem die Einstellungen übernommen werden sollen ('Vererbung von Parametern' → Seite 11-73).

■ **SSID**

Service Set Identifier – unter diesem Namen wird das logische WLAN-Netzwerk für die WLAN-Clients angeboten.

■ **VLAN-ID**

VLAN-ID für dieses logische WLAN-Netzwerk ('Dynamische VLAN-Zuweisung' → Seite 11-76).

Bitte beachten Sie, dass für die Nutzung der VLAN-IDs in einem logischen WLAN-Netzwerk die Einstellung einer Management-VLAN-ID ('Management-VLAN-ID' → Seite 11-68) erforderlich ist! Mit der Definition einer VLAN-ID für ein WLAN-Profil wird auf den damit verwalteten Access Points automatisch das VLAN-Modul eingeschaltet.

■ **Autarker Weiterbetrieb**

Zeit in Minuten, für die der Access Point im Managed-Modus mit seiner aktuellen Konfiguration weiterarbeitet.

Die Konfiguration wird dem Access Point vom WLAN-Controller zugewiesen und optional im Flash gespeichert (in einem Bereich, der nicht mit LANconfig oder anderen Tools auszulesen ist). Falls die Verbindung zum WLAN-Controller unterbrochen wird, arbeitet der Access Point für die hier eingestellte Zeit mit seiner Konfiguration aus dem Flash weiter. Auch nach einem eigenen Stromausfall kann der Access Point mit der Konfiguration aus dem Flash weiterarbeiten.

Wenn die eingestellte Zeit abgelaufen ist und die Verbindung zum WLAN-Controller noch nicht wiederhergestellt wurde, wird die Konfiguration im Flash gelöscht – der Access Point stellt seinen Betrieb ein. Sobald der WLAN-Controller wieder erreichbar ist, wird die Konfiguration erneut vom WLAN-Controller zum Access Point übertragen.

Durch diese Option kann der Access Point auch dann weiter arbeiten, wenn die Verbindung zum WLAN-Controller kurzfristig unterbrochen wird. Außerdem stellt diese Maßnahme einen wirksamen Schutz gegen Diebstahl dar, da die sicherheitsrelevanten Parameter der Konfiguration nach Ablauf der eingestellten Zeit automatisch gelöscht werden.

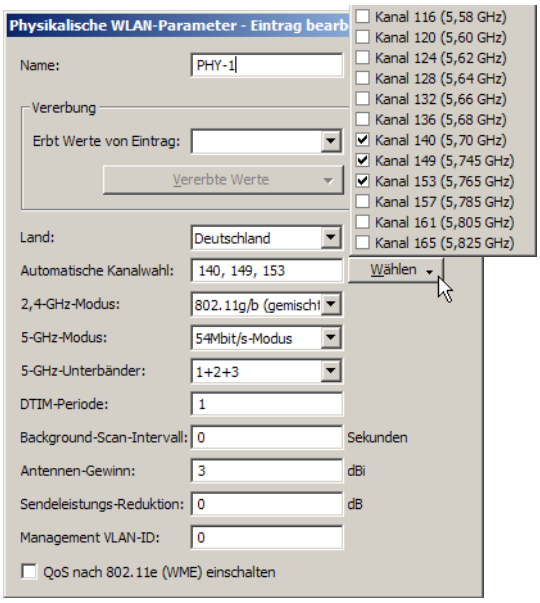
Stellt der Access Point im Backupfall eine Verbindung zu einem sekundären WLAN-Controller her, so wird der Ablauf der Zeit für den autarken Weiterbetrieb unterbrochen ('Backup mit primären und sekundären WLAN-Controllern' → Seite 11-78). Der Access Point bleibt also mit seinen WLAN-Netzwerken auch über diese eingestellte Zeit hinaus aktiv, solange er eine Verbindung zu einem WLAN-Controller hat.

Bitte beachten sie, dass die Konfigurationsdaten im Flash erst nach Ablauf der eingestellten Zeit für den autarken Weiterbetrieb gelöscht werden, nicht jedoch durch die Trennung vom Stromnetz!

Alle weiteren Parameter der WLAN-Netzwerke entsprechen denen der üblichen Konfiguration für Access Points.

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 die folgenden Parameter definieren:



LANconfig: WLAN-Controller ▶ Profile ▶ Physikalische WLAN-Parameter

WEBconfig: LCOS-Menübaum ▶ Setup ▶ WLAN-Management ▶ AP-Konfiguration ▶ Radioprofile

- **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 ('Vererbung von Parametern' → Seite 11-73).

- **Land**

  Land, in dem die Access Points betrieben werden sollen. Aufgrund dieser Information werden landesspezifische Einstellungen wie die erlaubten Kanäle etc. festgelegt.

- **Automatische Kanalwahl**

  Standardmäßig können die Access Points alle Kanäle nutzen, die aufgrund der Ländereinstellung erlaubt sind. Um die Auswahl auf bestimmte Kanäle zu beschränken, können hier die gewünschten Kanäle als kommaseparierte Liste eingetragen werden. Dabei ist auch die Angabe von Bereichen (z.B. '1,6,11') möglich.

- **Management-VLAN-ID**

  Die VLAN-ID, die für das Management-Netz der Access Points verwendet wird.

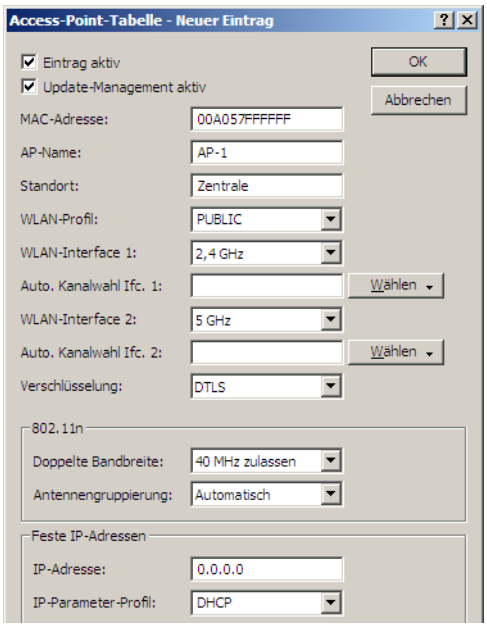
Die Management-VLAN-ID **muss** auf einen Wert ungleich null eingestellt werden, um VLANs auf den WLAN-Netzwerken nutzen zu können. Das gilt auch dann, wenn das Management-Netz selbst nicht mit VLAN-IDs getaggt werden soll (Mgmt-VLAN-ID = 1).

Die VLAN-Aktivierung gilt jeweils nur für diejenigen WLAN-Netzwerke, die mit diesen physikalischen WLAN-Parametern verbunden sind.

Alle weiteren physikalischen WLAN-Parameter entsprechen denen der üblichen Konfiguration für Access Points.

11.8.8 Liste der Access Points

Die AP-Tabelle ist ein zentraler Aspekt der Konfiguration für WLAN-Controller. Hier werden den Access Points über ihre MAC-Adresse WLAN-Profile (also Kombinationen aus logischen und physikalischen WLAN-Parametern) zugeordnet. Außerdem hat die reine Existenz eines Eintrags in der AP-Tabelle für einen bestimmten Access Point Auswirkungen auf die Möglichkeit, eine Verbindung zu einem WLAN-Controller aufbauen zu können. Für jeden Access Point können Sie die folgenden Parameter definieren:



LANconfig: WLAN-Controller ▶ AP-Konfig. ▶ Access-Point-Tabelle

WEBconfig: LCOS-Menübaum ▶ Setup ▶ WLAN-Management ▶ AP-Konfiguration ▶ Basisstationen

- **Update-Management aktiv**

  Wenn Sie für den Access-Point das Update-Management aktivieren, können neue Firmware- oder Script-Versionen automatisch geladen werden. Nehmen Sie alle weiteren Einstellungen unter AP-Update vor.

- **MAC-Adresse**

  MAC-Adresse des Access Points.

- **AP-Name**

  Name des Access Point im Managed-Modus.

- **Standort**

  Standort des Access Point im Managed-Modus.

- **WLAN-Profil**

  WLAN-Profil aus der Liste der definierten Profile ('WLAN-Profile' → Seite 11-66).

- **WLAN-Interface 1**

  Frequenzband für das erste WLAN-Modul. Mit diesem Parameter kann das WLAN-Modul auch deaktiviert werden.

- **Auto. Kanalwahl Ifc 1**

  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. 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.

- **WLAN-Interface 2**

  Frequenzband für das zweite WLAN-Modul. Mit diesem Parameter kann das WLAN-Modul auch deaktiviert werden.

- **Auto. Kanalwahl Ifc 2**

  Automatische Kanalwahl für das zweite WLAN-Modul.



Die Einstellungen für das zweite WLAN-Modul werden ignoriert, wenn das verwaltete Gerät nur über ein WLAN-Modul verfügt.

- **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.

- **Doppelte Bandbreite**

  Für LANCOM Access Points nach IEEE 802.11n kann hier die Nutzung der doppelten Bandbreite aktiviert werden.

- **Antennengruppierung**

  Um den Gewinn durch Spatial-Multiplexing zu optimieren, kann die Antennengruppierung konfiguriert werden.

- **IP-Adresse**

  Spezifizieren Sie hier die feste IP-Adresse des Access-Points.

- **IP-Parameterprofil**

  Geben Sie hier den Profilnamen an über den die IP-Einstellungen für den Access-Point referenziert werden. Wenn Sie den Standardwert DHCP beibehalten, wird die Angabe der festen IP-Adresse ignoriert, so dass der Access-Point seine IP-Adresse über DHCP beziehen muss.

11.8.9 Stationstabelle (ACL-Tabelle)

Mit Hilfe der Stationstabelle legen Sie fest, welche WLAN-Clients sich in den WLAN-Netzwerken der LANCOM Wireless Router und LANCOM Access Points anmelden können, die durch den WLAN-Controller zentral verwaltet werden. Außerdem können sie den einzelnen WLAN-Clients auf diesem Wege sehr komfortabel eine Passphrase zur Authentifizierung und eine VLAN-ID zuweisen.

Zur Nutzung der Stationstabelle muss grundsätzlich der RADIUS-Server im WLAN-Controller aktiviert sein. Alternativ kann auch eine Weiterleitung zu einem anderen RADIUS-Server konfiguriert werden. Weitere Information zu RADIUS finden Sie unter 'RADIUS' → Seite 16-27.

Für jedes logische WLAN-Netzwerk, in dem die WLAN-Clients über RADIUS geprüft werden sollen, muss die MAC-Prüfung aktiviert werden.

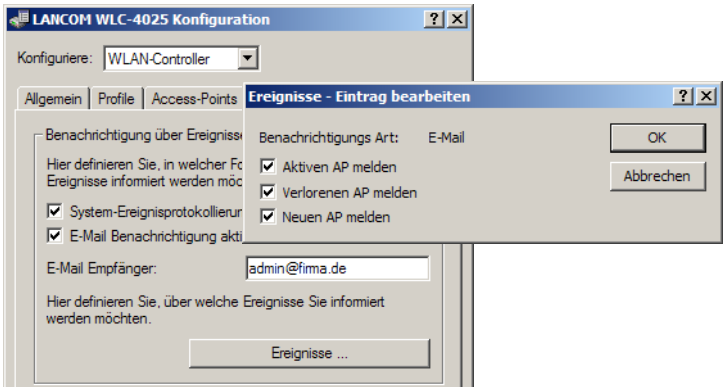
Die Beschreibung der ACL-Tabelle finden Sie unter 'Access Control List' → Seite 11-31.

11.8.10 Optionen für den WLAN-Controller

Im Bereich der 'Optionen' werden die Benachrichtigungen bei Ereignissen im WLAN-Controller 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 ▶ Benachrichtigungen

WEBconfig: LCOS-Menübaum ▶ Setup ▶ WLAN-Management ▶ Benachrichtigung

- **SYSLOG**

  Aktiviert die Benachrichtigung über SYSLOG.

  □ Mögliche Werte: Ein/Aus.

- **E-Mail**

  Aktiviert die Benachrichtigung über E-Mail.

  □ Mögliche Werte: Ein/Aus.

■ **Ereignisse**

Wählt die Ereignisse, die über die eine Benachrichtigung erfolgen soll.

□ Mögliche Werte:

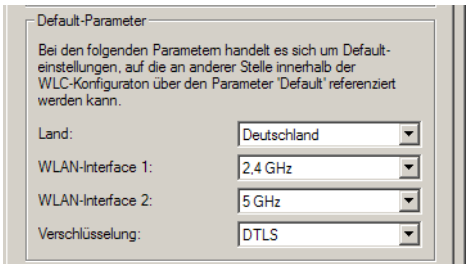
▶ Aktiven Access Point melden

▶ Verlorenen Access Point melden

▶ Neuen Access Point 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 ▶ Optionen ▶ Default-Parameter

WEBconfig: LCOS-Menübaum ▶ Setup ▶ WLAN-Management ▶ AP-Konfiguration

■ **Land**

Land, in dem die Access Points betrieben werden sollen. Aufgrund dieser Information werden landesspezifische Einstellungen wir die erlaubten Kanäle etc. festgelegt.

■ **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.

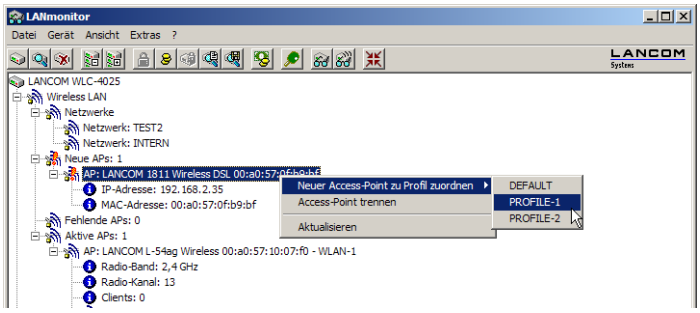
11.8.11 Neue Access Points manuell in die WLAN- Struktur aufnehmen

Wenn Sie die Access Points nicht automatisch in die WLAN-Struktur aufnehmen wollen (Auto-Accept, 'Automatische Annahme neuer APs (Auto-Accept)' → Seite 11-65), können sie die Access Points auch manuell akzeptieren.

Access Points akzeptieren über den LANmonitor

Neue Access Points können sehr komfortabel über den LANmonitor akzeptiert werden. Dabei wird eine Konfiguration ausgewählt, welche dem Access Point nach der Übertragung eines neuen Zertifikats zugewiesen wird.

Klicken Sie dazu im LANmonitor mit der rechten Maustaste auf den neuen Access Points, 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 Access Point in der AP-Tabelle des WLAN-Controllers eingetragen. Es dauert jedoch einige Sekunden, bis der WLAN-Controller dem Access Point auch ein Zertifikat zugewiesen hat und dieser ein aktives Element der zentralen WLAN-Struktur wird. Der neu aufgenommene

Access Point wird also für eine kurze Zeit als „Lost AP" mit der roten Lost-AP-LED, im Gerätedisplay und im LANmonitor angezeigt, bis die Zertifikatszuweisung abgeschlossen ist.

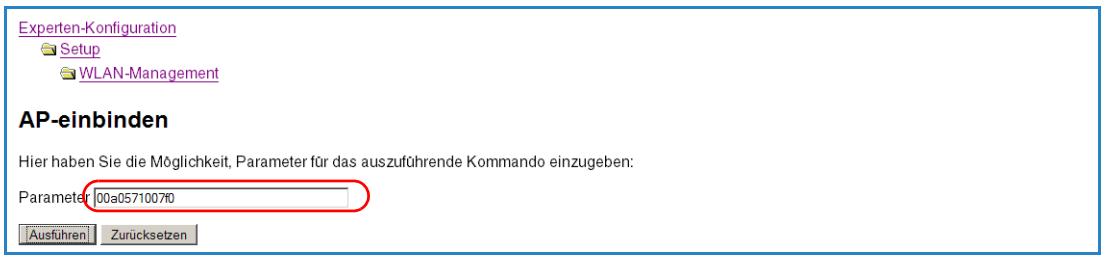
Access Points akzeptieren über WEBconfig mit Zuweisung eines Zertifikats

Neue Access Points, 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 LANCOM WLAN Controller mit WEBconfig.

② Wählen Sie unter **Experten-Konfiguration** ▶ **Setup** ▶ **WLAN-Management** die Aktion **AP-einbinden**.

③ Geben sie als Parameter für die Aktion die MAC-Adresse des Access Points ein, den Sie akzeptieren möchten, und bestätigen Sie mit **Ausführen**.



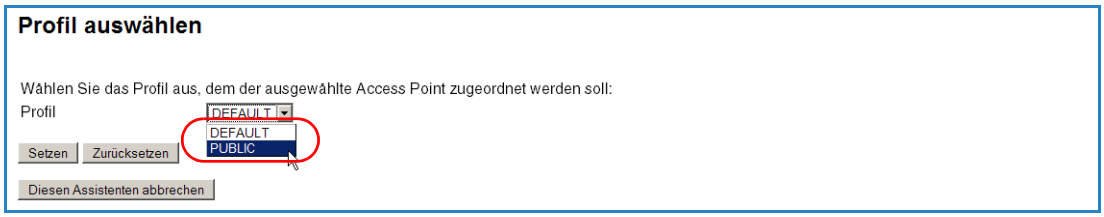
Access Points akzeptieren über WEBconfig mit Zuweisung von Zertifikat und Konfiguration

Neue Access Points, 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 Access Point nach der Übertragung eines neuen Zertifikats zugewiesen wird.

① Öffnen Sie die Konfiguration des LANCOM WLAN Controller mit WEBconfig. Wenn neue Access Points gefunden wurden, zeigt WEBconfig das auf der Startseite mit einer entsprechenden Meldung an.



② Klicken Sie auf den Link, um den Assistenten zu starten. Wählen Sie den gewünschten Access Point anhand seiner MAC-Adresse aus und geben Sie die WLAN-Konfiguration an, die dem Access Point zugewiesen werden soll.



Mit dem Zuweisen der Konfiguration wird der Access Point in der AP-Tabelle des WLAN-Controllers eingetragen. Es dauert jedoch einige Sekunden, bis der WLAN-Controller dem Access Point auch ein Zertifikat zugewiesen hat und er damit aktives Element der zentralen WLAN-Struktur wird. Der neu aufgenommene Access Point wird also für eine kurze Zeit als „Lost AP" mit der roten Lost-AP-LED, im Gerätedisplay und im LANmonitor angezeigt, bis die Zertifikatszuweisung abgeschlossen ist.

11.8.12 Access Points manuell aus der WLAN-Struktur entfernen

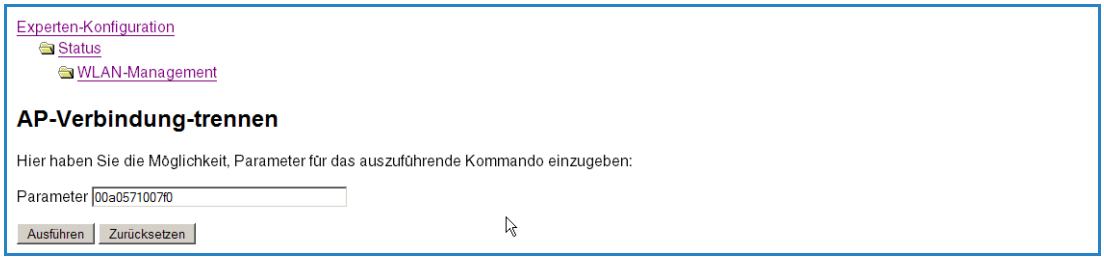
Um einen Access Point, der vom WLAN-Controller verwaltet wird, aus der WLAN-Struktur zu entfernen, müssen Sie folgende Aktionen ausführen:

① Stellen Sie im Access Point die WLAN-Betriebsart für die WLAN-Module von 'Managed' auf 'Client' oder 'Access-Point' um.

② Löschen Sie im WLAN-Controller die Konfiguration für den Access Point bzw. deaktivieren Sie die 'Automatische Zuweisung der Default-Konfiguration'.

③ Trennen Sie die Verbindung zum Access Point unter WEBconfig im Bereich **Experten-Konfiguration ▶ 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 Access Points ein, zu dem Sie die Verbindung trennen möchten, und bestätigen Sie mit **Ausführen**.



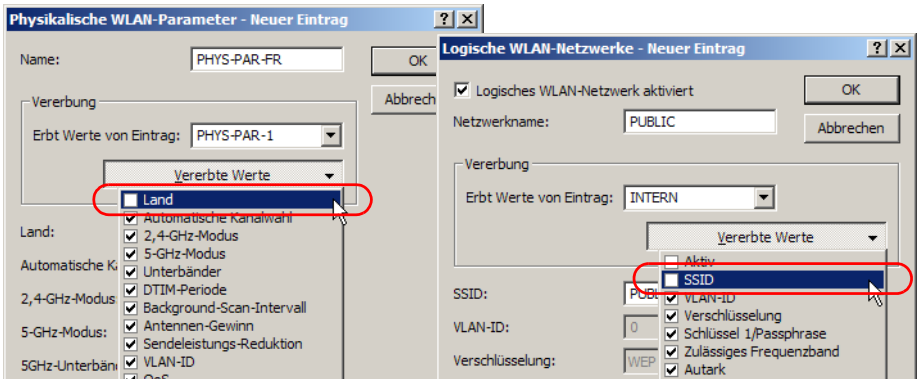
11.8.13 Vererbung von Parametern

Mit einem LANCOM WLAN Controller können sehr viele unterschiedliche Access Points an verschiedenen Standorten verwaltet werden. Nicht alle Einstellungen in einem WLAN-Profil eignen sich dabei für jeden der verwalteten Access Points 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 Access Points 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.

11.8.14 Sicherung der Zertifikate

Ein LANCOM WLAN Controller erzeugt beim ersten Systemstart die grundlegenden Zertifikate für die Zuweisung der Zertifikate an die Access Points – darunter die Root-Zertifikate für die CA (Certification Authority) und die RA (Registration Authority). Auf der Grundlage dieser beiden Zertifikate stellt der WLAN-Controller die Geräte-Zertifikate für die Access Points aus.

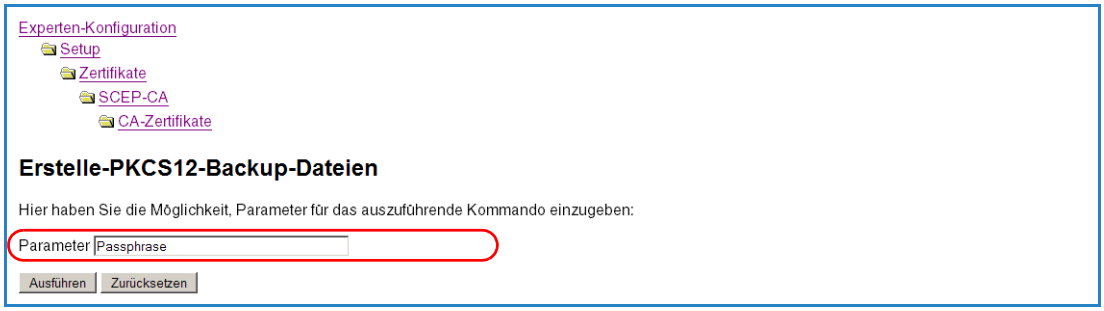
Wenn mehrere WLAN-Controller in der gleichen WLAN-Infrastruktur parallel eingesetzt werden (Load-Balancing) oder wenn ein Gerät ersetzt bzw. neu konfiguriert werden muss, sollten immer die gleichen Root-Zertifikate verwendet werden, um einen reibungslosen Betrieb der verwalteten Access Points zu gewährleisten.

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 LANCOM WLAN Controller erzeugt werden. Außerdem sollten folgende noch weitere Dateien mit Informationen über die ausgestellten Geräte-Zertifikate gesichert werden ('Sichern und Wiederherstellen weiterer Dateien der SCEP-CA' → Seite 11-75). 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.

① Öffnen Sie die Konfiguration des LANCOM WLAN Controller mit WEBconfig im Bereich **Experten-Konfiguration ▶ 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.



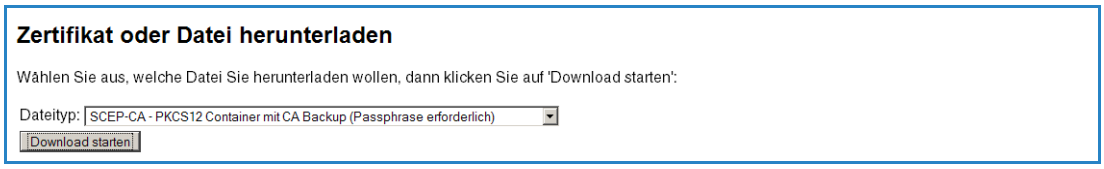
Mit dieser Aktion werden die Zertifikate und privaten Schlüssel in die PKCS12-Dateien gespeichert und können dann aus dem Gerät heruntergeladen werden.

Zertifikats-Backup aus dem Gerät herunterladen

① Wählen Sie auf der Startseite von WEBconfig den Befehl **Zertifikat oder Datei herunterladen**.

② Wählen Sie dann als Dateityp nacheinander die beiden Einträge für die SCEP-CA und bestätigen Sie mit **Download starten**:

- □ PKCS12-Container mit CA-Backup
- □ PKCS12-Container mit RA-Backup



Die Backup-Datei wird damit auf Ihren Datenträger gespeichert. Die Passphrase wird erst beim Einspielen in einen LANCOM WLAN Controller wieder benötigt.

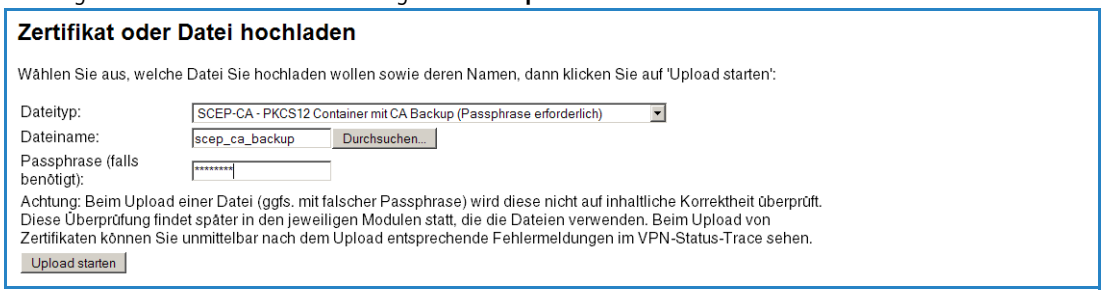
Zertifikats-Backup in das Gerät einspielen

① Wählen Sie auf der Startseite von WEBconfig den Befehl **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 Danach muss im Verzeichnis /Setup/Certificates/SCEP-Client der Befehl Reinit aufgerufen werden:

cd /Setup/Certificates/SCEP-Client

do Reinit

11.8.15 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 Access Points wichtig.

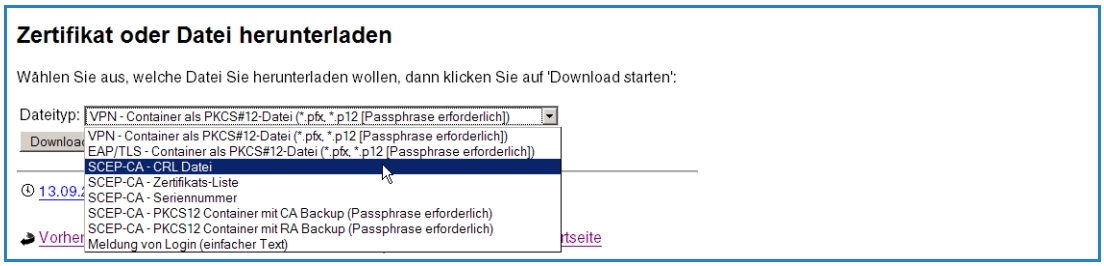
Wenn nur die Root-Zertifikate gesichert werden, können die ausgestellten Geräte-Zertifikate nicht mehr zurückgerufen werden!

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.

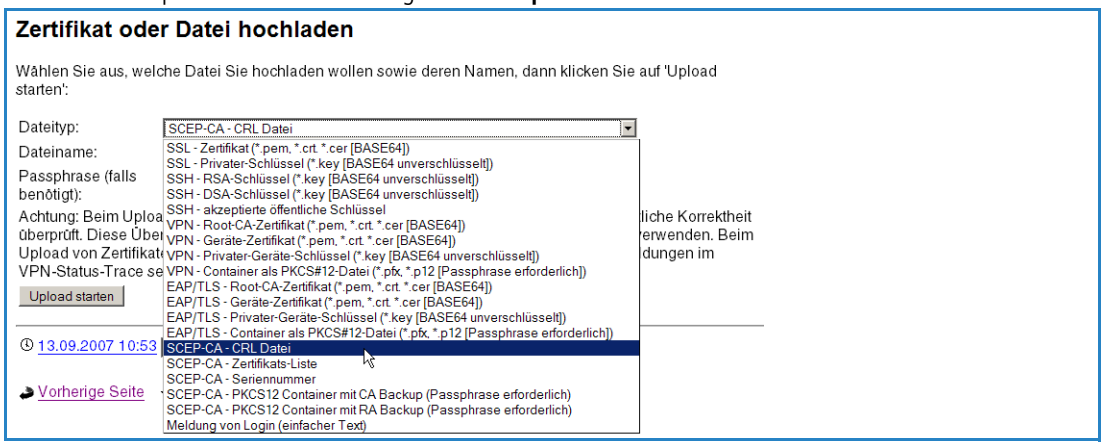
① Wählen Sie auf der Startseite von WEBconfig den Befehl **Zertifikat oder Datei herunterladen**.

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.

11.8.16 Load-Balancing zwischen den WLAN-Controllern

Wenn in einem Netzwerk mehrere WLAN-Controller verfügbar sind, werden die Access Points automatisch gleichmäßig auf die WLAN-Controller verteilt.

Der Access Point sendet zu Beginn der Kommunikation eine „Discovery Request Message", um die verfügbaren WLAN-Controller zu ermitteln.

- Wenn der Access Point Antworten von primären und sekundären WLAN-Controllern erhält, werden primäre Controller bevorzugt.
- Aus den verfügbaren WLAN-Controllern wählt der Access Point den mit der geringsten Auslastung, also dem kleinsten Verhältnis von gemanagten Access Points zu den maximal möglichen Access Points.
- Bei zwei oder mehreren gleich „guten" WLAN-Controllern wählt der Access Point den im Netzwerk nächsten, also den mit der geringsten Antwortzeit.

Auf diese Art und Weise können z. B. beim Aktivieren von mehreren WLAN-Controllern über die automatische Zuweisung von Konfigurationen ('Automatische Zuweisung der Default-Konfiguration' → Seite 11-65) alle WLAN-Controller gleichmäßig mit Konfigurationen für einen Teil der Access Points „gefüllt" werden.

11.8.17 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 Access Points 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 Access Points 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 ('VLAN-ID' → Seite 11-67) wird die VLAN-ID dabei dem WLAN-Client von einem RADIUS-Server direkt zugewiesen.

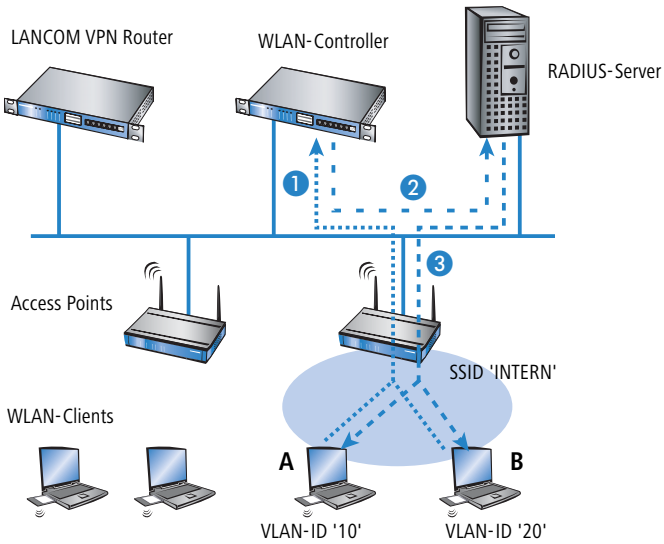
Beispiel:

- Die WLAN-Clients der Mitarbeiter buchen sich über einen Access Point in das WPA-gesicherte WLAN mit der SSID 'INTERN' ein. Bei der Anmeldung werden die RADIUS-Anfragen der WLAN-Clients an den Access Point gestellt. Wenn sich das entsprechende WLAN-Interface in der Betriebsart 'Managed' befindet, werden die RADIUS-Anfragen automatisch an den WLAN-Controller 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 Access Point 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 LANCOM WLAN Controller eine VLAN-ID zugewiesen werden (‘Stationstabelle (ACL-Tabelle)’ → Seite 11-70).



① Aktivieren Sie das VLAN-Tagging für den WLAN-Controller. Tragen Sie dazu als Management-VLAN-ID in den physikalischen Parametern des Profils einen Wert größer als '0' ein (‘Management-VLAN-ID’ → Seite 11-68).

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 WLAN-Controller ein RADIUS-Server erforderlich. Der WLAN-Controller trägt sich dabei automatisch in den von ihm verwalteten Access Points als RADIUS-Server ein – alle RADIUS-Anfragen an die Access Points werden daher direkt an den WLAN-Controller 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 **Experten-Konfiguration ▶ 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.

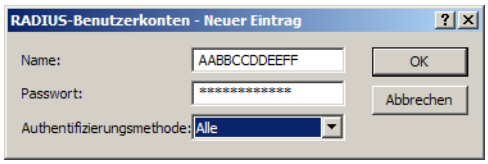
⑤ Konfigurieren Sie die Einträge im RADIUS-Server entsprechend, damit den anfragenden WLAN-Clients anhand bestimmter Merkmale die richtigen VLAN-IDs zugewiesen werden.

Weitere Information zu RADIUS finden Sie in der Dokumentation Ihres RADIUS-Servers.

11.8.18 Prüfung der WLAN-Clients über RADIUS (MAC-Filter)

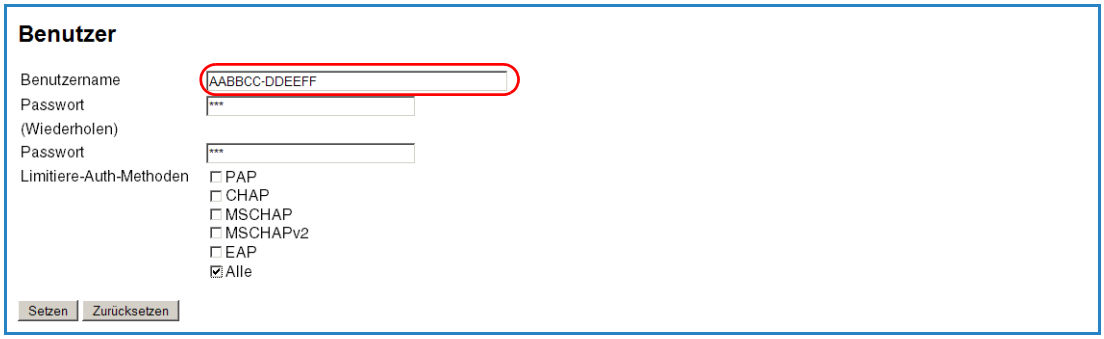
Bei der Nutzung von RADIUS zur Authentifizierung der WLAN-Clients kann neben einem externen RADIUS-Server auch die interne Benutzertabelle der LANCOM WLAN Controller genutzt werden, um nur bestimmten WLAN-Clients anhand ihrer MAC-Adresse den Zugang zum WLAN zu erlauben.

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'.



Alternativ tragen Sie die zugelassenen MAC-Adressen über WEBconfig ein unter **Experten-Konfiguration ▶ Setup ▶ RADIUS ▶ Server ▶ Benutzer**.

Als 'Benutzername' **und** 'Passwort' wird jeweils die MAC-Adresse in der Schreibweise 'AABBCC-DDEEFF' eingetragen.



11.8.19 Access Point deaktivieren oder dauerhaft aus der WLAN-Struktur entfernen

In manchen Fällen ist es notwendig, einen vom WLAN-Controller verwalteten Access Point entweder vorübergehend zu deaktivieren oder dauerhaft aus der WLAN-Struktur zu entfernen.

Access Point deaktivieren

Um einen Access Point 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 Access Point gelöscht.

Die WLAN-Module und die WLAN-Netzwerke (SSIDs) werden auch dann abgeschaltet, wenn der autarke Weiterbetrieb ('Autarker Weiterbetrieb' → Seite 11-67) aktiviert ist.

Ein so deaktivierter Access Point bleibt mit dem WLAN-Controller verbunden, die Zertifikate bleiben erhalten. Der WLAN-Controller kann also jederzeit durch das Aktvieren des Eintrags in der AP-Tabelle oder durch einen neuen Eintrag in der AP-Tabelle für die entsprechende MAC-Adresse den Access Point und seine WLAN-Module im Managed-Modus wieder einschalten.

Wird die Verbindung zu einem deaktivierten Access Point getrennt (unbeabsichtigt z. B. durch Störung im LAN oder gezielt durch den Administrator), dann beginnt der Access Point eine neue Suche nach einem passenden WLAN-Controller. Der bisherige WLAN-Controller kann zwar das Zertifikat auf Gültigkeit prüfen, hat aber keinen (aktiven) Eintrag in der AP-Tabelle – er wird also zum sekundären WLAN-Controller für diesen Access Point. Findet der Access Point einen primären WLAN-Controller, so wird er sich bei diesem anmelden.

Access Point dauerhaft aus der WLAN-Struktur entfernen

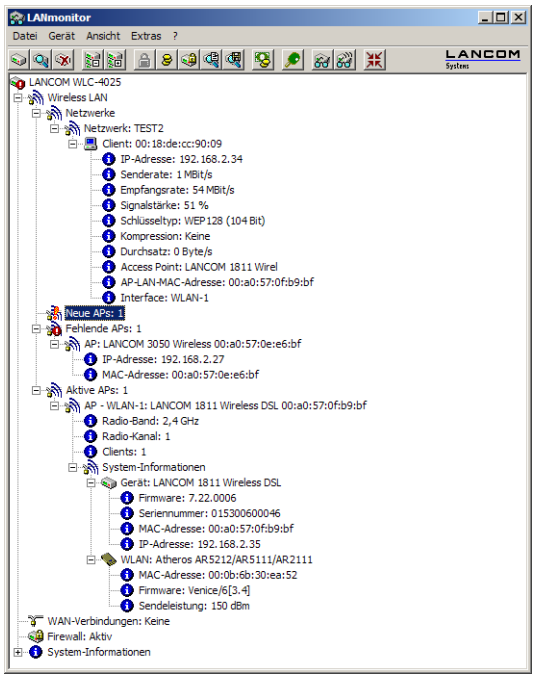
Damit ein Access Point auf Dauer nicht mehr Mitglied der zentral verwalteten WLAN-Struktur ist, müssen die Zertifikate im SCEP-Client gelöscht oder widerrufen werden.

- Wenn Sie Zugriff auf den Access Point 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 WLAN-Controllers widerrufen werden. Wechseln Sie dazu unter WEBconfig in den Bereich **Status ▶ Zertifikate ▶ SCEP-CA ▶ Zertifikate** in die **Zertifikatsstatus-Tabelle**. Löschen Sie dort das Zertifikat für die MAC-Adresse des Access Points, den Sie aus der WLAN-Struktur entfernen möchten. Die Zertifikate werden dabei nicht gelöscht, aber als abgelaufen markiert.

Bei einer Backup-Lösung mit redundanten WLAN-Controllern müssen die Zertifikate in allen WLAN-Controllern widerrufen werden!

11.8.20 Anzeigen und Aktionen im LANmonitor

Über den LANmonitor haben sie einen schnellen Überblick über die LANCOM WLAN Controller im Netzwerk und die Access Points in der WLAN-Struktur. LANmonitor zeigt dabei u. a. die folgenden Informationen:



- Aktive WLAN-Netzwerke mit den eingebuchten WLAN-Clients sowie der Bezeichnung des Access Points, bei dem der WLAN-Client eingebucht ist.
- Anzeige der neuen Access Points mit IP- und MAC-Adresse
- Anzeige der fehlenden Access Points mit IP- und MAC-Adresse
- Anzeige der gemanagten Access Points mit IP- und MAC-Adresse, verwendetem Frequenzband und Kanal

Über die rechte Maustaste kann auf den Access Points ein Kontext-Menü geöffnet werden, in dem folgende Aktionen zur Auswahl stehen:

- **Neuen Access Point zu Profil zuordnen**

  Bietet die Möglichkeit, einem neuen Access Point eine Konfiguration zuzuordnen und ihn so in die WLAN-Struktur aufzunehmen (‘Access Points akzeptieren über den LANmonitor’ → Seite 11-71).

- **Access Point trennen**

  Trennt die Verbindung zwischen Access Point und WLAN-Controller. Der Access Point sucht dann erneut nach einem zuständigen WLAN-Controller. Diese Aktion wird z. B. verwendet, um Access Points nach einem Backup-Fall vom Backup-Controller zu trennen und wieder auf den eigentlichen WLAN-Controller zu leiten.

- **Aktualisieren**

  Aktualisiert die Anzeige des LANmonitors.

11.8.21 Konfiguration der Access Points

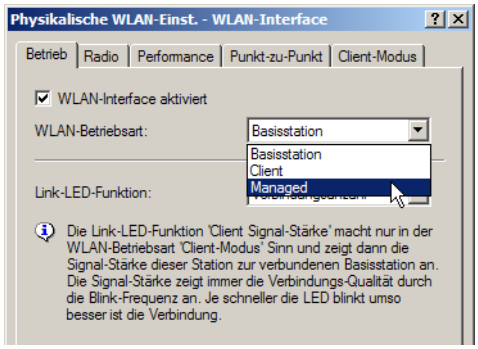
Ab der Firmware-Version LCOS 7.20 unterscheiden sich LANCOM Access Points (z. B. LANCOM L-54ag) und LANCOM Wireless Router (z. B. LANCOM 1811 Wireless) bzgl. der Einstellung der WLAN-Module im Auslieferungszustand.

- Bei LANCOM Access Points sind im Auslieferungszustand die WLAN-Module auf die Betriebsart 'Managed' eingestellt. In diesem Modus suchen die LANCOM Access Points nach einem zentralen WLAN-Controller, der ihnen eine Konfiguration zuweisen kann, und bleiben so lange im „Such-Modus“, bis sie einen passenden WLAN-Controller gefunden haben oder die Betriebsart für die WLAN-Module manuell geändert wird.
- Bei LANCOM Wireless Routern sind im Auslieferungszustand die WLAN-Module auf die Betriebsart 'Access-Point' eingestellt. In diesem Modus arbeiten die LANCOM Wireless Router als autarke Access Points mit einer im Gerät lokal gespeicherten Konfiguration. Um Teilnehmer einer zentral über WLAN-Controller verwalteten WLAN-

Struktur zu werden, muss die Betriebsart für die WLAN-Module in den gewünschten LANCOM 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 WLAN-Controller 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 (7.22 / 23.08.2007)
lang English
flash 0
cd Setup/Interfaces/WLAN/Operational
set WLAN-1 0 managed-AP 0
# done
exit
```

11.8.22 Automatische Funkfeldoptimierung mit LANCOM WLAN Controllern

Mit der Auswahl des Kanals in der Kanal-Liste wird der Teil des Frequenzbandes festgelegt, den ein Access Point für seine logischen WLANs verwendet. Alle WLAN-Clients, die sich mit einem Access Point 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 Access Point Daten übertragen. Um in der Funkreichweite eines anderen Access Points ein WLAN mit maximaler Bandbreite betreiben zu können, muss jeder Access Point einen separaten Kanal nutzen – anderenfalls müssen sich die WLANs die Bandbreite des Kanals teilen.

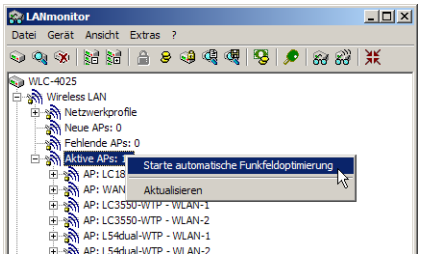
Bei einer völlig offenen Kanalliste werden die Access Points möglicherweise automatisch Kanäle wählen, die sich gegenseitig teilweise überlappen und so die Signalqualität reduzieren. Außerdem könnten die Access Point evtl. Kanäle wählen, welche die WLAN-Clients aufgrund der Ländereinstellung nicht nutzen können. Um die Access Points 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 Access Points ist es manchmal schwierig, für jeden Access Point einen geeigneten Kanal einzustellen. Mit der automatischen Funkfeldoptimierung bieten die LANCOM WLAN Controller ein Verfahren, um die optimalen Kanäle der Access Points für das 2.4 GHz-Band automatisch einzustellen.

WEBconfig: **Setup ▶ WLAN-Management ▶ Start-automatic-radio-field-optimization**

Die Optimierung kann auch gezielt für einen einzelnen Access Point gestartet werden, indem die MAC-Adresse als Parameter für die Aktion eingetragen wird.

LANmonitor: Klick mit der rechten Maustaste auf die Liste der aktiven Access Points oder auf ein bestimmtes Gerät, dann im Kontextmenü **Starte automatische Funkfeldoptimierung** wählen.



Die Optimierung läuft dann in den folgenden Schritten ab:

① Der WLAN-Controller löscht die AP-Kanalliste aller Access Points im 2.4 GHz-Bereich. Da die Kanalliste der Access Points dann leer ist, wird ihnen über ein Konfigurations-Update die Kanalliste ihres Profils zugewiesen.

② Der WLAN-Controller schaltet alle Funkmodule im 2.4 GHz-Bereich aus.

③ Die Access Points werden nacheinander eingeschaltet. Dabei werden sie in der Reihenfolge bearbeitet, in der sie sich beim WLAN-Controller angemeldet haben.

④ Automatische Einmessung: Nach dem Einschalten sucht sich der Access Point selbständig den für ihn besten Kanal aus der Kanalliste. Zur Bestimmung des am besten geeigneten Kanals führt der Access Point jeweils eine Interferenz-Messung durch, so dass die Signalstärken und Kanäle anderer Access Points entsprechend berücksichtigt werden. Da die bisherige Liste in der Konfiguration des WLAN-Controllers gelöscht wurde, ist dies nun die Profilkanalliste. Wenn die Profilkanalliste leer ist, hat der Access Point die freie Auswahl aus den nicht durch andere Funk-Module belegten Kanälen.

⑤ Der gefundene Kanal wird zurück an den WLAN-Controller gesendet und dort in der AP-Kanalliste gespeichert. Deswegen erhält der Access Point beim nächsten Verbindungsaufbau wieder diesen Kanal. Die AP-Kanalliste hat so gesehen ein höheres Gewicht als die Profilkanalliste.

Verfügt ein Access Point über mehrere WLAN-Module, so wird dieser Vorgang für jedes WLAN-Modul nacheinander ausgeführt.

11.9 Zentrales Firmware- und Skript-Management

Neu mit LCOS 7.6:

- Interner Skript-Speicher (Skript-Management ohne HTTP-Server)

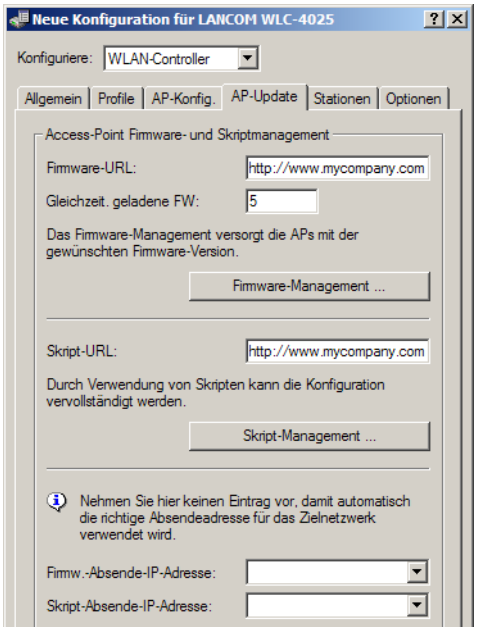
Mit einem LANCOM WLAN Controller kann die Konfiguration von mehreren LANCOM Wireless Routern und LANCOM Access Points von einer Stelle aus komfortabel und konsistent verwaltet werden. Mit dem zentralen Firmware- und Skript-Management können auch Firmware- und Skript-Uploads auf allen verwalteten WLAN-Geräten automatisch ausgeführt werden.

Dazu werden die Firmware- und Skript-Dateien auf einem Web-Server abgelegt (Firmware als *.UPX, Skripte als *.LCS). Der WLAN-Controller 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 Access Point läuft, lädt der WLAN-Controller diese vom Webserver herunter und spielt sie in die entsprechenden Wireless Router und Access Points 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 Access Point automatisch neu.
- Wenn der Access Point schon verbunden ist, startet das Gerät danach **nicht** automatisch neu. In diesem Fall wird der Access Point manuell über die Menüaktion "/Setup/WLAN-Management/Central-Firmware-Management/Reboot-updated-APs" oder zeitgesteuert per Cron-Job neu gestartet.
- Mit der Aktion "/Setup/WLAN-Management/Central-Firmware-Management/Update-Firmware-and-Script-Information" können Skript- und Firmwareverzeichnisse aktualisiert werden.



Sie finden die Parameter zur Konfiguration auf folgenden Pfaden:

LANconfig: **WAN-Controller ▶ AP-Update**

WEBconfig: **Setup ▶ WLAN-Management ▶ Zentrales-Firmware-Management**

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

■ **Gleichzeitig geladene FW**

Anzahl der gleichzeitig im Arbeitsspeicher des WLAN-Controllers 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' fur 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.

Firmware-Management-Tabelle

Tabelle mit Gerätetyp, MAC-Adresse und Firmware-Version zur gezielten Steuerung der verwendeten Firmware-Dateien.

■ **Gerätetypen**

Wählen Sie hier aus, für welchen Gerätetyp die in diesem Eintrag spezifizierte Firmware-Version verwendet werden soll.

- □ Mögliche Werte: Alle bzw. 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.

- □ Mögliche Werte: Firmware-Version in der Form `X.XX`
- □ Default: Leer

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

■ **Skript-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' für 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.

Skript-Management-Tabelle

Tabelle mit Skript-Dateiname und WLAN-Profil zur Zuordnung der Skripte zu einem WLAN-Profil.

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 Access Points 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 WLAN-Controller bei einer neuen oder geänderten Skript-Datei mit gleichem Dateinamen feststellen, ob die Skript-Datei erneut übertragen werden muss.

■ **Skript-Dateiname**

Name der zu verwendenen Skript-Datei.

- □ 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

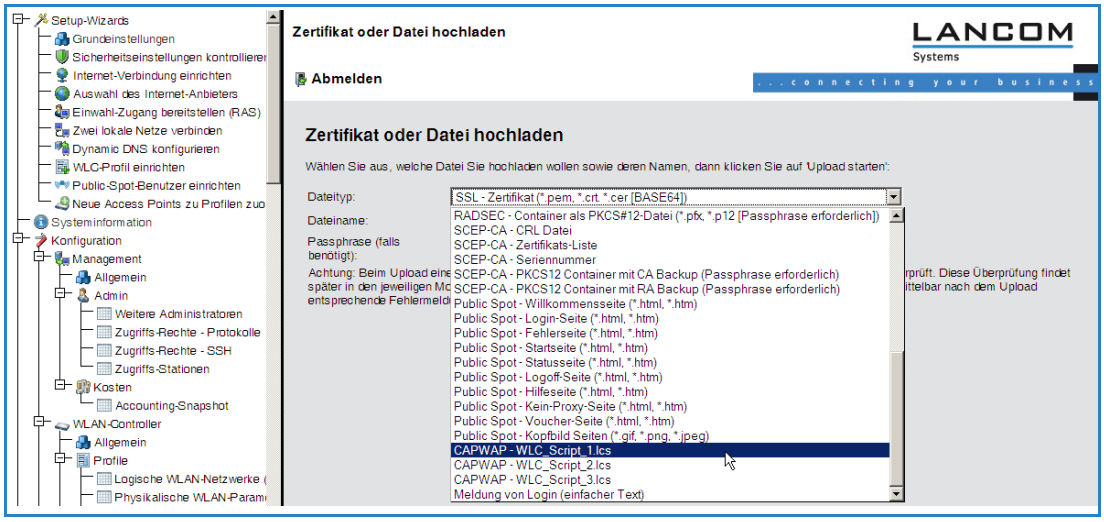
Interner Skript-Speicher (Skript-Management ohne HTTP-Server)

Skripte haben im Gegensatz zu Firmware-Dateien oft nur ein geringes Datenvolumen. Im internen Skript-Speicher der WLAN-Controller 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!



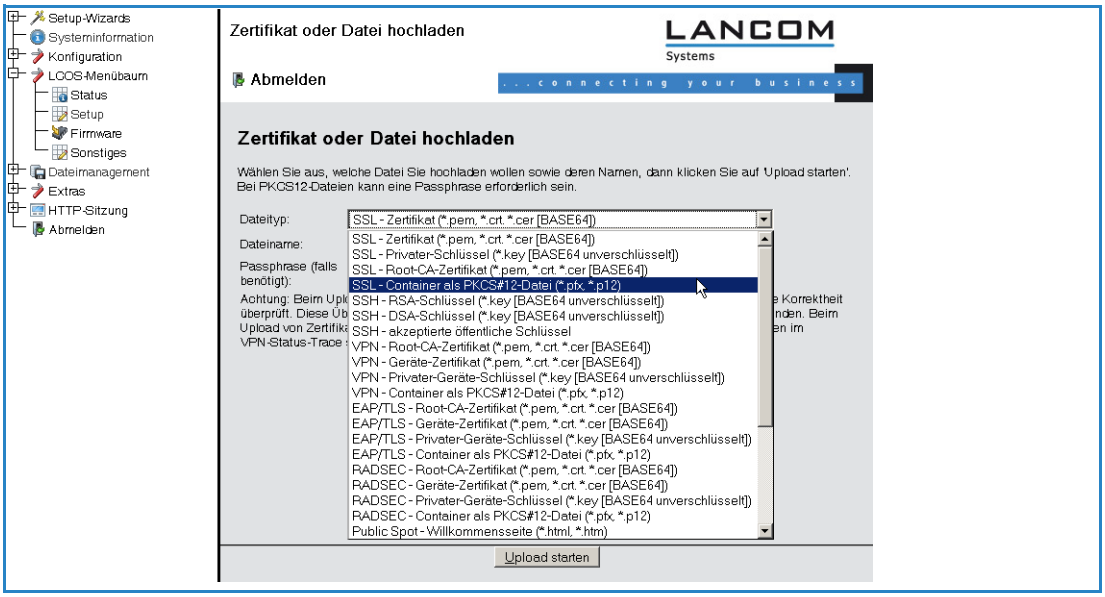
11.10 Mehrstufige Zertifikate für PublicSpots

Neu mit LCOS 7.6:

■ Mehrstufige Zertifikate für PublicSpots

SSL-Zertifikatsketten können in Form eines PKCS#12-Containers in das LANCOM geladen werden. Diese Zertifikatsketten können für die PublicSpot-Authentifizierungsseiten über den im LCOS implementierten HTTPS-Server verwendet werden. Zertifikate von allgemein anerkannten Trust-Centern sind üblicherweise mehrstufig. Offiziell signierte Zertifikate im PublicSpot sind notwendig, um Zertifikatsfehlermeldungen des Browsers bei PublicSpot-Authentifizierungen zu vermeiden.

Das Zertifikat laden Sie z.B. unter WEBconfig 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 PublicSpot anstelle einer internen IP-Adresse den DNS-Namen des Zertifikats als Ziel angeben (LCOS Menübaum/Setup/Public-Spot-Modul/Geraete-Hostname). Dieser Name muss im DNS-Server auf die entsprechende IP-Adresse des PublicSpots aufgelöst werden.



11.11 DFS 2: Freilassen von Kanälen für Wetter- Radar

Beim für 5 GHz WLANs geforderten DFS-Verfahren (Dynamic Frequency Selection) wird automatisch eine freie Frequenz gewählt, z. B. um das Stören von Radaranlagen zu verhindern und um die WLAN-Geräte möglichst gleichmäßig über das ganze Frequenzband zu verteilen. Die Signale von Wetter-Radarstationen können jedoch manchmal nicht sicher erkannt werden.

Die europäische Kommission fordert daher in Ergänzung zu den Standards ETSI EN 301 893 V1.3.1 und ETSI EN 310 893 V1.4.1, im Unterband 2 des 5 GHz-Bandes drei Kanäle (120, 124 und 128) auszusparen und nicht für die automatische Kanalwahl zu verwenden. Verfahren zur Erkennung der Wetter-Radar-Signaturen befinden sich in Entwicklung.

11.12 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 Access Point oder im Client-Modus.

11.12.1 Einstellung als Access Point

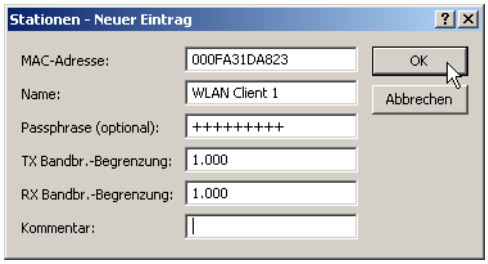
In der Betriebsart als Access Point können die maximal zulässigen Bandbreiten in Tx- und RX-Richtung für die WLAN-Clients festgelegt werden, die sich beim Access Point einbuchen. Dazu werden in der MAC-Zugangs-Liste die

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 Access Point steht Rx für „Daten senden“ und Tx für „Daten empfangen“.

Konfiguration mit LANconfig

Die maximalen Bandbreiten für die angeschlossenen Clients werden im LANconfig im Konfigurationsbereich 'Wireless-LAN' auf der Registerkarte 'Stationen' in der MAC-Zugangs-Liste eingetragen.



Konfiguration mit WEBconfig, Telnet oder SSH

Unter WEBconfig, Telnet oder SSH-Client finden Sie die MAC-Zugangs-Liste auf folgenden Pfaden:

Konfigurationstool	Menü/Tabelle
WEBconfig	Experten-Konfiguration ▶ Setup ▶ WLAN ▶ Access List
Terminal/Telnet	`Setup/WLAN/Access-List`

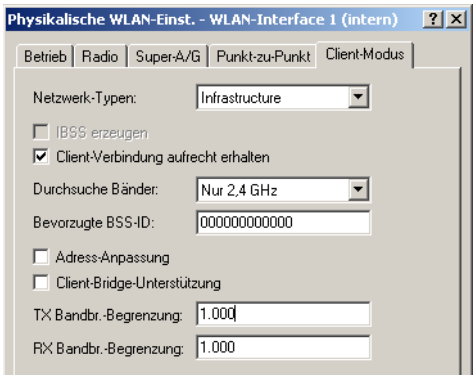
11.12.2 Einstellung als Client

Wird das Gerät selbst als WLAN-Client betrieben, kann das Gerät beim Einbuchen beim Access Point seine maximalen Bandbreiten übermitteln. Der Access Point 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“.

Konfiguration mit LANconfig

Die maximalen Bandbreiten für ein Gerät im Client-Modus werden im LANconfig im Konfigurationsbereich 'Interfaces' auf der Registerkarte 'Wireless LAN' bei den' physikalischen WLAN-Einstellungen' auf der Registerkarte 'Client-Modus' eingetragen.



Konfiguration mit WEBconfig, Telnet oder SSH

Unter WEBconfig, Telnet oder SSH-Client finden Sie die Client-Einstellungen auf folgenden Pfaden:

Konfigurationstool	Menü/Tabelle
WEBconfig	Experten-Konfiguration ▶ Setup ▶ Interfaces ▶ WLAN ▶ Client Mode
Terminal/Telnet	`Setup/Interfaces/WLAN/Client-Mode`

- **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.

Konfiguration mit WEBconfig oder Telnet

Unter WEBconfig oder Telnet bzw. Terminalprogramm finden Sie die Zugangs-Liste für das Funknetzwerk auf folgenden Pfaden:

Konfigurationstool	Gerätetyp	Menü/Tabelle
WEBconfig	LANCOM Wireless Router LANCOM Access Point	Experten-Konfiguration ▶ Setup ▶ WLAN ▶ Zugangs-Liste
WEBconfig	LANCOM WLAN Controller	Experten-Konfiguration ▶ Setup ▶ WLAN-Controller ▶ Zugangs-Liste

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.

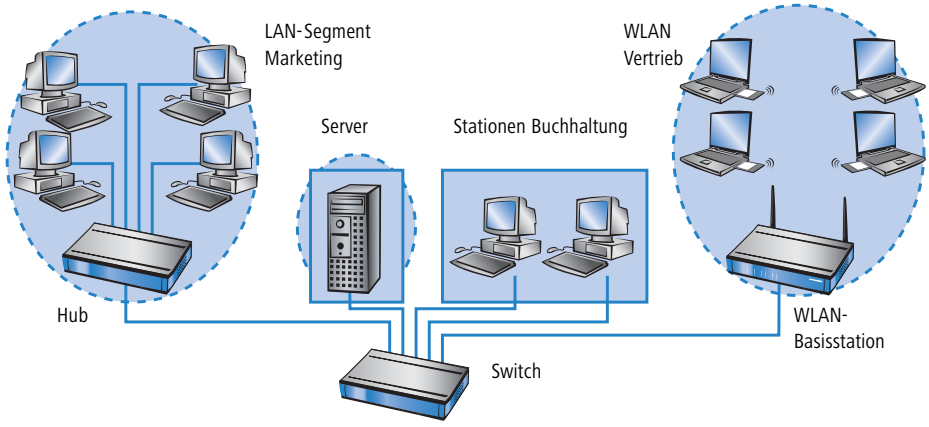
Eine Möglichkeit, diese Probleme zu überwinden, stellen die virtuellen LANs (VLAN) dar, wie sie in IEEE 802.1p/q beschrieben sind. Bei diesem Konzept werden auf einem physikalischen LAN mehrere virtuelle LANs definiert, die sich gegenseitig nicht behindern und die auch den Datenverkehr der jeweils anderen 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 erreichet 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 können. Außerdem sollen Sie auf den Server zugreifen. 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 ('Die Porttabelle' → Seite 6).

- **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.



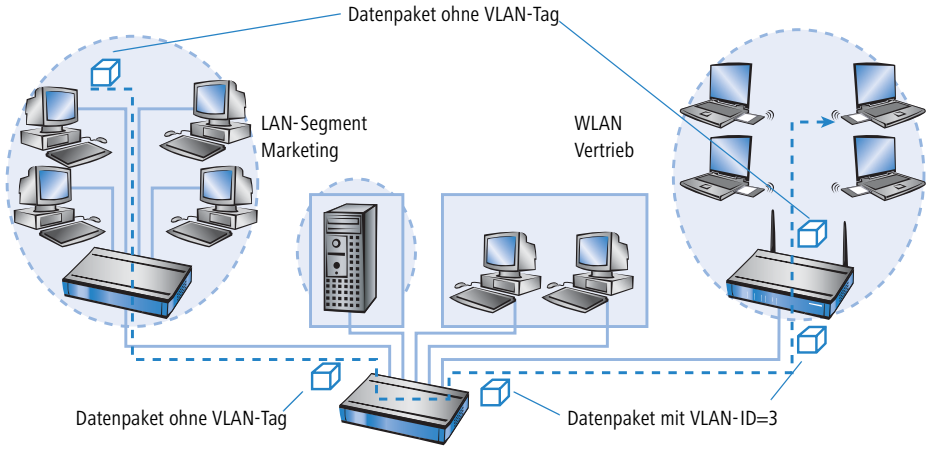
Ältere Switches im LAN können überlange Frames möglicherweise nicht richtig zwischen den einzelnen Ports weiterleiten und verwerfen die getaggten Pakete.

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 Datenpakte 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 VLAN Q-in-Q-Tagging

VLANs nach IEEE 802.1q werden üblicherweise eingesetzt, um mehrere Netzwerke auf einem gemeinsamen physikalischen Medium zu betreiben, die dennoch untereinander abgeschirmt werden sollen. In manchen Fällen werden VLANs aber auch auf öffentlichen Netzen der Provider verwendet, um die Netzwerke von verschiedenen Unternehmen zu trennen. Damit können sowohl im LAN als auch der WAN-Strecke VLAN-Tags zum Einsatz kommen – VLAN-getaggte LAN-Pakete müssen zur Übertragung im WAN daher mit einem weiteren VLAN-Tag versehen werden. Zur Steuerung des VLAN-Taggings kann das Verhalten für jeden Port separat definiert werden.

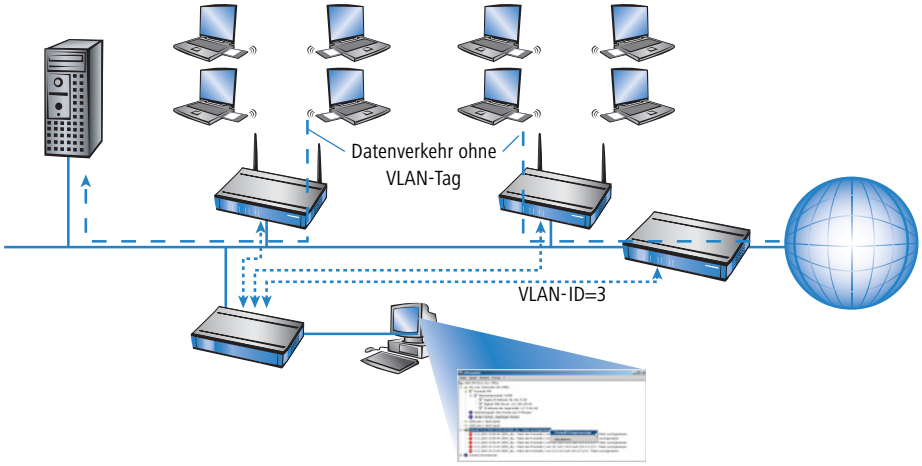
12.2.4 Anwendungsbeispiele

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.

Management- und User-Traffic auf einem LAN

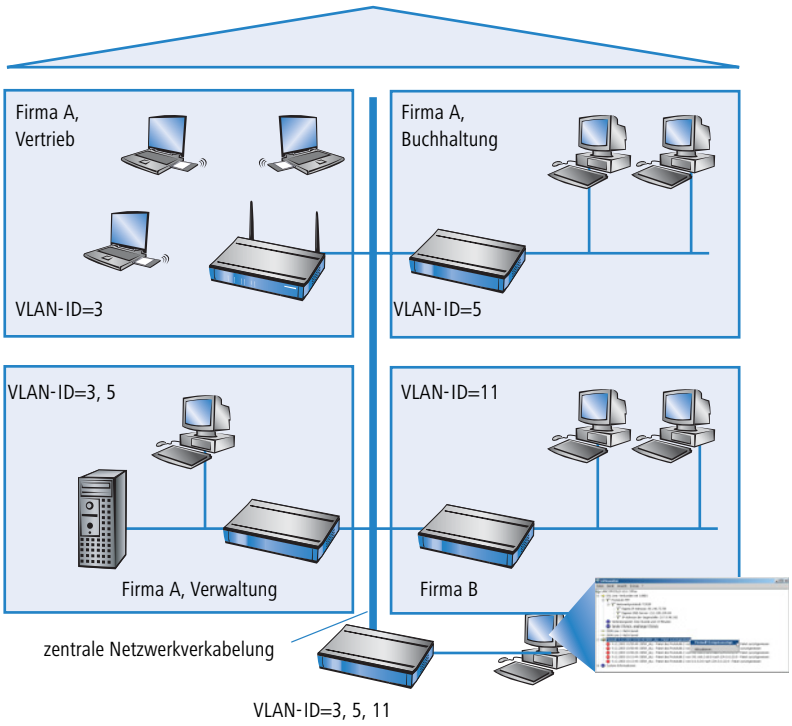
Auf dem Campus einer Universität werden mehrere Hot-Spots aufgestellt. Damit ist den Studenten über Notebooks mit WLAN-Karten der Zugang zum Server der Bibliothek und zum Internet möglich. Die Hot-Spots sind an das LAN der Universität angeschlossen. Über dieses LAN greifen die Administratoren auch auf die Basisstationen zu, um über SNMP verschiedene Management-Aufgaben zu erledigen.



Mit dem Einrichten eines virtuellen LANs zwischen den Basisstationen und dem Switch des Administratoren wird der Management-Datenverkehr von dem "öffentlichen" Verkehr auf dem LAN abgeschirmt.

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

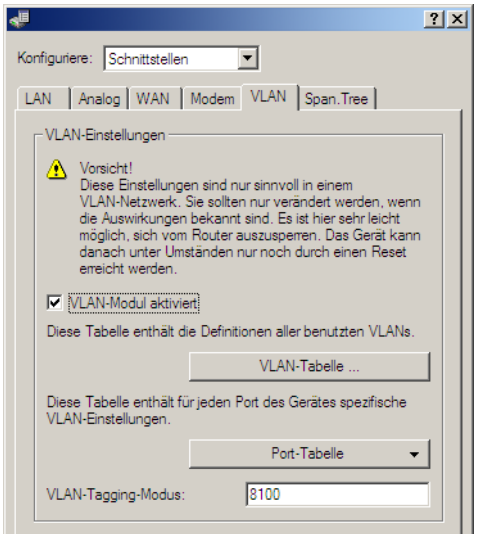
12.3.1 VLAN und ARF

In manchen Fällen reicht eine Konfiguration der VLAN-Einstellungen auf Basis der IP-Netzwerke aus (Advanced Routing and Forwarding, ARF). In diesem Fall wird für ein IP-Netzwerk eine VLAN-ID definiert. Alle ausgehenden Pakete dieses Netzwerkes werden dann mit dieser VLAN-ID getaggt, alle eingehenden Pakete müssen mit dieser VLAN-ID getaggt sein, damit sie dem Netzwerk zugeordnet werden können. Bitte beachten Sie die entsprechenden Hinweise im Abschnitt zu ARF.

12.3.2 VLAN und WLAN-Controller

LANCOM Access Points und LANCOM Wireless Router können in größeren Anwendungen von einem zentralen WLAN-Controller verwaltet werden. Der WLAN-Controller übernimmt dabei die Definition der WLAN-Netzwerke (SSIDs) und kann den SSIDs dabei auch eine VLAN-ID zuweisen. Durch die Zuweisung der VLAN-ID zu einer SSID auf dem WLAN-Controller und das Aktivieren des Management-VLANs (ID größer 0) wird auf dem verwalteten Access Point automatisch das VLAN-Modul eingeschaltet. Bitte beachten Sie dazu auch die Hinweise im Abschnitt zum zentralen WLAN-Management.

12.3.3 Allgemeine Einstellungen



LANconfig: Schnittstellen ▶ VLAN

WEBconfig: LCOS-Menübaum ▶ Setup ▶ VLAN

VLAN-Modul aktivieren

Schalten Sie das VLAN-Modul nur ein, wenn Sie mit den Auswirkungen der VLAN-Nutzung vertraut sind.

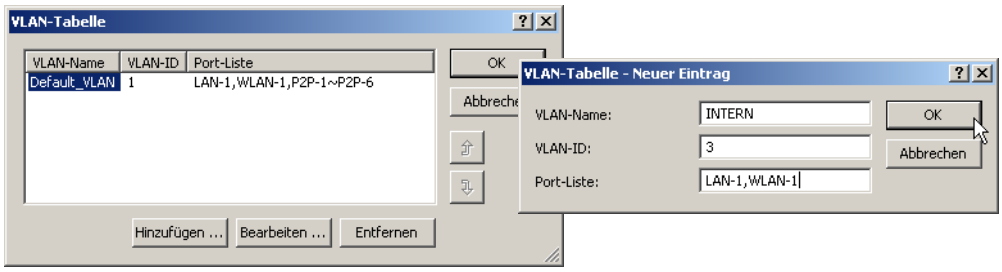
Mit fehlerhaften VLAN-Einstellungen können Sie den Konfigurationszugang zum Gerät verhindern.

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'.

12.3.4 Die Netzwerktabelle

In der Netzwerktabelle werden die virtuellen LANs definiert, an denen das Gerät teilnehmen soll.



LANconfig: Schnittstellen ▶ VLAN ▶ VLAN-Tabelle

WEBconfig: LCOS-Menübaum ▶ Setup ▶ VLAN ▶ Netzwerke

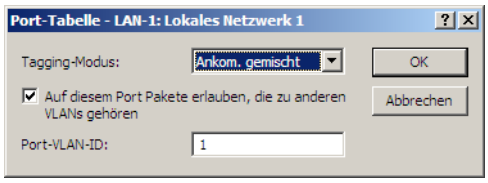
- **VLAN-Name**: Der Name des VLANs dient nur der Beschreibung bei der Konfiguration. Dieser Name wird an keiner anderen Stelle verwendet.
- **VLAN-ID**: Diese Nummer kennzeichnet das VLAN eindeutig.
- **Portliste**: In dieser Liste werden die Interfaces des Geräts eingetragen, die zu dem VLAN gehören.

  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".

Die erste SSID des ersten WLAN-Moduls heisst WLAN-1, die weiteren SSID WLAN-1-2 bis WLAN-1-8. Falls das Gerät über zwei WLAN-Module verfügt, heissen die SSIDs hier WLAN-2, WLAN-2-2 bis WLAN-2-8.

12.3.5 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

WEBconfig: LCOS-Menübaum ▶ Setup ▶ VLAN ▶ Port-Tabelle

- **Port**: Der Name des Ports, nicht editierbar
- **Tagging-Modus**

  Steuert die Verarbeitung und Zuweisung von VLAN-Tags auf diesem Port.

  - Niemals: Ausgehende Pakete erhalten auf diesem Port kein VLAN-Tag. Eingehende Pakete werde 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.
  - 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.
  - 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.
  - Ankommend gemischt: Ankommende Pakete können ein VLAN-Tag haben oder nicht, ausgehende Pakete bekommen nie ein VLAN-Tag.
  - Default: Ankommend gemischt
- **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**

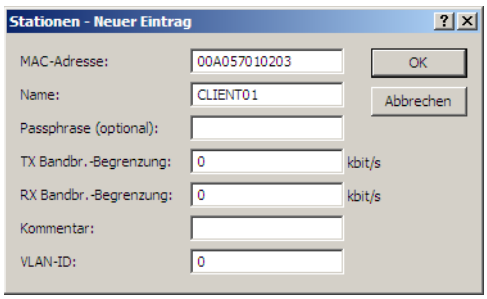
  Diese Port-ID hat zwei Funktionen:

  - Ungetaggte Pakete, die auf diesem Port im Modus 'Gemischt' oder 'ankommend gemischt' empfangen werden, werden diesem VLAN zugeordnet, ebenso sämtliche ankommenden Pakete im Modus 'Niemals'.
  - Im Modus '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 LANCOM 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 ▶ Stationen

WEBconfig: LCOS-Menübaum ▶ Setup ▶ WLAN ▶ Access-List

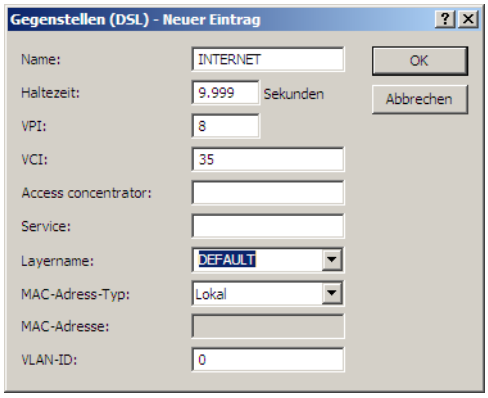
Die client-spezifische VLAN-ID kann Werte von 0 bis 4094 annehmen. der Defaultwert von '0' steht für eine nicht spezifizierte VLAN-ID. In diesem Fall wird der Client dem VLAN-Port des logischen WLAN-Netzwerks zugeordnet.

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 gemeinsamen genutzten Übertragungsmedien eingesetzt werden. Um diese VLAN-Tags im LANCOM Router richtig verarbeiten zu können, kann zu jeder DSL-Gegenstelle eine entsprechende VLAN-ID definiert werden.



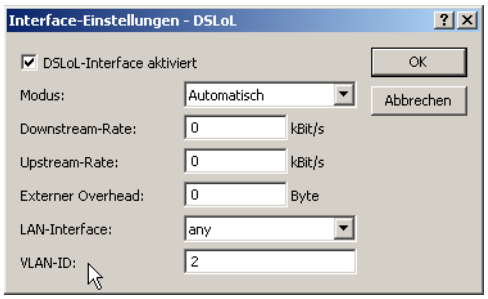
LANconfig: Kommunikation ▶ Gegenstellen ▶ Gegenstellen (DSL)

WEBconfig: LCOS-Menübaum ▶ 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 von restlichen Traffic separieren zu können, kann für das DSLoL-Interface unter `Setup/Interfaces/DSLoL` oder im LANconfig im Konfigurationsbereich 'Interfaces' auf der Registerkarte 'WAN' bei den Interface-Einstellungen für das DSLoL-Interface im Feld 'VLAN-ID' eingestellt werden.



12.5 VLAN-Tags auf Layer 2/3 im Ethernet

12.5.1 Einleitung

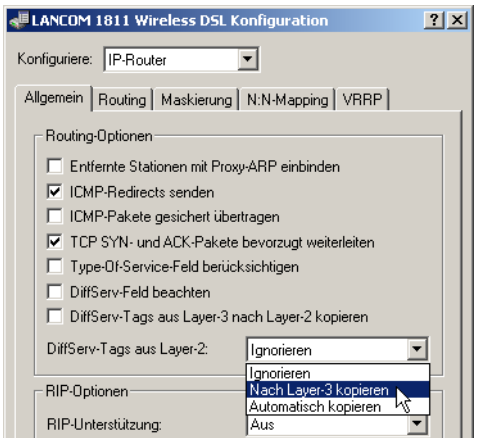
VLAN-Tags bieten auch bei solchen Switches, die keine IP-Header auswerten können, die Möglichkeit einer einfachen QoS-Steuerung. Der Standard IEEE 802.1p definiert ein Prioritäts-Tag im VLAN-Header mit einer Länge von drei Bit, das den ersten drei Bit des DSCP-Felder (Differentiated Services Code Point – 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 das LANCOM 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 oder H.323, 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

WEBconfig: LCOS-Menübaum ▶ 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.

LANCOM Referenzhandbuch Teil 5

- Voice over IP (VoIP)

Stand: LCOS 7.6 mit Addendum 7.7 (siehe Anhang)
(letztes Update August 2009)

LANCOM
Systems

© 2009 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®, Windows Vista™, Windows NT® und Microsoft® sind eingetragene Marken von Microsoft, Corp.

Das LANCOM Systems-Logo, LCOS und die Bezeichnung LANCOM sind eingetragene Marken der LANCOM Systems GmbH. Alle übrigen verwendeten Namen und Bezeichnungen können Marken oder eingetragene Marken ihrer jeweiligen Eigentümer sein.

LANCOM Systems behält sich vor, die genannten Daten ohne Ankündigung zu ändern und übernimmt keine Gewähr für technische Ungenauigkeiten und/oder Auslassungen.

Produkte von LANCOM Systems enthalten Software, die vom „OpenSSL Project" für die Verwendung im „OpenSSL Toolkit" entwickelt wurde (http://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.

Produkte von LANCOM Systems enthalten Komponenten, die als Open Source Software im Quelltext verfügbar sind und speziellen Lizenzen sowie den Urheberrechten verschiedener Autoren unterliegen. Im Besonderen enthält die Firmware Komponenten, die der GNU General Public License, Version 2 (GPL) unterliegen. Die Lizenzvereinbarung mit dem Text der GPL ist auf der LANCOM CD im Produktverzeichnis zu finden. Auf Anfrage können die Quelltexte und alle Lizenzhinweise elektronisch vom FTP-Server der LANCOM Systems GmbH bezogen werden.

Die Firmware des LANCOM VP-100 enthält Komponenten, die als Open Source Software im Quelltext verfügbar sind und speziellen Lizenzen sowie den Urheberrechten verschiedener Autoren unterliegen. Im Besonderen enthält die Firmware Komponenten, die der GNU General Public License, Version 2 (GPL) unterliegen. Die Lizenzvereinbarung mit dem Text der GPL ist auf der LANCOM CD im Produktverzeichnis als LC-VP100-License-DE.txt zu finden. Auf Anfrage können die Quelltexte und alle Lizenzhinweise elektronisch vom FTP-Server der LANCOM Systems GmbH bezogen werden.

LANCOM Systems GmbH

Adenauerstr. 20/B2

52146 Würselen

Deutschland

www.lancom.de

Würselen, August 2009

110654/0809

Inhalt

13 Voice over IP (VoIP) 13 -1

13.1 Einleitung 13 - 1

13.2 VoIP-Implementation im LANCOM VoIP Router 13 - 2
13.2.1 Anwendungsbeispiele 13 - 2
13.2.2 Die zentrale Position der LANCOM VoIP Router 13 - 4

13.3 Die Gesprächsvermittlung: Call-Routing 13 - 6
13.3.1 SIP-Proxy und SIP-Gateway 13 - 6
13.3.2 Die Anmeldung von Benutzern am SIP-Proxy 13 - 7
13.3.3 Rufnummernumsetzung an Netz-Übergängen 13 - 9
13.3.4 Der Call-Manager 13 - 9
13.3.5 Telefonieren mit dem LANCOM VoIP Router 13 - 10
13.3.6 Halten, Makeln, Verbinden 13 - 12
13.3.7 Übertragung von DTMF-Tönen 13 - 13
13.3.8 Gebühreninformationen an die internen ISDN-Busse übertragen 13 - 13
13.3.9 Unterstützung digitaler Rufe 13 - 14

13.4 Konfiguration der VoIP-Parameter 13 - 14
13.4.1 Allgemeine Einstellungen 13 - 14
13.4.2 Konfiguration der Benutzer 13 - 15
13.4.3 Konfiguration der Leitungen 13 - 21

13.5 Konfiguration des Call-Managers 13 - 31
13.5.1 Ablauf des Call-Routings 13 - 32
13.5.2 Behandlung der Calling Party ID 13 - 32
13.5.3 Die Parameter der Call-Routing-Tabelle 13 - 33
13.5.4 Codecs 13 - 37
13.5.5 Erweiterte Einstellungen 13 - 38

13.6 Telefonanlagenfunktion für LANCOM VoIP Router (PBX-Funktionen) 13 - 39
13.6.1 Anrufweiterschaltung (Verbinden und Rufumleitung) 13 - 39
13.6.2 Spontane Anrufsteuerung durch den Benutzer 13 - 43
13.6.3 Feste Anrufweiterschaltung konfigurieren 13 - 44
13.6.4 Faxen über T.38 – Fax over IP (FoIP) 13 - 45
13.6.5 Gruppenrufe mit Ruf-Verteilung 13 - 46
13.6.6 Mehrfachanmeldung (Multi-Login) 13 - 48

13.7 VoIP-Media-Proxy – Optimierte Verwaltung von SIP-Verbindungen 13 - 48

13.8 SIP-ID als Stammnummer bei Trunk-Leitungen 13 - 50

13.9 Vermittlung beim SIP-Provider 13 - 50

13.10 Behandlung kanonischer Rufnummern 13 - 51

13.11 Verarbeitung der Ziel-Domänen 13 - 51
13.11.1 Anmeldung an übergeordneten Vermittlungsstellen 13 - 51
13.11.2 Vermittlung von internen Rufen 13 - 51

13.12 Konfiguration der ISDN-Schnittstellen 13 - 52
13.12.1 Punkt-zu-Mehrpunkt und Punkt-zu-Punkt-Anschlüsse 13 - 52
13.12.2 Busterminierung, Life-Line-Support und Spannungsweiterleitung 13 - 52
13.12.3 Protokoll-Einstellung 13 - 53
13.12.4 Taktung der ISDN-Anschlüsse 13 - 54

13.13 Konfigurationsbeispiele 13 - 54
13.13.1 VoIP-Telefonie im Stand-alone-Einsatz 13 - 54
13.13.2 VoIP-Telefonie als Ergänzung zur übergeordneten ISDN-TK-Anlage 13 - 60
13.13.3 VoIP-Telefonie als Ergänzung zur untergeordneten ISDN-TK-Anlage 13 - 65
13.13.4 VoIP-Telefonie als Ergänzung zu vorhandenen ISDN-Telefonen 13 - 68
13.13.5 Anbindung an übergeordnete SIP-TK-Anlage 13 - 70
13.13.6 VoIP-Kopplung von Standorten ohne SIP-TK-Anlage 13 - 74
13.13.7 LANCOM VoIP Router an einem P2P-Anschluss (Anlagenanschluss) 13 - 77
13.13.8 SIP-Trunking 13 - 79
13.13.9 Remote Gateway 13 - 81

13.14 Diagnose der VoIP-Verbindungen 13 - 83
13.14.1 SIP Traces 13 - 83
13.14.2 Diagnose der Verbindungen mit dem LANmonitor 13 - 83

13 Voice over IP (VoIP)

13.1 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.) mit denen die Sprachkommunikation in IP-Netzwerken ermöglicht wird.

Im allgemeinen Sprachgebrauch werden für das Telefonieren über ein Netzwerk (LAN oder Internet) verschiedene Begriffe verwendet. Die Begriffe „Voice over IP" oder „IP-Telefonie" werden gleichwertig verwendet, obwohl sie im eigentlichen Sinn unterschiedliche Bedeutung 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 so genannten 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 so genannten „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.

Eine andere Möglichkeit bieten VoIP-Router, die in der Lage sind, VoIP-Gespräche auf eine ISDN-Leitung zu vermitteln. Beispiele sind verschiedene LANCOM VoIP Router mit SIP-Gateway und ISDN-Schnittstellen. Bei der Überleitung der Gespräche ins Festnetz werden die üblichen Gebühren des Telefonbetreibers berechnet.

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.

13.2 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). Einen Sonderfall stellt die ISDN-ISDN Brückenfunktion dar, die aktiviert wird, wenn ISDN-Protokolle nicht in SIP abgebildet werden können und daher eine bittransparente Verbindung zwischen einem ISDN-TE (externer ISDN-Anschluss) und ISDN-NT (interner ISDN-Anschluss) geschaffen wird.

Darüber hinaus wird die bittransparente Verbindung grundsätzlich bei Gesprächen zwischen mehreren lokalen ISDN Schnittstellen verwendet, um höchstmögliche Kompatibilität und Qualität zu erreichen.

13.2.1 Anwendungsbeispiele

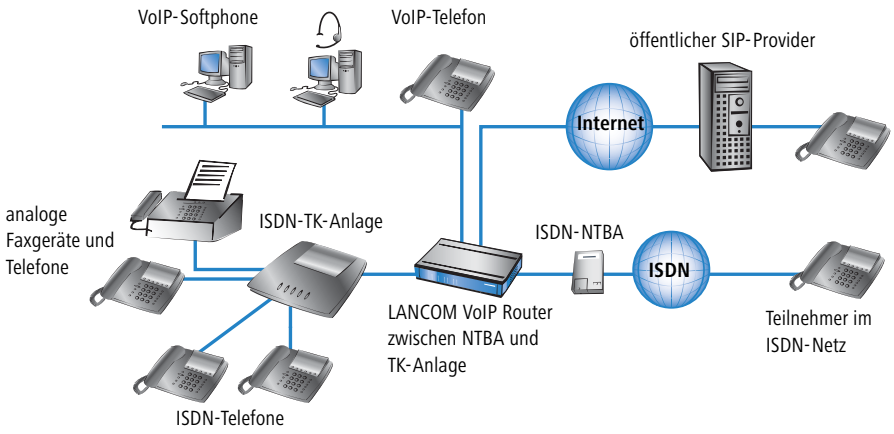
Voice-over-IP-Lösungen bringen Ihre Vorteile in einem sehr breiten Anwendungsspektrum ein, angefangen von kleinen Unternehmen bis hin zu großen Konzernen mit ausgedehntem Filialbetrieb. In diesem Abschnitt stellen wir einige Beispiele vor.



Konkrete Hinweise zur Konfiguration finden Sie im Kapitel 'Konfiguration der VoIP-Funktionen'.

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:

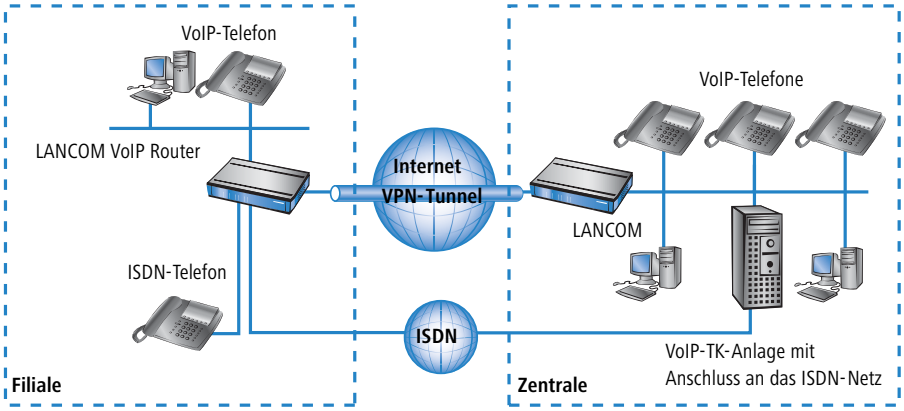
- Zu den bisher verwendeten ISDN-Telefonen können auch VoIP-Telefone oder VoIP-Softphones in die Telefonstruktur aufgenommen werden. Die VoIP-Teilnehmer im eigenen LAN können auch die externen Teilnehmer im ISDN-Netz erreichen.
- Die ISDN-Telefone lassen sich weiterhin verwenden, können aber zusätzlich 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.

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.

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.

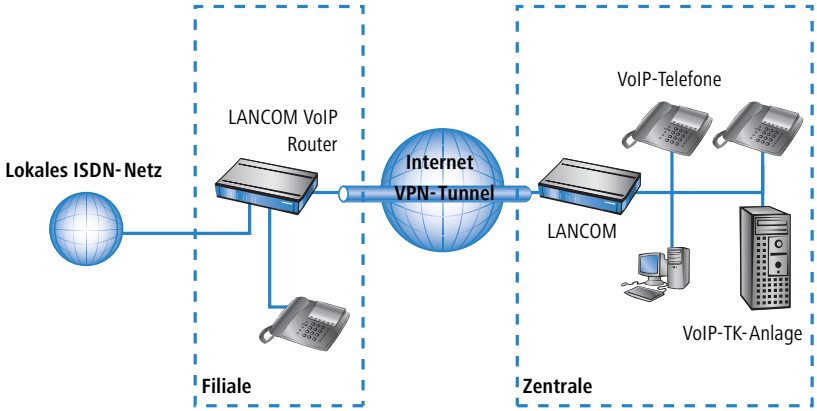
Einbindung lokaler ISDN-Anschlüsse mit Remote-SIP-Gateway

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.

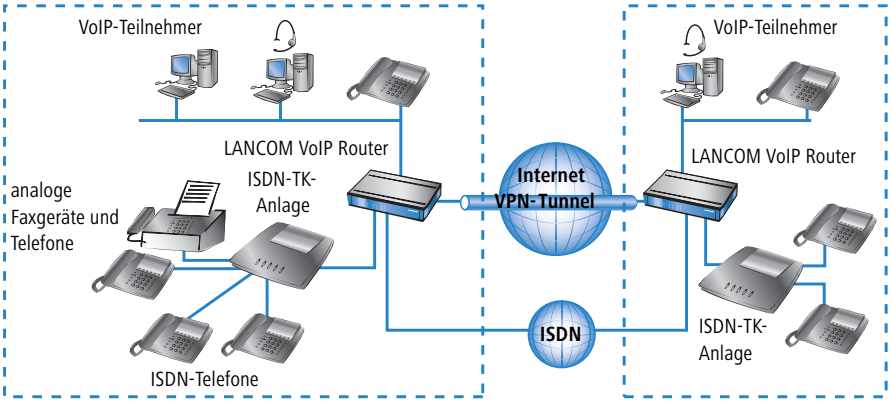


Die Vorteile des SIP-Gateways:

- 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.

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.

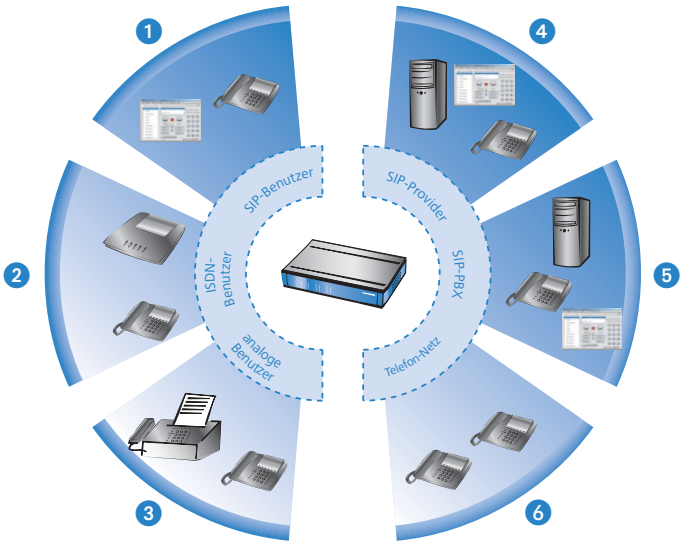
Die Vorteile der Peer-to-Peer-Standortverbindung

- 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.

13.2.2 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



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

  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

  Über LAN, WLAN und DMZ 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

  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

  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.

13.3 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 überlicherweise 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.

13.3.1 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

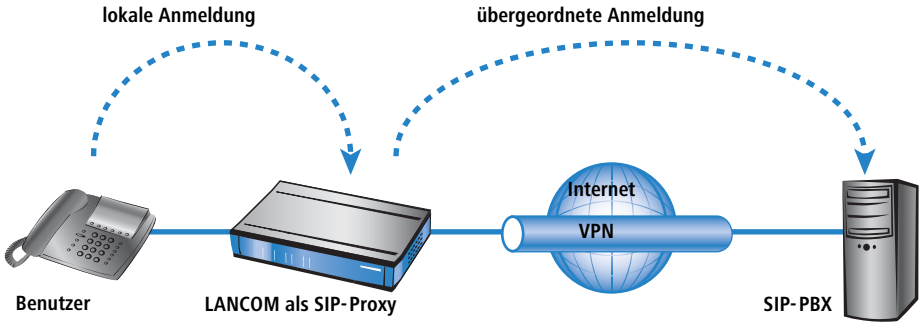
  Das SIP-Gateway übernimmt die Funktion des Umsetzers zwischen IP-basierender Telefonie auf Basis des SIP-Protokolls und anderen (Fernmelde-) Netzwerken, z.B. dem ISDN-Netz.

13.3.2 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 Anmeldungswunsch 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.

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. Gültig sind die interne VoIP- Domäne des LANCOM VoIP Router und alle Domänen, die in einer SIP- Leitung eingetragen sind.

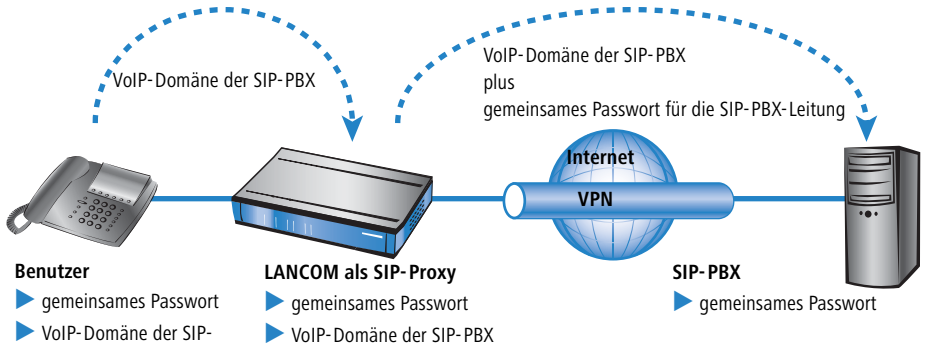
- Die Domäne wird bei SIP- Endgeräten im LAN (SIP- Telefon oder SIP- Softphone) in der Konfiguration eingetragen. Ein Eintrag als SIP- Benutzer in der Konfiguration des LANCOM ist nicht erforderlich. Diese Variante wird auch als „automatische Anmeldung" bezeichnet.
- Bei ISDN- Endgeräten kann die Domäne 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 (→ Dynamische ISDN- Benutzer an Anlagenanschlüssen).
- Um Anmeldungen von unbekannten Teilnehmern zu verhindern, kann für die lokale Anmeldung eine Authentifizierung am SIP- Proxy vorgeschrieben werden (lokale Authentifizierung). In diesem Fall ist immer ein Eintrag als SIP- oder ISDN- Benutzer in der Konfiguration des LANCOM notwendig.

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.

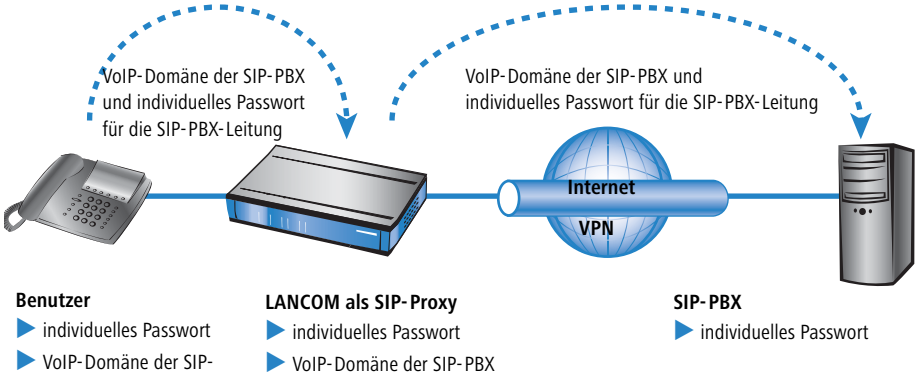
Anmeldung an übergeordnete SIP- PBX (übergeordnete Anmeldung)

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.



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?

Zur Beantwortung dieser Fragen unterscheiden wir folgende Konstellationen:

- 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 übemitteln 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.

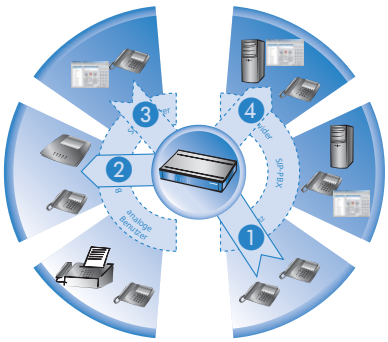
Durch einen ISDN-Benutzer-Eintrag mit einem #-Zeichen als Platzhalter für die Rufnummern können alle ISDN-Endgeräte mit den jeweiligen Durchwahlen als dynamische ISDN-Benutzer angelegt werden.

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.

13.3.3 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. So wird z.B. bei einem Anruf aus dem Festnetz an eine öffentliche MSN die Ziel-Rufnummer auf die interne Rufnummer eines ISDN-Benutzers umgesetzt. Die entsprechenden Umsetzungen werden auch als „Mapping" bezeichnet. Das Mapping umfasst dabei neben der **gerufenen** Nummer, die das Ziel darstellt, auch die **rufende** Nummer für die Quelle.



Mapping der Zielrufnummer
1. externe MSN aus dem ISDN-Netz
2. interne Rufnummer des ISDN-Benutzers

Mapping der Quellrufnummer
3. interne Rufnummer des SIP-Benutzers
4. externe SIP-Rufnummer im Netz des SIP-Providers

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.

13.3.4 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.

13.3.5 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.

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.

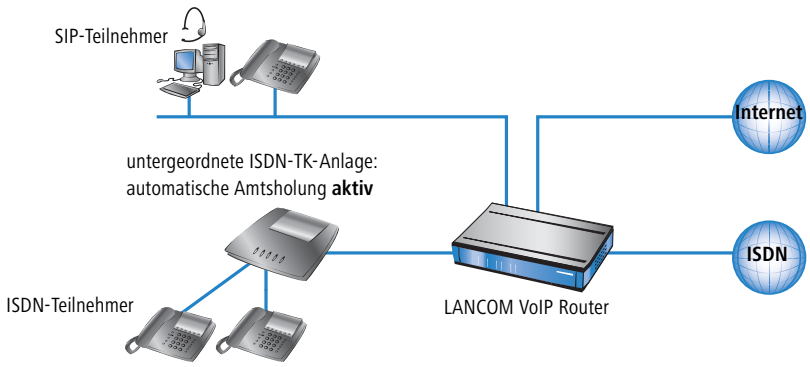
- Wenn die automatische Amtsholung eingeschaltet ist, werden alle Rufe zunächst als Gespräch über ein öffentliches Telefonnetz geführt.

  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

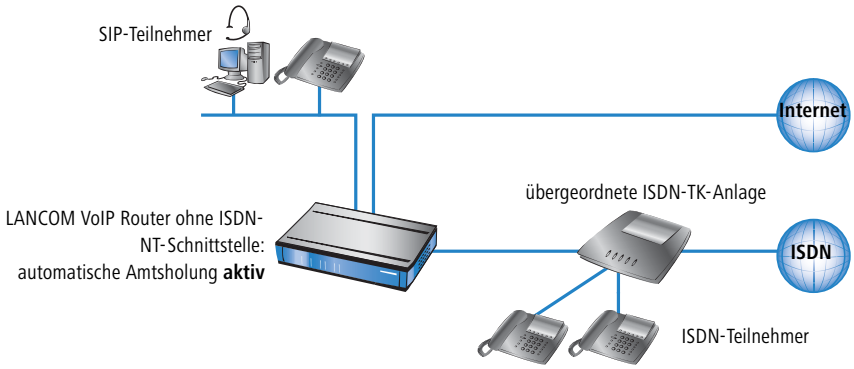
Ein LANCOM VoIP Router wird zwischen dem ISDN-Amtsanschluss und die vorhandene ISDN-TK-Anlage geschaltet. In der TK-Anlage wird die automatische Amtsholung aktiviert, die Einstellungen im Call-Router des LANCOM VoIP Router entscheiden darüber, ob bei den angeschlossenen ISDN- und SIP-Teilnehmern eine „0" für die Amtsholung vorgewählt werden muss.



Wenn der LANCOM VoIP Router in dieser Konstellation z.B. durch Stromausfall nicht zur Verfügung steht, wird der ISDN-Anschluss der untergeordneten ISDN-TK-Anlage automatisch auf den externen ISDN-Anschluss „gebrückt" (bei aktiviertem Life-Line-Support). Bei einem LANCOM VoIP Router **ohne** automatische Amtsholung dürfen die ISDN-Teilnehmer für die Zeit des Life-Line-Betriebes der Rufnummer keine „0" voranstellen.

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.



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 ('Automatische Amtsholung' → Seite 13-10) 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 ('Automatische Amtsholung' → Seite 13-10) 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 ('Automatische Amtsholung' → Seite 13-10) muss ggf. eine „0" vorangestellt werden.

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.

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.

13.3.6 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.

13.3.7 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.

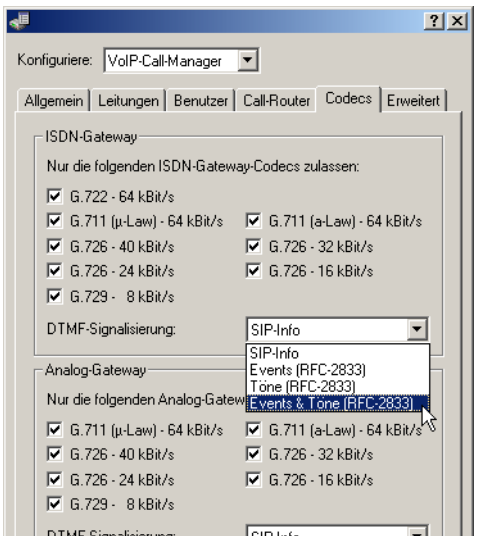
Grundsätzlich können die DTMF-Töne bei VoIP-Anwendungen auf zwei Arten übertragen werden:

- 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)
  - RC 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.

Konfiguration der DTMF-Signalisierung

Bei der Konfiguration der DTMF-Signalisierung wird eingestellt, welche Variante zur Übertragung der DTMF-Töne verwendet werden soll:



LANconfig: VoIP-Call-Manager ▶ Erweitert

WEBconfig: LCOS Menübaum ▶ Setup ▶ Voice-Call-Manager ▶ Allgemein

13.3.8 Gebühreninformationen an die internen ISDN-Busse übertragen

LANCOM VoIP Router unterstützen zwei verschiedene Varianten des Dienstmerkmals AOC (Advice of Charge) zur Übermittlung von Gebühreninformationen:

- AOC-D bezeichnet die Übertragung der Gebühreninformationen während des Gespräches.
- AOC-E bezeichnet die Übertragung der Gebühreninformationen nach Beendigung des Gespräches.

Die Gebühreninformationen nach den beiden AOC-Varianten werden vom LANCOM VoIP Router zwischen internen und externen ISDN-Bussen übertragen. AOC-D Gebühreninformationen können in Richtung der analogen Benutzer

an den internen Analog-Schnittstellen auf einen Gebührenimpuls umgesetzt werden, wenn die entsprechende Option aktiviert ist.

13.3.9 Unterstützung digitaler Rufe

LANCOM VoIP Router unterstützen digitale Rufe, wie sie z.B. bei der Nutzung von Faxgeräten der Gruppe 4 oder bei der Verwendung von ISDN-Endgeräten zur Einwahl in bestimmte Netze verwendet werden. Um diese Rufe zielgerichtet über ein ISDN-Interface des LANCOM VoIP Router zu leiten, können der Zielrufnummer beim Wählen spezielle Kennziffern vorangestellt werden ('Wählen über bestimmte Leitungen' → Seite 13-12).

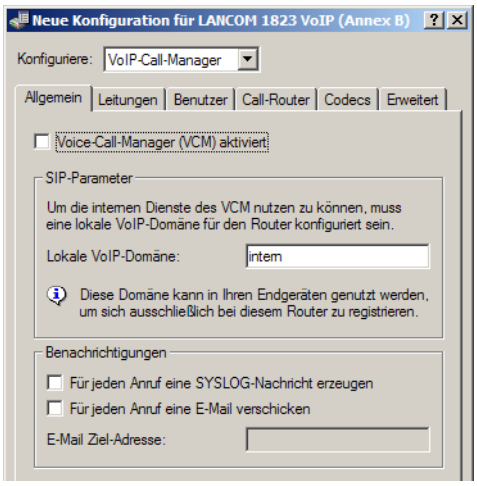
13.4 Konfiguration der VoIP-Parameter

Änderungen mit LCOS 7.6:

- Angabe des folgenden Parameters für SIP-, ISDN- und Analog-User:
  - CLIR
- Angabe der folgenden Parameter für SIP-Provider- und SIP-PBX-Lines:
  - Lokale-Portnummer
  - (Re-)Registrierung
  - Leitungsüberwachung
  - Überwachungsintervall
  - Vertrauenswürdig
  - Privacy-Methode
- Angabe der folgenden Parameter für Analog-Lines:
  - Caller-ID Signaling
  - Caller-ID Transmission Requirements

13.4.1 Allgemeine Einstellungen

LANconfig: VoIP-Call-Manager ▶ Allgemein



- **Voice-Call-Manager (VCM) aktiviert**
  Schaltet den Voice-Call-Manager aktiv / nicht aktiv
- **Domain**
  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 zur Nutzung dieser Funktion die entsprechenden SYSLOG-Einstellungen vorgenommen werden müssen ('SYSLOG' → Seite 5-10).

■ **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 zur Nutzung dieser Funktion ein SMTP-Konto eingerichtet sein muss.

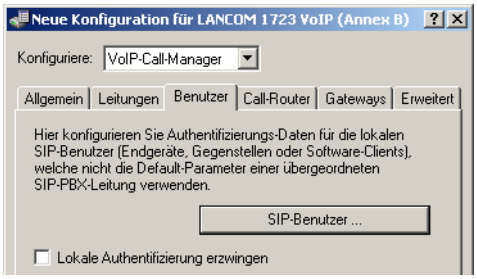
13.4.2 Konfiguration der Benutzer

Lokale Benutzer sind die am LANCOM VoIP Router angeschlossenen Endgeräte/Telefone. Es wird unterschieden zwischen:

- SIP-Benutzer: Benutzer, die über ein SIP-Telefon an das LAN angeschlossen sind. Dabei ist es für die Konfiguration des Benutzers egal, ob das LAN direkt am LANCOM angeschlossen ist, oder über ein VPN (über das Internet) angeschlossen ist.
- ISDN-Benutzer: Benutzer, die über ISDN angeschlossen sind. Sie verwenden das SIP-Gateway, um über die VoIP-Funktion zu telefonieren.
- Analog-Benutzer: Benutzer, die an die analogen Schnittstellen angeschlossen sind. Sie verwenden das SIP-Gateway, um über die VoIP-Funktion zu telefonieren.

Allgemeine Einstellungen für alle SIP-Benutzer

LANconfig: VoIP-Call-Manager ▶ Benutzer



WEBconfig: LCOS-Menübaum ▶ Setup ▶ Voice-Call-Manager ▶ General

■ **Lokale Authentifizierung erzwingen**

Normalerweise akzeptiert der SIP-Proxy Anmeldung von allen SIP-Benutzern, die sich mit einer gültigen Domain anmelden. Wird die lokale Authentifizierung erzwungen, können sich nur solche Teilnehmer beim SIP-Proxy anmelden, die in einer der Benutzertabellen mit den entsprechenden Zugangsdaten hinterlegt sind.

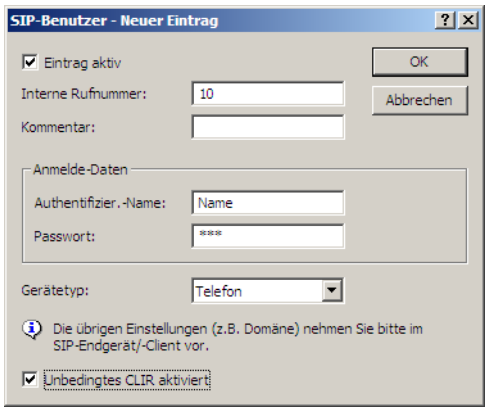
Die automatische Anmeldung ohne Eintrag eines Passworts ist auf die SIP-Benutzer im LAN beschränkt. SIP-Benutzer aus dem WAN und ISDN- sowie Analog-Benutzer müssen immer über einen entsprechenden Benutzer-Eintrag mit Passwort authentifiziert werden.

SIP-Benutzer

Je nach Modell können unterschiedlich viele SIP-Benutzer angelegt werden. Mehr als die erlaubte Anzahl Benutzer können nicht angelegt werden, ebenso werden gleiche Namen oder gleiche Rufnummern nicht zugelassen.

Die vom SIP-Teilnehmer verwendete Domäne wird üblicherweise im Endgerät selbst eingestellt.

LANconfig: VoIP-Call-Manager ▶ Benutzer ▶ SIP-Benutzer



WEBconfig: LCOS-Menübaum ▶ Setup ▶ Voice-Call-Manager ▶ User ▶ SIP-User

Zur Definition eines SIP-Benutzers können die folgenden Parameter eingetragen werden:

- **Number/Name**

  Telefonnummer des SIP-Telefons oder Name des Benutzers (SIP-URI).

- **Auth-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).

- **Secret**

  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-Line) anmelden.

- **Device-Type**

  Typ des angeschlossenen Geräts.

- **CLIR**

  Schaltet die Übermittlung der Absenderinformationen ein oder aus.

- **Active**

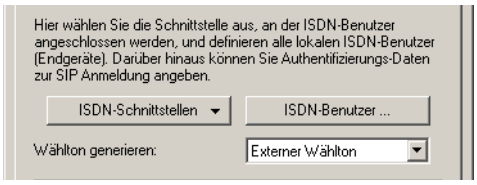
  Aktiviert oder deaktiviert den Eintrag.

- **Kommentar**

  Kommentar zu diesem Eintrag

Allgemeine Einstellungen für alle ISDN-Benutzer

LANconfig: VoIP-Call-Manager ▶ Benutzer



WEBconfig: LCOS-Menübaum ▶ Setup ▶ Voice-Call-Manager ▶ General

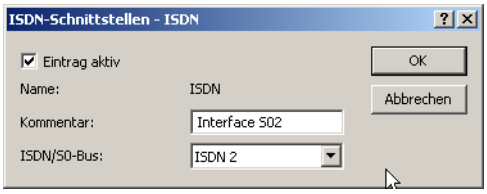
- **Wählton generieren**

  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, 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.

ISDN-Schnittstellen

Für die Benutzer, die über die ISDN-Leitung angeschlossen sind, wird global das verwendete Interface konfiguriert. 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.

LANconfig: VoIP-Call-Manager ▶ Benutzer ▶ ISDN-Schnittstellen

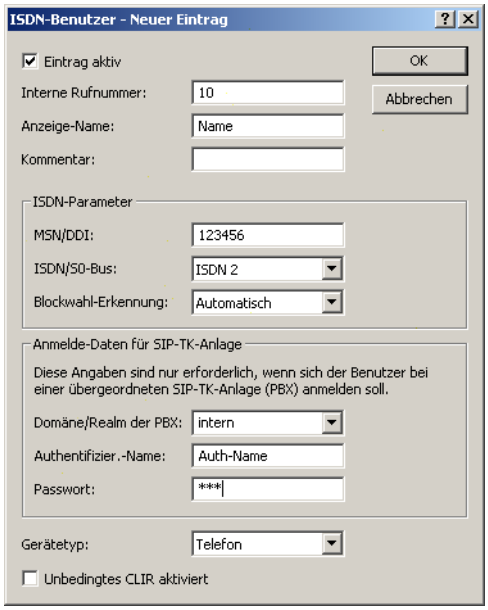


WEBconfig: LCOS-Menübaum ▶ Setup ▶ Voice-Call-Manager ▶ User ▶ Interfaces

- **ISDN-Schnittstelle**
  Interface, an das die ISDN-Teilnehmer angeschlossen sind.
- **Eintrag aktiv**
  Interface ist aktiv / nicht aktiv
- **Kommentar**
  Kommentar zum ISDN-Interface

ISDN-Benutzer

LANconfig: VoIP-Call-Manager ▶ Benutzer ▶ ISDN-Benutzer



WEBconfig: LCOS-Menübaum ▶ Setup ▶ Voice-Call-Manager ▶ User ▶ ISDN-User

- **Number/Name**
  Interne Rufnummer des ISDN-Telefons oder Name des Benutzers (SIP-URI).

Mit dem #-Zeichen als Platzhalter können ganze Gruppen von Rufnummern z.B. bei der Verwendung von Durchwahlnummern an einem Anlagenanschluss in einem einzigen Eintrag erfaßt werden. Mit der Rufnummer '#' und der DDI '#' werden z.B. die Durchwahlnummern ohne Veränderung in interne Rufnummern umgesetzt. Mit der Rufnummer '3#' und der DDI '#' wird z.B. ein ankommender Ruf für die Durchwahl '55' an die interne Rufnummer '355' weitergeleitet, bei ausgehenden Rufen von der internen Rufnummer '377' wird die '77' als Durchwahl verwendet.

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.

- **Ifc**

  ISDN-Interface, das für den Verbindungsaufbau verwendet werden soll.

- **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 ganze Gruppen von Rufnummern z.B. bei der Verwendung von Durchwahlnummern in einem einzigen Eintrag erfaßt 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.

- **Auth-Name**

  Name zur Authentifizierung an einer übergeordneten SIP-TK-Anlage, wenn die Domäne des Benutzers mit der Domäne einer SIP-PBX-Line übereinstimmt.

- **Display-Name**

  Name, der auf dem angerufenen Telefondisplay erscheinen soll.

- **Secret**

  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.

- **Domain**

  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.

- **Device-Type**

  Typ des angeschlossenen Gerätes.

- **DialCompl**

  Blockwahlerkennung.

- **CLIR**

  Schaltet die Übermittlung der Absenderinformationen ein oder aus.

- **Active**

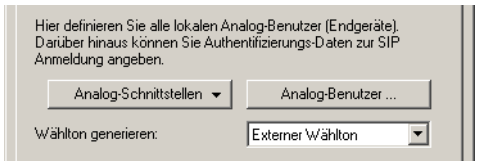
  Aktiviert oder deaktiviert den Eintrag.

- **Kommentar**

  Kommentar zu diesem Eintrag.

Allgemeine Einstellungen für alle Analog-Benutzer

LANconfig: VoIP-Call-Manager ▶ Benutzer



WEBconfig: LCOS-Menübaum ▶ Setup ▶ Voice-Call-Manager ▶ General

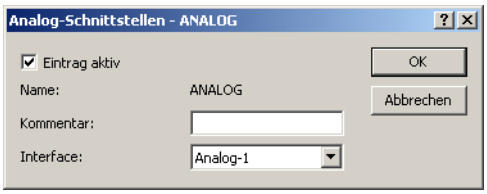
- **Wählton generieren**

  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: VoIP-Call-Manager ▶ Benutzer ▶ Analog-Schnittstellen



WEBconfig: LCOS-Menübaum ▶ Setup ▶ Voice-Call-Manager ▶ User ▶ Interfaces

- **Interface**

  Ein internes Interface, an das Analog-Teilnehmer angeschlossen sind.

- **Eintrag aktiv**

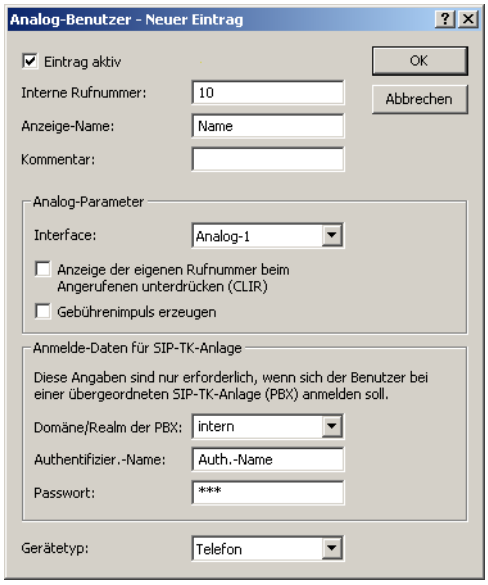
  Interface ist aktiv / nicht aktiv

- **Kommentar**

  Kommentar zur Analog-Schnittstelle

Analog-Benutzer

LANconfig: VoIP-Call-Manager ▶ Benutzer ▶ Analog-Benutzer



WEBconfig: LCOS-Menübaum ▶ Setup ▶ Voice-Call-Manager ▶ User ▶ Analog-User

- **Number/Name**

  Interne Rufnummer des Analog-Telefons oder Name des Benutzers (SIP-URI).

- **Auth-Name**

  Name zur Authentifizierung an einer übergeordneten SIP-TK-Anlage, wenn die Domäne des Benutzers mit der Domäne einer SIP-PBX-Line übereinstimmt.

- **Display-Name**

  Name, der auf dem angerufenen Telefondisplay erscheinen soll.

- **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.

- **Ifc**

  Analoges-Interface, das für den Verbindungsaufbau verwendet werden soll.

- **CLIR**

  Schaltet die Übermittlung der Absenderinformationen ein oder aus.

- **Gebührenimpuls**

  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.

- **Domain**

  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.

- **Device-Type**

  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.

- **Active**

  Aktiviert oder deaktiviert den Eintrag.

- **Kommentar**

  Kommentar zu diesem Eintrag

Allgemeine Einstellungen für alle SIP-, ISDN- und Analog-Benutzer

LANconfig: VoIP-Call-Manager ▶ Benutzer



WEBconfig: LCOS-Menübaum ▶ Setup ▶ Voice-Call-Manager ▶ General

- **Wählende-Erkennung nach**

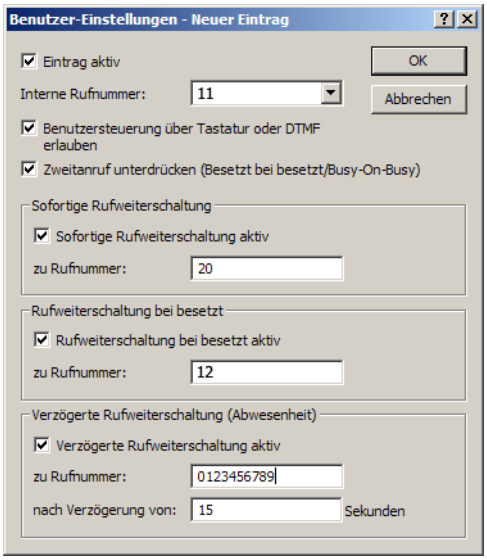
  Für diese Zeit wird bei der Wahl von einem ISDN-Telefon gewartet, bis die Rufnummer als vollständig angesehen wird und an den Call-Router übergeben wird.

  Sonderwerte: Bei einer Wählverzögerung von '0' muss die Eingabe der Rufnummer mit einem '#' abgeschlossen werden. Die Eingabe des Zeichens '#' nach der Rufnummer verkürzt die Wählverzögerung manuell.

Benutzer-Einstellungen

Zur Konfiguration der Benutzer-Einstellungen im LANCOM stehen folgende Parameter bereit:

LANconfig: VoIP-Call-Manager ▶ Benutzer ▶ Benutzer-Einstellungen



WEBconfig: LCOS-Menübaum ▶ Setup ▶ Voice-Call-Manager ▶ User ▶ Extensions

- **Eintrag aktiv**

  Aktiviert oder deaktiviert den 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. auch das „Anklopfen" wird verhindert. 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.

- **Sofortige Rufweiterschaltung (CFU)**

  Aktiviert oder deaktiviert die sofortige Rufweiterschaltung (CFU) ohne Bedingung.

- **zu Rufnummer**

  Ziel für die sofortige Rufweiterschaltung ohne Bedingung.

- **Rufweiterschaltung bei besetzt (CFB)**

  Aktiviert oder deaktiviert die Weiterschaltung bei „besetzt".

- **zu Rufnummer**

  Ziel für die Weiterschaltung bei „besetzt".

- **Verzögerte Rufweiterschaltung (CFNR)**

  Aktiviert oder deaktiviert die verzögerte Rufweiterschaltung (bei Abwesenheit; CFNR).

- **zu Rufnummer**

  Ziel für die verzögerte Rufweiterschaltung.

- **Verzögerung**

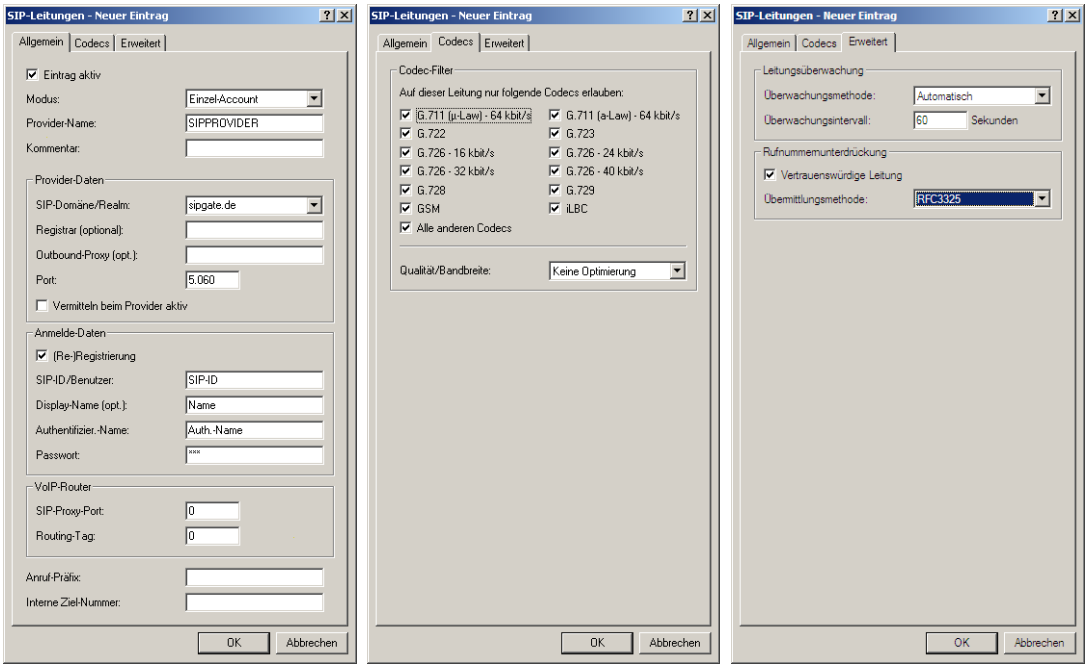
  Wartezeit für die verzögerte Rufweiterschaltung. Nach Ablauf dieser Zeit wird der Anruf an das Rufziel weitergeleitet, wenn der Teilnehmer den Anruf nicht annimmt.

13.4.3 Konfiguration der Leitungen

SIP-Provider-Line

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.

LANconfig: VoIP-Call-Manager ▶ Leitungen ▶ SIP-Leitungen



WEBconfig: LCOS-Menübaum ▶ Setup ▶ Voice-Call-Manager ▶ Line ▶ SIP-Provider

■ **Name**

Der Name der Leitung, darf nicht identisch sein mit einer anderen in dem Gerät konfigurierten Leitung.

■ **Mode**

Mit dieser Auswahl bestimmen Sie die Betriebsart der SIP-Leitung.

Mögliche Werte:

□ Einzel-Account-Modus: 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.

Tabelle für die Rufnummernumsetzung:

Einzel-Account	An der Leitung anliegende SIP-Nummer	Von der Leitung abgesetzte SIP-Nummer
Ausgehender Ruf	"From:"	Beim Provider registrierte Nummer (User-ID)
Eingehender Ruf	"To:"	User-ID

□ Trunk-Modus: 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 nur durch die zur Verfügung stehende Bandbreite begrenzt.

Tabelle für die Rufnummernumsetzung:

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-Modus: 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 regel-

mäßig 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 nur durch die zur Verfügung stehende Bandbreite begrenzt.

Tabelle für die Rufnummernumsetzung:

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-Modus: 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 nur durch die zur Verfügung stehende Bandbreite begrenzt.

Tabelle für die Rufnummernumsetzung:

Link	An der Leitung anliegende SIP-Nummer	Von der Leitung abgesetzte SIP-Nummer
Ausgehender Ruf	"From:"	"From:"
Eingehender Ruf	"To:"	"To:"

■ **Domain**

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.

■ **Rtg-Tag**

Routing-Tag zur Auswahl einer bestimmten Route über die Routing-Tabelle für Verbindungen zu diesem SIP-Provider.

■ **Port**

TCP/UDP-Port beim SIP-Provider, an den die SIP-Pakete gesendet werden.



In der Firewall muss dieser Port freigeschaltet sein, damit die Verbindung funktionieren kann.

■ **User-id**

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 der Leitungstyp SIP-PBX-Leitung gewählt werden.

■ **Auth-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 der Leitungstyp SIP-PBX-Leitung gewählt 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 bzw. auf dem Endgerät hinterlegten Daten bei einer übergeordneten Instanz registriert werden sollen, muss der Leitungstyp SIP-PBX-Leitung gewählt werden.

■ **Secret**

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 bzw. auf dem Endgerät hinterlegten Daten bei einer übergeordneten Instanz registriert werden sollen, muss der Leitungstyp SIP-PBX-Leitung gewählt werden.

■ **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).

■ **Outb-proxy**

Der Outbound-Proxy des SIP-Providers nimmt alle vom LANCOM ausgehenden SIP-Signalisierungen 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 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).

■ **Cln-Prefix**

Das Anruf-Präfix ist eine Nummer, die den Anrufer-Nummern (CLI; SIP „From:") aller ankommenden Anrufe auf dieser SIP-Provider-Leitung vorangestellt wird, um eindeutige Rückruf-Nummern zu erzeugen.

Beispielsweise kann hier eine Nummer ergänzt werden, die im Call-Router bei abgehenden Rufen (dem Rückruf) zur Leitungsauswahl ausgewertet und wieder entfernt wird.

■ **Number/Name**

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.

■ **Codecs**

Die beteiligten Endgeräte handeln beim Verbindungsaufbau aus, welche Codecs für die Komprimierung der Sprachdaten verwendet werden sollen. Mit dem Codec-Filter können Sie die erlaubten Codecs einschränken und nur bestimmte Codecs zulassen.

Falls die Schnittmenge an verfügbaren Codecs der beteiligten Endgeräte hier ausgeschaltet wird, kommt keine Verbindung zustande.

■ **Codec-Order**

Mit diesem Parameter beeinflussen Sie die Reihenfolge, in der die möglichen Codecs beim Verbindungsaufbau angeboten werden.

■ **Refer-weiterleiten**

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 vebindende Gesprächsteilnehmer über diese SIP-Provider-Leitung erreicht werden (andernfalls übernimmt der Media-Proxy im LANCOM die Vermittlung der Medienströme, z.B. beim Verbinden zwischen zwei SIP-Provider-Leitungen).

Eine Übersicht über die wichtigsten SIP-Provider, die diese Funktion unterstützen, finden Sie im Support-Bereich auf der Internet-Seite.

■ **Lokale-Portnummer**

Dies ist der Port des LANCOM-Proxies zur Kommunikation mit dem Provider.

Wenn die (Re-)Registrierung der Leitung deaktiviert ist, muss der lokale Port fest vorgegeben und als Zielport auch auf der Providerseite eingetragen werden (z.B. bei Nutzung eines regsitrierungslosen Trunks im Firmen-VPN), damit sich beide Seiten SIP-Signalisierungen senden können.

■ **(Re-)Registrierung**

Hiermit wird die (wiederholte) Registrierung der SIP-Provider-Leitung aktiviert. Die Registrierung kann auch zur Leitungsüberwachung herangezogen werden.

Für die Nutzung der (Re-)Registrierung muss die Methode der Leitungsüberwachung entsprechend auf "Registrierung" oder "Automatisch" gestellt werden. Die Registrierung wird jeweils nach Ablauf des Überwachungsintervalls wiederholt. Wenn der SIP-Registrar des Providers ein anderes Intervall vorschlägt, wird dieses automatisch übernommen.

■ **Leitungsüberwachung**

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:

- □ Auto: 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 sowohl auf die Leitungsüberwachung mit Register-Request als auch mit Option-Request aus. Das Überwachungsintervall muss mindestens 60 Sekunden betragen und legt fest, nach welcher Zeit die Überwachungsmethode erneut angewendet wird. Wenn die (Re-)Registrierung aktiviert ist, wird das Überwachungsintervall auch als Zeitraum bis zur nächsten Registrierung verwendet.

Falls die Gegenstelle in der Antwort auf einen Option-Request einen anderen Wert für das Überwachungsintervall vorschlägt, so wird dieser akzeptiert und in der Folgezeit verwendet.

■ **Vertrauenswürdig**

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.

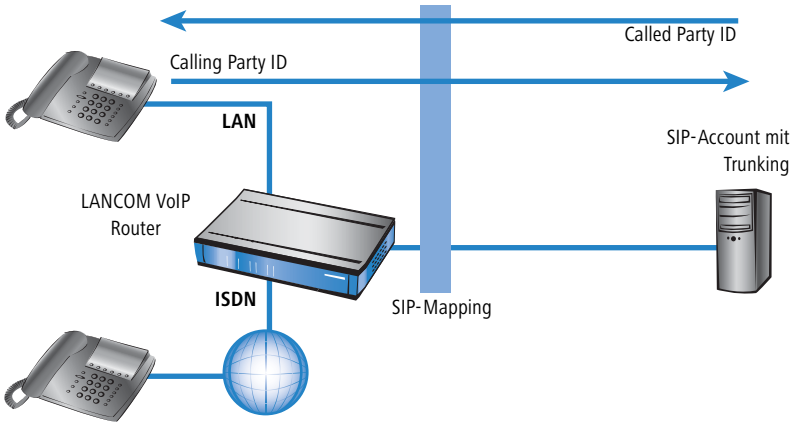
- **Privacy-Methode**
  Spezifiziert die verwendete Methode zur Übermittlung der Caller ID im separaten SIP-Header-Feld.
- **Active**
  Aktiviert oder deaktiviert den Eintrag.
- **Kommentar**
  Kommentar zu diesem Eintrag.

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.

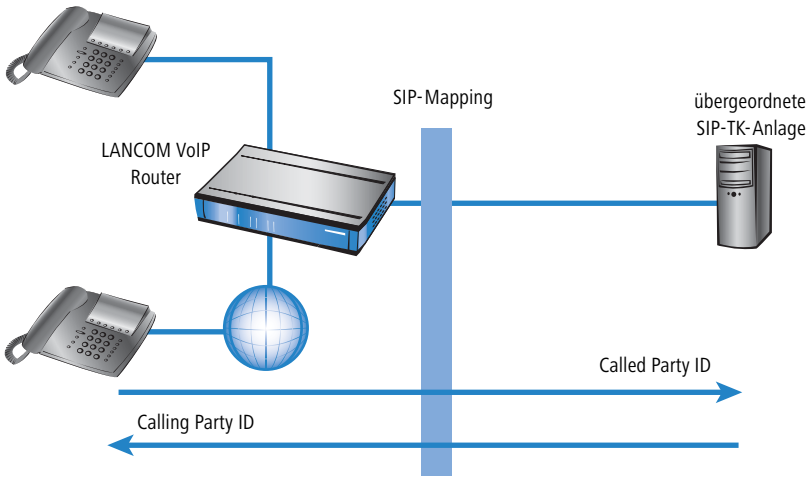
- Bei einer SIP-Leitung im Trunk-Modus wird eine Anpassung der intern verwendeten Rufnummern an den Rufnummernkreis des SIP-Accounts vorgenommen.
  - Bei ankommenden Rufen wird die Zielrufnummer (Called Party ID) verändert. Die interne Nummer wird eingesetzt, wenn die Called Party ID mit der externen 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.

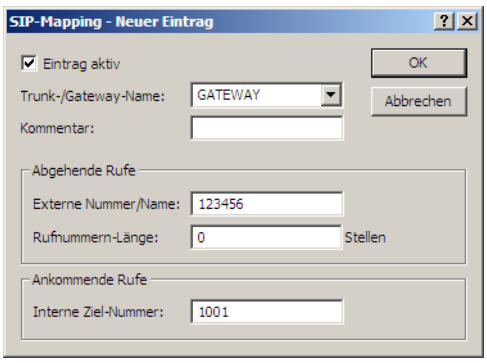


- Bei einer SIP-Leitung im Gateway-Modus wird eine Anpassung des Rufnummernplans der übergeordneten SIP-TK-Anlage an die internen Nummern des Call-Routers vorgenommen.
  - Bei ankommenden Rufen (von der SIP-Leitung) wird die Absenderrufnummer (Calling Party ID) verändert. Die interne Nummer wird eingesetzt, 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.



LANconfig: VoIP-Call-Manager ▶ Leitungen ▶ SIP-Mapping



WEBconfig: LCOS-Menübaum ▶ Setup ▶ Voice-Call-Manager ▶ Line ▶ SIP-Provider ▶ Mapping

■ **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**

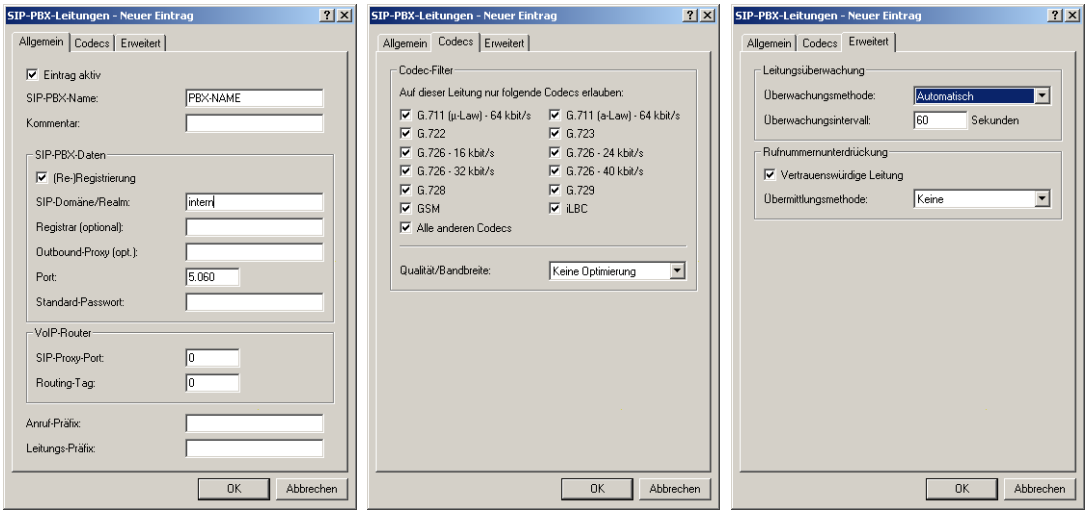
Rufnummer im Bereich des LANCOM VoIP Router.

Mit dem #-Zeichen als Platzhalter können ganze Rufnummernblöcke in einer Regel erfasst werden.

SIP-PBX-Line

Über diese Leitungen werden Verbindungen zu übergeordneten SIP-TK-Anlagen konfiguriert, die in der Regel über VPN angebunden sind.

LANconfig: VoIP-Call-Manager ▶ Leitungen ▶ SIP-PBX-Leitungen



WEBconfig: LCOS-Menübaum ▶ Setup ▶ Voice-Call-Manager ▶ Line ▶ SIP-PBX

- **Name**

  Name der Leitung, darf nicht identisch sein mit einer anderen in dem Gerät konfigurierten Leitung.

- **Domain**

  SIP-Domäne/Realm der übergeordneten SIP-TK-Anlage.

- **Rtg-Tag**

  Routing-Tag zur Auswahl einer bestimmten Route über die Routing-Tabelle für Verbindungen zu dieser SIP-TK-Anlage.

- **Port**

  TCP/UDP-Port der übergeordneten SIP-TK-Anlage, an den die SIP-Pakete vom LANCOM aus gesendet werden.



In der Firewall muss dieser Port freigeschaltet sein, damit die Verbindung funktionieren kann.

- **Secret**

  Gemeinsames Passwort zum Anmelden an der SIP-TK-Anlage. Dieses Passwort wird nur benötigt, wenn sich SIP-Teilnehmer an der TK-Anlage anmelden sollen, die nicht als SIP-Benutzer mit eigenen Zugangsdaten in der Liste der SIP-Benutzer angelegt sind, oder keine lokale Authentifizierung erzwungen wird, so dass sich SIP-Benutzer ohne Passwort am LANCOM anmelden können, aber mit einem gemeinsamen Passwort bei der übergeordneten SIP-TK-Anlage angemeldet werden, wenn die Domäne der SIP-Benutzer mit der Domäne der SIP-PBX-Line übereinstimmt.

- **Registrar**

  Der SIP-Registrar ist die Stelle, welche die Anmeldung mit den konfigurierten Authentifizierungsdaten für diesen Account in der SIP-TK-Anlage entgegen nimmt.

- **Cln-Prefix**

  Das Anruf-Präfix ist eine Nummer, die den Anrufer-Nummern (CLI; SIP „From:“) aller ankommenden Anrufe auf dieser SIP-PBX-Leitung vorangestellt wird, um eindeutige Rückruf-Nummern zu erzeugen.

  Beispielsweise kann hier eine Nummer ergänzt werden, die im Call-Router bei abgehenden Rufen (dem Rückruf) zur Leitungsauswahl ausgewertet und wieder entfernt wird.

- **Line-Prefix**

  Bei ausgehenden Anrufen über diese Leitung wird der angerufenen Rufnummer dieses Präfix vorangestellt, um eine vollständige für diese Leitung gültige Rufnummer zu erzeugen. Bei ankommenden Rufen wird dieses Präfix entfernt, falls vorhanden.

- **Codecs**

  Die beteiligten Endgeräte handeln beim Verbindungsaufbau aus, welche Codecs für die Komprimierung der Sprachdaten verwendeten werden sollen. Mit dem Codec-Filter können Sie die erlaubten Codecs einschränken und nur bestimmte Codecs zulassen.

Falls die Schnittmenge an verfügbaren Codecs der beteiligten Endgeräte hier ausgeschaltet wird, kommt keine Verbindung zustande.

- **Codec-Order**

  Mit diesem Parameter beeinflussen Sie die Reihenfolge, in der die möglichen Codecs beim Verbindungsaufbau angeboten werden.

- **Lokale-Portnummer**

  Dies ist der Port des LANCOM-Proxies zur Kommunikation mit der übergeordneten SIP-TK-Anlage.

Wenn die (Re-)Registrierung der Leitung deaktiviert ist, muss der lokale Port fest vorgegeben und als Zielport auch in der SIP-TK-Anlage eingetragen werden, damit sich beide Seiten SIP-Signalisierungen senden können.

- **(Re-)Registrierung**

  Hiermit wird die (wiederholte) Registrierung der SIP-PBX-Leitung aktiviert. Die Registrierung kann auch zur Leitungsüberwachung herangezogen werden.

Für die Nutzung der (Re-)Registrierung muss die Methode der Leitungsüberwachung entsprechend auf "Registrierung" oder "Automatisch" gestellt werden. Die Registrierung wird jeweils nach Ablauf des Überwachungsintervalls wiederholt. Wenn der SIP-Registrar der SIP-TK-Anlage ein anderes Intervall vorschlägt, wird dieses automatisch übernommen.

- **Leitungsüberwachung**

  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.

- **Überwachungsintervall**

  Das Intervall der Leitungsüberwachung in Sekunden. Dieser Wert wirkt sich sowohl auf die Leitungsüberwachung mit Register-Request als auch mit Option-Request aus. Das Überwachungsintervall muss mindestens 60 Sekunden betragen und legt fest, nach welcher Zeit die Überwachungsmethode erneut angewendet wird. Wenn die (Re-)Registrierung aktiviert ist, wird das Überwachungsintervall auch als Zeitraum bis zur nächsten Registrierung verwendet.

Falls die Gegenstelle in der Antwort auf einen Option-Request einen anderen Wert für das Überwachungsintervall vorschlägt, so wird dieser akzeptiert und in der Folgezeit verwendet.

- **Vertrauenswürdig**

  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.

- **Privacy-Methode**

  Spezifiziert die verwendete Methode zur Übermittlung der Absenderinformationen im separaten SIP-Feld.

- **Active**

  Aktiviert oder deaktiviert den Eintrag.

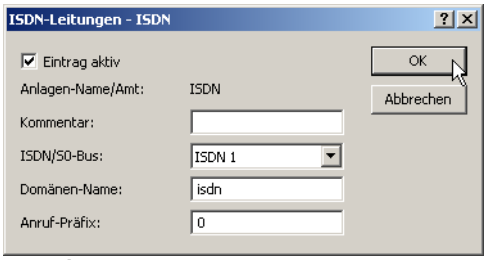
- **Kommentar**

  Kommentar zu diesem Eintrag.

ISDN-Leitungen

LANconfig: VoIP-Call-Manager ▶ Leitungen ▶ ISDN-Leitungen

WEBconfig: LCOS-Menübaum ▶ Setup ▶ Voice-Call-Manager ▶ Line ▶ ISDN



- **Anlagen- Name/Amt**

  Name der Leitung, darf nicht identisch sein mit einer anderen in dem Gerät konfigurierten Leitung.

- **ISDN/S_0- Bus, Ifc**

  ISDN- Schnittstelle(n), über die der LANCOM Wireless Router an das ISDN- Netz angeschlossen ist. Die eingetragenen Leitungen werden normalerweise als ISDN-TE konfiguriert.

- **Domänen- Name, Domain**

  Domäne, unter der die Anrufe von / zu der ISDN- Leitung in der SIP- Welt des LANCOM verwaltet werden.

- **Anruf- Präfix, Cln- Prefix**

  Bei eingehenden Anrufen über diese Leitung wird der anrufenden Rufnummer dieses Präfix vorangestellt, um bei einem Rückruf automatisch die richtige Leitung auswählen zu können.

- **Eintrag aktiv, Active**

  Leitung ist aktiv / nicht aktiv

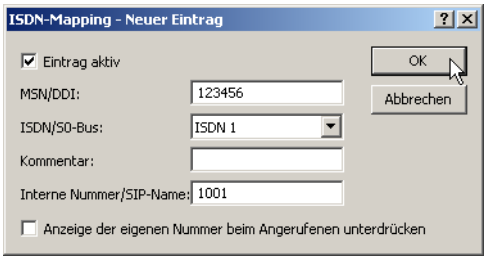
- **Kommentar**

  Kommentar zur Leitung

ISDN- Mapping

Mit dem ISDN- Mapping wird eine Zuordnung von externen ISDN- Rufnummern (MSN oder DDI) zu den intern verwendeten Rufnummern vorgenommen.

LANconfig: VoIP- Call- Manager ▶ Leitungen ▶ ISDN- Mapping



WEBconfig: LCOS- Menübaum ▶ Setup ▶ Voice- Call- Manager ▶ Line ▶ ISDN ▶ Mapping

- **MSN/DDI**

  Externe Telefonnummer des Anschlusses im ISDN- Netz.

  Für ankommende Rufe, die an diese Nummer gerichtet sind, wird die zugehörige interne Rufnummer als Zielnummer eingetragen. Für ausgehende Rufe wird diese Nummer als eigene Nummer des Anrufenden eingetragen, wenn dies nicht unterdrückt ist.

  - □ MSN: Nummer des Telefonanschluss
  - □ DDI (Direct Dialing in): Durchwahlnummer des Telefons, wenn der Anschluss als Anlagenanschluss konfiguriert ist.



Mit dem #-Zeichen als Platzhalter können ganze Gruppen von Rufnummern z.B. bei der Verwendung von Durchwahlnummern in einem einzigen Eintrag erfaßt werden.

- **ISDN/S_0- Bus, Ifc**

  ISDN- Schnittstelle(n), über die Endgeräte an den LANCOM Wireless Router angeschlossen sind. Diese Leitungen müssen als ISDN- NT konfiguriert sein.

- **Rufnummer/SIP- Name, Number/Name**

  Interne Telefonnummer des ISDN-Telefons oder Name des Benutzers (SIP- URL).

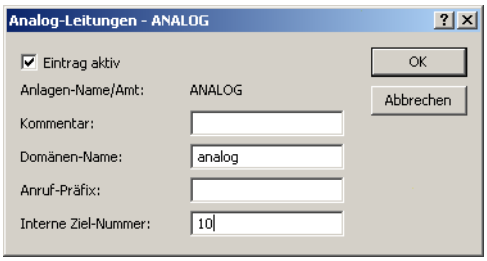
Für ankommende Rufe ist das der SIP-Name oder interne Telefonnummer des Telefons, an das der Ruf von diesem Interface mit der zugehörigen MSN/DDI vermittelt wird. Für ausgehende Rufe wird der SIP-Name durch die MSN/DDI des zugehörigen Eintrages ersetzt.

Mit dem #-Zeichen als Platzhalter können ganze Gruppen von Rufnummern z.B. bei der Verwendung von Durchwahlnummern in einem einzigen Eintrag erfaßt werden.

- **Anzeige der eigenen Rufnummer beim Angerufenen unterdrücken, CLIR**
  Anzeige der eigenen Rufnummer wird beim angerufenen Teilnehmer unterdrückt.
- **Eintrag aktiv, Active**
  Externe Telefonnummer ist aktiv / nicht aktiv
- **Kommentar**
  Kommentar zur externen Telefonnummer

Analog-Line

LANconfig: VoIP-Call-Manager ▶ Leitungen ▶ Analog-Leitungen



WEBconfig: LCOS-Menübaum ▶ Setup ▶ Voice-Call-Manager ▶ Line ▶ Analog

- **Name**
  Name der Leitung, darf nicht identisch sein mit einer anderen in dem Gerät konfigurierten Leitung.
- **Domain**
  Domänen-Name der Analog-Leitung, der für die Adressierung in SIP verwendet wird.
- **Cln-Prefix**
  Das Anruf-Präfix ist eine Nummer, die den Anrufer-Nummern (CLI; SIP „From:") aller ankommenden Anrufe auf dieser Analog-Leitung vorangestellt wird, um eindeutige Rückruf-Nummern zu erzeugen.

  Beispielsweise kann hier eine Nummer ergänzt werden, die im Call-Router bei abgehenden Rufen (dem Rückruf) zur Leitungsauswahl ausgewertet und wieder entfernt wird.
- **Number/Name**
  Interne Rufnummer/SIP-URI, den jeder Anruf auf diese Analog-Leitung als Rufziel erhält. Diese Rufnummer kann sich von der tatsächlichen Rufnummer des Telefonie-Anbieters für den analogen Leitungs-Anschluss unterscheiden (Mapping).

Tragen Sie hier z.B. die Rufnummer einer Gruppe ein, die jeden eingehenden Anruf erhält und steuern Sie darüber flexibel, welche Telefone bei Rufen klingeln oder leiten Sie den Ruf nach einer Zeit auf eine Mobilnummer oder den Anrufbeantworter um.

- **Active**
  Aktiviert oder deaktiviert den Eintrag.
- **Kommentar**
  Kommentar zu diesem Eintrag.
- **Caller-ID Signaling**
  Die Anbieter von analogen Telefonanschlüssen unterstützen unterschiedliche Dienstmerkmale, zu denen auch die Übertragung der Caller ID, also die Anzeige des anrufenden Teilnehmers auf dem Display des gerufenen Endgerätes gehört. Dieser Dienst ist auch als Calling Line Identification Presentation (CLIP) bekannt. Die Caller ID wird je nach Land und Anbieter durch zwei verschiedene Modulationsverfahren über die analoge Verbindung übertragen (FSK oder DTMF).
- **Caller-ID Transmission Requirements**
  Neben der Auswahl des Modulationsverfahrens ist bei der Übertragung der Caller ID auch die zeitliche Steuerung der Signalisierung auf analogen Leitungen je nach Land und Anbieter unterschiedlich geregelt. Damit das geru-

fene Endgerät die Caller ID zum richtigen Zeitpunkt erwartet, wird das vom Anbieter genutzte Verfahren entsprechend eingestellt.

Mögliche Werte:

- □ Default: In dieser Einstellung werden die Standardwerte für das Land verwendet, in dem das Gerät eingesetzt wird.
- □ During-Ringing: Die Caller ID wird während des Klingel-Vorgangs übertragen, und zwar zwischen dem ersten und zweiten Klingelton.
- □ RP-AS: Die Übertragung der Caller ID ist zeitlich nicht mit dem Klingeln verbunden, sondern wird durch ein spezielles "Alarmsignal" angekündigt. Dieses Alarmsignal wird durch Klingelimpulse dargestellt (Ringing Pulse Alerting Signal, RP-AS). Nach dem Klingelimpuls kann die Caller ID übertragen werden.
- □ Line-Reversal: Die Übertragung der Caller ID ist zeitlich nicht mit dem Klingeln verbunden, sondern wird durch ein spezielles "Alarmsignal" angekündigt. Das Alarmsignal wird durch das kurzzeitige Vertauschen der Polarität auf der Leitung dargestellt (Line Reversal). Nach dem Line Reversal kann die Caller ID übertragen werden.

13.5 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.

13.5.1 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 Parameter der Call-Routing-Tabelle' → Seite 13-34). 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.

13.5.2 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.

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' → Seite 13-26.

- 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.

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.

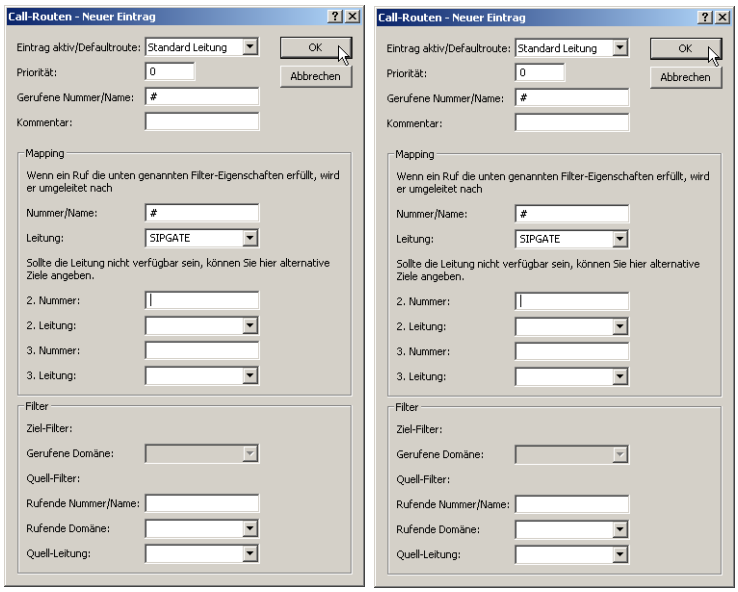
Die Veränderung läuft wie folgt ab:

- 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.

13.5.3 Die Parameter der Call-Routing-Tabelle

LANconfig: VoIP-Call-Manager ▶ Call-Router



WEBconfig: LCOS-Menübaum ▶ Setup ▶ Voice-Call-Manager ▶ Call-Router

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, Active**

  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 des Eintrages, Prio**

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/Name, Called ID**

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 der #-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.

■ **Nummer/Name, Dest-ID**

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 „Nummer/Name", „1. Backup-Nr." oder „2.Backup-Nr." muss einen Inhalt haben. Die Auswertung erfolgt in dieser Reihenfolge. Ein leeres Feld wird übersprungen.

■ **Leitung, Dest-Line**

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.
- □ USER leitet den Ruf an lokale SIP- bzw. ISDN-Teilnehmer weiter.
- □ RESTART beginnt mit der zuvor gebildeten „Nummer/Name" 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. Nummer, Dest-ID-2**

Diese Rufnummer wird für den weiteren Verbindungsaufbau verwendet, wenn unter „Nummer/Name" nichts eingetragen ist oder die zugehörige „Leitung" nicht erreichbar ist. Kann über diese 2. Rufnummer und die zugehörige 2. Leitung keine Verbindung hergestellt werden, werden die 3. Rufnummer und die 3. Leitung verwendet.

■ **2. Leitung, Dest-Line-2**

Über diese Leitung wird die Verbindung aufgebaut, wenn die 2. Rufnummer für den Verbindungsaufbau verwendet wird. Hier können die gleichen Leitungen ausgewählt werden wir bei „Leitung".

■ **3. Nummer, Dest-ID-3**

Bedeutung analog zu 2. Nummer.

■ **3. Leitung, Dest-Line-3**

Bedeutung analog zu 2. Leitung.

■ **Gerufene Domäne, Cld Domain**

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 Wireless Router.
- □ Alle bei den SIP- und SIP-PBX-Leitungen eingetragenen Domänen.

■ **Rufende Nummer/Name, Calling ID**

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.

Folgende Sonderfunktionen können als rufende Nummer eingetragen werden:

- □ LOCAL schränkt auf interne Rufnummern ein (ohne führende „0").
- □ EMPTY kann für nicht angegebene Calling Party IDs verwendet werden.

■ **Rufende Domäne, Cln Domain**

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 Wireless 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, Src-Line**

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.

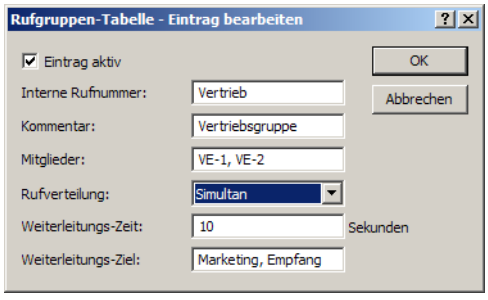
■ **Kommentar**

Kommentar zum aktuellen Routing-Eintrag

Gruppenruf-Funktionen

Zur Konfiguration der Gruppenruf-Funktionen im LANCOM stehen folgende Parameter bereit:

LANconfig: VoIP-Call-Manager ▶ Call-Router ▶ Rufgruppen-Tabelle



WEBconfig: LCOS-Menübaum ▶ Setup ▶ Voice-Call-Manager ▶ Groups

■ **Eintrag aktiv**

Aktiviert oder deaktiviert den Eintrag.

- □ Default: Aktiv

■ **Interne Rufnummer**

Unter dieser Rufnummer bzw. dieser SIP-ID ist die Rufgruppe erreichbar.

- □ Mögliche Werte: Maximal 64 alphanumerische Zeichen.

Namen für Rufgruppen dürfen nicht mit Namen von Benutzern (SIP, ISDN oder Analog) übereinstimmen.

■ **Kommentar**

Kommentar zum definierten Eintrag (64 Zeichen).

■ **Mitglieder**

Kommaseparierte 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' → Seite 13-37 möglich.

■ **Weiterleitungs-Methode**

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.

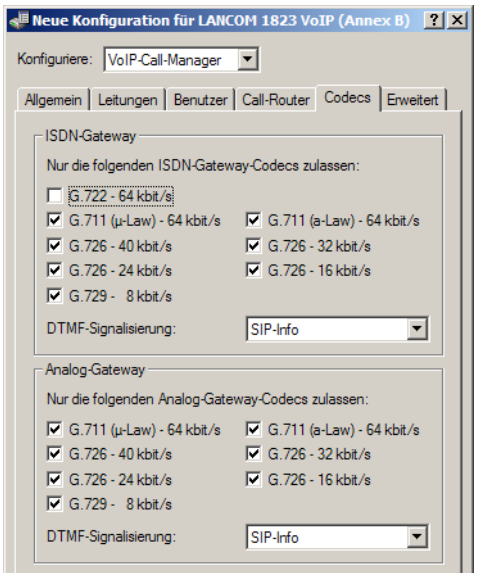
- □ Mögliche Ziele: Benutzer, Rufgruppen, externe Rufnummern
- □ Mögliche Werte: Maximal 64 alphanumerische Zeichen.

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' → Seite 13-37.

13.5.4 Codecs

LANconfig: VoIP-Call-Manager ▶ Codecs



WEBconfig: LCOS-Menübaum ▶ Setup ▶ Voice-Call-Manager ▶ General ▶ ISDN-Gateway-Codecs

WEBconfig: LCOS-Menübaum ▶ Setup ▶ Voice-Call-Manager ▶ General ▶ Analog-Gateway-Codecs

■ **ISDN-Gateway**

Die beteiligten ISDN-Endgeräte handeln beim Verbindungsaufbau aus, welche Codecs für die Komprimierung der Sprachdaten verwendeten werden sollen. Mit dem Codec-Filter können Sie die erlaubten Codecs einschränken und nur bestimmte Codecs zulassen.

■ **Analog-Gateway**

Mit dem Codec-Filter können Sie die erlaubten Codecs für Analog-Endgeräte einschränken und nur bestimmte Codecs zulassen.

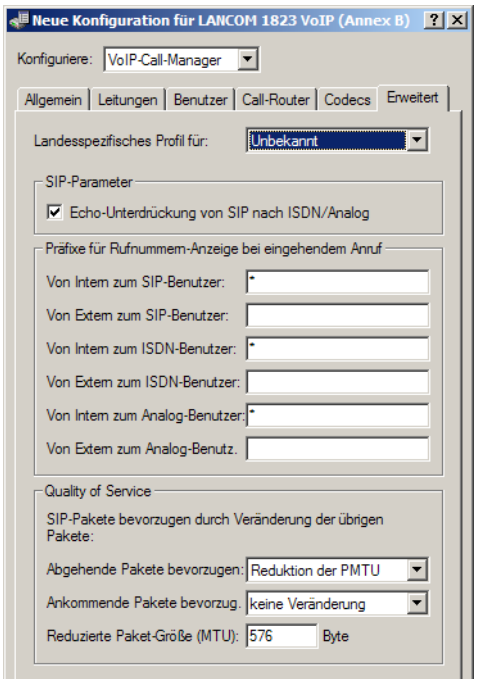
■ **DTMF-Signalisierung**

- □ SIP-Info: Überträgt die DTMF-Töne nach dem SIP-Info-Standard (RFC-2976)
- □ Events (RFC-2833): Überträgt die Ereignisse im Klartext nach dem RFC-2833-Standard
- □ Töne (RFC-2833): Überträgt die Töne nach dem RFC-2833-Standard
- □ Events&Töne (RFC-2833): Überträgt die Ereignisse im Klartext und als Töne nach dem RFC-2833-Standard

Die Einstellung der DTMF-Signalisierung muss zu den Anforderungen des SIP-Providers passen. Eine fehlerhafte Einstellung der DTMF-Signalisierung kann dazu führen, dass kein Verbindungsaufbau über den SIP-Provider möglich ist.

13.5.5 Erweiterte Einstellungen

LANconfig: VoIP-Call-Manager ▶ Erweitert



WEBconfig: LCOS-Menübaum ▶ Setup ▶ Voice-Call-Manager ▶ General ▶ ISDN-Gateway-Codecs

- **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 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.

Weitere Informationen zur Behandlung der Calling Party ID finden Sie unter 'Behandlung der Calling Party ID' → Seite 13-33.

- **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 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 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.

  - **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**

    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 (‘Reduzierung der Paketlänge’ → Seite 11-325).

- **Ankommende Pakete bevorzugen**

  Analog zu den abgehenden Datenpakete wird hier die Behandlung der Nicht-VoIP-Datenpakete bei Bandbreitenreservierung für SIP-Daten eingestellt.

  - **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.

13.6 Telefonanlagenfunktion für LANCOM VoIP Router (PBX-Funktionen)

LANCOM VoIP Router bieten alle Funktionen einer klassischen Telefonanlage (TK-Anlage) 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. Es wird empfohlen, als Endgeräte LANCOM VP-100 und LANCOM Advanced VoIP Client zu verwenden.

13.6.1 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.

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-, 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

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").

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.

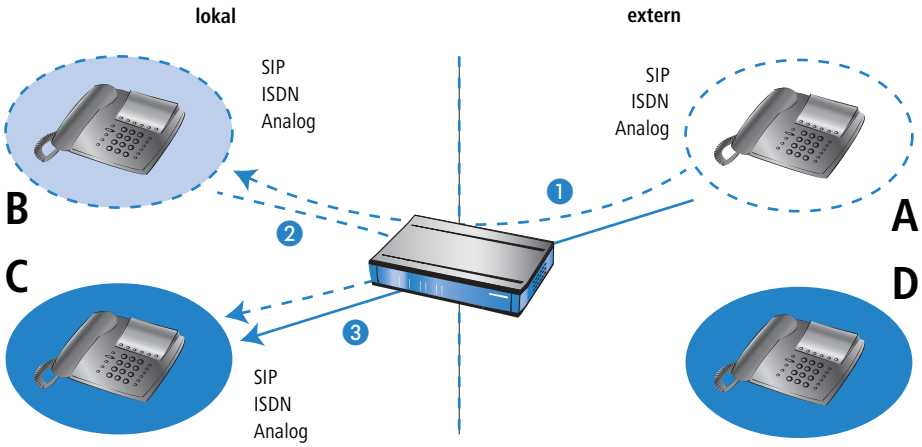
Aufgabe der LANCOM VoIP Router bei der Anrufweiterschaltung

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.

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.

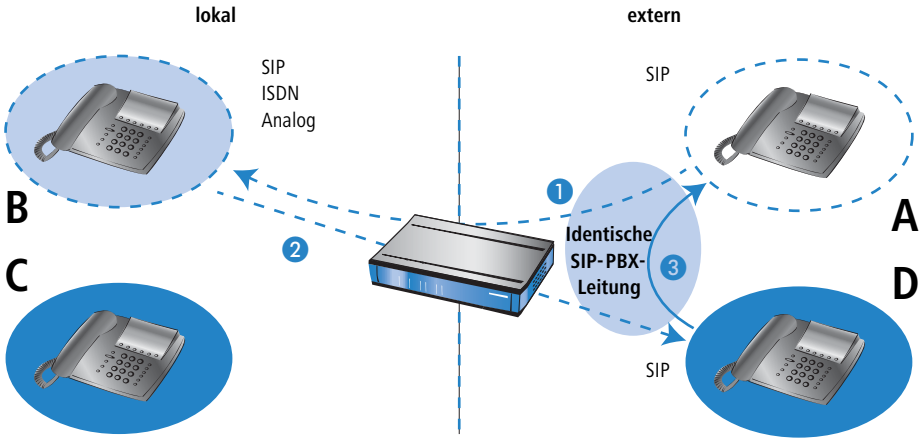


Setzt im Fall von SIP beim externen Teilehmer voraus, dass Transfer in SIP (Re-Invite) vollständig und korrekt unterstützt wird.

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.

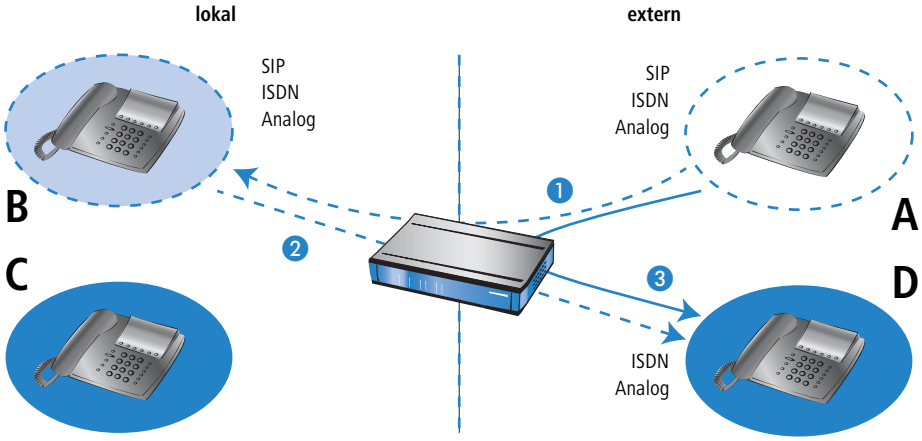


Setzt voraus, dass die VoIP-TK-Anlage Transfers in SIP (Re-Invites) vollständig und korrekt unterstützt.

Aktive Weiterschaltung zu externen ISDN- oder Analog-Benutzern

Bei der Anrufweiterschaltung zu externen ISDN- oder Analog-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 oder Analog) baut ein Gespräch zu einem internen Benutzer **B** (SIP, ISDN oder Analog) auf.
2. **B** baut ein weiteres Gespräch zu einem externen Teilnehmer **D** (ISDN oder Analog) 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 oder Analog) 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.

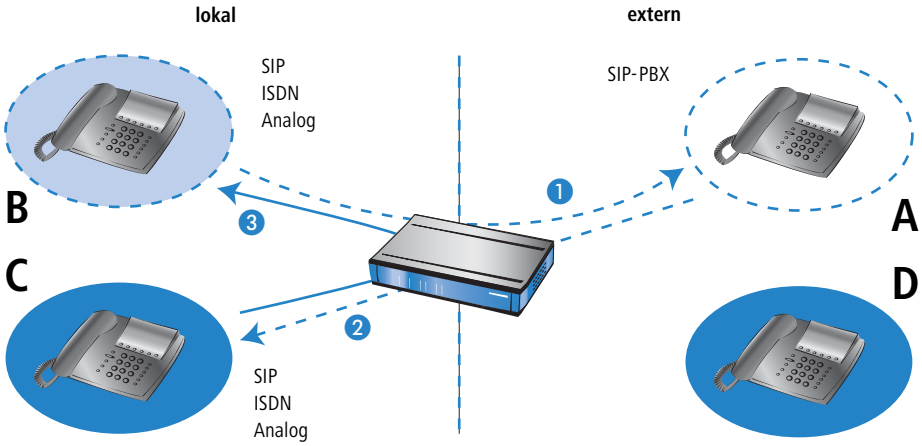


Setzt voraus, dass die VoIP-TK-Anlage Transfers in SIP (Re-Invites) vollständig und korrekt unterstützt.

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.

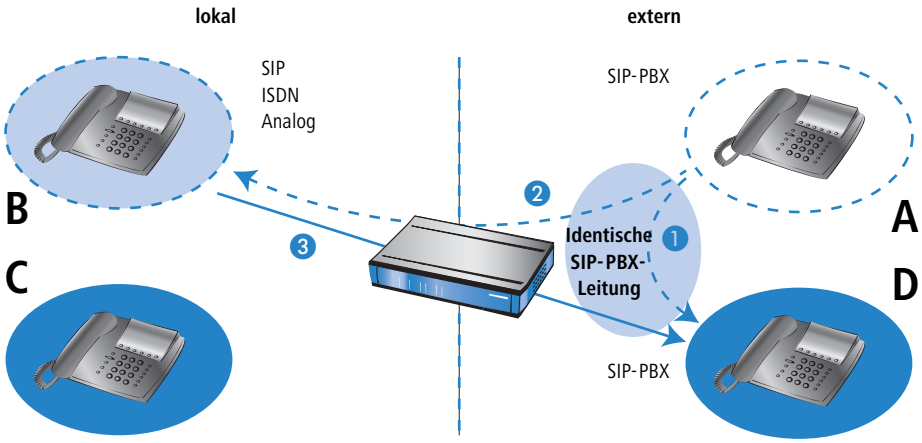


Setzt voraus, dass die VoIP-TK-Anlage Transfers in SIP (Re-Invites) vollständig und korrekt unterstützt.

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.

13.6.2 Spontane Anrufsteuerung durch den Benutzer

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").

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)*.

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*. Sie können die Rückfrage mit einer entsprechenden Menüfunktion des Telefons (z.B. 'Beenden') oder 'R 1' (Analog) beenden.*	AUFLEGEN	AUFLEGEN	AUFLEGEN

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 (bzw. 'R') 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	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*	BEENDEN oder AUFLEGEN*	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.* 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.	VERBINDEN oder AUFLEGEN*	VERBINDEN oder AUFLEGEN*	R 4 oder AUFLEGEN
Sie haben nun keinen aktiven Anruf mehr. Sie können entweder auflegen oder einen neuen Anruf starten.	AUFLEGEN 123456789	AUFLEGEN 123456789	AUFLEGEN 123456789

Anrufweiterschaltung ohne Rückfrage	SIP	ISDN	Analog
Um während eines Gespräches eine zweite Leitung aufzubauen, drücken Sie zunächst die Halten-Taste. Der Gesprächsteilnehmer kann Sie nun nicht mehr hören.	HALTEN	HALTEN	HALTEN
Wählen sie die Rufnummer des zweiten Gesprächspartners, der erste Anruf wird gehalten.	123456789	123456789	123456789
Drücken Sie die Verbinden-Taste (bzw. 'R' und '4' bei Analog-Telefonen) oder legen Sie den Hörer auf, bevor die zweite Verbindung aufgebaut ist.* Die beiden Gesprächspartner werden nun „im Hintergrund" verbunden.	VERBINDEN oder AUFLEGEN*	VERBINDEN oder AUFLEGEN*	R 4 oder AUFLEGEN
Sie haben nun keinen aktiven Anruf mehr. Sie können entweder auflegen oder einen neuen Anruf starten.	AUFLEGEN 123456789	AUFLEGEN 123456789	AUFLEGEN 123456789



*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").

13.6.3 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.

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.

Konfiguration der Benutzer-Einstellungen über LANconfig siehe 'Benutzer-Einstellungen' → **Seite 13-20**

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*MSN#	*21*ZielNr#
Ausschalten	#21#	#21#*MSN	#21#
Vorübergehend ausschalten, Weiterschaltungs-Ziel beibehalten	#22#	#22*MSN#	#22#
Wiedereinschalten, definiertes Weiterschaltungs-Ziel beibehalten	*22#	*22*MSN#	*22#

Rufweiterschaltung bei „besetzt"	SIP	ISDN	Analog
Einschalten und Weiterschaltungs-Ziel definieren	*67*ZielNr#	*67*ZielNr*MSN#	*67*ZielNr#
Ausschalten	#67#	#67*MSN#	#67#

Verzögerte Rufweiterschaltung	SIP	ISDN	Analog
Einschalten und Weiterschaltungs-Ziel definieren	*61*ZielNr#	*61*ZielNr*MSN#	*61*ZielNr#
Ausschalten	#61#	#61*MSN#	#61#

Bitte beachten Sie bei der Nutzung der Zeichenfolgen für die Konfiguration der Anrufweiterschaltung folgende Hinweise:

1. 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.

13.6.4 Faxen über T.38 – Fax over IP (FoIP)

Mit der Migration der Telefoninfrastrukturen 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 zur Kompression 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 des §14, 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, das 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, dem IFP (Internet Facsimilé Protocol), was eine Einbettung in UDP/TCP-Pakete durchführt.

Um eine Faxübertragung nach T.38 zu ermöglichen, müssen entweder die beteiligten Faxgeräte selbst den T.38-Standard unterstützen oder über geeignete Fax-Gateways mit dem Internet verbunden sein. LANCOM VoIP Router und LANCOM Router mit LANCOM VoIP Advanced Option oder LANCOM VoIP Basic Option 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:

- Demodulation ankommender T.30-Faxsignale
- Umwandlung T.30-Faxsignale in T.38-IFP-Pakete
- Übertragung IFP-Pakete zwischen Sender- und Empfänger-Gateways
- Umwandlung T.30-IFP-Pakete in T.30-Faxsignale
- Modulation der T.30-Faxsignale und Übertragung zum Faxgerät

LANCOM VoIP Router erkennen ein zu versendendes Fax automatisch, wenn in den Analog- oder ISDN-Benutzer-Einstellungen 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.

13.6.5 Gruppenrufe mit Ruf-Verteilung

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.

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.

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 Verzwei-

gungen 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.

Konfiguration der Gruppenruf- Funktionen siehe 'Gruppenruf- Funktionen' → **Seite 5- 29**

13.6.6 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'.
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.

13.7 VoIP- Media- Proxy – Optimierte Verwaltung von SIP- Verbindungen

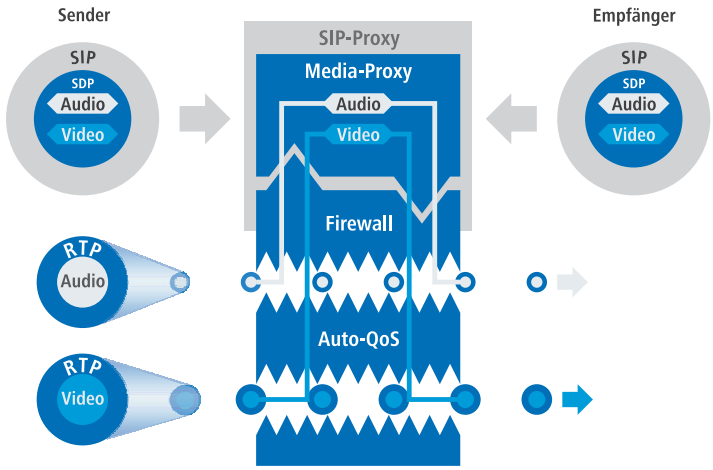
Beim Verbinden von bzw. bei Anrufweiterschaltungen zwischen entfernten Teilnehmern über unterschiedliche SIP-Leitungen versucht der SIP-Proxy im LANCOM VoIP Router, durch einen REFER bzw. einen Re-INVITE die beiden Teilnehmer zu verbinden. Da die beiden externen Teilnehmer sich nicht immer direkt erreichen 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

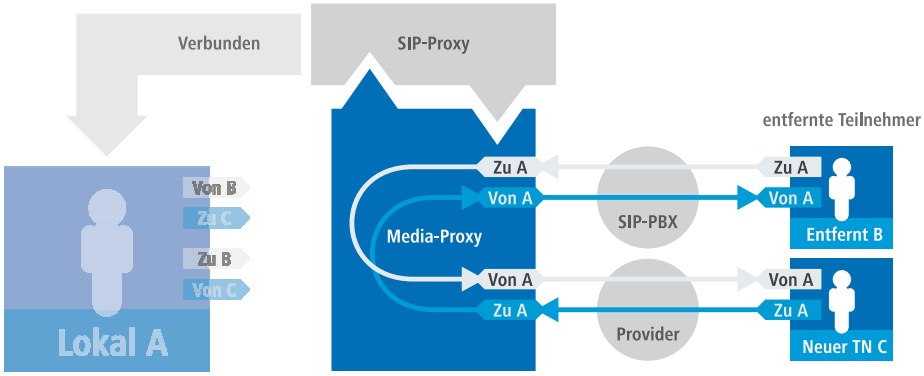
Das SIP-Protokoll kann in einer Sitzung (Session) mehrere Datenströme aushandeln, z. B. einzelne Media-Ströme für Audio und Video. Die einzelnen Ströme werden separat behandelt – jeder Datenstrom wird im Media-Proxy zunächst terminiert und dann „auf der anderen Seite" weitergeführt, der Datenstrom erhält 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.



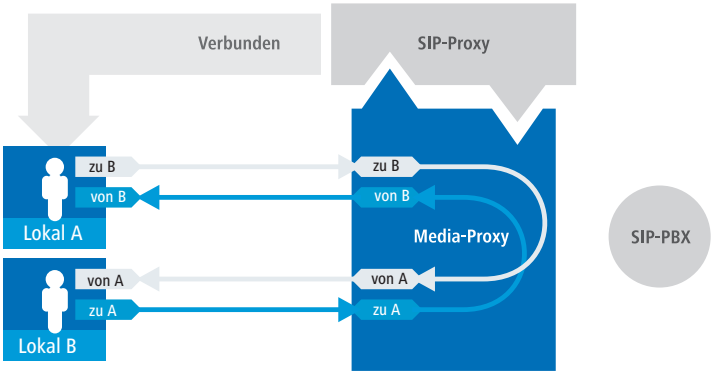
Dabei werden alle Datenströme auch einzeln durch die Firewall geführt, was u.a. eine differenzierte Regelung der QoS-Einstellungen ermöglicht.

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 und 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.

13.8 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.

Ab LCOS 7.52 kann daher – genau wie beim ISDN-Mapping – in der SIP-Mapping-Tabelle explizit angegeben werden, wie die Rufnummern verarbeitet werden sollen.

0123456789# -> #

Damit werden dann direkt die Durchwahlnummern des Trunks 1:1 auf interne Rufnummern umgesetzt.

Falls Sie bisher einen Trunk mit automatischer Stammnummern-Umsetzung genutzt haben, müssen Sie nach dem Update auf LCOS 7.52 auf jeden Fall einen entsprechenden Eintrag in der SIP-Mapping-Tabelle vornehmen.

13.9 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.

LANconfig: **VoIP-Call-Manager** ▶ **Leitungen** ▶ **SIP-Leitungen**

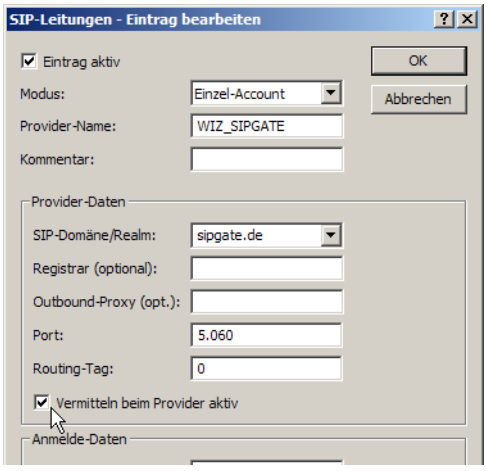
WEBconfig: **Setup** ▶ **Voice-Call-Manager** ▶ **Line** ▶ **SIP-Provider** ▶ **Line**

- **Vermitteln beim Provider aktiv (ReferForwarding)**

  Wenn diese Option aktiviert ist, wird beim Vermitteln von zwei externen Verbindungen ein REFER an den Provider weitergeleitet, damit dieser den Transfer durchführt. Dies hat den Vorteil, dass im LANCOM VoIP Router keine Bandbreite mehr benötigt wird.

  - □ Mögliche Werte: Ein, Aus
  - □ Default: Aus

Vorraussetzung für die Vermittlung beim Provider ist, dass beide Verbindungen über die gleiche Providerleitung aufgebaut wurden.



13.10 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.

Ab LCOS 7.52 kann diese automatisch Umwandlung abgeschaltet werden, sodass kanonische Rufnummern in der Call-Routing-Tabelle verarbeitet werden können. Somit können z. B. für kanonische Rufnummern eigene Leitungen definiert werden.

- WebConfig: **Setup** ▶ **Voice-Call-Manager** ▶ **General**
- **Convert-Canoncials**

  Aktiviert bzw. deaktivert die Umwandlung von kanonischen Rufnummern in Standard-Rufnummern.

  - Mögliche Werte: Ja, Nein
  - Default: Ja

13.11 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

13.11.1 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 ('Lokale Authentifizierung erzwingen' → Seite 13-15).

13.11.2 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.

13.12 Konfiguration der ISDN-Schnittstellen

LANCOM VoIP Router verfügen über mehrere ISDN-Schnittstellen, die zum Anschluss an ISDN-Amtsleitungen oder zum Anschluss von ISDN-Endgeräten genutzt werden 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 sind die mit ☒ gekennzeichneten ISDN-Schnittstellen auf den TE-Modus, die mit ☎ gekennzeichneten ISDN-Schnittstellen auf den NT-Modus eingestellt. Je nach Bedarf können die ISDN-Schnittstellen entsprechend umgestellt werden:

- Mit mehreren TE-Schnittstellen können z.B. bis zu acht B-Kanäle für Backup- oder Einwahlzwecke genutzt werden.
- Mit mehreren NT-Schnittstellen können z.B. einer untergeordneten ISDN-TK-Anlage bis zu acht B-Kanäle bereitgestellt werden.

Je nach Kombination von ISDN-Schnittstellen im TE- und NT-Modus müssen hardwareseitig ggf. die Funktionen Busterminierung, Life-Line-Support und Spannungsweiterleitung sowie softwareseitig das passende Protokoll eingestellt werden. Die Protokoll-Einstellung berücksichtigt dabei auch den verwendeten ISDN-Anschlusstyp (Punkt-zu-Mehrpunkt oder Punkt-zu-Punkt).

13.12.1 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.

13.12.2 Busterminierung, Life-Line-Support und Spannungsweiterleitung

Mit den DIP-Schaltern an der Unterseite der LANCOM VoIP Router werden die Hardware-Funktionen der ISDN-Schnittstellen eingestellt.

- 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.



Beim Anschluss an eine ISDN-Schnittstelle, die von der Defaulteinstellung abweicht, muss zwingend der beiliegende Adapter verwendet werden. Mit diesem Adapter werden die Kontakte der ISDN-Schnittstelle gekreuzt. Ohne Verwendung des Adapters können sowohl der LANCOM VoIP Router als auch die verbundenen Geräte Schaden nehmen!

Nicht bei allen LANCOM VoIP Router

- Bei aktiviertem **Life-Line-Support** werden die Schnittstellen ISDN 1 und ISDN 2 gebrückt, wenn das Gerät durch Stromausfall nicht zur Verfügung steht oder die ISDN-2-Schnittstelle ausgeschaltet ist (Default: ein). Der Life-Line-Support wird eingesetzt beim Anschluss des Geräts über eine TE-Schnittstelle an eine externe ISDN-Leitung bei gleichzeitigem Betrieb von ISDN-Endgeräten am internen ISDN-Anschluss einer NT-Schnittstelle. Im gebrückten Zustand können die ISDN-Endgeräte direkt den externen ISDN-Bus nutzen.

  Zum Aktivieren des Life-Line-Supports müssen sich alle vier DIP-Schalter (3 bis 6) in der oberen Position befinden, zum Deaktivieren müssen alle vier DIP-Schalter in die untere Position gebracht werden.

Deaktivieren Sie den Life-Line-Support, wenn beide ISDN-Schnittstellen im gleichen Modus betrieben werden, also z.B. zweimal TE- oder zweimal NT. In diesen Anwendungsfällen dürfen die Schnittstellen bei Stromausfall nicht gebrückt werden!

- Mit der **ISDN-Spannungsweiterleitung** wird die Busspannung eines externen ISDN-Busses an ISDN 1 an die angeschlossenen Endgeräte eines anderen ISDN-Busses weitergeschaltet. Damit können am internen ISDN-Bus des LANCOM VoIP Router auch ISDN-Endgeräte ohne eigene Spannungsversorgung betrieben werden.

Deaktivieren Sie unbedingt die ISDN-Spannungsweiterleitung, wenn beide ISDN-Schnittstellen im TE-Modus betrieben werden, also z.B. beide ISDN-Schnittstellen mit einem ISDN-NTBA verbunden sind. Durch die Spannungsweiterleitung würde in diesem Fall ein Kurzschluss entstehen, der das Gerät und die ISDN-NTBAs beschädigen kann!

Weitere Informationen zur Einstellung von Life-Line-Support und ISDN-Spannungsweiterleitung finden Sie im Benutzerhandbuch zu Ihrem LANCOM VoIP Router.

13.12.3 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, siehe 'Taktung der ISDN-Anschlüsse'
- **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, siehe 'Taktung der ISDN-Anschlüsse'
- **DSS1 Takt** zur Übernahme des ISDN-Taktes einer angeschlossenen ISDN-Leitung, siehe 'Taktung der ISDN-Anschlüsse'
- **Aus**

Der Betrieb im NT-Modus muss immer von Hand eingestellt werden.

Wenn ein ISDN-Endgerät an einer ISDN-Schnittstelle im Automatik-Modus nicht richtig erkannt wird, stellen Sie das verwendete Protokoll direkt ein.

13.12.4 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.

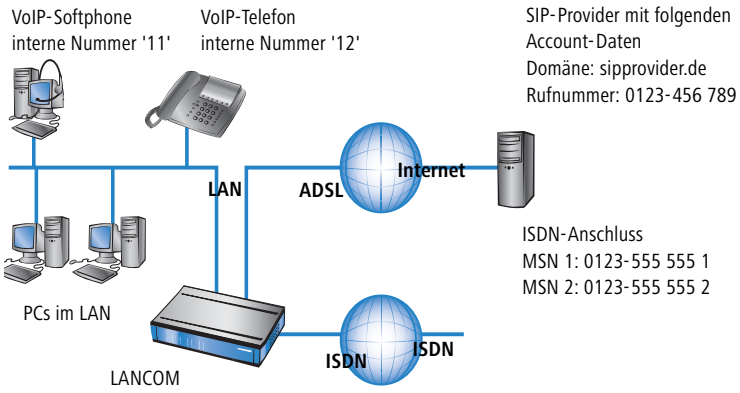
Zur Definition der ISDN-Schnittstelle, über die ein LANCOM VoIP Router den ISDN-Takt empfängt (der dann an alle Geräte an NT-Schnittstellen weitergegeben wird), stehen verschiedene Einstellungen für die ISDN-Schnittstellen zur Verfügung:

- **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.

13.13 Konfigurationsbeispiele

13.13.1 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.



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.

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.

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
interne VoIP-Domain	✔	✔
interne Rufnummern	✔	✔
externe SIP-Rufnummer	✔	
Zugangsdaten SIP-Account	✔	
externe ISDN-Rufnummern (MSNs)	✔	
Landes- und Ortsnetzvorwahl	✔	

Konfiguration des LANCOM

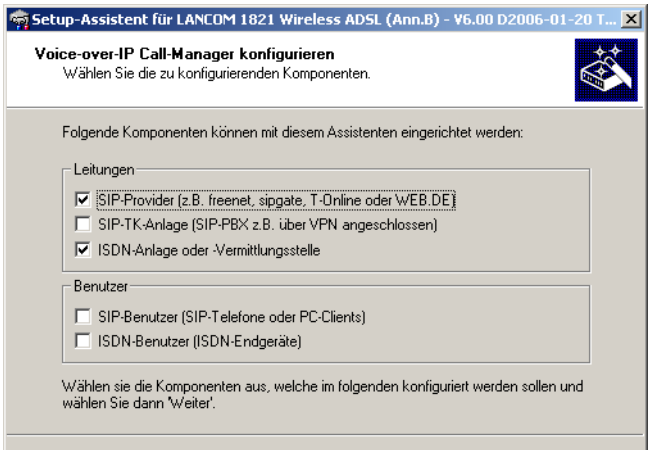
Bei der Konfiguration des LANCOM werden die folgenden Schritte durchführt:

- 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 LANCOM im Detail:

① Führen Sie unter LANconfig den Setup-Assistenten zur Konfiguration des VoIP-Call-Managers aus. Aktivieren Sie die Optionen 'SIP-Provider' und 'ISDN-Anlage oder -Vermittlungsstelle'.



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)

Die Bezeichnung der Server benötigen Sie in der Regel nicht, sie wird mit Hilfe der SIP-Domäne über eine DNS-Anfrage ermittelt. Tragen Sie hier nur eine Serverbezeichnung ein, falls Ihnen Ihr Provider entsprechende Adressen mitgeteilt hat.

- 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.

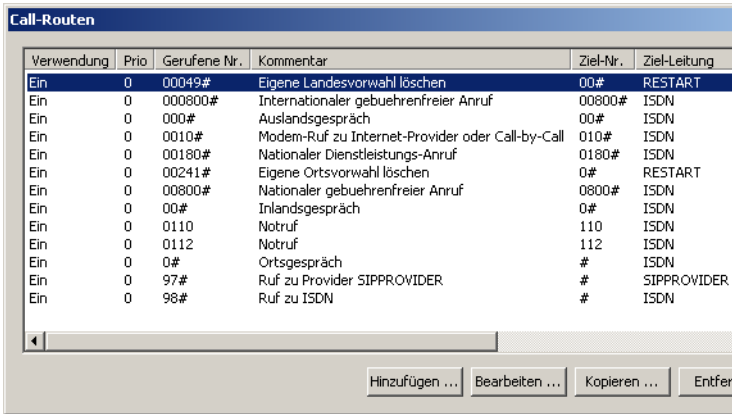
Diese Beschreibung bezieht sich auf eine „benutzerdefinierte Konfiguration". Falls Sie einen speziellen SIP-Provider aus der Liste auswählen, wird ein Teil der Parameter automatisch vorkonfiguriert.

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'

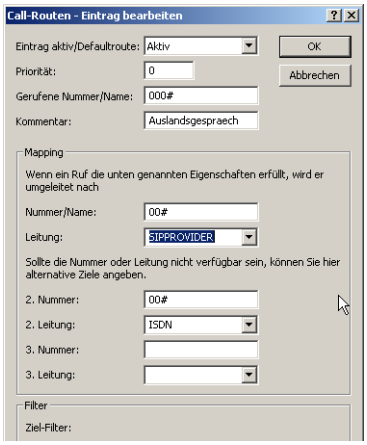
⑤ Geben Sie die Orts- und Landesvorwahl für den Standort des Gerätes an. Anhand dieser Informationen kann der Voice-Call-Manager unterscheiden, ob es sich bei abgehenden Anrufen um Ortsgespräche, nationale oder internationale Ferngespräche handelt.

⑥ Mit den bisherigen Angaben erstellt LANconfig einen Vorschlag für die Call-Routing-Tabelle, den Sie nachfolgend an Ihre Bedürfnisse anpassen können:



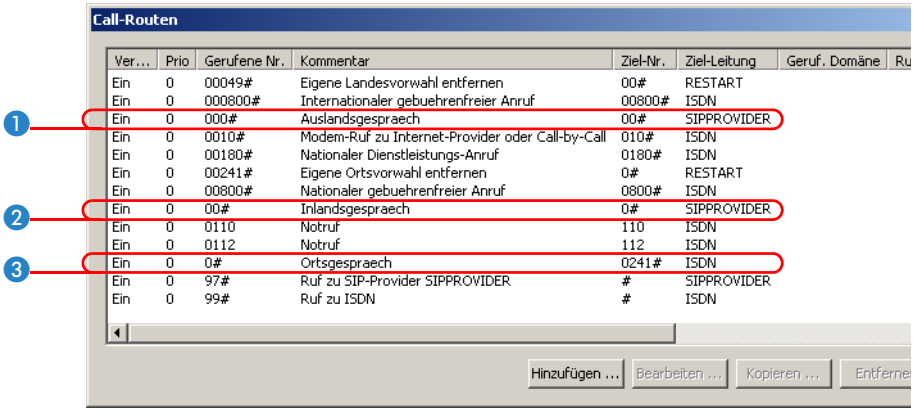
Das #-Zeichen steht als Platzhalter für beliebige Zeichenfolgen. Der Eintrag '0#' passt also auf alle gerufenen Nummern, die mit mindestens einer führenden '0' beginnen.

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 Backupleitung bei Bedarf entsprechend von SIP auf ISDN umzustellen!

Nach der Anpassung für internationale (1) und nationale (2) Ferngespräche sieht die Call-Routing-Tabelle dann z.B. so aus:



Konfiguration der VoIP-Endgeräte

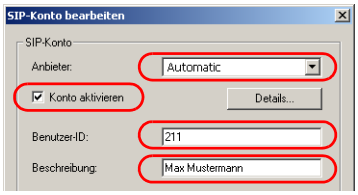
Stellen Sie im Softphone die Anmeldedaten für den ersten SIP-Benutzer ein (Beispiel für LANCOM Advanced VPN Client).

SIP-Konto im LANCOM Advanced VPN Client zur Anmeldung am LANCOM VoIP Router oder an einer TK-Anlage einrichten

Stellen Sie im LANCOM Advanced VPN Client die Anmeldedaten für den ersten SIP-Benutzer ein.

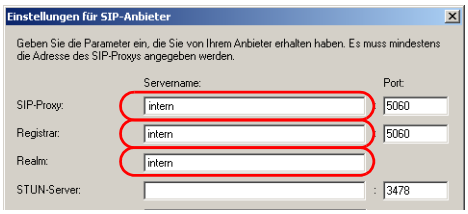
① Wählen Sie dazu auf der Registerkarte 'SIP-Konten' die Schaltfläche **Hinzufügen** zum Anlegen eines neuen SIP-Kontos.

② Behalten Sie als Anbieter den Eintrag 'Benutzerdefiniert' bei und aktivieren Sie das neue Konto.



③ Geben Sie als 'Benutzer-ID' die interne Rufnummer ein, auf der dieser LANCOM Advanced VPN Client Anrufe entgegennehmen soll und tragen Sie optional unter 'Beschreibung' den Namen ein, der im Display der Gegenstelle angezeigt werden soll.

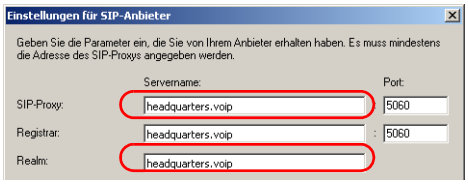
④ Öffnen Sie mit der Schaltfläche **Details** den Dialog für die erweiterten Einstellungen und geben Sie folgende Daten ein:



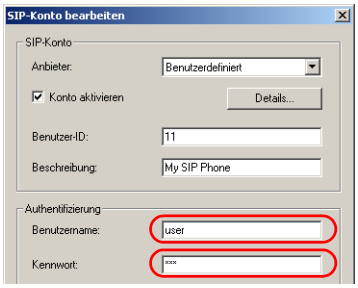
- □ Als 'SIP-Proxy' und 'Registrar' die interne VoIP-Domain Ihres LANCOM VoIP Router (Default: 'intern'), wenn dieser auch DNS-Server für den Client ist, sonst die LAN-IP-Adresse.
- □ Als 'Realm' immer die interne VoIP-Domain.

Mit diesen Angaben kann sich der LANCOM Advanced VPN Client bei einem LANCOM VoIP Router lokal registrieren und so die dort definierten Leitungen zum Telefonieren verwenden.

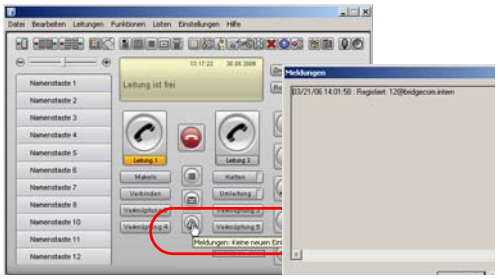
⑤ Wenn sich der LANCOM Advanced VPN Client nicht nur lokal am LANCOM VoIP Router registrieren soll, sondern auch an einer übergeordneten SIP-TK-Anlage (z.B. in der Firmenzentrale) anmelden soll, geben Sie als 'SIP-Proxy', 'Registrar' und als 'Realm' die VoIP-Domäne der SIP-TK-Anlage in der Zentrale ein. Auf dem LANCOM VoIP Router muss eine entsprechende SIP-PBX-Leitung mit derselben Domäne konfiguriert und der Router muss DNS-Server für den LANCOM Advanced VPN Client sein.



⑥ Geben Sie für das SIP-Konto zusätzlich den Benutzernamen und das Kennwort zur Anmeldung an der SIP-TK-Anlage ein.



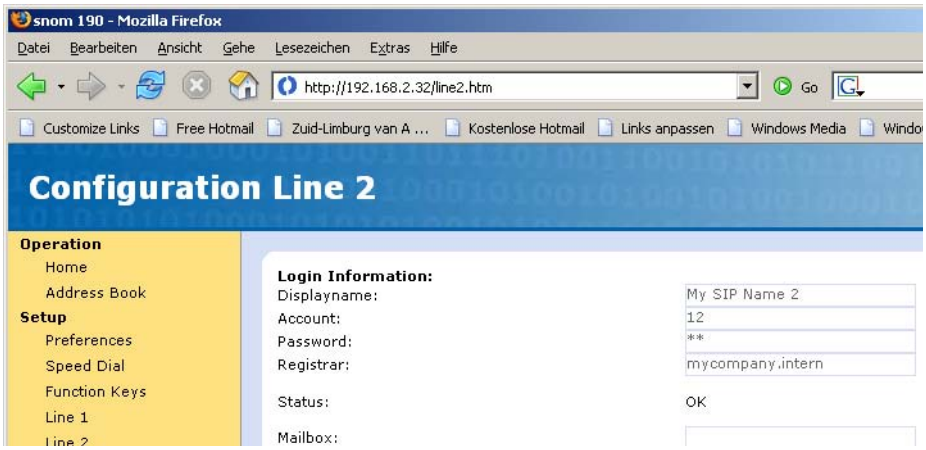
⑦ Durch einen Blick in die Liste der vorliegenden Meldungen (via Button oder Menü) können Sie prüfen, ob die Registrierung erfolgreich war.



Auf der Registerkarte 'Standort' stellen sie ihre Landesvorwahl und die Ortsvorwahl jeweils ohne führende Null sowie die nationalen und internationalen Präfixe ein (z.B. '0' und '00'). In dem Feld 'Amtsholung' wird der individuelle Wert eingetragen, den Ihre Telefonanlage oder Ihr LANCOM VoIP Router für die Amtsholung benötigen (z.B. '0' oder '*').

Stellen Sie im VoIP-Telefon die Anmeldedaten für den zweiten SIP-Benutzer ein (Beispiel für Snom 190).

① Wählen Sie im Menü **Setup** eine der möglichen Leitungen, z.B. 'Line 2'.



② Geben Sie folgende Werte ein:

- Registrar: interne VoIP-Domain des LANCOM.
- Account: interne Rufnummer des Benutzers.
- Displayname: Name des Benutzers, wie er bei der Gegenstelle angezeigt werden soll.

Falls Sie ein anderes Softphone bzw. ein anderes VoIP-Telefon verwenden, finden Sie Informationen zur Konfiguration der Software in der zugehörigen Dokumentation.

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	❸ 0#		0241#: 0241 555 555	ISDN
③	VoIP-Telefon	0 0123 666 666	❷ 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 ❸ 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 ❷ 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.

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:

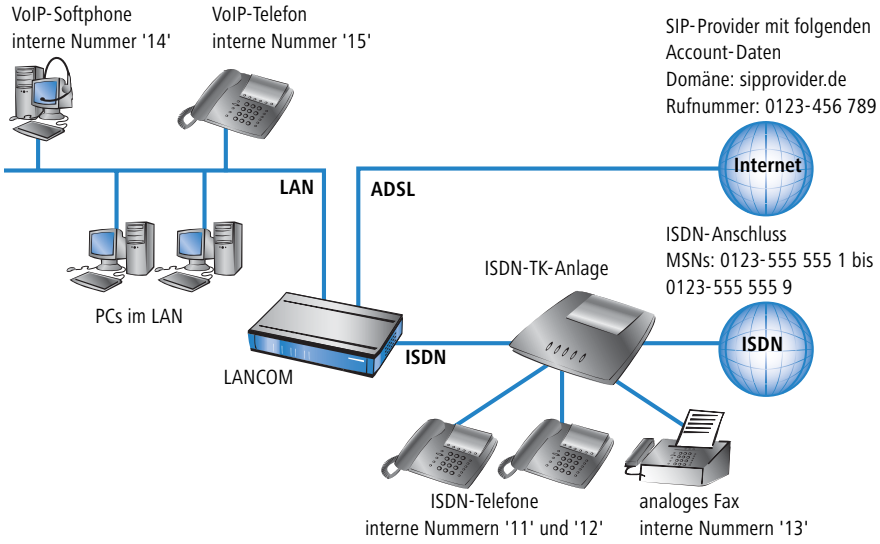
	Gegenstelle wählt	Call-Router empfängt	Zuordnung über	verwendete Nummer	passende Call-Route	Ziel-Leitung
①	0 123 456 789	456 789	interne Zielnummer für SIP-Leitung	11	keine	intern
②	0 123 555 555 1	555 555 1	ISDN-Mapping	11	keine	intern
③	0 123 555 555 2	555 555 2	ISDN-Mapping	12	keine	intern

13.13.2 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 wird an einem Nebenstellenanschluss der TK-Anlage betrieben.



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 (‘Konfiguration der ISDN-TK-Anlage’ → Seite 13-64).
- Erreichbarkeit der internen Endgeräte (ISDN und SIP) über die MSNs.
- Gespräche zu Not- und Sonderrufnummern über ISDN.

Voraussetzungen

- LANCOM 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.

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	✔	✔	✔	✔
externe SIP-Rufnummer	✔			
Zugangsdaten SIP-Account	✔			
externe ISDN-Rufnummern (MSNs)			✔	
Landes- und Ortsnetzvorwahl	✔			

Konfiguration des LANCOM

Bei der Konfiguration des LANCOM werden die folgenden Schritte durchgeführt:

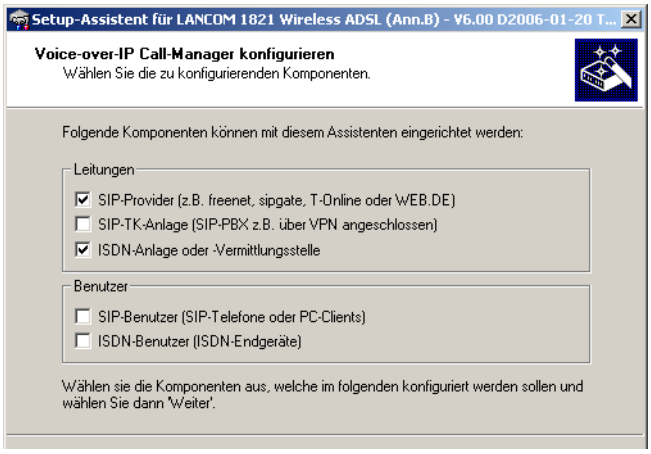
- Einrichten der Leitung zum SIP-Provider
- Aktivieren der ISDN-Schnittstelle und Zuordnung der internen MSNs der TK-Anlage zu den internen Rufnummern im LANCOM VoIP Router
- Anpassen der Call-Routing-Tabelle

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 im Detail:

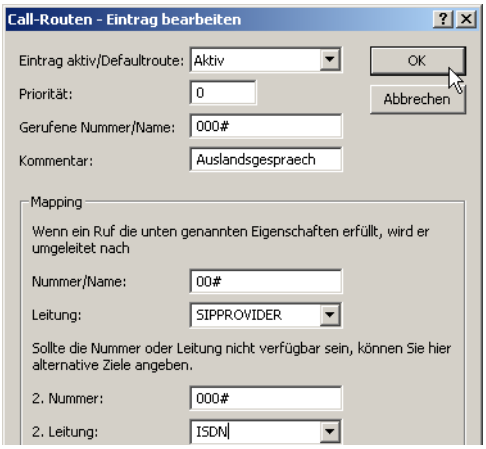
① Führen Sie unter LANconfig den Setup-Assistenten zur Konfiguration des VoIP-Call-Managers aus. Aktivieren Sie die Optionen 'SIP-Provider' und 'ISDN-Anlage oder -Vermittlungsstelle'.



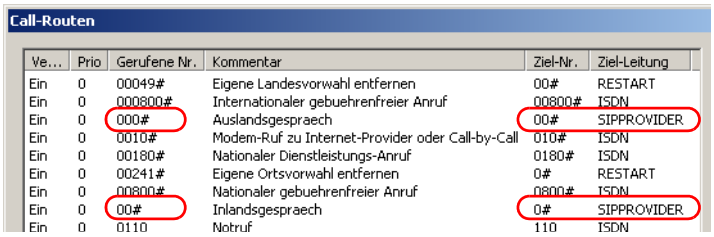
② Richten Sie ein wie in den vorhergehenden Beispielen beschrieben:

- □ 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.



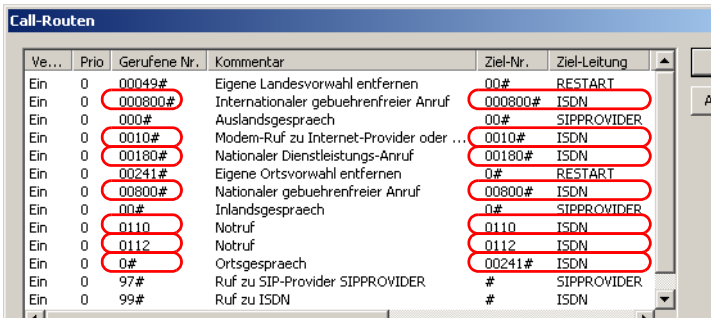
Nach der Anpassung sieht die Call-Routing-Tabelle dann z.B. so aus:



Bei jedem Ferngespräch wird also die führende '0' aus der Rufnummer entfernt, der Ruf wird über den SIP-Provider geführt.

④ 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.

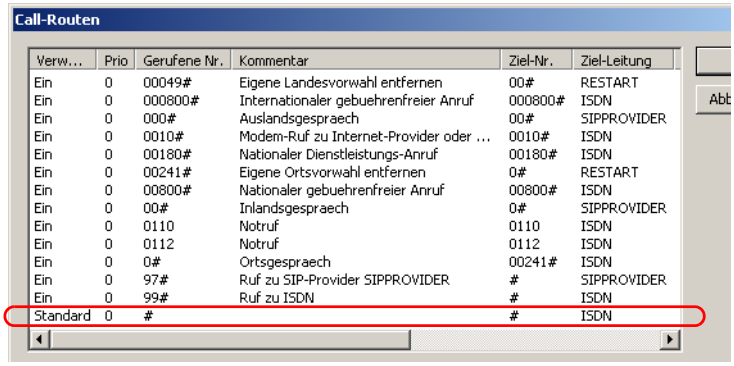
Nach der Anpassung sieht die Call-Routing-Tabelle dann z.B. so aus:



Ve...	Prio	Gerufene Nr.	Kommentar	Ziel-Nr.	Ziel-Leitung
Ein	0	00049#	Eigene Landesvorwahl entfernen	00#	RESTART
Ein	0	000800#	Internationaler gebuehrenfreier Anruf	000800#	ISDN
Ein	0	000#	Auslandsgespraech	00#	SIPPROVIDER
Ein	0	0010#	Modem-Ruf zu Internet-Provider oder ...	0010#	ISDN
Ein	0	00180#	Nationaler Dienstleistungs-Anruf	00180#	ISDN
Ein	0	00241#	Eigene Ortsvorwahl entfernen	0#	RESTART
Ein	0	00800#	Nationaler gebuehrenfreier Anruf	00800#	ISDN
Ein	0	00#	Inlandsgespraech	0#	SIPPROVIDER
Ein	0	0110	Notruf	0110	ISDN
Ein	0	0112	Notruf	0112	ISDN
Ein	0	0#	Ortsgespraech	00241#	ISDN
Ein	0	97#	Ruf zu SIP-Provider SIPPROVIDER	#	SIPPROVIDER
Ein	0	99#	Ruf zu ISDN	#	ISDN

⑤ 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:



Verw...	Prio	Gerufene Nr.	Kommentar	Ziel-Nr.	Ziel-Leitung
Ein	0	00049#	Eigene Landesvorwahl entfernen	00#	RESTART
Ein	0	000800#	Internationaler gebuehrenfreier Anruf	000800#	ISDN
Ein	0	000#	Auslandsgespraech	00#	SIPPROVIDER
Ein	0	0010#	Modem-Ruf zu Internet-Provider oder ...	0010#	ISDN
Ein	0	00180#	Nationaler Dienstleistungs-Anruf	00180#	ISDN
Ein	0	00241#	Eigene Ortsvorwahl entfernen	0#	RESTART
Ein	0	00800#	Nationaler gebuehrenfreier Anruf	00800#	ISDN
Ein	0	00#	Inlandsgespraech	0#	SIPPROVIDER
Ein	0	0110	Notruf	0110	ISDN
Ein	0	0112	Notruf	0112	ISDN
Ein	0	0#	Ortsgespraech	00241#	ISDN
Ein	0	97#	Ruf zu SIP-Provider SIPPROVIDER	#	SIPPROVIDER
Ein	0	99#	Ruf zu ISDN	#	ISDN
Standard	0	#		#	ISDN

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.

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.

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.

Konfiguration der ISDN-Endgeräte

Die Konfiguration der ISDN-Endgeräte beschränkt sich in der Regel auf den Eintrag der verwendeten internen MSN der TK-Anlage.

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
②	VoIP-Telefon	11	❸ # (Standard)		#: 11	ISDN
③	ISDN-Telefon	14	■ TK-Anlage	VoIP-Softphone	14	intern
④	VoIP-Telefon	0 555 555	❷ 0#		00241#: 0 555 555	ISDN
⑤	ISDN-Telefon	0 555 555	■ TK-Anlage		555 555	ISDN-Amt
⑥	VoIP-Telefon	0 0123 666 666	❶ 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 ❸ 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 ❷ 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 ❶ 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.

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 4	14	■ ISDN-TK-Anlage ■ 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.

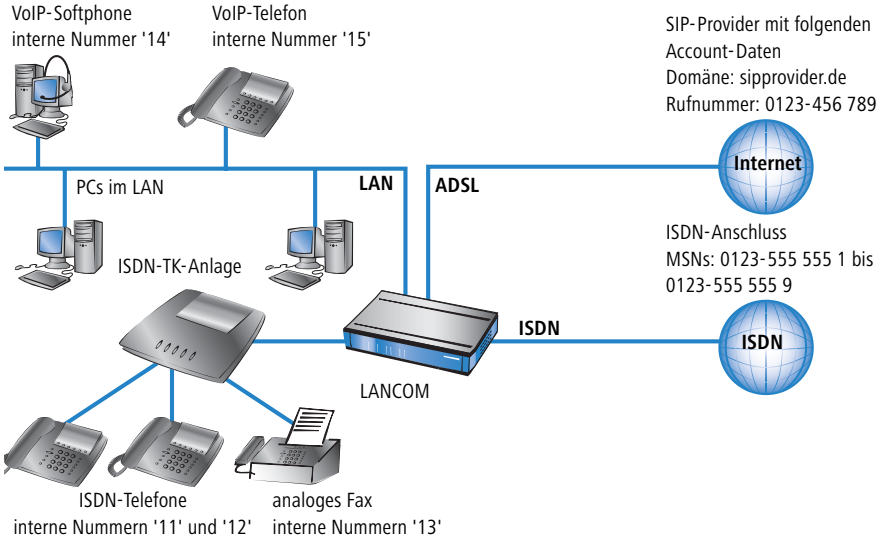
③ Die eingehenden Anrufe an die MSNs für die VoIP-Endgeräte werden von der TK-Anlage mit der internen MSN auf dem internen ISDN-Bus ausgegeben. Der Call-Router empfängt diese Anrufe wie interne Rufe und gibt sie an die passenden Benutzer weiter, da auch hier kein Eintrag in der Call-Routing-Tabelle zutrifft.

13.13.3 VoIP-Telefonie als Ergänzung zur untergeordneten ISDN-TK-Anlage

Dieses Beispiel zeigt die Konfiguration eines LANCOM, wenn eine untergeordnete 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. Das LANCOM wird nun zwischen den öffentlichen ISDN-Anschluss und die ISDN-TK-Anlage geschaltet.

Die TK-Anlage ist so konfiguriert, dass die Teilnehmer beim Abheben des Hörers sofort ein Amt für externe Anrufe erhalten.

Die ISDN-TK-Anlage wird als untergeordnete TK-Anlage an der ISDN-NT-Schnittstelle des LANCOM betrieben.



Ziel

- Internes Telefonieren der ISDN- und SIP-Telefone sowie SIP-Softphones.
- Externes Telefonieren der ISDN- und SIP-Endgeräte über ISDN.
- Erreichbarkeit der internen Endgeräte (ISDN und SIP) über die MSNs.

Voraussetzungen

- LANCOM angeschlossen an LAN und WAN, eine ISDN-NT-Schnittstelle ist mit dem Amts-Eingang der ISDN-TK-Anlage 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.

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	✔	✔	✔	✔
externe SIP-Rufnummer	✔			
Zugangsdaten SIP-Account	✔			
externe ISDN-Rufnummern (MSNs)	✔			
Landes- und Ortsnetzvorwahl	✔			

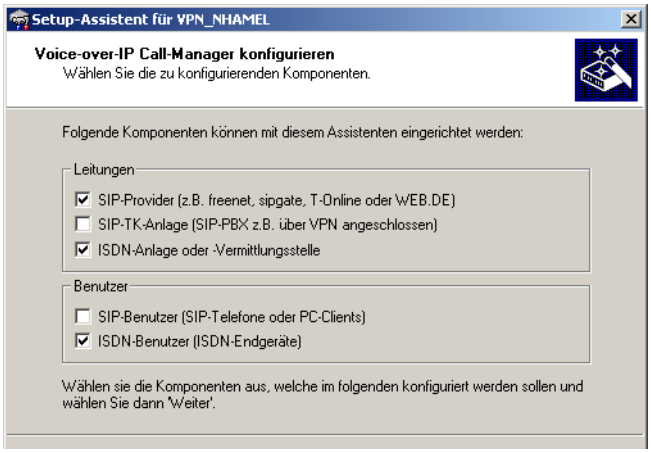
Konfiguration des LANCOM

Bei der Konfiguration des LANCOM werden die folgenden Schritte durchgeführt:

- Einrichten der Leitung zum SIP-Provider
- Aktivieren der ISDN-Schnittstelle und Zuordnung der MSNs zu den internen Rufnummern im LANCOM VoIP Router
- Anlegen der ISDN-Benutzer
- Anpassen der Call-Routing-Tabelle

So konfigurieren Sie das LANCOM im Detail:

① Führen Sie unter LANconfig den Setup-Assistenten zur Konfiguration des VoIP-Call-Managers aus. Aktivieren Sie die Optionen 'SIP-Provider', 'ISDN-Anlage oder -Vermittlungsstelle' und 'ISDN-Benutzer'.



② Richten Sie ein wie in den vorhergehenden Beispielen beschrieben:

- □ eindeutige lokale VoIP-Domäne
- □ eine Leitung zu einem SIP-Provider

③ Aktivieren Sie den externen ISDN-Amtsanschluss und den internen ISDN-Bus für die Nutzung der VoIP-Funktionen. Tragen Sie in der ISDN-Mapping-Tabelle alle externen MSNs des ISDN-Amtsanschlusses ein mit der Zuordnung zu den internen Rufnummern aus dem VoIP-Bereich.

④ Tragen Sie alle angeschlossenen ISDN-Endgeräte als ISDN-Benutzer mit folgenden Werten ein:

- □ Rufnummer / SIP-Name: Diese Rufnummer wird dem ISDN-Endgerät als „interne Rufnummer" zugewiesen. Die Telefonstruktur bleibt übersichtlich, wenn Sie hier die gleiche interne Rufnummer verwenden, die das Endgerät auch in seinem ISDN-Umfeld verwendet.
- □ MSN/DDI: Tragen Sie hier die externe MSN des ISDN-Amtsanschlusses ein, die auch über die ISDN-TK-Anlage dem Endgerät zugewiesen wird.

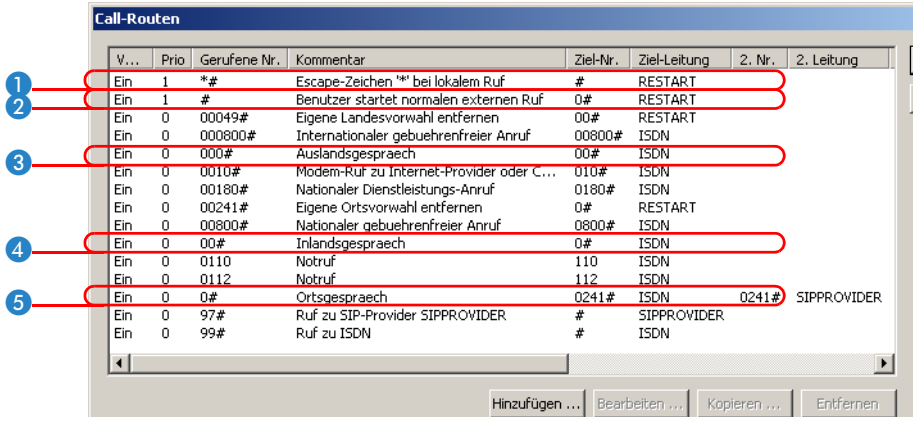
⑤ Aktivieren Sie die spontane Amtsholung für ISDN- und SIP-Benutzer, um das Telefonverhalten der Gesprächsteilnehmer möglichst konsistent zu halten.

⑥ Die vom Setup-Assistenten vorgeschlagene Call-Routing-Tabelle berücksichtigt die spontane Amtsholung für ISDN- und SIP-Benutzer 1 und 2.

Routen für die spontane Amtsholung

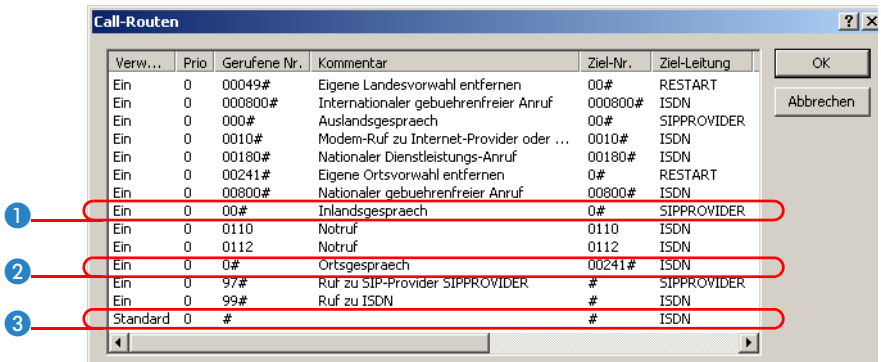
Die Angabe der Quell-Leitung 'USER' ist auf dem Screenshot nicht sichtbar. Durch diesen Filter gilt die Route nur für Rufe, die von einem lokalen Benutzer stammen. Die Ziel-Leitung 'RESTART' veranlasst einen erneuten Durchlauf durch die Call-Routing-Tabelle, wobei jedoch die Quell-Leitung gelöscht wird. Durch die fehlende Quell-Leitung passt die Route im zweiten Durchlauf nicht auf diesen Ruf.

Durch die beiden Routen wird bei jedem Anruf von einem lokalen Benutzer ein evtl. vorangestellter Stern '*' aus der Rufnummer entfernt. Bei allen anderen Anrufen von lokalen Benutzern wird der Rufnummer eine '0' vorangestellt, da es sich dann um einen externen Verbindungsaufbau handeln muss.



Mit den übrigen Routen werden z.B. internationale 3 und nationale 4 Ferngespräche sowie Ortsgespräche 5 standardmäßig auf der ISDN-Leitung ausgegeben. Dabei entfernt der Call-Router die führenden Nullen wieder aus der Rufnummer und setzt die Rufe auf der ISDN-Leitung ab.

Um spezielle Anrufziele wie z.B. internationale und nationale Ferngespräche nicht über ISDN, sondern 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 Backupleitung bei Bedarf entsprechend von SIP auf ISDN umzustellen!



Diese Call-Routing-Tabelle gilt ausdrücklich nur für eine TK-Anlage, die das Sonderzeichen Stern '*' für die internen Gespräche auf ihrem externen ISDN-Bus weitergibt. Verarbeitet die TK-Anlage dieses Zeichen anders, muss die Tabelle entsprechend angepasst werden.

Konfiguration der VoIP-Endgeräte

Die Konfiguration der VoIP-Endgeräte verläuft so wie in den vorhergehenden Beispielen beschrieben mit internen VoIP-Domäne und internen Rufnummern des eigenen Standortes.

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. Als externe MSN der VoIP-Endgeräte gegenüber der TK-Anlage kann hier die interne Rufnummer der SIP-Benutzer verwendet werden.

Konfiguration der ISDN-Endgeräte

Die Konfiguration der ISDN-Endgeräte beschränkt sich in der Regel auf den Eintrag der verwendeten internen MSN der TK-Anlage.

Ablauf des Call-Routings bei abgehenden Rufen

	Benutzer	wählt	passende Call-Route	passender Benutzer	Mapping, verwendete Nummer	Ziel-Leitung
①	VoIP-Telefon	*14	1 *#	VoIP-Softphone	#: 14	intern
②	VoIP-Telefon	*11	1 *#	ISDN-Benutzer	#: 11	ISDN

① Interner Anruf zwischen zwei VoIP-Endgeräten. Im ersten Durchlauf wird nur der Stern aus der Rufnummer entfernt, die Quell-Leitung wird gelöscht. Beim zweiten Durchlauf passt keine Route mehr auf diesen Ruf, der Call-Router findet jedoch einen passenden Eintrag eines SIP-Benutzers in der Liste der angemeldeten Benutzer und kann den Ruf zustellen.

② Interner Anruf von VoIP nach ISDN. Im ersten Durchlauf wird wieder der Stern aus der Rufnummer entfernt, die Quell-Leitung wird gelöscht. Beim zweiten Durchlauf passt keine Route mehr auf diesen Ruf, der Call-Router findet jedoch einen passenden Eintrag eines ISDN-Benutzers in der Liste der angemeldeten Benutzer und gibt den Ruf über die für diesen Benutzer konfigurierte ISDN-Schnittstelle aus. Dabei wird die Ziel-Rufnummer durch die für diesen Benutzer eingetragene MSN '555 555 1' ersetzt. Die TK-Anlage empfängt den Ruf zu '555 555 1' auf ihrem externen ISDN-Bus und deutet diese Nummer wieder als externe MSN und kann den Ruf an das zugehörige ISDN-Telefon zustellen.

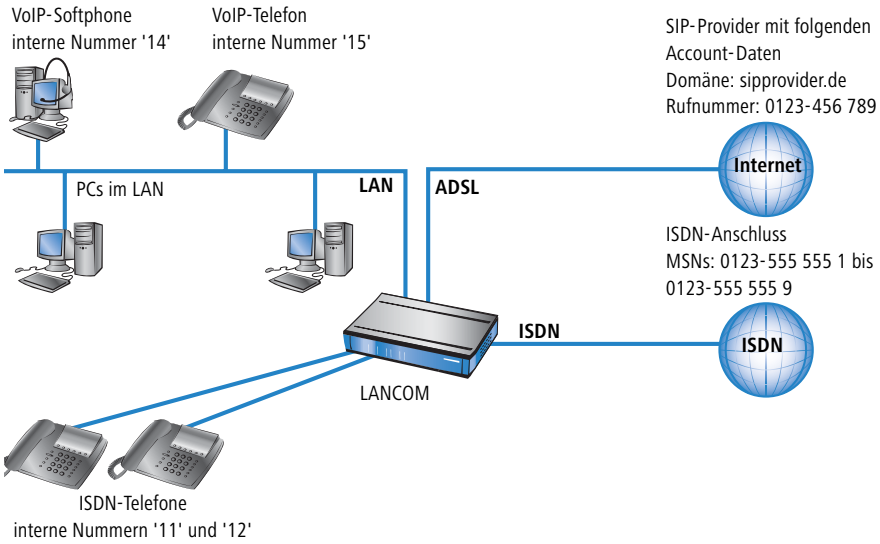
Ablauf des Call-Routings bei eingehenden Rufen

	Gegenstelle wählt	Call-Router empfängt	Zuordnung über	verwendete Nummer	passende Call-Route	Ziel-Leitung
①	0 123 555 555 1	555 555 1	■ ISDN-Mapping-Tabelle ■ Liste der lokalen ISDN-Benutzer	11		ISDN NT

① Der eingehende Anruf über die Rufnummer an die MSNs für die angeschlossenen ISDN-Endgeräte wird über die ISDN-Mapping-Tabelle in eine interne Rufnummer umgesetzt und 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 mit der für diesen Benutzer eingetragenen MSN '555 555 1' auf der ISDN-Leitung aus. Die TK-Anlage empfängt den Ruf zu '555 555 1' auf ihrem externen ISDN-Bus und deutet diese Nummer wieder als externe MSN und kann den Ruf an des zugehörige ISDN-Telefon zustellen.

13.13.4 VoIP-Telefonie als Ergänzung zu vorhandenen ISDN-Telefonen

Dieses Beispiel zeigt die Konfiguration eines LANCOM, wenn die bisher verwendeten ISDN-Telefone um die Möglichkeiten der VoIP-Telefonie erweitert werden. Die externen MSNs '555 555 1' und '555 555 2' auf dem ISDN-Bus am NTBA werden bisher für zwei ISDN-Telefone verwendet. Das LANCOM wird nun zwischen den öffentlichen ISDN-Anschluss und den internen ISDN-Bus mit den angeschlossenen ISDN-Telefonen geschaltet.



Ziel

- Internes Telefonieren der ISDN- und SIP-Telefone sowie SIP-Softphones.
- Externes Telefonieren der ISDN- und SIP-Endgeräte über ISDN.
- Erreichbarkeit der internen Endgeräte (ISDN und SIP) über die MSNs.

Voraussetzungen

- LANCOM angeschlossen an LAN und WAN, eine ISDN-NT-Schnittstelle ist mit den ISDN-Telefonen verbunden, eine ISDN-TE-Schnittstelle mit dem ISDN-Amt (NTBA). Der Internetzugang ist eingerichtet.
- Ein Rufnummernplan mit einer eindeutigen internen Rufnummer für jedes anzuschließende Endgerät.
- Ein Account bei einem SIP-Provider.

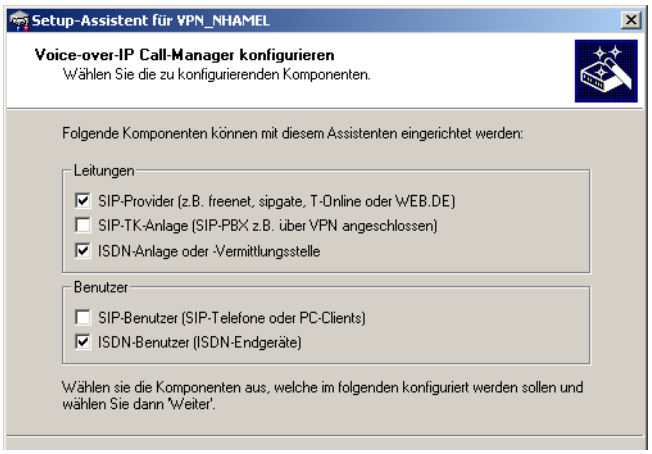
Konfiguration des LANCOM

Bei der Konfiguration des LANCOM werden die folgenden Schritte durchführt:

- Einrichten der Leitung zum SIP-Provider
- Aktivieren der ISDN-Schnittstelle und Zuordnung der MSNs zu den internen Rufnummern im LANCOM VoIP Router
- Anlegen der ISDN-Benutzer
- Anpassen der Call-Routing-Tabelle

So konfigurieren Sie das LANCOM im Detail:

① Führen Sie unter LANconfig den Setup-Assistenten zur Konfiguration des VoIP-Call-Managers aus. Aktivieren Sie die Optionen 'SIP-Provider', 'ISDN-Anlage oder -Vermittlungsstelle' und 'ISDN-Benutzer'.



② Richten Sie ein wie in den vorhergehenden Beispielen beschrieben:

- □ eindeutige lokale VoIP-Domäne
- □ eine Leitung zu einem SIP-Provider

③ Aktivieren Sie den externen ISDN-Amtsanschluss und den internen ISDN-Bus für die Nutzung der VoIP-Funktionen. Tragen Sie in der ISDN-Mapping-Tabelle alle externen MSNs des ISDN-Amtsanschlusses ein mit der Zuordnung zu den internen Rufnummern aus dem VoIP-Bereich.

④ Tragen Sie alle angeschlossenen ISDN-Endgeräte als ISDN-Benutzer mit folgenden Werte ein:

- Rufnummer / SIP-Name: Diese Rufnummer wird dem ISDN-Endgerät als „interne Rufnummer" zugewiesen. Die Telefonstruktur bleibt übersichtlich, wenn Sie hier die gleiche interne Rufnummer verwenden, die das Endgerät auch in seinem ISDN-Umfeld verwendet.
- MSN/DDI: Tragen Sie hier die externe MSN des ISDN-Amtsanschlusses ein, die vorher schon im ISDN-Telefon eingetragen war.

Zuordnung von externen MSNs und internen Rufnummern

Die externen MSNs und die internen Rufnummern werden in diesem Beispiel „über Kreuz" zugewiesen:

- In der ISDN-Mapping-Tabelle wird der externen MSN '555 555 1' z.B. die interne Rufnummer '11' zugeordnet. Ein externer Anruf an die '555 555 1' wird also in der Vermittlung des LANCOM als Ruf an die '11' behandelt.
- Mit der Zuweisung der MSN '555 555 1' zur internen Rufnummer des ISDN-Benutzers '11' wird der Ruf auf dem internen ISDN-Bus des LANCOM mit der Ziel-Rufnummer '555 555 1' ausgegeben.

Da das ISDN-Telefon wie vor dem Einsatz des LANCOM VoIP Router auf seine MSN „hört", wird der Ruf an das richtige Endgerät zugestellt.

Sollte der LANCOM VoIP Router durch einen Stromausfall ausfallen, können bei aktiviertem Life-Line-Support und Spannungsweiterleitung auf dem ISDN-Bus die angeschlossenen ISDN-Telefone auch ohne das zwischengeschaltete Gerät telefonieren.

⑤ Aktivieren Sie die spontane Amtsholung für ISDN- und SIP-Benutzer, um das Telefonverhalten der Gesprächsteilnehmer möglichst konsistent zu halten.

⑥ Alle weiteren Konfigurationen sowie die Anpassung der Call-Routing-Tabelle werden synonym zum Beispiel 'VoIP-Telefonie als Ergänzung zur untergeordneten ISDN-TK-Anlage' vorgenommen.

Konfiguration der VoIP-Endgeräte

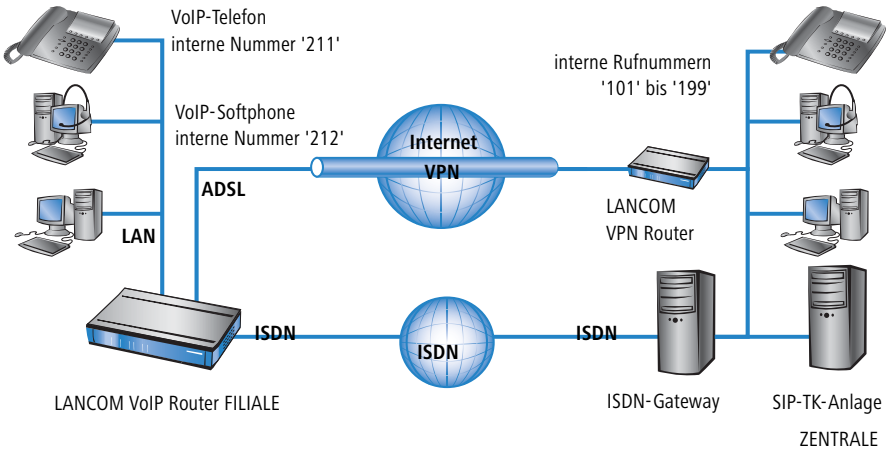
Die Konfiguration der VoIP-Endgeräte verläuft so wie in den vorhergehenden Beispielen beschrieben mit der internen VoIP-Domäne und den internen Rufnummern des eigenen Standortes.

Konfiguration der ISDN-Telefone

Die Konfiguration der ISDN-Endgeräte beschränkt sich in der Regel auf den Eintrag der verwendeten externen MSN. Da diese bei den vorher schon vorhandenen ISDN-Telefonen in der Regel schon eingetragen waren, sind hier keine Änderungen nötig.

13.13.5 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'.



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.

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.
- Ein Account bei einem SIP-Provider.

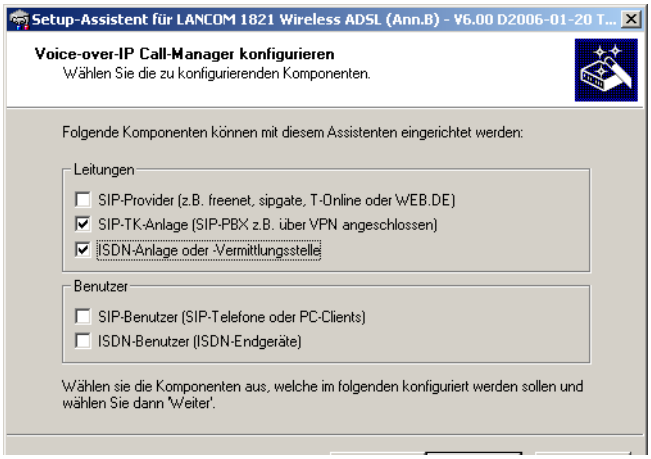
Konfiguration des LANCOM

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	■ Gerufene Nummer '2#' ■ Ziel-Leitung 'LOCATION_B' ■ Ziel-Nummer '2#'		

So konfigurieren Sie das LANCOM im Detail:

① Führen Sie unter LANconfig den Setup-Assistenten zur Konfiguration des VoIP-Call-Managers aus. Aktivieren Sie die Optionen 'SIP-TK-Anlage' und 'ISDN-Anlage oder -Vermittlungsstelle'.



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.

Gemeinsames oder benutzerabhängiges SIP-PBX-Passwort

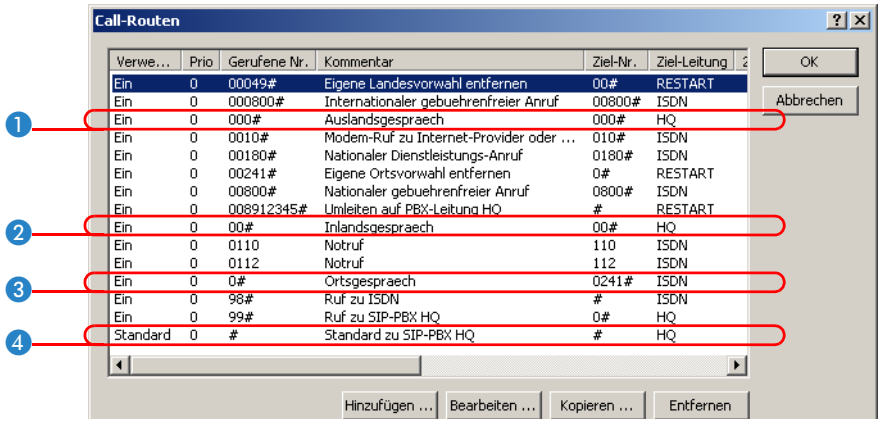
Falls die Anmeldung mit einem gemeinsamen Passwort nicht erwünscht ist, kann auch für jeden SIP-Benutzer ein eigenes Passwort verwendet werden. In diesem Fall wird jeder SIP-Benutzer im LANCOM mit einem eigenen Passwort konfiguriert.

- □ 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 ① und nationalen ② Ferngesprächen über die SIP-PBX in der Zentrale.

Eine **Standard-Route** ④ 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.



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.

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 ('Gemeinsames oder benutzerabhängiges SIP-PBX-Passwort' → Seite 13-73).

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.

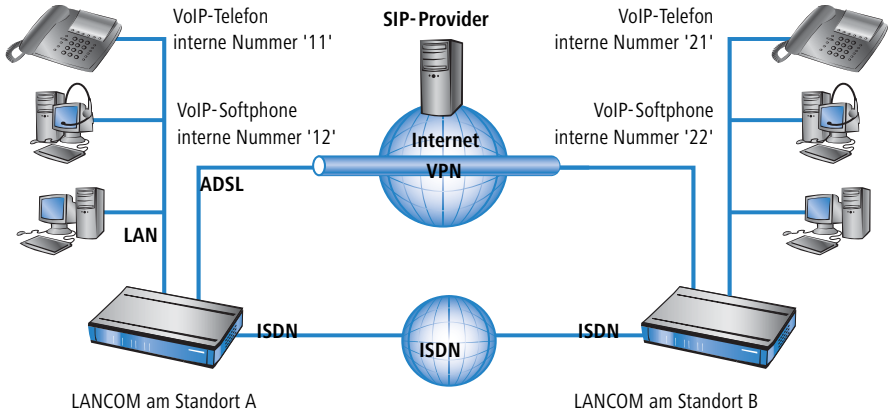
② Interner Anruf zwischen einem VoIP-Endgerät in der Filiale und dem internen Teilnehmer '199' in der Zentrale. Die gewählte Nummer '199' passt im ersten Durchlauf auf keine Route der Call-Routing-Tabelle, auch in der Liste der lokalen Benutzer wird kein passender Eintrag gefunden. Im zweiten Durchlauf 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.

13.13.6 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.



Ziel

- Internes Telefonieren über beide Standorte hinweg.
- Externes Telefonieren über den SIP-Provider mit Backup über ISDN.
- Gespräche zu Not- und Sonderrufnummern über ISDN.

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.

Konfiguration des LANCOM

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

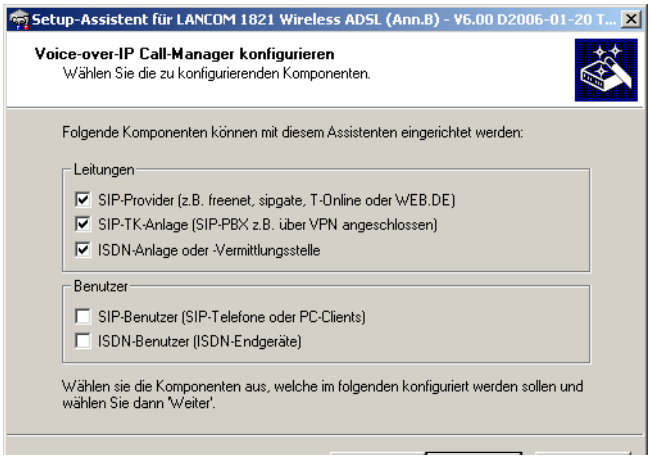
	LANCOM Standort A	SIP-Endgeräte Standort A	LANCOM Standort B	SIP-Endgeräte Standort B
interne VoIP-Domain	location_A.intern	location_A.intern	location_B.intern	location_B.intern
interne Rufnummern		10 bis 19		20 bis 29
externe SIP-Rufnummer	✔		✔	
Zugangsdaten SIP-Account	✔		✔	
externe ISDN-Rufnummern (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	■ Gerufene Nummer '2#' ■ Ziel-Leitung 'LOCATION_B' ■ Ziel-Nummer '2#'		■ Gerufene Nummer '1#' ■ Ziel-Leitung 'LOCATION_A' ■ 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 VoIP-Call-Managers aus. Aktivieren Sie die Optionen 'SIP-Provider', 'SIP-TK-Anlage' und 'ISDN-Anlage oder -Vermittlungsstelle'.



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:

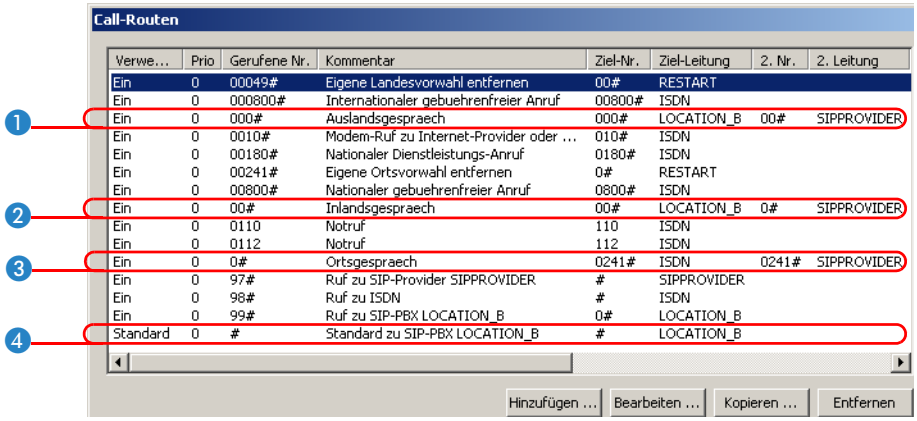
- □ SIP-PBX-Leitungs-Name: eindeutiger Name für die Leitung zum entfernten Standort.
- □ PBX SIP-Domäne/Realm: interne VoIP-Domäne des entfernten Standortes.
- □ Registrar (FQDN oder IP): Adresse des LANCOM am entfernten Standort, falls das Gerät nicht über DNS-Auflösung der VoIP-Domäne (PBX SIP-Domäne/Realm) identifiziert werden kann.

Verwenden Sie hier die private, über VPN erreichbare IP-Adresse des LANCOM, nicht die öffentliche IP.

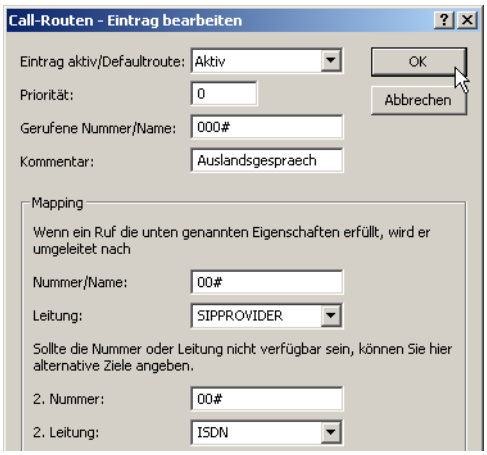
- □ Lassen Sie das Feld für das gemeinsame Passwort bei der Anmeldung an der SIP-PBX frei.
- □ Lassen Sie das Feld für die öffentliche PBX-Nummer frei.

⑤ Die vom Setup-Assistenten vorgeschlagene Call-Routing-Tabelle sieht die Ausführung von internationalen ❶ und nationalen ❷ Ferngesprächen über die Leitung des entfernten Standortes vor, Ortsgespräche ❸ werden über ISDN geleitet.

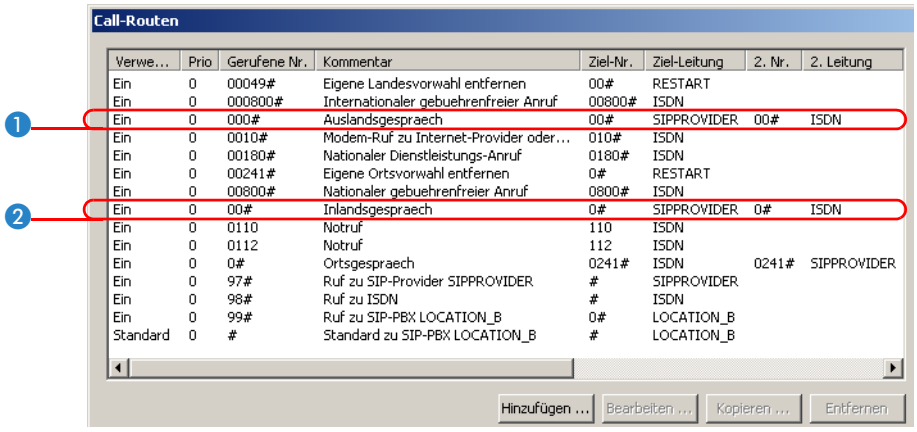
Eine **Standard-Route** ❹ wird zudem genutzt, um alle nicht auflösbaren Rufnummern über die Leitung des entfernten Standortes auszuführen.



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 1 und nationale 2 Ferngespräche sieht die Call-Routing-Tabelle dann z.B. so aus:



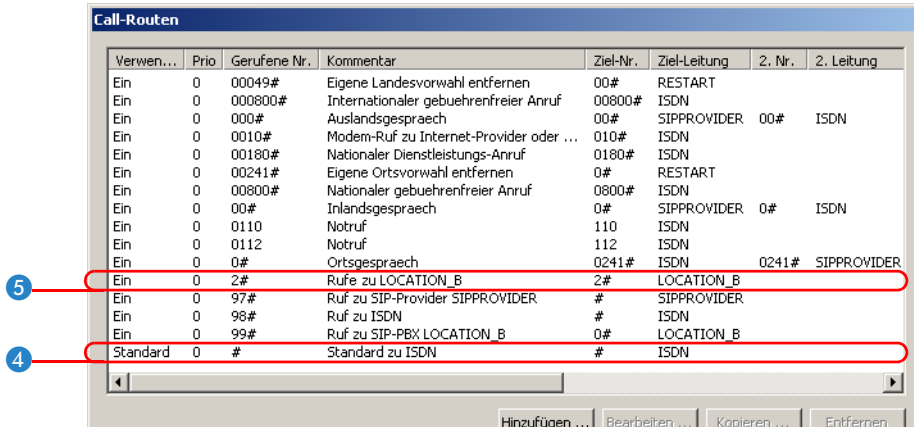
⑦ In diesem Zustand werden alle von der Call-Routing-Tabelle nicht auflösbaren Rufe, für die es auch keinen passenden Eintrag in der Liste der lokalen Benutzer gibt, automatisch an den entfernten Standort weitergeleitet.

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 5 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 4 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:



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.

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.

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

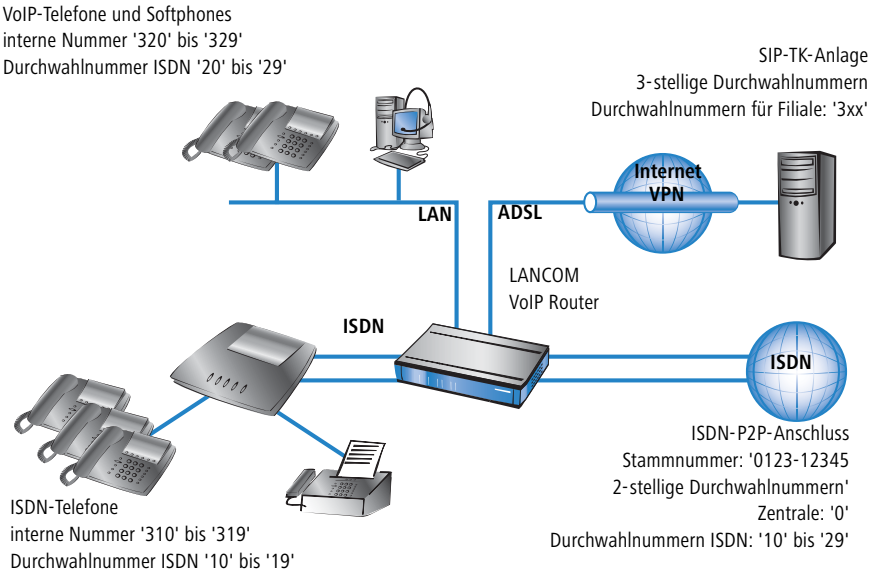
① Interner Anruf zwischen zwei VoIP-Endgeräten an Standort A und B. Die gewählte Nummer '21' passt auf die Route 5 '2#' der Call-Routing-Tabelle. Der Call-Router führt den Anruf mit der unveränderten Rufnummer über die Leitung zur entfernten SIP-PBX aus.

13.13.7 LANCOM VoIP Router an einem P2P-Anschluss (Anlagenanschluss)

Viele Unternehmen nutzen statt des ISDN-Anschlusses in Punkt-zu-Mehrpunkt-Ausführung (auch als „Mehrgeräteanschluss" bezeichnet) einen ISDN-Anschluss in Punkt-zu-Punkt-Ausführung („Anlagenanschluss"). Der Anlagenanschluss bietet zwei wesentliche Vorteile:

- Über die Durchwahlfähigkeit (DDI – Direct Dialing In) können alle Endgeräte über eine gemeinsame Stammnummer mit nachgestellter Durchwahl zur Auswahl der einzelnen Geräte erreicht werden.
- Eine größere Anzahl von B-Kanälen kann mit dem gleichen Rufnummernkreis genutzt werden, während beim Mehrgeräteanschluss zu einem Anschluss immer nur zwei B-Kanäle mit üblicherweise bis zu 10 Rufnummern gehören.

ISDN-P2P-Anschlüsse sind als Basisanschluss (Basic Rate Interface – BRI) mit jeweils zwei B-Kanälen oder als Primärmultiplexanschluss (Primary Rate Interface – PRI) mit üblicherweise 30 B-Kanälen verfügbar. LANCOM VoIP Router unterstützen ausschliesslich ISDN-Basisanschlüsse. Um mehr als vier B-Kanäle zu nutzen, können bei einem P2P-Anschluss mehrere Basisanschlüsse mit dem gleichen Rufnummernkreis zusammengeschaltet werden.



Zielsetzung für den Einsatz des LANCOM VoIP Router

- Anschluss von zusätzlichen SIP-Endgeräten in der Filiale.
- Internes Telefonieren mit Benutzern in der Zentrale und anderen Filialen über die SIP-PBX der Zentrale (über VPN-Verbindung).

Voraussetzungen

- LANCOM angeschlossen an LAN und WAN (über DSL/ADSL), ISDN-TE-Schnittstelle(n) sind mit dem ISDN-P2P-Anschluss verbunden, ISDN-NT-Schnittstelle(n) sind mit einer ISDN-TK-Anlage 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.

Konfiguration des LANCOM

Die Konfiguration der SIP-Clients bzw. der Verbindung zur SIP-TK-Anlage als SIP-PBX-Leitung mit dem Namen 'HQ' wurden schon in anderen Anwendungsbeispielen beschrieben und werden hier als bekannt vorausgesetzt. Die SIP-TK-Anlage der Zentrale verwendet die SIP-Domäne 'mycompany.HQ', die Filiale die interne Domöne 'mycompany.BRANCH01'.

So konfigurieren Sie das LANCOM für den Betrieb am Anlagenanschluss:

① In der ISDN-Mapping-Tabelle wird eine Umsetzung der DDI (Durchwahlnummern) zu den internen Rufnummern zur Verarbeitung als SIP-Ruf vorgenommen.

MSN/DDI	ISDN/S0-Bus	interne Nummer	Kommentar
0	ISDN1, ISDN2	300	Setzt die DDI '0' auf die interne Nummer '300' um
#	ISDN1, ISDN2	3#	Stellt allen anderen DDI '0' jeweils eine '3' für die interne Nummer voran

Beide Einträge gelten in diesem Beispiel für die ISDN-Interfaces 1 und 2, die mit dem ISDN-Anschluss verbunden sind. Durch die Aktivierung von zwei ISDN-Interfaces stehen vier B-Kanäle zur Verfügung. Wenn beide B-Kanäle einer ISDN-Schnittstelle besetzt sind, wird automatisch versucht, die Verbindung über eine andere ISDN-Schnittstelle mit freien B-Kanälen aufzubauen.

② Mit den Einträgen für die ISDN-Benutzer wird eine Rückübersetzung der internen Rufnummern zu den DDI vorgenommen.

interne Nummer	MSN/DDI	ISDN/S0-Bus	Kommentar
300	0	ISDN3, ISDN4	Setzt die interne Nummer '300' auf die DDI '0' um. Sinnvoll, wenn sich die Zentrale an der ISDN-TK-Anlage befindet.
31#	1#	ISDN3, ISDN4	Schneidet bei allen mit '31 beginnenden internen Rufnummern die führende '3' ab.

Mit dem zweiten Eintrag werden die ISDN-Endgeräte mit den ISDN-Durchwahlen '10' bis '19' als ISDN-Benutzer im VoIP-System bekannt gemacht. Ein einzelner Eintrag reicht hier für alle Teilnehmer. Die Anmeldedaten für die SIP-TK-Anlage werden von allen ISDN-Benutzern gemeinsam genutzt.

Die mit dem #-Zeichen eingetragenen ISDN-Benutzer können von der SIP-TK-Anlage nur erreicht werden, wenn die SIP-TK-Anlage keine Registrierung erfordert. Für eine Registrierung der ISDN-Benutzer sind separate Einträge in der ISDN-Benutzer-Liste erforderlich.

Beide Einträge gelten in diesem Beispiel für die ISDN-Interfaces 3 und 4, die mit der ISDN-TK-Anlage verbunden sind. Auch hier können die vier B-Kanäle der beiden Schnittstellen „dynamisch" für die Verbindung zwischen ISDN-TK-Anlage und LANCOM VoIP Router genutzt werden.

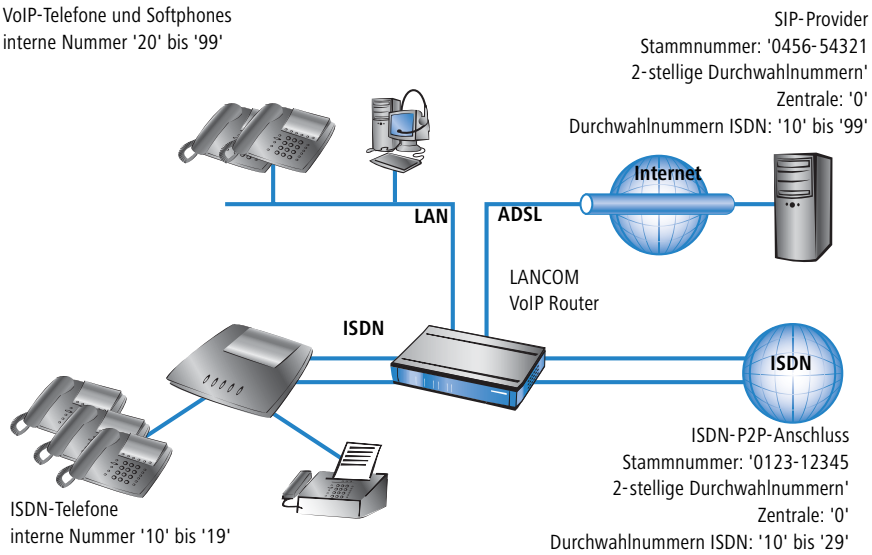
③ Das Routing der Rufe wird über die Call-Routing-Tabelle geregelt. Bei der Verwendung der Assistenten von LANconfig wird die Call-Routing-Tabelle so vordefiniert, dass alle abgehenden Rufe von ISDN- und SIP-Geräten über die SIP-TK-Anlage der Zentrale geleitet werden bis auf Ortsgespräche und Gespräche zu Sonderrufnummern wie z.B. Notrufnummern oder „0800er"-Nummern.

13.13.8 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 den vorhandenen ISDN-Anlagenanschluss mit 20 Durchwahlen um einen SIP-Trunking-Account mit bis zu 100 Durchwahlnummern erweitern 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 '0123-12345 12' ebenso reagieren wie auf Rufe an '0456-54321 12'.

Abgehende Anrufe sollen in der Regel über den SIP-Account geführt werden bis auf die bestimmten Ausnahmen (Notrufnummern und Sonderrufnummern wie „0800er"-Nummern). Durch die Signalisierung der SIP-Rufnummer bei den Gesprächspartnern wird der mittelfristige Wegfall der ISDN-Rufnummern vorbereitet.

Zielsetzung für den Einsatz des LANCOM VoIP Router

- Anschluss von zusätzlichen SIP-Endgeräten.
- Internes Telefonieren zwischen ISDN- und SIP-Endgeräten.
- Beibehalten der Erreichbarkeit über die bisherigen ISDN-Rufnummern.
- Günstiges Telefonieren über einen gemeinsam genutzten SIP-Account.

Voraussetzungen

- LANCOM angeschlossen an LAN und WAN (über DSL/ADSL), ISDN-TE-Schnittstelle(n) sind mit dem ISDN-P2P-Anschluss verbunden, 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.

Konfiguration des LANCOM

So konfigurieren Sie das LANCOM für den Betrieb am Anlagenanschluss:

① Das LANCOM wird mit zwei einfachen Einträgen in der ISDN-Mapping-Tabelle und in der Liste der ISDN-Benutzer für den Betrieb am Anlagenanschluss konfiguriert.

ISDN-Mapping-Tabelle:

MSN/DDI	ISDN/S0-Bus	interne Nummer	Kommentar
#	ISDN1, ISDN2	#	Gibt die DDI unverändert als interne Rufnummer aus.

ISDN-Benutzer-Liste

interne Nummer	MSN/DDI	ISDN/S0-Bus	Kommentar
#	#	ISDN3, ISDN4	Gibt die internen Rufnummern unverändert als DDI aus.

② 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.

③ Für den SIP-Account wird eine SIP-Provider-Leitung angelegt. Dabei wird als Betriebsmodus für diese Leitung die Option 'Trunk' ausgewählt.

④ 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 bis auf Ortsgespräche und Gespräche zu Sonderrufnummern wie z.B. Notrufnummern oder „0800er"-Nummern.

Ablauf des Call-Routing

Das Call-Routing profitiert in diesem Beispiel von den eindeutigen internen Rufnummern.

- Bei ankommenden Rufen – egal ob über ISDN oder SIP – 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, siehe 'ISDN-Mapping' → Seite 13-30 und 'SIP-Mapping' → Seite 13-26.

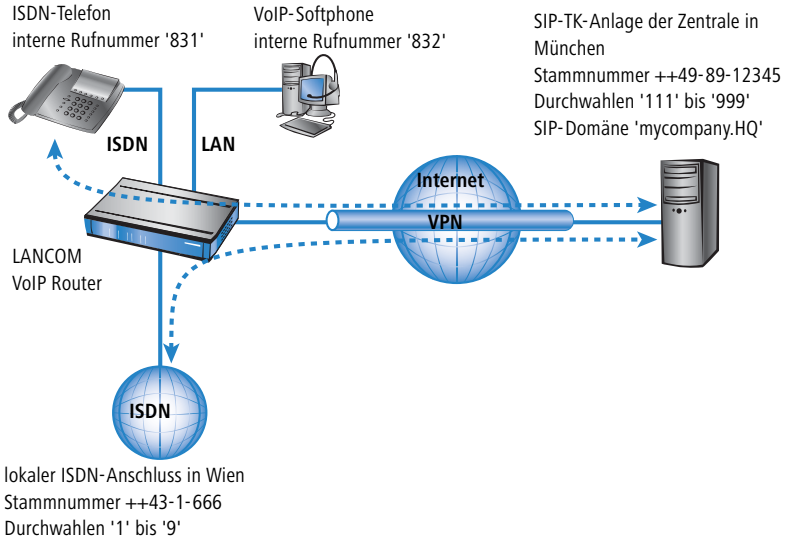
- Bei den abgehenden Rufen kann über die Call-Routing-Tabelle gesteuert werden, ob die Rufe über ISDN oder SIP ausgeführt werden. In der Standard-Einstellung nach Verwendung der Assistenten gilt SIP als normale Ziel-Leitung (bis auf Ortsgespräche und Sonderrufnummern). Durch das Umstellen eines Eintrags 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.

13.13.9 Remote Gateway

In verteilten Unternehmensstrukturen sind in den Filialen üblicherweise ISDN-Anschlüsse vorhanden, um den Mitarbeitern mit den entsprechenden ISDN-Endgeräten lokal einen Zugang zum Telefonnetz bereitzustellen.

- Mit einem LANCOM VoIP Router kann sehr komfortabel eine Anbindung der lokalen ISDN-Endgeräte an eine SIP-TK-Anlage in der Zentrale eingerichtet werden.
- Mit der Funktion des „Remote Gateway" können darüber hinaus nicht nur die Endgeräte, sondern auch die lokalen ISDN-Anschlüsse an die zentrale TK-Anlage angebunden werden. Die Vorteile des Remote Gateway:
  - Die lokalen ISDN-Anschlüsse stehen allen Benutzern im Unternehmensnetz zur Verfügung. Gespräche in das lokale ISDN-Netz können von allen Standorten aus als Ortsgespräche geführt werden, auch über Ländergrenzen hinweg.
  - Alle Gespräche – auch von den lokalen Benutzern ins „eigene" Ortsnetz – können über die SIP-TK-Anlage geführt werden und ermöglichen so eine zentrale Administration und Protokollierung.



In diesem Beispiel betrachten wir ein Unternehmen mit der Zentrale in München. Die Filiale in Wien soll über die internen Rufnummern mit der Zentrale telefonieren können. Dazu werden aus dem Rufnummernkreis der Zentrale die „83-er"-Nummern für Wien reserviert. Die Abteilungen Support und Vertrieb in der Zentrale sollen auch aus Österreich über ein Ortsgespräch bzw. ein nationales Ferngespräch in Wien erreichbar sein. Der Einkauf möchte Lieferanten in Österreich ebenfalls über nationale Ferngespräche erreichen können.

Zielsetzung für den Einsatz des LANCOM VoIP Router

- Internes Telefonieren mit Benutzern in der Zentrale und anderen Filialen über die SIP-PBX der Zentrale (über VPN-Verbindung).
- Einbindung der lokalen ISDN-Schnittstelle in die Telefonstruktur des Unternehmens.

Voraussetzungen

- LANCOM angeschlossen an LAN und WAN (über DSL/ADSL), ISDN-TE-Schnittstelle(n) sind mit dem ISDN-Anschluss verbunden, ISDN-NT-Schnittstelle(n) sind mit einer ISDN-TK-Anlage oder den ISDN-Endgeräten 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.

Konfiguration des LANCOM

Die Konfiguration des LANCOM VoIP Router setzt sich aus folgenden Einzelschritten zusammen:

- Für jeden ISDN-Benutzer wird ein Eintrag angelegt, damit sich die Endgeräte bei der übergeordneten SIP-TK-Anlage anmelden können.
- Für die SIP-Clients werden diese Anmelde-Informationen im VoIP-Telefon bzw. im Softphone eingetragen.
- Die Verbindung zur SIP-TK-Anlage als SIP-PBX-Leitung mit dem Namen 'HQ' wurden schon in anderen Anwendungsbeispielen beschrieben und werden hier als bekannt vorausgesetzt.
- Neben dieser Leitung muss eine weitere Leitung zur SIP-TK-Anlage als „Gateway" angelegt werden, mit deren Hilfe der lokale ISDN-Anschluss in der übergeordneten SIP-TK-Anlage bekannt gemacht wird.
- Über die Einträge in der Call-Routing-Tabelle wird die Verbindung zwischen lokalem ISDN-Anschluss und der entfernten SIP-TK-Anlage vorgenommen.

So konfigurieren Sie das LANCOM für den Betrieb als Remote Gateway:

① In der ISDN-Mapping-Tabelle wird eine Umsetzung der lokalen DDI (Durchwahlnummern) zu den internen Rufnummern zur Verarbeitung als SIP-Ruf vorgenommen.

MSN/DDI	ISDN/S0-Bus	interne Nummer	Kommentar
#	ISDN1, ISDN2	#	Alle an den ISDN-Schnittstellen anliegenden DDI werden unverändert weiter vermittelt.

② In der Liste der SIP-Provider-Leitungen wird ein neuer Eintrag erstellt mit folgenden Daten:

- □ Name der Leitung: 'GW.HQ'
- □ Modus: Gateway
- □ SIP-Domäne: SIP-Domäne der Zentrale 'mycompany.HQ'
- □ SIP-ID: Accountbezeichnung für das SIP-Gateway in der SIP-TK-Anlage der Zentrale
- □ Authentifizierungsname und Passwort: Anmeldedaten für das SIP-Gateway

③ In der Call-Routing-Tabelle werden zusätzliche Einträge vorgenommen, um die Anrufe zwischen der Zentrale und dem lokalen ISDN-Anschluss zu vermitteln:

gerufene Nummer	Ziel-Nummer	Quell-Leitung	Ziel-Leitung	Kommentar
#	83#	ISDN	GW.HQ	Leitet alle Anrufe, die über ISDN beim LANCOM VoIP Router eingehen, über die Gateway-Leitung in die Zentrale weiter. Dabei wird der gemeldeten DDI eine '83' vorangestellt, um die Zuordnung zu den internen Rufnummern zu erreichen.
9	555	ISDN	GW.HQ	Leitet alle Anrufe, die über ISDN beim LANCOM VoIP Router für die Durchwahl '9' eingehen, über die Gateway-Leitung in die Zentrale weiter. Dabei wird als Rufnummer die '555' für den Support verwendet.
0043#	0#	GW.HQ	ISDN	Leitet alle Anrufe aus der Zentrale für das Landesnetz Österreich ohne die Landesvorwahl an den lokalen ISDN-Anschluss weiter.
#	#			Leitet alle anderen Anrufe unverändert weiter.

Ablauf des Call-Routings bei Rufen

	Benutzer	wählt	Call-Router empfängt	Call-Router sendet	Zuordnung über	Quell-Leitung	Ziel-Leitung
①	ISDN-Netz D	089-12345-831	831	831	■ Liste der lokalen ISDN-Benutzer	GW.HQ	intern
②	ISDN-Netz A	666-1	1	831	■ Call-Routing-Tabelle ■ Liste der lokalen ISDN-Benutzer	ISDN	GW.HQ
③	ISDN-Netz A	666-9	9	555	■ Call-Routing-Tabelle	ISDN	GW.HQ
④	SIP Zentrale	0043-662-33333	0043-662-33333	0662-33333	■ Call-Routing-Tabelle	GW.HQ	ISDN

① Anruf vom Kunden aus Hamburg an den Mitarbeiter in Wien. Der Kunde wählt die Nummer der Zentrale aus München mit der entsprechenden Durchwahl '089-12345-831'. Die TK-Anlage der Zentrale empfängt nur die DDI '831' und gibt diese über die SIP-PBX-Leitung weiter, weil hier der ISDN-Benutzer mit der internen Rufnummer angemeldet ist. Der LANCOM VoIP Router empfängt die '831', findet einen passenden Eintrag in der Liste der lokal angemeldeten Benutzer und kann den Ruf zustellen.

② Anruf vom Kunden aus Wien an die Filiale in Wien. Der Kunde wählt die Nummer der Filiale in Wien mit der zugehörigen Durchwahl '666-1'.

- □ Der LANCOM VoIP Router empfängt die DDI '1' und findet keinen passenden Eintrag in der Liste der lokal angemeldeten Benutzer. Über die Call-Routing-Tabelle wird die Rufnummer in die '831' geändert und über die SIP-Gateway-Leitung an die TK-Anlage nach München weitergegeben. Die TK-Anlage kennt den angemeldeten ISDN-Benutzer mit der internen Rufnummer '831' und leitet den Ruf über die SIP-PBX-Leitung an den LANCOM VoIP Router zurück.
- □ Der LANCOM VoIP Router empfängt nun die '831', findet den passenden Eintrag in der Liste der lokal angemeldeten Benutzer und kann den Ruf zustellen.

③ Anruf vom Kunden aus Salzburg an die Support-Rufnummer in Wien. Der Kunde wählt die Nummer der Filiale in Wien mit der zugehörigen Support-Durchwahl '666-9'. Der Anruf wird über die Call-Routing-Tabelle automatisch an die interne Rufnummer '555' für den Support zugestellt.

④ Anruf vom Mitarbeiter in München an den Kunden in Salzburg. Der Mitarbeiter wählt '0043-662-33333'. Die TK-Anlage in München ist so eingestellt, dass alle Rufe nach Österreich über die SIP-Gateway-Leitung an den LANCOM VoIP Router weitergeleitet werden. Der Call-Router empfängt die vollständige Rufnummer, schneidet anhand der Routing-Tabelle mit der Quell-Leitung 'GW.HQ' die Landesvorwahl aus und gibt die restliche Rufnummer auf der ISDN-Leitung aus.



Bei diesem Anruf wird der Gegenstelle die Rufnummer aus München angezeigt.

13.14 Diagnose der VoIP-Verbindungen

13.14.1 SIP Traces

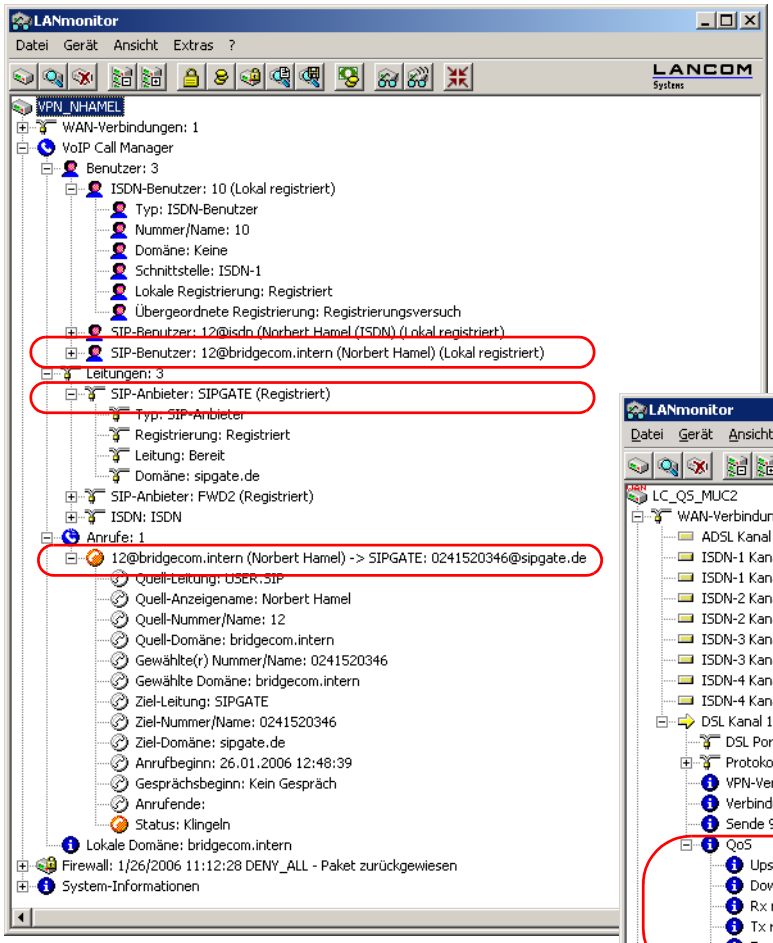
Zur Kontrolle der internen Abläufe in den LANCOM-Geräten während oder nach der Konfiguration bieten sich Trace-Ausgaben an. Mit einem SIP-Trace werden alle SIP-Informationen angezeigt, die zwischen einem LANCOM VoIP Router und einem SIP-Provider bzw. einer übergeordneten SIP-TK-Anlage ausgetauscht werden. Der SIP-Trace wird mit folgendem Befehl eingeschaltet:

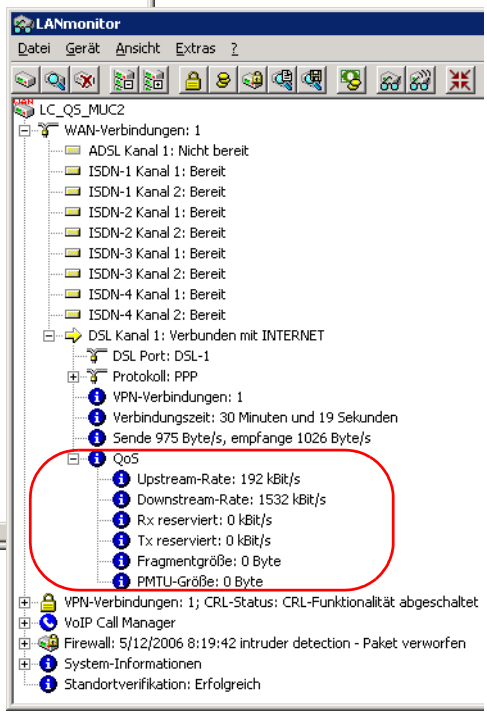
```
trace + sip-packet
```

13.14.2 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.


LANmonitor
Datei Gerät Ansicht Extras ?
LANCOM Systems
VPN_NHAMEL
WAN-Verbindungen: 1
VoIP Call Manager
Benutzer: 3
ISDN-Benutzer: 10 (Lokal registriert)
Typ: ISDN-Benutzer
Nummer/Name: 10
Domäne: Keine
Schnittstelle: ISDN-1
Lokale Registrierung: Registriert
Übergeordnete Registrierung: Registrierungsversuch
SIP-Benutzer: 12@isdn (Norbert Hamel (ISDN)) (Lokal registriert)
SIP-Benutzer: 12@bridgecom.intern (Norbert Hamel) (Lokal registriert)
Leitungen: 3
SIP-Anbieter: SIPGATE (Registriert)
Typ: SIP-Anbieter
Registrierung: Registriert
Leitung: Bereit
Domäne: sipgate.de
SIP-Anbieter: FWD2 (Registriert)
ISDN: ISDN
Anrufe: 1
12@bridgecom.intern (Norbert Hamel) -> SIPGATE: 0241520346@sipgate.de
Quell-Leitung: USER.SIP
Quell-Anzeigename: Norbert Hamel
Quell-Nummer/Name: 12
Quell-Domäne: bridgecom.intern
Gewählte(r) Nummer/Name: 0241520346
Gewählte Domäne: bridgecom.intern
Ziel-Leitung: SIPGATE
Ziel-Nummer/Name: 0241520346
Ziel-Domäne: sipgate.de
Anrufbeginn: 26.01.2006 12:48:39
Gesprächsbeginn: Kein Gespräch
Anrufende:
Status: Klingeln
Lokale Domäne: bridgecom.intern
Firewall: 1/26/2006 11:12:28 DENY_ALL - Paket zurückgewiesen
System-Informationen


LANmonitor
Datei Gerät Ansicht Extras ?
LC_QS_MUC2
WAN-Verbindungen: 1
ADSL Kanal 1: Nicht bereit
ISDN-1 Kanal 1: Bereit
ISDN-1 Kanal 2: Bereit
ISDN-2 Kanal 1: Bereit
ISDN-2 Kanal 2: Bereit
ISDN-3 Kanal 1: Bereit
ISDN-3 Kanal 2: Bereit
ISDN-4 Kanal 1: Bereit
ISDN-4 Kanal 2: Bereit
DSL Kanal 1: Verbunden mit INTERNET
DSL Port: DSL-1
Protokoll: PPP
VPN-Verbindungen: 1
Verbindungszeit: 30 Minuten und 19 Sekunden
Sende 975 Byte/s, empfange 1026 Byte/s
QoS
Upstream-Rate: 192 kBit/s
Downstream-Rate: 1532 kBit/s
Rx reserviert: 0 kBit/s
Tx reserviert: 0 kBit/s
Fragmentgröße: 0 Byte
PMTU-Größe: 0 Byte
VPN-Verbindungen: 1; CRL-Status: CRL-Funktionalität abgeschaltet
VoIP Call Manager
Firewall: 5/12/2006 8:19:42 intruder detection - Paket verworfen
System-Informationen
Standortverifikation: Erfolgreich

LANCOM Referenzhandbuch Teil 6

- Backup-Lösungen
- Bürokommunikation mit LANCAPI
- Weitere Dienste

Stand: LCOS 7.6 (letztes Update Februar 2009)

LANCOM
Systems

© 2009 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®, Windows Vista™, Windows NT® und Microsoft® sind eingetragene Marken von Microsoft, Corp.

Das LANCOM Systems-Logo, LCOS und die Bezeichnung LANCOM sind eingetragene Marken der LANCOM Systems GmbH. Alle übrigen verwendeten Namen und Bezeichnungen können Marken oder eingetragene Marken ihrer jeweiligen Eigentümer sein.

LANCOM Systems behält sich vor, die genannten Daten ohne Ankündigung zu ändern und übernimmt keine Gewähr für technische Ungenauigkeiten und/oder Auslassungen.

Produkte von LANCOM Systems enthalten Software, die vom „OpenSSL Project" für die Verwendung im „OpenSSL Toolkit" entwickelt wurde (http://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.

Produkte von LANCOM Systems enthalten Komponenten, die als Open Source Software im Quelltext verfügbar sind und speziellen Lizenzen sowie den Urheberrechten verschiedener Autoren unterliegen. Im Besonderen enthält die Firmware Komponenten, die der GNU General Public License, Version 2 (GPL) unterliegen. Die Lizenzvereinbarung mit dem Text der GPL ist auf der LANCOM CD im Produktverzeichnis zu finden. Auf Anfrage können die Quelltexte und alle Lizenzhinweise elektronisch vom FTP-Server der LANCOM Systems GmbH bezogen werden.

Die Firmware des LANCOM VP-100 enthält Komponenten, die als Open Source Software im Quelltext verfügbar sind und speziellen Lizenzen sowie den Urheberrechten verschiedener Autoren unterliegen. Im Besonderen enthält die Firmware Komponenten, die der GNU General Public License, Version 2 (GPL) unterliegen. Die Lizenzvereinbarung mit dem Text der GPL ist auf der LANCOM CD im Produktverzeichnis als LC-VP100-License-DE.txt zu finden. Auf Anfrage können die Quelltexte und alle Lizenzhinweise elektronisch vom FTP-Server der LANCOM Systems GmbH bezogen werden.

LANCOM Systems GmbH

Adenauerstr. 20/B2

52146 Würselen

Deutschland

www.lancom.de

Würselen, Februar 2009

110655/0209

Inhalt

14 Backup-Lösungen 14 -1

14.1 Hochverfügbarkeit von Netzwerken 14 - 1
14.1.1 Wie wird die Störung einer Netzwerkverbindung erkannt? 14 - 1
14.1.2 Hochverfügbarkeit der Leitungen – die Backup-Verbindung 14 - 3
14.1.3 Hochverfügbarkeit der Gateways – redundante Gateways mit VPN Load Balancing 14 - 5
14.1.4 Hochverfügbarkeit des Internetzugangs – Multi-PPPoE 14 - 5
14.1.5 Anwendungsbeispiele 14 - 6

14.2 Backup-Lösungen und Load-Balancing mit VRRP 14 - 8
14.2.1 Einleitung 14 - 8
14.2.2 Das Virtual Router Redundancy Protocol 14 - 8
14.2.3 Anwendungsszenarien 14 - 13
14.2.4 Zusammenspiel mit internen Diensten 14 - 14
14.2.5 VRRP im WAN 14 - 18
14.2.6 Konfiguration 14 - 18
14.2.7 Statusinformationen 14 - 20

15 Bürokommunikation mit LANCAPI 15 -1

15.1 Welche Vorteile bietet die LANCAPI ? 15 - 1

15.2 Das Client-Server-Prinzip 15 - 1
15.2.1 Konfiguration des LANCAPI-Servers 15 - 1
15.2.2 Installation des LANCAPI-Clients 15 - 3
15.2.3 Konfiguration des LANCAPI-Clients 15 - 3

15.3 So setzen Sie die LANCAPI ein 15 - 4

15.4 Das LANCOM CAPI Faxmodem 15 - 4

15.5 LANCOM Faxmodem-Option 15 - 4

15.6 Unterstützte B-Kanal-Protokolle 15 - 4

16 Weitere Dienste 16 -1

16.1 Automatische IP-Adressverwaltung mit DHCP 16 - 1
16.1.1 Einleitung 16 - 1
16.1.2 Konfiguration der DHCP-Parameter mit LANconfig 16 - 2
16.1.3 Konfiguration der DHCP-Parameter mit Telnet oder WEBconfig 16 - 5
16.1.4 DHCP-Relay-Server 16 - 9
16.1.5 Konfiguration der Stationen 16 - 9
16.1.6 IP-Adressen im LAN überprüfen 16 - 9

16.2 Vendor-Class- und User-Class-Identifier im DHCP-Client 16 - 10

16.3 DNS 16 - 10
16.3.1 Was macht ein DNS-Server? 16 - 10
16.3.2 DNS-Forwarding 16 - 11
16.3.3 So stellen Sie den DNS-Server ein 16 - 12
16.3.4 URL-Blocking 16 - 13
16.3.5 Dynamic DNS 16 - 14

16.4 Accounting 16 - 15

16.5 Gebührenmanagement 16 - 16
16.5.1 Verbindungs-Begrenzung für DSL und Kabelmodem 16 - 16
16.5.2 Gebührenabhängige ISDN-Verbindungsbegrenzung 16 - 17
16.5.3 Zeitabhängige ISDN-Verbindungsbegrenzung 16 - 17
16.5.4 Einstellungen im Gebührenmodul 16 - 18

16.6 Zeit-Server für das lokale Netz 16 - 18
16.6.1 Konfiguration des Zeit-Servers unter LANconfig 16 - 18
16.6.2 Konfiguration des Zeit-Servers mit WEBconfig oder Telnet 16 - 19
16.6.3 Konfiguration der NTP-Clients 16 - 19
16.6.4 Fehlererkennung und Protokollierung der WLAN-Aktivitäten 16 - 19

16.7 Scheduled Events 16 - 21
16.7.1 Zeitautomatik für LCOS-Befehle 16 - 21
16.7.2 CRON-Jobs mit Zeitverzögerung 16 - 22
16.7.3 Konfiguration der Zeitautomatik 16 - 22

16.8 PPPoE-Server 16 - 23
16.8.1 Einleitung 16 - 23
16.8.2 Anwendungsbeispiel 16 - 24
16.8.3 Konfiguration 16 - 25

16.9 Remote-Bridge 16 - 26

16.10 RADIUS 16 - 27
16.10.1 Funktionsweise von RADIUS 16 - 28
16.10.2 Konfiguration von RADIUS als Authenticator bzw. NAS 16 - 28
16.10.3 Konfiguration von RADIUS als Server 16 - 33

16.11 Erweiterungen im RADIUS-Server 16 - 34
16.11.1 Neue Authentifizierungs-Verfahren 16 - 34
16.11.2 EAP-Authentifizierung 16 - 35
16.11.3 RADIUS-Forwarding 16 - 35
16.11.4 Parameter des RADIUS-Servers 16 - 36

16.12 RADSEC 16 - 37
16.12.1 Konfiguration von RADSEC für den Client 16 - 37
16.12.2 Zertifikate für RADSEC 16 - 38

16.13 Betrieb von Druckern am USB-Anschluss des LANCOM 16 - 38
16.13.1 Konfiguration des Printservers im LANCOM 16 - 38
16.13.2 Konfiguration der Drucker auf dem Rechner 16 - 39

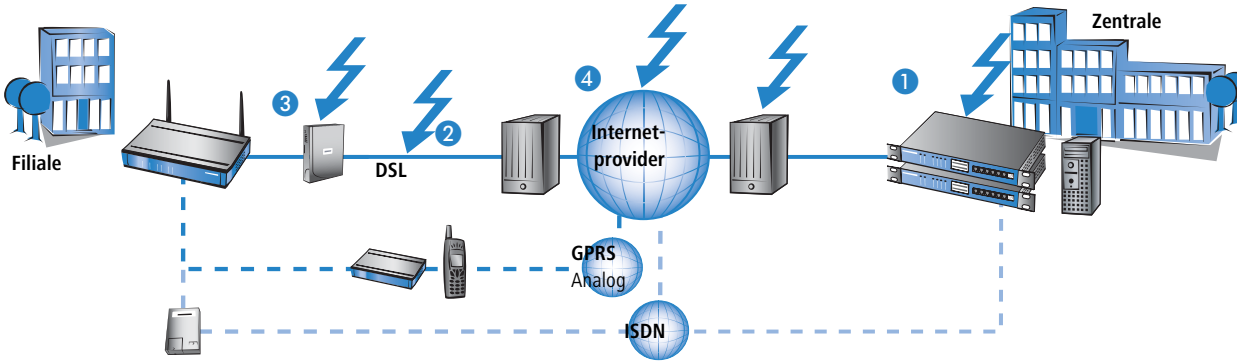
14 Backup-Lösungen

14.1 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 immer mehr 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-Leitungen noch ihren Dienst versehen.
- Das Netzwerk des Providers (4) kann gestört sein oder ausfallen.



Internet Router und Access Points von LANCOM bieten eine Reihe von Sicherheits- und Backup-Funktionen, mit denen Sie Ihr Netz vor den Folgen dieser Störungen schützen können.

14.1.1 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).

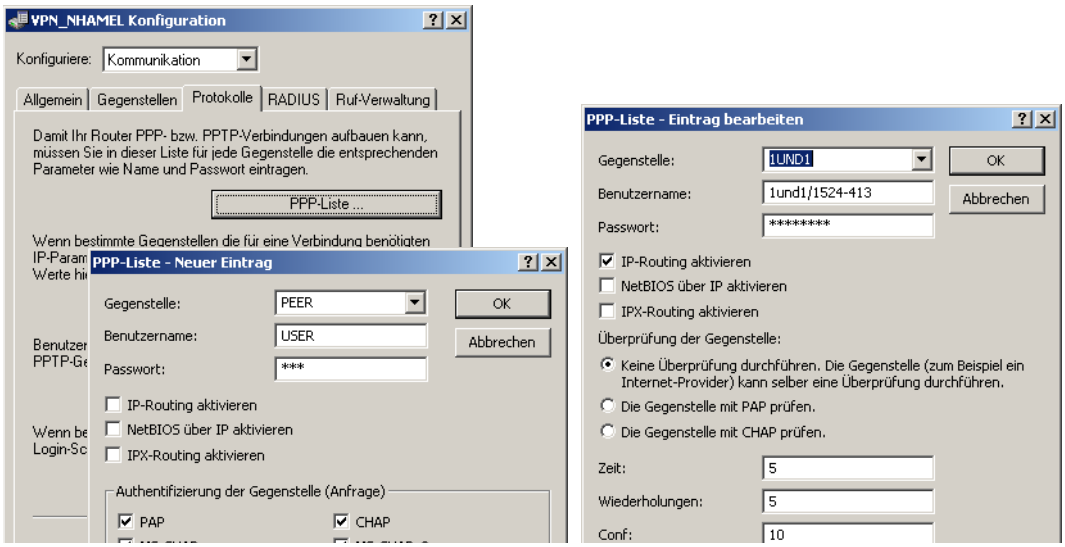
PPP LCP Echo Monitoring

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 werdend dabei 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 Interval 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.



LANconfig: Kommunikation ▶ Protokolle ▶ PPP-Liste

WEBconfig: LCOS-Menübaum ▶ Setup ▶ WAN ▶ PPP

ICMP Polling

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-Interval 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.

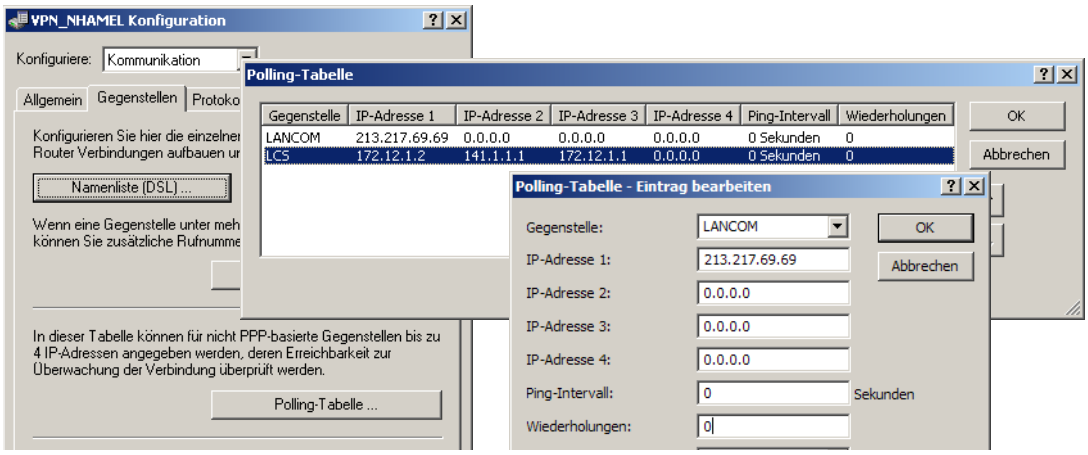
Zu jeder Gegenstelle können dabei bis zu vier verschiedene IP-Adressen eingetragen werden, die parallel im entfernten Netz geprüft werden. Nur wenn alle eingetragenen IP-Adressen nicht erreichbar sind, gilt die Leitung als gestört.

Mit dem ICMP-Polling kann eine komplette Verbindung von Ende zu Ende überwacht werden.

- **Name der Gegenstelle**
- **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.



LANconfig: Kommunikation ▶ Gegenstellen ▶ Polling-Tabelle

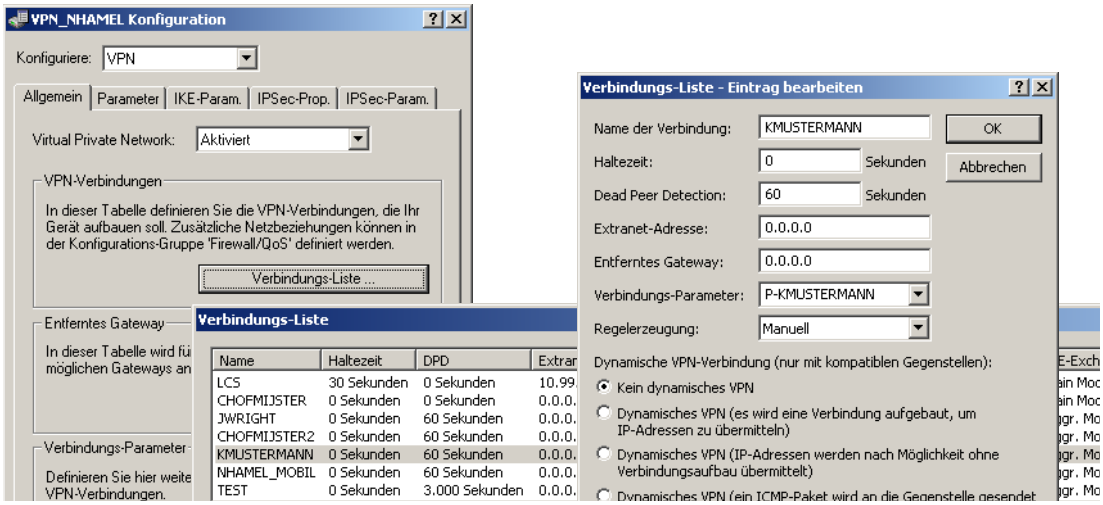
WEBconfig: LCOS-Menübaum ▶ Setup ▶ WAN ▶ Polling-Tabelle

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 wiederherstellen der VPN-Verbindung eine erneute Anmeldung mit der gleichen Identity. Für VPN-Clients wird die DPD-Zeit üblicherweise auf 60 Sekunden eingestellt.



LANconfig: VPN ▶ Allgemein ▶ Verbindungs-Liste

WEBconfig: LCOS-Menübaum ▶ Setup ▶ VPN ▶ Namen-Liste

14.1.2 Hochverfügbarkeit der Leitungen – die Backup-Verbindung

Wenn eine Verbindung zum Internet-Provider oder zu einem entfernten Netzwerk gestört ist, 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:

- ISDN-Leitung als Backup für einen DSL-Internetzugang
- ISDN-Leitung als Backup für eine VPN-Netzwerkkopplung

- Modem-Verbindung (GSM oder analog) als Backup für DSL- oder ISDN-Leitungen und VPN-Verbindungen

Konfiguration der Backup-Verbindung

Zur Definition einer Backup-Verbindung sind im Prinzip die folgenden Konfigurationsschritte notwendig:

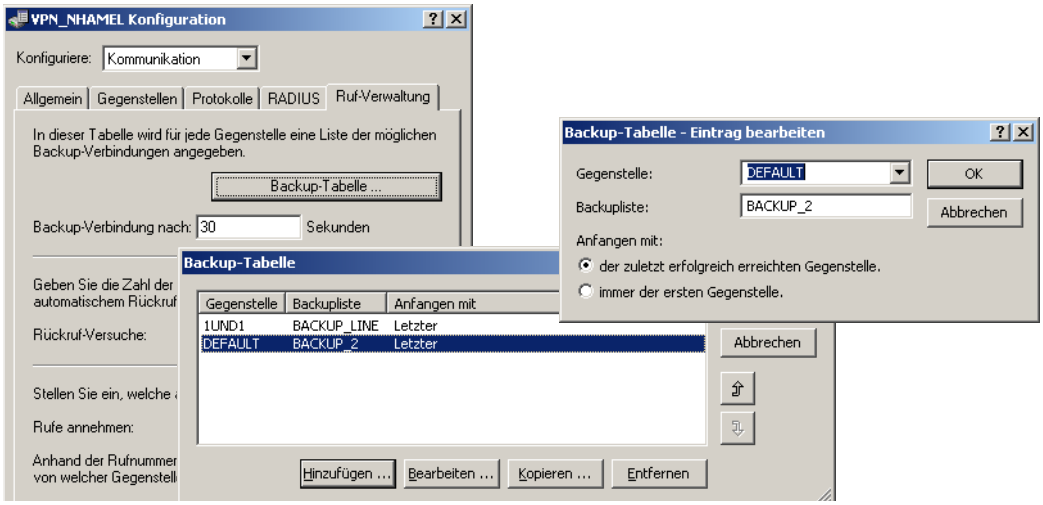
① Für die Backup-Verbindung wird auf der entsprechenden WAN-Schnittstelle die Gegenstelle so eingerichtet, dass sie über diesen alternativen Weg erreichbar ist. Soll z.B. die ISDN-Leitung als Backup-Verbindung dienen, wird die Gegenstelle als ISDN-Gegenstelle angelegt (mit den zugehörigen Einträgen bei den Kommunikations-Layern und in der PPP-Liste).

② Ggf. 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 Bedarfsfalle zuerst aufgebaut werden soll:

- Die zuletzt erfolgreich erreichte Gegenstelle
- Immer die erste Gegenstelle in der Liste



LANconfig: LANconfig: VPN ▶ Ruf-Verwaltung ▶ Backup-Tabelle

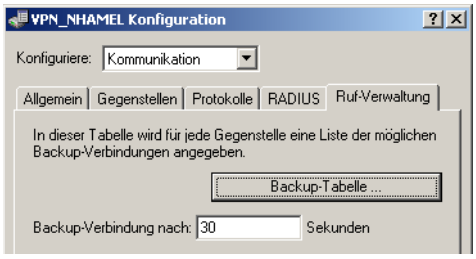
WEBconfig: LCOS-Menübaum ▶ Setup ▶ WAN ▶ Backup-Tabelle

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' auf der Registerkarte 'Ruf-Verwaltung' eingetragen oder alternativ unter telnet unter `/Setup/WAN/Backup-St.-Sekunden`.



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, 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.

14.1.3 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.

Weitere Informationen zu redundanten Gateways und zum „Load Balancing" finden Sie unter 'VPN-Verbindungen: hohe Verfügbarkeit mit „Lastenausgleich"' → Seite 10-64.

14.1.4 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).

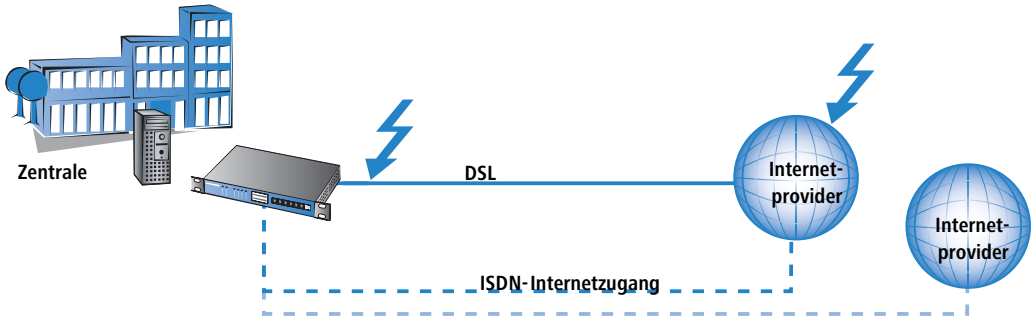
Zur Definition dieser Backup-Lösungen als alternative Internetzugänge richten Sie in Ihrem Gerät z.B. über die Setup-Assistenten nacheinander zwei Internet-Zugänge ein. Der Internet-Zugang, der im Normalfall verwendet werden soll, wird dabei als letzter konfiguriert. Dadurch werden die Einträge in der 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.

Weitere Informationen zur Definition mehrerer PPPoE-Verbindungen finden Sie unter 'Multi-PPPoE' → Seite 7-23.

14.1.5 Anwendungsbeispiele

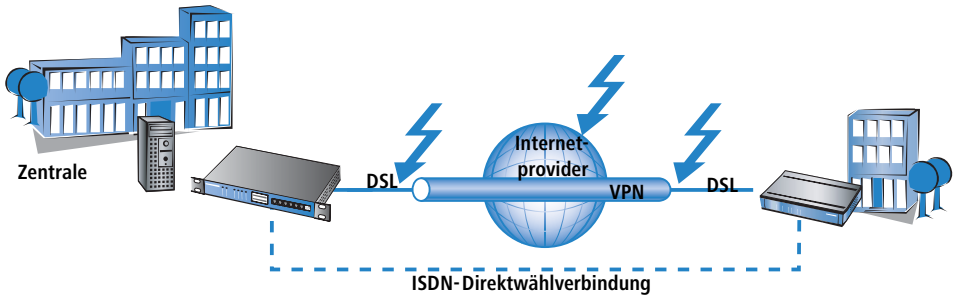
DSL- Internetzugang mit ISDN- Internetzugang absichern



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.

Dynamic- VPN- Netzwerkkopplung mit ISDN- Direktwählverbindung absichern



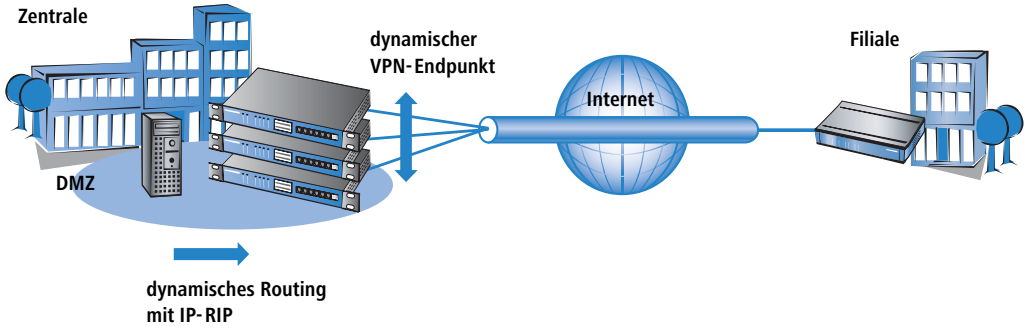
Bei der Anbindung einer Filiale über eine VPN-Verbindung an die Zentrale kann es sinnvoll sein, die internetbasierte VPN-Verbindung durch eine direkte ISDN-Wählverbindung abzusichern. Falls die Internetverbindung bei einem der beiden Router ausfällt, kann die Datenübertragung über die ISDN- Kopplung 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.

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.

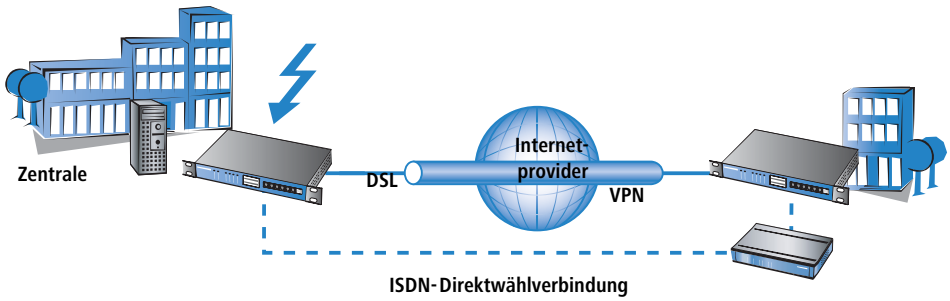
Mit der Möglichkeit, mehrere „Remote- Gateway"- Adressen als „dynamischer VPN- Endpunkt" für eine VPN- Verbindung zu konfigurieren, bieten LANCOM VPN- Gateways eine hohe Verfügbarkeit durch den Einsatz redundanter Geräte. Dabei werden in der Zentrale mehrere Gateways mit gleicher VPN- Konfiguration eingesetzt. 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").

Weitere Informationen zu redundanten Gateways und zum „VPN Load Balancing" finden Sie unter 'VPN- Verbindungen: hohe Verfügbarkeit mit „Lastenausgleich"' → Seite 10- 64.

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

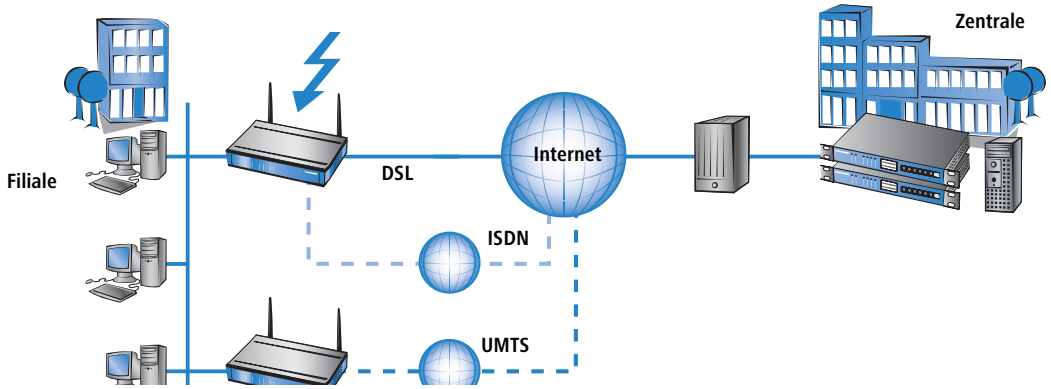
im ISDN-Router eingetragene Route automatisch die „bessere" Lösung, alle Datenpakete werden nun über die ISDN-Strecke geführt. Sobald die VPN-Verbindung wieder hergestellt ist, ändert sich die Distanz wieder auf einen Wert unterhalb der ISDN-Verbindung, der Backup-Fall endet wie gewünscht.

14.2 Backup-Lösungen und Load-Balancing mit VRRP

14.2.1 Einleitung

Die hohe Verfügbarkeit von Datenverbindungen stellen vor allem im geschäftlichen Umfeld eine unverzichtbare Anforderung an die eingesetzten Netzwerkkomponenten dar. Die Geräte von LANCOM Systems stellen verschiedenen Mechanismen zur Sicherung der Datenübertragung als Backup-Lösungen bereit:

- Die verschiedenen WAN-Schnittstellen (DSL, ISDN, UMTS) 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 mehrere Router installiert, die sich beim Ausfall eines Gerätes gegenseitig vertreten können.
- Zusätzlich zum normalen VRRP kann bei LANCOM-Geräten das Auslösen des Backup-Falls an die Verfügbarkeit einer Datenverbindung geknüpft werden. Mit dieser Zusatzfunktion können LANCOM-Geräte mit mehreren WAN-Interfaces (z.B. DSL- und ISDN-Interface) sehr flexibel in Backuplösungen eingesetzt werden. Der Backup-Fall wird dabei z.B. dann ausgelöst, wenn die Default-Route über das DSL-Interface nicht mehr erreichbar ist. Das ISDN-Interface des Gerätes kann aber einen weiteren Platz in der Backup-Kette einnehmen, wenn auch der Backup-Router gestört ist ('Backup-Ketten' → Seite 14-12).



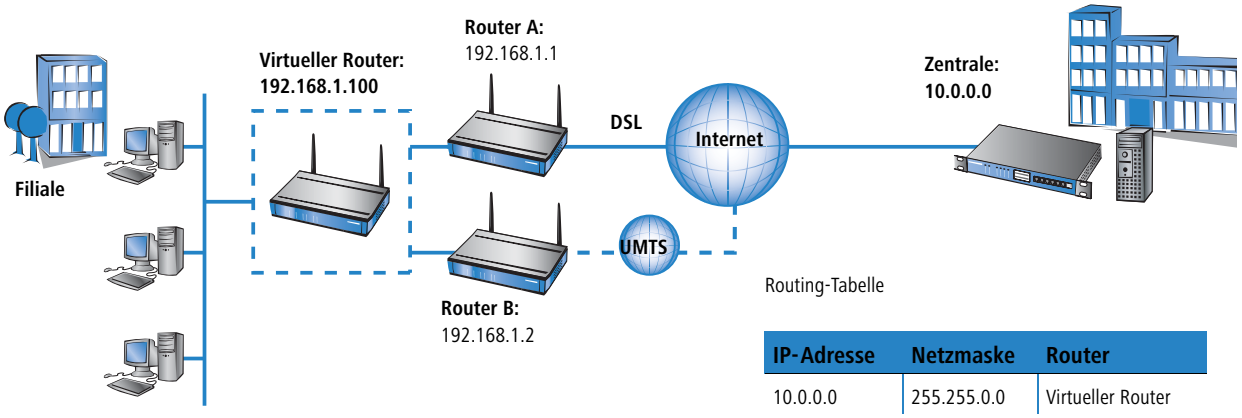
14.2.2 Das Virtual Router Redundancy Protocol

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.

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.

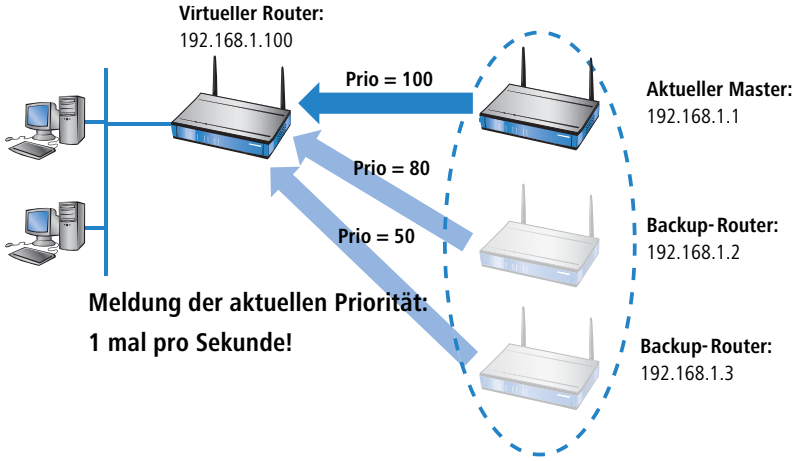
Geräte-, Leitungs- oder Gegenstellen-Backup

Die Möglichkeit, dass sich ein Gerät selbst aus dem VRRP-Verbund abmelden kann deutet schon drauf hin, dass sich die Möglichkeiten von VRRP nicht nur auf den kompletten Ausfall eines Gerätes beziehen kann.

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, ISDN oder UMTS) 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.

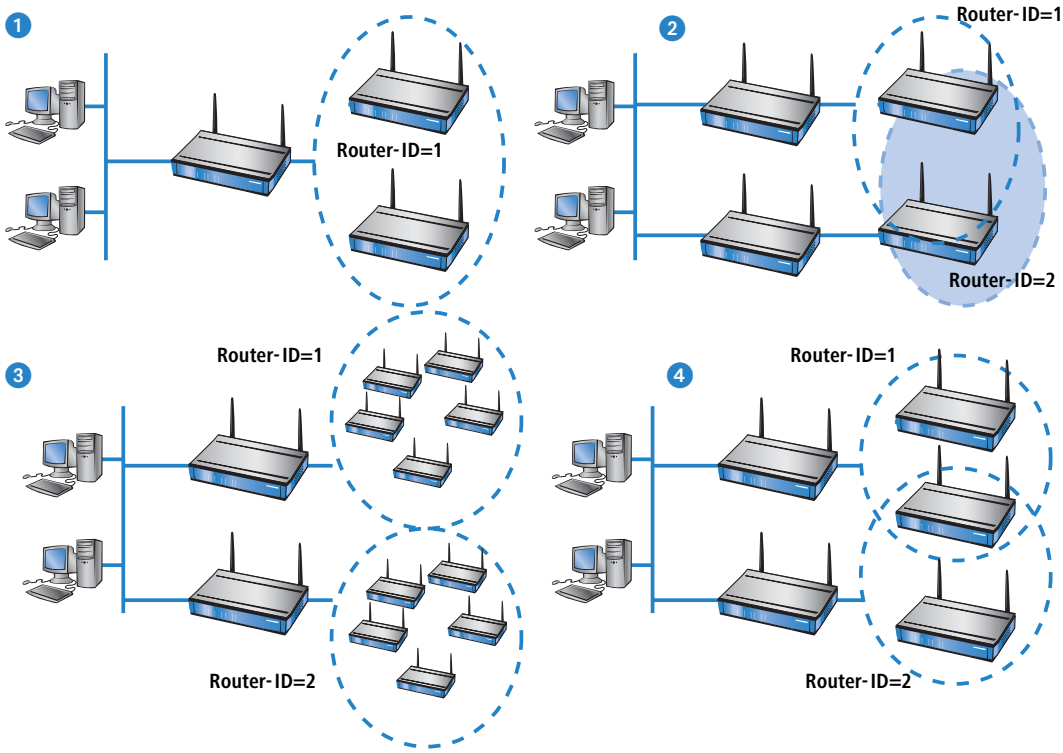
- Die Router-ID kann einen Wert zwischen 1 und 255 annehmen. Aus der Router-ID ergibt sich auch die virtuelle MAC-Adresse des Routers zu 00:00:5E:00:01:Router-ID. Die Router-ID 0 ist unzulässig.
- Die IP-Adresse des virtuellen Router ist frei wählbar, sie muss sich natürlich innerhalb des lokalen Netzes 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 254 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.



Router-ID definiert „Standby-Gruppen"

Mit der bei der Definition eines virtuellen Routers festgelegten Router-ID können die physikalischen Router den virtuellen Router 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 mehrere Router **eine** Standby-Gruppe. In beiden 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.



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 LANCOM-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 LANCOM-Geräte und den Aufbau von Backup-Ketten zu ermöglichen, werden jedem virtuellen LANCOM-Router zwei Prioritäten zugeordnet: eine Haupt- und eine Backup-Priorität.

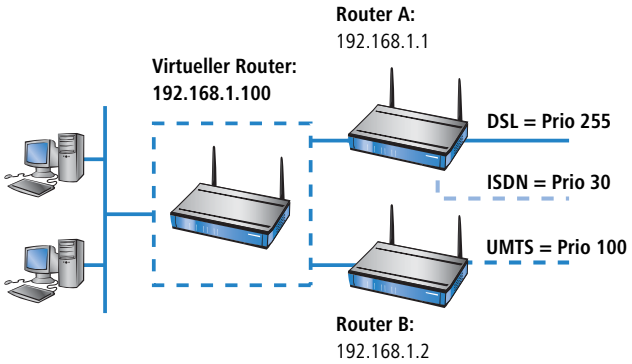
- Die Haupt-Priorität wird verwendet (ins Netzwerk propagiert), solange sich das Gerät im normalen Betriebszustand befindet (also die Gegenstelle der Hauptverbindung noch erreichbar ist).
- Die Backup-Priorität wird propagiert, wenn sich das Gerät im Backup-Zustand befindet (d.h. das Backup-Delay ist 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 ('Backup-Ketten' → Seite 14-12).

Die Zuordnung der Prioritäten zu den verschiedenen WAN-Interfaces der Geräte ergibt sich aus Konfiguration der Backup-Verbindungen in der Backup-Tabelle (unter LANconfig im Konfigurationsbereich 'Kommunikation' auf der Registerkarte 'Ruf-Verwaltung').

- 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.

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.

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.

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.

14.2.3 Anwendungsszenarien

VRRP wird üblicherweise in zwei verschiedenen Anwendungenfällen eingesetzt:

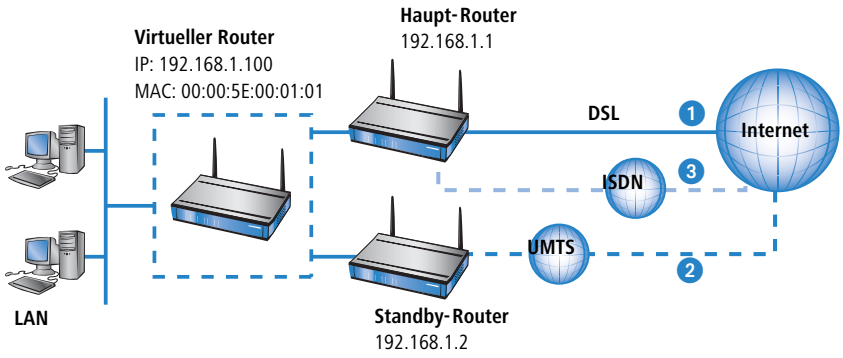
- Im einfachen Backup-Fall mit zwei Routern stellt ein Gerät im normalen Betrieb die Verbindung ins Internet her. Das zweite Gerät wird nur als „Standby-Gerät" im Wartezustand betrieben und übernimmt die Aufgabe des Haupt-Routers, wenn dieser ausfällt.
- Im zweiten Fall arbeiten zwei oder mehrere Geräte 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.

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.

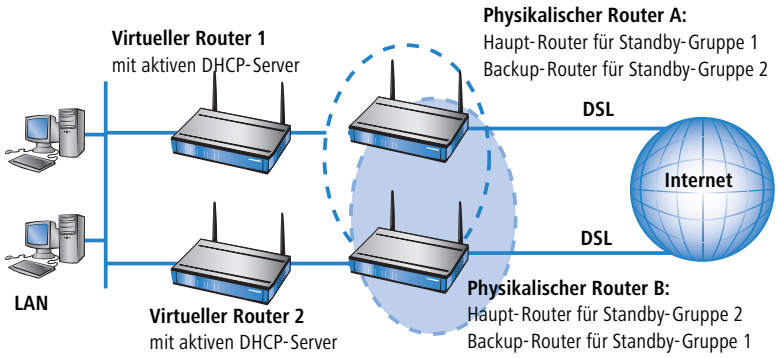
Da fast alle LANCOM-Geräte mit DSL-Interface gleichzeitig auch ein ISDN-Interface haben, kann der Haupt-Router auch das ISDN-Backup am Ende der Backup-Kette übernehmen – solange kein vollständiger Ausfall der Hardware vorliegt.



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 (siehe auch 'Adresszuweisung über DHCP mit mehreren DHCP-Servern im LAN' → Seite 14-9). 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.



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
	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

14.2.4 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.

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 das LANCOM 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 das LANCOM 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 das LANCOM 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.

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 das LANCOM nur antworten, wen es 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 das LANCOM 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 LANCOM 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.

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 ('Load-Balancing' → Seite 14-13) 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

LANCOM A definiert folgende virtuellen Router:

Router-ID	virt.-Address	Prio	B-Prio	Peer
1	10.0.0.1	100	50	INTERNET
2	10.0.0.2	60	50	INTERNET

und LANCOM B entsprechend:

Router-ID	virt.-Address	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 LANCOM A oder LANCOM B entscheidet, als Gateway die 10.0.0.1 bzw. die 10.0.0.2 zugewiesen und somit zunächst auf beide LANCOM verteilt.

An diesem Beispiel wird auch deutlich, wie das Load-Balancing mit dem Backup verknüpft werden kann: Fällt LANCOM A in den Backup-Fall, so wird LANCOM B für alle Clients zum Master. Sollte nun noch LANCOM B ausfallen, so wird LANCOM 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 LANCOM zur Verfügung stellt, wie z.B. DNS- und NBNS-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 und NBNS eine Sonderbehandlung geben muss.

DNS-Server

Da der RFC es verbietet, dass ein virtueller Router zusätzliche Dienste anbietet, wenn der physikalische Router nicht „Besitzer" der virtuellen IP-Adresse ist, bedarf es einer Sonderbehandlung für den DNS-Server des LANCOM. Das LANCOM 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 LANCOM 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 LANCOM 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 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 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 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.

NBNS/NetBIOS-Proxy

Da ein NetBIOS-Proxy keine Pakete weiterleitet, ist die Frage nach den angesprochenen virtuellen oder physikalischen Adressen hier nicht von Bedeutung. Wichtig ist allerdings, dass alle Router und Backup-Router im VRRP-Verbund die gleichen von der remoten Seite gelernten Host-, Gruppen- und Serveradressen in der eigenen Datenbank speichern und beim Verbindungsaufbau propagieren können. Nur so ist gewährleistet, dass eine NBNS-Anfrage in jedem Fall beantwortet werden kann.

Da der NetBIOS-Proxy beim Verbindungsaufbau alle von der remoten Seite gelernten Host-, Gruppen- und Serveradressen propagiert, muss nur dafür gesorgt werden, dass diese Informationen auch von den Backup-Routern in ihre Datenbank aufgenommen werden. Im Normalfall wird genau dies jedoch durch die Routenprüfung verhindert.

Da die Übernahme der Adressen normalerweise durch die Routenprüfung verhindert wird, werden im VRRP-Betrieb die Adressen nur dann angenommen, wenn **alle** der folgenden Bedingungen erfüllt sind:

- Es besteht eine WAN-Route zur propagierten Adresse.
- Die zugehörige Gegenstelle ist mit einem virtuellen Router verbunden.
- Die jeweilige Adresse wird vom Master dieses virtuellen Routers propagiert.
- Der Schalter 'Internal-Services' ist aktiviert.

Nur wenn alle Bedingungen erfüllt sind wird die jeweilige Adresse in die Datenbank übernommen. Hierdurch wird sichergestellt, dass die Datenbanken der einzelnen Router in sich konsistent bleiben und alle Adressen sofort bekannt sind, wenn ein Backup-Router zum Master wird.

Auch auf den NetBIOS-Proxy wirkt sich die Stellung der Schalters 'Internal-Services' aus.

- Wenn er aktiviert ist, akzeptiert der NetBIOS-Proxy NBNS-Anfragen, die an virtuelle Router gestellt werden.
- Ist zudem ein virtueller Router mit der Default-Route verbunden, so wird dieser vom DHCP-Server des LANCOM als NBNS-Server zugewiesen.
- Sind mehrere virtuelle Router mit der Default-Route verbunden so wird derjenige mit der höchsten Priorität zugewiesen (wie bei den Gateway-Adressen).

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 bekannten virtuellen Router propagiert werden.
- Wenn das LANCOM 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

NTP

Wenn der Schalter 'Internal- Services' aktiviert ist, dann akzeptiert das LANCOM auch (S)NTP- Anfragen, die an virtuelle Router gestellt werden, da die genaue Adresse der Zeit- Quelle für einen NTP- Client unerheblich ist.

Weitere Dienste

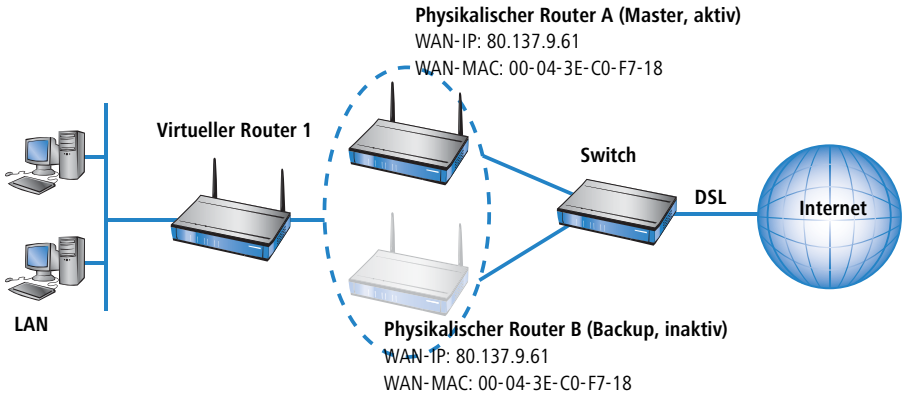
Alle anderen Dienste bearbeitet das LANCOM nur, wenn es unter seiner physikalischen Adresse angesprochen wurde.

14.2.5 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 RIP o.ä. Um trotzdem auch mit VRRP eine WAN- seitige Ausfallsicherung zu ermöglichen, sieht das VRRP im LANCOM zwei Möglichkeiten vor.

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 das LANCOM 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.

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 vor dem Verbindungsabbau noch alle Netze als nicht mehr erreichbar ins WAN und sorgt so für eine schnelle Änderung der Routing- Prioritäten.

14.2.6 Konfiguration

Zur Konfiguration von Ausfallsicherung oder Load- Balancing über VRRP können folgende Parameter eingestellt werden:

- **Aktivierung**: Mit dem Schalter 'VRRP aktiviert' lässt sich das VRRP- Modul ein- und ausschalten (Default = aus).
- **VRRP- Liste**: In der VRRP- Liste können bis zu 16 virtuelle Router definiert werden. Diese Tabelle hat die folgenden Felder:
  - □ **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 ('Router- ID definiert „Standby- Gruppen"' → Seite 14-10).
  - □ **Router- IP**: IP- Adresse des virtuellen Routers.

Alle Router auf denen der virtuelle Router eingerichtet ist, müssen diesem die gleiche IP-Adresse zuweisen.

- **Haupt-Priorität**: Die Haupt-Priorität des virtuellen Routers bezieht sich bei Routern mit mehreren Interfaces auf das Haupt-Interface, also z.B. bei Routern mit DSL- und ISDN-Unterstützung auf das DSL-Interface. Es sind Werte zwischen 0 und 255 zulässig. Dabei haben die Werte 0 und 255 eine Sonderbedeutung:

  '0' schaltet den virtuellen Router aus.

  '255' wird nur akzeptiert, 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 ISDN-Unterstützung auf das ISDN-Interface. Es sind wiederum Werte zwischen 0 und 255 zulässig. Auch hier haben die Werte 0 und 255 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.

  255 wird nur akzeptiert, 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

Wenn im Backup-Fall auch die Backup-Verbindung nicht aufgebaut werden kann meldet sich der virtuelle Router vollständig ab und versucht ebenfalls in, über das Reconnect-Delay angegebenen, Intervallen entweder die Haupt- oder die Backup-Verbindung erneut aufzubauen.

- **Gegenstelle**: Name der Gegenstelle, die das Verhalten des virtuellen Routers steuert. Die Gegenstelle kann auch weiteren virtuellen Routern zugeordnet werden.

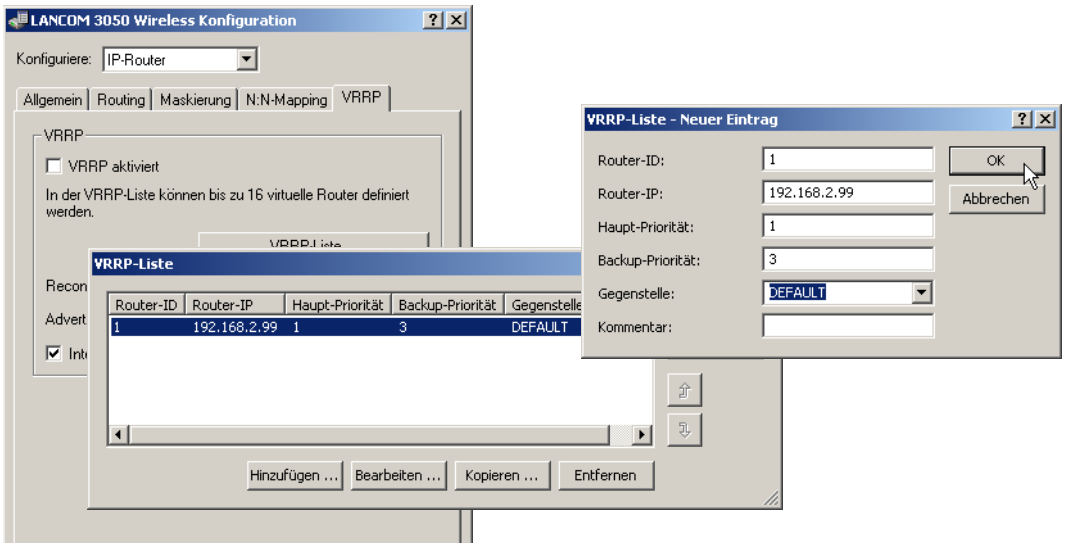
Die Angabe der Gegenstelle ist optional. Mit der Bindung der Backup-Bedingung an eine Gegenstelle wird die LANCOM-spezifische Erweiterung von VRRP genutzt, nicht nur den Ausfall eines Gerätes (VRRP-Standard), sondern zusätzlich auch die Störung eines Interfaces oder einer Gegenstelle abzusichern.

- **Kommentar**: 64 Zeichen langer Kommentar zur Beschreibung des virtuellen Routers.

- **Reconnect-Delay-Zeit**: Die Reconnect-Delay-Zeit gibt an, nach wie vielen Minuten ein abgemelder 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.
- **Advert.-Intervall**: Das Advertising-Intervall gibt an nach wie vielen Sekunden ein virtueller Router neu propagiert wird. Der Defaultwert beträgt 1 Sekunde.

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.

- **Internal-Services**: Der Schalter Internal-Services steuert, wie sich das Gerät verhalten soll, wenn es unter der Adresse eines virtuellen Routers angesprochen wird.
  - In der Stellung 'An' reagiert das LANCOM bei bestimmten Diensten genau so, als wäre es unter seiner realen Adresse angesprochen worden. Dies geschieht natürlich nur, wenn das Gerät auch selbst der Master des virtuellen Routers ist. Gleichzeitig Ändert sich das Verhalten des DHCP-Servers (‘Zusammenspiel mit internen Diensten’ → Seite 14-14).
  - Die Einstellung 'Aus' bewirkt RFC-konformes Verhalten, d.h. entsprechende Pakete werden stillschweigend verworfen.
  - Die Default-Einstellung ist 'An'.



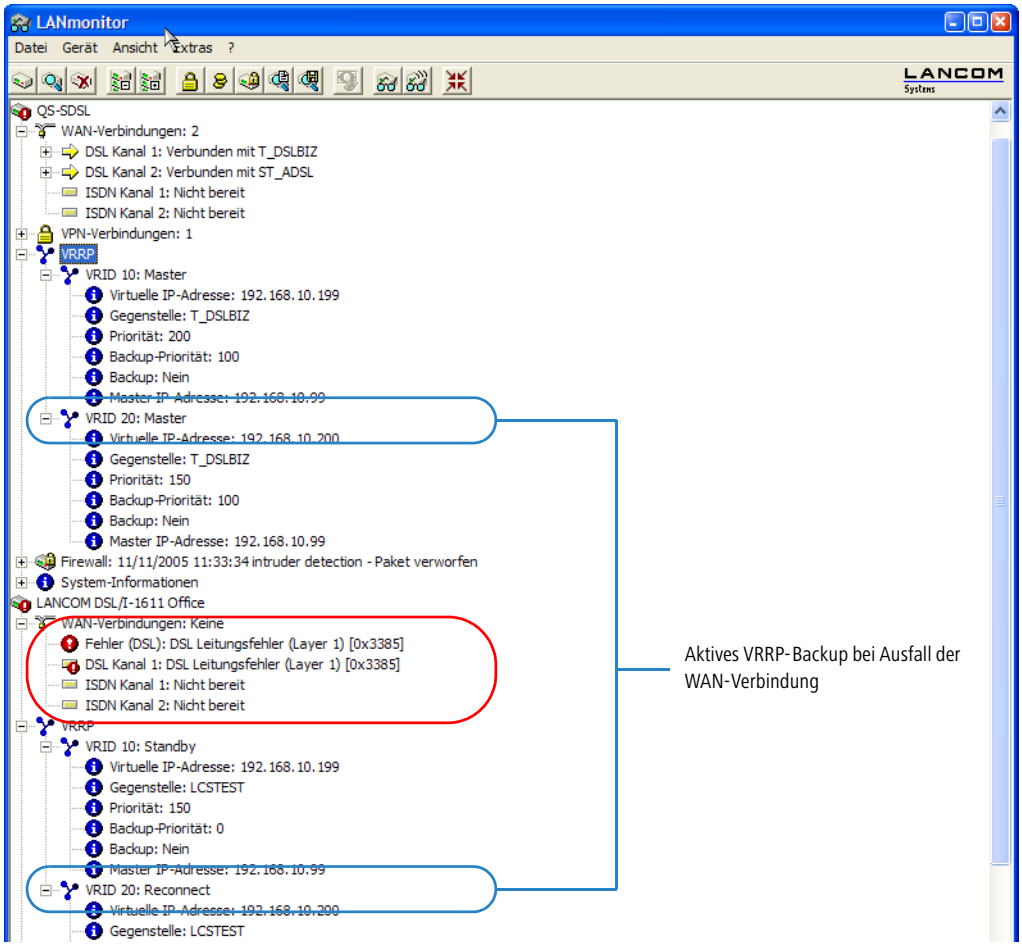
LANconfig: LANconfig: IP-Router ▶ VRRP

WEBconfig: LCOS-Menübaum ▶ Setup ▶ IP-Router ▶ VRRP

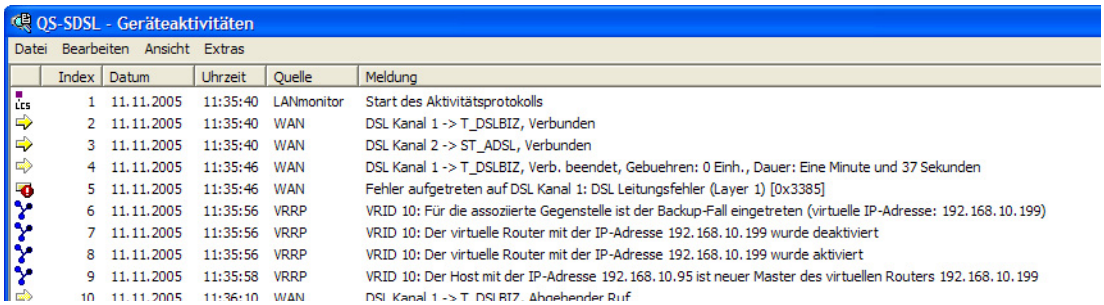
14.2.7 Statusinformationen

Statusabfrage über LANmonitor

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.



Statusabfrage über WEBconfig, Telnet oder SSH

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.

15 Bürokommunikation mit LANCAPI

Die Ausführungen dieses Abschnittes beziehen sich nur auf Geräte mit ISDN-Schnittstelle.

Die LANCAPI von LANCOM Systems ist eine spezielle Form der weit verbreiteten ISDN CAPI-Schnittstelle. CAPI steht für Common ISDN Application Programming Interface und stellt die Verbindung von ISDN-Adaptern zu Kommunikationsprogrammen her. Diese Programme wiederum stellen den Rechnern Funktionen der Bürokommunikation, wie z.B. ein Fax oder einen Anrufbeantworter, bereit.

15.1 Welche Vorteile bietet die LANCAPI ?

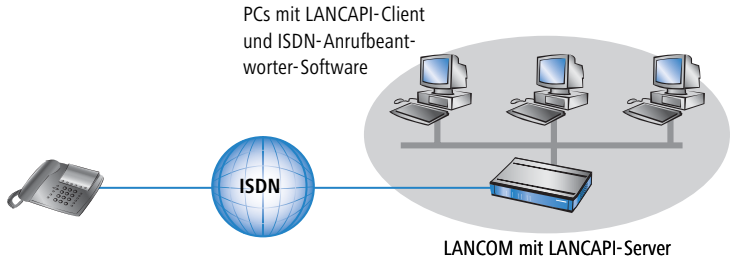
Der Einsatz der LANCAPI bringt vor allem wirtschaftliche Vorteile. Alle Windows-Arbeitsplätze, die im LAN integriert sind, erhalten über die LANCAPI uneingeschränkten Zugriff auf ISDN-Bürokommunikations-Funktionen wie Fax, Anrufbeantworter, Onlinebanking und Eurofiletransfer. Ohne zusätzliche Hardware an jedem einzelnen Arbeitsplatz werden alle ISDN-Funktionen über das Netzwerk bereitgestellt. Dadurch entfallen kostspielige Ausstattungen der Arbeitsplätze mit ISDN-Adaptern oder Modems. Lediglich die Software für die Bürokommunikation wird auf den einzelnen Arbeitsplätzen installiert.

Beim Versenden von Faxen wird z.B. am Arbeitsplatz ein Faxgerät simuliert. Mit der LANCAPI leitet der PC das Fax über das Netzwerk an einen Router weiter, welcher die Verbindung zum Empfänger herstellt.

Alle Anwendungen, die Sie über die LANCAPI betreiben, verwenden direkte ISDN-Verbindungen und laufen nicht über die Router-Funktion des Geräts. Daher werden Firewall- und Gebührenüberwachungsfunktionen in diesem Zusammenhang nicht berücksichtigt. Die LANCAPI ist ebenso unabhängig von allen Routing oder VPN-Funktionen (‘System-Design’ → Seite 1).

15.2 Das Client-Server-Prinzip

Die LANCAPI besteht aus zwei Komponenten, einem Server (im LANCOM) und einem Client (auf den PCs). Der LANCAPI-Client wird nur auf den Rechnern im lokalen Netz installiert, die die Funktionen der LANCAPI nutzen möchten.



15.2.1 Konfiguration des LANCAPI-Servers

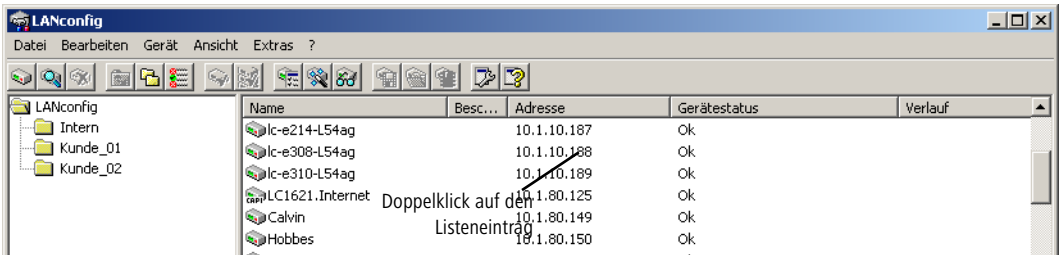
Bei der Konfiguration des LANCAPI-Servers im LANCOM werden im Prinzip zwei Fragen behandelt:

- Auf welche Rufnummer aus dem ISDN-Netz soll die LANCAPI reagieren?
- Welche der Rechner im lokalen Netz sollen über die LANCAPI Zugang zum Telefonnetz erhalten?

Die Konfiguration am Router erfolgt über die Konfigurationstabellen von LANconfig oder WEBconfig. In den folgenden beiden Abschnitten finden Sie Schritt-für-Schritt-Anleitung für jedes dieser Konfigurationsprogramme.

Anleitung für LANconfig

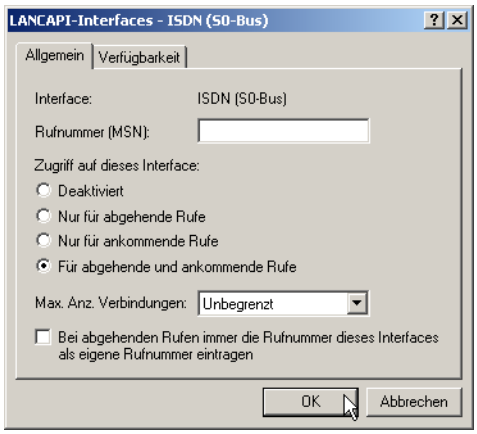
① Öffnen Sie die Konfiguration des Routers durch einen Doppelklick auf den Gerätenamen in der Liste und geben Sie auf Nachfrage Ihr Kennwort ein.



② Wählen Sie im Konfigurationsbereich 'LANCAPI' auf der Registerkarte 'Allgemein' bei den **LANCAPI-Interfaces** die ISDN-Schnittstelle aus.



③ Aktivieren Sie den LANCAPI-Server für abgehende und ankommende Rufe, oder lassen Sie nur abgehende Anrufe zu.



Wenn der LANCAPI-Server auch ankommende Rufe entgegen nehmen soll, so geben Sie im Feld 'Rufnummern (MSN/EAZ)' alle eigenen ISDN-Rufnummern an, auf denen die LANCAPI Anrufe entgegennehmen soll. Mehrere Rufnummern werden voneinander durch Semikola getrennt. Wenn Sie hier keine Rufnummer eingeben, nimmt die LANCAPI Anrufe an allen eigenen ISDN-Rufnummern entgegen.

Anleitung für WEBconfig

① Wählen Sie im Hauptmenü die **LCOS-Menübaum**.

② Wählen Sie in den folgenden Menüs **Setup** ▶ **LANCAPI** ▶ **Interface-Tabelle**.

③ Wählen Sie in der **Interface-Tabelle** den (einzigen) Eintrag **S0-1**.

④ Aktivieren Sie den LANCAPI-Server für abgehende und ankommende Rufe ('Ein'), oder lassen Sie nur abgehende Anrufe zu ('Abgehend').



Wenn der LANCAPI-Server auch ankommende Rufe entgegen nehmen soll, so geben Sie im Feld 'EAZ/MSNs' alle eigenen ISDN-Rufnummern an, auf denen die LANCAPI Anrufe entgegennehmen soll. Mehrere Rufnummern werden voneinander durch Semikola getrennt. Wenn Sie hier keine Rufnummer eingeben, nimmt die LANCAPI Anrufe an allen eigenen ISDN-Rufnummern entgegen. Bestätigen Sie Ihre Angaben mit **Setzen**.

15.2.2 Installation des LANCAPI-Clients

Für die Installation des LANCAPI-Clients auf einem System unter Windows XP oder Windows 2000 benötigen Sie Administrator-Rechte.

① Legen Sie an einem Client-PC die LANCOM-CD in Ihr CD-ROM-Laufwerk ein. Wenn das Setup-Programm beim Einlegen der CD nicht automatisch startet, klicken Sie im Explorer von Windows einfach auf die 'autorun.exe' im Hauptverzeichnis der LANCOM-CD.

② Wählen Sie den Eintrag **LANCOM Systems Software installieren**.

③ Markieren Sie die Option **LANCAPI**. Klicken Sie auf **Weiter**, und folgen Sie den Hinweisen der Installationsroutine. Zum Abschluss wird (sofern erforderlich) ein Neustart des Rechners durchgeführt.

Der LANCAPI-Client startet von nun an automatisch. Seinen Status zeigt das zusätzliche Icon in der Windows-Taskleiste (neben der Uhr) an.



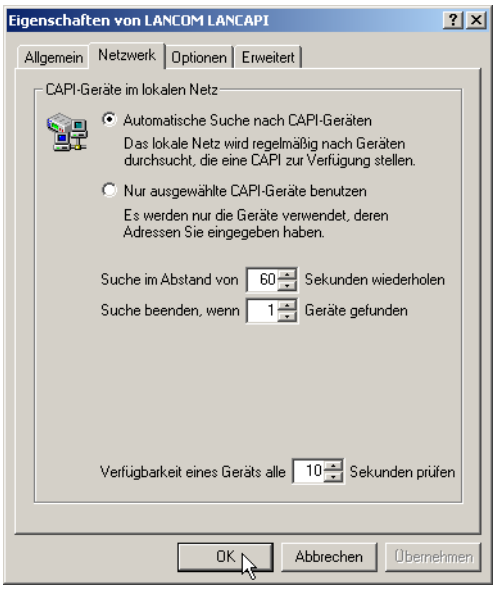
15.2.3 Konfiguration des LANCAPI-Clients

Bei der Einstellung der PC-Clients für die LANCAPI legen Sie fest, welche LANCAPI-Server verwendet werden sollen und wie diese überprüft werden. Wenn Sie nur einen LANCOM in Ihrem LAN als LANCAPI-Server betreiben, können Sie im Prinzip alle Parameter in den Voreinstellungen belassen.

① Starten Sie den LANCAPI-Client aus der Programmgruppe 'LANCOM Systems'. Auf der Registerkarte 'Allgemein' finden Sie Informationen zum Treiber des bereitgestellten Dienstes.

② Wechseln Sie im LANCAPI-Client auf das Register **Netzwerk**. Hier können Sie zunächst wählen, ob der PC seinen LANCAPI-Server selbst suchen soll oder ob ein bestimmter Server (und damit eine bestimmte ISDN-Leitung) verwendet werden soll.

- Im ersten Fall legen Sie fest, in welchem zeitlichen Intervall der Client nach einem Server sucht. Dabei sucht er so lange, bis er die im nächsten Feld eingestellte Anzahl an Servern gefunden hat. Hat er die geforderte Zahl an Servern gefunden, hört er mit der Suche auf.
- Wenn der Client nicht automatisch nach Servern suchen soll, geben Sie in der Liste die IP-Adressen der Server an, die der Client verwenden soll. Diese Festlegung ist z.B. dann sinnvoll, wenn Sie mehrere LANCOM in Ihrem LAN als LANCAPI-Server betreiben und eine Gruppe von PCs einen bestimmten Server verwenden sollen.
- Für beide Optionen können Sie auch einstellen, in welchem Intervall der Client prüft, ob die gefundenen oder per Liste definierten Server noch aktiv sind.



15.3 So setzen Sie die LANCAPI ein

Zur Verwendung der LANCAPI gibt es zwei Möglichkeiten:

- Sie setzen eine Software ein, die direkt auf einer CAPI-Schnittstelle (in diesem Fall der LANCAPI) aufsetzt. Eine solche Software sucht bei der Installation nach der CAPI und verwendet diese anschließend automatisch.
- Andere Programme, wie LapLink, können Verbindungen über verschiedene Wege aufbauen, z.B. über das DFÜ-Netzwerk von Windows. Beim Anlegen einer neuen DFÜ-Verbindung können Sie auswählen, welches der installierten Kommunikationsgeräte Sie verwenden möchten. Wählen Sie für die LANCAPI den Eintrag 'ISDN WAN Line 1'.

15.4 Das LANCOM CAPI Faxmodem

Mit dem LANCOM CAPI Faxmodem steht Ihnen unter Windows ein Faxtreiber (Fax Class 1) zur Verfügung, der als Schnittstelle zwischen dem LANCAPI-Client und der Faxanwendung auf dem PC den Betrieb von Standard-Faxprogrammen über ein LANCOM ermöglicht.

Das LANCOM CAPI Faxmodem emuliert die Modem-Funktion sowie die Fax-Protokolle in der Software auf dem PC. Hierzu wird eine ausreichende Rechnerleistung (ab ca. 500 MHz Pentium) benötigt.

Installation

Das LANCOM CAPI Faxmodem wird über das CD-Setup installiert. Installieren Sie das LANCOM CAPI Faxmodem immer zusammen mit der aktuellen LANCAPI. Nach dem Neustart steht Ihnen im System das LANCOM CAPI Faxmodem zur Verfügung, z. B. unter Windows 98 unter **Start ▶ Einstellungen ▶ Systemsteuerung ▶ Modems**.

Faxen über CAPI Faxmodem

Das CAPI Faxmodem wird von den gängigen Faxprogrammen bei der Installation automatisch erkannt und als 'Class 1'-Faxmodem identifiziert. Damit sind Faxübertragungen mit bis zu 14.400 bit/s möglich. Falls Ihr Faxprogramm eine Unterscheidung erlaubt (z.B. WinFax bzw. Talkworks Pro), wählen Sie bei der Einrichtung des Modems die Option 'CLASS 1 (Software Flow Control)' aus

Faxen unter Windows 2000 und XP

Windows XP oder Windows 2000 bieten im Zusammenspiel mit dem CAPI Faxmodem volle Faxfunktionalität. Ein zusätzliches Faxprogramm ist nicht erforderlich.

Dazu starten Sie in der Systemsteuerung unter "Software" "Windows Komponenten hinzufügen / entfernen" und wählen die "Faxdienste" aus.

Nach der Installation befindet sich das Fax unter "Drucker und Faxgeräte", und kann von jedem Windows-Programm anstelle eines Druckers ausgewählt werden.



Das CAPI Faxmodem ist nur dann für die Übertragung von Faxnachrichten bereit, wenn die LANCAPI aktiv ist.

15.5 LANCOM Faxmodem-Option

Neben dem CAPI Faxmodem steht für einige LANCOM-Modelle (LANCOM 800, 4000, 4100) darüber hinaus die Faxmodem-Option zur Verfügung. Bei dieser Lösung sind die Fax- und Modem-Dienste im LANCOM selbst realisiert, die PCs werden von den Belastungen der Modem-Emulation befreit.

15.6 Unterstützte B-Kanal-Protokolle

Folgende CAPI-Protokolle werden unterstützt:

Wert		Bemerkung
B1-Protokoll		
	0	64 KBit/s mit HDLC Framing
	1	64 KBit/s transparent mit Byte-Framing des Netzwerks
	2	V.110 asynchron mit Start-Stop-Byte-Framing
	4*	T.30-Modem für Fax Gruppe 3
	7*	Modem mit vollständiger Verhandlung (B2 muss 7 sein)

Wert		Bemerkung
B2-Protokoll		
	0	ISO 7776 (X.75 SLP)
	1	Transparent
	4*	T.30 für Fax Gruppe 3
	7*	Modem mit vollständiger Verhandlung (z.B. V.42 bis, MNP 5)
	9	V.120 asynchron
B3-Protokoll		
	0	Transparent
	1	T.90NL, kompatibel zu T.70NL in Übereinstimmung mit T.90, Anhang II
	2	ISO 8208 (X.25 DTE-DTE)
	4*	T.30 für Fax Gruppe 3
	5*	T.30 für Fax Gruppe 3 erweitert
	7*	Modem

* = Gilt nur für LANCOM Faxmodem-Option

□ Unterstützte B- Kanal- Protokolle

16 Weitere Dienste

Ein LANCOM bietet eine Reihe von Dienstleistungen für die PCs im LAN an. Es handelt sich dabei um zentrale Funktionen, die von den Arbeitsplatzrechnern genutzt werden können. Im Einzelnen handelt es sich um:

- Automatische Adressverwaltung mit DHCP
- Namenverwaltung von Rechnern und Netzwerken mit DNS
- Gebührenerfassung
- Bürokommunikations-Funktionen mit LANCAPI
- Zeit-Server

16.1 Automatische IP-Adressverwaltung mit DHCP

Neu in LCOS 7.60:

- BOOTP: Zuweisung von festen IP-Adressen oder Boot-Images an bestimmte Stationen in Abhängigkeit vom IP-Netzwerk (ARF)

16.1.1 Einleitung

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- und NBNS-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, allen Rechnern im Netz „von Hand" diese Adressen 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 LANCOM-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
- NBNS-Server
- Gültigkeitsdauer der zugewiesenen Parameter

Der DHCP-Server entnimmt die IP-Adressen entweder aus einem frei definierten Adress-Pool oder ermittelt die Adressen selbstständig aus der eigenen IP-Adresse. Ein völlig unkonfiguriertes Gerät kann sogar im DHCP-Automodus die IP-Adressen für sich selbst und für die Rechner im Netz selbstständig festlegen. Im einfachsten Fall müssen Sie daher 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 den LANCOM-Geräten mehrere IP-Netzwerke definiert werden. Die DHCP-Einstellungen beziehen sich daher – bis auf einige allgemeine Einstellungen – auf ein bestimmtes IP-Netzwerk.

DHCP-Relay

Wenn im lokalen Netz schon ein anderer DHCP-Server vorhanden ist, kann das Gerät alternativ im DHCP-Client-Modus selbst die benötigten Adress-Informationen von dem anderen DHCP-Server beziehen.

Darüber hinaus kann ein LANCOM sowohl als DHCP-Relay-Agent als auch als DHCP-Relay-Server arbeiten.

- Als DHCP-Relay-Agent leitet ein LANCOM DHCP-Anfragen an einen weiteren DHCP-Server weiter.
- Als DHCP-Relay-Server kann ein LANCOM von DHCP-Relay-Agents weitergeleitete DHCP-Anfragen bearbeiten.

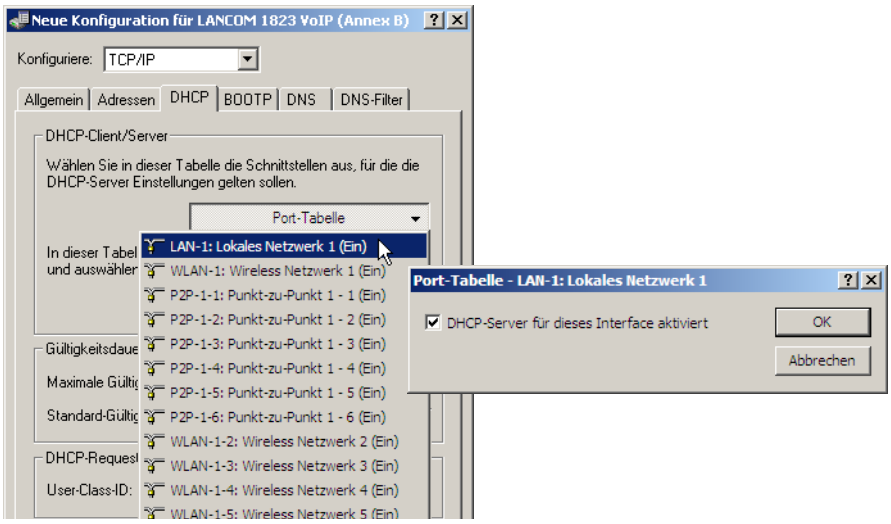
BOOTP

Über das Bootstrap- Protokoll (BOOTP) kann 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.

16.1.2 Konfiguration der DHCP- Parameter mit LANconfig

DHCP- Server für bestimmte logische Interfaces aktivieren oder deaktivieren

Der DHCP- Server kann für jedes logische Interface (z. B. LAN-1, WLAN-1, P2P-1-1 etc.) separat aktiviert oder deaktiviert werden. Wählen Sie dazu in der Port- Liste das entsprechende logische Interface und schalten Sie den DHCP- Server für dieses Interface ein oder aus. Die Parameter zur Aktivierung der Ports finden Sie in LANconfig im Konfigurationsbereich "TCP/IP" auf der Registerkarte "DHCP".



DHCP- Netzwerke konfigurieren

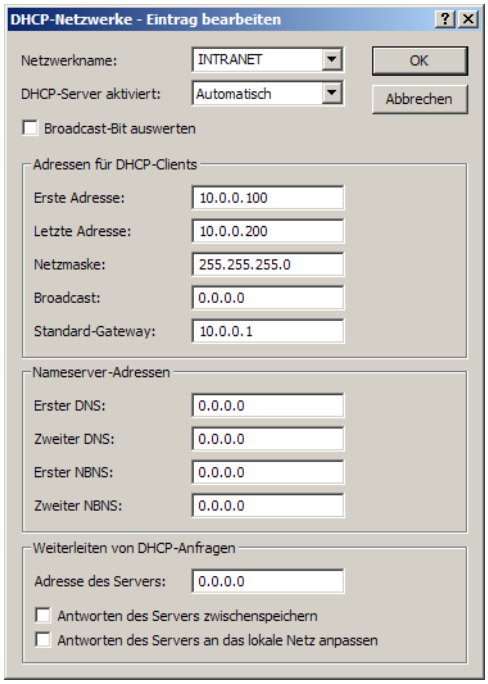
Für jedes im Gerät definierte IP- Netzwerk können die zugehörigen DHCP- Einstellungen separat festgelegt werden. Die Parameter zur Definition der DHCP- Netzwerke finden Sie in LANconfig im Konfigurationsbereich "TCP/IP" auf der Registerkarte "DHCP".

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.



■ Auswahl des IP-Netzwerks

Wählen Sie aus, für welches IP-Netzwerk die folgenden DHCP-Einstellungen gelten sollen. Die Einstellungen für die IP-Netzwerke finden Sie in LANconfig im Konfigurationsbereich "TCP/IP" auf der Registerkarte "Allgemein".

■ Betriebsmodus des DHCP-Servers einstellen

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.
- 'Auto': In diesem Zustand sucht das Gerät regelmäßig im lokalen Netz nach anderen DHCP-Servern. Diese Suche ist erkennbar durch ein kurzes Aufleuchten der LAN-Rx/Tx-LED.
  - □ Wird mindestens ein anderer DHCP-Server gefunden, schaltet das Gerät seinen eigenen DHCP-Server aus. Ist für den LANCOM Router noch keine IP-Adresse konfiguriert, dann wechselt er in den DHCP-Client-Modus und bezieht eine IP-Adresse vom DHCP-Server. Damit wird u.a. verhindert, dass ein unkonfiguriertes 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 LANCOM Router deaktiviert.
- 'Client': 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.

- 'Weiterleiten': Der DHCP-Server ist eingeschaltet, 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.

Ob der DHCP-Server letztendlich ein- oder ausgeschaltet ist, kann den DHCP-Statistiken entnommen werden.

Die Default-Einstellung für den Zustand ist 'Auto'.

■ Zuweisung von IP-Adressen

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 End-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 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.

■ Zuweisung der Netzmaske

Die Zuweisung der Netzmaske erfolgt analog zur Adresszuweisung. Wenn in DHCP-Einstellungen eine Netzmaske eingetragen ist, wird diese bei der Zuweisung verwendet. Ansonsten wird die Netzmaske aus dem IP-Netzwerk verwendet.

■ Zuweisung der Broadcast-Adresse

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 wird die zu verwendende Broadcast-Adresse in den DHCP-Einstellugnen eingetragen.

Die Änderung der Voreinstellung für die Broadcast-Adresse wird nur für erfahrene Netzwerk-Spezialisten empfohlen. Eine Fehlkonfiguration in diesem Bereich kann zu unerwünschten, kostenpflichtigen Verbindungsaufbauvorgängen führen!

■ Zuweisung des Standard-Gateways

Das LANCOM weist dem anfragenden Rechner standardmäßig seine eigene IP-Adresse in diesem Netzwerk als Gateway-Adresse zu. Falls erforderlich, kann durch den Eintrag einer entsprechende IP-Adresse auch ein anderes Gateway übertragen werden.

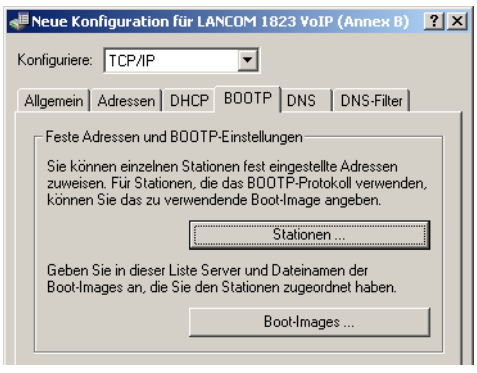
■ Zuweisung von DNS- und NBNS-Server

IP-Adressen der DNS- und NBNS-Nameserver, an den DNS- und NBNS-Anfragen weitergeleitet werden sollen.

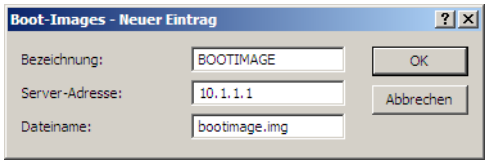
Ist bei den entsprechenden Feldern kein Server angegeben, so gibt der Router seine eigene IP-Adresse in diesem Netzwerk als DNS- bzw. NBNS-Adresse weiter, wenn der DNS-Server für dieses Netzwerk aktiviert ist. Ist der DNS-Server für dieses Netzwerk nicht aktiv, so wird die IP-Adresse aus den globalen TCP/IP-Einstellungen als DNS-Server übermittelt.

Zuweisung von festen IP-Adressen an bestimmte Stationen konfigurieren

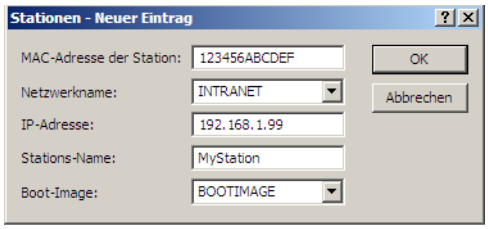
Die Parameter zur Konfiguration von BOOTP finden Sie in LANconfig im Konfigurationsbereich "TCP/IP" auf der Registerkarte "BOOTP".



Optional: Definieren Sie in der Liste der Boot-Images ein Boot-Image, dass Sie einer Station zuweisen möchten.



Definieren Sie in der Liste der Stationen die MAC-Adresse einer Station, der Sie eine bestimmte IP-Adresse zuweisen möchten. Wählen Sie optional ein Boot-Image aus, das dieser Station zugewiesen werden soll. Wenn diese Adress-Zuweisung nur dann verwendet werden soll, wenn sich die Station in einem bestimmten IP-Netzwerk befindet, geben Sie zusätzlich das entsprechende IP-Netzwerk an.



16.1.3 Konfiguration der DHCP-Parameter mit Telnet oder WEBconfig

Allgemeine DHCP-Einstellungen

- **User-Class-Identifer**

  Der DHCP-Client im LANCOM 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, z.B. 'LANCOM L-54ag'. Die Vendor-Class-ID wird immer übertragen. Der User-Class-Identifier (DHCP-Option 77) gibt einen benutzerdefinierten String an. Die User-Class-ID wird nur übertragen, wenn der Benutzer einen Wert konfiguriert hat.

- **Default-Gueltigkeit-Minuten**

  Wenn ein Client eine IP-Adresse anfordert, ohne eine Gültigkeitsdauer für diese Adresse zu fordern, wird dieser Adresse als Gültigkeistdauer der hier eingestellte Wert zugewiesen.

- **Max.-Gueltigkeit-Minuten**

  Wenn ein Client eine IP-Adresse bei einem DHCP-Server anfordert, kann er eine Gültigkeitsdauer für diese Adresse anfordern. Dieser Wert kontrolliert die maximale Gültigkeitsdauer, die ein Client anfordern darf.

Alias-Liste

In der Alias-Liste werden die Bezeichnungen für die Boot-Images definiert, über welche die Images in der Host-Tabelle referenziert werden können.

- **Image-Alias**

  Geben Sie eine beliebige Bezeichnung für dieses Boot-Image ein. Diese Bezeichnung wird verwendet, wenn Sie in der Stations-Liste ein Boot-Image einer bestimmten Station zuordnen.

- **Image-Server**

  Geben Sie die IP-Adresse des Servers ein, der das Boot-Image zur Verfügung stellt.

- **Image-File**

  Geben Sie den Namen der Datei auf dem Server an, die das Boot-Image enthält.

DHCP-Tabelle

Die DHCP-Tabelle gibt eine Übersicht über die in den IP-Netzwerken verwendeten IP-Adressen. Bei der DHCP-Tabelle handelt es sich um eine reine Status-Tabelle, in der keine Parameter konfiguriert werden können.

- **IP-Adresse**

  IP-Adresse, die von der Station verwendet wird.

- **MAC-Adresse**

  MAC-Adresse der Station.

- **Timeout**

  Gültigkeitsdauer der Adresszuweisung in Minuten.

- **Rechnername**

  Name der Station, sofern dieser ermittelt werden konnte.

- **Typ**

  Im Feld 'Typ' wird angegeben, wie die Adresse zugewiesen wurde. Das Feld kann die folgenden Werte annehmen:

  - neu: Der Rechner hat zum ersten Mal angefragt. Der DHCP-Server überprüft die Eindeutigkeit der Adresse, die dem Rechner zugewiesen werden soll.
  - unbek.: 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.
  - stat.: 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.
  - dyn.: Der DHCP-Server hat dem Rechner eine Adresse zugewiesen.

- **LAN-Ifc**

  Logische Interface, über das die Station mit dem Gerät verbunden ist.

- **Ethernet-Port**

  Physikalisches Interface, über das die Station mit dem Gerät verbunden ist.

- **VLAN-ID**

  Die von dieser Station verwendete VLAN-ID.

- **Netzwerkname**

  Name des IP-Netzwerks, in dem sich die Station befindet.

Host-Tabelle

Über das Bootstrap-Protokoll (BOOTP) kann einer Station beim Starten eine IP-Adresse und weitere Parameter übermittelt werden. Dazu wird die MAC-Adresse der Station in die Host-Tabelle eingetragen.

- **MAC-Adresse**

  Geben Sie hier die MAC-Adresse der Station ein, der eine IP-Adresse zugewiesen werden soll.

- **Netzwerkname**

  Hier wird der Name eines konfigurierten IP-Netzwerks eingetragen. Nur wenn sich die anfragende Station in diesem IP-Netzwerk befindet, wird der Station die für die MAC-Adresse definierte IP-Adresse zugewiesen.



Befindet sich die anfragende Station in einem IP-Netzwerk, zu dem es keinen passenden Eintrag in der Host-Tabelle gibt, so wird der Station dynamisch eine IP-Adresse aus dem IP-Adress-Pool des jeweiligen IP-Netzwerks zugewiesen.

- **IP-Adresse**

  Geben Sie hier die IP-Adresse der Station ein, die der Station zugewiesen werden soll.

- **Rechnername**

  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.



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.

Netzliste

In dieser Tabelle werden die DHCP-Einstellungen zu den IP-Netzwerken definiert.

- **Netzwerkname**

  Name des Netzwerks, für das die Einstellungen des DCHP-Servers gelten sollen.

- **DHCP-Server aktiviert**

  Betriebsart des DHCP-Servers für dieses Netzwerk. Je nach Betriebsart kann sich der DHCP-Server selbst aktivieren bzw. deaktivieren. Ob der DHCP-Server aktiv ist, kann den DHCP-Statistiken entnommen werden.

  Mögliche Werte:

- □ Nein: Der DHCP-Server ist dauerhaft abgeschaltet.
- □ Automatisch: In diesem Zustand sucht das Gerät regelmäßig im lokalen Netz nach anderen DHCP-Servern. Diese Suche ist erkennbar durch ein kurzes Aufleuchten der LAN-Rx/Tx-LED.

  Wird mindestens ein anderer DHCP-Server gefunden, schaltet das Gerät seinen eigenen DHCP-Server aus. Ist für den LANCOM Router noch keine IP-Adresse konfiguriert, dann wechselt er in den DHCP-Client-Modus und bezieht eine IP-Adresse vom DHCP-Server. Damit wird u.a. verhindert, dass ein unkonfiguriertes 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 LANCOM Router deaktiviert.
- □ 'Ja': 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 für das Netzwerk 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.
- □ 'Anfragen Weiterleiten': Der DHCP-Server ist eingeschaltet, 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).

Default:

- □ Automatisch



Verwenden Sie die Einstellung "Ja" nur dann, wenn sichergestellt ist, dass kein anderer DHCP-Server im LAN aktiv ist.



Verwenden Sie die Einstellung "Client-Modus" nur dann, wenn sichergestellt ist, das ein anderer DHCP-Server im LAN aktiv ist und die Zuweisung der IP-Adress-Informationen übernimmt.

■ **Broadcast-Bit auswerten**

Wählen Sie hier, ob das von den Clients gemeldete Broadcast-Bit ausgewertet wird oder nicht. Wenn das Bit nicht ausgewertet wird, werden alle DHCP-Nachrichten als Broadcast versendet.

■ **Erste Adresse**

Erste IP-Adresse des Adressbereiches, der den Clients zur Verfügung steht. Wenn hier keine Adresse eingetragen ist, dann verwendet der DHCP-Server die erste freie IP-Adresse aus diesem Netzwerk (wird bestimmt aus Netzadresse und Netzmaske).

■ **Letzte Adresse**

Letzte IP-Adresse des Adressbereiches, der den Clients zur Verfügung steht. Wenn hier keine Adresse eingetragen ist, dann verwendet der DHCP-Server die letzte freie IP-Adresse aus diesem Netzwerk (wird bestimmt aus Netzadresse und Netzmaske).

■ **Netzmaske**

Zugehörige Netzmaske für den Adressbereich, der den Clients zur Verfügung steht. Wenn hier keine Adresse eingetragen ist, dann verwendet der DHCP-Server die Netzmaske aus dem zugehörigen Netzwerk.

■ **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 wird die zu verwendende Broadcast-Adresse im DHCP-Modul eingetragen.



Die Änderung der Voreinstellung für die Broadcast-Adresse wird nur für erfahrene Netzwerk-Spezialisten empfohlen. Eine Fehlkonfiguration in diesem Bereich kann zu unerwünschten, kostenpflichtigen Verbindungsaufbauvorgängen führen!

■ **Standard-Gateway**

Der LANCOM weist dem anfragenden Rechner standardmäßig seine eigene IP-Adresse als Gateway-Adresse zu. Falls erforderlich, kann durch den Eintrag einer entsprechende IP-Adresse auch ein anderes Gateway übertragen werden.

- **Erster DNS**

  IP-Adresse des DNS-Nameservers, an den DNS-Anfragen weitergeleitet werden sollen.

- **Zweiter DNS**

  IP-Adresse des Backup-DNS-Nameservers, an den DNS-Anfragen weitergeleitet werden sollen, wenn der erste Nameserver ausfällt.

- **Erster NBNS**

  IP-Adresse des NetBIOS-Nameservers, an den NBNS-Anfragen weitergeleitet werden sollen.

- **Zweiter NBNS**

  IP-Adresse des Backup-NBNS-Nameservers, an den NBNS-Anfragen weitergeleitet werden sollen, wenn der erste Nameserver ausfällt.

- **Adresse des Servers**

  Hier wird die IP-Adresse des übergeordneten DHCP-Servers eingetragen, an den DHCP-Anfragen weitergeleitet werden, wenn für das Netzwerk die Betriebsart 'Anfragen Weiterleiten' gewählt wurde.

- **Antworten des Servers zwischenspeichern**

  Mit dieser Option können die Antworten des übergeordneten DHCP-Servers im LANCOM Router gespeichert werden. Spätere Anfragen können dann vom LANCOM Router selbst beantwortet werden. Diese Option ist nützlich, wenn der übergeordnete DHCP-Server nur über eine kostenpflichtige Verbindung erreicht werden kann.

- **Antworten des Servers an das lokale Netz anpassen**

  Mit dieser Option können die Antworten des übergeordneten DHCP-Servers an das lokale Netzwerk angepasst werden. Bei aktivierter Anpassung ersetzt ein LANCOM in den Antworten des übergeordneten DHCP-Servers folgende Einträge durch seine eigene Adresse (bzw. lokal konfigurierte Adressen):

  - Gateway
  - Netzmaske
  - Broadcast-Adresse
  - DNS-Server
  - NBNS-Server
  - Server-ID

  Diese Option ist sinnvoll, wenn der übergeordnete DHCP-Server keine getrennte Konfiguration für DHCP-Clients in einem anderen Netzwerk zulässt.

Port-Tabelle

In der Port-Tabelle wird der DHCP-Server für die jeweiligen logischen Interfaces des Geräts freigegeben.

- **Port**

  Auswahl des logischen Interfaces, für das der DHCP-Server aktiviert bzw. deaktiviert werden soll.

- **DHCP-freigeben**

  Aktiviert bzw. deaktiviert den DHCP-Server für das gewählte logische Interface.

Zusaetzliche-Optionen

Mit den DHCP-Optionen können zusätzliche Konfigurationsparameter an die Stationen übertragen werden. Der Vendor-Class-Identifier (DHCP-Option 60) zeigt so z. B. den Gerätetyp an. In dieser Tabelle werden zusätzliche Optionen für den DHCP-Betrieb definiert.

- **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 vollständige Liste aller DHCP-Optionen finden Sie im RFC 2132 – DHCP Options and BOOTP Vendor Extensions der Internet Engineering Task Force (IETF).

- **Netzwerkname**

  Name des IP-Netzwerks, in dem diese DHCP-Option verwendet werden soll.

- **Options-Wert**

  In diesem Feld wird der Inhalt der DHCP-Option definiert. Für die Option "17" wird hier z. B. der Pfad zu einem Boot-Image eingetragen, über welches ein PC ohne eigene Festplatte über BOOTP sein Betriebssystem beziehen kann.

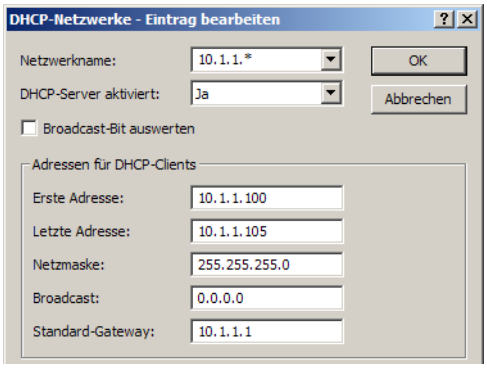
Die mögliche Länge des Optionswertes hängt von der gewählten Optionsnummer ab. Der RFC 2132 listet für jede Option ein zulässige Länge auf.

16.1.4 DHCP-Relay-Server

Ein LANCOM kann nicht nur DHCP-Anfragen an einen übergeordneten DHCP-Server weiterleiten, es kann auch selbst als zentraler DHCP-Server fungieren (DHCP-Relay-Server).

Um einen LANCOM 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 Accesspoints 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 den LANCOM 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.

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.

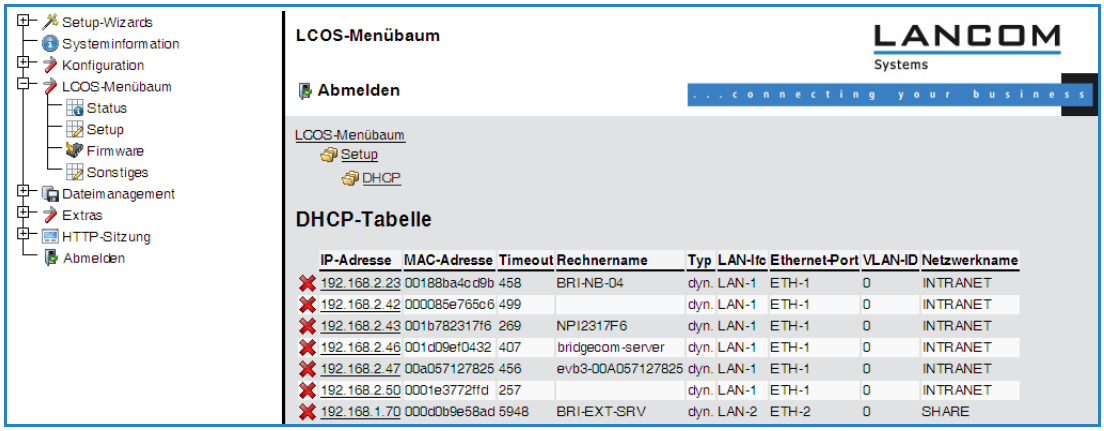
16.1.5 Konfiguration der Stationen

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.

16.1.6 IP-Adressen im LAN überprüfen

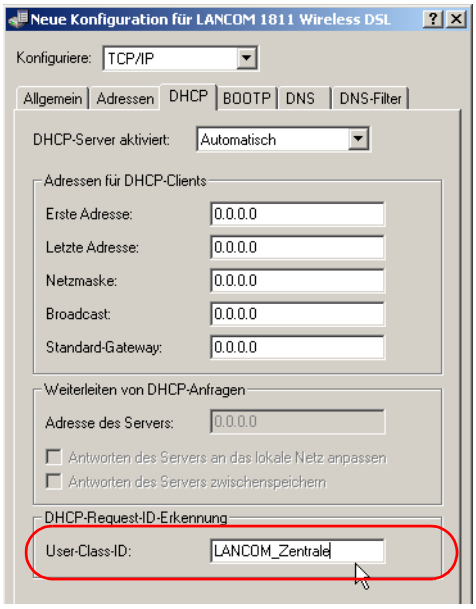
Eine Übersicht über die IP-Adressen im LAN gibt die DHCP-Tabelle (WEBconfig: Setup/DHCP/Tabelle-DHCP). Sie zeigt die zugewiesene bzw. verwendete IP-Adresse, die MAC-Adresse, die Gültigkeitsdauer, den Namen des Rechners (falls vorhanden) sowie den Typ der Adresszuweisung.



16.2 Vendor-Class- und User-Class-Identifier im DHCP-Client

Der DHCP-Client im LANCOM 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, z.B. 'LANCOM L-54ag'. 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 'TCP/IP' auf der Registerkarte 'DHCP' im Feld 'User-Class-ID' eingetragen werden kann (Default: leer). Die User-Class-ID wird nur übertragen, wenn der Benutzer einen Wert konfiguriert hat.



16.3 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, um z.B. einer Anfrage nach 'www.lancom.de' die entsprechende IP-Adresse zurückliefern zu können. 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.

16.3.1 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 LANCOM anzusiedeln:

- Ein LANCOM 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.
- Beim Routing von Windows-Netzen über NetBIOS kennt ein LANCOM außerdem die Rechnernamen und IP-Adressen in den anderen angeschlossenen NetBIOS-Netzen. Außerdem melden sich auch die Rechner mit fest eingestellter IP-Adresse ggf. in der NetBIOS-Tabelle an und sind damit mit Namen und Adressen bekannt.
- Der DNS-Server im LANCOM 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.

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.
- Findet der DNS-Server in den vorausgegangenen Tabellen keine Informationen über den Namen, werden die Listen des NetBIOS-Moduls durchsucht. Auch die Verwendung der NetBIOS-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.

16.3.2 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.

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.

Generelles DNS-Forwarding

Alle DNS-Anfragen, die nicht auf sonstige Weise aufgelöst werden können, werden an einen DNS-Server weitergeleitet. Dieser DNS-Server bestimmt sich nach folgenden Regeln:

Der Router sucht zunächst in seinen eigenen Einstellungen, ob ein DNS-Server eingetragen ist. Wird er dort fündig, holt er die gewünschte Information von diesem Server. Bis zu zwei übergeordnete DNS-Server können angegeben werden.

LANconfig: TCP/IP ▶ Adressen ▶ Erster DNS-Server / Zweiter DNS-Server

WEBconfig: LCOS-Menübaum ▶ Setup ▶ TCP/IP ▶ DNS-Default ▶ DNS-Backup

- Gibt es keinen eingetragenen DNS-Server im Router, versucht er auf einer evtl. bestehenden PPP-Verbindung (z. B. zum Internet-Provider) einen DNS-Server zu erreichen, und holt die Zuordnung der IP-Adresse zum Namen von dort. Das gelingt natürlich nur dann, wenn während der PPP-Verhandlung die Adresse eines DNS-Servers an den Router übermittelt worden ist.
- Besteht keine Verbindung, wird die Default-Route aufgebaut und dort nach dem DNS-Server gesucht.

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.

16.3.3 So stellen Sie den DNS-Server ein

Die Einstellungen für den DNS-Server finden Sie im folgenden Menü bzw. in folgender Liste:

LANconfig: TCP/IP ▶ DNS-Server

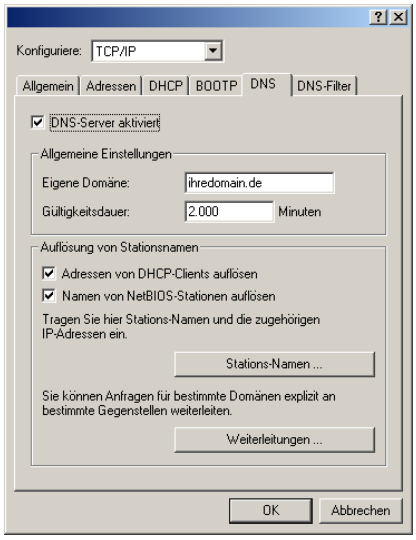
WEBconfig: LCOS-Menübaum ▶ Setup ▶ DNS

Gehen Sie zur Einstellung des DNS-Servers wie folgt vor:

① Schalten Sie den DNS-Server ein.

② Geben Sie die Domain ein, in der sich der DNS-Server befindet. Mit Hilfe dieser Domain erkennt der DNS-Server bei Anfrage, ob sich der gesuchte Name im eigenen LAN befindet oder nicht. Die Angabe der Domain ist optional.

③ Geben Sie an, ob die Informationen aus dem DHCP-Server und dem NetBIOS-Modul verwendet werden sollen.



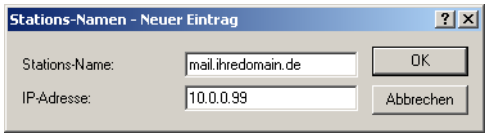
Aktivierter DNS-Server in der TCP-IP-Konfiguration

④ Der DNS-Server dient hauptsächlich dazu, Anfragen nach Namen im Internet von den Anfragen nach Namen bei anderen Gegenstellen zu trennen. Tragen Sie daher alle Rechner in die Stations-Namen-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.

Mit folgenden Befehlen fügen Sie Stationen zur Stations-Namen-Tabelle hinzu:

Wenn Sie z. B. in einem externen Büro arbeiten und 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 Sie nun das Mailprogramm starten, wird es vermutlich automatisch den Server 'mail.ihredomain.de' suchen. Der DNS-Server gibt daraufhin die IP-Adresse '10.0.0.99' zurück. Das Mailprogramm sucht dann nach dieser IP-Adresse. Mit entsprechenden Einträgen in IP-Routing-Tabelle und Gegenstellenliste etc. wird dann automatisch die Verbindung zum Netz in der Zentrale hergestellt, wo der Mailserver schließlich gefunden wird.

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 die Wildcards '?' für einzelne Zeichen und '*' für mehrere Zeichen verwendet werden.

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

16.3.4 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: TCP/IP ▶ DNS-Filter ▶ DNS-Filter ▶ Hinzufügen

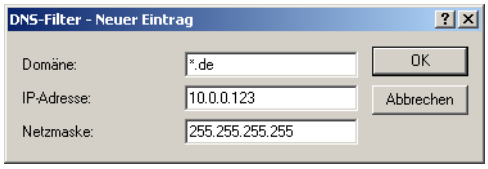
WEBconfig: … ▶ Filter-Liste ▶ Hinzufügen



Der Index '001' kann bei der Konfiguration über Telnet oder WEBconfig 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.

16.3.5 Dynamic DNS

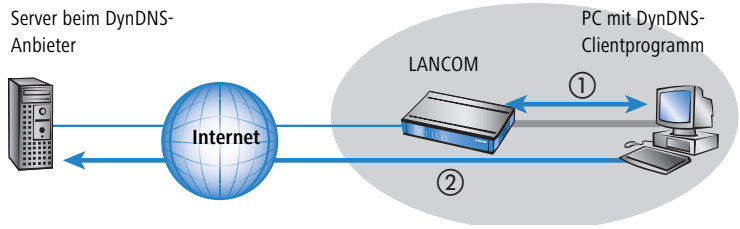
Damit auch Systeme mit dynamischen IP-Adressen über das WAN - also beispielsweise über das Internet - erreichbar sind, existieren eine Reihe von sog. Dynamic DNS-Server Anbietern (z.B. www.dynDNS.org).

Damit wird ein LANCOM immer unter einem bestimmten Namen (FQDN - 'fully qualified domain name') erreichbar (z.B. "http://MyLANCOM.dynDNS.org").

Der Vorteil liegt auf der Hand: Wenn Sie z.B. eine Fernwartung an einem Anschluss ohne ISDN durchführen wollen (z.B über WEBconfig / HTTPS), oder über den LANCOM VPN-Client auf eine Außenstelle mit dynamischer IP-Adresse zugreifen wollen, dann brauchen Sie lediglich den Dynamic DNS-Namen zu kennen.

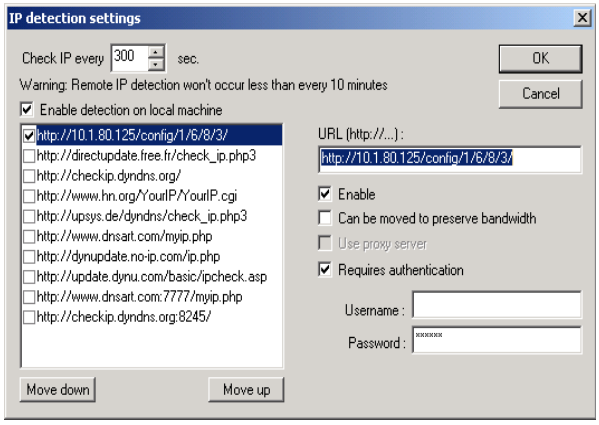
Wie gelangt die aktuelle IP-Adresse zum Dynamic DNS Server?

Dynamic DNS Anbieter unterstützen eine Reihe von PC-Clientprogrammen, die über verschiedene Methoden die aktuell zugewiesene IP-Adresse eines LANCOM ermitteln können ①, und im Falle einer Änderung an den jeweiligen Dynamic DNS Server übertragen ②.

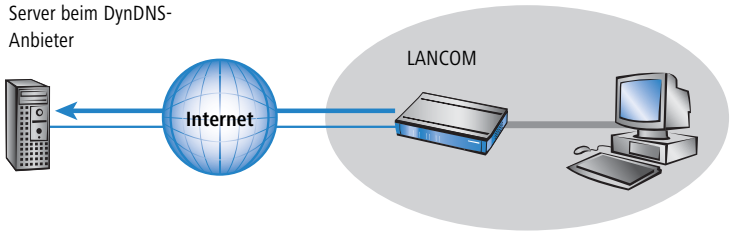


Die aktuelle WAN-seitige IP-Adresse eines LANCOM kann unter folgender Adresse ausgelesen werden:

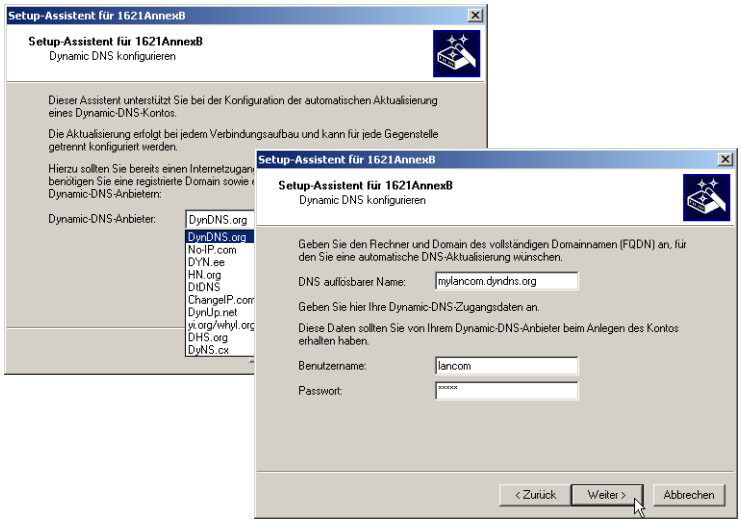
```
http://<Adresse des LANCOM>/config/1/6/8/3/
```



Alternativ kann das LANCOM die aktuelle WAN-IP auch direkt an den DynDNS-Anbieter übertragen:



Die dazu notwendigen Einstellungen können komfortabel mit dem Setup-Assistenten von LANconfig vorgenommen werden:

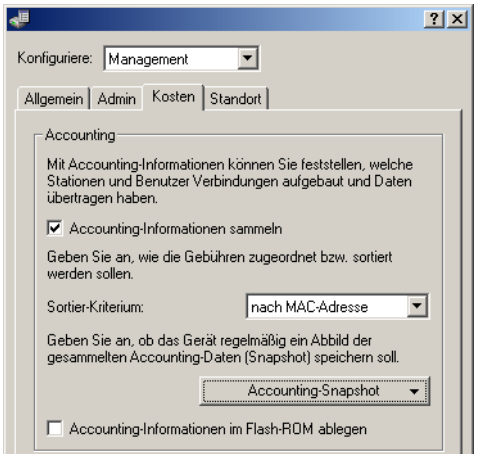


16.4 Accounting

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.

Konfiguration des Accounting

Bei der Konfiguration des Accounting werden die allgemeinen Parameter festgelegt:



LANconfig: Management ▶ Kosten

WEBconfig: LCOS-Menübaum ▶ Setup ▶ Accounting

- **Accounting-Informationen sammeln**
  - □ Accounting ein- oder ausschalten.
- **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.
- **Sortierkriterium**

  Auswahl des Merkmals, nach dem die Accounting-Daten kumuliert werden:
  - □ MAC-Adresse: Die Daten werden anhand der MAC-Adresse der Clients gesammelt.
  - □ IP-Adresse: Die Daten werden anhand der IP-Adresse der Clients gesammelt.

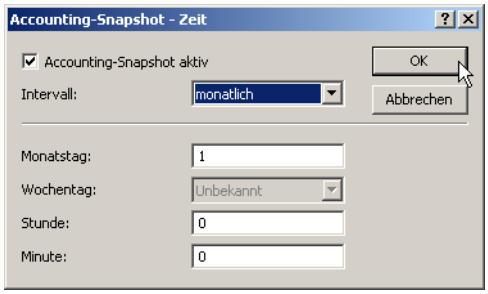
Die Option 'IP-Adresse' kann bei wechselnden IP-Adressen, z.B. bei Verwendung eines DHCP-Servers, zu ungenauen Accounting-Daten führen. Eine Zuordnung der Daten zu Benutzern ist dann ggf. nicht exakt möglich. Auf der anderen Seite können mit dieser Einstellung die Daten von Clients separiert werden, die sich hinter einem weiteren Router befinden und daher mit der gleichen MAC-Adresse des Routers in der Accounting-Liste auftauchen.

- **Sortieren nach**

  Wählen Sie hier aus, ob die Daten in der Accounting-Tabelle nach Verbindungszeiten oder Datenvolumen sortiert werden sollen.

Konfiguration des Snapshots

Bei der Konfiguration des Snapshots wird das Interval festgelegt, in dem die Accounting-Daten in einem Snapshot zwischengespeichert werden:



LANconfig: Management ▶ Kosten ▶ Accounting-Snapshot

WEBconfig: LCOS-Menübaum ▶ Setup ▶ Accounting ▶ Zeit-Schnappschuss

Die Snapshot-Funktion kann nur dann genutzt werden, wenn das Gerät über eine gültige Systemzeit verfügt.

- **Accounting-Snapshot aktiv**
  - Zwischenspeichern der Accounting-Daten ein- oder ausschalten.
- **Interval**
  - täglich, wöchentlich oder monatlich
- **Monatstag**

  Der Tag im Monat, an dem die Zwischenspeicherung vorgenommen wird. Nur beim Interval 'monatlich' von Bedeutung.
- **Wochentag**

  Der Wochentag, an dem die Zwischenspeicherung vorgenommen wird. Nur beim Interval 'wöchentlich' von Bedeutung.
- **Stunde**

  Die Stunde, zu der die Zwischenspeicherung vorgenommen wird:
- **Minute**

  Die Minute, zu der die Zwischenspeicherung vorgenommen wird:

16.5 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 die LCOS verschiedene Möglichkeiten:

- Die verfügbaren Online-Minuten können für eine bestimmte Periode eingeschränkt werden.
- Für ISDN-Verbindungen kann für eine bestimmte Periode ein Gebührenlimit oder ein Zeitlimit festgelegt werden.

16.5.1 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 LANCOM erfolgt, beispielsweise für Kabelmodem-Verbindungen.

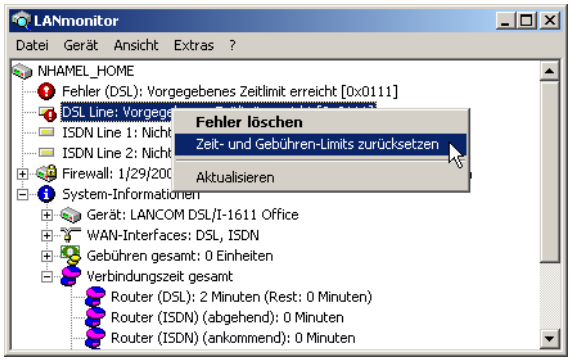
Um die Kosten begrenzen zu können, kann die maximale Verbindungsdauer mit Hilfe der Zeit gesteuert werden. Dazu wird ein Zeit-Limit für DSL-Verbindungen in einer Periode vereinbart. Im Auslieferungszustand dürfen die DSL-Verbindungen z.B. für maximal 600 Minuten in sechs Tagen genutzt werden.

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:

WEBconfig: LCOS-Menübaum ▶ Setup ▶ Gebuehren ▶ 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.

16.5.2 Gebührenabhängige ISDN-Verbindungsbegrenzung

Werden an einem ISDN-Anschluss Gebühreninformationen übermittelt, können die anfallenden Verbindungsgebühren recht einfach eingeschränkt werden. Im Default-Zustand dürfen z.B. maximal 830 Gebühreneinheiten in sechs Tagen verbraucht werden. Ist diese Grenze erreicht, erlaubt der Router keinen weiteren aktiven Verbindungsaufbau.

Die Gebührenüberwachung des Routers können Sie am besten bei freigeschalteter „Gebühreninformation **während** der Verbindung" im ISDN-Netz (nach AOCD) nutzen. Beantragen Sie ggf. die Freischaltung dieses Merkmals bei Ihrer Telefongesellschaft. Eine Gebührenüberwachung mit dem Merkmal „Gebühreninformation **nach** der Verbindung" ist im Prinzip auch möglich, jedoch werden dabei ggf. Dauerverbindungen nicht erkannt!

Wenn Sie das Least-Cost-Routing für die Router-Module eingeschaltet haben, werden ggf. auch Verbindungen über Provider aufgebaut, die keine Gebühreninformationen übertragen!

16.5.3 Zeitabhängige ISDN-Verbindungsbegrenzung

Der Mechanismus der ISDN-Gebührenüberwachung greift nicht, wenn am ISDN-Anschluss keine Gebühreninformationen übertragen werden. Das ist z.B. dann der Fall, wenn die Übermittlung der Gebühreninformationen entweder nicht beantragt wurde oder die Telefongesellschaft diese Informationen grundsätzlich nicht übermittelt.

Um die Kosten für ISDN-Verbindungen auch ohne Gebühreninformationen begrenzen zu können, kann die maximale Verbindungsdauer mit Hilfe der Zeit gesteuert werden. Dazu wird ein Zeitbudget für eine Periode vereinbart. Im Default-Zustand dürfen z.B. für maximal 210 Minuten innerhalb von sechs Tagen Verbindungen aktiv aufgebaut werden.

Wird die Grenze eines Budgets erreicht, werden automatisch alle offenen Router-Verbindungen beendet, die der Router selbst aufgebaut hat. Erst nach dem Ablauf der aktuellen Periode werden die Budgets wieder freigegeben und aktive Verbindungen ermöglicht. Der Administrator kann die Budgets natürlich auch vorzeitig wieder freigeben!

Mit einem Budget von 0 Einheiten bzw. 0 Minuten kann die Gebühren- bzw. Zeitüberwachung der Routerfunktionen ausgeschaltet werden.

Nur die Router-Funktionen sind durch den Gebühren- oder Zeitschutz abgesichert! Verbindungen über die LANCAPI werden davon nicht erfasst.

16.5.4 Einstellungen im Gebührenmodul

LANconfig: Management ▶ Kosten

WEBconfig: LCOS-Menübaum ▶ Setup ▶ Gebuehren

Im Gebührenmodul können Sie die Onlinezeit überwachen und für den Aufbauschutz nutzen.

- Tage/Periode
  Dauer einer Überwachungsperiode in Tagen angegeben
- Budget-Einheiten, Online-Minuten-Budget
  Maximale ISDN-Einheiten bzw. Online-Minuten in einer Überwachungsperiode

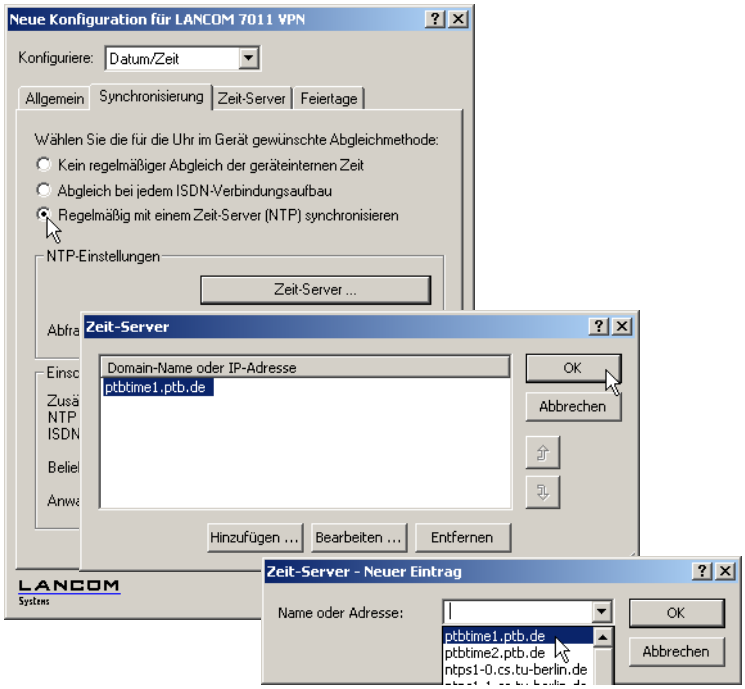
Die Informationen über die Gebühren und Verbindungszeiten werden über einen Bootvorgang hinaus gesichert (z. B. beim Einspielen einer neuen Firmware) und gehen erst verloren, wenn das Gerät ausgeschaltet wird. Alle hier erwähnten Zeitangaben werden in Minuten gemacht.

16.6 Zeit-Server für das lokale Netz

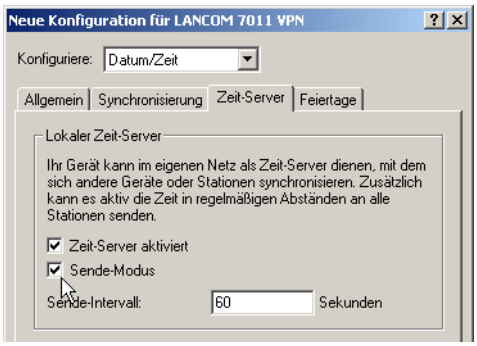
LANCOM Router können hochgenaue Zeitinformationen entweder über ISDN beziehen, oder aber über öffentlich zugängliche Zeit-Server im Internet (NTP-Server mit 'Open Access'-Policy, z.B. von der Physikalisch-Technischen Bundesanstalt). Die so ermittelte Zeit kann das LANCOM allen Stationen im lokalen Netz zur Verfügung stellen.

16.6.1 Konfiguration des Zeit-Servers unter LANconfig

Damit ein LANCOM die aktuelle Zeit im Netzwerk bekannt machen kann, wird im Konfigurationsbereich 'Datum/Zeit' auf der Registerkarte 'Synchronisierung' der regelmäßig Abgleich mit einem Zeitserver aktiviert. In den 'NTP-Einstellungen' wird dann mit der Schaltfläche **Zeit-Server** die Liste der Zeitserver geöffnet. Mit der Schaltfläche **Hinzufügen** können weitere Server in die Liste aufgenommen werden.



Mit diesen Einstellungen bezieht zunächst nur das LANCOM selbst die Zeit von den öffentlichen Zeitservern. Um die aktuelle Zeit auch im LAN den anderen Geräte bekannt zu machen, wird auf der Registerkarte 'Zeit-Server' der Zeit-Server aktiviert. Außerdem wird der Sendemodus eingeschaltet, wenn das LANCOM die Zeit in festen Intervallen aktiv in das Netz senden soll.



16.6.2 Konfiguration des Zeit-Servers mit WEBconfig oder Telnet

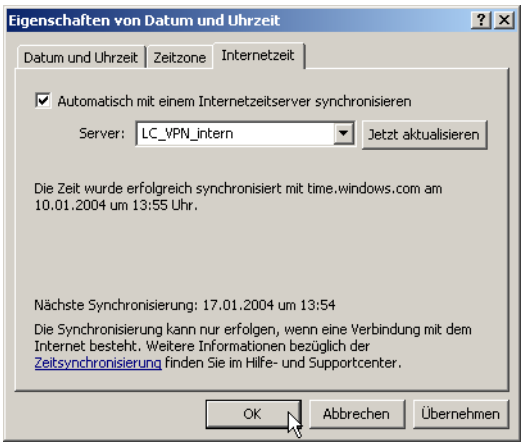
Bei der Konfiguration mit WEBconfig oder Telnet finden sich die benötigten Parameter in folgenden Bereichen:

WEBconfig: LCOS-Menübaum ▶ Setup ▶ NTP

16.6.3 Konfiguration der NTP-Clients

Die NTP-Clients müssen so konfiguriert sein, dass sie die Zeitinformationen vom LANCOM verwenden. Nicht alle Betriebssysteme verfügen über einen integrierten NTP-Client: Windows XP verfügt über einen solchen, für andere Windows-Betriebssysteme ist ein separater NTP-Client notwendig, bei Linux-Distributionen muss NTP entsprechend mitinstalliert sein.

Die 'Eigenschaften von Datum und Zeit' in einem XP-System werden mit einem Doppelklick auf die Uhrzeit unten rechts im Bildschirm geöffnet. Auf der Registerkarte 'Internetzeit' kann dort der Server zur Synchronisation der Zeit ausgewählt werden.



16.6.4 Fehlererkennung und Protokollierung der WLAN-Aktivitäten

Alle WLAN-Aktivitäten eines Access Points können in einer Protokolldatei gespeichert werden. Bei automatisch erkannten Access Points läßt sich diese Funktion unter dem Menüpunkt **Access Point ▶ Optionen** aktivieren. Auch im laufenden Betrieb werden die wichtigsten Informationen aus den Protokoll-Dateien im WLANmonitor angezeigt:

- **Anmeldehistorie**

  Die Anmeldehistorie ist über das Kontextmenü der Access Points bzw. der Clients erreichbar. Sie beinhaltet erfolgreiche An- und Abmeldungen sowie fehlgeschlagene Einwahlversuche auf dem Access Point bzw. An- und Abmeldevorgänge eines Clients bei (verschiedenen) Access Points. Die Anmeldehistorie kann auch über das Kontextmenü der Gruppe über alle in Ihr befindlichen Access-Points abgerufen werden. Hierüber kann z.B. der Versuch eines unbefugten Zugriffs auf das WLAN aufgedeckt werden.

- **Aktuelle Fehler**

  Die aktuellen Fehler werden unterhalb der Access Point- bzw. Clientliste angezeigt. Beim Access Point meldet diese Liste z.B., wenn ein Access Point nicht mehr erreichbar ist, wenn er eine falsche Firmware hat oder wenn sein WLAN-Zugang deaktiviert ist. Bei Clients können z.B. Login- oder Roaming-Fehler auftreten. Auftretende

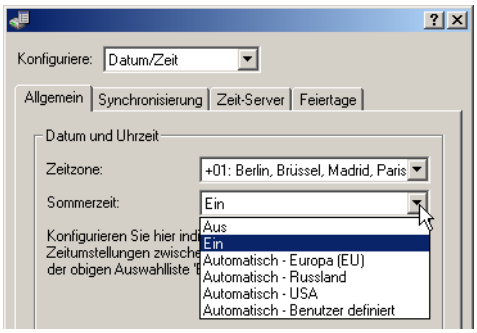
Fehler werden zudem in der Statusleiste angezeigt. Durch die Liste der aktuellen Fehler wird gewährleistet, dass Sie auftretende Fehler umgehend registrieren und so schnell beheben können.

■ **Ereignishistorie**

In der Ereignishistorie von Access Points und Clients erfolgt eine Aufzeichnung aller WLAN-Ereignisse auf dem jeweiligen Gerät. Sie wird jeweils unterhalb der aktuellen Fehler angezeigt. Besonders hilfreich kann sie bei der Analyse von auftretenden Fehlern sowie bei der laufenden Überwachung des Netzwerkes sein.

■ **Uhrzeitumstellung nach UTC**

LANCOM-Geräte arbeiten 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

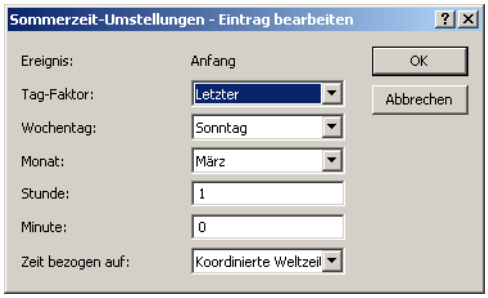
WEBconfig: LCOS-Menübaum > Setup > Zeit > Sommerzeit

■ **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 (EU, USA, Russland): 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.

Benutzerdefinierte Sommerzeitumstellung

Für den Beginn und das Ende der automatischen Sommerzeitumstellung können benutzerdefinierte Werte festgelegt werden.



LANconfig: Datum/Zeit ▶ Allgemein ▶ Sommerzeit-Umstellungen

WEBconfig: LCOS-Menübaum ▶ Setup ▶ Zeit ▶ Umstellung-Sommerzeit

■ **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 per ISDN geholt oder manuell gesetzt, wird immer angenommen, dass es sich um eine Zeitangabe gemäß Sommerzeit handelt.

16.7 Scheduled Events

16.7.1 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 LANCOM Kommandozeilenfunktion. Es können damit also alle LANCOM 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 LANCOM 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 LANCOM 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

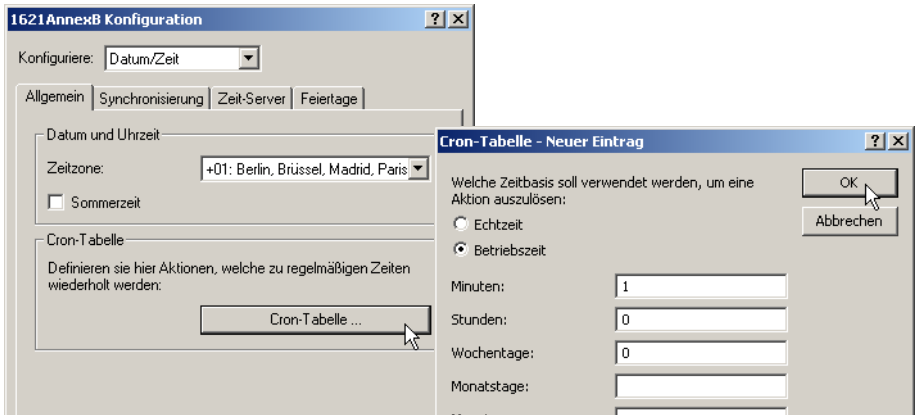
  Bei manchen Tabellen im LCOS macht es Sinn, die Inhalte regelmäßig zu löschen. Wenn Ihr Internetanschluss z.B. an eine monatliche Volumenbeschränkung gebunden ist, können Sie mit dem monatlichen Löschen der Accounting-Tabelle den Überblick über das tatsächlich jeden Monat verbrauchte Datenvolumen behalten.

16.7.2 CRON-Jobs mit Zeitverzögerung

Mit Hilfe von CRON-Jobs lassen sich regelmäßige Aktionen zu bestimmten Zeiten automatisch auf einem LANCOM 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.

16.7.3 Konfiguration der Zeitautomatik

Zur Konfiguration der CRON-Jobs im LANCOM stehen folgende Parameter bereit:



LANconfig: Datum/Zeit ▶ Allgemein ▶ Cron-Tabelle

WEBconfig: LCOS-Menübaum > Setup > Config > Cron-Tabelle

- **Eintrag aktiv**

  Aktiviert oder deaktiviert den Eintrag.

  - Default: Aktiv

- **Zeitbasis**

  Das Feld 'Zeitbasis' bestimmt ob die zeitliche Steuerung auf Grundlage der Echtzeit oder auf Grundlage der Betriebszeit des Gerätes ausgeführt werden soll.

  - Echtzeit: Diese Regeln werten alle Zeit-/Datumsangaben aus.
  - Betriebszeit: Diese Regeln werten nur die Minuten- und Stundenangaben seit dem letzten Gerätestart aus.
  - Default: Echtzeit

- **Minuten**
- **Stunden**
- **Wochentage**
- **Monatstage**
- **Monate**

  Die Werte 'Minute' bis 'Monate' definieren die Zeitpunkte, an denen ein Kommando ausgeführt werden soll. Wird ein Wert nicht angegeben, so wird er auch nicht in die Steuerung einbezogen.
  Pro Parameter kann auch eine Komma-separierte Liste von Werten, oder aber ein Bereich (angegeben als "Minimalwert-Maximalwert") eingegeben werden.

  Die Syntax des 'Wochentage'-Feldes entspricht dabei der üblichen cron- Interpretation:

  - 0: Sonntag
  - 1: Montag
  - 2: Dienstag
  - 3: Mittwoch
  - 4: Donnerstag
  - 5: Freitag
  - 6: Samstag

- **Befehl**

  Das auszuführende Kommando oder eine Komma-separierte Kommando-Liste. Ausgeführt werden kann dabei **jede** beliebige LANCOM Kommandozeilenfunktion.

■ **Besitzer**

Als Besitzer des Cron-Jobs kann ein im Gerät definierter Administrator ausgewählt werden. Sofern ein Besitzer angegeben ist, werden die Befehle des Cron-Jobs mit den Rechten des Besitzers ausgeführt.

□ Default: root

■ **Variation**

Dieser Parameter gibt eine Zeit in Minuten an, um welche die Ausführung eines CRON-Jobs gegenüber der definierten Startzeit maximal verzögert wird. Die tatsächliche Verzögerungszeit wird zufällig ermittelt und liegt zwischen Null und der hier eingetragenen Zeit.

□ Default: 0

□ Mögliche Werte: 0 bis 65535 Sekunden

□ Besondere Werte: Bei einer Variation von Null wird der CRON-Job exakt zur definierten Zeit ausgeführt.

Echtzeit-basierte Regel können nur ausgeführt werden, sofern das Gerät über einen gültigen Zeitbezug verfügt, also z.B. via NTP.

Beispiele:

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@mylancom.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

- Der erste Eintrag trennt jeden Morgen um 4:00 Uhr die Verbindung zum Internetprovider (Zwangstrennung).
- Der zweite Eintrag sendet jeden Morgen um 3:59, 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.

Zeitgesteuerte Regeln werden mit einer Genauigkeit von einer Minute ausgeführt.
Bitte beachten Sie, dass die Sprache der eingetragenen Befehle zur eingestellten Konsolensprache passt, da ansonsten die Kommandos der Zeitautomatik nicht beachtet werden. Die Defaultsprache Englisch kann dazu bei Bedarf auf Deutsch umgestellt werden ('Die Sprache der Konsole auf Deutsch ändern' → Seite 35).

16.8 PPPoE-Server

16.8.1 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.

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

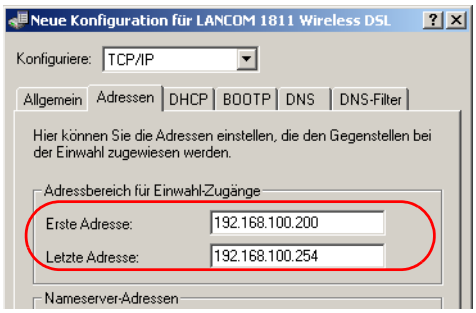
16.8.2 Anwendungsbeispiel

Alle Mitarbeiter der Abteilung 'Einkauf' müssen sich per PPPoE erst am LANCOM authentisieren (IP-Routing, Prüfung mit PAP), damit sie auf das Internet zugreifen dürfen.

Randbedingung: Das LANCOM ist als Router, Firewall und Gateway für die Benutzer im LAN direkt zu erreichen, d.h. es sind keine weiteren Router dazwischengeschaltet.

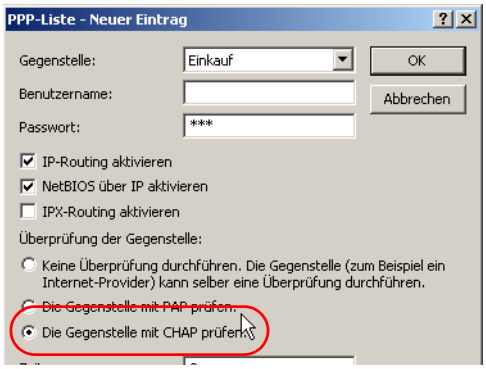
Die Rechner im Einkauf bekommen über die Liste der Adressen für Einwahlzugänge (LANconfig ▶ TCP/IP ▶ Adressen) eine IP-Adresse aus einem bestimmten Adressbereich zugewiesen (z.B. 192.168.100.200 bis 192.168.100.254).

Das LANCOM selbst steht dabei in einem anderem IP-Adressbereich!

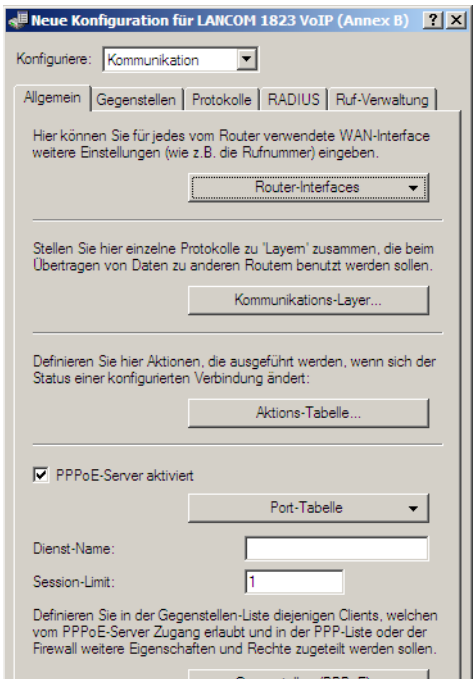


Damit die Anwender die Authentifizierung nicht umgehen können, wird in der Firewall eine DENY-ALL-Regel angelegt, die alle lokalen Verbindungen unterbindet.

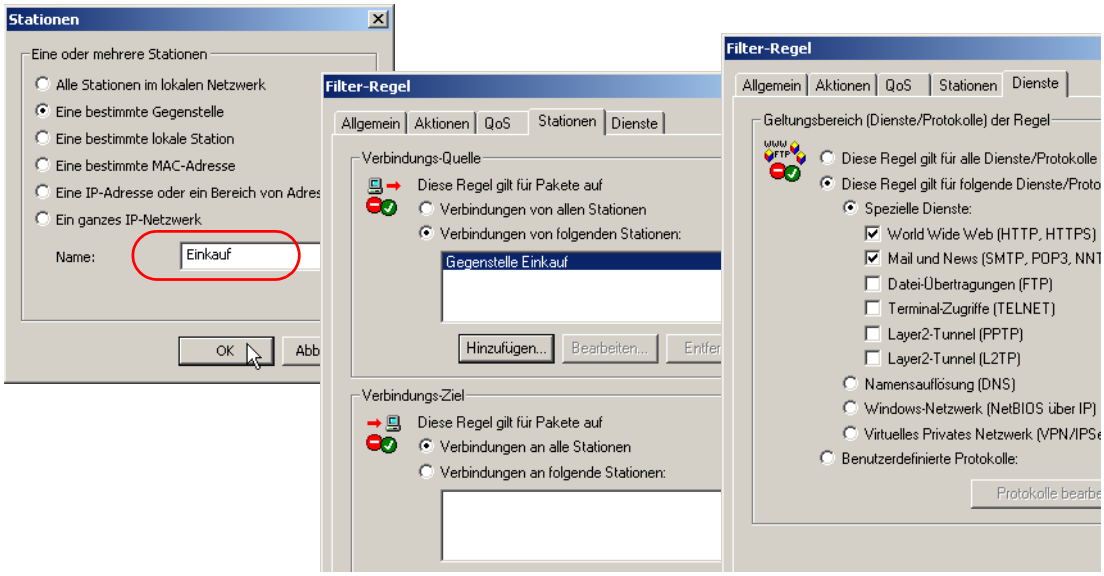
Dazu wird der Benutzer 'Einkauf' als Gegenstelle ohne Benutzername, aber mit einem gemeinsamen Kennwort für alle Mitarbeiter in der Abteilung in der PPP-Liste angelegt (LANconfig ▶ Kommunikation ▶ Protokolle) und die Authentifizierung (verschlüsselt) über CHAP vorgegeben. Für diesen PPP-Benutzer werden sowohl IP-Routing als auch NetBIOS (Windows Networking) aktiviert:



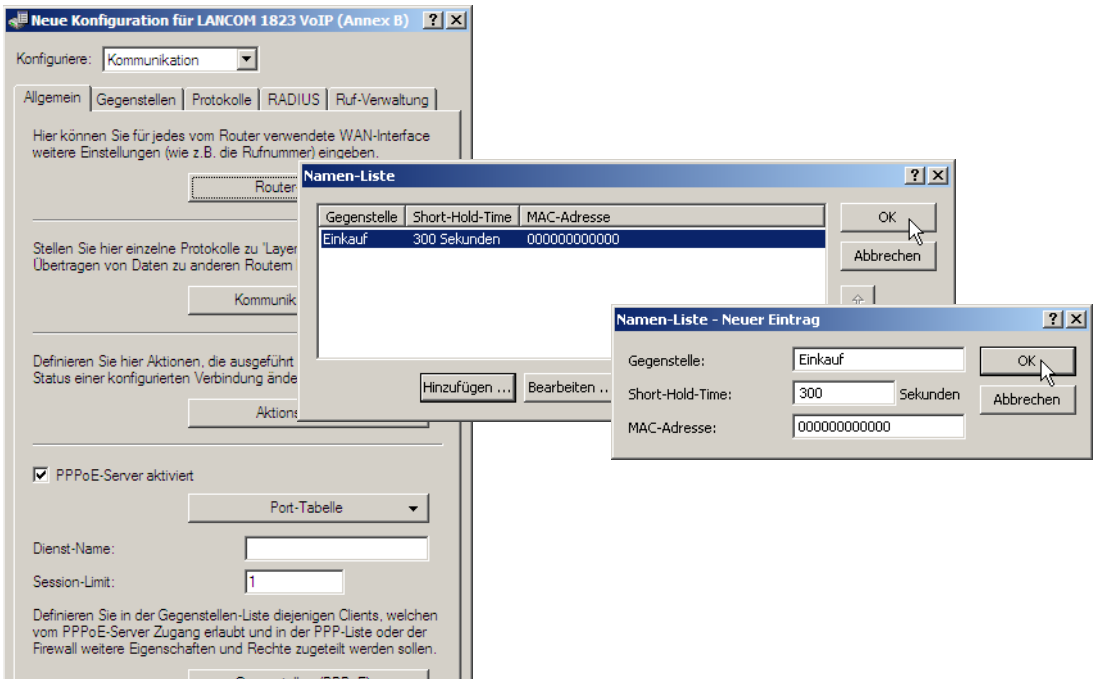
Neben der Aktivierung des PPPoE-Servers (LANconfig ▶ Kommunikation ▶ Allgemein) können weitere Einschränkungen (z.B. auf die erlaubten MAC-Adressen) ebenfalls im PPPoE-Server definiert werden. Dieses Beispiel nutzt aber den dort vorhandenen Eintrag 'DEFAULT' mit der MAC-Adresse '00.00.00.00.00.00', so dass alle MAC-Adressen erlaubt sind.



Mit Hilfe der Firewall (LANconfig ▶ Firewall/QoS ▶ Regeln) können die erlaubten Dienste für die Mitarbeiter des Einkaufs gesteuert werden (z.B. nur Freischalten von HTTP und EMAIL).



16.8.3 Konfiguration



LANconfig: Kommunikation ▶ Allgemein

WEBconfig: LCOS-Menübaum ▶ Setup ▶ PPPoE-Server

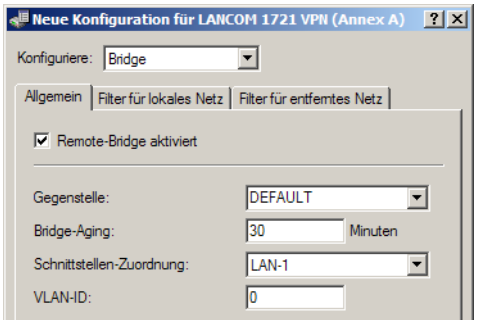
- **Operating**: Mit dem Schalter 'Operating' wird der Server ein- bzw. ausgeschaltet. Defaultwert ist 'Aus'. Der PPPoE-Server kann für jedes logische Interface getrennt aktiviert oder deaktiviert werden.
- **Service**: Unter 'Service' wird der Name des angebotenen Dienstes eingetragen. Das ermöglicht einem PPPoE-Client die Auswahl eines bestimmten PPPoE-Servers, der dazu beim Client eingetragen wird.
- **Session-Limit**: Das 'Session-Limit' gibt an, wie oft ein Client mit der gleichen MAC-Adresse gleichzeitig angemeldet sein kann. Ist das Limit erreicht, dann antwortet der Server nicht mehr auf empfangene Anfragen des Clients. Defaultwert ist '1', Maximalwert '99'. Ein Session-Limit von '0' steht für eine unbegrenzte Session-Anzahl.
- **Namenliste**: In der Namenliste können Benutzern verschiedene Parameter (z.B. Shorthold-Time und MAC-Adresse) zugeordnet werden.

Eine MAC-Adresse von '000000000000' bedeutet, dass sich der Benutzer mit einer beliebigen MAC-Adresse anmelden darf. Ist eine MAC-Adresse eingetragen, so wird die PPP-Verhandlung abgebrochen, wenn sich der User von einer anderen MAC-Adresse anmeldet. Nach der Anmeldung wird die Shortholdzeit des Benutzers gesetzt. Existiert kein Eintrag, so wird die des Users 'DEFAULT' verwendet.

Zusätzlich zu dieser Tabelle muss ein Eintrag in der PPP-Tabelle vorgenommen werden, in dem das Passwort, die Rechte (IP, IPX, NetBIOS) und sonstige PPP-Parameter (LCP-Polling etc.) eingetragen werden. Der Benutzer kann daher auch über einen RADIUS-Server authentifiziert werden.

16.9 Remote-Bridge

Über die Remote-Bridge werden zwei entfernte Netzwerke so miteinander gekoppelt, als wären sie physikalisch verbunden. Sie sind völlig unabhängig von den eingesetzten Netzwerkprotokollen.



LANconfig: Bridge ▶ Allgemein

WEBconfig: LCOS-Menübaum > Setup > Bridge

- **Gegenstelle**
  Name der Gegenstelle, an welche die Remote-Bridge gebunden ist
- **Bridge-Aging**
  Zeit nach der eine einmal gelernte MAC-Adresse wieder gelöscht wird
- **Schnittstellen-Zuordnung**
  Logisches Interface, dem die Remote-Bridge zugeordnet wird.

Bei der Schnittstellenzuordnung sind WLANs nicht möglich, da die WAN-Bridge nur in Geräten ohne WLAN vorhanden ist. Daher ist auch die Schnittstellenzuordnung "beliebig" nicht möglich.

- **VLAN-ID**
  ID des VLANs, auf dem die Remote-Bridge aktiv sein soll.

16.10 RADIUS

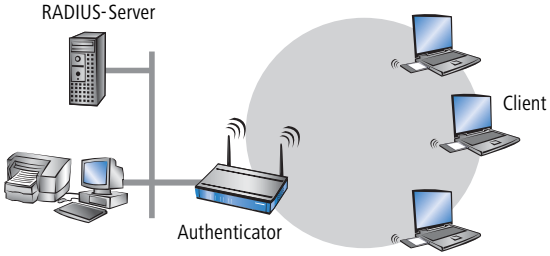
RADIUS steht für „Remote Authentication Dial-In User Service“ und wird als „Triple-A-Protokoll“ bezeichnet. Dabei stehen die drei „A“ für

- 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.

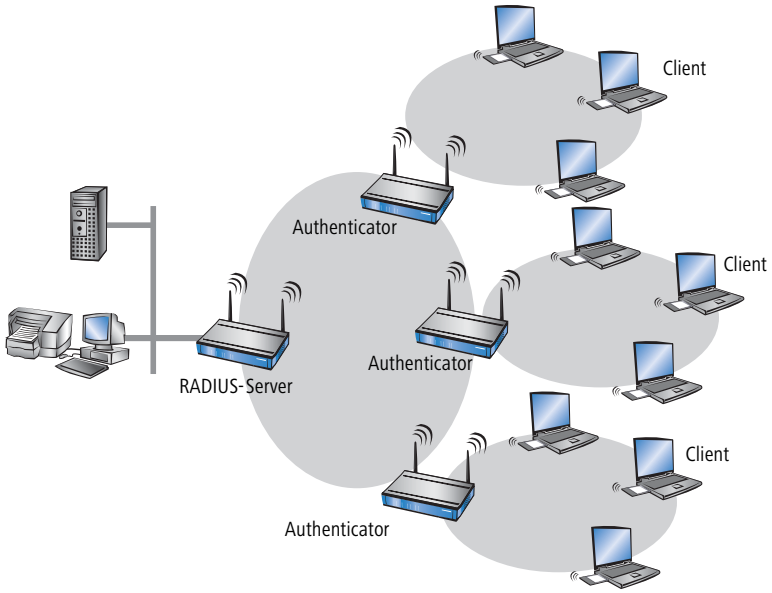
Damit RADIUS funktioniert, sind 3 verschiedene Geräte nötig.

- 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 LANCOM 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 Authen-

ticator erreichbar. Auch für diese Aufgabe kann in entsprechenden Szenarien ein LANCOM Access Point eingesetzt werden.



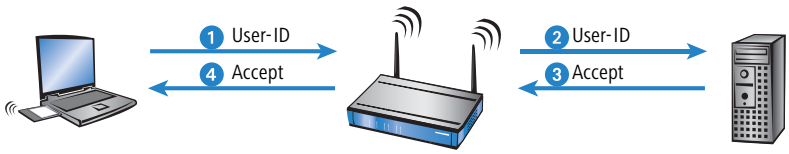
Der Authenticator hat zunächst keine Informationen über die Clients, die sich anmelden wollen. Diese sind alle in einer Datenbank des RADIUS-Servers gespeichert. Welche Anmeldeinformationen der RADIUS-Server für die Authentifizierung benötigt, ist dort in der Datenbank hinterlegt und kann von Netzwerk 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:

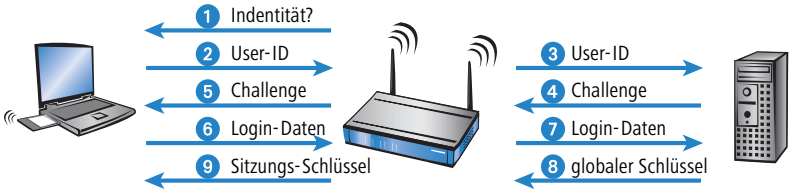
- Über PPP bei der Einwahl in ein Netzwerk ('Einwahl über PPP und RADIUS' → Seite 30)
- Über WLAN ('Einwahl über WLAN und RADIUS' → Seite 31)
- Über einen Public Spot für Benutzer, die sich per Browser anmelden ('Einwahl über einen Public Spot und RADIUS' → Seite 32
- über das 802.1x-Protokoll ('Einwahl über 802.1x und RADIUS' → Seite 32)

16.10.1 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:

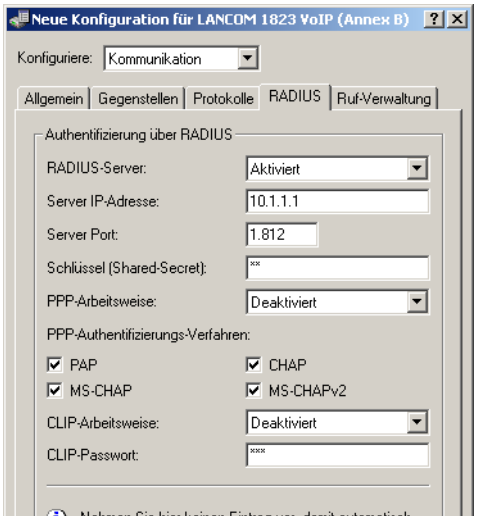


16.10.2 Konfiguration von RADIUS als Authenticator bzw. NAS

Das RADIUS-Protokoll wird von LANCOM-Geräten in unterschiedlichen Anwendungsfällen unterstützt. Für jeden dieser Fälle gibt es einen eigenen Satz von Parameter, 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.

Allgemeine Einstellungen

Die allgemeinen Einstellungen gelten für alle RADIUS-Anwendungen. Die Default-Werte sind so gewählt, dass sie im Normalfall nicht geändert werden müssen.



LANconfig: Kommunikation ▶ RADIUS

WEBconfig: LCOS-Menübaum ▶ Setup ▶ RADIUS-Modul

- **Timeout [Default: 5.000]**

  Dieser Wert gibt an, nach wievielen Millisekunden eine erneute RADIUS-Authentifizierung versucht werden soll.

Bitte beachten Sie bei der PPP-Authentifizierung über RADIUS, dass das einwählende Gerät den hier konfigurierten RADIUS-Timeout akzeptiert.

- **Wiederholungen [Default: 3]**

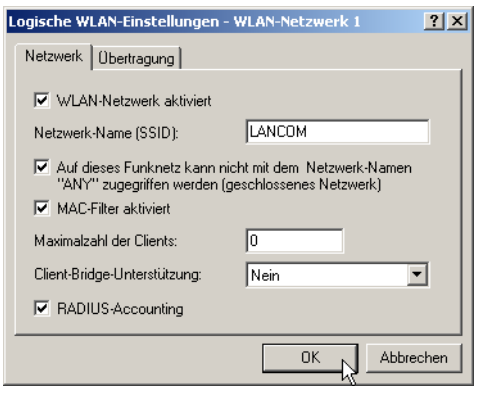
  Dieser Wert gibt an, wieviele Authentifizierungs-Versuche insgesamt durchgeführt werden, bevor eine Ablehnung erfolgt.

RADIUS-Accounting

Für ein logisches WLAN-Netzwerk kann ein Accounting über einen RADIUS-Server aktiviert werden. Dazu wird für das Netzwerk in den logischen WLAN-Einstellungen die Option „RADIUS-Accounting“ aktiviert.

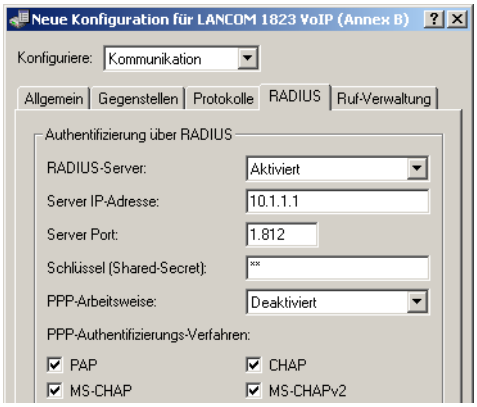
LANconfig: Interfaces ▶ Wireless LAN ▶ logische WLAN-Einstellungen

WEBconfig: LCOS-Menübaum ▶ Setup ▶ RADIUS-Modul



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.



LANconfig: Kommunikation ▶ RADIUS

WEBconfig: LCOS-Menübaum ▶ Setup ▶ WAN ▶ RADIUS

■ **Radius-Server [Default: deaktiviert]**

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.
- □ 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.

■ **Server IP-Adresse**

Geben Sie hier die IP-Adresse Ihres RADIUS-Servers an, mit dem Sie zentral die Benutzer verwalten.

■ **Server Port [Default: 1.812]**

Geben Sie hier den Port an, über den Sie mit Ihrem RADIUS-Server kommunizieren.

■ **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.

■ **PPP-Arbeitsweise [Default: deaktiviert]**

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.
- □ 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. die erlaubten Protokolle IP, IPX und/oder NetBIOS).

■ **CLIP-Arbeitsweise [Default: deaktiviert]**

Bei der Einwahl über PPP kann zur Steuerung eines Rückrufs ein RADIUS-Server genutzt werden.

- □ Deaktiviert: Die Rückruf-Funktion wird nicht über RADIUS gesteuert, es werden **ausschließlich** die Einträge der Namenliste verwendet.
- □ Aktiviert: Die RADIUS-Funktion für den Rückruf ist eingeschaltet. Die von den Clients gemeldete Rufnummer wird **zuerst** über die Namenliste geprüft. Ist in der Namenliste kein passender Eintrag vorhanden, dann wird

die Rufnummer über den RADIUS-Server geprüft. Verläuft die Prüfung in Namenliste **oder** RADIUS-Server positiv, kann ein Rückruf aufgebaut werden.

Wenn die übermittelte Rufnummer in der Namenliste enthalten ist, dort aber kein Rückruf aktiv ist, erfolgt keine weitere Prüfung über RADIUS.

□ Exklusiv: Die RADIUS-Funktion für den Rückruf ist eingeschaltet. Die von den Clients gemeldete Rufnummer wird **ausschließlich** über den RADIUS-Server geprüft.

Zur Nutzung der Rückrufsteuerung über RADIUS muss im RADIUS-Server für jede zu authentifizierende Rufnummer ein Benutzer angelegt werden, dessen Name der Rufnummer entspricht, und der als Passwort das hier angegebene CLIP-Passwort hat.

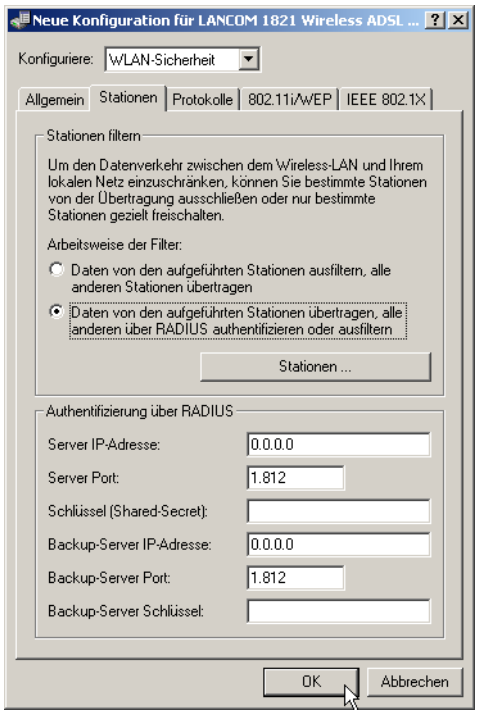
■ **CLIP-Passwort**

Passwort für die Rückrufsteuerung.

Die allgemeinen Werte für Wiederholung und Timeout müssen ebenfalls konfiguriert werden (s. 'Konfiguration von RADIUS als Authenticator bzw. NAS' → Seite 28). Sie sind bei PPP auf der gleichen Seite wie die PPP-Parameter zu finden.

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.



LANconfig: WLAN-Sicherheit ▶ Stationen

WEBconfig: LCOS-Menübaum ▶ Setup ▶ WLAN ▶ RADIUS -Zugriffsprüfung

Zur Nutzung der RADIUS-Funktion für WLAN-Clients muss für den Parameter „Stationen filtern" die Option „Daten von den aufgeführten Stationen übertragen, alle anderen über RADIUS authentifizieren" ausgewählt sein.

■ **Server IP-Adresse**

Geben Sie hier die IP-Adresse Ihres RADIUS-Servers an, mit dem Sie zentral die Benutzer verwalten.

■ **Server Port [Default: 1.812]**

Geben Sie hier den Port an, über den Sie mit Ihrem RADIUS-Server kommunizieren.

■ **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.

■ **Backup-Server IP-Adresse [Default: 1.812]**

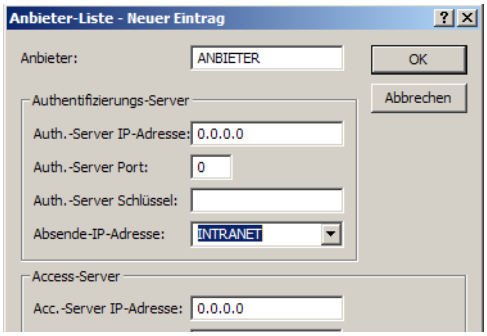
Geben Sie hier die IP-Adresse Ihres Backup-RADIUS-Servers an, mit dem Sie zentral die Benutzer verwalten.

- **Backup-Server Port**
  Geben Sie hier den Port an, über den Sie mit Ihrem Backup-RADIUS-Server kommunizieren.
- **Backup-Schlüssel**
  Geben Sie hier den Schlüssel an, mit dem die Kodierung der Daten vorgenommen werden soll. Der Schlüssel muss ebenfalls im Backup-RADIUS-Server konfiguriert sein.

Die allgemeinen Werte für Wiederholung und Timeout müssen ebenfalls konfiguriert werden (s. 'Konfiguration von RADIUS als Authenticator bzw. NAS' → Seite 28)

Einwahl über einen Public Spot und RADIUS

Bei der Konfiguration eines Public-Spot (Aktivierung über Software-Option für die LANCOM Access Points) 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 LANCOM Access Point nicht wichtig, da diese Daten transparent an den RADIUS-Server weitergereicht werden.



LANconfig: Public-Spot ▶ Public-Spot-Benutzer ▶ Anbieter-Liste

WEBconfig: LCOS-Menübaum ▶ Setup ▶ WLAN ▶ Radius-Accounting

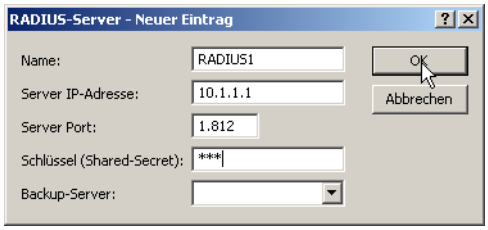
- **Anbieter**
  Name des Anbieters, für den der RADIUS-Server definiert werden soll.
- **Auth. Server IP-Adresse**
  Die IP-Adresse des RADIUS-Servers für diesen Anbieter an.
- **Auth.-Server Port**
  Der Port, über den der LANCOM Access Point mit dem RADIUS-Server für diesen Anbieter kommunizieren kann.
- **Auth. Server Schlüssel**
  Schlüssel (Shared Secret) für den Zugang zum RADIUS-Server des Anbieters. Der Schlüssel muss ebenfalls im entsprechenden RADIUS-Server konfiguriert sein.
- **Acc. Server IP-Adresse**
  IP-Adresse des Accounting-Servers für die Zugänge zum Public-Spot.
- **Acc.-Server Port**
  Der Port, über den der LANCOM Access Point mit dem Accounting-Server kommunizieren kann.
- **Acc Server Schlüssel**
  Schlüssel (Shared Secret) für den Zugang zum Accounting-Server. Der Schlüssel muss ebenfalls im Accounting-Server konfiguriert sein.
- **Backup**
  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 (s. 'Konfiguration von RADIUS als Authenticator bzw. NAS' → Seite 28)

Einwahl über 802.1x und RADIUS

WLAN-Clients können sich über das 802.1x-Protokoll in ein Netzwerk anmelden. Der LANCOM Access Point kann die Anmeldung über dieses Protokoll an den RADIUS-Server weiterleiten. Die MAC-Adresse wird zur Identifizierung der Benutzer verwendet.

Weitere Informationen über das 802.1x-Protokoll finden Sie unter 'EAP und IEEE 802.1x' → Seite 20.



LANconfig: WLAN-Sicherheit ▶ IEEE 802.1X ▶ RADIUS-Server

WEBconfig: LCOS-Menübaum ▶ Setup ▶ IEEE802.1x ▶ 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 IP-Adresse**

  Geben Sie hier die IP-Adresse Ihres 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.

- **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.

- **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 (s. 'Konfiguration von RADIUS als Authenticator bzw. NAS' → Seite 28)

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.

16.10.3 Konfiguration von RADIUS als Server

Neben der Funktion als RADIUS-Authenticator oder NAS kann ein LANCOM 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.

Parameter des RADIUS-Servers

Zur Konfiguration des RADIUS-Servers wird definiert, 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 Authenticator.

LANconfig: WLAN-Sicherheit ▶ RADIUS

WEBconfig: LCOS-Menübaum ▶ Setup ▶ Radius ▶ Server

- **Authentifizierungs-Port [Default: 0]**

  Geben Sie hier den Port an, über den die Authenticator mit dem RADIUS-Server im LANCOM Access Point kommunizieren. Üblicherweise wird der Port '1812' verwendet.

  Der Port '0' schaltet den RADIUS-Server aus.

Neben dem Port können bis zu 16 Authenticator eingetragen werden, die mit dem RADIUS-Server kommunizieren können. Die Einträge werden in der entsprechenden Tabelle mit folgenden Parametern vorgenommen:

- **IP-Adresse**

  IP-Adresse des Authenticators, der mit dem RADIUS-Server im LANCOM Access Point kommunizieren darf.

- **Secret**

  Kennwort, das der Authenticator für den Zugang zum RADIUS-Server im LANCOM Access Point benötigt.

Neben der Konfiguration des RADIUS-Servers muss die Quelle für die Client-Informationen festgelegt werden 'WLAN-Zugangsliste als Basis für RADIUS-Informationen' → Seite 34.

WLAN-Zugangsliste als Basis für RADIUS-Informationen

In der Zugangsliste können 512 WLAN-Clients eingetragen werden, die sich an einem LANCOM 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.

LANconfig: WLAN-Sicherheit ▶ RADIUS

WEBconfig: LCOS-Menübaum ▶ Setup ▶ WLAN ▶ RADIUS-Zugriffspruefung

- **Server-Datenbank verwenden [Default: ja]**

  Dieser Parameter gibt an, ob die WLAN-Zugangsliste als Informationsquelle für den RADIUS-Server im LANCOM 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.

- **Prüfzyklus [Default: 0]**

  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.

Ein Prüfzyklus von '0' schaltet die regelmäßige Prüfung aus, die WLAN-Clients bleiben solange angemeldet, bis sie sich selbst abmelden.

16.11 Erweiterungen im RADIUS-Server

16.11.1 Neue Authentifizierungs-Verfahren

Bis zu Version 6.30 unterstützt der LCOS-RADIUS-Server nur PAP als Authentifizierungsverfahren, d.h. der RADIUS-Client (im Weiteren als NAS bezeichnet – Network Access Server) übermittelt den Benutzernamen und das Passwort, der Server beantwortet diese Anfrage mit einem Access- Accept oder Access-Reject. Dieses Verfahren ist allerdings nur eine Möglichkeit aus einer Reihe von Authentifizierungsverfahren, die über RADIUS abgewickelt werden können. Mit der LCOS-Version unterstützt der RADIUS-Server im LANCOM weitere Authentifizierungsverfahren:

- 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.
- MS-CHAP: 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).
- MS-CHAPv2: 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.

16.11.2 EAP-Authentifizierung

EAP ist kein festes Authentifizierungsverfahren sondern es bietet einen Rahmen für beliebige Authentifizierungsverfahren. Der LCOS-RADIUS-Server unterstützt eine Reihe von EAP-Verfahren:

- EAP/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.
- EAP/MSCHAPv2, definiert in draft-kamath-pppext-eap-mschapv2-01.txt. 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.
- EAP/TLS, definiert in RFC2716. Der Einsatz von EAP/TLS erfordert ein Root-Zertifikat, eine 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.

- EAP/TTLS, definiert in draft-ietf-pppext-eap-ttls-05.txt. 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
- EAP/PEAPv0, definiert in draft-kamath-pppext-peapv0-00.txt. 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.

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.

16.11.3 RADIUS-Forwarding

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-Servers 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. Sofern es definiert ist, wird der Realm über ein @-Zeichen getrennt an den Benutzernamen angehängt in der Form:

```
benutzer@realm
```

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:

- Default-Realm: Dieser Realm wird verwendet, wenn ein Realm übermittelt wird, für den kein expliziter Forwarding-Server definiert ist. Für den Default-Realm selbst muss in der Weiterleitungs-Tabelle allerdings ein entsprechender Eintrag angelegt werden.
- Leer-Realm: Dieser Realm wird verwendet, wenn **kein** Realm, sondern nur der Benutzername übermittelt wird.

Im Default-Zustand enthält die Weiterleitungs-Tabelle keine Einträge, der Default- und der Leer-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 Default- und der Leer-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.

16.11.4 Parameter des RADIUS-Servers

Zur Konfiguration des RADIUS-Servers wird definiert, welche Clients auf den RADIUS-Server zugreifen dürfen (inklusive Kennwort) und über welchen UDP-Port die Clients mit dem RADIUS-Server kommunizieren können. Der Authentifizierungs-Port gilt dabei global für alle Clients.

WEBconfig: LCOS-Menübaum ▶ Setup ▶ Radius ▶ Server

Globale Einstellungen für den RADIUS-Server

- **Authentifizierungs-Port [Default: 0]**

  Geben Sie hier den Port an, über den die Authenticator mit dem RADIUS-Server im LANCOM Access Point kommunizieren. Üblicherweise wird der Port '1812' verwendet.

  □ Der Port '0' schaltet den RADIUS-Server aus.
- **Default-Realm**

  Dieser Realm wird verwendet, wenn der übermittelte Benutzername einen **unbekannten** Realm verwendet, der nicht in der Liste der Weiterleitungs-Server enthalten ist.
- **Empty-Realm**

  Dieser Realm wird verwendet, wenn der übermittelte Benutzername **keinen** Realm enthält.

RADIUS-Clients

In der Clients-Tabelle können bis zu 16 Clients eingetragen werden, die mit dem RADIUS-Server kommunizieren können.

- **IP-Adresse**

  Tragen Sie hier die IP-Adresse des Clients ein, der mit dem RADIUS-Server im LANCOM Access Point kommunizieren darf.
- **Secret**

  Kennwort, das der Client für den Zugang zum RADIUS-Server im LANCOM Access Point benötigt.



Neben der Konfiguration des RADIUS-Servers muss die Quelle für die Benutzer-Informationen festgelegt werden.

RADIUS-Benutzer

In der Benutzer-Tabelle können bis zu 64 Benutzer eingetragen werden, die über den RADIUS-Server ohne weitere Datenbanken authentifiziert werden können. Diese Benutzer-Tabelle wird für lokale Anfragen an den RADIUS-Server verwendet, also für Anfragen mit Benutzernamen ohne Realm.

- **Benutzername**

  Name des Benutzers.

- **Passwort**
  Passwort des Benutzers.
- **Limitierte Auth-Methoden**
  Mit dieser Option können die für den Benutzer erlaubten Authentifizierungsverfahren eingeschränkt werden.
  - Mögliche Werte: PAP, CHAP, MSCHAP, MSCHAPv2, EAP, Alle
  - Default: Alle

Weiterleitungs-Server

In der Tabelle der Weiterleitungs-Server werden bis zu 16 Realms mit den zugehörigen Weiterleitungs-Zielen eingetragen.

- **Realm**
  Zeichenkette, mit der das Weiterleitungs-Ziel identifiziert wird.
- **IP-Adresse**
  IP-Adresse des RADIUS-Servers, an den die Anfrage weitergeleitet werden soll.
- **Port**
  Offener Port, über den mit dem Weiterleitungs-Server kommuniziert werden kann.
- **Secret**
  Kennwort, das für den Zugang zum Weiterleitungs-Server benötigt wird.
- **Backup**
  Alternativer Weiterleitungs-Server, an den Anfragen weitergeleitet werden, wenn der erste Weiterleitungs-Server nicht erreichbar ist.

EAP-Optionen für den RADIUS-Server

- **EAP-Tunnel-Server**
  Realm als Verweis auf den Eintrag in der Tabelle der Weiterleitungs-Server, der für getunnelte TTLS bzw. PEAP-Anfragen verwendet werden soll.
- **TLS-Pruefe-Benutzernamen**
  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 in der RADIUS-Benutzertabelle enthalten ist.

16.12 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.

16.12.1 Konfiguration von RADSEC für den Client

LANCOM als RADIUS-Client

In der Funktion als RADIUS-Client wird ein LANCOM 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.

Diese Einstellungen werden an allen Stellen vorgenommen, an denen ein LANCOM als RADIUS-Client konfiguriert wird:

WEBconfig: **Setup ▶ WAN ▶ RADIUS**

WEBconfig: **Setup ▶ WLAN ▶ RADIUS-Zugriffspruefung**

WEBconfig: **Setup ▶ WLAN ▶ RADIUS-Accounting**

WEBconfig: **Setup ▶ Public-Spot-Modul ▶ Anbieter-Tabelle**

WEBconfig: **Setup ▶ IEEE802.1x ▶ RADIUS-Server**

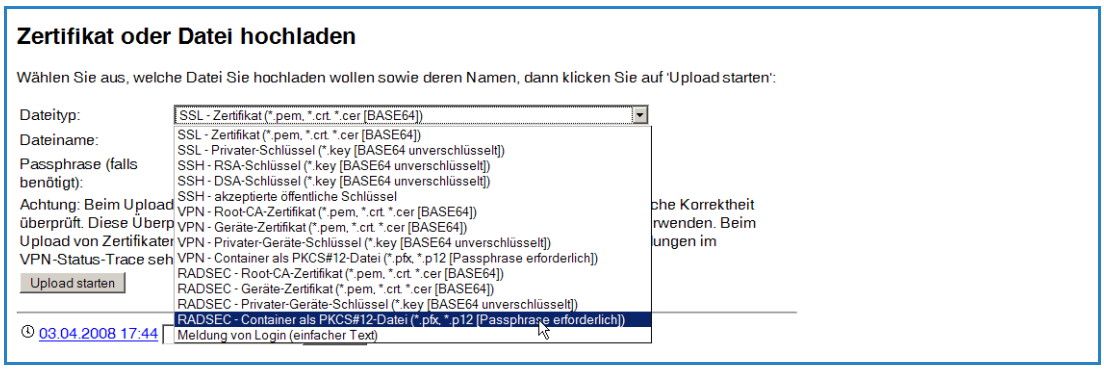
LANCOM als RADIUS-Server

Arbeitet ein LANCOM 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. RADIUS für die Clients im LAN, die zuverlässigere RADSEC-Variante über TCP für externe Anmeldungen über das Internet eingesetzt werden.

16.12.2 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**



16.13 Betrieb von Druckern am USB-Anschluss des LANCOM

Über den bei verschiedenen Modellen vorhandenen USB-Port können Drucker an das LANCOM angeschlossen und so im gesamten Netzwerk verfügbar gemacht werden. Das LANCOM 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 LANCOM arbeitet die anliegenden Aufträge nacheinander ab.

16.13.1 Konfiguration des Printservers im LANCOM

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.

Druckertabelle

Die Druckertabelle enthält die Einstellungen für die angeschlossenen Drucker.

WEBconfig: LCOS-Menübaum ▶ Setup ▶ Drucker ▶ 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.

- **Drucker [Default: *]**

  Der Name des Druckers.

- **RawIP-Port [Default: 9100]**

  Über diesen Port können Druckaufträge über RawIP angenommen werden.

RawIP wird von Windows als Standard verwendet und kann für den Betrieb von Druckern am USB-Port empfohlen werden.

- **LDP-Port [Default: 515]**

  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.

- **Aktiv [Default: Nein]**
  - □ Ja: Der Printserver ist aktiv.
  - □ Nein: Der Printserver ist nicht aktiv.
- **Bidirektional [Default: Nein]**
  - □ Ja: Das LANCOM versendet die Statusinformationen des Druckers in regelmäßigen Abständen an die angeschlossenen Rechner.
  - □ Nein: Das LANCOM versendet keine Statusinformationen.

Zugangs-Liste

In der Zugangsliste werden bis zu 16 Netzwerke eingetragen, die Zugriff auf die konfigurierten Drucker haben.

LANconfig: Drucker ▶ Allgemein ▶ Zugangsliste

WEBconfig: LCOS-Menübaum ▶ Setup ▶ Drucker ▶ Zugangs-Liste

- **IP-Adresse**
  IP-Adresse des Netzwerks, dessen Clients Zugriff auf den Drucker haben dürfen.
- **Netzmaske**
  Netzmaske zu den erlaubten Netzwerken.

Wenn die Zugangsliste keine Einträge enthält, können Rechner mit beliebigen IP-Adressen einen Drucker am USB-Port des LANCOM nutzen.

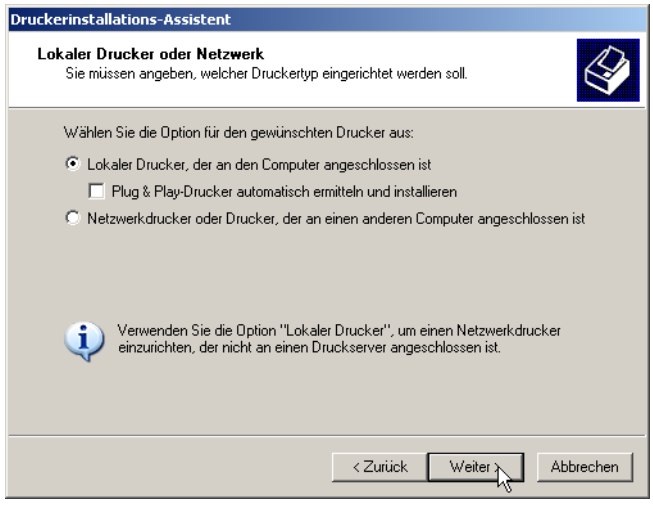
Der Zugang zu einem Drucker am USB-Port des LANCOM über das WAN ist aus Sicherheitsgründen grundsätzlich nicht möglich.

16.13.2 Konfiguration der Drucker auf dem Rechner

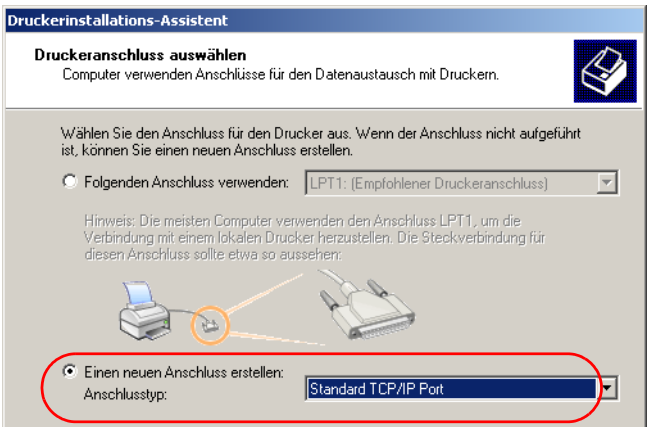
Zur Nutzung des Druckers am USB-Port über das Netzwerk muss auf den Rechnern der Druckertreiber mit einem entsprechenden Druckeranschluss verbunden werden. Die nachfolgende Beschreibung zeigt die Einrichtung unter Windows XP, die Konfiguration unter Windows 2000 verläuft sehr ähnlich. Ältere Windows-Versionen 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.

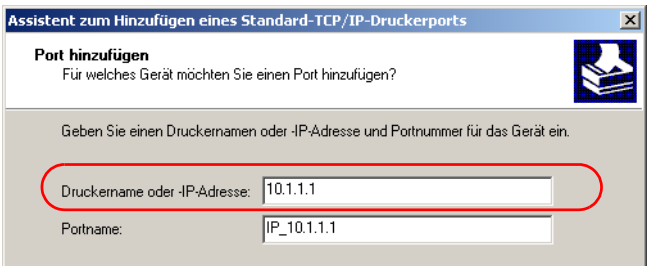
② Wählen Sie die Option für einen lokalen Drucker und deaktivieren Sie den Plug and Play-Mechanismus.



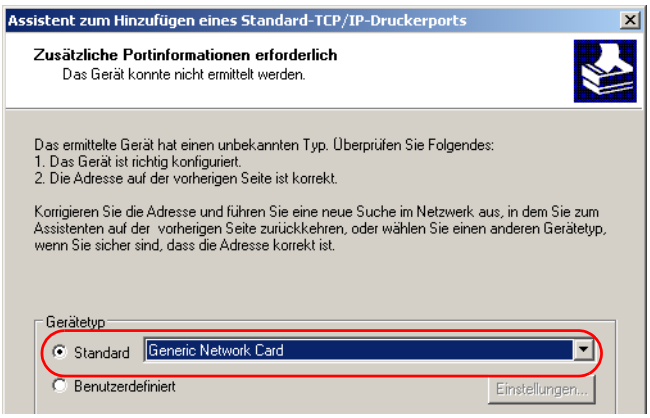
③ Wählen Sie die Option zum Erstellen eines neuen Druckeranschlusses.



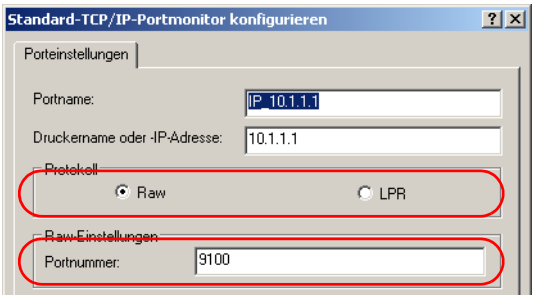
④ Geben Sie die IP-Adresse des LANCOM als IP-Adresse für den Druckeranschluss ein. Der Name des Druckeranschlusses wird automatisch mit 'IP_<IP-Adresse des LANCOM>' vorbelegt.



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.



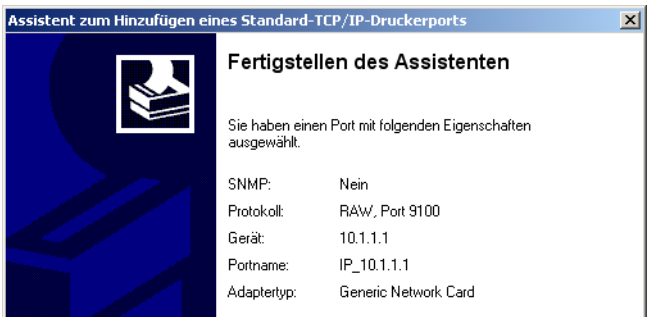
⑥ Alternativ können Sie mit der Auswahl 'Benutzerdefiniert' und der Schaltfläche **Einstellungen** einen zusätzlichen Dialog aufrufen. In diesem Dialog können Sie das Protokoll auswählen, das für die Übertragung der Druckaufträge zum Drucker am USB-Port des LANCOM verwendet werden soll ('Raw' – RawIP 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 LANCOM-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.

⑦ 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.

A Anhang

A.1 Fehlermeldungen im LANmonitor

Es besteht die Möglichkeit über den LANmonitor VPN - Fehlermeldungen auszulesen. Diese Fehlermeldungen werden in diesem Dokument aufgelistet, interpretiert und ein Workflow vorgeschlagen.

A.1.1 Allgemeine Fehlermeldungen

Verbindungsaufbau abgebrochen	
Vorgegebenes Gebührenlimit erreicht	
Keine Absenderrufnummer angegeben	
Keine Gegenstelle angegeben	
Gegenstelle doppelt	
Gegenstelle gesperrt	
Keine Gebühreninformationen vorhanden	
Mehrere Verbindungen nicht erlaubt	
Zielrufnummer gesperrt	
Gegenstelle besetzt	
Gegenstelle antwortet nicht	
ICMP Verbindungsfehler	
Keine Antwort	
DHCP-Server hat nicht geantwortet	
PPTP keine Antwort	
VPN-Gegenstelle hat nicht geantwortet	
Default-Gateway hat den ARP-Request nicht beantwortet	
Fehler der Gegenstelle	
Verbindung abgelehnt	
Zielrufnummer geändert	
Gegenstelle nicht bereit	
Rufnummer falsch	
Eigene Leitung besetzt	
Leitung der Gegenstelle besetzt	
Engpaß im Netz	
Eigene Leitung gesperrt	
Dienstmerkmal nicht erlaubt	
Dienst nicht eingerichtet	
Dienstmerkmal nicht eingerichtet	
Gegenstelle nicht kompatibel	
Unspezifizierter Fehler	
Verbindungsaufbau fehlgeschlagen (D-Kanal Layer 1)	Bus-Aktivierung fehlgeschlagen
Verbindungsaufbau fehlgeschlagen (D-Kanal Layer 2)	kein UA auf SABME
Verbindungsaufbau fehlgeschlagen (Layer 1)	a/b-Ports
Verbindungsaufbau fehlgeschlagen (Layer 2)	a/b-Ports
ISDN Leitungsfehler (Layer 1)	Kabel nicht gesteckt
Fehler Signalisierungkanal (D-Kanal Layer 2)	
Fehler Signalisierungskanal (D-Kanal Layer 3)	
Verbindungsabbruch (Layer 2)	X.75 / V.110
Vermittlungsstelle antwortet nicht	
Dienstmerkmal nicht unterstützt	

Verbindungsaufbau abgebrochen	
Eingestellter Kommunikationslayer passt nicht zur Schnittstelle"	
Lokaler Fehler	Angeforderte Ressource nicht verfügbar -> ISDN-Problem, TK-Anlage booten
Fehler Signalisierungskanal (D-Kanal Layer 3)	
Unzulässige Call Reference	
LCP abgelehnt	
Authentifizierung fehlgeschlagen (Username oder Passwort falsch)	
Authentifizierungsanforderung abgelehnt	
LCP Verbindungs-Fehler	
PPP Anmeldung bei Gegenstelle - PAP abgelehnt	Gegenstelle kann nur PAP, es ist aber CHAP gefordert
PPP Anmeldung von Gegenstelle - Timeout (PPP-PAP RX)	Gegenstelle hat PAP-Request nicht gesendet
PPP Anmeldung bei Gegenstelle - Timeout (PPP-PAP TX)	Gegenstelle hat PAP-Requests nicht beantwortet
PPP Anmeldung von Gegenstelle - Passwort falsch (PPP-PAP RX)	
PPP Anmeldung - Gegenstelle hat Einwahl abgelehnt (PAP-NAK empfangen), weitere Infos im PPP-Trace (Embedded-Message des PAP-NAK)	
PPP Anmeldung von Gegenstelle - CHAP abgelehnt	auf ein CHAP-Challenge wird ein CHAP-Reject empfangen
PPP Anmeldung von Gegenstelle - Timeout (PPP-CHAP RX)	Gegenstelle hat CHAP-Response nicht gesendet
PPP Anmeldung bei Gegenstelle - Timeout (PPP-CHAP TX)	Gegenstelle hat CHAP-Response nicht beantwortet
PPP Anmeldung von Gegenstelle - Username/Passwort falsch (PPP-CHAP)	
PPP Anmeldung bei Gegenstelle - Username/Passwort falsch (PPP-CHAP)	
PPP Anmeldung - CHAP Gegenstelle unbekannt	
IPXCP abgelehnt	
IPXCP-Netzwerk falsch	
IPXCP-Netzwerk abgelehnt	
IPXCP-Route unbekannt	
IPCP abgelehnt	
Datenkompression abgelehnt (PPP-CCP)	
Kein NCP verfügbar	
Vorgegebenes Zeitlimit erreicht	genau wie Gebührenlimit...
Verbindungsaufbau fehlgeschlagen (Layer 1)	keine HDLC-Flags gefunden
Verbindungsaufbau fehlgeschlagen (Layer 2)	X.75 / V.110 funktioniert nicht
DSL Leitungsfehler (Layer 1)	Kabel nicht gesteckt
Dienst nicht verfügbar	
Allgemeiner Fehler	wird so vom Accessconcentrator gemeldet, sollte nie auftreten...
ungültiger Access Concentrator	
Name des Access Concentrators falsch	
Fehler der Gegenstelle	
Ungültige Session-ID	wird so vom Accessconcentrator gemeldet, sollte nie auftreten...
Verbindung wurde von der Gegenstelle getrennt	
Verbindung wurde auf lokaler Seite manuell getrennt	
Shorthold-Timer ist auf lokaler Seite abgelaufen	
Physikalische Verbindung wurde getrennt	
Physikalische Verbindung ist ungültig	
Verbindung wurde von der Gegenstelle getrennt. Die Gegenstelle startete eine neue Dynamic-VPN-Verhandlung	
Lokale Konfiguration der Gegenstelle wurde geändert	
Gegenstelle wurde aus der lokalen Konfiguration entfernt	

A.1.2 VPN-Fehlermeldungen

Zur korrektuen Auswertung der Fehlermeldungen zu VPN-Verbindungen muss auf beiden LANCOM-Geräten mindestens die LCOS-Version 3.22 installiert sein.

Bei einer VPN-Verbindung handelt es sich immer um eine ausgehende oder ankommenden Verbindung. Um die Fehlersuche schneller und effizienter zu machen, werden die Meldungen zwischen einem Initiator und einem Responder unterschieden. Der Initiator ist die Gegenstelle, die die Verbindung iniziiert. Beim Responder handelt es sich um denjenigen, der die Verbindung annimmt. Nachdem die Fehlermeldung ausgelesen wurde, schauen Sie anschließend in dem entsprechenden Menüpunkt auf der jeweiligen Gegenstelle nach.

Beispiel:

Bei der Fehlermeldung 'Zeitüberschreitung während IKE- oder IPSec-Verhandlung (Initiator)' kann kein direktes Fehlerbild entdeckt werden. Der Responder jedoch hat einen Fehler z.B. 'Kein übereinstimmendes Proposal gefunden (Responder, IPSec)' festgestellt, den er mittels eines SNMP-Trap an einem SNMP-Client (LANmonitor) geschickt hat. Anhand dieser Fehlermeldung kann man in der Konfiguration die entsprechenden Parameter kontrollieren und ggf. ändern. Daher ist es immer erforderlich, die Fehlermeldungen auf beiden Seiten zu verifizieren.

Meldung	Initiator	Responder	
Lizenzüberschreitung - keine VPN-Kanäle mehr verfügbar	x	x	Die Anzahl der maximal möglichen VPN - Kanäle wurde erreicht.
Kein Übertragungskanal verfügbar	x	x	
Kein Route zum entfernten Gateway	x	x	Die Router zum entfernten Gateway konnte nicht gefunden werden. Bitte überprüfen Sie die öffentliche IP-Adresse oder den DynDNS Namen der Gegenstelle.
Dynamic VPN - kein passender Eintrag in PPP-Liste vorhanden	x		Beim dynamischen VPN konnte der abgehende Ruf nicht mit den gesendeten PPP - Daten autentifizieren. Bitte gleichen Sie den PPP - Benutzernamen und das PPP - Passwort auf beiden Seiten unter "Konfiguriere --> Kommunikation --> Protokolle --> PPP - Liste --> Gegenstellenname" ab.
Dynamic VPN - kein passender Eintrag in PPP-Liste vorhanden		x	Der eingehende Ruf konnte nicht mit den empfangenen PPP - Daten authentifiziert werden. Bitte gleichen Sie den PPP - Benutzernamen und das PPP - Passwort auf beiden Seiten unter "Konfiguriere --> Kommunikation --> Protokolle --> PPP - Liste --> Gegenstellenname" ab.
Dynamic VPN - Zeitüberschreitung während Signalisierung oder Authentifizierung	x	x	
Zeitüberschreitung während IKE- oder IPSec-Verhandlung	x	x	Es wurde eine Zeitüberschreitung erreicht. Der Router auf der Gegenstelle reagiert nicht mehr. Bitte überprüfen Sie VPN - Fehlermeldung im LANmonitor auf der Gegenstelle.
Leitungsüberwachung (Line Polling) zum entfernten Gateway fehlgeschlagen			Das LCP Polling ist fehlgeschlagen. Bitte überprüfen Sie auf der Gegenseite ob das Ping - Blockieren in dem Firewallmenü unter "Konfiguriere -- > Firewall --> Allgemein --> "Ping Blockieren"
Kein Eintrag in der Pollingtabelle und Keep-Alive ist eingestellt			Die Haltezeit des VPN - Tunnels unter "Konfiguriere --> VPN --> Verbindungs-Liste --> VPN Gegenstellennamen" ist auf Keep - Alive (9999 s) eingestellt. Das erforderliche ICMP Polling fehlt jedoch. Bitte fügen Sie unter "Konfiguriere --> Kommunikation --> Gegenstellen --> " Polling - Tabelle " hinzu. Als Gegenstelle tragen Sie die VPN - Gegenstelle, als IP-Adresse tragen Sie eine IP - Adresse aus dem LAN auf der Gegenstelle.
Dynamic VPN - vorgegebenes Gebührenlimit erreicht	x		Das Gebührenlimit unter "Konfiguriere --> Kosten --> Gebühren - Limit (ISDN)" wurde erreicht. Bitte das Gerät neu booten.
Dynamic VPN - vorgegebenes Zeitlimit erreicht	x		Das Zeitlimit unter "Konfiguriere --> Kosten --> Zeit - Limit (ISDN)" wurde erreicht. Bitte das Gerät neu booten.
Dynamic VPN - keine ISDN Rufnummer für Verhandlungskanal	x		Beim dynamsichen VPN zur VPN Gegenstelle fehlt die ISDN - Rufnummer. Bitte tragen Sie die Rufnummer unter "Konfiguriere --> Kommunikation --> Gegenstellen --> Gegenstelle (ISDN/seriell) --> "Gegenstellenname" " ein.
Dynamic VPN - keine ISDN Gegenstelle für Verhandlungskanal	x		
Dynamic VPN - ISDN Gegenstelle für Verhandlungskanal gesperrt	x		
Dynamic VPN - Mehrere Verbindungen auf ISDN Interface für Verhandlungskanal nicht erlaubt			Beim Aufbau mehrerer ISDN Verbindungen wurde ein Limit erreicht. Bitte überprüfen Sie unter "Konfiguriere --> Management --> Interfaces --> interface - Einstellungen --> ISDN --> max. abgehende Rufe".
Dynamic VPN - ISDN Fehler auf Verhandlungskanal			

Meldung	Initiator	Responder	
Vorgegebenes Gebührenlimit erreicht	x		Das Gebührenlimit wurde erreicht "Konfiguriere --> Management --> Kosten --> Gebührenlimit (ISDN)". Signalisiert durch ein gleichzeitiges blinken der Power LED.
Vorgegebenes Zeitlimit erreicht	x		Das Zeitlimit wurde erreicht "Konfiguriere --> Management --> Kosten --> Zeitlimit (ISDN)". Signalisiert durch ein gleichzeitiges blinken der Power LED.
Keine Rufnummer(	x		
Keine Gegenstelle	x		
Keine IP-Adresse für PPTP Server	x		Die IP - Adresse des einzuwählenden PPTP Servers ist nicht eingetragen. Tragen Sie die IP-Adresse unter "Konfiguriere --> Kommunikation --> Protokolle --> PPTP - Liste".
(2 map vpn_lan) (Initiator) gesperrt	x		
Mehrere Verbindungen auf Interface nach (2 map vpn_lan) nicht erlaubt	x		
ISDN- oder DSL-Fehler auf Interface nach (2 map vpn_lan)			
Exchange type nicht übereinstimmend (Main bzw. Aggressive Mode)		x (IKE)	Der Exchange Type stimmt nicht mit der Gegenstelle überein. Bitte überprüfen Sie den Wert unter "Konfiguriere --> VPN --> Verbindungs - Liste --> VPN-Gegenstelleneintrag editieren --> IKE Exchange"
Kein übereinstimmendes Proposal gefunden	x (IKE)		Die IKE Prposals stimmen nicht überein. -- > VPN Regeln überprüfen
Kein übereinstimmendes Proposal gefunden		x (IKE)	Die IKE Prposals stimmen nicht überein. -- > VPN Regeln überprüfen
IKE Gruppen stimmen nicht überein		x (IKE)	Bitte überprüfen Sie die IKE - Gruppen auf beiden Gegenstellen unter "Konfiguriere --> VPN --> Verbindungs - Parameter --> "VPN Gegenstellenname" --> IKE - Gruppe"
Life type - Angabe wird nicht unterstützt (andere als kByte oder Sekunden?)		x (IKE)	Der Wert für die Gültigkeitsdauer wird nicht unterstützt. Bitte entweder Lifetype in "sec = Sekunden" oder "kb = Kilobyte" verwenden. Überprüfen Sie diese Einstellung unter "Konfiguriere --> VPN --> Parameter --> Gültigkeitsdauer".
Life time - keine übereinstimmenden Angaben		x (IKE)	Die eingestellte Lifetime stimmt nicht mit der Gegenstelle überein. Überprüfen Sie diese Einstellung unter "Konfiguriere --> VPN --> Parameter --> Gültigkeitsdauer".
ID type - Angabe wird nicht unterstützt (andere als IP Netzwerk, Domain oder E-Mail)		x (IKE)	Falsche Eingabe der Identität. Biite korrogieren Sie Ihre Eingabe "Konfiguriere --> VPN --> IKE --> IKE - Schlüssel"
ID type - keine übereinstimmende Angaben (z.B. IP Netzwerk, Domain oder E-Mail)		x (IKE)	Beide Gegenstellen verwenden unterschiedliche Identitäten. Gleichen Sie die Identitäten auf beiden Geegnstellen ab "Konfiguriere --> VPN --> IKE --> IKE - Schlüssel"
Keine Regel für ID gefunden - unbekannte Verbindung oder fehlerhafte ID (z.B. Definition des entfernten Gateways)		x (IKE)	Die eingehende VPN - Verbindung konnte keiner Gegenstelle zugeordnet werden.
IKE Schlüssel stimmen nicht überein	x (IKE)		Überprüfen Sie die Preshared-Keys unter "Konfiguriere --> VPN --> IKE --> IKE - Schlüssel"
IKE Schlüssel stimmen nicht überein		x (IKE)	Überprüfen Sie die Preshared-Keys unter "Konfiguriere --> VPN --> IKE --> IKE - Schlüssel"
Allgemeiner Fehler	x (IKE)		
Nicht genügend Speicher	x (IKE)		Die Anzahl der VPN Verbindungen hat den Speicher des Gerätes ausgelastet. Weitere VPN - Verbindungen sollten aus Stabilitätsgründen des Gerätes nicht erstellt werden.
Nicht genügend Speicher		x (IKE)	Die Anzahl der VPN Verbindungen hat den Speicher des Gerätes ausgelastet. Weitere VPN - Verbindungen sollten aus Stabilitätsgründen des Gerätes nicht erstellt werden.
Keine Regel für ID´s gefunden - unbekannte Verbindung oder fehlerhafte ID (z.B. IP-Netzwerkdefinition)		x (IKE)	Die eingehende Verbindung konnte keiner Gegenstelle zugewiesen werden. Bitte folgende Parameter überprüfen : ID type stimmt nicht überein (Siehe dieses Dokument) , falsche Netzwerkdefinition, VPN Regeln stimmen nicht (siehe VPN REGEL).
Kein übereinstimmendes Proposal gefunden	x (IPsec)	x (IPsec)	Die Gegenstellen konnten sich auf kein übereinstimmendes Proposal einigen. Bitte überprüfen Sie die Einstellungen unter "Konfiguriere --> VPN --> IKE -- IKE - Prposals" sowie unter "Konfiguriere --> VPN --> IPSec-Parameter --> IPSec - Proposal - Listen".
IPSec PFS Gruppen stimmen nicht überein			Bitte überprüfen Sie die PFS (Perfect Forward Secrecy) unter "Konfiguriere --> VPN --> Verbindungs - Parameter --> "VPN Gegenstellenname" --> PFS - Gruppe"

A.2 SNMP-Traps

MIB2-Traps	Erklärung
coldstart	Gerät wurde durch Aus- und Einschalten der Stromzufuhr neu gestartet.
warmstart	LCOS wurde neu gestartet, z.B. durch einen Software-Reboot
authentication failed (= console login failed)	Anmeldung beim Zugriff auf die Konfiguration fehlgeschlagen

Enterprise specific Traps	Erklärung
Firmware upload started	Firmware-Upload gestartet
Configuration upload started	Einspielen der Firmware bzw. der Konfiguration gestartet
Upload succeeded	Einspielen der Firmware bzw. der Konfiguration erfolgreich
Upload failed (timeout)	Einspielen der Firmware bzw. der Konfiguration fehlgeschlagen: Überschreitung der Maximalzeit
Upload failed (incomplete)	Einspielen der Firmware bzw. der Konfiguration fehlgeschlagen: Unvollständige Konfiguration
Upload failed (bad device)	Einspielen der Firmware bzw. der Konfiguration fehlgeschlagen: Falsches Gerät
Configuration download started	Auslesen der Konfiguration gestartet
Download succeeded	Auslesen der Konfiguration erfolgreich
Console login	Anmeldung zur Konfiguration erfolgt
Console logout	Abmeldung von der Konfiguration erfolgt
Firewall-Trap	Information über ein Firewall-Ereignis
Connection status	WAN-Verbindungsstatus
VPN Connection status	VPN-Verbindungsstatus
WAN-Ethernet UP/DOWN	WAN-Interface verfügbar oder nicht verfügbar

WLAN-Traps	Betriebsmodus	Erklärung
WLAN Scan started	Access-Point oder Client	WLAN-Station hat einen Scan nach freien Funkkanälen gestartet
Started WLAN BSS ID	Access-Point	WLAN-Station hat eine neue Funkzelle aufgebaut
Joined WLAN BSS ID	Client	WLAN-Station hat eine Funkzelle gefunden
Authenticated WLAN station	Access-Point	Authentifizierung einer Client-WLAN-Station erfolgreich
Deauthenticated WLAN station	Access-Point	Client-WLAN-Station hat sich abgemeldet
Associated WLAN station	Access-Point	Client-WLAN-Station verbunden
Reassociated WLAN station	Access-Point	Client-WLAN-Station erneut verbunden, war zuvor bei einem anderen Access Point angemeldet
RADIUS access check for WLAN station succeeded	Access-Point	Überprüfung des RADIUS-Zugangs der WLAN-Station erfolgreich
RADIUS access check for WLAN station failed	Access-Point	Überprüfung des RADIUS-Zugangs der WLAN-Station fehlgeschlagen
Disassociated WLAN station due to station request	Access-Point	WLAN-Station abgemeldet aufgrund einer Anforderung der Station
Rejected association from WLAN station	Access-Point	Anmeldung der WLAN-Station zurückgewiesen
WLAN card hung, resetting	Access-Point oder Client	WLAN-Karte angehalten, Reset

A.3 Unterstützte RFCs

RFC	Titel
1058	Routing Information Protocol
1331	The Point-to-Point Protocol (PPP) for the Transmission of Multi-protocol Datagrams over Point-to-Point Links
1334	PPP Authentication Protocols
1389	RIP Version 2 MIB Extensions
1483	Multiprotocol Encapsulation over ATM Adaptation Layer 5

RFC	Titel
1542	Clarifications and Extensions for the Bootstrap Protocol
1552	The PPP Internetworking Packet Exchange Control Protocol (IPXCP)
1577	Classical IP and ARP over ATM
1631	The IP Network Address Translator (NAT)
1877	PPP Internet Protocol Control Protocol Extensions for Name Server Addresses
1974	PPP Stac LZS Compression Protocol
2284	Extensible Authentication Protocol
2104	HMAC: Keyed-Hashing for Message Authentication
2131	Dynamic Host Configuration Protocol
2132	DHCP Options and BOOTP Vendor Extensions
2225	Classical IP and ARP over ATM
2364	PPP Over AAL5
2401	Security Architecture for the Internet Protocol
2402	IP Authentication Header
2403	The Use of HMAC-MD5-96 within ESP and AH
2404	The Use of HMAC-SHA-1-96 within ESP and AH
2405	The ESP DES-CBC Cipher Algorithm With Explicit IV
2406	IP Encapsulating Security Payload (ESP)
2407	The Internet IP Security Domain of Interpretation for ISAKMP
2408	Internet Security Association and Key Management Protocol (ISAKMP)
2409	The Internet Key Exchange (IKE)
2410	The NULL Encryption Algorithm and Its Use With IPsec
2412	The OAKLEY Key Determination Protocol
2451	The ESP CBC-Mode Cipher Algorithms
2516	A Method for Transmitting PPP Over Ethernet (PPPoE)
2684	Multiprotocol Encapsulation over ATM Adaptation Layer 5
3280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

A.4 Glossar

802.11	Funk-LAN Spezifikation des IEEE; Datenrate bis 2 Mbit/s; im 2,4 GHz ISM Band; FHSS und DSSS; auch Infrarot Spektrum Kommunikation vorgesehen
802.11a	802.11 Erweiterung; Datenrate bis 54 Mbit/s; im 5 GHz Band; OFDM
802.11b	802.11 Erweiterung; Daten bis 11 Mbit/s; im 2,4 GHz Band; hohe Marktdurchdringung; DSSS/CCK
802.11g	802.11 Erweiterung; Datenrate bis 54 Mbit/s; im 2,4 GHz Band; OFDM und DSSS
802.11h	802.11a Anpassung, Datenrate bis 54 Mbit/s; im 5 GHz Band; im Bereich der Sendeleistung und Frequenz-management; für den Einsatz in Europa; OFDM
802.11i	Zukünftige 802.11 Erweiterung mit zusätzlichen Sicherheitsmerkmalen
802.1x	Spezifikation eines portbasierenden Authentisierungsmechanismus durch IEEE
AES	Advanced Encryption Standard
Access Point	Basisstation in einem Wireless LAN; unabhängige LAN-WLAN-Bridge; verbindet Stationen eines LAN (lokales Netz) mit einem WLAN (Funknetz) im Point-to-Multipoint Betrieb; verbindet zwei Netze über ein Funknetz im Point-to-Point Betrieb
Access Router	Aktive Netzwerkkomponente für die Anbindung eines lokalen Netzwerks an das Internet oder ein Firmennetzwerk
ADSL	Asymmetrical Digital Subscriber Line - Übertragungsverfahren für die Hochgeschwindigkeitsdatenübertragung über normale Telefonverkabelungen. Mit ADSL sind Übertragungen (Downstream) bis zu 6 Mbit/s über normale Telefonkabel realisierbar, für die bidirektionale Übertragung steht ein zweites Frequenzband mit Übertragungsgeschwindigkeiten bis zu 640 kbit/s (Upstream) zur Verfügung - daher auch die Bezeichnung asymmetrisch.
Bandbreite	Datensatz mit welcher ein Nutzer im Internet surfen kann; je höher die Bandbreite, desto schneller
Breitband	Dienst, der sich durch hohe Bandbreite auszeichnet; z.B.: DSL oder WLAN
Bridge	Transportprotokoll-unabhängige, transparente Netzwerkkomponente; überträgt alle Pakete, die als "nicht lokal" identifiziert werden und kennt nur den Unterschied zwischen "lokal" und "remote". Arbeitet auf Layer-2 des OSI-Modells
Broadcast	Broadcasts sind Pakete an alle Stationen eines lokalen Netzes; Bridges übertragen Broadcasts; Router übertragen keine Broadcasts
BSS	Basic Service Set
CAPI	Common ISDN Application Programming Interface - CAPI ist ein Standard zur Ansteuerung von ISDN-Adaptern
CCK	Code Complementary Keying; Modulationsart bei DSSS
Client	Jeder mit einem LAN-Adapter (Netzwerk-Karte) ausgestattete Rechner, der von anderen Teilnehmers des Netzwerkes Dienste in Anspruch nimmt
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance; Zugriffsverfahren auf den Funkkanal bei 802.11
CRC	Cyclic Redundancy Check; Bitfehler Erkennungsverfahren
Datendurchsatz	Geschwindigkeit, mit der im Internet gesurft werden kann; abhängig von der Bandbreite und der Anzahl der Nutzer
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Service - Rechner kommunizieren mit Rechnern in entfernten Netzen über IP-Adressen; DNS-Server übersetzten Namen in IP-Adressen; ohne DNS-Server müsste man sich alle IP-Adressen merken und könnte nicht mit Namen arbeiten (www.lancom.de)
Domäne	in sich geschlossener Netzwerkbereich; => Intranet
Download / Downstream	Download / Downstream kennzeichnet die Richtung des Datenflusses in einem WAN. Bei Downstream handelt es sich um die Richtung vom Head-End/Internet zu dem am Netz angeschlossenen Teilnehmer.
DS	Distribution System
DSL	Digital Subscriber Line - DSL-Verfahren sind alle Verfahren zur digitalen breibandigen Nutzung von Telefonleitungen im Anschlussbereich, wie ADSL, HDSL, SDSL, VDSL usw., die auch als xDSL bezeichnet werden
DSSS	Direct Sequence Spread Spectrum; Codemultiplex - Bandspreizverfahren
Dynamic DNS	IPSec-VPN-Implementation, welche die transparente Einbindung von lokalen Netzwerken in eine VPN-Lösung erlaubt, selbst wenn deren Router mit dynamischen Adressen (Dial-Up) arbeiten
EAP	Extensible Authentication Protocol
EAP-MD5	EAP-Variante, die Passwörter zur einseitigen Authentisierung benutzt
EAP-TLS	EAP-Transport-Layer Security; EAP-Variante, die Zertifikate zur gegenseitigen Authentisierung benutzt
EAP-TTLS	EPA-Tunneled-Transport-Layer Security; EAP-Variante, die Zertifikate zur gegenseitigen Authentisierung benutzt
EIRP	Effective Isotropic Radiated Power, mittlere äquivalente isotrope Strahlungsleistung
ESS	Extended Service Set
ESSID	Extended Service Set Identity; "Netzwerkname" des Funk-LAN

Ethernet	Strang- oder sternförmig aufgebautes, physikalisches Transportmedium; alle Stationen können gleichzeitig senden; Kollisionen werden erkannt und durch das Netzwerk-Protokoll behoben
FHSS	Frequency Hopping Spread Spectrum; Frequenzsprung - Bandspreizverfahren
Firewall	Schutzmechanismen für ein Intranet gegen Zugriffe von außen
Frequenz	Anzahl der Schwingungen pro Sekunde (angegeben in Hertz; 1 Hz = 1 Schwingung pro Sekunde; GHz = Gigahertz = 1 Mrd. Hertz Schwingungen pro Sekunde)
FTP	File Transfer Protocol - Filetransfer-Protokoll dient dem Dateitransfer zwischen verschiedenen Systemen und der einfachen Dateihandhabung; FTP basiert auf dem Übertragungsprotokoll TCP
Frequenzband	Zusammenhängender Frequenzbereich, der sich durch gleiche Übertragungs-eigenschaften auszeichnet
Funkfrequenz	Jede Funkanwendung findet in weltweit streng reglementierten Funkfrequenzen statt
Gateway	Netzwerkkomponente, die auf einem Layer des => OSI-Modells Zugang zu anderen Netzwerkkomponenten bietet. Pakete, die nicht an eine lokale Gegenstelle gehen, werden an das Gateway geschickt. Das Gateway kümmert sich um die Kommunikation mit entfernten Netzen.
Hub	Netzwerkkomponente; Verteiler; Kollektor; auch zur Umsetzung von einem Anschluss-Typ auf einen anderen
HotSpot	Lokal begrenztes Funknetz dessen Basisstation über einen Internetzugang verfügt; öffentlicher drahtloser Internetzugang
IAPP-Roaming	Roaming zwischen den Zellen eines Funknetzwerks über das IAPP (Inter Access Point Protocol)
IBSS	Independent Basic Service Set
IDS	Intrusion Detection System - frühest mögliches Erkennen von Angriffen auf das Netzwerk
IEEE	Institute of Electrical and Electronics Engineers, New York - www.ieee.org
IP	Internet Protocol
IP-Masquerading	Kombination aus PAT (Port Adress Translation) und NAT (Network Adress Translation) von LANCOM Systems verwendetes Verfahren zur Anbindung eines Intranets (mehrere Workstations) ans Internet über eine einzige IP-Adresse; gleichzeitig sind die internen Rechner vor Zugriffen von außen geschützt
IPSec	Internet Protocol Security
IP Quality-of-Service	Diese Funktionen geben Vorfahrt für unternehmenskritische Applikationen, bestimmte Dienste oder Benutzergruppen
ISDN	Integrated Services Digital Network - schneller Verbindungsaufbau; zwei unabhängige Kanäle; höhere Übertragungsraten als analog (bis 128 Kbit/s); nutzt die alten analogen Leitungen; Komfortmerkmale (Rufumleitung, Rückruf bei besetzt etc.); unterstützt sowohl analoge als auch digitale Dienste
ISM-Frequenzband	Industrial-Scientific-Medical, lizenzfrei nutzbare Frequenzbänder, die für industrielle, wissenschaftliche und medizinische Zwecke verwendet werden können
ISP	Internet Service Provider - Dienstleister, der über eine Verbindung ins Internet verfügt (Backbone) und Einwahlpunkte für Endkunden bereitstellt
LCOS	LANCOM Operating System - einheitliches Betriebssystem für die LANCOM-Produkte
LAN	Local Area Network - lokales Netzwerk; standortbegrenzt
LANcapi	Virtuelle CAPI, die über das Netzwerk angeboten wird; mit der in allen LANCOM-Routern mit ISDN-Schnittstelle implementierten LANcapi kann auch ein im LAN angeschlossener PC ISDN-Telematikdienste nutzen
LANconfig	Software zur Konfiguration von LANCOM-Geräten unter Windows
LANtools	Umfangreiches, benutzfreundliches Set für Management und Überwachung der LANCOM-Produkte und -Lösungen
MAC-Filter	Media Access Control; Funkzugriffsprotokoll auf ISO Layer 2 Data Link; es definiert Paket-Format, Paket-Adressierung und Fehlerdetektion
MAC-Adresse	Seriennummer einer Netzkomponente, die durch den Hersteller vergeben wird
Mbit	Megabit: Standardgröße für die Angabe von Datenmengen im Zusammenhang mit Bandbreiten
MIC	Message Integrity Check, kryptographischer Integritätsschutzmechanismus
NetBios	Network Basic Input/Ouput System. Von IBM entwickeltes und später von Microsoft übernommenes, nicht routbares Netzwerkprotokoll für lokale Netze.
NTBA	Network Termination Basic Adaptor . Der NTBA (Netzabschlussadapter) ist bei einem ISDN-Basisanschluss für die Umsetzung des von der Telefongesellschaft verlegten Anschlusses auf den S0-Bus zuständig.
OFDM	Orthogonal Frequency Divison Multiplex
PEAP	Protected EAP, EAP-Variante zur gegenseitigen Authentisierung
PKI	Public Key Infrastructure
PPP	Point to Point Protocol: Netzwerkprotokoll für die Verbindung zwischen zwei Rechnern. PPP setzt auf TCP/IP auf.
PPTP	Point to Point Tunneling Protocol: Netzwerkprotokoll zum Aufbau virtueller privater Netze über das Internet.
Point-to-Multipoint (WLAN)	Mehrere WLAN-Stationen buchen sich auf eine Basis-Station ein und bilden mit den fest verkabelten Stationen ein gemeinsames Netzwerk

Point-to-Point (WLAN)	Zwei Basis-Stationen verbinden zwei kabelgebundene Netze über WLAN; der Point-to-Point Betrieb ermöglicht Kopplungen von Netzwerken auch über Straßen hinweg ohne Kabel
QoS	Quality-of-Service (siehe hierzu IP Quality-of-Service)
RADIUS	Remote Authentication Dial-In User Service; Authentisierungs- und Überwachungsprotokoll auf Anwendungsebene für Authentisierung, Integritätsschutz und Accounting im Bereich Netzzugang
RC4	Stromchiffrierverfahren von Ron Rivest, "Rens Code"
RFC	Request for Comments
Router	intelligente Netzwerkkomponente; vergleichbar mit einer Poststelle, die aufgrund von logischer Zieladresse eines Paketes entscheiden kann, an welche nächste Netzwerkkomponente dieses Paket übertragen wird; kennt die gesamte Topologie des Netzes
SDSL	Symmetric Digital Subscriber Line - Downstream und Upstream mit 2,048 Mbit/s (zweiadriges Kabel)
Server	Rechner, der im Netzwerk Dienste (z.B. Dateien, NEWS, EMail, WWW-Seiten) zur Verfügung stellt
SINA	Sichere Inter-Netzwerk Architektur
SMTP	Simple Mail Transfer Protocol - SMTP-Protokoll ist der Internet-Standard zur Verteilung von elektronischer Post; das Protokoll setzt auf dem TCP-Protokoll auf
SNMPv3	Simple Network Management Protocol Version 3
SSID	Service Set Identity; "Netzwerkname" des Funk-LANs
SSL	Secure Socket Layer
Splitter	Der Splitter ist vergleichbar mit einer Audio-Frequenzweiche; bei einem ADSL-Anschluss trennt der Splitter die ISDN-Signale von den DSL-Signalen; die ISDN-Signale gehen zum NTBA; die DSL-Signale gehen zum DSL-Modem
Switch	Ein zentraler Verteiler in einem sternförmigen Netz; jede Station hat die volle Bandbreite zur Verfügung; wenn eine Station ausfällt, wird der Rest des Netzes nicht beeinträchtigt; wird zur Kollisionsvermeidung eingesetzt; erhöht den Gesamtdurchsatz des Netzes; Switches sind kaskadierbar
TAE	Telefon-Anschluss-Einheit. Stecker zum Anschluss von analogen Geräten wie ein Telefon oder Modem an das Telefonnetz.
TCP/IP	Transmission Control Protocol/Internet Protocol; Familie von Protokollen (ARP, ICMP, IP, UDP, TCP, HTTP, FTP, TFTP) wird hauptsächlich im Internet verwendet, hält aber auch immer mehr Einzug in Intranets
TKIP	Temporal Key Integrity
TLS	Transport-Layer Security
TPC	Transmission Power Control
Upload/Upstream	Upload / Upstream kennzeichnet die Richtung des Datenflusses in einem WAN; bei Upstream handelt es sich um die Richtung vom am Netz angeschlossenen Teilnehmer zum Head-End/Internet
Verkettung	Aneinandergehängte Bitfolgen
VPN	Virtual Private Network - ein VPN ist ein Netzwerk bestehend aus virtuellen Verbindungen, über welche nichtöffentliche bzw. firmeninterne Daten sicher übertragen werden können, auch wenn öffentliche Netzwerkinfrastrukturen genutzt werden
WAN	Wide Area Network - Netzwerk-Verbindung über weite Strecken (z.B. über ISDN mit einem LANCOM-Router)
WECA	Wireless Ethernet Compatibility Alliance; Vereinigung von Herstellern von Funk-LAN-Komponenten nach IEEE 802.11; umbenannt zu WiFi-Alliance
WEBconfig	Webbasierte Konfigurationsoberfläche für LANCOM-Geräte.
WEP	Wired Equivalent Privacy
WiFi	Wireless Fidelity; Marketing Begriff generiert durch WECA
WiFi-Alliance	Vereinigung von Herstellern von Funk-LAN-Komponenten nach IEEE 802.11;früher WECA
WLAN	Wireless Local Area Network - lokales Funknetz
WPA	WiFi Proteced Access; Bezeichnung für über IEEE 802.11 hinaus gehende Sicherheitsmechanismen; generiert durch die WiFi-Alliance
WISP	Wireless Internet Service Provider
xDSL	xDSL steht für die Familie der Digital Subscriber Line Techniken
XOR	Logische Verknüpfung "exklusiv oder"

A.5 Übersicht über die Funktionen nach Modellen und LCOS*-Versionen

800/1000/1100		I-10 HW-Rv. A	I-10 HW-Rv. C	DSL/I-10+	800+	821	821+	1511	1521
Interfaces									
ADSL-Modem						✔	✔		✔
ADSL 2+							5.20		ADSL 2
VLAN							7.00	✔	✔
DMZ-Port				5.20	5.20	1)	5.20	5.20	5.20
Switch-Ports				3	4	4	4	4	4
Ethernet Port Mapping				5.00			✔	5.00	5.00
DSLoL						3.10			
Security									
Stateful Inspection, DoS, IDS	2.80	2.80	2.80	✔	✔	2.80	✔	✔	✔
IP-QoS, Traffic Shaping	3.30	3.30	3.30	✔	✔	3.30	✔	3.30	✔
SSH-Konfigurations-Zugang				✔	✔	4.00	✔	4.00	4.00
ISDN basierende Diebstahlsicherung				5.00	5.00	5.00	✔	5.00	5.00
Standortverifikation über GPS									
Management									
Rechteverwaltung für Admins				✔	✔	4.00	✔	4.00	4.00
mehrere Loopback-Adressen				✔	✔	4.00	✔	4.00	4.00
Modembetrieb an serieller Schnittstelle				4.10	4.10	4.10	✔	4.10	4.10
Scripting				5.00	5.00	5.00	✔	5.00	5.00
CRON	3.10	3.10	3.10	✔	✔	3.10	✔	✔	✔
Port Monitor				5.00	5.00		✔	5.00	5.00
Automatische Funkfeldoptimierung mit LANCOM WLAN Controllern									
Zentrales Firmware- und Skript-Management mit LANCOM WLAN Controllern									
weitere Funktionen									
Advanced Routing and Forwarding (ARF-Netze)				2 7.00	2 7.00		8 7.00	2 7.00	2 7.00
DHCP Auto Client Modus	3.42	3.42	3.42	✔	✔	3.42	✔	3.42	3.42
N:N-Mapping				4.10	4.10	4.10	✔	✔	4.10
Dynamic DNS	3.10	3.10	3.10	✔	✔	3.10	✔	✔	✔
Freies Port-Mapping				✔	✔	4.00	✔	4.00	4.00
Multi-PPPoE				✔		4.00	✔	4.00	4.00
Load Balancing (Kanäle)				2 5.00		2 5.00	2	2 5.00	2 5.00
Policy-based Routing				5.00	5.00	5.00	✔	5.00	5.00
VRRP				5.20	5.20	5.20	5.20	5.20	5.20
PPPoE-Server				5.20	5.20	5.20	5.20	5.20	5.20
WAN-RIP				5.20	5.20	5.20	5.20	5.20	5.20

800/1000/1100		I-10 HW-Rv. A	I-10 HW-Rv. C	DSL/I-10+	800+	821	821+	1511	1521
Spanning-Tree-Protokoll								5.20	5.20
Layer-2-QoS-Tagging							6.10	6.10	6.10
VPN-Funktionen									
VPN-Kanäle									
VPN Hardwarebeschleunigung									
AES, 3-DES, DES, Blowfish, CAST									
digitale Zertifikate (X.509) inkl. PKCS #12									
Certificate Revocation List - CRL									
Zertifikatsenrollment über SCEP									
vereinfachte Einwahl mit Zertifikaten									
mehrstufige Zertifikate									
AES 256 / IPCOMP									
Redundante VPN-Gateways									
NAT Traversal (NAT-T)									
IKE-Config-Mode									
WLAN-Funktionen									
IEEE-802.11b								✔	✔
IEEE-802.11g								✔	✔
IEEE-802.11a (inkl. Turbo-Modus)									
IEEE-802.11n Draft 2.0									
LEPS								4.00	4.00
Multi-SSID, IP-Redirect								3.42	3.42
Super A/G								3.42	3.42
Standard-WEP-Verschlüsselung								4.00	4.00
802.11i m. HW-AES								3.50	3.50
802.11i für P2P im WLAN								4.00	4.00
WLANmonitor								5.00	5.00
Gruppenkonfiguration								5.00	5.00
volltransparenter Client Bridge Mode								5.00	5.00
Bandbreitenbegrenzung im WLAN								5.20	5.20
QoS für WLAN (IEEE 802.11e, WMM/WME)								6.10	6.10
RADIUS-Server								6.10	6.10
RADSEC-Unterstützung									
Voucher-Druck für Public-Spot-Benutzer									
VoIP-Funktionen (detaillierte Informationen über die VoIP-Funktionen Ihres Gerätes entnehmen Sie bitte dem Benutzerhandbuch)									
SIP-Benutzer									
ISDN-Benutzer									
SIP-Leitungen									
Leitungen zu SIP-TK-Anlagen									
externe ISDN-Busse für VoIP									
interne ISDN-Busse für VoIP									
Anschlüsse für analoges Amt									
Anschlüsse für analoge Endgeräte									
VoIP-Media-Proxy									

□ Übersicht über die Funktionen nach Modellen und LCOS*-Versionen

800/1000/1100	I-10 HW-Rv. A	I-10 HW-Rv. C	DSL/I-10+	800+	821	821+	1511	1521
Software-Optionen								
ISDN Festverbindungs-Option	int. ab 6.10	int. ab 6.10	int. ab 6.10	int. ab 6.10	int. ab 6.10	int. ab 6.10	int. ab 6.10	int. ab 6.10	int. ab 6.10
Public Spot Option								✔	✔
Faxmodem Option	✔	✔							
VPN-25 Option									
VPN-500 Option									
VPN-1000 Option									
VoIP-32 Option									

* Die Zahlen in der Tabelle geben die LCOS-Version an, mit der die Funktion implementiert wurde.

[1] Port-Separierung (Private Mode)

[2] nicht bei 11-MBit-WLAN-Karten

[3] optional VPN-500 und VPN-1000 erhältlich

[4] Kompatibel zu ADSL und ADSL2

[5] bei 3050 nur mit externer MC-54-Karte

[6] Mit VoIP-32 Option

	1611	1611+	1620	1621	1711	1721	1722	1723	1724	1751
Interfaces										
UMTS-Modem										✔
ADSL-Modem			✔	✔		✔	✔	✔	✔	✔
ADSL 2+			✔			✔	✔	✔	✔	✔
VLAN		7.00	7.00		7.00	7.00	7.00	✔	✔	✔
DMZ-Port		5.20	✔	1)	5.20	5.20	✔	✔	✔	✔
Switch-Ports		3	4	4	4	4	4	2	2	4
Ethernet Port Mapping		✔	✔		5.00	✔	✔	✔	✔	✔
DSLoL				3.10						
Security										
Stateful Inspection, DoS, IDS	2.80	✔	✔	2.80	✔	✔	✔	✔	✔	✔
IP-QoS, Traffic Shaping	3.30	✔	✔	3.30	✔	✔	✔	✔	✔	✔
SSH-Konfigurations-Zugang	4.00	4.00	✔	4.00	4.00	✔	✔	✔	✔	✔
ISDN basierende Diebstahlsicherung	5.00	✔		5.00	5.00	✔	✔	✔	✔	✔
Standortverifikation über GPS										✔
Management										
Rechteverwaltung für Admins	4.00	4.00	✔	4.00	4.00	✔	✔	✔	✔	✔
mehrere Loopback-Adressen	4.00	4.00	✔	4.00	4.00	✔	✔	✔	✔	✔
Modembetrieb an serieller Schnittstelle	4.10	4.10	✔	4.10	4.10	✔	✔	✔	✔	✔
Scripting	5.00	✔	✔	5.00	5.00	✔	✔	✔	✔	✔
CRON	3.10	✔	✔	3.10	✔	✔	✔	✔	✔	✔
Port Monitor		✔	✔		5.00	✔	✔	✔	✔	✔
Automatische Funkfeldoptimierung mit LANCOM WLAN Controllern										
Zentrales Firmware- und Skript-Management mit LANCOM WLAN Controllern										
weitere Funktionen										
Advanced Routing and Forwarding (ARF-Netze)		2 7.00	2 7.00		8 7.00	8 7.00	8 7.00	8 7.00	8 7.00	8
DHCP Auto Client Modus	3.42	3.42	✔	3.42	3.42	✔	✔	✔	✔	✔
N:N-Mapping	3.30	✔	✔	3.30	✔	✔	✔	✔	✔	✔
Dynamic DNS	3.10	✔	✔	3.10	✔	✔	✔	✔	✔	✔
Freies Port-Mapping	4.00	4.00	✔	4.00	4.00	✔	✔	✔	✔	✔
Multi-PPPoE	4.00	4.00	✔	4.00	4.00	✔	✔	✔	✔	✔
Load Balancing		2	2	2 5.00	4 Kanäle 5.00	4 Kanäle	4 Kanäle	2 Kanäle	2 Kanäle	4 Kanäle
Policy-based Routing	5.00	✔	✔	5.00	5.00	✔	✔	✔	✔	✔
VRRP	5.20	5.20	✔	5.20	5.20	✔	✔	✔	✔	✔
PPPoE-Server	5.20	5.20	✔	5.20	5.20	✔	✔	✔	✔	✔

□ Übersicht über die Funktionen nach Modellen und LCOS*-Versionen

	1611	1611+	1620	1621	1711	1721	1722	1723	1724	1751
WAN-RIP	5.20	5.20	✔	5.20	5.20	✔	✔	✔	✔	✔
Spanning-Tree-Protokoll										✔
Layer-2-QoS-Tagging		6.10	6.10		6.10	6.10	6.10	✔	✔	✔
VPN-Funktionen										
VPN-Kanäle	5	5	5	5	5	5	5	5	5	5
VPN Hardwarebeschleunigung					mit VPN-25-Option	mit VPN-25-Option	mit VPN-25-Option	mit VPN-25-Option	mit VPN-25-Option	mit VPN-25-Option
AES, 3-DES, DES, Blowfish, CAST	3.32	✔	✔	3.32	✔	✔	✔	✔	✔	✔
digitale Zertifikate (X.509) inkl. PKCS #12	5.00	✔	✔	5.00	5.00	✔	✔	✔	✔	✔
Certificate Revocation List - CRL					6.10	6.10	6.10	✔	✔	✔
Zertifikatsenrollment über SCEP					7.00	7.00	7.00	7.00	7.00	✔
vereinfachte Einwahl mit Zertifikaten					6.20	6.20	6.20	6.20	6.20	✔
mehrstufige Zertifikate					7.52	7.52	7.52	7.52	7.52	7.52
AES 256 / IPCOMP	5.00	✔	✔	5.00	5.00	✔	✔	✔	✔	✔
Redundante VPN-Gateways	4.00	4.00	✔	4.00	4.00	✔	✔	✔	✔	✔
NAT Traversal (NAT-T)	5.20	5.20	✔	5.20	5.20	✔	✔	✔	✔	✔
IKE-Config-Mode	4.00	4.00	✔	4.00	4.00	✔	✔	✔	✔	✔
WLAN-Funktionen										
IEEE-802.11b										
IEEE-802.11g										
IEEE-802.11a (inkl. Turbo-Modus)										
IEEE-802.11n Draft 2.0										
LEPS										
Multi-SSID, IP-Redirect										
Super A/G										
Standard-WEP-Verschlüsselung										
802.11i m. HW-AES										
802.11i für P2P im WLAN										
WLANmonitor										
Gruppenkonfiguration										
volltransparenter Client Bridge Mode										
Bandbreitenbegrenzung im WLAN										
QoS für WLAN (IEEE 802.11e, WMM/WME)										
RADIUS-Server										
RADSEC-Unterstützung										
Voucher-Druck für Public-Spot-Benutzer										
VoIP-Funktionen (detaillierte Informationen über die VoIP-Funktionen Ihres Gerätes entnehmen Sie bitte dem Benutzerhandbuch)										
SIP-Benutzer		4/-[7]					8/32[6]	8/32[6]	8/32[6]	
ISDN-Benutzer		40					40	40	40	
SIP-Leitungen		16					16	16	16	
Leitungen zu SIP-TK-Anlagen		4					4	4	4	
externe ISDN-Busse für VoIP		1					0-2	0-1	0-4	
interne ISDN-Busse für VoIP							0-2	0-2	0-4	

	1611	1611+	1620	1621	1711	1721	1722	1723	1724	1751
Anschlüsse für analoges Amt								0-1		
Anschlüsse für analoge Endgeräte								2		
VoIP-Media-Proxy							7.52	7.52	7.52	
Software-Optionen										
ISDN Festverbindungs-Option	int. ab 6.10	int. ab 6.10		int. ab 6.10	int. ab 6.10	int. ab 6.10	int. ab 6.10	int.	int.	int.
Public Spot Option										
Faxmodem Option										
VPN-25 Option	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
VPN-500 Option										
VPN-1000 Option										
VoIP-32 Option							✔	✔	✔	

* Die Zahlen in der Tabelle geben die LCOS-Version an, mit der die Funktion implementiert wurde.

[1] Port-Separierung (Private Mode)

[2] nicht bei 11-MBit-WLAN-Karten

[3] optional VPN-500 und VPN-1000 erhältlich

[4] Kompatibel zu ADSL und ADSL2

[5] bei 3050 nur mit externer MC-54-Karte

[6] Mit VoIP-32 Option

Übersicht über die Funktionen nach Modellen und LCOS*-Versionen

	1811	1821	1821+	1823	3050 3550	3850	4000 4100	6000 6001 6021	7011	7111	8011
Interfaces											
UMTS-Modem						extern Cardbus					
ADSL-Modem		✔	✔	✔							
ADSL 2+		ab Hard-ware Release E	✔	✔							
VLAN	3.30	✔	✔	✔	3.30	✔			7.00	7.00	7.00
DMZ-Port	5.20	5.20	✔	✔					✔	5.20	5.20
Switch-Ports	4	4	4	2		2				4	4
Ethernet Port Mapping	5.00	5.00	✔	✔		✔				5.00	5.00
DSLoL						✔					
UMTS-Unterstützung					ab 6.20 inte-griert	✔					
Security											
Stateful Inspection, DoS, IDS	✔	✔	✔	✔	2.80	✔	2.80	2.80	2.80	✔	✔
IP-QoS, Traffic Shaping	✔	✔	✔	✔	3.30	✔	3.30	3.30	3.30	✔	✔
SSH-Konfigurations-Zugang	4.00	4.00	✔	✔	4.00	✔	4.00	4.00	4.00	✔	4.00
ISDN basierende Diebstahlsicherung	5.00	5.00	✔	✔			5.00	5.00	5.00	5.00	5.00
Standortverifikation über GPS											
Management											
Rechteverwaltung für Admins	4.00	4.00	✔	✔	4.00	✔	4.00	4.00	4.00	✔	4.00
mehrere Loopback-Adressen	4.00	4.00	✔	✔	4.00	✔	4.00	4.00	4.00	✔	4.00
Modembetrieb an serieller Schnittstelle	4.10	4.10	✔	✔		✔				4.10	4.10
Scripting	5.00	5.00	✔	✔	5.00	✔	5.00	5.00	5.00	5.00	5.00
CRON	✔	✔	✔	✔	3.10	✔	3.10	3.10	3.10	✔	3.10
Port Monitor	5.00	5.00	✔	✔		✔				5.00	5.00
Automatische Funkfeldoptimierung mit LANCOM WLAN Controllern	7.52	7.52	7.52	7.52	7.52	7.52					
Zentrales Firmware- und Skript-Management mit LANCOM WLAN Controllern	7.52	7.52	7.52	7.52	7.52	7.52					
weitere Funktionen											
Advanced Routing and Forwarding (ARF-Netze)	8 7.00	8 7.00	8	8 7.00	8 7.00	8			2 7.00	64 7.00	64 7.00
DHCP Auto Client Modus	3.42	3.42	✔	✔	3.42	✔	3.42	3.42	3.42	✔	3.42
N:N-Mapping	3.30	✔	✔	✔	3.30	✔	3.30	3.30	3.30	✔	✔
Dynamic DNS	✔	✔	✔	✔	3.10	✔	3.10	3.10	3.10	✔	✔
Freies Port-Mapping	4.00	4.00	✔	✔	4.00	✔	4.00	4.00	4.00	✔	4.00
Multi-PPPoE	4.00	4.00	✔	✔	4.00	✔			4.00	✔	4.00

	1811	1821	1821+	1823	3050 3550	3850	4000 4100	6000 6001 6021	7011	7111	8011
Load Balancing	4 Kanäle 5.00	4 Kanäle 5.00	4 Kanäle	2 Kanäle						4 Kanäle 5.00	4 Kanäle 5.00
Policy-based Routing	5.00	5.00	✔	✔	5.00	✔	5.00	5.00	5.00	5.00	5.00
VRRP	5.20	5.20	✔	✔	5.20	✔	5.20	5.20	5.20	5.20	5.20
PPPoE-Server	5.20	5.20	✔	✔	5.20	✔	5.20	5.20	5.20	5.20	5.20
WAN-RIP	5.20	5.20	✔	✔	5.20	✔	5.20	5.20	5.20	5.20	5.20
Spanning-Tree-Protokoll	5.20	5.20	✔	✔	5.20	✔					
Layer-2-QoS-Tagging	6.10	6.10	✔	✔	6.10	✔	6.10	6.10	6.10	6.10	6.10
VPN-Funktionen											
VPN-Kanäle	5	5	5	5				100	200	100	200
VPN Hardwarebeschleunigung	mit VPN-25-Option	mit VPN-25-Option	mit VPN-25-Option	mit VPN-25-Option		mit VPN-25-Option				✔	✔
AES, 3-DES, DES, Blowfish, CAST	3.32	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
digitale Zertifikate (X.509) inkl. PKCS #12	5.00	5.00	✔	✔	5.00	✔			5.00	5.00	5.00
Certificate Revocation List - CRL	7.00	7.00	✔	✔	6.10	✔				6.10	6.10
Zertifikatsenrollment über SCEP	7.00	7.00	✔	7.00	7.00	✔				7.00	7.00
vereinfachte Einwahl mit Zertifikaten	7.00	7.00	✔	✔	6.20	✔				6.20	6.20
mehrstufige Zertifikate	7.52	7.52	7.52	7.52	7.52	7.52				7.52	7.52
AES 256 / IPCOMP	5.00	5.00	✔	✔	5.00	✔	5.00	5.00	5.00	5.00	5.00
Redundante VPN-Gateways	4.00	4.00	✔	✔	4.00	✔	4.00	4.00	4.00	✔	4.00
NAT Traversal (NAT-T)	5.20	5.20	✔	✔	5.20	✔	5.20	5.20	5.20	5.20	5.20
IKE-Config-Mode	4.00	4.00	✔	✔	4.00	✔	4.00	4.00	4.00	✔	4.00
WLAN-Funktionen											
IEEE-802.11b	✔	✔	✔	✔	✔	✔					
IEEE-802.11g	✔	✔	✔	✔	✔ 5)	✔					
IEEE-802.11a (inkl. Turbo-Modus)	✔	✔	✔	✔	✔ 5)	✔					
IEEE-802.11n Draft 2.0											
LEPS	4.00	4.00	✔	✔	4.00	✔					
Multi-SSID, IP-Redirect	3.42	3.42	✔	✔	3.42 2)	✔					
Super A/G	3.42	3.42	✔	✔	3.42 2)	✔					
Standard-WEP-Verschlüsselung	4.00	4.00	✔	✔	4.00	✔					
802.11i m. HW-AES	3.50	3.50	✔	✔	- / 3.50	✔					
802.11i für P2P im WLAN	4.00	4.00	✔	✔	4.00 2)	✔					
WLANmonitor	5.00	5.00	✔	✔	5.00	✔					
Gruppenkonfiguration	5.00	5.00	✔	✔	5.00	✔					
volltransparenter Client Bridge Mode	5.00	5.00	✔	✔	5.00 2)	✔					

□ Übersicht über die Funktionen nach Modellen und LCOS*-Versionen

	1811	1821	1821+	1823	3050 3550	3850	4000 4100	6000 6001 6021	7011	7111	8011
Bandbreitenbegrenzung im WLAN	5.20	5.20	✔	✔	5.20	✔					
QoS für WLAN (IEEE 802.11e, WMM/WME)	6.10	6.10	✔	✔	6.10 [2)]	✔					
RADIUS-Server	6.10	6.10	✔	✔	6.10	✔					
RADSEC-Unterstützung	7.52	7.52	7.52	7.52	7.52	7.52					
Voucher-Druck für Public-Spot-Benutzer	7.52	7.52	7.52	7.52	7.52	7.52					
VoIP-Funktionen (detaillierte Informationen über die VoIP-Funktionen Ihres Gerätes entnehmen Sie bitte dem Benutzerhandbuch)											
SIP-Benutzer				8/32[6)]							
ISDN-Benutzer				40							
SIP-Leitungen				16							
Leitungen zu SIP-TK-Anlagen				4							
externe ISDN-Busse für VoIP				0-1							
interne ISDN-Busse für VoIP				0-2							
Anschlüsse für analoges Amt				0-1							
Anschlüsse für analoge Endgeräte				2							
VoIP-Media-Proxy				7.52							
Software-Optionen											
ISDN Festverbindungs-Option	int. ab 6.10	int. ab 6.10	integriert	integriert			integriert	integriert	integriert	integriert	integriert
Public Spot Option	✔	✔	✔	✔	✔	✔					
Faxmodem Option											
VPN-25 Option	✔	✔	✔	✔	✔	✔	✔				
VPN-500 Option											✔
VPN-1000 Option											✔
VoIP-32 Option				✔							

* Die Zahlen in der Tabelle geben die LCOS-Version an, mit der die Funktion implementiert wurde.

[1)] Port-Separierung (Private Mode)

[2)] nicht bei 11-MBit-WLAN-Karten

[3)] optional VPN-500 und VPN-1000 erhältlich

[4)] Kompatibel zu ADSL und ADSL2

[5)] bei 3050 nur mit externer MC-54-Karte

[6)] Mit VoIP-32 Option

	L-2	IL-2	L-11	IL-11	L-54g	L-54ag IAP	L-54 dual	L-305 agn	L-310 agn	OAP	XAP
Interfaces											
ADSL-Modem											
ADSL 2+											
VLAN			✔	✔	✔	✔	✔	✔	✔	✔	✔
DMZ-Port											
Switch-Ports							2	2	2		
Ethernet Port Mapping										5.00	
DSLoL	3.10	3.10	3.10	3.10	3.10	3.10	✔	✔	✔		✔
Security											
Stateful Inspection, DoS, IDS	2.80	2.80	2.80	2.80	2.80	2.80	✔	✔	✔	✔	✔
IP-QoS, Traffic Shaping	3.30	3.30	3.30	3.30	3.30	3.30	✔	✔	✔	✔	✔
SSH-Konfigurations-Zugang					4.00	4.00	✔	✔	✔	✔	✔
ISDN basierende Diebstahlsicherung											
Standortverifikation über GPS											
Management											
Rechteverwaltung für Admins					4.00	4.00	✔	✔	✔	✔	✔
mehrere Loopback-Adressen					4.00	4.00	✔	✔	✔	✔	✔
Modembetrieb an serieller Schnittstelle					4.10	4.10	✔	✔	✔		
Scripting					5.00	5.00	✔	✔	✔	5.00	5.00
CRON	3.10	3.10	3.10	3.10	3.10	3.10	✔	✔	✔	✔	✔
Port Monitor								✔	✔	5.00	
Automatische Funkfeldoptimierung mit LANCOM WLAN Controllern					7.52	7.52	7.52	7.52	7.52	7.52	7.52
Zentrales Firmware- und Skript-Management mit LANCOM WLAN Controllern					7.52	7.52	7.52	7.52	7.52	7.52	7.52
weitere Funktionen											
Advanced Routing and Forwarding (ARF-Netze)					8 7.00	8 7.00	8 7.00	8 7.00	8 7.00	8 7.00	8 7.00
DHCP Auto Client Modus					3.42	3.42	✔	✔	✔	✔	✔
N:N-Mapping					4.10	4.10	✔	✔	✔	✔	✔
Dynamic DNS	3.10	3.10	3.10	3.10	3.10	3.10	✔	✔	✔	✔	✔
Freies Port-Mapping					4.00	4.00	✔	✔	✔	✔	✔
Multi-PPPoE					4.00	4.00	✔	✔	✔	✔	✔
Load Balancing											
Policy-based Routing					5.00	5.00	✔	✔	✔	5.00	5.00
VRRP					5.20	5.20	✔	✔	✔	5.20	5.20
PPPoE-Server					5.20	5.20	✔	✔	✔	5.20	5.20
WAN-RIP					5.20	5.20	✔	✔	✔	5.20	5.20
Spanning-Tree-Protokoll					5.20	5.20	✔	✔	✔	5.20	5.20

□ Übersicht über die Funktionen nach Modellen und LCOS*- Versionen

	L-2	IL-2	L-11	IL-11	L-54g	L-54ag IAP	L-54 dual	L-305 agn	L-310 agn	OAP	XAP
Layer-2-QoS-Tagging					6.10	6.10	✔	✔	✔	6.10	6.10
VPN-Funktionen											
VPN-Kanäle											
VPN Hardwarebeschleunigung										mit VPN-25-Option	
AES, 3-DES, DES, Blowfish, CAST											
digitale Zertifikate (X.509) inkl. PKCS #12										5.00	
Certificate Revocation List - CRL											
Zertifikatsenrollment über SCEP										7.00	
vereinfachte Einwahl mit Zertifikaten											
mehrstufige Zertifikate											
AES 256 / IPCOMP										5.00	
Redundante VPN-Gateways										✔	
NAT Traversal (NAT-T)										5.20	
IKE-Config-Mode										✔	
WLAN-Funktionen											
IEEE-802.11b	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
IEEE-802.11g					✔	✔	✔	✔	✔	✔	✔
IEEE-802.11a (inkl. Turbo-Modus)						✔	✔	✔	✔	✔	✔
IEEE-802.11n Draft 2.0								✔	✔		
LEPS					4.00	4.00	✔	✔	✔	✔	✔
Multi-SSID, IP-Redirect					3.42	3.42	✔	✔	✔	✔	✔
Super A/G					3.42	3.42	✔	✔	✔	✔	✔
Standard-WEP-Verschlüsselung					4.00	4.00	✔	✔	✔	✔	✔
802.11i m. HW-AES					3.50	3.50	✔	✔	✔	✔	✔
802.11i für P2P im WLAN					4.00	4.00	✔	✔	✔	✔	✔
WLANmonitor					5.00	5.00	✔	✔	✔	5.00	✔
Gruppenkonfiguration					5.00	5.00	✔	✔	✔	5.00	✔
volltransparenter Client Bridge Mode					5.00	5.00	✔	✔	✔	5.00	✔
Bandbreitenbegrenzung im WLAN					5.20	5.20	✔	✔	✔	5.20	✔
QoS für WLAN (IEEE 802.11e, WMM/WME)					6.10	6.10	✔	✔	✔	6.10	✔
RADIUS-Server					6.10	6.10	✔	✔	✔	6.10	✔
RADSEC-Unterstützung					7.52	7.52	7.52	7.52	7.52	7.52	7.52
Voucher-Druck für Public-Spot-Benutzer					7.52	7.52	7.52	7.52	7.52	7.52	7.52
VoIP-Funktionen (detaillierte Informationen über die VoIP-Funktionen Ihres Gerätes entnehmen Sie bitte dem Benutzerhandbuch)											
SIP-Benutzer											
ISDN-Benutzer											
SIP-Leitungen											
Leitungen zu SIP-TK-Anlagen											
externe ISDN-Busse für VoIP											

	L-2	IL-2	L-11	IL-11	L-54g	L-54ag IAP	L-54 dual	L-305 agn	L-310 agn	OAP	XAP
interne ISDN-Busse für VoIP											
Anschlüsse für analoges Amt											
Anschlüsse für analoge Endgeräte											
VoIP-Media-Proxy											

Software-Optionen											
ISDN Festverbindungs-Option		int. ab 6.10		int. ab 6.10							
Public Spot Option	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
Faxmodem Option											
VPN-25 Option										✔	
VPN-500 Option											
VPN-1000 Option											
VoIP-32 Option											

* Die Zahlen in der Tabelle geben die LCOS-Version an, mit der die Funktion implementiert wurde.

[1] Port-Separierung (Private Mode)

[2] nicht bei 11-MBit-WLAN-Karten

[3] optional VPN-500 und VPN-1000 erhältlich

[4] Kompatibel zu ADSL und ADSL2

[5] bei 3050 nur mit externer MC-54-Karte

[6] Mit VoIP-32 Option

Index

Numerics

1-1-Mapping 7-33
2,4 GHz ISM-Frequenzband 12-15
3-DES 10-4, 10-70, 17-12, 17-15, 17-17, 17-20
5 GHz Frequenzband 12-13
802.11 12-6, 17-8
802.11i 6-9
  PMK-Caching 12-19
  VoIP 12-19
802.11x
  Rekeying 12-18

A

AAL-5 7-17
Access Control List 12-27
Access Point 12-58, 17-9
Access Point-Modus 12-1
Access Points 4-38
Access Points manuell akzeptieren 12-68
Access Router 17-9
Administratoren 3-26
Administratorengruppe 3-27
Adress-Pool 16-4
Adressverwaltung 16-1
ADSL 2-2, 5-2, 17-9
ADSL-Modem 17-11, 17-14, 17-16, 17-19
AES 10-4, 10-70, 12-16, 17-8, 17-12, 17-15, 17-17, 17-20
AES-CCM 12-18
Aggressive Mode 10-4
AH 10-4, 10-69, 10-70
Allow-All 8-8, 8-18
Alternative WLAN- Controller 12-63
Anfrage von Zertifikaten mittels CERTREQ 10-45
Anruferkennung 6-5
Anrufweiterschaltung 13-45
Antennen-Gewinn 12-35
Antennen-Kalkulator 12-51
Antennen-Leistungen 12-52
AOCD 16-21
Application Gateway 8-5
asymmetrischen Verschlüsselung 10-24
AT-Befehle 7-47
ATM 5-2
ATM-Anpassungsschicht 7-17
Ausschluss-Routen 7-3
autark 12-1
Autarker Weiterbetrieb 12-64
Authentifizierung 7-41, 12-16, 12-17, 12-61
Authentifizierungsverfahren
  TLS 12-18
  TTLS 12-18
Authentizität 10-24
auto reconnect 7-41
Auto-Accept 12-62
Automatische Annahme neuer APs 12-62
Automatische Kanalwahl 12-65
Automatische Zuweisung der Default-Konfiguration 12-62, 12-69

B

Background-Scanning 12-21, 12-49
Backup mit primären und sekundären WLAN- Controllern 12-74
Backup mit redundanten WLAN- Controllern 12-73
Backup-Lösungen 14-1
Backuplösungen 12-72
Backup-Verbindung 7-48, 14-4
Bandbreite 17-9
Benutzergruppe 12-2
Benutzername 3-17, 6-5
Benutzerrechte 3-28
B-Kanal
  Protokoll 6-5
B-Kanal-Protokolle 15-4
Blacklist 12-33
Blowfish 10-4, 10-70, 12-16
Bonk 8-35
Breitband 17-9
Bridge 17-9
Broadcast 12-63, 17-9
Brute-Force 6-2
Bruttodatenrate 9-4
BSS 17-9
Bundesnetzagentur 10-26

C

CA 10-26, 12-61
Called Party ID 13-9
Calling Line Identifier Protocol 6-6
Call-Routing 13-6
Call-Routing-Tabelle 13-10
CAPI 17-9
CAPI Faxmodem 15-4
CAPI Protokolle 15-4
CAPI Schnittstelle 15-1
CAPWAP 12-59, 12-60, 12-62
CAPWAP-Tunneling 12-60
CAST 10-4, 10-70
CCK 17-9
Certificate Revocation List 10-45
Certification Authority 10-26, 12-61
CHAP 6-5
Client 17-9
Client-Modus 12-5, 12-38, 12-47, 12-50
CLIP 6-5, 6-6
Collision Domain 11-1
Common ISDN Application Programming Interface (CAPI) 15-1
Control And Provisioning of Wireless Access Points 12-59
CRC 17-9
CRL 10-45
CRON 17-12, 17-14, 17-17, 17-19
CRON-Dienst 16-27
Cron-Job 12-81
CSMA/CA 17-9

D

Datagram Transport Layer Security 12-59
Datendurchsatz 17-9

Datenkanal 12-59
Datenkompressionsverfahren
LZS 7-43
Datenübertragung 7-43
Datenübertragung zu bewegten Objekten 12-5
Datum/Zeit 16-24
DDI 13-55
Dead-Peer-Detection 14-1, 14-3
Default-Gateway 6-10
Deflate 10-4
Denial of Service 2-1
Denial-of-Service 8-34
Bonk 8-35
Fragrouter 8-35
Konfiguration 8-35
LAND 8-34
Ping of Death 8-34
Smurf 8-34
SYN Flooding 8-34
Teardrop 8-35
Denial-of-Service-Angriffe 8-34
LAND 8-34
Smurf 8-34
SYN Flooding 8-34
Deny-All 8-19
DES 10-4, 10-70, 12-16
DFS 12-33, 12-51
DFÜ-Netzwerk 3-16, 6-5
DHCP 5-1, 7-17, 16-1, 17-9
Automodus für den DHCP-Server 16-1
DHCP-Server 16-14
Zuweisung der Broadcast-Adresse 16-4
Zuweisung der Netzmaske 16-4
Zuweisung des Standard-Gateways 16-4
Zuweisung von DNS- und NBNS-Server 16-4
Dienst 16-13
Dienstgüte – siehe Quality-of-Service
Differentiated Services – siehe DiffServ
Differentiated Services Code Point – siehe DSCP
Diffie-Hellman-Verfahren 10-72
DiffServ 9-1, 9-2
Assured Forwarding 9-1, 9-2
Best Effort 9-2
Class Selector 9-2
Expedited Forwarding 9-1, 9-2, 9-3
IPSec 9-1
Direct Dialing In 13-55
Discovery Request Message 12-61, 12-76
Distanz einer Route 7-3
D-Kanal 5-2, 6-5
DMZ-Port 17-11, 17-14, 17-16, 17-19
DMZ-Schnittstelle 2-1
DNS 5-1, 12-61, 16-13, 17-9
DNS-Forwarding 16-14
DNS-Server 16-1, 16-4, 16-13
DNS-Tabelle 16-16, 16-17
Dynamic DNS 7-55, 16-17
Filterliste im DNS-Server 16-17
Filtermechanismus des DNS-Servers 16-14
URL-Blocking 16-17
verfügbare Informationen im DNS-Server 16-14
Domain 16-13, 16-17
sperren 16-17
Domain Name Service (DNS) 16-13
Domäne 17-9
DoS 17-12, 17-14, 17-16, 17-19
Konfiguration 8-35
Download 1-2, 17-9
Downstream 17-9
Downstreamrate 9-4
DPD 14-1, 14-3
Drucker am USB-Anschluss 16-45
DS 17-9
DSCP 9-2
DSL 2-2, 17-9
DSLoL 2-2, 17-11, 17-14, 17-16, 17-19
DSSS 12-16, 17-9
DTLS 12-59, 12-61
Durchsatz 7-43
Dynamic DNS 7-55, 16-17, 17-9, 17-12, 17-14, 17-17, 17-20
Dynamic Frequency Selection 12-33, 12-51
Dynamic Host Configuration Protocol (DHCP) 16-1
Dynamic VPN
Beispiele 10-63
dynamisch - dynamisch 10-8, 10-65
dynamisch - statisch 10-7, 10-63
Einführung 10-6
Funktionsweise 10-7
ICMP 10-63
PPP-Liste 10-14
statisch - dynamisch 10-7, 10-64
UDP 10-63
Dynamic-VPN 14-6
dynamische Frequenzwahl 12-51
Dynamische Kanalbündelung 7-43
Dynamische VLAN-Zuweisung 12-76
Dynamisches Routing 7-2
dynDNS 16-17

E

EAP 12-17, 12-59, 17-9
Ablauf einer mittels EAP geschützten Sitzung 12-17
RADIUS-Server 12-17
EAP/802.1x 16-44
Master Secret 12-18
EAP-MD5 17-9
EAP-TLS 17-9
EAP-TTLS 17-9
EIRP 17-9
E-Mail 12-67
E-Mail-Benachrichtigung 8-16
E-Mail-Viren 8-21
Encapsulation 7-17
End-Adresse 16-4
Enhanced Passphrase Security 12-20
Enterprise specific Traps 17-4
ESP 10-4, 10-69
ESS 17-9

ESSID 17-9
ETH-10 7-17
Ethernet 17-9
exposed host 7-19
Extensible Authentication Protocol 12-17, 12-44

F

Fast Call Back 6-6
Fax 15-4
Fax Class 1 15-4
Faxmodem Option 17-13, 17-16, 17-18, 17-21
Faxmodem-Option 15-5
Faxtreiber 15-4
Faxübertragung 15-4
Fehlende Gebühreninformationen 16-21
Fehlersuche 4-30
Fernkonfiguration 3-1
Fernüberwachung 7-31
Fernverbindung 3-16
Fernwartung
  mit N-N-Mapping 7-32
FHSS 17-9
Filterliste 8-7, 8-8
Firewall 6-10, 8-1, 15-1, 17-9
  Alarmierungsfunktionen 8-16
  Allow-All 8-8, 8-18
  Anwendungsfälle 8-21
  Application Gateway 8-5
  Assistent 8-22
  Aufgaben 8-3
  Authentifizierungs-Port 8-12
  Beispielkonfiguration Basic Internet 8-21
  Beispielkonfiguration IPSec/PPTP-Freischaltung 8-21
  Beispielkonfiguration ISDN-Einwahl 8-22
  Beispielkonfiguration Netzwerkkopplung 8-22
  Beispielkonfiguration V.110-Einwahl 8-22
  Beispielkonfiguration VPN-Einwahl 8-21
  Benachrichtigung per E-Mail 8-16
  Benachrichtigung per SNMP-Trap 8-18
  Besondere Protokolle 8-8
  Default-Einstellung 8-20
  Deny-All 8-19, 8-21
  Diagnose 8-28
  DMZ 8-19
  DMZ (Schaubild) 8-19
  dualhomed Gateway 8-5
  Einstellungen 8-10
  Ereignisanzeige 8-28
  Filterliste 8-7, 8-29
  Firewall-Tabelle 8-28
  Fragmente 8-10
  Hostsperrliste 8-7, 8-32
  ICMP 8-11
  ICMP-Verbindungen 8-9
  Komponenten 8-2
  Logging-Tabelle 8-28
  NAT 8-20
  paketfilterbasiert 8-3
  Parameter der Firewall-Regeln 8-12
  Ping-Blocking 8-11
  Portsperrliste 8-7, 8-32
  Prüfen mit mehreren Listen 8-8
  Schaubild 8-7
  Sitzungswiederherstellung 8-10
  Stafeful Inspection 8-4
  Stateful-Inspection 8-20
  Stationen sperren 6-10
  Strategien für die Einstellung 8-18
  SYSLOG 8-16
  TCP-Stealth-Modus 8-11
  TCP-Verbindungen 8-9
  Tipps zur Einstellung 8-20
  Typen 8-3
  UDP-Verbindungen 8-8
  Verbindungsliste 8-7, 8-31
Firewall/QoS-Aktivierung 8-10
Firewall-Regel
  Absender-Adresse sperren 8-16
  Aktionstabelle 8-28
  Aufbau 8-14
  Bedingung 8-13, 8-15
  E-Mail-Nachricht senden 8-15
  Konfiguration 8-26
  Limit 8-13, 8-15
  Objekttabelle 8-27
  Paket-Aktion 8-13, 8-15
  Priorität 8-12
  Quality of Service 8-13, 8-16
  Regel-Tabelle 8-26
  Schaubild 8-14
  SNMP senden 8-15
  Sonstige Maßnahmen 8-13, 8-15
  Syslog-Nachricht senden 8-15
  Trigger 8-13, 8-15
  Verbindung 8-13, 8-14
  Verbindung trennen 8-15
  Verknüpfung 8-12
  VPN-Regel 8-12, 8-13
  Ziel-Port sperren 8-16
Firewall-Tabelle 8-28
Firmware 1-2, 3-24
  zentrale Verwaltung 12-81
Firmware-Management 12-81
Firmware-Updates 4-6
Firmware-Upload 3-22
  mit Terminalprogramm 3-23
  mit TFTP 3-23
Firmware-Versionen 4-7
Flash 12-59, 12-64
Flash-No-Modus 4-14
Flash-Yes-Modus 4-14
Flatrate 7-40
FQDN 16-17
Fragrouter 8-35
Frame-Tagging 11-2
Frequenz 17-9
Frequenzband 17-9
Fresnel-Zone 12-52
FTP 17-9
  aktives FTP 9-9
  passives FTP 9-9
  TCP-gesicherte Übertragung 9-5
FTP-Datentransfer 9-5

FTP-Download 9-1
Funkfrequenz 17-9
Funkkanäle 17-4
Funknetzwerk 12-1
Funktionsrechte 3-27

G

Gateway 16-1, 17-9
Gebühren
  Begrenzung 16-20
  Einheiten 7-43, 16-21
  Information 7-43, 16-21
  Management 16-20
  Zeit-Limit 16-21
Gebührenüberwachung 15-1
Gegenstellen 7-48
Gezieltes VPN-Accounting mit Zwischenspeicherung 16-19
GPS 6-6
Gruppen-Konfiguration 4-22
Gültigkeitsdauer 16-1

H

Halten 13-12, 13-45, 13-46
Haltezeit 7-43
Hard-Roaming 12-49
Hash 10-30
Hash-Algorithmen 10-4
HDLC 7-17
Hidden-Station 12-43
Hinweis-Symbole 1-3
Hohe Telefonkosten 16-20
Home-Office 7-23
Host 16-13
Hostsperrliste 8-7, 8-8
HotSpot 17-10
Hotspot 12-2
HSCSD 7-17
HTTPS 3-4
Hub 17-10

I

IAPP-Roaming 17-10
IBSS 17-10
ICMP 6-10, 8-22, 10-23, 10-63
ICMP Polling 3-33, 14-1, 14-2
ICMP-Verbindungen 8-9
Identifikationskontrolle 6-5
Identifizierung des Anrufers 6-5
IDS 17-10, 17-12, 17-14, 17-16, 17-19
  Konfiguration 8-33
IEEE 17-10
IEEE 802.11a 12-6, 12-13
IEEE 802.11b 12-6, 12-15
IEEE 802.11e 9-15
IEEE 802.11g 12-6, 12-15
IEEE 802.11n 12-60
IEEE 802.1p 11-7
IEEE 802.1p/q 11-1
IEEE 802.1x/EAP 12-44
IEEE 802.3 7-17, 12-6
IETF 12-59
IKE 10-4, 10-72
IKE Config Mode 10-15
IKE-Proposals 10-37
Inband 3-1
  Konfiguration über Inband 3-1
  mit Telnet 3-10
Indoor-Funktion 12-23
Industrieanwendungen 12-5
Integrität 10-24
Internet-Zugang 7-38
Intrusion Detection 2-1, 8-32
  Konfiguration 8-33
Intrusion-Detection
  IP-Spoofing 8-33
  Portscan 8-33
Inverses Masquerading 7-19, 7-31
IP 17-10
  Filter 6-10
  Ports sperren 6-10
IP Quality-of-Service 17-10
IP-Adresse 4-31, 6-10, 7-37
IP-Adressen
  dynamische 10-6
  statische 10-6
IP-Adressverwaltung 16-1
IPCOMP 10-4
IP-Header 9-1
IP-Masquerading 2-1, 5-1, 6-10, 7-31, 17-10
IP-Module 2-1
IP-Parameter 10-14
IP-Redirect 2-1
IP-Router 2-1
IP-Routing
  Standard-Router 7-5
IP-Routing-Tabelle 7-2
IPSec 10-4, 10-67, 17-10
IP-Spoofing 8-33
IP-Telefonie 9-5
IPv4-Adresse 7-31
IPv6 10-68
IPX-Router 2-2
ISAKMP 10-4, 10-72
ISDN 2-2, 17-10
  B-Kanal 10-8, 10-9
  D-Kanal 6-6, 10-8
  Euro-ISDN (DSS-1) 10-8
  LLC 10-8
ISDN Festverbindungs-Option 17-13, 17-16, 17-18, 17-21
ISDN-Administrationszugang 6-3
ISDN-Fernzugang 3-16
ISDN-Life-Line 13-55
ISM-Frequenzband 12-15, 17-10
ISP 17-10

K

Kanalbündelung 7-43
  Dynamisch 7-43
  Statisch 7-43
Keep Alive 10-23
Keep-alive 7-40
Keep-Alive-Verbindungen 14-5, 14-12
Kompatibilitätsmodus 12-6
Konfiguration 12-62
  Verfahren 3-1

Konfigurationsdatei 6-11
Konfigurationskennwort 6-9
Konfigurations-Schnittstelle 3-1
Konfigurationsupdates 4-13
Kontaktbelegung 7-49
Kontrollkanal 12-59
Kosten begrenzen 16-20

L

L2F 10-68
L2TP 10-68
LAN 17-10
  logisch 11-2
  physikalisch 11-2
LAN-Bridge 2-1
LANCAPI 2-2
LANcapi 17-10
LANCOM-Betriebssystem 2-1
LANconfig 3-2, 3-16, 4-1, 17-10
  Script downloaden 4-15
  Spaltenansicht 4-5
  Verwaltung mehrerer Geräte 3-3
LAND 8-34
LANmonitor 4-27, 12-68, 12-79
  Access Point trennen 12-79
  Accounting-Informationen 4-28
  Aktivitätsprotokoll 4-29
  Anzeige-Optionen 4-30
  Firewall-Ereignisanzeige 4-29
  Internet-Verbindung kontrollieren 4-30
  Neuer Access Point zu Profil zuordnen 12-79
  System-Informationen 4-30
  Traces 4-32, 5-4
  VPN-Verbindungen 4-28
LANtools 17-10
Lastenausgleich 10-65
Layer-2 7-17
Layer-2-Switch 11-1
Layer-3 7-17
Layer-3-Roaming 12-60
Layername 7-17
LCOS 1-2, 2-1, 17-10, 17-11
LCP-Echo-Reply 7-37
LCP-Echo-Request 7-37
LCR 16-21
LDP 16-45
Least-Cost-Routing 16-21
LEPS 12-20
Life-Line 13-55
LLC-MUX 7-17
Load-Balancing 12-76
local break out 13-3
Local-Mac 12-60
Logging-Tabelle 8-28
Login 3-21
Login-Sperre 6-2
Login-Versuche 6-2
logische Funknetze 12-22
logische Senderichtung 9-9
logisches LAN 11-2
Loopback-Adresse 7-33
Lost-AP-LED 12-68, 12-69
LZS-Datenkompression 7-43

M

MAC 17-10
MAC-Adresse 12-21, 17-10
MAC-Filter 12-77
MAC-Filter aktiviert 12-41
MAC-Frame 11-2
MAC-Funktionen 12-59
Mailserver 16-16
Main Mode 10-4
Makeln 13-12, 13-45, 13-46
Managed-Modus 12-1
Management-VLAN-ID 12-65
Maximalbandbreite 9-1, 9-3
Mbit 17-10
MIB2 17-4
MIC 17-10
Mindestbandbreite 9-1, 9-2, 9-3
  beim Empfang 9-2
  beim Senden 9-2
MLPPPoE 7-24
Modem 7-17
Modem Adapter Kit 7-45
Modem-Parameter 7-45
MS-CHAP 7-36
MSN 13-55
MTU 7-49
Multilink PPP (MLPPP) 7-43
Multilink-PPP (MLPPP) 7-36
Multilink-PPPoE (MLPPPoE) 7-36
Multiple Subscriber Number 13-55
Multi-PPPoE 7-23, 7-24, 14-5
Multi-SSID 12-40
Multithreading 4-6

N

N
  N-Mapping 2-1, 17-12, 17-14, 17-17, 17-19
NAT 7-31
NBNS-Server 16-1
NetBIOS 5-1, 16-14
  NBNS 10-14
NetBios 17-10
NetBIOS/IP 10-14
NetBIOS-Netze 16-14
NetBIOS-Proxy 8-20, 10-14
Nettodatenrate 9-4
Network Address Translation 7-31
Netzkopplung 7-31
Netzmaske 6-10
Netzwerk-Management 4-1
Netzwerknamen 16-13
N-N-Mapping 7-31
  dezentrales Mapping 7-33
  DNS-Forwarding 7-34
  Firewall 7-34
  Konfiguration 7-33
  Loopback-Adresse 7-34
  NAT-Tabelle 7-33
  Netzwerkkopplung über VPN 7-32
  Routing-Tabelle 7-34

VPN-Regel 7-34
zentrales Mapping 7-33
NTBA 17-10
NTP-Clients 16-25
NTP-Server 3-33, 16-24

O

OFDM 12-13, 17-10
Online-Minuten 16-20
OpenSSL 10-34
Outband 3-1
Konfiguration über Outband 3-1
Overhead 9-1

P

Paket-Dump 5-2
Paketfilter 8-3
PAP 6-5
passwd 6-2
Passwort 3-16, 3-17, 4-31, 6-1, 6-5
Passwortschutz 4-8
PCKS12-Container 12-71
PEAP 17-10
Periode 16-20
PHY-Layer 12-59
physikalische Senderichtung 9-9
physikalische WLAN-Schnittstelle 12-22
physikalisches LAN 11-2
ping 8-22
Ping of Death 8-34
Ping-Befehl 5-14
Ping-Blocking 8-11
ping-Blocking
Konfiguration 8-36
PKCS#12-Datei 10-32
PKI 10-26, 17-10
PMTU-Reduzierung 9-6
Point-to-Multipoint 12-3
Point-to-Multipoint (WLAN) 17-10
Point-to-Point 12-3
Point-to-Point (WLAN) 17-10
Point-to-Point Tunneling
Protocol (PPTP) 7-40
Policy-based Routing 7-3
Polling-Tabelle 10-23
Port Address Translation 7-31
Portscan 8-33
Port-Separierung 17-14, 17-16, 17-19, 17-21
Portsperrliste 8-7, 8-8
PPP 4-31, 6-5, 7-17, 7-43, 17-10
LCP Extensions 7-42
Leitungsüberprüfung mit LCP 7-37
Rückruf-Funktionen 7-41
Verhandlungsphase 3-17
Zuweisung von IP-Adressen 7-37
PPP LCP Echo Monitoring 14-1
PPP-Client 3-16
PPPoE 7-17
PPP-Verbindung 3-17
PPTP 2-2, 7-40, 10-68, 17-10
Precedence 9-2
Preshared Key 10-4
Pre-Shared-Key 12-16
Preshared-Key-Verfahren 10-27
Primäre Controller 12-75
Printserver 16-45
Private 10-25
Private Key 10-25
Private Mode 17-14, 17-16, 17-19, 17-21
Proadaptives VPN 10-44
Projektmanagement 4-1
Prüfsumme 10-30
PSK 12-16
PSK-Verfahren 10-27
Public Key 10-24
Public-Key 10-72
Public-Key-Infrastructure 10-26
Public-Key-Verfahren 10-25
Punkt-zu-Mehrpunkt 13-54
Punkt-zu-Punkt 12-50, 13-54

Q

QoS 9-5, 17-10, 17-12, 17-14, 17-16, 17-19
Richtung der Datenübertragung 9-9
VLAN-Tag 9-15
QoS –
siehe Quality-of-Service
Quality of Service 2-1
802.11e 9-15
Quality-of-Service 9-1
Queue 9-3

R

Radarsignal 12-33
RADIUS 12-17, 12-59, 12-77, 16-44, 17-10
WLAN-Zugangsliste 16-40
RADIUS-Server 16-40, 16-42
RADSEC 16-44
RAS 10-1, 10-2
RawIP 16-45
RC 2833 13-13
RC4 12-16, 17-10
Rechner-Namen 16-13
Rechteverwaltung 3-20, 3-26
Redirect 12-26
redundante Gateways 14-5
Relais-Modus 12-4
Remote Access 7-37
Remote-MAC 12-59
Reset 12-21
Reset-Schalter 3-26
RFC 17-10
RFC 2976 13-13
RFCs 17-8
Rijndael 10-70
RIP 5-1
Roaming 12-21, 12-49
Rogue AP Detection 4-39, 12-21
Rogue Client Detection 4-39
Roll-Out 4-13
Router 7-3, 17-10
Router-Interface-Liste 7-44
Routing-Tabelle 6-10
Routing-Tag 8-12

RSA 10-4, 12-16
RTP Payload for DTMF Digits 13-13
RTS/CTS-Protokoll 12-43
RTS-Schwellwert 12-43
Rückfrage 13-45, 13-46
Rückruf 6-5
Fast Call Back 6-6, 7-42
nach Microsoft CBCP 7-41
nach RFC 1570 7-42
schnelles LANCOM-Verfahren 7-42
RX-Rate 4-38

S

SCEP 12-61
Scheduled Events 16-27
Schlüssel
Öffentlich 10-24
privat 10-25
Schlüssellängen 10-4
Schutz
für die Konfiguration 6-1
Scripting 4-13
Befehle 4-18
SDSL 17-10
Security Association 10-22, 10-69
Security Parameter Index 10-69
Sekundäre Controller 12-75
Serielle Schnittstelle 3-1
seriellen Schnittstelle 7-44
Server 17-10
Sicherheit 6-1, 8-1
Sicherheits-Checkliste 6-9
Sicherheitseinstellungen 1-2
Sicherungsverfahren 6-5
Simple Certificate Encryption Protocol 12-61
SINA 17-10
SIP-Gateway 13-3
SIP-Mapping 13-25
SIP-Provider 13-2
SIP-Proxy 13-7
SIP-Telefon 12-60
SIP-TK-Anlage 13-4
SIP-Trace 13-85
Skalierbarkeit 12-60
Skript
zentrale Verwaltung 12-81
Skript-Management 12-81
Smart-Controller 12-59, 12-60
SMTP 17-11
Smurf 8-34
SNMP 3-14, 3-28, 4-30
Konfiguration schützen 6-10
SNMP-ID 3-11
SNMP-Lesezugriff 4-8
SNMP-Trap 7-33, 8-16, 8-18
SNMP-Traps 17-4
SNMPv3 17-11
Soft-Roaming 12-49
Spannungsweiterleitung 13-55
Speicherauslastung 4-30
Split-MAC 12-59
Split-Management 12-62
Splitter 17-11
Sprachkommunikation 13-1
SSH-Authentifizierung 3-15
SSH-Zugang 3-14
SSID 4-38, 12-48, 12-64, 17-11
SSL 17-11
Stac-Datenkompression 7-43
Stand alone Windows CA 10-31
Standard-Faxprogramme 15-4
Standort-Verifikation 6-6
Start-Adresse 16-4
Stateful Inspection 17-12, 17-14, 17-16, 17-19
Stateful-Packet-Inspection 8-4
Stations-Namen-Tabelle 16-16
Statische Kanalbündelung 7-43
Statisches Routing 7-2
Statistik 7-47, 7-49
Stealth-Modus
Konfiguration 8-36
Support 1-3
Switch 17-11
symmetrische Verschlüsselung 10-24
SYN Flooding 8-34
SYN/ACK-Speedup 7-9
SYSLOG 5-10, 8-16, 12-67, 16-22
SYSLOG-Meldung 8-16

T

TAE 17-11
TCP 6-10, 9-1
TCP/IP 7-2, 17-11
TCP/IP-Filter 6-10
TCP/IP-Netze 16-13
TCP-Stealth-Modus 8-11
TCP-Steuerungspakete 9-3
TCP-Verbindungen 8-9
Teardrop 8-35
Teil-Konfiguration 4-22
Telnet 2-1, 3-16, 6-10
Ausgabe der SNMP-ID 3-11
Temporal Key Integrity Protocol 12-18
Terminalprogramm 3-22
TFTP 2-1, 3-14, 3-28, 6-10
TFTP laden 3-24
Timeout 7-43
TKIP 17-11
TLS 12-59, 16-44, 17-11
ToS 9-1, 9-2
High Reliability 9-1
IPSec 9-1
Low Delay 9-1, 9-3
Priorität 9-2
TPC 17-11
Trace
Ausgaben 5-1
Beispiele 5-3
Schlüssel und Parameter 5-1
starten 5-1
Trace-Ausgaben 7-47
Trace-Konfiguration 4-32, 5-4
Traces 4-32, 5-4
Transportmodus 10-4, 10-70

Triple-DES 10-4, 10-70
Trojaner 8-21
Tunnelmodus 10-4, 10-70
Turbo-Modus 12-13, 12-15
TX-Rate 4-38
Type-of-Service – siehe ToS

U

Übertragungsraten 4-31
Überwachung 4-30
UDP 6-10, 9-1, 10-63
UDP-Verbindungen 8-8
Uhrzeitumstellung nach UTC 16-26
Upload 3-21, 17-11
Upstream 17-11
Upstreamrate 9-4
URL-Blocking 16-17
USB 16-45
UTC 16-26

V

V.110 7-17
VC-MUX 7-17
Verbinden 13-12
Verbindungsbegrenzung 16-21
Verbindungsliste 8-7, 8-8
Vereinfachte Netzwerkanbindung mit Zertifikaten 10-44
Vererbung 12-64, 12-65, 12-70
Verkettung 17-11
Verschlüsselte Konfiguration 3-14
Verschlüsselung 10-3, 10-70, 10-72, 12-16, 12-66, 12-68
  asymmetrisch 10-24
  asymmetrische 12-16
  Kombination symmetrisch/asymmetrisch 10-25
  symmetrisch 10-24
  symmetrische 12-16
Verschlüsselungsmethode 12-48
Verschlüsselungsverfahren
  AES-CCM 12-18
Vertraulichkeit 10-23
Virtual Private Network 10-1
virtuelles LAN 11-1
VLAN 11-1, 17-11, 17-14, 17-16, 17-19
  Abschirmung des SNMP-Traffics 11-3
  Anschluss von WLAN-Stationen 11-3
  Default-VLAN-ID 11-2
  ID 11-2
  Konfiguration 11-4
  Layer-2-Tagging 11-7
  Management des LAN-Traffics 11-3
  Netzwerktabelle 11-5
  Nutzung einer zentralen Verkabelung 11-3
  Port 11-5
  Portliste 11-5
  Porttabelle 11-5
  Priorität 11-2
  Umsetzung in den Schnittstellen 11-2
  Verschiedene Organisationen auf einem LAN 11-3
  VLAN-ID 11-5
VLAN-ID 11-2, 12-64, 12-76
Voice oder WLAN 9-15
Voice-over-IP 9-1, 9-2, 13-1
VoIP 13-1
  Amtsholung 13-10
  Anbindung von Filialen oder Heimarbeitsplätzen 13-3
  Anlagen-Anschluss 13-55
  Anlagenanschluss 13-79
  automatische Amtsholung 13-10
  Basic Rate Interface 13-79
  Busterminierung 13-55
  DDI 13-79, 13-81
  Direct Dialing In 13-79
  Durchwahlfähigkeit 13-79
  Ergänzung zur ISDN-TK-Anlage 13-2
  Halten 13-12
  interne Rufnummern 13-11
  ISDN-Protokoll 13-55
  ISDN-Spannungsweiterleitung 13-55
  ISDN-Takt 13-56
  Life-Line-Support 13-55
  lokale Anmeldung 13-7
  Makeln 13-12
  Mehrgeräte-Anschluss 13-55
  Mehrgeräteanschluss 13-79
  NT-Schnittstelle 13-54
  Peer-to-Peer 13-4
  Point-to-Multipoint 13-54
  Point-to-Point 13-54
  Primary Rate Interface 13-79
  Punkt-zu-Mehrpunkt 13-54, 13-79
  Punkt-zu-Punkt 13-54, 13-79
  RC 2833 13-13
  Remote Gateway 13-83
  SIP INFO 13-13
  SIP-Proxy 13-7
  SIP-Trunking 13-81
  spontane Amtsholung 13-10
  Stammnummer 13-79
  TE-Schnittstelle 13-54
  transparenten Proxy 13-7
  übergeordnete Anmeldung 13-7
  übergeordnete TK-Anlage 13-11
  untergeordnete TK-Anlage 13-11
  Verbinden 13-12
VoIP – siehe Voice-over-IP
VoIP-Benutzer 13-5
VoIP-Call-Router
  Call-Router 13-6
VoIP-Call-Routing-Tabelle
  Call-Routing-Tabelle 13-6
VoIP-Leitungen 13-5
VoIP-Softphone 13-2
VoIP-TK-Anlage 13-3
VoWLAN 9-15
VpIP
  RFC 2976 13-13
VPN 2-2, 10-1, 17-11, 17-15, 17-20
  Anfrage von Zertifikaten mittels CERTREQ 10-45
  Beispiele 10-62
  Client 8-21
  dynamisch - dynamisch 10-65

dynamisch - statisch 10-63
Fernwartung über N-N-Mapping 7-32
Gateway 8-21
Gezieltes VPN-Accounting mit Zwischenspeicherung 16-19
Konfiguration 10-10
Konfiguration mit LANconfig 10-17
Konfiguration mit WEBconfig 10-20
Netzwerkkopplung mit N-N-Mapping 7-32
Proadaptives VPN 10-44
statisch - dynamisch 10-63
statisch - statisch 10-63
Vereinfachte Netzwerkanbindung mit Zertifikaten 10-44
VPN Anwendungsbeispiel 10-3
VPN Load Balancing 14-5
VPN-Client 10-5
VPN-Gateway 14-7
VPN-Haltezeit 10-23
VPN-Netzbeziehungen 10-16
VPN-Regeln 10-13
VPN-Verbindungen 10-65
Diagnose 10-23
manuelles Einrichten 10-14
Setup-Assistent 10-11

W

WAN 17-11
Warteschlangen 9-3
gesicherte Queue 9-3
Standard-Queue 9-3
Urgent Queue II 9-3
Urgent-Queue I 9-3
WEBconfig 2-1, 3-3, 17-11
HTTPS 3-4
WECA 17-11
well known groups 10-4
WEP 6-9, 12-21, 12-28, 17-11
Einzel-WEP-Einstellungen 12-28
Erklärung des Verfahrens 12-20
Whitelist 12-33
WiFi 17-11
Wi-Fi Multimedia 9-15
Wifi Protected Access 12-19
Wi-Fi-Alliance 9-15
WiFi-Alliance 17-11
Wildcards 16-17
Windows Netzwerke 10-14
WINS-Server 10-14
Wired Equivalent Privacy 12-20
Wireless LAN 12-1
Wireless Local Area Network 12-1
Wireless Multimedia Extension 9-15
WISP 17-11
WLAN 17-11
ACL 12-27
Adress-Anpassung 12-39
ARP-Behandlung 12-23
Background-Scanning 12-21
Basisstations-Dichte 12-36
Betriebsart 12-32
Bevorzugte BSS-ID 12-38
Client-Bridge-Unterstützung 12-39
Client-Modus 12-38, 12-47
Client-Verbindung aufrecht erhalten 12-38
DFS-Verfahren 12-33
Durchsuchte Bänder 12-38, 12-48
Frequenzband 12-33
Indoor-Funktion 12-23
Kanalnummer 12-34
Ländereinstellung 12-22
Link-Fehler-Erkennung 12-23
Maximaler Abstand 12-36
Netzwerkeinstellungen 12-41
Protokoll-Filter 12-24
Punkt-zu-Punkt-Verbindungen 12-37
Radio-Einstellungen 12-32
Redirect 12-26
Roaming 12-21
Rogue AP Detection 4-39, 12-21
Rogue Client Detection 4-39
Sendeleistungs-Reduktion 12-35
SSID 12-41
Unterband 12-33
WEP-Gruppen-Schlüssel 12-30
WLAN Controller
Firmware-Management 12-81
Skript-Management 12-81
WLAN- Controller 12-3, 12-58
WLANmonitor 4-38
Rogue Client Detection 4-39
WLAN-Profil 12-63, 12-66
WLAN-Schnittstelle
logisch 12-40
physikalisch 12-31
WLAN-Sicherheit 12-16
802.1x 12-17
EAP 12-17
TKIP 12-19
WEP 12-20
WPA 12-19
WME 9-15
WMM 9-15
WPA 6-9, 12-19, 17-11
Handshake-Verfahren 12-19
Master Secret, 12-19
Michael 12-19
Passphrase 12-18
TKIP 12-18, 12-19

X

X.509 10-4
X.509-Zertifikat 16-44
X.75 7-17
xDSL 17-11
XOR 17-11

Y

Y-Verbindung 7-44

Z

Zeitabhängige Verbindungs-begrenzung 16-21
Zeitautomatik 16-27
Zeitbudget 16-22
Zeit-Server 16-24

Zero-Touch-Management 12-62
Zertifikat 10-45, 12-62, 12-68, 12-69, 12-70
Zertifikate 10-23
Aufbau 10-28
Dateitypen 10-29
Export 10-33, 10-34
Gültigkeit 10-29
OpenSSL 10-34
PKCS#12-Datei 10-32
Sicherheitsklassen 10-30
Sichern 12-70
Vereinfachte Einwahl 10-43
Vorteile 10-27
X.509-Standard 10-28
Zertifikatsperrliste 10-45
Zertifizierung
Anbieter 10-26
ZLIB 10-4
Zufallszahl 12-61
Zugangsschutz 6-5
für die Konfiguration 6-5
Zugangsschutz für die Konfiguration
nach geprüfter Nummer 6-5
nach Nummer 6-5

A Addendum zur LCOS-Version 7.7

A.1 Übersicht

■ 'Erweiterung des Temperaturbereichs für L-305/310' → Seite 1
■ 'Standard-Verschlüsselung mit WPA2' → Seite 2
■ 'APSD – Automatic Power Save Delivery' → Seite 2
■ 'BFWA – mehr Sendeleistung für mehr Reichweite' → Seite 3
■ 'RADIUS-Accounting neu starten' → Seite 4
■ 'Voucher für Public-Spot mit Zeitbudget' → Seite 4
■ 'Erweiterungen im RADIUS-Server' → Seite 9
■ 'IGMP Snooping' → Seite 11
■ 'TACACS+' → Seite 20
■ 'Versand von Anhängen mit dem mailto-Kommando' → Seite 27
■ 'Firmware-Upload für UMTS-Modul im LANCOM 1751 UMTS' → Seite 28
■ 'Performance Monitoring im LANmonitor' → Seite 28
■ 'Einrichten von Punkt-zu-Punkt-Verbindungen mit dem LANmonitor' → Seite 29

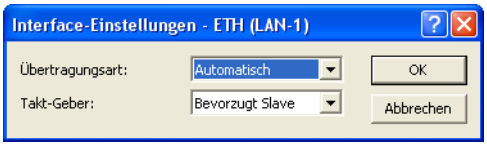
A.2 Erweiterung des Temperaturbereichs für L-305/310

In manchen Anwendungsfällen werden höhere Betriebstemperaturen benötigt als der standardmäßig definierte Temperaturbereich der Access Points LANCOM L-305agn und LANCOM L-310agn zulässt. Diese beiden Modelle können in einem erweiterten Temperaturbereich von bis zu 45° C betrieben werden, wenn die Geschwindigkeit der Gigabit-Ethernet-Schnittstelle auf 100 MBit/s begrenzt wird.

Ab der LCOS-Version 7.70 reduziert die automatische Einstellung der Schnittstellengeschwindigkeit die maximale Übertragungsrate auf 100 MBit/s, solange die standardmäßige Maximaltemperatur von 35° C überschritten wird. Da die erhöhten Temperaturen oft nur temporär (z.B. an besonders warmen Sommertagen) auftreten, resultieren aus der vorübergehenden Begrenzung der Übertragungsrate kaum Einschränkungen für den Betrieb der Geräte.

Die Einstellung der Übertragungsgeschwindigkeit für Ethernet-Ports finden Sie auf folgenden Pfaden:

LANconfig: Schnittstellen ▶ LAN ▶ Interface-Einstellungen



WEBconfig: LCOS-Menübaum ▶ Setup ▶ Schnittstellen

■ **Übertragungsart**

Wählen Sie hier aus, welche Übertragungsart Sie für die Verbindung zu Ihrem lokalen Netz verwenden.

Mögliche Werte:

□ Automatisch, 10 MBit/s halbduplex, 10 MBit/s vollduplex, 100 MBit/s halbduplex, 100 MBit/s vollduplex, 100 MBit/s automatisch, 1000 MBit/s vollduplex. Das Angebot der möglichen Werte kann modellabhängig variieren.

Besondere Werte:

□ In der Einstellung "Automatisch" wird die verwendete Übertragungsart passend zum verwendeten Anschluss automatisch ausgehandelt, dabei wird die maximal mögliche Übertragungsrate der beiden verbunden Schnittstellen verwendet.

□ Die Einstellung "100 MBit/s automatisch" entspricht der Einstellung "Automatisch", allerdings wird eine maximale Geschwindigkeit von 100 MBit/s ausgehandelt. Diese Einstellung ist im Zweifelsfall einer festen Einstellung auf 100 MBit/s vorzuziehen, da so mögliche Duplex-Konflikte verhindert werden können.

Default:

□ Automatisch

Durch die manuelle Einstellung auf "100 MBit/s vollduplex" kann bei einigen Modellen mit Gigabit-Schnittstelle und Temperatursensor ein erweiterter Temperaturbereich genutzt werden. Bei diesen Modellen wird die Übertragungsart in der Einstellung "Automatisch" auf maximal 100 MBit/s begrenzt, solange die aktuelle

Temperatur des Gerätes einen gerätespezifischen Wert überschreitet. Sinkt die Temperatur wieder unter den Grenzwert, wird automatisch die höhere Übertragungsrate verwendet. Eine Unterbrechung aufgrund der Aushandlung der Übertragungsrate ist in den WLAN-Netzwerken (SSIDs) der Access Points nicht festzustellen. Weitere Informationen zu den zulässigen Temperaturbereichen finden Sie in den technischen Daten der Geräte.

A.3 Standard-Verschlüsselung mit WPA2

Im werksseitigen Auslieferungszustand bzw. nach einem Reset unterscheiden sich LANCOM Access Points und LANCOM Wireless Router.

- Unkonfigurierte Access Points können im Auslieferungszustand nicht über die WLAN-Schnittstelle in Betrieb genommen werden. Die WLAN-Module sind ausgeschaltet, die Geräte suchen selbstständig im LAN einen LANCOM WLAN Controller, von dem sie automatisch eine Konfiguration beziehen können.
- Unkonfigurierte Wireless Router können auch im Auslieferungszustand über die WLAN-Schnittstelle in Betrieb genommen werden. Dazu wird standardmäßig die hier beschriebene Standard-Verschlüsselung mit WPA-PSK verwendet.

Der Preshared Key für die Standard-WPA-Verschlüsselung setzt sich aus dem Anfangsbuchstaben „L" gefolgt von der LAN-MAC-Adresse des Access Points in ASCII-Schreibweise zusammen. Die LAN-MAC-Adressen der LANCOM-Geräte beginnen immer mit der Zeichenfolge „00A057". Sie finden die LAN-MAC-Adresse auf einem Aufkleber auf der Unterseite des Gerätes. Verwenden Sie **nur** die als „LAN MAC address" gekennzeichnete Nummer, die mit „00A057" beginnt. Bei den anderen ggf. angegebenen Nummern handelt es sich **nicht** um die LAN-MAC-Adresse!



Für ein Gerät mit der LAN-MAC-Adresse „00A05713B178" lautet der Preshared Key also „L00A05713B178". Dieser Schlüssel ist in den 'WPA-/Einzel-WEP-Einstellungen' des Gerätes für jedes logische WLAN-Netzwerk als 'Schlüssel 1/Passphrase' eingetragen.

Um mit einer WLAN-Karte eine Verbindung zu einem LANCOM Wireless Router im Auslieferungszustand herzustellen, muss in der WLAN-Karte die WPA-Verschlüsselung aktiviert und der 13-stellige Preshared Key eingetragen werden.

Ändern Sie den Preshared Key für WPA nach der ersten Anmeldung, um eine sichere Verbindung zu gewährleisten.

A.4 APSD – Automatic Power Save Delivery

A.4.1 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 Access Points 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 Access Point 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.

A.4.2 Konfiguration

WEBconfig: LCOS-Menübaum ▶ 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.

A.4.3 Statistik

WEBconfig: LCOS-Menübaum ▶ 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.

■ **WEBconfig: LCOS-Menübaum ▶ Status ▶ WLAN ▶ Stationstabelle**

Zeigt in einer Bitmaske an, für welche Zugriffskategorien der eingebuchte WLAN-Client APSD nutzt:

□ Voice (höchste Priorität)

□ Video

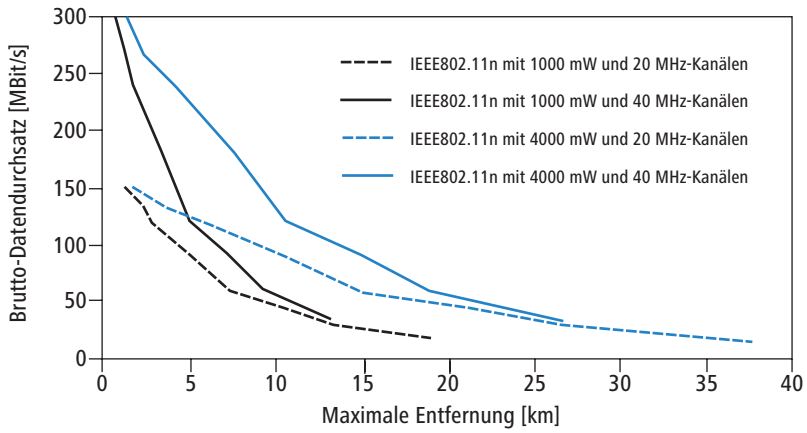
□ Best effort (einschließlich Datenverkehr von "Legacy Power Save"-Clients)

□ Background (geringste Priorität).

A.5 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 Access Points auf Basis von 802.11n sowie alle aktuellen LANCOM 54 Mbit/s Access Points unterstützen BFWA ab der LCOS-Version 7.70. Bei älteren Access Points 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.de.

A.6 RADIUS-Accounting neu starten

Die Accounting-Funktion im LANCOM 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.

WEBconfig: LCOS-Menübaum ▶ Setup ▶ WLAN ▶ RADIUS-Accounting

- **Neustart-Accounting**

  Beendet alle aktuellen Accounting-Sitzungen und eröffnet gegenüber dem RADIUS-Server entsprechende neue Accounting-Sitzungen.

A.7 Voucher für Public-Spot mit Zeitbudget

A.7.1 Einleitung

Mit Hilfe des Voucher Druck-Assistenten richten Sie zeitlich begrenzte Zugänge zu einem Public-Spot-WLAN mit wenigen Mausklicks ein. Dabei wird lediglich die Nutzungsdauer des Zugangs festgelegt, Benutzername und Kennwort werden automatisch vergeben und in die Konfiguration des LANCOM-Gerätes eingetragen. Als Ergebnis wird ein personalisierter Gutschein (Voucher) ausgedruckt, mit dem sich der Anwender im Public-Spot-WLAN für eine begrenzte Zeit anmelden kann.

Damit die Vouchers nicht immer genau in dem Moment ausgedruckt werden müssen, wenn ein Anwender einen Zugang zum Public-Spot-WLAN wünscht, können die Gutscheine auch auf Vorrat ausgedruckt werden. Dabei wird der Zugang so eingestellt, dass die Nutzungsdauer erst ab dem ersten Login mit den zugehörigen Zugangsdaten läuft. Dazu wird eine maximale Gültigkeitsdauer des Zugangs definiert – nach dieser Zeit wird der Zugang automatisch gelöscht, auch wenn die Nutzungsdauer noch nicht genutzt wurde.

Zeitlich begrenzte Public-Spot-Zugänge können nur eingerichtet werden, wenn das LANCOM über die korrekte Uhrzeit verfügt.

In den LCOS-Versionen vor 7.70 wurden Public-Spot-Zugänge über den Assistenten in der Benutzer-Liste des Public-Spot-Moduls eingetragen. Ab der LCOS-Version 7.70 speichert der Assistent die Public-Spot-Zugänge in der Benutzerdatenbank des internen RADIUS-Servers. Um diese Public-Spot-Zugänge nutzen zu können, muss der RADIUS-Server im LANCOM konfiguriert sein. Bitte beachten Sie dazu die Hinweise unter 'RADIUS-Server für Public-Spot-Nutzung konfigurieren' → Seite 5.

A.7.2 Public-Spot-Benutzer einrichten und Voucher drucken

Zum Einrichten des Public-Spot-Zugangs ruft der Mitarbeiter in seinem Browser die IP-Adresse des Wireless Routers oder Access Points auf (z. B. über eine Verknüpfung auf dem Desktop) und meldet sich mit seinem Benutzernamen und Kennwort an. Sofern sein Administrator-Zugang entsprechend eingestellt ist, kann der Mitarbeiter ausschließlich den Assistenten zum Einrichten der Public-Spot-Benutzer ausführen.

① Nach dem Starten des Assistenten stellen Sie die Nutzungsdauer für den Zugang ein.

② Wählen Sie aus, ob der Zugang sofort aktiviert werden soll oder ob die Nutzungsdauer erst mit dem ersten Login startet.

③ Bei einer Nutzungsdauer nach erstem Login geben Sie die Dauer in Tagen ein, nach welcher der Zugang spätestens abläuft (Gültigkeitsdauer).

④ Im Kommentarfeld tragen Sie optional einen Text ein, der den Nutzer eindeutig identifiziert (z.B. Name oder Raumnummer des Hotelgastes). Alternativ zum vordefinierten Kommentarfeld können auch bis zu fünf kundenspezifische Kommentarfelder verwendet werden.

⑤ Klicken Sie danach auf **Benutzerdaten speichern und drucken**, um die Zugangsdaten im Gerät zu speichern und auszudrucken.

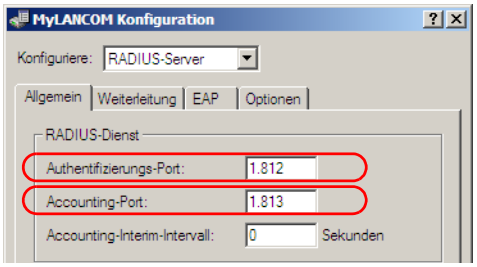
Hinweise zu den Rechten und Pflichten für Betreiber von öffentlichen Public-Spot-Zugängen finden Sie im entsprechenden LANCOM Whitepaper unter www.lancom.de.



A.7.3 RADIUS-Server für Public-Spot-Nutzung konfigurieren

In den LCOS-Versionen vor 7.70 wurden Public-Spot-Zugänge über den Assistenten in der Benutzer-Liste des Public-Spot-Moduls eingetragen. Ab der LCOS-Version 7.70 speichert der Assistent die Public-Spot-Zugänge nicht mehr in dieser Liste, sondern in der Benutzerdatenbank des internen RADIUS-Servers. Um diese Public-Spot-Zugänge nutzen zu können, **muss** der RADIUS-Server konfiguriert und das Public-Spot-Modul auf die Nutzung des RADIUS-Servers eingestellt sein.

① Damit die Benutzer-Datenbank im internen RADIUS-Server genutzt werden kann, muss der RADIUS-Server im LANCOM zunächst eingeschaltet werden. Aktivieren Sie den RADIUS-Server durch das Eintragen von Authentifizierungs- und Accouting-Port. Verwenden Sie den Authentifizierungs-Port 1.812 und den Accounting-Port 1.813.



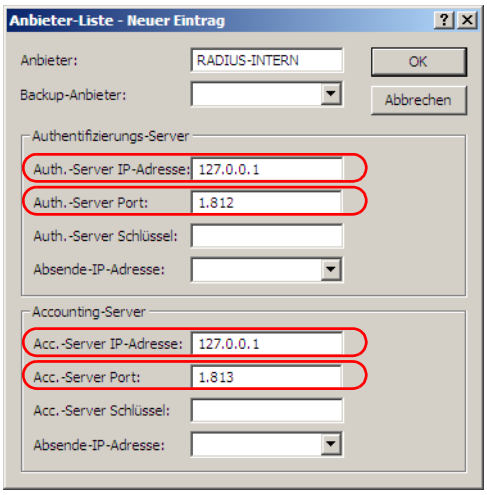
LANconfig: RADIUS ▶ Allgemein

WEBconfig: LCOS-Menübaum ▶ Setup ▶ RADIUS ▶ Server ▶ Authentifizierungs- und Accouting-Port

② Damit die Public-Spot-Zugänge am internen RADIUS-Server des LANCOMs authentifiziert werden können, muss der Public-Spot die Adresse des RADIUS-Servers kennen. Erstellen Sie dazu für den internen RADIUS-Server einen neuen Eintrag als "Anbieter". Tragen Sie die IP-Adresse des LANCOMs, in dem der RADIUS-Server aktiviert wurde, als Authentifizierungs- und Accouting-Server ein.

Wenn der Public-Spot und der RADIUS-Server vom gleichen LANCOM bereitgestellt werden, tragen Sie hier die interne Loopback-Adresse des Geräts (127.0.0.1) ein.

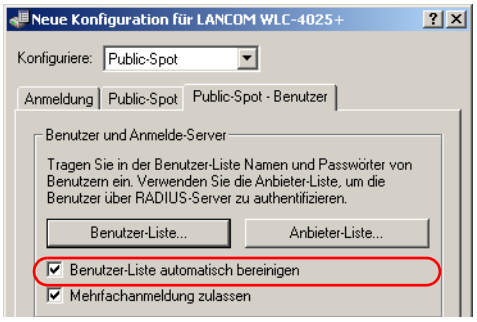
③ Übernehmen Sie Authentifizierungs- und Accouting-Port von der Einstellung im RADIUS-Server (1.812 und 1.813).



LANconfig: Public-Spot ▶ Public-Spot-Benutzer ▶ Anbieter-Liste

WEBconfig: LCOS-Menübaum ▶ Setup ▶ Public-Spot-Modul ▶ Anbieter-Tabelle

④ Aktivieren Sie im Public-Spot-Modul die Option zum Bereinigen der Benutzer-Liste, damit die nicht mehr benötigten Einträge automatisch gelöscht werden können.



LANconfig: Public-Spot ▶ Public-Spot-Benutzer

WEBconfig: LCOS-Menübaum ▶ Setup ▶ RADIUS ▶ Server

Nach einem Update auf LCOS 7.70 sind die mit der vorherigen LCOS-Version angelegten Benutzerkonten in der Benutzer-Liste des Public-Spot-Moduls weiterhin gültig.

A.7.4 Interner und externer RADIUS-Server kombiniert

Für die Authentifizierung der internen WLAN-Benutzer 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 wird dazu die entsprechende Weiterleitung der RADIUS-Anfragen an den externen RADIUS-Server definiert.

Die im folgenden beschriebenen Einstellungen sind nur dann notwendig, wenn Sie neben dem Public Spot im LANCOM 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.

Realm-Tagging für das RADIUS-Forwarding

Die Authentifizierungsanfragen der beiden Benutzergruppen müssen separat behandelt werden. Damit der WLAN Controller diese beiden Gruppen unterscheiden kann, werden so genannte "Realms" eingesetzt. Realms dienen der Adressierung von Domänen, innerhalb derer Benutzeraccounts gültig sind. Die Realms können mit der Authentifizierungsanfrage an den RADIUS-Server im WLAN Controller übermittelt werden. Alternativ kann der RADIUS-Server nach folgenden Regeln die Realms der Benutzernamen verändern, um das RADIUS-Forwarding zu steuern:

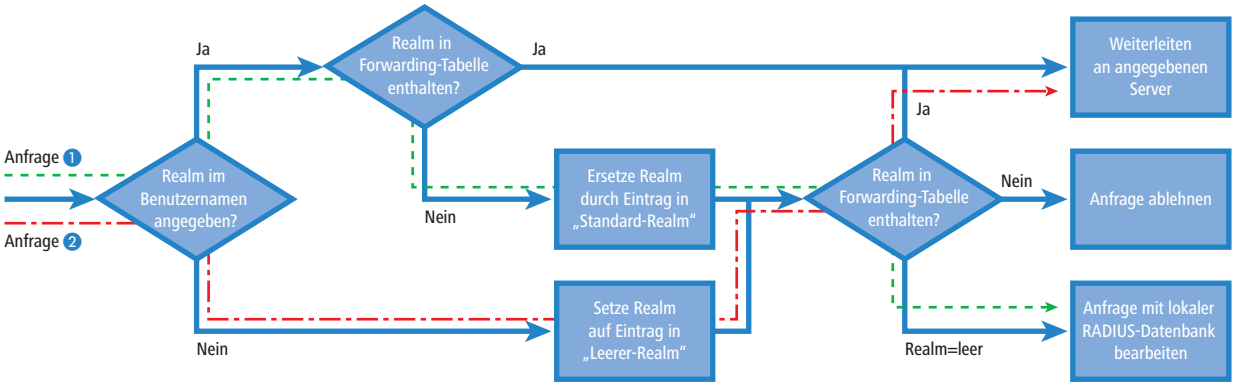
- Der als "Standard-Realm" definierte Wert ersetzt einen vorhandenen Realm einer eingehenden Anfrage, wenn für diesen Realm keine Weiterleitung definiert ist.

■ Der unter "Leerer-Realm" definierte Wert wird **nur dann** verwendet, wenn der eingehende Benutzername **noch keinen** Realm enthält.

Über einen Eintrag in der Weiterleitungstabelle können alle Authentifizierungsanfragen mit einem bestimmten Realm an einen RADIUS-Server weitergeleitet werden. Wenn in der Weiterleitungstabelle kein passender Eintrag vorhanden ist, wird die Anfrage abgelehnt.

Wenn nach der Ermittlung eines Realms ein leerer Realm festgestellt wird, so wird die Authentifizierungsanfrage **immer** mit der internen RADIUS-Datenbank des LANCOMs geprüft.

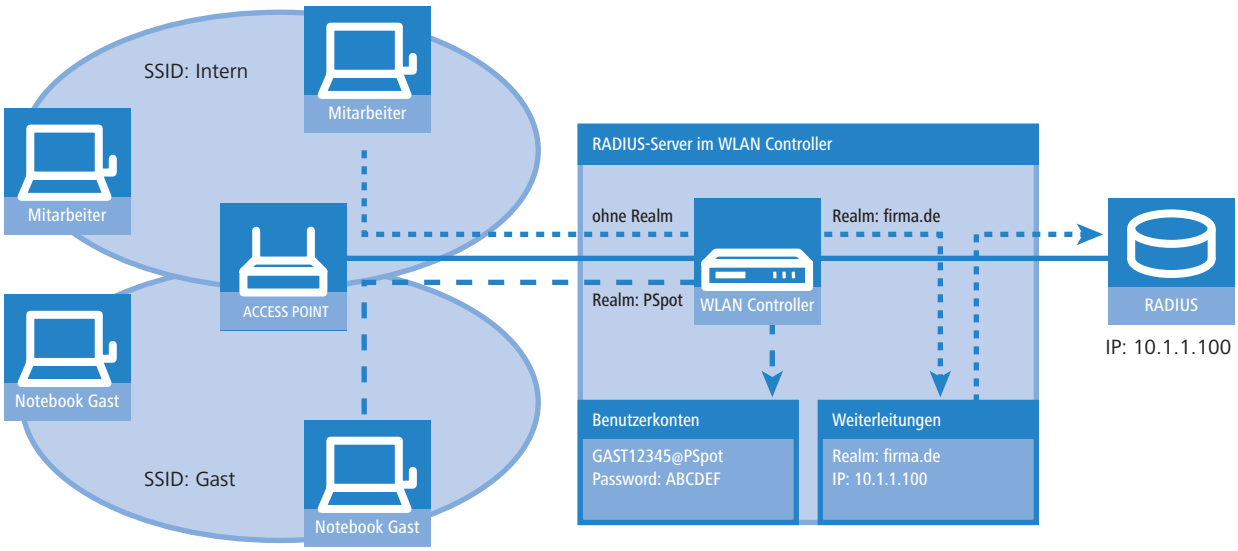
Das folgende Flussdiagramm zeigt schematisch die Arbeitsweise des RADIUS-Server bei der Verarbeitung von Realms:



Durch ein unterschiedliches Realm-Tagging können somit verschiedene RADIUS-Server angesprochen werden. Den Entscheidungsweg im RADIUS-Server des LANCOMs 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, werden alle Authentifizierungsanfragen mit diesem Realm an den internen RADIUS-Server weitergeleitet.

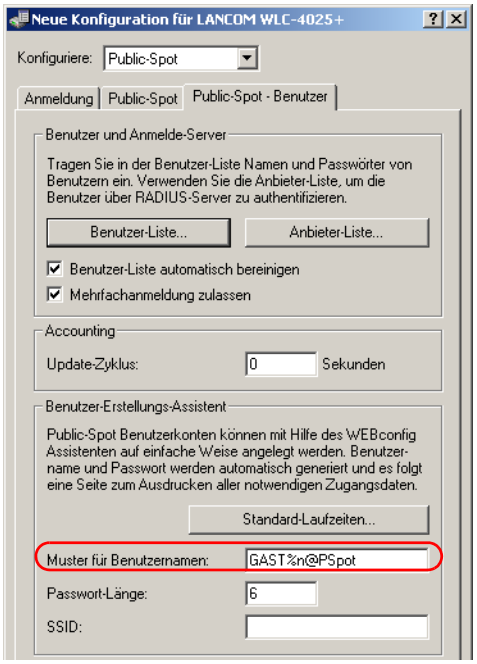
2. Um den Konfigurationsaufwand zu begrenzen, werden die internen Benutzer weiterhin ohne Realm geführt. Der RADIUS-Server im LANCOM kann einen leeren Realm automatisch durch einen anderen Realm ersetzen, mit dem die internen Benutzer identifiziert werden. In diesem Beispiel wird der leere Realm durch die Domäne der Firma "firma.de" ersetzt. Mit den Angaben in der Weiterleitungstabelle können alle Authentifizierungsanfragen mit diesem Realm an den externen RADIUS-Server weitergeleitet werden.



Konfiguration für das RADIUS-Forwarding

Mit den folgenden Konfigurationsschritten können Sie die separate Behandlung der internen Benutzer und der Gastzugänge definieren.

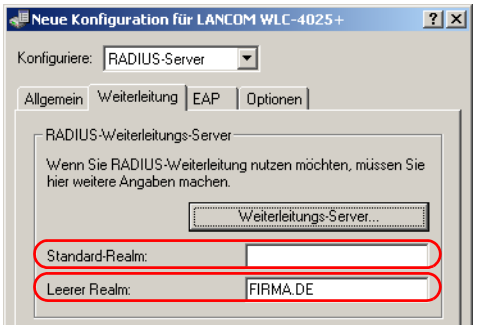
① Passen Sie im Public Spot das Muster für die Benutzernamen so an, dass ein eindeutiger Realm verwendet wird. Mit dem Muster "GAST%n@PSpot" werden z. B. Benutzernamen der Form "GAST12345@PSpot" erzeugt.



LANconfig: Public-Spot ▶ Public-Spot-Benutzer

WEBconfig: LCOS-Menübaum ▶ Setup ▶ Public-Spot-Modul

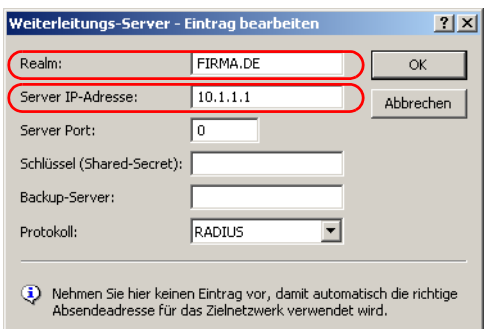
② Tragen Sie im RADIUS-Server des WLAN Controllers einen "leeren Realm" ein (z. B. "FIRMA.DE"). Dieser Realm wird für alle Benutzernamen verwendet, die ohne Realm eine Authentifizierungsanfrage bei dem WLAN Controller stellen. Das sind in dieser Anwendung die internen Benutzer, für die kein Realm definiert ist. Damit der RADIUS-Server des WLAN Controllers für diese Benutzernamen auch keinen Realm einsetzt, muss der "Standard-Realm" unbedingt leer bleiben.



LANconfig: RADIUS-Server ▶ Weiterleitung

WEBconfig: LCOS-Menübaum ▶ Setup ▶ RADIUS ▶ Server

③ Damit die Authentifizierungsanfragen der internen Benutzer an den externen RADIUS-Server weitergeleitet werden, 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.



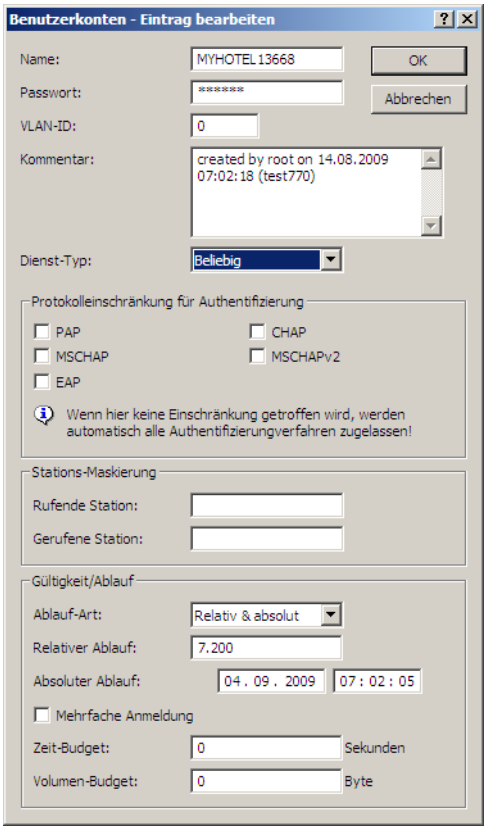
LANconfig: RADIUS-Server ▶ Weiterleitung ▶ Weiterleitungs-Server

WEBconfig: LCOS-Menübaum ▶ Setup ▶ RADIUS ▶ Server ▶ Weiterleit.-Server

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.

A.8 Erweiterungen im RADIUS-Server

Für die Einrichtung von Public-Spot-Benutzern mit Zeit- und Volumen-Budgets sind zusätzliche Parameter in der Benutzertabelle des RADIUS-Servers erforderlich.



LANconfig: RADIUS ▶ Allgemein ▶ Benutzerkonten

WEBconfig: LCOS-Menübaum ▶ Setup ▶ RADIUS ▶ Server ▶ Benutzer

■ **Mehrfach-Logins**

Erlaubt die mehrfache Anmeldung mit einem Benutzer-Account zur gleichen Zeit.

Mögliche Werte:

□ Ja, Nein

Default:

□ Ja

Die Option für die Mehrfach-Logins muss deaktiviert werden, wenn der RADIUS-Benutzer ein Zeit-Budget erhalten soll. Die Einhaltung des Zeit-Budgets kann nur überwacht werden, wenn für den Benutzer zu jeder Zeit nur eine Sitzung aktiv ist.

■ **Ablauf-Art**

Diese Option legt fest, wie die Gültigkeitsdauer des Benutzer-Accounts bestimmt wird.

Mögliche Werte:

□ Absolut: Die Gültigkeit des Benutzer-Accounts endet zu einem festen Zeitpunkt.

□ Relativ: Die Gültigkeit des Benutzer-Accounts endet eine bestimmte Zeitspanne nach dem ersten erfolgreichen Login des Benutzers.

Default:

□ Leer: Die Gültigkeit des Benutzer-Accounts endet nie, es sei denn, ein definiertes Zeit- oder Volumen-Budget wird erreicht.

Die beiden Optionen können kombiniert werden. In diesem Fall endet die Gültigkeit des Benutzer-Accounts dann, wenn einer der beiden Grenzwerte erreicht wird.

Für die Nutzung der Zeit-Budgets bei Benutzer-Accounts muss das Gerät über eine gültige Zeit verfügen, da ansonsten der Ablauf der Gültigkeit nicht geprüft werden kann.

■ **Abs.-Ablauf**

Wenn der Ablauf-Typ "Absolut" aktiviert ist, endet die Gültigkeit des Benutzer-Accounts zu dem in diesem Wert angegebenen Zeitpunkt.

Mögliche Werte:

□ Gültige Zeitinformation aus Datum und Uhrzeit. Maximal 20 Zeichen aus `0123456789/:.Pp`

Default:

□ Leer

Besondere Werte:

□ 0 schaltet die Überwachung der absoluten Ablaufzeit aus.

■ **Rel.-Ablauf**

Wenn der Ablauf-Typ "Relativ" aktiviert ist, endet die Gültigkeit des Benutzer-Accounts nach der in diesem Wert angegebenen Zeitspanne nach dem ersten erfolgreichen Login des Benutzers.

Mögliche Werte:

□ Zeitspanne in Sekunden. Maximal 10 Zeichen aus `0123456789`

Default:

□ 0

Besondere Werte:

□ 0 schaltet die Überwachung der relativen Ablaufzeit aus.

■ **Zeit-Budget**

Maximale Nutzungsdauer für diesen Benutzer-Account. Diese Nutzungsdauer kann der Benutzer bis zum Erreichen einer ggf. definierten relativen oder absoluten Ablaufzeit ausschöpfen.

Mögliche Werte:

□ Zeitspanne in Sekunden. Maximal 10 Zeichen aus `0123456789`

Default:

□ 0

Besondere Werte:

□ 0 schaltet die Überwachung der Nutzungsdauer aus.

■ **Volumen-Budget**

Maximales Datenvolumen für diesen Benutzer-Account. Dieses Datenvolumen kann der Benutzer bis zum Erreichen einer ggf. definierten relativen oder absoluten Ablaufzeit ausschöpfen.

Mögliche Werte:

□ Volumen-Budget in Bytes. Maximal 10 Zeichen aus `0123456789`

Default:

□ 0

Besondere Werte:

□ 0 schaltet die Überwachung des Datenvolumens aus.

■ **Kommentar**

Kommentar zu diesem Eintrag.

■ **Service-Typ**

Der Service-Typ ist ein spezielles Attribut des RADIUS-Protokoll, welches der NAS (Network Access Server) mit dem Authentication Request übermittelt. Der Request wird nur dann positiv beantwortet, wenn der angefragte Service-Typ mit dem Service-Typ des Benutzer-Accounts übereinstimmt.

Mögliche Werte:

□ Umrahmt: Für Prüfung von WLAN-MAC-Adressen über RADIUS bzw. bei IEEE 802.1x.

□ Login: Für Public-Spot-Anmeldungen.

□ Nur-Auth.: Für Einwahl-Gegenstellen über PPP, die mit RADIUS authentifiziert werden.

□ Beliebig

Default:

□ Beliebig

Die Anzahl der Einträge mit dem Service-Typ "Beliebig" oder "Login" ist je nach Modell auf 64 oder 256 begrenzt. So wird die Tabelle nicht vollständig mit Einträgen von Public-Spot-Zugängen belegt (die den Service-Typ "Beliebig" verwenden) und ermöglicht eine parallele Nutzung für Anmeldungen über 802.1x.

A.9 IGMP Snooping

A.9.1 Einleitung

Alle LANCOM-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 ungedingt 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 LANCOM 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) stellt die TCP/IP-Protokollfamilie ein Protokoll bereit, mit dem 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 nutzt 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.

IGMP kann als Layer-3-Protokoll 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 zunächst keine Funktionen bietet, 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-Subnetzen weiterleiten kann. Dieses Verfahren wird als IGMP 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 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 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-Subnetzen weiterleiten kann.
- Eine Multicast-Gruppe ist "nicht registriert", wenn kein Port der Bridge Mitglied dieser Multicast-Gruppe ist.

A.9.2 Ablauf des IGMP 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.

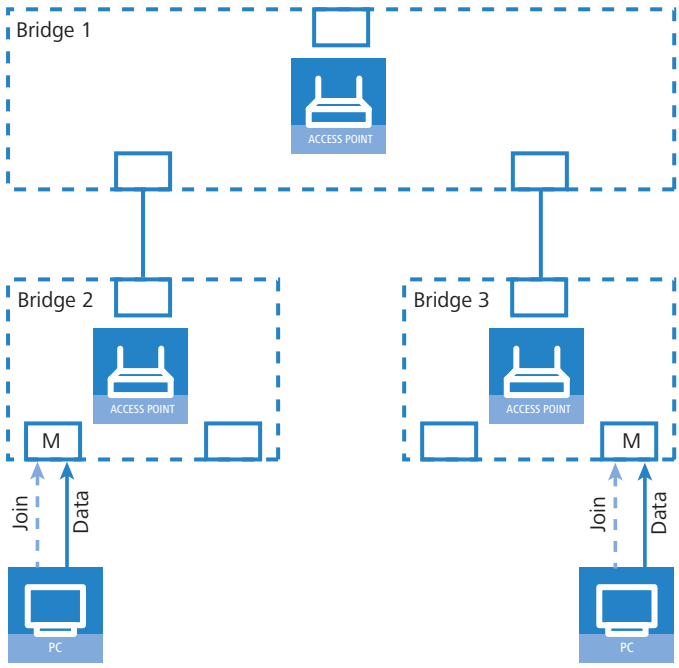
Für die IP-Multicast-Pakete werden zwei Typen unterschieden (abgeschnittene Pakete oder Pakete mit ungültiger Prüfsumme werden dabei verworfen):

- IGMP-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.
  - Entsprechend führt eine Leave-Message dazu, dass der Port, über den das Paket eingeht, aus der entsprechenden Multicast-Gruppe entfernt wird. Auch diese Nachricht wird nur an Router-Ports weitergeleitet.
  - Eine eingehende IGMP-Anfrage macht den Port zu einem Router-Port. Diese Nachrichten werden an alle Ports weitergeleitet.
  - Alle anderen IGMP-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-Nachricht handelt, wird die Ziel-Adresse ausgewertet. Pakete für die Zieladresse "224.0.0.x" werden dabei an alle Ports weitergeleitet, weil dieser "reservierte" Bereich von Protokollen ohne richtige IGMP-Registrierung verwendet wird. Für alle anderen Pakete wird die Zieladresse in der Tabelle der IGMP-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.

  In beiden Fällen werden die Pakete an alle Router-Ports weitergeleitet.

A.9.3 IGMP Snooping über mehrere Bridges hinweg

Wie beschrieben leitet IGMP 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-Anfragen zu Router-Ports werden können, muss einer der Multicast-fähigen Router im Netzwerk die Aufgabe übernehmen, die benötigten IGMP-Anfragen in Netzwerk zu streuen. Dieser Router wird auch als IGMP-Querier bezeichnet. Für den Fall, dass kein Multicast-Router im Netzwerk vorhanden ist, können die LANCOM 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-Informationen durch den Querier lässt sich an folgendem Beispiel erklären:

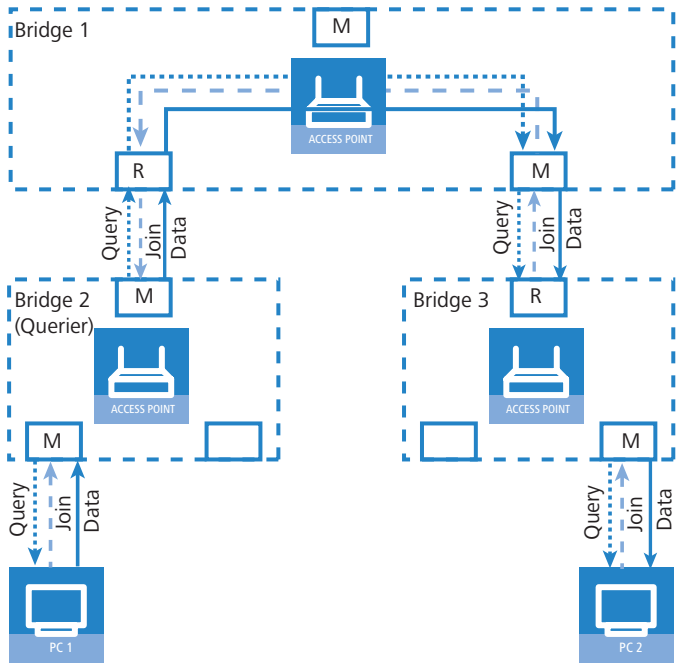
① Der Querier (im Beispiel Bridge 2) sendet in regelmäßigen Abständen IGMP-Anfragen über alle verfügbaren Ports aus (gepunktete Linien). Diese Anfragen kennzeichnen in der nächsten Bridge (Bridge 1) den Port, auf dem die Anfrage eingeht, als Router-Port (R). PC 1 antwortet auf diese Anfrage mit einer 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 diese 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.

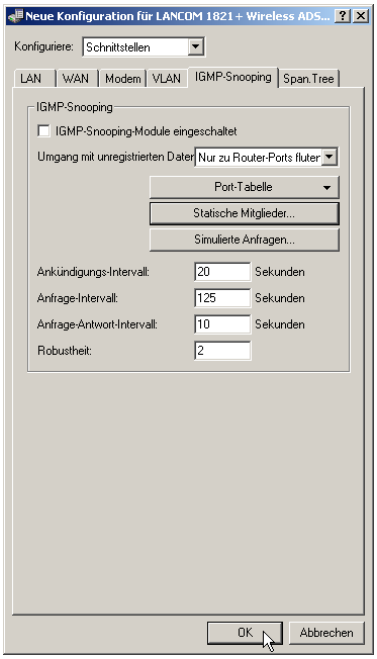
⑤ Im letzten Schritt leitet Bridge 1 die Join-Nachricht von PC 2 über den Router-Port weiter an Bridge 2, wo der empfangende Port ebenfalls Mitglied der Multicast-Gruppen von PC 2 wird.



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.

A.9.4 Konfiguration

Allgemeine Einstellungen



LANconfig: Schnittstellen ▶ IGMP-Snooping

WEBconfig: LCOS-Menübaum ▶ Setup ▶ LAN-Bridge ▶ IGMP-Snooping

■ **In-Betrieb**

Aktiviert oder deaktiviert IGMP Snooping für das Gerät und alle definierten Querier-Instanzen. Ohne IGMP Snooping verhält sich die Bridge wie ein einfacher Switch und sendet alle Multicast auf alle Ports weiter.

Mögliche Werte:

□ Ja, Nein

Default:

□ Nein

Wenn diese Funktion deaktiviert ist, werden alle IP-Multicast-Pakete auf alle Ports gesendet. Bei einer Änderung des Betriebszustandes wird die IGMP-Snooping-Funktion vollständig zurückgesetzt, d.h. alle dynamische gelernten Werte (Mitgliedschaften, Router-Port-Eigenschaften) werden gelöscht.

■ **Anfrage-Intervall**

Intervall in Sekunden, in dem ein Multicast-fähiger Router (oder ein simulierter Querier) IGMP-Anfragen an die Multicast-Adresse 224.0.0.1 schickt und damit Rückmeldungen der Stationen über die Mitgliedschaft in Multicast-Gruppen auslöst. Diese regelmäßigen Abfragen beeinflussen den Zeitpunkt, nach dem die Mitgliedschaft in bestimmten Multicast-Gruppen "altern" und gelöscht werden.

- □ Ein Querier sendet nach der Anfangsphase IGMP-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, beeinflusst das Timing zwischen den IGMP-Anfragen und dem Altern der Router-Ports bzw. Mitgliedschaften.

Intervall in Sekunden, in dem ein Multicast-fähiger Router (oder ein simulierter Querier) Antworten auf seine IGMP-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-Protokolls. Diese Option toleriert den Paketverlust von IGMP-Anfragen gegenüber den Join-Nachrichten.

Mögliche Werte:

- □ Zahl aus 10 Ziffern größer als 0.

Default:

- □ 2

■ **Werbe-Intervall**

Das Intervall in Sekunden, in dem die Geräte Pakete aussenden, mit denen sie sich als Multicast-fähige Router bekanntmachen. Aufgrund dieser Information können andere IGMP Snooping-fähige Geräte schneller lernen, welche ihrer Ports als Router-Ports verwendet werden 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-Anfragen.

Mögliche Werte:

- □ 4 bis 180 Sekunden

Default:

- □ 20

■ **Unregistrierte-Datenpakete-Behandlung**

Diese Option definiert die Verarbeitung von Multicast-Paketen mit Ziel-Adressen außerhalb des reservierten Adress-Bereiches "224.0.0.x", für die weder dynamisch gelernte noch statisch konfigurierte Mitgliedschaften vorhanden sind.

Mögliche Werte:

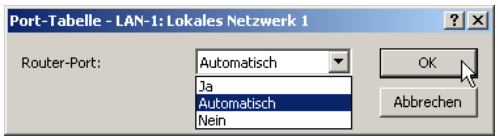
- □ Nur-Router-Ports: Sendet diese Pakete an alle Router-Ports.
- □ Fluten: Sendet diese Pakete an alle Ports.
- □ Verwerfen: Verwirft diese Pakete.

Default:

- □ Nur-Router-Ports

Port-Einstellungen

In dieser Tabelle werden die Port-bezogenen Einstellungen für IGMP Snooping vorgenommen.



LANconfig: Schnittstellen ▶ IGMP-Snooping ▶ Port-Tabelle

WEBconfig: LCOS-Menübaum ▶ Setup ▶ LAN-Bridge ▶ IGMP-Snooping ▶ Port-Einstellungen

■ **Port**

Auf diesen Port geziehen 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:

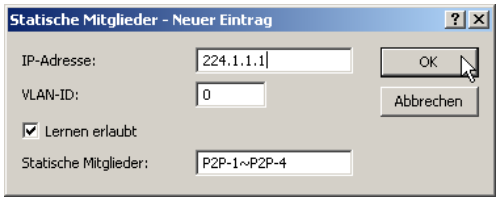
- □ Ja: Dieser Port verhält sich immer wie ein Router-Port, unabhängig von den IGMP-Anfragen oder Router-Meldungen, die auf diesem Port evtl. empfangen werden.
- □ Nein: Dieser Port verhält sich nie wie ein Router-Port, unabhängig von den IGMP-Anfragen oder Router-Meldungen, die auf diesem Port evtl. empfangen werden.
- □ Auto: Dieser Port verhält sich wie ein Router-Port, wenn eine IGMP-Anfragen oder Router-Meldung empfangen wurde. Der Port verliert diese Eigenschaft wieder, wenn für die Dauer von "Robustheit*Anfrage-Intervall+(Anfrage-Antwort-Intervall/2)" keine entsprechenden Pakete empfangen wurden.

Default:

- □ Auto

Statische-Mitglieder

Diese Tabelle erlaubt die manuelle Definition von Mitgliedschaften, die z.B. nicht automatisch gelernt werden können oder sollen.



LANconfig: Schnittstellen ▶ IGMP-Snooping ▶ Statische Mitglieder

WEBconfig: LCOS-Menübaum ▶ Setup ▶ LAN-Bridge ▶ IGMP-Snooping ▶ Statische-Mitglieder

■ **Adresse**

Die IP-Adresse der manuell definierten Multicast-Gruppe.

Mögliche Werte:

□ Gültige IP-Multicast-Adresse.

Default:

□ Leer

■ **VLAN-Id**

Die VLAN-ID, auf welche diese statische Mitgliedschaft angewendet werden soll. Für eine IP-Multicast-Adresse können durchaus mehrere Einträge mit unterschiedlichen VLAN-IDs gemacht werden.

Mögliche Werte:

□ 0 bis 4096.

Default:

□ 0

Besondere Werte:

□ Wenn "0" als VLAN gewählt wird, werden die IGMP-Anfragen ohne VLAN-Tag ausgegeben. Dieser Wert ist daher nur sinnvoll, wenn die Verwendung von VLAN generell deaktiviert ist.

■ **Lernen-erlauben**

Mit dieser Option wird das automatische Lernen von Mitgliedschaften für diese Multicast-Gruppe aktiviert. Wenn das automatische Lernen deaktiviert ist, werden die Pakete nur über die für die Multicast-Gruppe manuell definierten Ports verschickt.

Mögliche Werte:

□ Ja, Nein.

Default:

□ Ja

■ **Statische-Mitglieder**

An diese Ports werden die Pakete mit der entsprechenden IP-Multicast-Adresse immer zugestellt, unabhängig von empfangenen Join-Nachrichten.

Mögliche Werte:

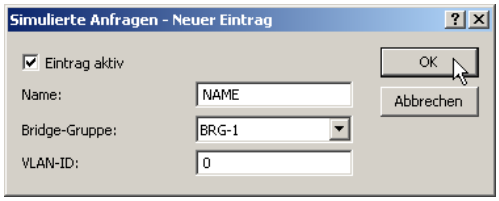
□ Kommaseparierte Liste der gewünschten Ports, maximal 215 alphanumerische Zeichen.

Default:

□ Leer

Simulierte-Anfrager

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 Snooping benötigt werden. Um die Querier auf bestimmte Bridge-Gruppen oder VLANs einzuschränken, können mehrere unabhängige Querier definiert werden, welche dann die entsprechenden VLAN-IDs nutzen.



LANconfig: Schnittstellen ▶ IGMP-Snooping ▶ Simulierte Anfragen

WEBconfig: LCOS-Menübaum ▶ Setup ▶ LAN-Bridge ▶ IGMP-Snooping ▶ Simulierte-Anfrager

■ **Name**

Name der Querier-Instanz.

Mögliche Werte:

□ 8 alphanumerische Zeichen.

Default:

□ Leer

■ **In-Betrieb**

Aktiviert oder deaktiviert die Querier-Instanz.

Mögliche Werte:

□ Ja, Nein.

Default:

□ Nein

■ **Bridge-Gruppe**

Schränkt die Querier-Instanz auf eine bestimmte Bridge-Gruppe ein.

Mögliche Werte:

□ Auswahl aus der Liste der verfügbaren Bridge-Gruppen, keine.

Default:

□ keine

Besondere Werte:

□ Wenn "keine" Bridge-Gruppe gewählt wird, werden die IGMP-Anfragen auf allen Brigde-Gruppen ausgegeben.

■ **VLAN-Id**

Schränkt die Querier-Instanz auf ein bestimmtes VLAN ein.

Mögliche Werte:

□ 0 bis 4096.

Default:

□ 0

Besondere Werte:

□ Wenn "0" als VLAN gewählt wird, werden die IGMP-Anfragen ohne VLAN-Tag ausgegeben. Dieser Wert ist daher nur sinnvoll, wenn die Verwendung von VLAN generell deaktiviert ist.

A.9.5 IGMP Status

Allgemeine Statistiken

Die Status-Meldungen zu IGMP Snooping finden Sie auf folgenden Pfaden:

WEBconfig: LCOS-Menübaum ▶ Status ▶ LAN-Bridge-Statistiken ▶ IGMP-Snooping

■ **In-Betrieb**

Zeigt an, ob das IGMP 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.

■ **Daten-Pakete**

Zeigt die gesamte Anzahl der nicht beschädigten IPv4-Multicast-Pakete, die auf allen Ports empfangen wurden, und bei denen es sich nicht um IGMP-Pakete handelt.

■ **Steuer-Pakete**

Zeigt die gesamte Anzahl der nicht beschädigten IGMP-Pakete, die auf allen Ports empfangen wurden.

■ **Defekte-Pakete**

Zeigt die gesamte Anzahl der beschädigten Daten- oder IGMP-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-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.

Port-Status

Diese Tabelle zeigt alle Port-bezogenen Statistiken.

WEBconfig: LCOS-Menübaum ▶ 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.
- **Daten-Pakete**
  Zeigt die gesamte Anzahl der nicht beschädigten IPv4-Multicast-Pakete, die auf diesem Port empfangen wurdenund bei denen es sich nicht um IGMP-Pakete handelt.
- **Steuer-Pakete**
  Zeigt die gesamte Anzahl der nicht beschädigten IGMP-Pakete, die auf diesem Port empfangen wurden.
- **Defekte-Pakete**
  Zeigt die gesamte Anzahl der beschädigten Daten- oder IGMP-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-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.

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.

WEBconfig: LCOS-Menübaum ▶ 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.

Simulierte-Anfrager

Die Tabelle zeigt den Status aller definierten und aktiven IGMP-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-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-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-Anfragen.

A.10 TACACS+

A.10.1 Einleitung

TACACS+ (Terminal Access Control Access Control Server) ist ein Protokoll für Authentifizierung, Authorisierung 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 einen 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 LANCOM 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, Authorisierung und Accounting möglich	Authentifizierung, Authorisierung 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 Authorisierung immer zusammen gehören, kann TACACS+ Authentifizierung und Authorisierung 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 LANCOM-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.

A.10.2 Konfiguration der TACACS+-Parameter

Die Parameter für die Konfiguration von TACACS+ finden Sie auf folgenden Pfaden:

WEBconfig: LCOS-Menübaum ▶ 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**

Aktiviert die Authentifizierung über einen TACACS+-Server. Wenn die TACACS+-Authentifizierung aktiviert ist, werden alle Authentifizierung-Anfragen über das TACACS+-Protokoll an den konfigurierten TACACS+-Server übertragen.

Mögliche Werte:

□ aktiviert, deaktiviert

Default

□ deaktiviert

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 LANCOM 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 LANCOM möglich wäre.

■ **Authorisierung**

Aktiviert die Authorisierung über einen TACACS+-Server. Wenn die TACACS+-Authorisierung aktiviert ist, werden alle Authorisierungs-Anfragen über das TACACS+-Protokoll an den konfigurierten TACACS+-Server übertragen.

Mögliche Werte:

□ aktiviert, deaktiviert

Default

□ deaktiviert

Die TACACS+-Authorisierung wird nur dann aktiviert, wenn ein erreichbarer TACACS+-Server definiert ist. Wenn die TACACS+-Authorisierung 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 LANCOM 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 LANCOM 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 LANCOM 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 LANCOM-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 Authorisierung voraussetzen. Da LANmonitor diese Werte regelmäßig abfragt, würde so eine große Zahl von eigentlich unnötigen TACACS+-Verbindungen aufgebaut. Wenn Authentifizierung, Authorisierung und Accounting für TACACS+ aktiviert sind, werden für jede Anfrage drei Sitzungen auf dem TACACS+-Server gestartet.

Mit diesem Parameter kann das Verhalten der LANCOM-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 LCOS-Menübaum ▶ 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-Authorisierung**

Mit diesem Parameter kann das Verhalten der LANCOM-Geräte bei SNMP-Zugriffen geregelt werden, um TACACS+-Sitzungen für die Authorisierung 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 Authorisierung über den TACACS+-Server erforderlich.

□ alle: In dieser Einstellung wird für alle SNMP-Zugriffe eine Authorisierung 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 Authorisierung 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.

A.10.3 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 TACSACS-Server finden Sie auf folgenden Pfaden:

WEBconfig: LCOS-Menübaum ▶ Setup ▶ TACACS+ ▶ Server

- **Server-Adresse**

  Adresse des TACACS+-Server, an den die Anfragen für Authentifizierung, Authorisierung und Accounting weitergeleitet werden sollen.

  Mögliche Werte:

  - Gültiger DNS-auflösbarer Name oder gültige IP-Adresse.

  Default

  - Leer

- **Loopback-Adresse**

  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

- **Kompatibilitätsmodus**

  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

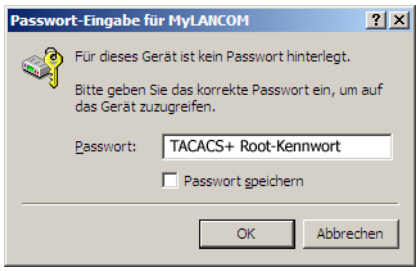
  - deaktiviert

A.10.4 Anmelden am TACACS+-Server

Sobald die Verwendung von TACACS+ für die Authentifizierung und ggf. Authorisierung aktiviert ist, werden alle Logins auf dem Gerät an den TACACS+-Server weitergeleitet. Der weitere Ablauf des Logins unterscheidet sich je nach Zugangsart.

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 die vollen Rechte eines Supervisors verfügt und somit die Konfiguration ohne Wechsel des Rechteniveaus bearbeiten darf. Wenn die Authorisierung benutzt wird entscheidet dies der TACACS+-Server.

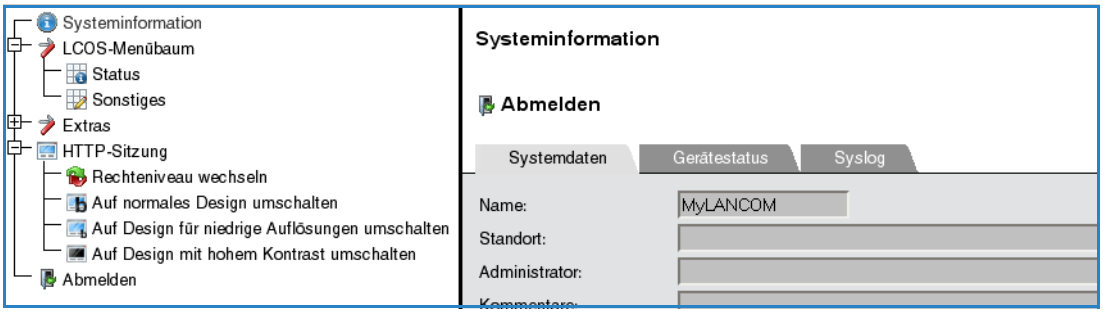
Wenn für das Gerät neben der Authentifizierung auch die Authorisierung aktiviert ist, müssen im TACACS+-Server für den Benutzer "root" die Befehle "readconfig" und "writeconfig" erlaubt werden, damit der Benutzer die Konfiguration aus dem Gerät auslesen und nach Änderung wieder einspielen kann ('Rechtezuweisung unter TACACS+' → Seite 25).

TACACS+-Anmeldung über WEBconfig

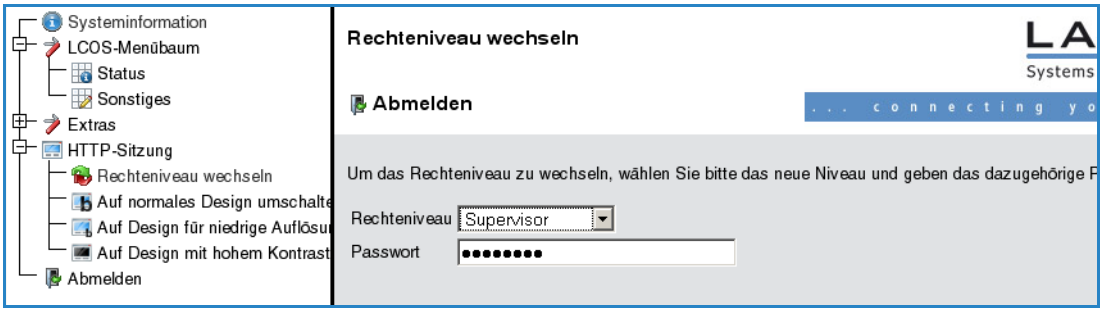
Die Anmeldung über WEBconfig an einem Gerät mit aktivierter TACACS+-Authentifizierung gelingt allen Benutzern, die im TACACS+-Server konfiguriert sind. Geben Sie beim Login über WEBconfig den Benutzernamen ein, der im TACACS+-Server konfiguriert ist, und wählen Sie den Server aus, an dem die Authentifizierung 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.

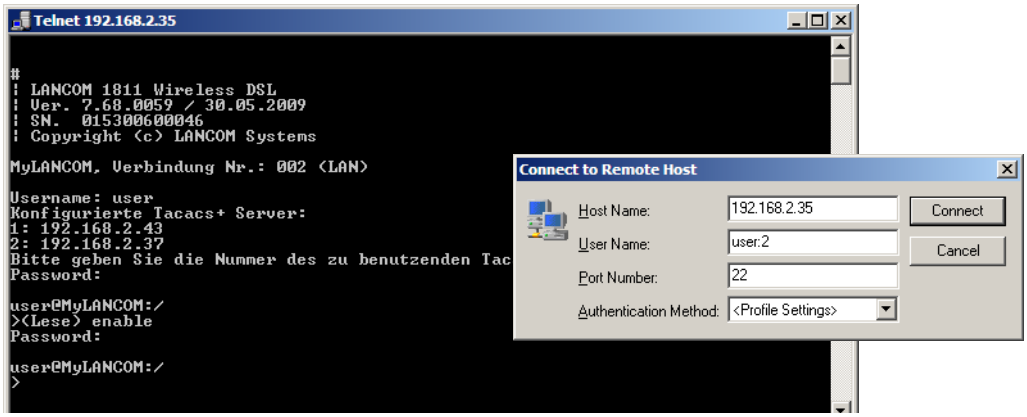
Die Kennwörter für die einzelnen Benutzerrechte werden dazu im TACACS+-Server als "enable"-Kennwörter konfiguriert.

Wenn für das Gerät neben der Authentifizierung auch die Authorisierung 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+' → Seite 25).

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-Komando nimmt als Parameter die Zahlen 1-15. 1 ist das niedrigeste, 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 Authorisierung 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+' → Seite 25).

A.10.5 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)

A.10.6 Authorisierung von Funktionen

Wenn für das Gerät neben der Authentifizierung auch die Authorisierung 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.

LANconfig

Befehl	Argumente	Bemerkung
readconfig	keine	Komplette Konfiguration auslesen
writeconfig	keine	Komplette Konfiguration schreiben

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.

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
time	Name des Parameters	Zeit einstellen
feature	Name des Parameters	Funktion hinzufügen
repeat	Name des Parameters	Befehl wiederholen
readmib	keine	SNMP-MIB auslesen
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.

SNMP

Befehl	Argumente	Bemerkung
get	SNMP-ID des Menüeintrags	Wert auslesen
set	SNMP-ID des Menüeintrags	Wert setzen

A.11 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 Ergebnis 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.

A.12 Firmware-Upload für UMTS-Modul im LANCOM 1751 UMTS

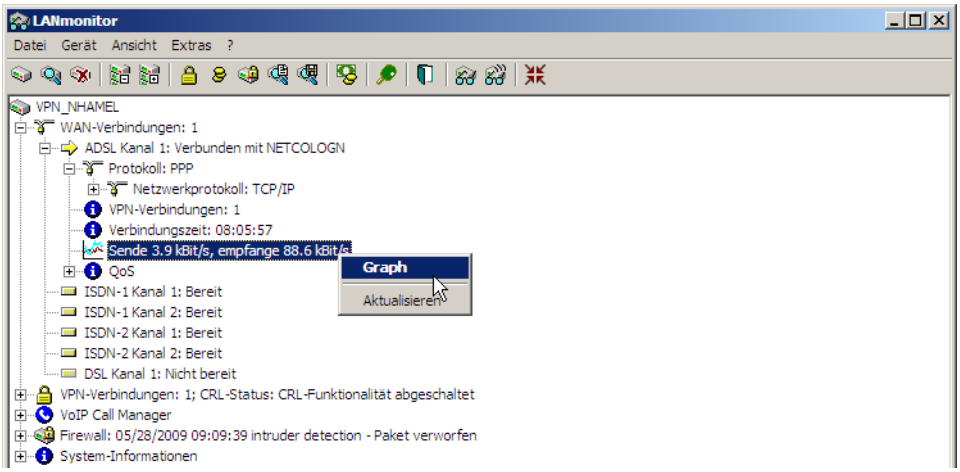
Für LANCOM 1751 UMTS mit einer Firmware ab der LCOS-Version 7.70 kann auch die Firmware für das UMTS-Modul komfortabel aktualisiert werden. Eine Firmware für das UMTS-Modul im UPX-Format kann auf allen Wegen in das LANCOM 1751 UMTS geladen werden, die auch für den Upload der LANCOM-Firmware bereitstehen.

A.13 Performance Monitoring im LANmonitor

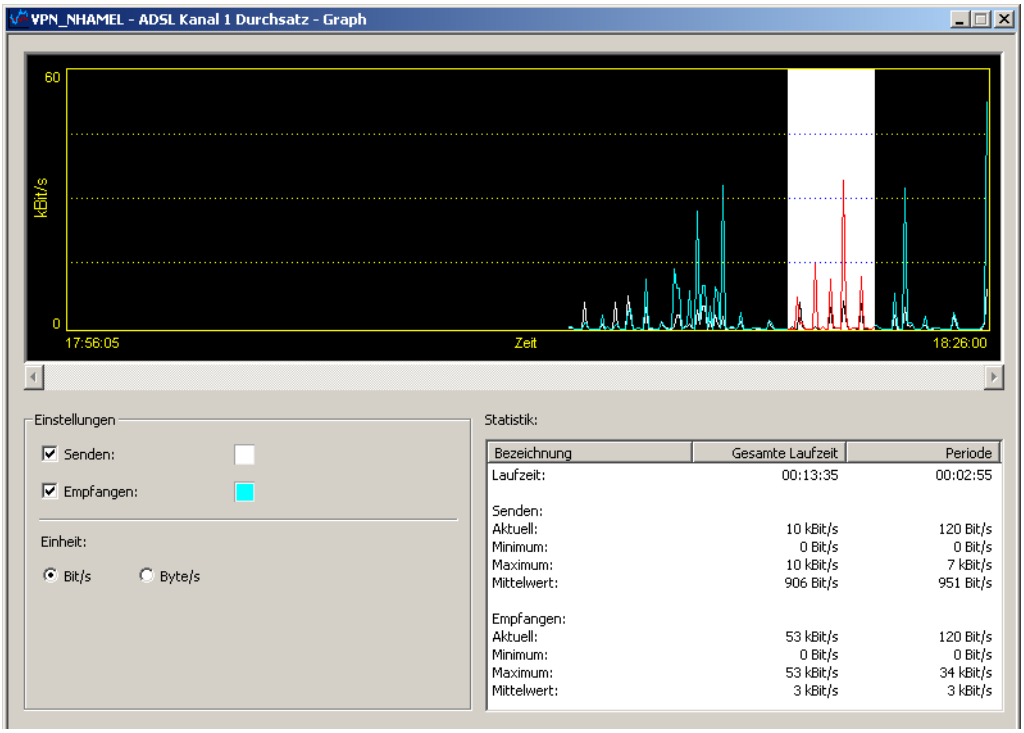
Der LANmonitor zeichnet verschiedene Kenngrößen der Geräte auf und stellt diese grafisch dar:

- 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 werden im LANmonitor direkt in der entsprechenden Gruppe angezeigt.



Mit einem Klick auf den Eintrag **Graph** im Kontextmenü öffnen Sie ein weiteres Fenster, in dem der zeitliche Verlauf der Kennwerte dargestellt wird.



Mit der linken Maustaste können Sie im aktuellen Graph eine Periode markieren, deren Werte in der Statistik separat angezeigt werden.

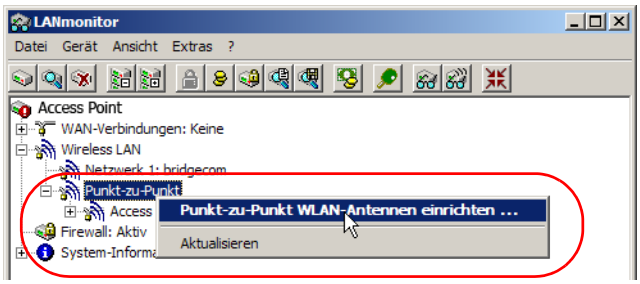
In diesem Dialog werden die aufgezeichneten Werte der letzen 24 Stunden dargestellt.

Bitte beachten Sie, dass die angezeigte Werte gelöscht werden, sobald der Dialog geschlossen wird. Für eine längere Überwachung lassen Sie das Fenster dauerhaft geöffnet.

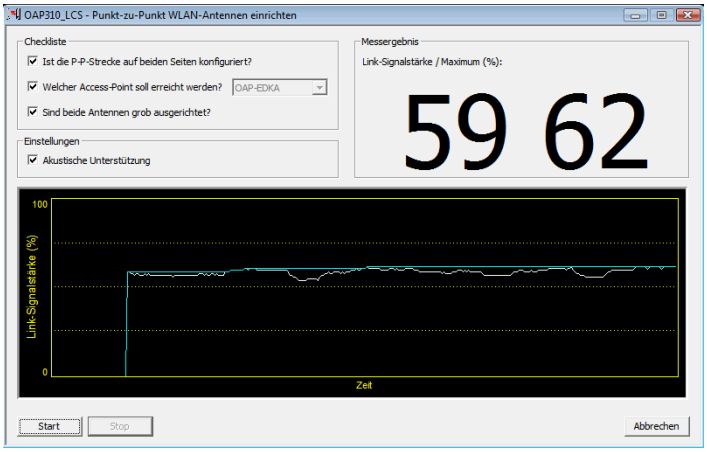
A.14 Einrichten von Punkt-zu-Punkt-Verbindungen mit dem LANmonitor

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 wir 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.

A Addendum zur LCOS-Version 7.8

A.1 Übersicht

■ 'DHCP-Cluster' →Seite 1
■ 'Abschalten von Ethernet-Schnittstellen' →Seite 2
■ 'ARF-Netzwerk für IAPP' →Seite 2
■ 'Routen von lokalen Diensten/ARP-Handling schaltbar' →Seite 3
■ 'XAUTH mit externem RADIUS-Server' →Seite 3
■ 'Erweiterte Zertifkats-Unterstützung' →Seite 4
■ 'Wildcard Matching von Zertifikaten' →Seite 5
■ 'Mehrere WLAN-Profile im Client-Modus' →Seite 6
■ 'Mittelwert der CPU-Lastanzeige' →Seite 7
■ 'TACACS+-Umgehung' →Seite 8
■ 'Erweiterungen für die seriellen COM-Ports' →Seite 8
■ '32 zusätzliche Gateways für PPTP-Verbindungen' →Seite 10
■ 'Zusätzliche Kommentarfelder zur Beschreibung der Geräte' →Seite 11
■ 'DHCP-Optionen mit LANconfig' →Seite 12
■ 'Ermittlung des Routing-Tags für lokale Routen' →Seite 13
■ 'Globale Einstellung von DiffServ für SIP & RTP' →Seite 13
■ 'Erhöhter DoS-Schwellwert für Zentralgeräte' →Seite 14

A.2 DHCP-Cluster

A.2.1 Einleitung

Wenn mehrere DHCP-Server in einem Netz aktiv sind, dann "verteilen" sich die Stationen im Netz gleichmäßig auf diese Server. Der DNS-Server der LANCOM-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.

A.2.2 Konfiguration

Der Betrieb eines DHCP-Servers im Cluster kann für jedes einzelne ARF-Netz in den zugehörigen DHCP-Einstellungen aktiviert bzw. deaktiviert werden.

WEBconfig: LCOS-Menübaum ▶ Setup ▶ DHCP ▶ Netzliste

■ **Cluster**

Wählen Sie hier aus, ob der DHCP-Server für dieses ARF-Netz im Cluster oder separat betrieben werden soll.

Mögliche Werte:

□ Ja: 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.

□ Nein: Der DHCP-Server verwaltet nur Informationen über die bei ihm selbst angeschlossenen Stationen.

Default:

□ Nein

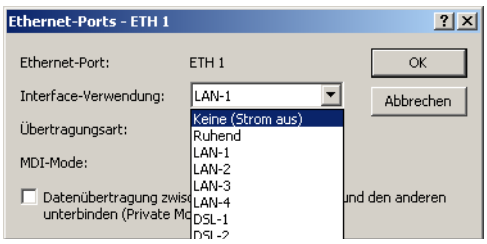


Wenn die Lease-Time der über DHCP zugewiesenen Informationen abläuft, schickt eine Station eine Anfrage zur Erneuerung an den DHCP-Server, von dem sie die Informationen erhalten hat (Renew-Request).
Falls der ursprüngliche DHCP-Server auf diesen Request nicht antwortet, versendet die Station eine Anfrage 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 regist-

riert 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).

A.3 Abschalten von Ethernet-Schnittstellen

Die Ethernet-Schnittstellen von öffentlich zugänglichen LANCOM-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 ▶ Interface-Einstellungen

WEBconfig: LCOS-Menübaum ▶ Setup ▶ Schnittstellen

■ **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.
- □ 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.

A.4 ARF-Netzwerk für IAPP

Access Points nutzen das IAPP-Protokoll, um sich über die Roaming-Vorgänge der eingebuchten WLAN-Clients zu informieren. Die Access Points senden dazu regelmäßig bestimmte Multicast-Nachrichten aus (Announces), mit deren Hilfe die Geräte die BSSIDs und IP-Adressen der anderen Access Points lernen. Bei einem Roaming-Vorgang informiert der WLAN-Client den neuen Access Point darüber, bei welchem Access Point er bisher eingebucht war. Der neue Access Point kann mit den aus den IAPP-Announces gelernten Informationen den bisherigen Access Point informieren, der den WLAN-Client umgehend aus seiner Tabelle der eingebuchten Clients entfernen kann.

Wenn in einem Access Point 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.

WEBconfig: LCOS-Menübaum ▶ 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.

A.5 Routen von lokalen Diensten/ARP-Handling schaltbar

A.5.1 Einleitung

Antwortpakete für interne Dienste (z.B. telnet, http/https, tftp, ...) des LANCOM 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: LANconfig/Gerätesuche).

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 Fällem empfielt sich die Einstellung "Interne Dienste routen".

A.5.2 Konfiguration

Mit einer entsprechenden Option in den Einstellungen für das IP-Routing können die internen Dienste des LANCOM über den Router geleitet werden.

WEBconfig: LCOS-Menübaum ▶ 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: Die Pakete werden direkt an den Absender zurückgeschickt.

Default:

- □ Nein

A.6 XAUTH mit externem RADIUS-Server

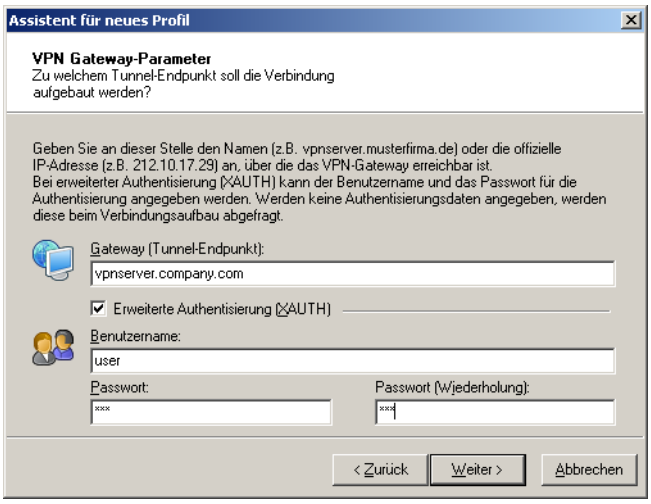
Seit der LCOS-Version 7.60 kann ein LANCOM die Gegenstelle auch über das Extended Authentication Protocol (XAUTH) identifizieren und authentifizieren. Zur Authentifizierung wurden dabei die Benutzerdaten aus der PPP-Liste herangezogen.

Ab der LCOS-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.

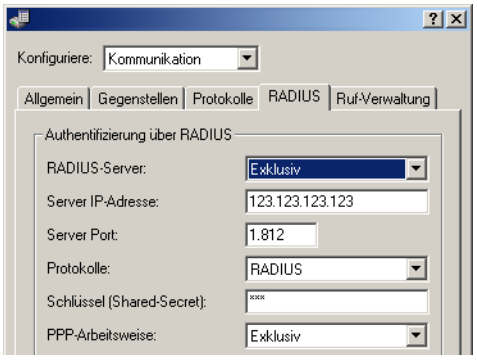
Um einen Einwahlzugang über VPN zusätzlich mit XAUTH zu authentifizieren, gehen Sie folgendermaßen vor:

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** auf der Registerkarte **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.

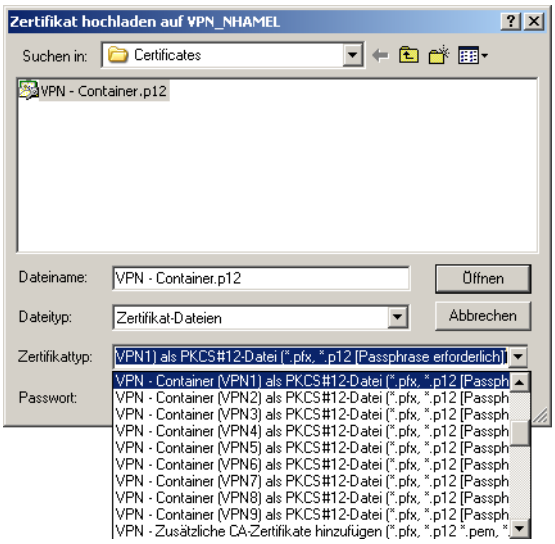
⑤ Stellen Sie auch die PPP-Arbeitsweise auf "Exklusiv" ein, damit die eingehenden XAUTH-Anfragen ausschließlich über den RADIUS-Server authentifiziert werden.

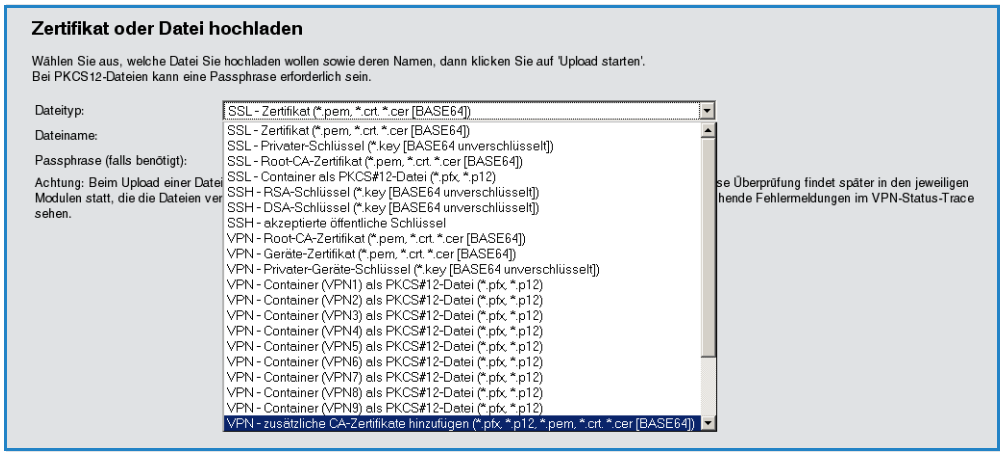
A.7 Erweiterte Zertifkats-Unterstützung

Zur Unterstützung von mehreren Zertifikatshierarchien können ab der LCOS-Version 7.80 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

WEBconfig: Dateimanagement ▶ Zertifikat oder Datei hochladen





Die im Gerät vorhandenen Zertifikate können im Statusbereich eingesehen werden:

WEBconfig: Status ▶ 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.

A.8 Wildcard Matching von Zertifikaten

A.8.1 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*'

A.8.2 Konfiguration

Der flexible Identitätsvergleich kann in der VPN-Konfiguration aktiviert bzw. deaktiviert werden.

WEBconfig: LCOS-Menübaum ▶ Setup ▶ VPN

- **Flexible-ID-Comparison**

  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.

A.9 Mehrere WLAN-Profile im Client-Modus

A.9.1 Einleitung

Zur Anbindung von einzelnen Geräten mit einer Ethernet-Schnittstelle in ein WLAN können LANCOM Access Points in den sogenannten Client-Modus versetzt werden, in dem sie sich wie ein herkömmlicher WLAN-Client verhalten und nicht wie ein Access Point (AP).

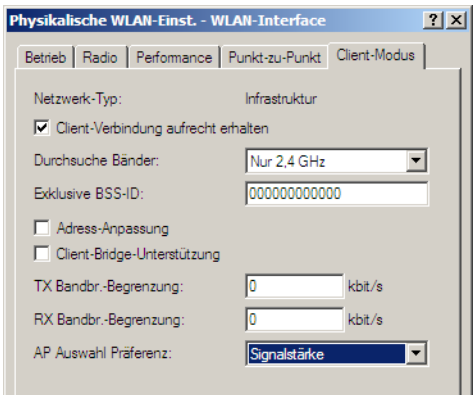
WLAN-Clients wie Notebooks können in der Regel über das Betriebssystem oder über die gerätespezifische Software verschiedene Profile speichern und verwalten, um je nach Umgebung auf verschiedene Access Points zuzugreifen (z.B. für ein WLAN im Unternehmen und für ein weiteres WLAN im Home-Office). In 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 Access Points können bis zu acht 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 Access Point verbinden kann, auch wenn mehrere WLAN-Profile definiert sind.

A.9.2 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: WLAN ▶ Allgemein ▶ Physikalische WLAN-Einstellungen ▶ Client-Modus

WEBconfig: LCOS-Menübaum ▶ 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).

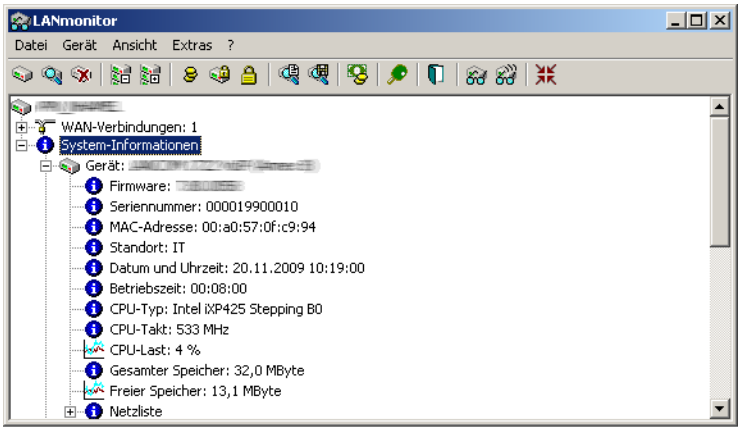
Default:

□ Signalstärke.

A.10 Mittelwert der CPU-Lastanzeige

A.10.1 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).



A.10.2 Konfiguration

Je nach Bedarf können Sie einstellen, über welchen Zeitraum die angezeigte CPU-Last gemittelt werden soll.

WEBconfig: LCOS-Menübaum ▶ 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.

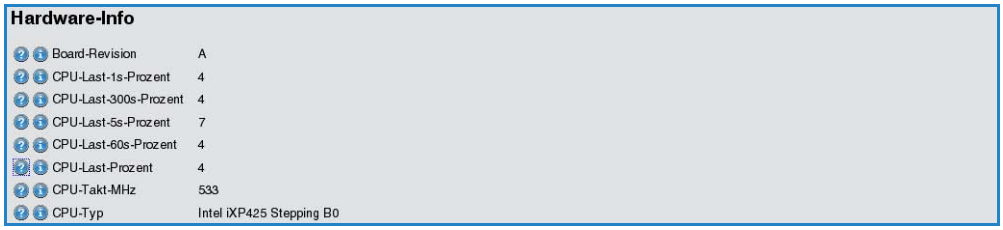
Mögliche Werte:

□ 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.



A.11 TACACS+-Umgehung

A.11.1 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.

A.11.2 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.

WEBconfig: LCOS-Menübaum ▶ 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!

A.12 Erweiterungen für die seriellen COM-Ports

A.12.1 Einleitung

Die Konfiguration der COM-Ports wurde um verschiedene Parameter erweitert.

A.12.2 Konfiguration

Die zusätzlichen Parameter befinden sich in den Netzwerkeinstellungen der COM-Ports.

WEBconfig: LCOS-Menübaum ▶ Setup ▶ COM-Ports ▶ COM-Port-Server ▶ Netzwerk-Einstellungen

■ **Nehme-Binaermodus-an**

Manche Netzwerkgeräte, die an einem seriellen COM-Port angeschlossen sind, versenden Datenstrukturen, die als Steuerzeichen (CR/LF – Carriage Return / Line Feed) interpretiert werden können. In der Standardeinstellung werten die COM-Ports in den LANCOM-Geräten diese Informationen aus, um den Datenfluss zu steuern. Mit dem "Binärmodus" kann ein COM-Port angewiesen werden, alle Daten binär weiterzuleiten und keine Anpassungen dieser Steuerzeichen vorzunehmen.

Mögliche Werte:

□ Ja, nein.

Default:

□ Nein.

■ **Newline-Konversion**

Wählen Sie hier aus, welches Zeichen auf dem seriellen Port ausgegeben wird, wenn der Binär-Modus aktiviert ist.

Die Einstellung ist abhängig von der Anwendung, die über den seriellen Port kommunizieren wird. Wenn an den Port ein weiteres LANCOM-Gerät angeschlossen ist, können Sie hier entweder CRLF oder nur CR wählen, da die Outband-Schnittstelle dieser Geräte ein "Carriage Return" zur automatischen Bestimmung der Datenübertragungsgeschwindigkeit erwartet. Manche Unix-Anwendungen würden CRLF allerdings als unerlaubte doppelte Zeilenschaltung interpretieren, in diesem Fall wählen Sie CR oder LF.

Mögliche Werte:

□ CRLF, CR, LF

Default:

□ CRLF

Diese Einstellung wird nur ausgewertet, wenn für diesen seriellen Port der Binär-Modus **deaktiviert** ist.

■ **TCP-Keepalive**

Der RFC 1122 definiert ein Verfahren, mit dem die Verfügbarkeit von TCP-Verbindungen geprüft werden kann (TCP-Keepalive). Ein inaktiver Transmitter sendet nach diesem Verfahren Anfragen nach dem Empfängerstatus an die Gegenstelle. Wenn die TCP-Sitzung zur Gegenstelle verfügbar ist, antwortet diese mit ihrem Empfängerstatus. Wenn die TCP-Sitzung zur Gegenstelle nicht verfügbar ist, wird die Anfrage in einem kürzeren Intervall solange wiederholt, bis die Gegenstelle mit ihrem Empfängerstatus antwortet (danach wird wieder ein längeres Intervall verwendet). Sofern die zugrunde liegende Verbindung funktioniert, die TCP-Sitzung zur Gegenstelle allerdings nicht verfügbar ist, sendet die Gegenstelle ein RST-Paket und löst so den Abbau der TCP-Sitzung bei der anfragenden Applikation aus.

Mögliche Werte:

□ inaktiv: Der TCP-Keepalive wird nicht verwendet.

□ aktiv: Der TCP-Keepalive ist aktiv, nur RST-Pakete führen zum Abbau von TCP-Sitzungen.

□ proaktiv: Der TCP-Keepalive ist aktiv, wiederholt die Anfrage nach dem Empfängerstatus der Gegenstelle aber nur für den als "TCP-Wdh.-Zahl" eingestellten Wert. Sofern nach dieser Anzahl von Anfragen keine Antwort mit dem Empfängerstatus vorliegt, wird die TCP-Sitzung als "nicht verfügbar" eingestuft und an die Applikation gemeldet. Wird während der Wartezeit ein RST-Paket empfangen, so löst dieses vorzeitig den Abbau der TCP-Sitzung aus.

Default:

□ inaktiv

Für Serverapplikationen wird die Einstellung "aktiv" empfohlen.

■ **TCP-Keepalive-Intervall**

Dieser Wert gibt an, in welchen Intervallen die Anfragen nach dem Empfängerstatus versendet werden, wenn die erste Anfrage nicht erfolgreich beantwortet wurde. Der dazu gehörende Timeout wird gebildet als Intervall / 3 (maximal 75 Sekunden).

Mögliche Werte:

□ maximal 10 Ziffern

Default:

□ 0

Besondere Werte:

□ 0 verwendet den Standardwert nach RFC 1122 (Intervall 7200 Sekunden, Timeout 75 Sekunden).

■ **TCP-Wdh.-Timeout**

Maximale Zeit für den Retransmission-Timeout. Dieser Timeout gibt an, in welchen Intervallen der Zustand einer TCP-Verbindung geprüft und das Ergebnis an die Applikation gemeldet wird, welche die entsprechende TCP-Verbindung nutzt.

Mögliche Werte:

□ 0 bis 99 Sekunden.

Besondere Werte:

□ 0 verwendet den Standardwert nach RFC 1122 (60 Sekunden).

Default:

□ 0

Die maximale Dauer der TCP-Verbindungsprüfung wird aus dem Produkt von TCP-Wdh.-Timeout und TCP-Wdh.-Zahl gebildet. Erst wenn der Timeout für alle Versuche abgelaufen ist, wird die entsprechende TCP-Anwendung informiert. Mit den Standardwerten von 60 Sekunden Timeout und maximal 5 Versuchen kann es bis zu 300 Sekunden dauern, bis eine nicht aktive TCP-Verbindung von der Applikation erkannt wird.

■ **TCP-Wdh.-Zahl**

Maximale Anzahl der Versuche, mit denen der Zustand einer TCP-Verbindung geprüft und das Ergebnis an die Applikation gemeldet wird, welche die entsprechende TCP-Verbindung nutzt.

Mögliche Werte:

□ 0 bis 9

Besondere Werte:

□ 0 verwendet den Standardwert nach RFC 1122 (5 Versuche).

Default:

□ 0

Die maximale Dauer der TCP-Verbindungsprüfung wird aus dem Produkt von TCP-Wdh.-Timeout und TCP-Wdh.-Zahl gebildet. Erst wenn der Timeout für alle Versuche abgelaufen ist, wird die entsprechende TCP-Anwendung informiert. Mit den Standardwerten von 60 Sekunden Timeout und maximal 5 Versuchen kann es bis zu 300 Sekunden dauern, bis eine nicht aktive TCP-Verbindung von der Applikation erkannt wird.

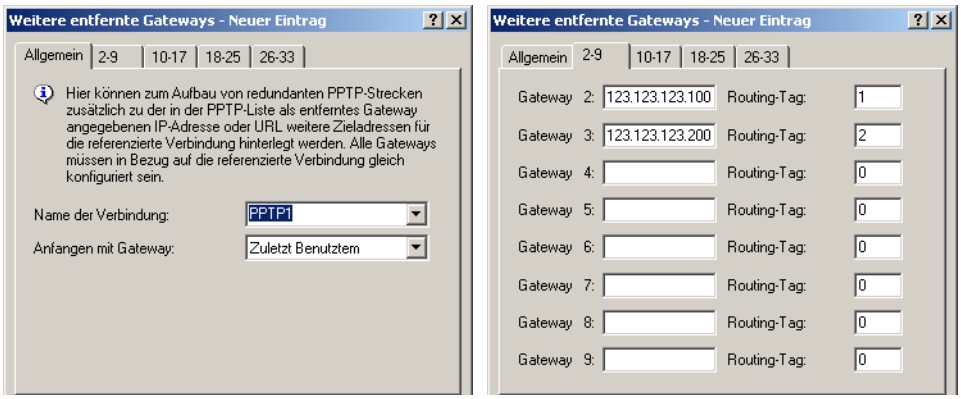
A.13 32 zusätzliche Gateways für PPTP-Verbindungen

A.13.1 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.

A.13.2 Konfiguration

Die zusätzlichen PPTP-Gateways weden in einer separaten Liste definiert.



LANconfig: Kommunikation ▶ Protokolle ▶ Weitere entfernte Gateways

WEBconfig: LCOS-Menübaum ▶ 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.

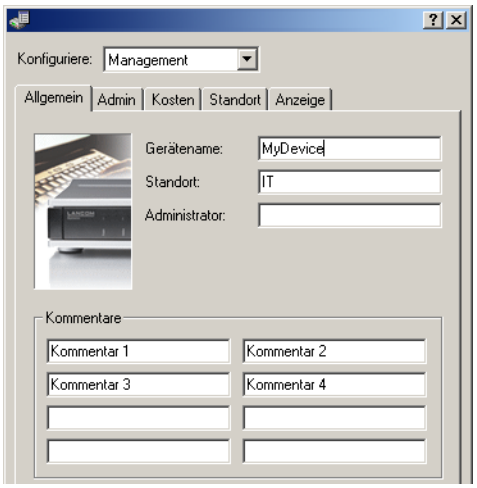
Default:

- □ 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.

A.14 Zusätzliche Kommentarfelder zur Beschreibung der Geräte

Zur Beschreibung der LANCOM-Geräte können bis zu acht Kommentare eingetragen werden.



LANconfig: Management ▶ Allgemein

WEBconfig: LCOS-Menübaum ▶ Setup ▶ SNMP

■ **Kommentar 1 bis 8**

Tragen Sie hier einen Kommentar ein.

Mögliche Werte:

- □ maximal 255 alphanumerische Zeichen.

Default:

- □ leer

A.15 DHCP-Optionen mit LANconfig

Mit den DHCP-Optionen können zusätzliche Konfigurationsparameter an die Stationen übertragen werden. Der Vendor-Class-Identifier (DHCP-Option 60) zeigt so z. B. den Gerätetyp an. In dieser Tabelle werden zusätzliche Optionen für den DHCP-Betrieb definiert.



LANconfig: Management ▶ Allgemein

WEBconfig: LCOS-Menübaum ▶ Setup ▶ DHCP ▶ Zusaetzliche-Optionen

■ **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.

Mögliche Werte:

□ maximal 3 Ziffern.

Default:

□ leer

Eine Liste aller DHCP-Optionen finden Sie im RFC 2132 – DHCP Options and BOOTP Vendor Extensions der Internet Engineering Task Force (IETF).

■ **Netzwerkname**

Name des IP-Netzwerks, in dem diese DHCP-Option verwendet werden soll.

Mögliche Werte:

□ Auswahl aus der Liste der im Gerät definierten IP-Netzwerke, maximal 16 Zeichen.

Default:

□ leer

■ **Typ**

Typ des Eintrags. Dieser Wert ist abhängig von der jeweiligen Option. Für die Option "35" wird hier im RFC 2132 z. B. der ARP Cache Timeout so definiert:

```
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.

Mögliche Werte:

□ String, Integer8, Integer16, Integer32, IP-Adresse

Default:

□ String

Den Typ der Option entnehmen Sie bitte dem entsprechenden RFC bzw. bei herstellerspezifischen DCHP-Optionen der jeweiligen Herstellerdokumentation.

■ **Wert**

In diesem Feld wird der Inhalt der DHCP-Option definiert.

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".

Mögliche Werte:

□ Maximal 128 Zeichen.

Default:

□ leer

Die mögliche Länge des Optionswertes entnehmen Sie bitte dem entsprechenden RFC bzw. bei herstellerspezifischen DCHP-Optionen der jeweiligen Herstellerdokumentation.

A.16 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 Wenn die Absenderadresse eines Pakets direkt einem im Gerät definierten IP-Netz zugeordnet werden kann, dann wird das Schnittstellen-Tag des IP-Netzes verwendet.

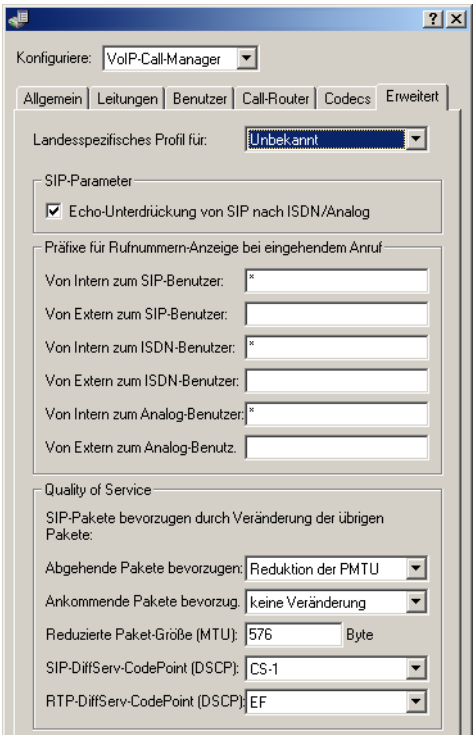
② Wenn an dem Interface, über das ein Paket empfangen wurde, nur ein IP-Netz gebunden ist, dann wird das Schnittstellen-Tag dieses IP-Netzes verwendet.

③ Wenn die Möglichkeiten ① und ② kein eindeutiges Ergebnis liefern, versucht das Gerät anhand der MAC-Adresse die IP-Adresse des Next-Hops zu ermitteln (reverse ARP-Lookup). Anhand dieser IP-Adresse versucht das Gerät, das zugehörige IP-Netz und so das Schnittstellen-Tag zu ermitteln.

④ Wenn die Möglichkeiten ① bis ③ kein eindeutiges Ergebnis liefern, versucht das Gerät anhand der Einträge in der Routing-Tabelle das zugehörige IP-Netz und so das Schnittstellen-Tag zu ermitteln.

A.17 Globale Einstellung von DiffServ für SIP & RTP

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.



LANconfig: Voice-Call-Manager ▶ Erweitert

WEBconfig: LCOS-Menübaum ▶ Setup ▶ Voice-Call-Manager ▶ General

■ **SIP-DiffServ-CodePoint (DSCP)**

Legen Sie hier fest, mit welchen DiffServ-CodePoints (DSCP) die SIP-Pakete (Anruf-Signalisierung) markiert werden.

Mögliche Werte:

□ BE, CS-0, CS-1, CS-2, CS-3, CS-4, CS-5, CS-6, CS-7, AF-11, AF-12, AF-13, AF-21, AF-22, AF-23, AF-31, AF-32, AF-33, AF-41, AF-42, AF-43, EF

Default:

□ CS-1

Die Verwendung von CS-1 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 großer Verbreitung im Markt empfehlen wir den Einsatz von CS-3.

■ **RTP-DiffServ-CodePoint (DSCP)**

Legen Sie hier fest, mit welchen DiffServ-CodePoints (DSCP) die RTP-Pakete (Voice-Datenstrom) markiert werden.

Mögliche Werte:

□ BE, CS-0, CS-1, CS-2, CS-3, CS-4, CS-5, CS-6, CS-7, AF-11, AF-12, AF-13, AF-21, AF-22, AF-23, AF-31, AF-32, AF-33, AF-41, AF-42, AF-43, EF

Default:

□ EF

Bei der Einstellung DSCP BE bzw. CS-0 werden die Pakete ohne Markierung versendet
Weitere Informationen zu den DiffServ-CodePoints finden Sie im Referenzhandbuch im Kapitel "QoS".

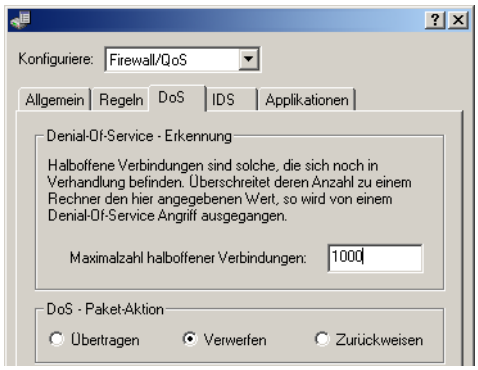
A.18 Erhöhter DoS-Schwellwert für Zentralgeräte

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 Schwellwert, 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-Schwellwert für die Erkennung der DoS-Angriffe.



LANconfig: Firewall/QoS ▶ DoS

WEBconfig: LCOS-Menübaum ▶ 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 wie 7100, 7111, 8011, 9100, 4025(+), 4100.

A Addendum zur LCOS-Version 8.0

A.1 Übersicht

■ 'IPSec over HTTPS' →Seite 1
■ 'Basic HTTP Fileserver für LCOS 8.0' →Seite 3
■ 'Automatisches Laden von Firmware oder Konfiguration von externen Datenträgern' →Seite 4
■ 'SSH-Client' →Seite 7
■ 'Alternative Boot-Config' →Seite 10
■ 'Alternative DHCP-Server zur Weiterleitung' →Seite 13
■ 'Kanallastanzeige im WLC-Betrieb' →Seite 14
■ 'Änderungen in LANconfig' →Seite 15
■ '802.1x-Accounting im WLAN-Controller für logische WLANs aktivieren' →Seite 16
■ 'LANCOM Content Filter' →Seite 17
■ 'DFS3' →Seite 35
■ 'Alternative URLs für CRLs' →Seite 36
■ 'Broken-Link-Detection' →Seite 36

A.2 IPSec over HTTPS

A.2.1 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 LANCOM VPN-Router die IPSec over HTTPS-Technologie.

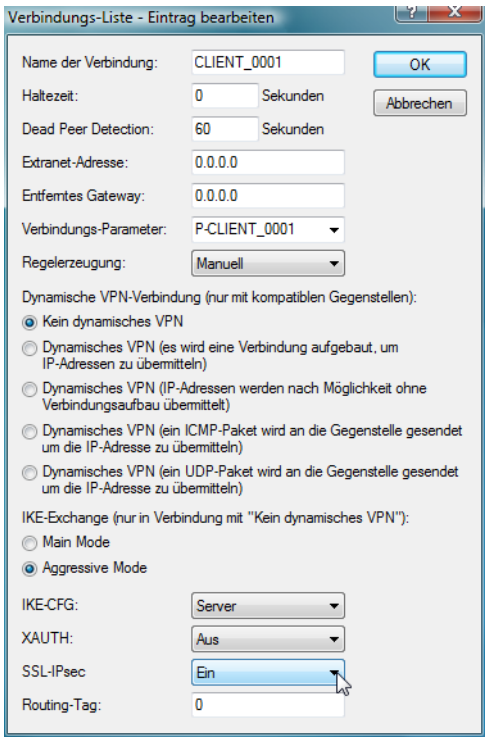
Dabei wird zunächst eine Datenübertragung über Standard-IPSec versucht. Kommt diese Verbindung nicht zustande (z.B. weil der IKE Port 500 in einem Mobilfunknetz gesperrt ist), so wird automatisch ein Verbindungsaufbau versucht, bei dem das IPSec VPN mit einem zusätzlichen SSL-Header (Port 443, wie bei 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 in LANCOM VPN-Routern mit LCOS 8.0 oder höher sowie im LANCOM Advanced VPN Client 2.22 oder höher.

A.2.2 Konfiguration der IPSec over HTTPS-Technologie

Für den aktiven Verbindungsaufbau eines LANCOM-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 ▶ Allgemein ▶ Verbindungsliste
■ WEBconfig: LCOS-Menübaum ▶ Setup ▶ VPN ▶ VPN-Gegenstellen



■ **SSL-IPsec**

Mit dieser Option aktivieren Sie die Nutzung der IPSec over HTTPS-Technologie beim aktiven Verbindungsaufbau zu dieser Gegenstelle.

Mögliche Werte:

□ Ein, Aus

Default:

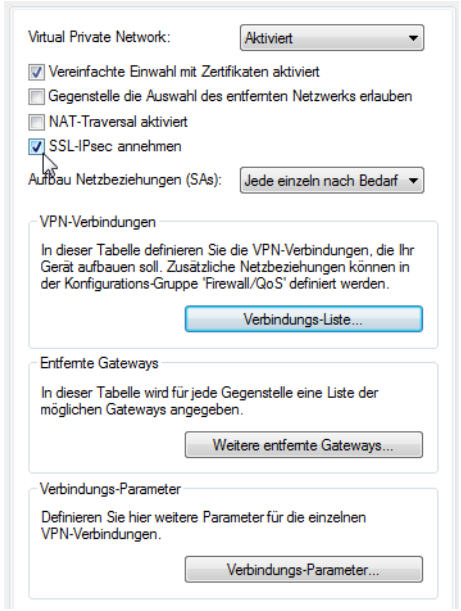
□ Aus

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 LANCOM-VPN-Gerät von einer anderen VPN-Gegenstelle mit Hilfe der IPSec over HTTPS-Technologie (LANCOM-VPN-Gerät oder LANCOM Advanced VPN Client) aktivieren Sie die Option in den allgemeinen VPN-Einstellungen.

■ LANconfig: VPN ▶ Allgemein

■ WEBconfig: LCOS-Menübaum ▶ Setup ▶ VPN



■ **SSL-IPsec 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.

A.2.3 Statusanzeigen der IPSec over HTTPS-Technologie

Die Statusanzeigen zu jeder aktiven VPN-Verbindung zeigen an, ob für die jeweilige Verbindung die IPSec over HTTPS-Technologie (SSL-Encaps.) 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-Laeng
CLIENT_0004	Verbindung	(none)	passiv	0	NETCOLOGN	9999	91.114.240.66	no-nat	nein	AES	128	HMAC_MD5	128	(none)	0
LCS	Verbindung	(none)	aktiv	9999	NETCOLOGN	9999	213.217.69.77	no-nat	nein	AES	128	HMAC_MD5	128	(none)	0

A.3 Basic HTTP Fileserver für LCOS 8.0

A.3.1 Einleitung

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

Diese Funktion wird von allen LANCOM-Geräten mit USB-Anschluss unterstützt.

A.3.2 Vorbereitung des USB-Speichermediums

So bereiten Sie ein USB-Medium für den Einsatz an einem LANCOM-Gerät vor:

■ Dateisystem: Formatieren Sie das USB-Medium mit FAT16 oder FAT32 Dateisystem.

■ Basisverzeichnis: Erstellen Sie auf dem USB-Medium ein 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.

■ USB-Verbindung: Verbinden Sie das Massenspeichergerät mit dem USB-Anschluss des LANCOM-Gerätes.

A.3.3 Einhängepunkt des USB-Mediums im LCOS ermitteln

Beim Anschließen eines USB-Mediums an ein LANCOM-Gerät wird automatisch ein Einhängepunkt erzeugt, der von LCOS zur internen Verwaltung des Mediums verwendet wird. Dieser Einhängepunkt bleibt für ein bestimmtes USB-Medium immer gleich, auch nach einem Reboot oder 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 können Sie über die Statustabelle ermitteln:

■ WEBconfig: LCOS-Menübaum ▶ Status ▶ Dateisystem ▶ Volumes

Volumes

ID	Mountpunkte	Dateisystem	Entmountbar?	Frei	Groesse
BlkDev-1	/PKBACK#.001, /usb	FAT32	1	53382 KB	122 MB
MiniFs	/minifs	MiniFs	0	209 KB	256 KB

Die Statustabelle 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 ist eingehängt unter /usb.

A.3.4 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://<IP adress of device>/filesrv/<mount point>/<file name>`

  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://<IP address of device>/filesrv/usb/coupon.jpeg`



Der Zugriff kann auch über HTTPS anstatt HTTP erfolgen.

A.3.5 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

A.3.6 Verzeichnisstruktur

Das Verzeichnis `public_html` kann Unterverzeichnisse beinhalten. Der HTTP-Server im LCOS hat bestimmte Regeln für den Zugriff auf Verzeichnisse:

- Wenn eine Datei 'index.html' in dem Unterverzeichnis existiert, dann wird diese zum HTTP-Client übertragen; andernfalls:
- Wenn eine Datei 'index.htm' in dem Unterverzeichnis existiert, dann wird diese zum HTTP-Client übertragen; andernfalls:
- Der Fileserver erstellt eine einfache Liste aller Dateien und Unterverzeichnisse im Hauptverzeichnis.

A.4 Automatisches Laden von Firmware oder Konfiguration von externen Datenträgern

A.4.1 Einleitung

LANCOM-Geräte mit USB-Anschluss können mit Hilfe eines externen Datenträgers sehr komfortabel in Betrieb genommen werden. Firmware-Dateien und Loader können ebenso wie vollständige Konfigurationen oder Skripte automatisch von einem USB-Medium in das Gerät geladen werden.

A.4.2 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 wird zunächst der Header der Dateien ausgelesen, die Dateien werden anschließend nach folgenden Regeln verwendet:

- Wird 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.
- Wird 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. Wenn zunächst ein Loader geladen wird, erfolgt nach dem Ladevorgang ein Neustart des Geräts 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.

Wenn der automatische Ladevorgang vollständig abgeschlossen ist, leuchten alle LEDs des Geräts für 30 Sekunden grün. Das USB-Medium kann dann entfernt werden.

A.4.3 Automatisches Laden von Konfigurations- und/oder Skript-Dateien

Wenn die Funktion aktiviert ist, sucht das Gerät beim Mounten eines USB-Mediums nach Konfigurations- und/oder Skript-Dateien im Verzeichnis "Config". In diesem Verzeichnis werden alle Dateien mit der Dateiendung ".lcs" oder ".lcf" für den automatischen Ladevorgang in Betracht gezogen, die zum aktuellen Gerätetyp passen. Dazu wird zunächst der Header der Dateien ausgelesen, die Dateien werden anschließend nach folgenden Regeln verwendet:

- Eine Voll-Konfiguration ".lcf" wird immer vor einem Skript ".lcs" geladen. Es werden nur Voll-Konfigurationen geladen, deren Gerätetyp-Eintrag gleich dem Typ des ladenden Geräts ist und deren Firmware-Versions-Eintrag im Header gleich der im ladenden Gerät aktiven Firmware ist. Liegen mehrere passende Voll-Konfigurationen vor, so wird die Auswahl nach den folgenden Kriterien in dieser Reihenfolge vorgenommen:
  - 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, wird die Konfiguration mit dem aktuellsten Datum verwendet.

Die Header-Parameter für Konfigurationsdateien können manuell im Datei-Dialog von LANconfig als Meta-Parameter gesetzt werden, wenn eine Offline-Konfiguration gespeichert wird.

- Sollte keine Voll-Konfiguration vorliegen, wird eine eventuell vorhandene Skript-Datei (".lcs") herangezogen. Liegen mehrere passende Skripte vor, so wird die Auswahl nach den folgenden Kriterien in dieser Reihenfolge vorgenommen:
  - 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, wird das Skript mit der neuesten Versionnummer bzw. mit dem aktuellsten Datum verwendet.

Die Header-Parameter für Scripte können manuell in einem Text-Editor in den entsprechenden Script-Dateien durch die Angabe "SERIAL:" und/oder "MAC:" und ggf. einer Firmwareversion gesetzt werden.

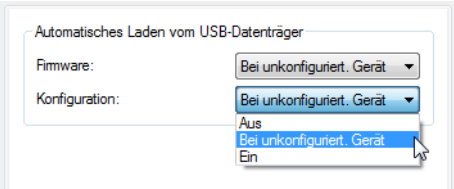
Während des automatischen Ladevorgangs blinken die Power- und die Online-LED am Gerät abwechselnd.

Wenn der automatische Ladevorgang vollständig abgeschlossen ist, leuchten alle LEDs des Geräts für 30 Sekunden grün. Das USB-Medium kann dann entfernt werden.

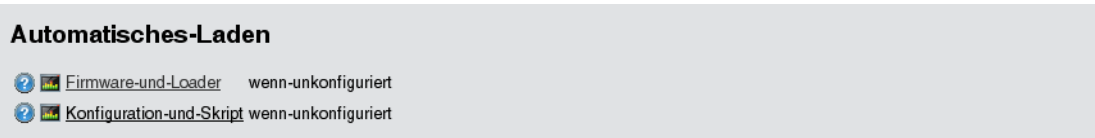
A.4.4 Konfiguration

Die Konfiguration für das automatische Laden finden Sie in folgendem Menü:

- LANconfig: Management ▶ USB-Datenträger



- WEBconfig: LCOS-Menübaum ▶ Setup ▶ Automatisches-Laden



■ **Firmware**

Mit dieser Option aktivieren Sie das automatische Laden von Loader- und/oder Firmware-Dateien von einem angeschlossenen USB-Medium.

Mögliche Werte:

□ Aus

Das automatische Laden von Loader- und/oder Firmware-Dateien für das Gerät ist deaktiviert.

□ 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.

□ Bei unkonfiguriert. Gerät

Das automatische Laden von Loader- und/oder Firmware-Dateien für das Gerät wird nur dann aktiviert, wenn sich das Gerät im Auslieferungszustand befindet. Durch einen Konfigurations-Reset kann ein Gerät jederzeit wieder auf den Auslieferungszustand zurückgesetzt werden.

Default:

□ Bei unkonfiguriert. Gerät

Durch den Assistenten für Sicherheitseinstellungen bzw. für Grundeinstellungen wird diese Option auf "inaktiv" gesetzt.

■ **Konfiguration**

Mit dieser Option aktivieren Sie das automatische Laden von Konfigurations- und/oder Skript-Dateien von einem angeschlossenen USB-Medium.

Mögliche Werte:

□ Aus

Das automatische Laden von Konfigurations- und/oder Skript-Dateien für das Gerät ist deaktiviert.

□ 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-Dateien in das Gerät zu laden. Das USB-Medium wird beim Einstecken in den USB-Anschluss am Gerät oder beim Neustart gemountet.

□ Bei unkonfiguriert. Gerät

Das automatische Laden von Konfigurations- und/oder Skript-Dateien für das Gerät wird nur dann aktiviert, wenn sich das Gerät im Auslieferungszustand befindet. Durch einen Konfigurations-Reset kann ein Gerät jederzeit wieder auf den Auslieferungszustand zurückgesetzt werden.

Default:

□ Bei unkonfiguriert. Gerät

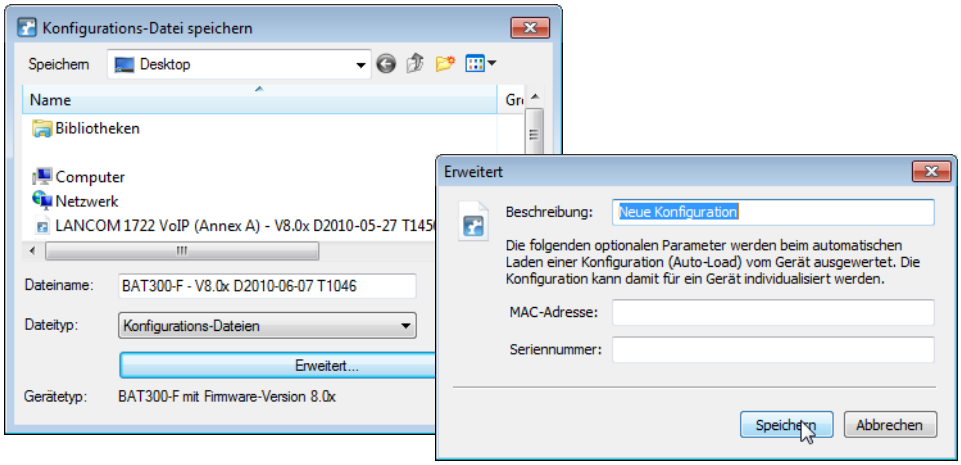
Durch den Assistenten für Sicherheitseinstellungen bzw. für Grundeinstellungen wird diese Option auf "inaktiv" gesetzt.

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.

A.4.5 Meta-Daten für Konfigurationsdateien

Für das automatische Laden von einem USB-Datenträger können Konfigurationsdateien mit der Seriennummer und/oder der MAC-Adresse eines Geräts gekennzeichnet werden. Die Geräte laden mit der Auto-Load-Funktion dann nur die Konfiguration bzw. das Script, bei denen die eingetragene Geräte-Seriennummer mit der Seriennummer des ladenden Gerätes übereinstimmt.

LANconfig bietet beim Speichern einer Konfiguration die Möglichkeit, diese Informationen als Meta-Parameter zu erfassen. Wählen Sie dazu beim Speichern der Konfiguration aus LANconfig die Schaltfläche **Erweitert**:



A.5 SSH-Client

A.5.1 Einleitung

Neben dem SSH-Server, der eine sichere und authentifizierte Einwahl in ein LANCOM-Gerät ermöglicht, stellt LCOS auch einen SSH-Client zur Verfügung. Über diesen SSH-Client können von einem LANCOM-Gerät aus SSH-Verbindungen zu einem entfernten Server – z.B. ein weiteres LANCOM-Gerät oder ein Unix-Server – aufgebaut werden. Diese Funktion ist sehr nützlich, wenn eine direkte Verbindung zu dem entfernten System nicht möglich ist, aber eine indirekte Verbindung über das LANCOM-Gerät existiert, das aus beiden Subnetzen erreicht werden kann.

Der SSH-Client kann über einfache Befehle auf der Kommandozeile gestartet werden, ähnlich dem OpenSSH-Client auf einem Linux- oder Unix-System.

A.5.2 CLI-Argumente für den SSH-Client

Die SSH-Verbindung zu einem entfernten System wird mit dem folgenden Befehl gestartet:

- `ssh [-?] [-h] [-b/-a loopback-address] [-p port] [-C] [-j interval] [user@]host [command]`
  - `-?`, `-h`: zeigen eine kurze Hilfe der möglichen Argumente
  - `-b`, `-a`: ermöglicht die Angabe der Absenderadresse (Loopback-Adresse). Diese Option ist besonders im Zusammenhang mit ARF wichtig.
  - `-p`: gibt den zu verwendenen Port an. Wird der Port nicht angegeben, wird der TCP-Port 22 verwendet.
  - `command`: der SSH-Client kann entweder eine interaktive Shell auf dem entfernten System starten oder nur einen einzelnen Befehl ausführen. Wird kein Befehl angegeben, wird eine interaktive Shell gestartet.
  - `user`: Benutzername für die Anmeldung am entfernten System. Nur wenn kein expliziter Benutzername angegeben ist, wird der aktuelle Nutzer der Anmeldung an der LCOS CLI verwendet.
  - `-C`: Wenn diese Option angegeben wird, 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 langsamen Verbindungen (z.B. über ISDN) sinnvoll. Auf schnellen Verbindungen ist der zusätzliche Overhead der Kompression meistens größer als der Gewinn durch die Datenreduzierung.
  - `-j 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 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 vom entfernten System als Leerlaufprozess interpretiert werden, die dem Gateway aber das Fortbestehen der Verbindung signalisieren. Mit diesem Argument wird das Interval in Sekunden angegeben, in dem die Keep-Alive-Pakete verschickt werden. 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.

A.5.3 CLI-Argumente für den Telnet-Client

Alternativ zum SSH-Client kann auch über Telnet eine Verbindung zu einem entfernten System mit dem folgenden Befehl gestartet werden:

- `telnet [-?] [-h] [-b loopback-address] host [port]`

- □ `-?`, `-h`: zeigen eine kurze Hilfe der möglichen Argumente
- □ `-b`: ermöglicht die Angabe der Absenderadresse (Loopback-Adresse). Diese Option ist besonders im Zusammenhang mit ARF wichtig.
- □ `port`: gibt den zu verwendenen Port an. Wird der Port nicht angegeben, wird der TCP-Port 23 verwendet.

A.5.4 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. 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 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.

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" in der Shell. 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 CLI-Sitzung selbst durch einen OpenSSH-Client geöffnet wurde, wird die Folge Tilde – Tilde – Punkt verwendet, da ansonsten die falsche Verbindung beendet wird.

A.5.5 Erzeugung von SSH-Schlüsseln

Die SSH-Authentifizierung unterstützt zwei unterschiedliche Verfahren:

- interaktiv mit der Passworteingabe über die Tastatur
- mit dem Austausch von öffentlichen Schlüsseln

Die Schlüssel müssen individuell und anwenderbezogen erstellt werden, es gibt keine vordefinierten Standardschlüssel. Im Auslieferungszustand unterstützen die LANCOM-Geräte daher nur die Authentifizierung über Passwort.

Die Erzeugung von Schlüsseln wird über den Befehl `sshkeygen` an der CLI des Gerätes gestartet, auf dem der Administrator den SSH-Client nutzen möchte. Dabei gilt folgende Syntax:

- `sshkeygen [-?] [-h] [-t dsa|rsa] [-b bits] [-f output-file]`
  - □ `-?`, `-h`: zeigen eine kurze Hilfe der möglichen Argumente
  - □ `-t`: dieses Argument bestimmt den Typ des Schlüssels.

    SSH unterstützt zwei 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 1024 bis 2048 Bit.

    DSS-Schlüssel folgen dem Standard 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. DSS-Schlüssel haben immer eine Länge von 1024 Bit, sind aber langsamer als die entsprechenden RSA-Schlüssel.

    Wird kein Typ angegeben, wird ein Schlüssel vom Typ RSA erzeugt.
  - □ `-b`: dieses Argument bestimmt die Länge des Schlüssels in Bit für RSA-Schlüssel.

    Wird keine Länge angegeben, wird ein Schlüssel mit einer Länge von 1024 Bit erzeugt.
  - □ `-f`: ermöglicht die Angabe eines Dateinamens für den Schlüssel.

Nachdem der Schlüssel erzeugt wurde, muss der öffentliche Teil auf das entfernte System übertragen werden. Der öffentliche Teil des Schlüssels kann mit dem folgenden Befehl angezeigt werden:

- `show ssh idkeys`

Diese Befehl erzeugt eine Ausgabe ähnlich der folgenden:

```
Configured Client-Side SSH Host Keys For User 'root':
ssh-rsa AAAAB3NzaC1yc2EAAAABEQAAAQEA2
8BtnFFInAi8I5B1aOwq5g2YfwIX2O/vMX+9SLZ
AJVAhFnhdOG4wjTpLVuaQRNlITpBESPaWPLqoA
...
wd0T0nkuNQ== root@sshctest
```

Bitte beachten Sie, dass es sich um einen einzelnen Schlüssel handelt, auch wenn die Ausgabe in mehrere Zeilen aufgeteilt wird, der aus drei Teilen besteht:

- 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.

Die Datei kann mit einer Funktion von WEBconfig komfortabel bearbeitet werden (WEBconfig ▶ Extras ▶ Liste erlaubter öffentlicher SSH-Schlüssel bearbeiten). Kopieren Sie 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.

A.5.6 Bearbeitung der Dateien

Während des Betriebs nutzt der SSH-Client verschiedene Dateien, die ggf. manuell bearbeitet werden müssen.

Die Liste der bekannten SSH-Server

Der SSH-Client nutzt die Liste der bekannten SSH-Server zum Speichern der entsprechenden Schlüssel. Diese Datei wird jedesmal verändert, wenn erstmalig eine Verbindung zu einem SSH-Server aufgebaut wird und der Administrator den angezeigten Schlüssel des entfernten Systems akzeptiert.

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.



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

Die Dateien ssh_id_rsa und ssh_id_dsa

Diese Dateien enthalten die Schlüssel, die mit dem Befehl `sshkeygen` erzeugt wurden, also die Schlüssel zur Authentifizierung der entfernten SSH-Server im PEM-Format. Die Schlüssel für alle LCOS-Administratoren sind in einer zentralen Datei gespeichert und nur für den root-Administrator über secure copy zugänglich, das Hoch- bzw. Herunterladen über WEBconfig ist jedoch nicht möglich.

Die ID-Dateien entsprechenden dem folgenden Aufbau, der die Nutzung eines Schlüssels für einen bestimmten LCOS-Administrator definiert:

```
*** User xyz
Schlüssel
*** End
```

A.5.7 Prioritäten für die SSH-Authentifizierung

Die Reihenfolge der SSH-Authentifizierung folgen einer festen Prioritätenfolge:

- Als erste Methode wird immer die Authentifizierung über öffentliche Schlüssel versucht, es sei denn, das entfernte System unterstützt diese Methode nicht oder der aktuelle LCOS-Administrator besitzt keine öffentlichen Schlüssel.
- Als zweite Methode wird die interaktive Authentifizierung über die Tastatur verwendet, wenn die Authentifizierung über öffentliche Schlüssel prinzipiell nicht verwendet werden kann oder wenn das entfernte System alle öffentlichen Schlüssel des aktuellen LCOS-Administrators abgelehnt hat. Die interaktive Authentifizierung kann

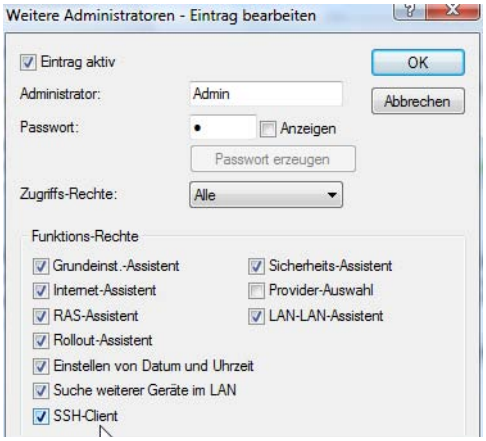
je nach Anwendung aus dem Austausch mehrerer Nachrichten zwischen SSH-Client und SSH-Server bestehen, im einfachsten Fall reicht ggf. nur ein Eingabe des Passworts.

A.5.8 Berechtigung zur Nutzung des SSH-Clients

Das Recht zur Nutzung des SSH-Clients kann für jeden einzelnen Administrator der LANCOM-Geräte separat eingeräumt werden.

Die Rechte für die Administratoren finden Sie in folgendem Menü:

- LANconfig: Management ▶ Admin ▶ Weitere Administratoren
- WEBconfig: LCOS-Menübaum ▶ Setup ▶ Config ▶ Admins



A.6 Alternative Boot-Config

A.6.1 Einleitung

Das Verhalten der LANCOM-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.

LANCOM-Geräte können drei verschiedene Boot-Konfigurationen nutzen:

- LANCOM-Werkseinstellungen: Diese enthält die Standardwerte für das jeweilige Modell im Auslieferungszustand, also den LANCOM-Standard. 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, der LANCOM-Standard aber nicht verwendet werden soll. Mit dieser Funktion werden LANCOM-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 vom LANCOM-Standard 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.

A.6.2 Verwenden der Boot-Konfigurationen

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

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

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

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:

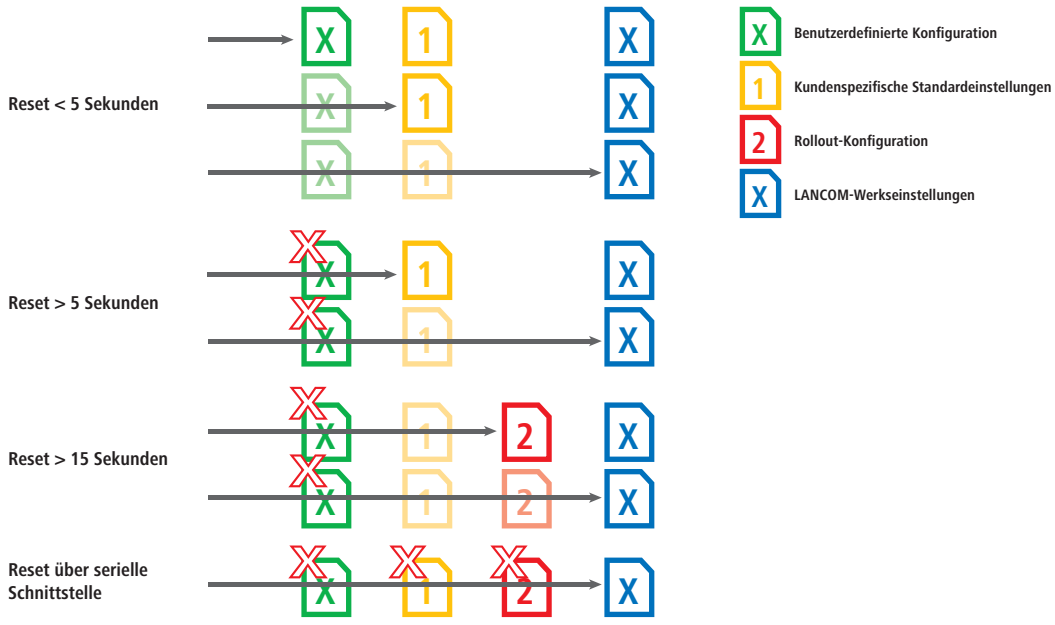
- weniger als 5 Sekunden: Booten (Neustart), dabei wird die benutzerdefinierte Konfiguration aus dem Konfigurationsspeicher geladen. Wenn die benutzerdefinierte Konfiguration leer ist, werden die kundenspezifischen Standardeinstellungen (erster Speicherplatz) geladen. Das Laden der kundenspezifischen Standardeinstellungen wird angezeigt, indem alle LEDs des Geräts einmal kurzzeitig rot aufleuchten. Wenn auch der erste Speicherplatz leer ist, werden die LANCOM 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 LANCOM 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 LANCOM 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 (benutzerdefinierte Konfiguration, kundenspezifische Standardeinstellungen, LANCOM Werkseinstellungen).

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

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

- Bei Drücken des Reset-Buttons für weniger als 5 Sekunden wird die benutzerdefinierte Konfiguration geladen, wenn die nicht vorhanden ist die kundenspezifischen Standardeinstellungen, wenn die auch nicht vorhanden sind die LANCOM-Werkseinstellungen.
- Bei Drücken des Reset-Buttons für mehr als 15 Sekunden wird immer die benutzerdefinierte Konfiguration, dann die Rollout-Konfiguration geladen, wenn die nicht vorhanden ist die LANCOM-Werkseinstellungen.



A.6.3 Wiederherstellen der LANCOM Werkseinstellungen über seriellen Zugang

Wenn beide Speicherplätze mit kundenspezifischen Standardeinstellungen **und** Rollout-Konfiguration belegt sind, kann das Gerät nicht mehr über den Reset-Taster auf die LANCOM Werkseinstellungen zurückgesetzt werden. Wenn ein Zugriff auf die Konfiguration nicht mehr möglich ist (z.B. weil das Kennwort nicht mehr vorliegt), können die LANCOM Werkseinstellungen nur über den seriellen Zugang wieder hergestellt werden.

Über die serielle Schnittstelle kann eine Firmware in das Gerät geladen werden. Wenn Sie dabei statt des Konfigurations-Passwortes die Seriennummer verwenden, wird die Konfiguration des Gerätes wie bei einem Reset vollständig auf den Auslieferungszustand zurückgesetzt. Auf diese Weise können Sie sich Zugang zu einem Gerät verschaffen, wenn die LANCOM Werkseinstellungen nicht auf einem anderen Weg wieder hergestellt werden können.

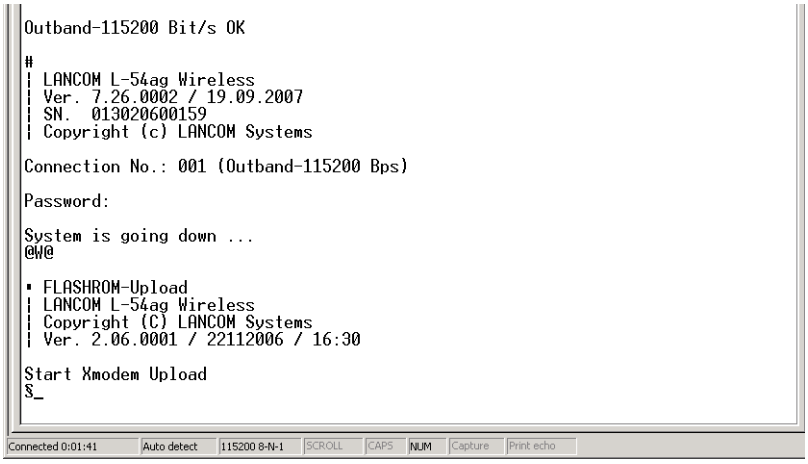
① Schließen Sie das Gerät über das serielle Konfigurationskabel an einen Rechner an.

② Starten Sie auf diesem Rechner ein Terminal-Programm, z. B. Hyperterminal.

③ Starten Sie eine Verbindung mit den Einstellungen 115200bps, 8n1, Hardware-Handshake (RTS/CTS).

④ Drücken Sie im Begrüßungsbildschirm des Terminal-Programms die Return-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 Return.



⑥ Das Gerät erwartet nun den Firmware-Upload. Klicken Sie dazu z. B. unter Hyperterminal auf **Übertragung** ▶ **Datei senden** und wählen Sie X-Modem als Übertragungsprotokoll aus.

Bei diesem Firmware-Upload wird die Konfiguration inklusive der Boot-Konfigurationen vollständig gelöscht und auf den Auslieferungszustand zurückgesetzt! Dabei werden alle im Gerät abgelegten Dateien gelöscht, z.B. auch 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.

A.6.4 Speichern und Hochladen der Boot-Konfigurationen

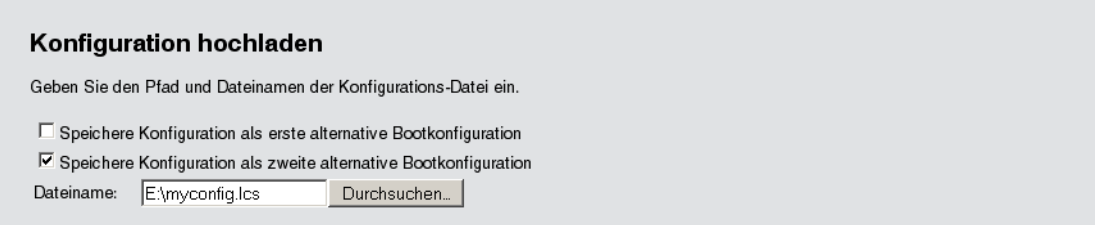
Kundenspezifische Standardeinstellungen oder Rollout-Konfiguration werden in einem komprimierten Format gespeichert. Über die Kommandozeile kann die aktuelle Konfiguration eines Gerätes als kundenspezifische Standardeinstellung oder Rollout-Konfiguration gespeichert werden. Nutzen Sie dazu den folgenden Befehl:

■ `bootconfig --savecurrent [1,2, all]` oder `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.

Auch über WEBconfig können die kundenspezifischen Standardeinstellungen oder die Rollout-Konfiguration in das Gerät geladen werden:

■ WEBconfig: LCOS-Menübaum ▶ Dateimanagement ▶ Konfiguration hochladen



Wählen Sie die zu verwendene Konfigurationsdatei aus und aktivieren Sie den Verwendungszweck als kundenspezifische Standardeinstellungen und/oder Rollout-Konfiguration.

Wenn beide Speicherplätze mit kundenspezifischen Standardeinstellungen **und** Rollout-Konfiguration belegt sind, kann das Gerät nicht mehr über den Reset-Taster auf die LANCOM Werkseinstellungen zurückgesetzt werden. Verwenden Sie in diesem Fall die Funktion 'Wiederherstellen der LANCOM Werkseinstellungen über seriellen Zugang' →Seite 12.

A.6.5 Löschen der Boot-Konfigurationen

Die alternative und die spezielle Boot-Konfiguration können nicht über die normalen Datei-Funktionen gelöscht werden. Nutzen Sie dazu den folgenden Befehl:

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

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

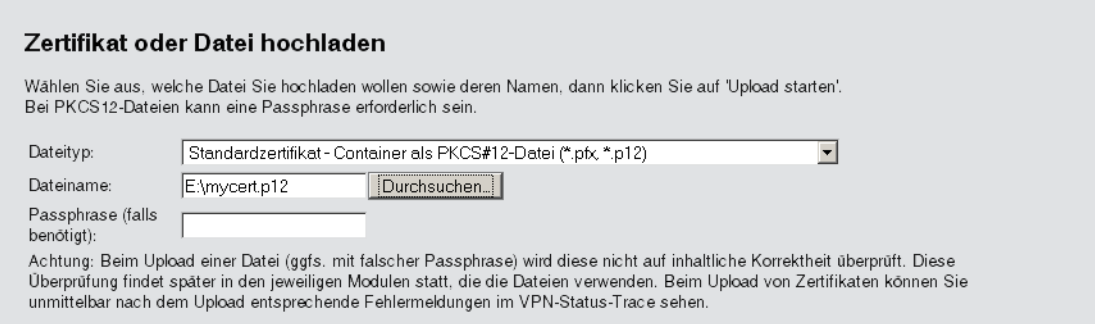
A.6.6 Verwendung von Zertifikaten

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 über WEBconfig in das Gerät hochladen.

- WEBconfig: LCOS-Menübaum ▶ Dateimanagement ▶ Zertifikat oder Datei hochladen



Wählen Sie das zu verwendene Zertifikat aus und starten Sie den Vorgang des Hochladens mit **Upload starten**.

A.7 Alternative DHCP-Server zur Weiterleitung

A.7.1 Einleitung

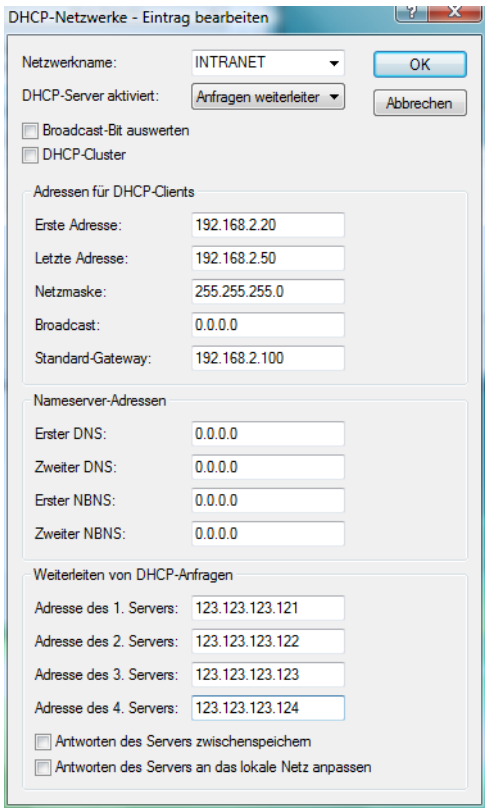
Der DHCP-Server erlaubt verschiedene Betriebsarten. Im Weiterleitungs-Modus agiert das Gerät im lokalen Netz als DHCP-Relay und leitet Anfragen an einen oder mehrere konfigurierte DHCP-Server weiter. Diese Einstellung erlaubt den Betrieb von zentralen DHCP-Servern in einem anderen Netz.

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.

A.7.2 Konfiguration

Die Konfiguration der DHCP-Server zur Weiterleitung finden Sie in folgendem Menü:

- LANconfig: TCP/IP ▶ DHCP ▶ DHCP-Netzwerke
- WEBconfig: LCOS-Menübaum ▶ Setup ▶ DHCP ▶ Netzliste



- **Adresse des 1. Servers**

  Hier wird die IP-Adresse des übergeordneten DHCP-Servers eingetragen, an den DHCP-Anfragen weitergeleitet werden, wenn für das Netzwerk die Betriebsart 'Anfragen Weiterleiten' gewählt wurde.

  Mögliche Werte:

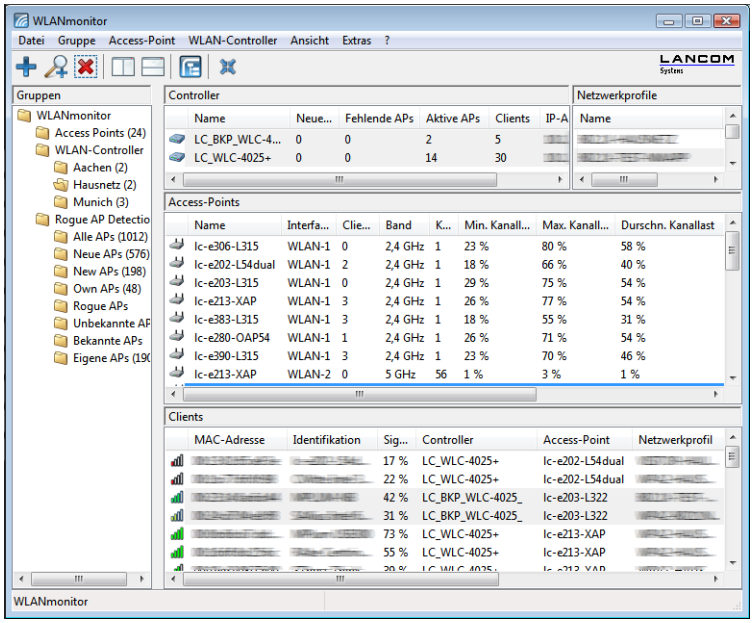
  - □ IP-Adresse oder die Broadcast-Adresse des Netzes, in dem der Server steht. Die Broadcast-Adresse ist die höchste Adresse in einem IP-Netz. Alle Pakete an diese Adresse werden von allen Hosts empfangen.

  Default:

  - □ 0.0.0.0

A.8 Kanallastanzeige im WLC-Betrieb

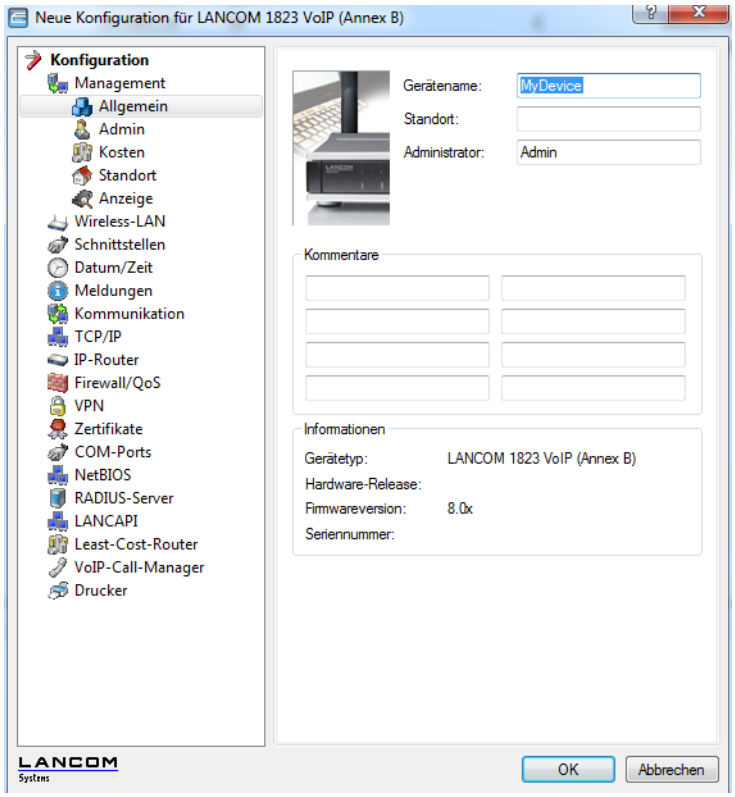
Für die von einem WLAN Controller verwalteten Access Points wird die Last auf den verwendeten Kanälen in drei Werten als minimale, maximale und durchschnittliche Kanallast angezeigt. Die angezeigten Werte werden in einem Messintervall von drei Minuten ermittelt. Die ersten Werte werden demnach auch erst nach drei Minuten angezeigt.



A.9 Änderungen in LANconfig

A.9.1 Konfigurationsbaum

Ab der Version 8.00 werden die beiden obersten Ebenen der Konfigurationsmenüs in LANconfig als "Konfigurationsbaum" permanent sichtbar in einem eigenen Bereich angezeigt. Diese neue Struktur erleichtert die Orientierung, erlaubt eine leichte Navigation und den schnellen Wechsel zwischen den Haupt-Konfigurationsbereichen.

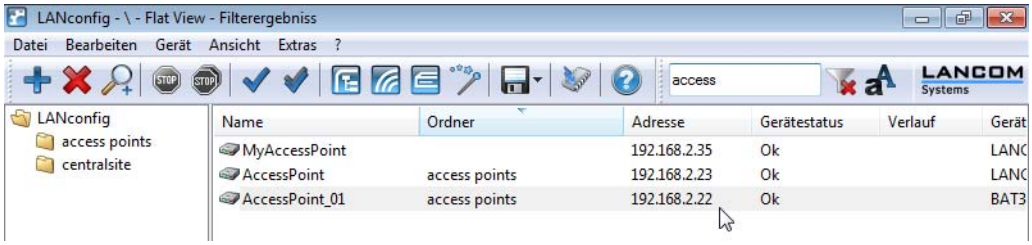


A.9.2 Dynamischer Filter

Mit dem dynamischen Filter in LANconfig können Sie sehr komfortabel die Anzeige auf die Geräte mit bestimmten Eigenschaften einschränken. Tragen Sie in das Filterfeld das gewünschte Filterkriterium ein. Als Filterkriterien können Sie alle angezeigten Eigenschaften verwenden, also z. B. Gerätename, Ordner, IP-Adresse, Gerätestatus, Gerätetyp, Seriennummer etc.

LANconfig reduziert die gewählte Ordneransicht auf die Einträge, welche das Filterkriterium an beliebiger Stelle (auch innerhalb von Begriffen) enthalten. Mit dem Filtersymbol neben dem Filterfeld können Sie den Filter zurück-

setzen. Mit dem Symbol für die Groß-Klein-Schreibung können Sie die exakte Übereinstimmung der Schreibweise des Filterkriteriums mit den aufgefundenen Stellen in den Eigenschaften erzwingen (Default: aus), andernfalls bleibt die Groß-Klein-Schreibung unbeachtet. Die Ordneransicht wird bei Verwendung des dynamischen Filters sofort bei der Eingabe angepasst. Der dynamische Filter bezieht sich immer auf den aktuell ausgewählten Ordner. Er kann auch mit der Ansicht "Flat View Modus" kombiniert werden, sodass zum ausgewählten Order auch alle Inhalte der untergeordneten Ordner hinzugezogen werden.



A.9.3 Zugriff auf Web-Server-Dienste einschränken

Der Zugriff auf ein Gerät über HTTP für die Konfiguration kann generell erlaubt, nicht erlaubt oder auf nur lesen eingeschränkt werden. Unabhängig davon kann der Zugriff auf die Web-Server-Dienste separat geregelt werden, z. B. um die Kommunikation von CAPWAP über HTTP zu ermöglichen, auch wenn der HTTP-Zugng generell nicht erlaubt ist.

- LANconfig: Management ▶ Admin ▶ Zugriff auf Web-Server-Dienste
- **HTTP-Port**

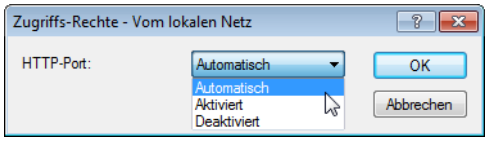
  Für jeden Zugriffsweg (je nach Gerät LAN, WAN, WLAN) stellen Sie hier das Zugriffsrecht von Web-Server-Diensten des Gerätes auf den HTTP-Server-Port ein.

  Mögliche Werte:

  - Automatisch: Der HTTP-Server-Port ist offen, solange ein Dienst angemeldet ist (z.B. CAPWAP). Ist kein Dienst mehr angemeldet, wird der Server-Port geschlossen.
  - Aktiviert: Der HTTP-Server-Port ist immer offen, auch wenn der Zugriff auf die Konfiguration über HTTP nicht erlaubt ist. Hiermit kann der direkte Konfigurationszugriff unterbunden werden, jedoch die automatische Konfiguration von APs über einen WLAN-Controller weiterhin erlaubt werden.
  - Deaktiviert: Der HTTP-Server-Port ist geschlossen, so dass kein Dienst den Web-Server benutzen kann. Wenn der Zugriff auf die Konfiguration über HTTP erlaubt ist, wird mit der entsprechenden Meldung quittiert, dass der Web-Server nicht erreichbar ist.

  Default:

  - Die Standardeinstellung für alle Zugangswege ist “Automatisch”.

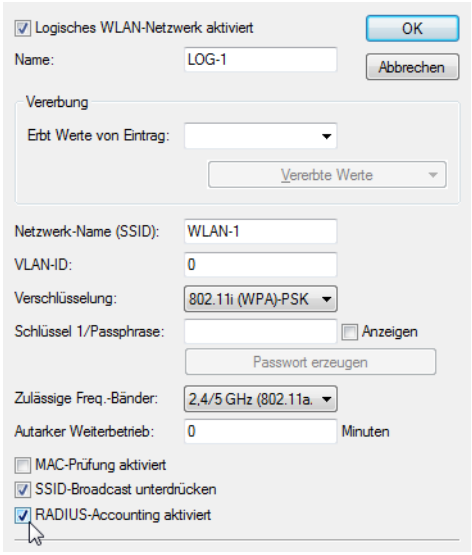


A.10 802.1x-Accounting im WLAN-Controller für logische WLANs aktivieren

Die Konfiguration der logischen WLAN-Netzwerke finden Sie in folgendem Menü:

- LANconfig: WLAN-Controller ▶ Profile ▶ Logische WLAN-Netzwerke (SSIDs)
- WEBconfig: LCOS-Menübaum ▶ Setup ▶ WLAN-Management ▶ AP-Konfiguration ▶ Netzwerkprofile

Ab LCOS 8.0 ist die Aktivierung des RADIUS-Accounting mit 802.1x individuell pro SSID möglich. In vorherigen Firmware-Versionen konnte das RADIUS-Accounting mit 802.1x nur global für alle SSIDs eingestellt werden.



■ **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 Access Points, die der WLAN-Controller mit diesem logischen WLAN-Netzwerk konfiguriert, müssen eine LCOS-Version 8.00 oder höher verwenden.

A.11 LANCOM Content Filter

A.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.

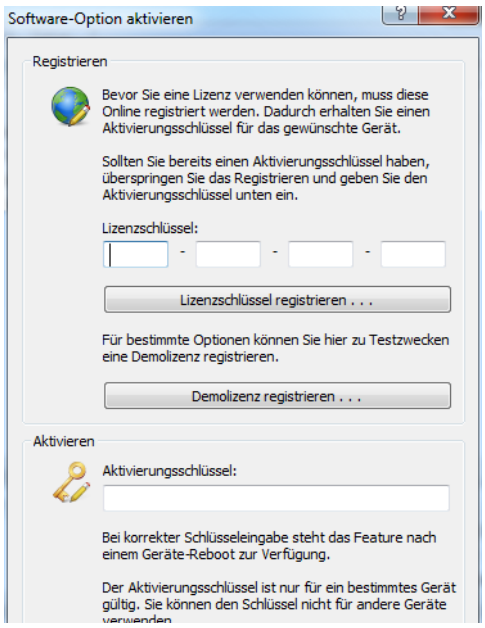
Der LANCOM Content Filter ist ein intelligenter Content-Filter und arbeitet dynamisch. Er kontaktiert einen Bewertungsserver, der gemäß den von Ihnen ausgewählten Kategorien die Bewertung der Internetseiten zuverlässig und korrekt vornimmt.

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 nur unverschlüsselte Webseiten über HTTP.

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.

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 vordefinierte Haupt- und Unterkategorien in Ihrem LANCOM Content Filter: 58 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.

A.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 und mit einer entsprechenden Firewall-Regel das Content-Filter-Profil auswählen.
3. Das Content-Filter-Profil muss für jeden Zeitraum das 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 unprüfter Zugriff auf die Webseiten möglich.

Wenn das Content-Filter-Profil nachträglich umbenannt wird, muss die Firewallregel ebenfalls angepasst werden.

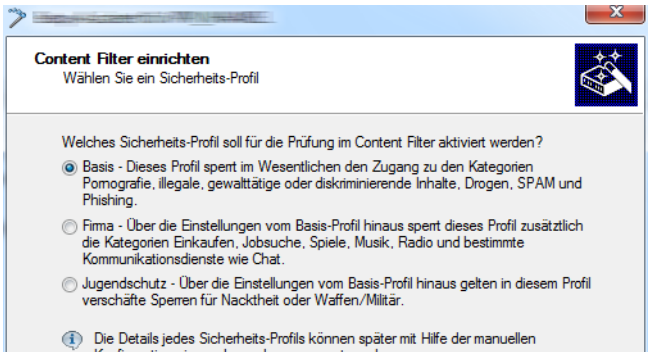
A.11.3 Quickstart

Nach der Installation des Content Filters sind alle Einstellungen für eine schnelle Inbetriebnahme vorbereitet.

Der Betrieb des Content Filters kann durch die Datenschutzrichtlinien in Ihrem Land oder Betriebsvereinbarungen in Ihrem Unternehmen eingeschränkt sein. Bitte prüfen Sie vor Inbetriebnahme die geltenen 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 verschäfte 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.

Detaillierte Informationen über die manuelle Konfiguration des Content-Filters finden Sie im Content-Filter-Handbuch als PDF als Download von www.lancom.de.

A.11.4 Die Standardeinstellungen im LANCOM Content Filter

In der Standardeinstellung sind im LANCOM Content Filter folgende Elemente angelegt:

- Eine Firewall-Regel
- Drei Firewall-Aktions-Objekte
- Drei Content-Filter-Profile
- Zwei Zeitrahmen
- Eine Blacklist
- Eine Whitelist
- Drei Kategorieprofile

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 und 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 (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.

Name	Zeitrahmen	Blacklisted	Whitelisted	Kategorie-Profil
CF-BASIC-PROFILE	ALWAYS	MY-BLACKLIST	MY-WHITELIST	BASIC-CATEGORIES
CF-PARENTAL-CONTROL-PROFILE	ALWAYS	MY-BLACKLIST	MY-WHITELIST	PARENTAL-CONTROL
CF-WORK-PROFILE	ALWAYS	MY-BLACKLIST	MY-WHITELIST	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

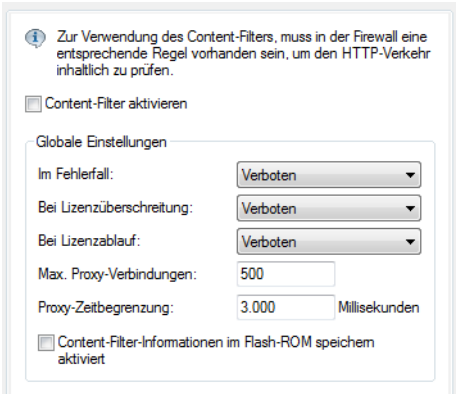
Die voreingestellte Whitelist hat den Namen "MY-WHITELIST"und ist leer. Tragen Sie hier optional die URLs ein, die für Ihre Anwendung erlaubt werden sollen.

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.

A.11.5 Allgemeine Einstellungen

Die globalen Einstellungen des LANCOM Content Filters nehmen Sie hier vor:



LANconfig: Content-Filter ▶ Allgemein

WEBconfig: LCOS-Menübaum ▶ Setup ▶ UTM ▶ Content-Filter ▶ Globale-Einstellungen

- **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.

  Mögliche Werte:

  - □ verboten, erlaubt

  Default:

  - □ 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.

Mögliche Werte:

□ verboten, erlaubt

Default:

□ verboten

Die Benutzer des Content-Filters werden automatisch aus der Benutzerliste entfernt, wenn von dieser IP-Adresse seit 24 Stunden 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 konfiguriert ist unter LANconfig: Meldungen ▶ Allgemein).

Hier können Sie bestimmen, was bei Ablauf der Lizenz passieren soll (blockieren oder ungeprüft durchlassen). 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.

Mögliche Werte:

□ verboten, erlaubt

Default:

□ verboten

■ **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.

Mögliche Werte:

□ 0 bis 999999 Verbindungen

Default:

□ geräteabhängig

■ **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.

Mögliche Werte:

□ 0 bis 999999 Millisekunden

Default:

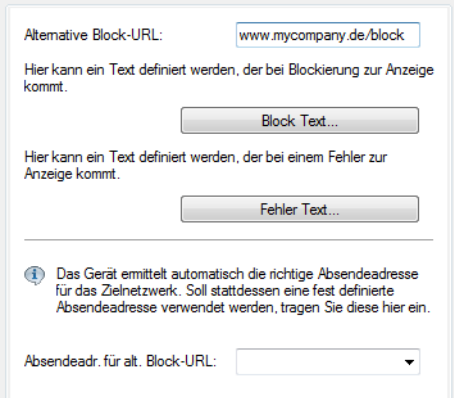
□ 3000 Millisekunden

Besondere Werte:

□ Der Wert 0 steht für keine Zeitbegrenzung. Werte kleiner als 100 Millisekunden sind nicht sinnvoll.

A.11.6 Einstellungen für das Blockieren

Die Einstellungen für das Blockieren von Webseiten nehmen Sie hier vor:



LANconfig: Content-Filter ▶ Blockieren

WEBconfig: LCOS-Menübaum ▶ 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 Blocktext 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 (Achtung: 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

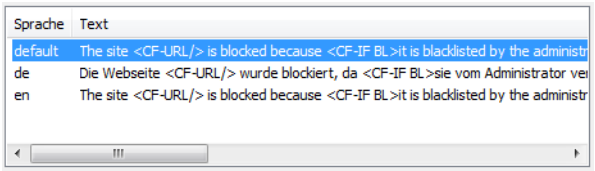
Default:

□ leer

Die hier eingestellte Absende-Adresse wird für jede Gegenstelle unmaskiert verwendet.

Block-Text

Hier können Sie einen Text definieren, der bei Blockierung angezeigt wird. Für unterschiedliche Sprachen kann jeweils ein eigener Blocktext definiert wird. Die Auswahl des verwendeten Blocktextes wird anhand des 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 eingestellten 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 vordefinierten 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 Blocktext für diese Sprache verwendet werden soll.

Mögliche Werte:

- 254 alphanumerische Zeichen

Default:

- leer

Besondere Werte:

Sie können für den Blocktext 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

Zum Ein- und Ausblenden von Teilen des Html-Dokuments wird ein Tag mit Attributen verwendet: <CF-IF att1 att2> ... </CF-IF>.

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.

  Da es getrennte Texttabellen für die Blockseite und die Fehlerseite gibt, ist das Tag nur sinnvoll, wenn Sie eine alternative Block-URL konfiguriert haben.
- OVERRIDEOK: wenn dem Benutzer ein Override erlaubt wurde (in diesem Fall sollte die Seite eine entsprechende Schaltfläche anzeigen)

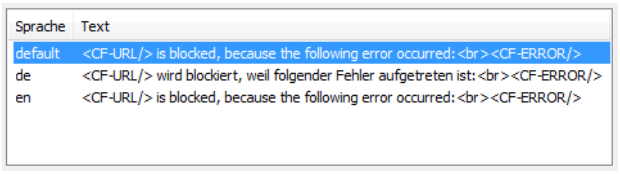
Werden in einem Tag mehrere Attribute angegeben, dann wird der Bereich eingeblendet, wenn mind. eine dieser Bedingungen erfüllt ist. Alle Tags und Attribute lassen sich mit den jeweils ersten zwei Buchstaben abkürzen (z.B. CF-CA oder CF-IF BL). Das ist notwendig, weil der Blocktext nur maximal 254 Zeichen 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.

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 eingestellten 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 vordefinierten 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 Fehlertext für diese Sprache verwendet werden soll.

Mögliche Werte:

- 254 alphanumerische Zeichen

Default:

- leer

Besondere Werte:

Sie können für den Fehlertext 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/>

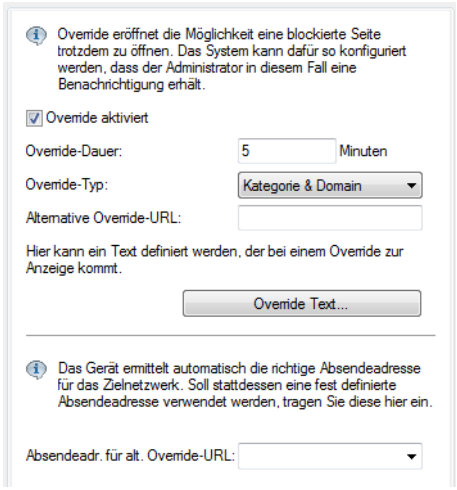
A.11.7 Override-Einstellungen

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 bestäti-

gen. Sie können die Konfiguration so einstellen, dass der Administrator bei Klick auf den Override-Button eine Benachrichtigung erhält (LANconfig: Content-Filter ▶ Optionen).

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. Nach dem Klick auf den Override-Button werden alle freigeschalteten Kategorien angezeigt. Wenn der Override-Typ "Domain" aktiviert ist wird die Domain freigeschaltet.

Die Einstellungen für die Override-Funktion finden Sie hier:



LANconfig: Content-Filter ▶ Override

WEBconfig: LCOS-Menübaum ▶ 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.

  Default:

  - Kategorie und Domain

- **Alternative Override-URL:**

  Hier können Sie eine alternative URL-Adresse eintragen. Im Falle des Override 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 Tags wie im Override-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

■ **Override-Absende-IP-Adresse:**

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 (Achtung: 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:

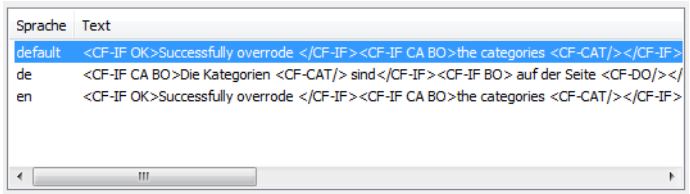
- □ leer



Die hier eingestellte Absende-Adresse wird für jede Gegenstelle unmaskiert verwendet.

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 eingestellten 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 vordefinierten 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 Blocktext 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.

Zum Ein- und Ausblenden von Teilen des Html-Dokuments wird ein Tag mit Attributen verwendet: <CF-IF att1 att2> ... </CF-IF>.

Attribute können sein:

□ 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> f&uuml;r <CF-DU/> Minuten freigeschaltet.<br><CF-LI/></CF-IF><CF-IF ERR>Override-Fehler:<br><CF-ERR/></CF-IF>
```

A.11.8 Profile des LANCOM Content Filters

Hier 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.

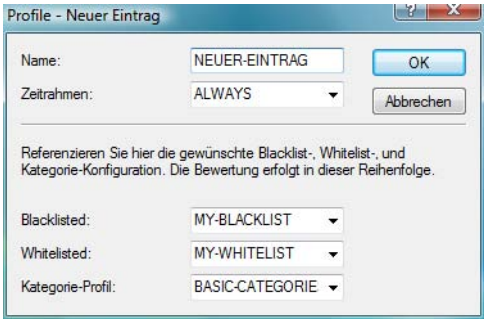
Um verschiedene Zeiträume unterschiedlich zu definieren, werden mehrere Content-Filter-Profileinträge mit dem gleichen Namen angelegt. Das Content-Filter-Profil besteht dann aus der Summe aller Einträge mit dem gleichen Namen.

Das Content-Filter-Profil wird über die Firewall angesprochen.

Bitte beachten Sie, dass Sie zur Nutzung der Profile im LANCOM Content Filters entsprechende Einstellungen in der Firewall vornehmen müssen.

Profile

Die Einstellungen für die Profile finden Sie hier:



LANconfig: Content-Filter ▶ Profile ▶ Profile

WEBconfig: LCOS-Menübaum ▶ Setup ▶ UTM ▶ Content-Filter ▶ Profile ▶ Profile

■ **Name**

Hier muss der Name des Profils angegeben werden, über das es in der Firewall referenziert wird.

Mögliche Werte:

□ Name eines Profils

Default:

□ leer

■ **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

WEBconfig: LCOS-Menübaum ▶ Setup ▶ Zeit ▶ Zeitrahmen

Zu einem Profil kann es auch mehrere Zeilen mit unterschiedlichen Zeitrahmen geben.

Mögliche Werte:

□ Always

□ Never

□ Name eines Zeitrahmenprofils

Default:

□ leer

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

Default:

□ leer

■ **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

Default:

□ leer

■ **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

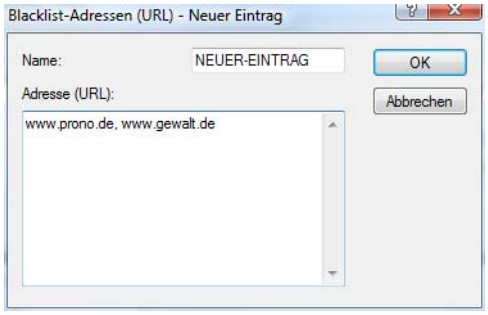
□ Neuer Name

Default:

□ leer

Blacklist-Adressen (URL)

Hier können Sie Webseiten konfigurieren, die anschließend verboten werden sollen.



LANconfig: Content-Filter ▶ Profile ▶ Blacklist-Adressen (URL)

WEBconfig: LCOS-Menübaum ▶ 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

Default:

□ leer

■ **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.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*.

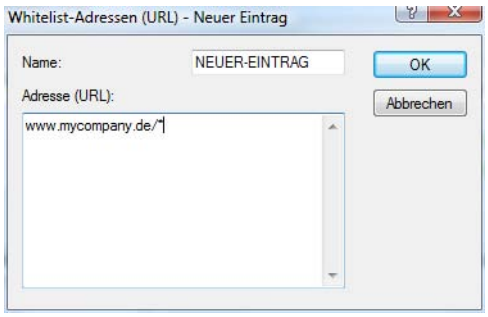
Einzelne URLs werden mit Leerzeichen getrennt.

Default:

□ leer

Whitelist-Adressen (URL)

Hier können Sie Webseiten konfigurieren, die gezielt erlaubt werden sollen.



LANconfig: Content-Filter ▶ Profile ▶ Whitelist-Adressen (URL)

WEBconfig: LCOS-Menübaum ▶ Setup ▶ UTM ▶ Content-Filter ▶ Profile ▶ Whitelists

■ **Name**

Hier muss der Name der Whitelist angegeben werden, über den sie im Content-Filter-Profil referenziert wird.

Mögliche Werte:

□ Name einer Whitelist

Default:

□ leer

■ **Adressen (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.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*.

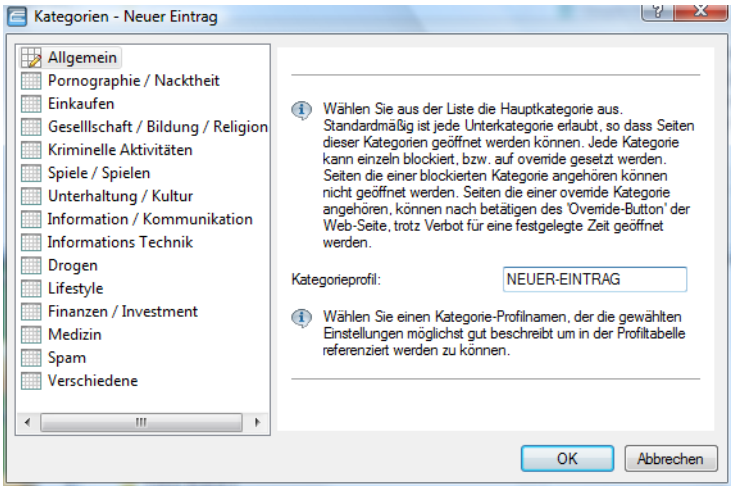
Einzelne URLs werden mit Leerzeichen getrennt.

Default:

□ leer

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-Filter ▶ Profile ▶ Kategorien

WEBconfig: LCOS-Menübaum ▶ Setup ▶ UTM ▶ Content-Filter ▶ Profile ▶ Kategorieprofile

■ **Kategorieprofil**

Hier wird der Name der Kategorieprofils angegeben, über den sie im Content-Filter-Profil referenziert wird.

Mögliche Werte:

□ Name eines Kategorieprofils

Default:

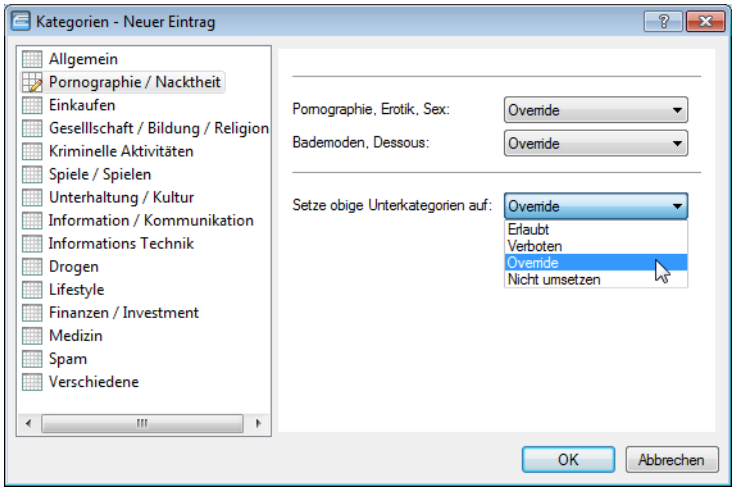
□ leer

■ **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
□ Informationstechnik
□ Drogen
□ Lifestyle
□ Finanzen/ Investement
□ Medizin
□ Spam
□ Verschiedene



Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

Mögliche Werte:

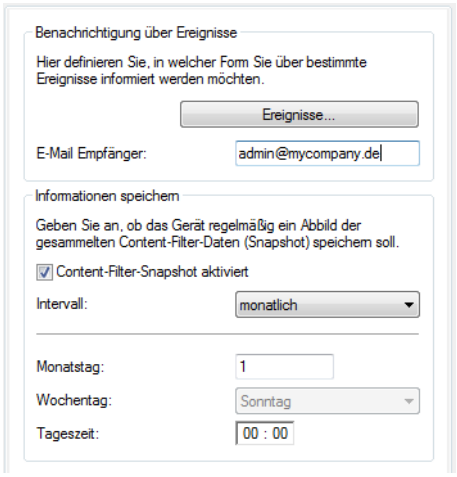
□ Erlaubt, Verboten, Override

Default:

□ Override

A.11.9 Optionen des LANCOM Content Filters

Hier können Sie einstellen, ob Sie über Ereignisse benachrichtigt werden und an wo die Informationen des LANCOM Content Filters gespeichert werden sollen.



LANconfig: Content-Filter ▶ Optionen

WEBconfig: LCOS-Menübaum ▶ Setup ▶ UTM ▶ Content-Filter ▶ Globale-Einstellungen

■ **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, über welchen Weg Meldungen ausgegeben werden sollen.

Fehler:

- □ Bei SYSLOG: Quelle "System", Priorität "Alarm".
- □ Default: Benachrichtigung SNMP

Lizenzablauf:

- □ Bei SYSLOG: Quelle "Verwaltung", Priorität "Alarm".
- □ Default: Benachrichtigung SNMP

Lizenz überschritten:

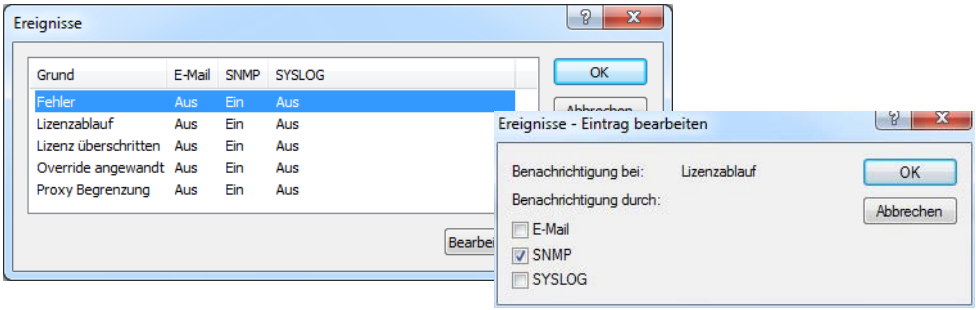
- □ Bei SYSLOG: Quelle "Verwaltung", Priorität "Alarm".
- □ Default: Benachrichtigung SNMP

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.

WEBconfig: LCOS-Menübaum ▶ Setup ▶ UTM ▶ Content-Filter ▶ Globale-Einstellungen ▶ Schnappschuss

■ **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 SnapShot monatlich, wöchentlich oder täglich angefertigt werden soll.

Mögliche Werte:

□ monatlich
□ wöchentlich
□ täglich

Default:

□ monatlich

■ **Monatstag:**

Ist eine monatliche Ausführung des SnapShot gewünscht, wählen Sie hier den Tag an dem der SnapShot angefertigt werden soll.

Mögliche Werte:

□ max. 2 Zeichen

Default:

□ 1



Wählen Sie als Monatstag sinnvollerweise eine Zahl zwischen 1 und 28, damit der Tag in jedem Monat vorkommt.

■ **Wochentag:**

Ist eine wöchentliche Ausführung des SnapShot gewünscht, selektieren Sie hier den Wochentag, an dem der SnapShot angefertigt werden soll.

Mögliche Werte:

□ Montag, Dienstag, Mittwoch, Donnerstag, Freitag, Samstag, Sonntag

Default:

□ Montag

■ **Tageszeit:**

Ist eine tägliche Ausführung des SnapShot gewünscht, tragen Sie hier die Tageszeit in Stunden und Minuten ein.

Mögliche Werte:

□ max. 5 Zeichen, Format HH:MM

Default:

□ 00:00

A.11.10 Zusätzliche Einstellungen für den LANCOM Content Filter

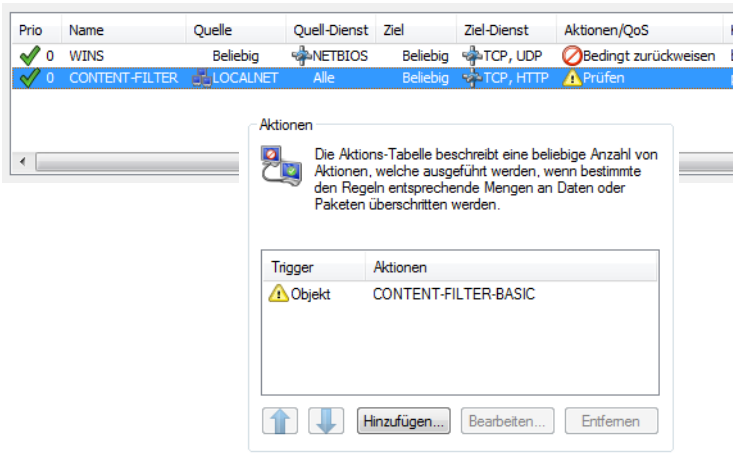
Firewall-Einstellungen für den Content-Filter

Die Firewall muss aktiviert sein, damit der LANCOM Content Filter arbeiten kann. Sie aktivieren die Firewall unter:

LANconfig: Firewall/QoS ▶ Allgemein

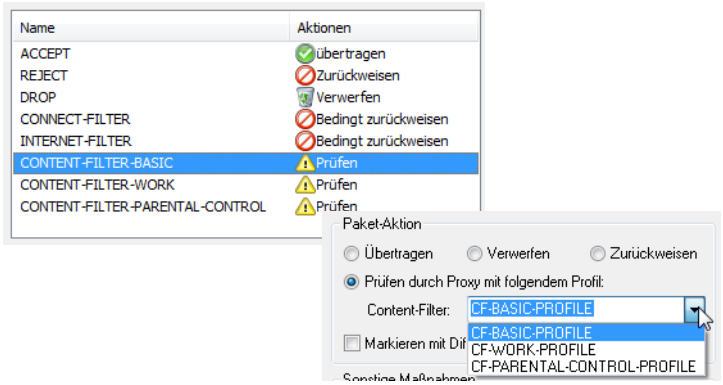
WEBconfig: LCOS-Menübaum ▶ Setup ▶ IP-Router ▶ Firewall

In der Default-Einstellung finden Sie die Firewall-Regel CONTENT-FILTER, die auf das Aktionsobjekt CONTENT-FILTER-BASIC zurückgreift:



Die Firewall-Regel sollte auf den Zieldienst "http" beschränkt werden, damit nur ausgehende HTTP-Verbindungen erfasst werden. Ohne diese Einschränkung werden alle Pakete über den Contentfilter geprüft, was zu einer Beeinträchtigung der Perfomance 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:

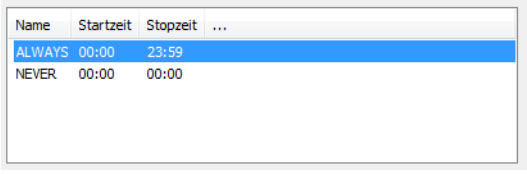


Beispiel: Beim Öffnen einer Webseite durchlaufen die Datenpakte die Firewall und werden von der Regel CONTENT-FILTER erfasst. Das Aktionsobjekt CONTENT-FILTER-BASIC prüft die Datenpakete mit dem Content-Filter-Profil CONTENT-FILTER-BASIC.

Zeitrahmen

Zeitrahmen werden 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.

Voreingestellt sind die Zeitrahmen "ALWAYS" und "NEVER". Weitere Zeitrahmen können Sie konfigurieren unter:



LANconfig: Datum/Zeit ▶ Allgemein ▶ Zeitrahmen

WEBconfig: LCOS-Menübaum ▶ Setup ▶ Zeit ▶ Zeitrahmen

■ **Name**

Hier muss der Name des Zeitrahmens angegeben werden, über den er im Content-Filter-Profil referenziert wird.

Mögliche Werte:

□ Name eines Zeitrahmens

Default:

□ leer

■ **Startzeit**

Hier kann die Startzeit (Tageszeit) angegeben werden, ab der das gewählte Profil gelten soll.

Mögliche Werte:

□ max. 5 Zeichen, Format HH:MM

Default:

□ 00:00

■ **Endzeit**

Hier kann die Endzeit (Tageszeit) angegeben werden, ab der das gewählte Profil nicht mehr gültig sein soll.

Mögliche Werte:

□ max. 5 Zeichen, Format HH:MM

Default:

□ 23:59

■ **Wochentage**

Hier können Sie die Wochentage auswählen, an denen der Zeitrahmen gültig sein soll.

Mögliche Werte:

□ Montag, Dienstag, Mittwoch, Donnerstag, Freitag, Samstag, Sonntag

Default:

□ Aktiviert für Montag, Dienstag, Mittwoch, Donnerstag, Freitag, Samstag, Sonntag

Zeitschemata lassen sich mit gleichem Namen, aber unterschiedlichen Zeiten auch über mehrere Zeilen hinweg definieren:

Name	Startzeit	Stopzeit	...
ALWAYS	00:00	23:59	
FREIZEIT	00:00	07:00	
FREIZEIT	12:01	13:00	
FREIZEIT	17:01	23:59	
NEVER	00:00	00:00	

A.12 DFS3

A.12.1 Einleitung

Mitte 2010 tritt eine neue Version (1.5.1) der EN 301 893 in Kraft, die einige Veränderungen für die Nutzung von WLAN-Frequenzen im Bereich 5,25 bis 5,35 und 5,47 bis 5,725 GHz mit sich bringt. Die neue EN 301 893-V1.5 regelt das DFS-Verfahren (Dynamic Frequency Selection) für diese Frequenzbereiche, mit dem Radarstationen vor dem Einfluss durch WLAN-Systeme geschützt werden. Bei der Erkennung von bestimmten Mustern in den empfangenen Funksignalen können WLAN-Systeme mit Hilfe von DFS die Radarstationen erkennen und einen automatischen Wechsel der verwendeten Kanäle durchführen. Im Unterschied zu den bisherigen Regelungen in EN 301 893-V1.3 (DFS2) wird DFS nach EN 301 893-V1.5 kurz als "DFS3" bezeichnet.

Generell wird ein Radarmuster durch die Werte Pulsrate, Pulsbreite und Anzahl der Pulse beschrieben. Nach den bisherigen DFS-Verfahren wurden nur feste Radarmuster geprüft, die durch definierte Kombinationen verschiedener Pulsraten und Pulsbreiten im WLAN-Gerät hinterlegt sind. Nach DFS3 müssen nun auch Muster aus wechselnden Pulsraten und Pulsbreiten als Radarmuster erkannt werden. Außerdem können innerhalb eines Radarsignals zwei oder drei unterschiedliche Pulsraten verwendet werden.

Für die Erkennung von Wetterradaren (Kanäle 120, 124 und 128 im Frequenzbereich 5,6 bis 5,65 MHz) gelten besondere Nutzungsbedingungen. Die DFS-Impentierung im LCOS unterstützt die verschärften Erkennungsbedingungen nicht, deshalb werden diese drei Kanäle von neueren LCOS-Versionen ausgespart.

A.12.2 Konfiguration

Alle WLAN-Systeme, die nach Inkrafttreten der EN 301 893-V1.5 in Betrieb genommen werden, müssen im 5 GHz-Band DFS3 verwenden. Um DFS3 in ihrem WLAN Gerät zu aktivieren, wählen Sie folgenden Menüeintrag:

WEBconfig: LCOS-Menübaum ▶ Setup ▶ Schnittstellen ▶ WLAN ▶ Radioeinstellungen

■ Bevorzugtes-DFS-Schema

Hier haben Sie die Möglichkeit zwischen DFS2 (EN 301 893-V1.3) und DFS3 (EN 301 893-V1.5) zu wählen.

□ Mögliche Werte:

EN 301 893-V1.5

EN 301 893-V1.3

□ Default:

EN 301 893-V1.5

Bei einem Upgrade von einer Firmware vor LCOS-Version 8.00 auf eine LCOS-Version 8.00 oder höher wird die vorherige Einstellung DFS2 (EN 301 893-V1.3) beibehalten.

Die Auswahl ist nicht möglich für WLAN-Geräte, die fest auf DFS3-Betrieb eingestellt sind, deren Prozessor die DFS3-Technologie nicht unterstützt oder die nur auf dem 2,4 GHz-Band senden.

A.13 Alternative URLs für CRLs

A.13.1 Einleitung

Die Adresse, von der eine Certificate Revocation List (CRL) abgeholt werden kann, wird normalerweise innerhalb der Zertifikate (als crlDistributionPoint) angegeben. Im LCOS 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.

A.13.2 Konfiguration

Die Tabelle für die alternativen CRL-URLs finden Sie auf folgenden Pfaden:

LANconfig: Zertifikate ▶ CRL-Client ▶ Alternative-URLs

WEBconfig: LCOS-Menübaum ▶ Setup ▶ Zertifikate ▶ CRLs ▶ Alternative-URL-Tabelle

■ Alternative-URL

Geben Sie hier die URL an, von der eine CRL abgeholt werden kann.

□ Mögliche Werte:

Gültige URL, max. 251 Zeichen.

□ Default:

Leer

A.14 Broken-Link-Detection

Wenn ein Access Point 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 Geräts deaktiviert werden, wenn die LAN-Verbindung verloren geht. So können die beim Access Point eingebuchten Clients einen anderen Access Point (mit ggf. schwächerem Signal) suchen und sich mit diesem verbinden.

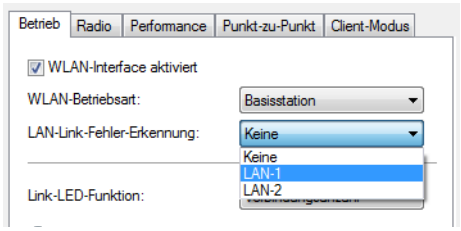
Bis zur LCOS-Version 7.80 bezog sich die Aktivierung der Link-Fehler-Erkennung immer auf LAN-1, auch wenn das Gerät über mehrere LAN-Interfaces verfügte. Außerdem wirkte sich die Deaktivierung auf alle verfügbaren WLAN-Module des Gerätes aus.

Ab LCOS-Version 8.00 kann die Link-Fehler-Erkennung gezielt an ein bestimmtes LAN-Interface gebunden werden.

Die Einstellung für die Link-Fehler-Erkennung finden Sie auf folgenden Pfaden:

LANconfig: Wireless-LAN ▶ Allgemein ▶ Physikalische WLAN-Einst. ▶ Betrieb

WEBconfig: LCOS-Menübaum ▶ Setup ▶ Schnittstellen ▶ WLAN ▶ Betriebs-Einstellungen



■ **LAN-Link-Fehler-Erkennung**

Mit dieser Funktion werden die WLAN-Module des Geräts deaktiviert, wenn das zugeordnete LAN-Interface nicht über einen Link zum LAN verfügt.

Mögliche Werte:

- □ Nein: Link-Fehler-Erkennung wird nicht genutzt.
- □ LAN-1 bis LAN-n (je nach verfügbaren LAN-Interfaces im Gerät): Alle WLAN-Module des Geräts werden deaktiviert, wenn das hier angegebene LAN-Interface keine Verbindung zum kabelgebundenen LAN hat.

Default:

- □ Nein

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.