LCOS 10.92

Public Spot

05/2025

LANCOM SYSTEMS

Inhalt

1 Public Spot.....5
1.1 Einführung.....5
1.1.1 Was ist ein "Public Spot"?.....5
1.1.2 Anwendungsszenarien.....6
1.1.3 Das Public Spot-Modul im Überblick.....13
1.2 Einrichtung und Betrieb.....16
1.2.1 Grundkonfiguration.....16
1.2.2 Sicherheitseinstellungen.....41
1.2.3 Erweiterte Funktionen und Einstellungen.....42
1.2.4 Alternative Anmeldeformen.....65
1.2.5 Geräteeigene und individuelle Voucher- und Authentifizierungsseiten (Templates).....100
1.2.6 Public Spot-Clients anzeigen.....122
1.2.7 Public Spot-Benutzern Werbung einblenden.....123
1.3 Zugriff auf den Public Spot.....124
1.3.1 Voraussetzungen für die Anmeldung.....124
1.3.2 Anmelden am Public Spot.....125
1.3.3 Informationen zur Sitzung.....126
1.3.4 Abmelden vom Public Spot.....126
1.3.5 Rat und Hilfe.....126
1.4 Tutorials zur Einrichtung und Verwendung des Public Spots.....128
1.4.1 Virtualisierung und Gastzugang über WLAN Controller mit VLAN.....128
1.4.2 Virtualisierung und Gastzugang über WLAN Controller ohne VLAN.....138
1.4.3 Einrichtung eines sicheren Hotspots mit Enhanced Open.....152
1.4.4 Einrichtung eines externen RADIUS-Servers für die Benutzerverwaltung.....153
1.4.5 Interner und externer RADIUS-Server kombiniert.....155
1.4.6 Prüfung von WLAN-Clients über RADIUS (MAC-Filter).....159
1.4.7 Einrichtung eines externen SYSLOG-Servers.....160
1.5 XML-Interface.....161
1.5.1 Funktion.....162
1.5.2 Einrichtung des XML-Interfaces.....163
1.5.3 Analyse des XML-Interfaces mit cURL.....165
1.5.4 Befehle.....165
2 Anhang.....173
2.1 Allgemein übermittelte RADIUS-Attribute.....173
2.1.1 Meldungen an den und vom Authentifizierungs-Server.....173
2.1.2 Meldungen an/vom Accounting-Server.....175
2.2 Durch WISPr übermittelte RADIUS-Attribute.....177
2.3 Dynamische Autorisierung durch RADIUS CoA (Change of Authorization).....178
2.3.1 Dynamische Autorisierung mit LANconfig konfigurieren.....178

2.4 Im- / Export von RADIUS-Benutzerdaten per CSV-Datei....180
2.4.1 Export von RADIUS-Benutzerdaten per CSV-Datei....180
2.4.2 Import von RADIUS-Benutzerdaten per CSV-Datei....180
2.5 Experteneinstellungen zur PMS-Schnittstelle....181
2.5.1 Accounting....181
2.5.2 Login-Formular....183
2.5.3 Gastname-Case-Sensitiv....186
2.5.4 Trennzeichen....187
2.5.5 Zeichensatz....187
2.6 SMS-Empfang und -Versand....188
2.6.1 Empfang von SMS-Nachrichten....188
2.6.2 Basiskonfiguration des SMS-Moduls....188
2.6.3 SMS-Nachrichten mit LANmonitor verwalten....189
2.6.4 SMS-Nachrichten mit LANmonitor versenden....190
2.6.5 URL-Platzhalter für den SMS-Versand....191
2.6.6 Zeichensatz für den SMS-Versand....191
2.7 Das SYSLOG-Modul....192
2.7.1 Aufbau der SYSLOG-Nachrichten....193
2.7.2 SYSLOG konfigurieren....195
2.7.3 Bedeutung von SYSLOG-Meldungen....201

Copyright

LANCOM Systems GmbH

A Rohde & Schwarz Company

Adenauerstr. 20/B2

52146 Würselen

Deutschland

www.lancom-systems.de

1 Public Spot

1.1 Einführung

Dieses Kapitel gibt Antworten auf die beiden folgenden Fragen:

- Was ist ein "Public Spot"?
- Welche Funktionen und Eigenschaften zeichnen das Public Spot-Modul aus?

1.1.1 Was ist ein "Public Spot"?

Public Spots, auch HotSpots genannt, sind Orte, an denen sich Benutzer mit ihren Endgeräten – z. B. einem Smartphone, Tablet-PC oder Notebook – in ein öffentlich zugängliches Netzwerk einwählen können. Üblicherweise stellen diese Netzwerke einen Zugang ins Internet bereit, doch kann ein Public Spot auch auf ein lokes Netzwerk beschränkt sein; z. B. um Besuchern einer musealen Einrichtung oder eines Messegeländes via Intranet zusätzliche Informationen bereitzustellen. Der Begriff wird dabei synonym zu den Geräten benutzt, über welche die Benutzer den Netzzugang schließlich herstellen, weshalb auch dieses Handbuch meistens nicht zwischen der Lokalität und dem Gerät unterscheidet.

Die Lösung: (W)LAN-Technologie

Für Public Spot-Szenarios bieten sich die bewährten (W)LAN-Technologien nach den internationalen IEEE 802.11/802.3-Standards an:

- Der Zugang über WLAN ermöglicht den schnellen und unkomplizierten Zugang über Funk: WLAN-Adapter gehören zur Standardausrüstung mobiler Endgeräte und unterstützen Bandbreiten, die selbst das ruckelfreie Abspielen von HD-Videos ermöglichen.
- Der Zugang über LAN ist – bei automatischer Adressvergabe via DHCP – ähnlich unkompliziert: Die meisten Notebooks besitzen standardmäßig einen LAN-Adapter, in den das Netzwerkkabel einzustecken ist.

Beim Zugang über LAN verliert der Anwender zwar seine stationäre und unterbrechungsfreie Flexibilität, allerdings ermöglicht diese Zugangsform – eine entsprechende Infrastruktur vorausgesetzt – selbst bei hoher Netzlast (z. B. durch Multimedia-Inhalte wie Video-on-Demand) und hoher Nutzerzahl (z. B. in einem großen Hotel) einen stabilen Netzbetrieb, wo Verbindungen via WLAN evtl. früher an ihre Grenzen stoßen. Ebenso ist es über einen Public Spot via LAN auch möglich, eine bereits bestehende, kabelgebundene Infrastruktur (z. B. in einer Hochschule) relativ kostengünstig um ein Public Spot-Angebot zu erweitern.

Besonderheiten beim Zugang über (W)LAN

Der Einsatz von herkömmlichen WLAN-Access-Points oder LAN-Routern als Public Spot wird dadurch erschwert, dass die Benutzer-Authentifizierung nur über RADIUS/802.1X möglich ist, was wiederum eine entsprechende Konfiguration erfordert. Aus diesem Grund ist der Einsatz von Geräten ohne Public Spot-Funktion nicht praktikabel, da diese Geräte nicht in der Lage sind, zwischen befugten und unbefugten Nutzern öffentlich zugänglicher Netze zu trennen und deren spezifische Netznutzung entsprechend zu protokollieren.

Benutzer-Autorisierung und -Authentifizierung

Sobald sich eine Person mit einem Endgerät in Reichweite eines Access Points befindet, kann sie zu diesem Access Point auch eine spontane Verbindung herstellen. Ähnliches gilt für frei zugängliche LAN-Anschlüsse. Daraus ergibt sich immer dann ein Problem, wenn der Zugang nicht jedermann, sondern nur bestimmten Benutzern zur Verfügung stehen soll. Genau diese Einschränkung ist beim Einsatz von Public Spots typisch.

Ein Public Spot muss daher in der Lage sein, den (W)LAN-Zugang auf Benutzerebene zu kontrollieren. Bei einfachen Public Spot-Installationen reicht es dabei aus, wenn die Benutzerdaten lokal im Router oder Access Point – oder alternativ in einem WLAN-Controller – gespeichert und verwaltet werden. Komplexere Installationen verwenden stattdessen für ein detaillierteres Accounting oder eine direkte Verwaltung Datenbankanbindungen an zentrale Authentifizierungs-Server. Solche zentralen Server arbeiten üblicherweise nach dem RADIUS-Verfahren.

Abrechnung (Accounting)

Möchte der Betreiber eines Public Spots diesen Service nicht kostenlos anbieten, muss er die Verbindungsdaten der einzelnen Nutzer erfassen und abrechnen. Üblich ist es beispielsweise, nach vorheriger Bezahlung eine befristete Benutzung zu gewähren (PrePaid-Modell), die verbrauchten Ressourcen im Nachhinein abzurechnen (PostPaid-Modell) oder die unbeschränkte Benutzung bis zu einem bestimmten Zeitpunkt zu erlauben (etwa bis zum Abreisetag in einem Hotel).

Auch für die Accounting-Funktion des Public Spots gilt bei kleinen Installationen, dass sie möglichst unkompliziert lokal im Gerät erfolgen sollte. Für größere Installationen ist eine zentrale Abrechnung über einen externen RADIUS-Server möglich. Je nach Anwendungsszenario, ist über eine Software-Schnittstelle optional auch die Anbindung an externe Systeme realisierbar, welche auf die Abrechnungsdaten zugreifen und die Authentifizierung der Anwender steuern (z. B. Hotelreservierungssysteme).

Logging

Das Public Spot-Modul stellt mittels RADIUS-Accounting und SYSLOG geeignete Schnittstellen zur Speicherung der Nutzungsdaten zur Verfügung.

Bitte beachten Sie, dass der Betrieb eines Public Spots (manchmal auch als "HotSpot" bezeichnet) in Ihrem Land rechtlichen Regulierungen unterliegen kann. Bitte informieren Sie sich vor der Einrichtung eines Public Spots über die jeweils geltenden Vorschriften. Informationen zu diesem Thema finden Sie auch im LANCOM Techpaper "Public Spot", erhältlich unter *www.lancom-systems.de*.

1.1.2 Anwendungsszenarien

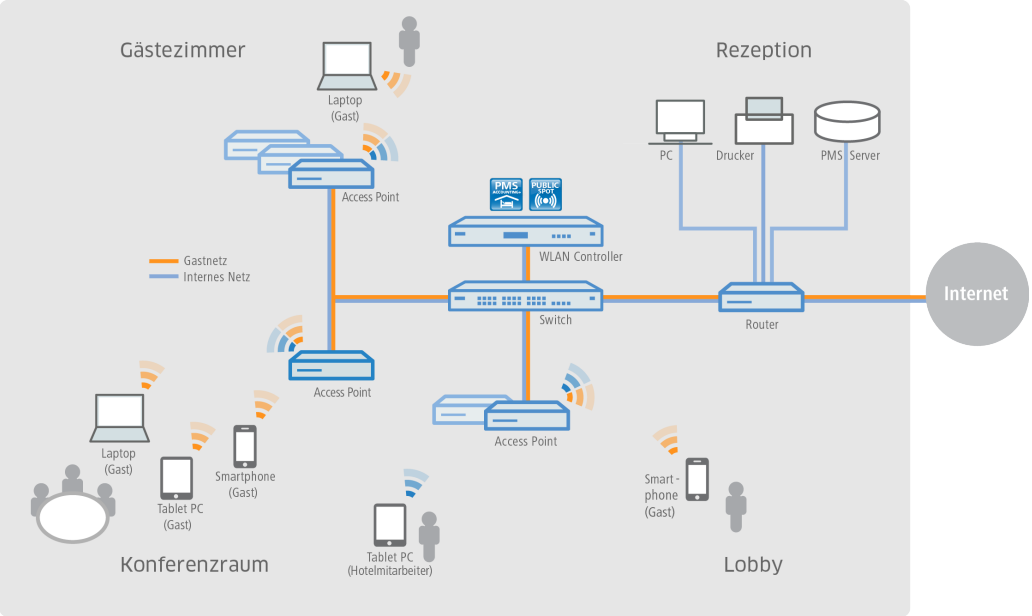
Gastzugänge im Hotel

Dank Wireless LAN ist es für Hotelbetreiber so einfach wie nie, ihren Gästen einen komfortablen Internetzugang zu bieten. Hotspot-Lösungen von LANCOM sind schnell installiert und geben Gästen die Möglichkeit, mit dem eigenem Laptop, Tablet oder Smartphone per WLAN auf das Internet zuzugreifen. Ob in der Lobby, dem Konferenzraum oder in Gästezimmern – absolut sicher getrennt vom internen Netz können überall dort, wo es gewünscht ist, Gastzugänge bereitgestellt werden.

Für die komfortable Abrechnung ist die LANCOM Public Spot PMS Accounting Plus Option ideal: Sämtliche Public Spot-Anmeldungen werden hierbei automatisch an den zentralen PMS-Server, auf welchem das Hotelabrechnungssystem installiert ist, weitergeleitet. Gäste können sich so z. B über die Zimmernummer und den Nachnamen am Hotspot anmelden. Bei kostenpflichtigen Internetzugängen können zudem die Nutzungsgebühren direkt auf die Zimmerrechnung verbucht werden. Alternativ sind natürlich auch kostenlose Gastzugänge in Hotels einfach einzurichten – je nach Bedarf.

- **Komfortable Inbetriebnahme und Konfiguration** – ein benutzerfreundlicher Einrichtungs- und Konfigurationsassistent garantiert eine einfache Inbetriebnahme des Hotspots. Genaueres erfahren Sie im Kapitel *Basis-Installation eines Public Spots für einfache Szenarien* auf Seite 16.
- **Kein Zugriff von Unbefugten auf interne Daten möglich** – per VLAN oder Layer-3-Tunnel erfolgt innerhalb einer Infrastruktur eine sichere Trennung des Haus- und Gastnetzes. Auch auf der Luftschnittstelle lassen sich die Daten sicher verschlüsseln, damit Gäste über das WLAN nicht in das Hotelnetz eindringen können. Genaueres erfahren Sie im Kapitel *Virtualisierung und Gastzugang über WLAN Controller mit VLAN* auf Seite 128.
- **Einfache Anmeldung des Gastes im WLAN** – durch die Smart Ticket-Funktion erhält der Gast die Zugangsdaten für den Public Spot ganz komfortabel automatisch per SMS oder E-Mail. Alternativ ist auch der Ausdruck eines Vouchers möglich oder die Anmeldung des Gastes über z. B. Zimmernummer/Nachname. Genaueres erfahren Sie im Kapitel *Alternative Anmeldeformen* auf Seite 65.

- **Einfache Abrechnung von kostenpflichtigen Internetzugängen** – mit der Erweiterung um die LANCOM Public Spot PMS Accounting Plus Option ist die Anbindung an Hotelabrechnungssysteme (wie Micros Fidelio) möglich. Genaueres erfahren Sie im Kapitel *Schnittstelle für Property-Management-Systeme* auf Seite 96.

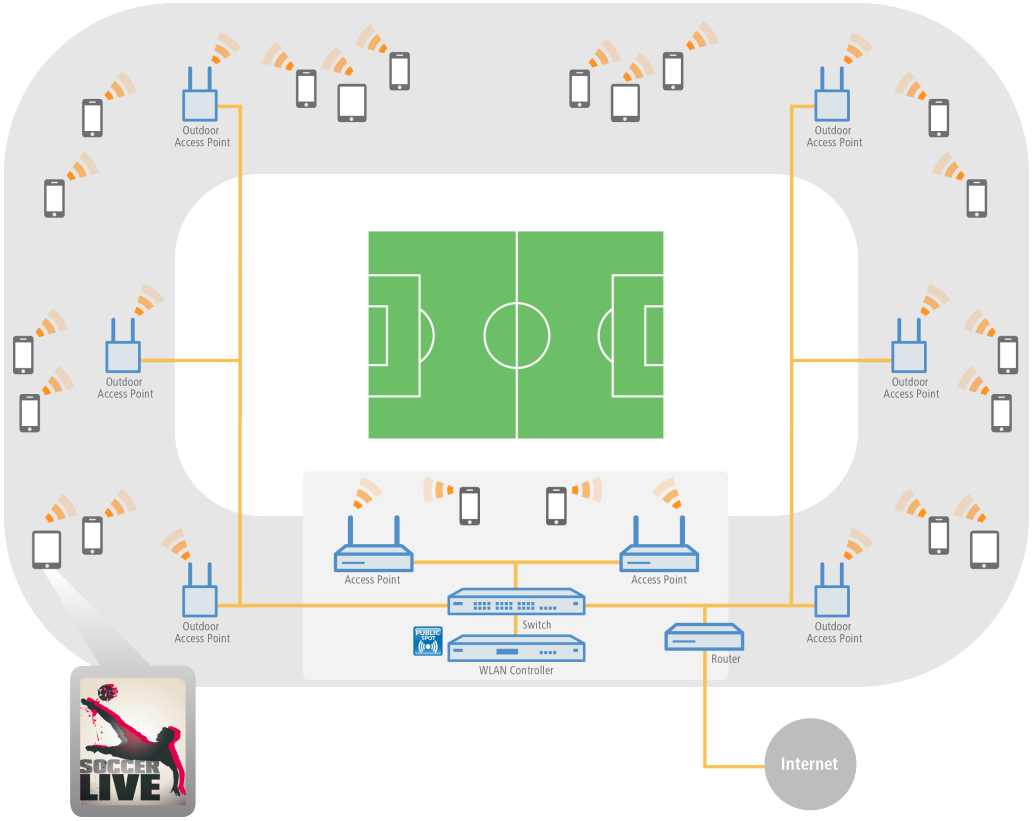


Gastzugänge in Sportstadien

Stadien, in denen große Sportveranstaltungen stattfinden, werden immer moderner und sollen auch einer sehr hohen Anzahl an Zuschauern ermöglichen, mit den eigenen Endgeräten den Komfort eines Internetzugangs zu nutzen, um z. B. Live-Content zur Veranstaltung abzurufen oder online zu surfen. Um den Gästen auf der Zuschauertribüne eine – im Vergleich zum überlasteten Mobilfunknetz – schnelle Internetverbindung zu bieten, ist ein Offloading in das Stadion-WLAN mithilfe von LANCOM Lösungen empfehlenswert. Durch die Einbindung der Clients in das Stadion-WLAN bietet sich dem Stadionbetreiber die Möglichkeit, zusätzliche Werbeflächen für Sponsoren und damit zusätzliche Einnahmequellen zu schaffen. So können beispielsweise die Hotspot-Anmeldeseite individuell gestaltet oder verschiedene Sponsoring-Websites freigeschaltet werden.

- **Multimediales Fan-Erlebnis** – durch einen WLAN-Internetzugang erhalten Fans die attraktive Möglichkeit, live aktuelle Sport-News und -informationen sowie beispielsweise Wiederholungen von Spielszenen aufzurufen.
- **Neue Werbeflächen generieren zusätzliche Einnahmen** – durch die individuelle Gestaltungsmöglichkeit der Hotspot-Anmeldeseite sowie die Konfiguration von vordefinierten Websites, die keine Anmeldung erfordern (Walled Garden-Funktion), stehen dem Stadionbetreiber zusätzliche, attraktive Werbeflächen zur Verfügung. Genaueres erfahren Sie im Kapitel *Anmeldungsfreie Netze* auf Seite 44.

- **Komfortable Inbetriebnahme und Konfiguration** – ein benutzerfreundlicher Einrichtungs- und Konfigurationsassistent garantiert eine einfache Inbetriebnahme des Hotspots. Genaueres erfahren Sie im Kapitel *Basis-Installation eines Public Spots für einfache Szenarien* auf Seite 16.



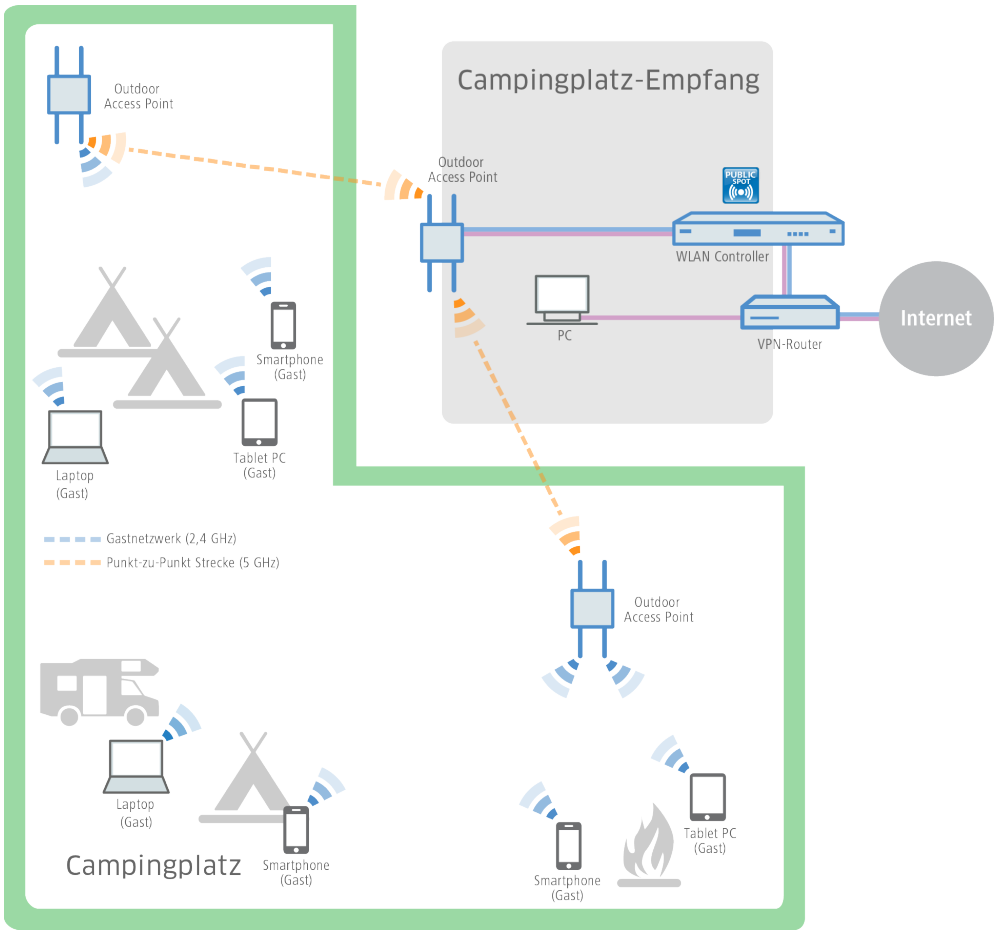
Gastzugänge auf Campingplätzen

Campingplätze befinden sich im Freien und sind meist sehr weitläufig. Trotzdem erwarten Urlauber auf modernen Campingplätzen den Komfort, mit dem eigenen Laptop, Tablet oder Smartphone jederzeit auf das Internet zuzugreifen. Ob im Zelt, im Wohnwagen oder am Lagerfeuer – ein überall verfügbarer Internetzugang ist ein echter Wettbewerbsvorteil für Campingplatzbetreiber.

Mit den robusten und wetterbeständigen Outdoor-Geräten von LANCOM und der LANCOM Public Spot Option, lassen sich auch diese anspruchsvollen Szenarien komfortabel umsetzen – ohne das aufwändige und kostenintensive Verlegen von Kabeln. So wird beispielsweise im Verwaltungsgebäude des Campingplatzes ein WLAN Controller (inkl. LANCOM Public Spot Option) mit einem LANCOM Dual Radio Outdoor Access Point verbunden. Von diesem wird das Signal nun über Punkt-zu-Punkt-Strecken im 5-GHz-Frequenzband an weitere Outdoor Access Points geleitet, welche die gewünschten Areale – wie z. B. Stellplätze oder Freizeitbereiche für die Gäste – mit WLAN im 2,4-GHz-Frequenzband abdecken. Dabei ist eine sichere Trennung des Gast- und Verwaltungsnetzes dank VLAN-Zuweisung gewährleistet.

- **Komfortabel online ohne Verlegung von Kabeln** – auch in großen Arealen können Gäste ohne aufwändige Installation mit dem Internet verbunden werden.
- **Komfortable Inbetriebnahme und Konfiguration** – ein benutzerfreundlicher Einrichtungs- und Konfigurationsassistent garantiert eine einfache Inbetriebnahme des Hotspots. Genaueres erfahren Sie im Kapitel *Basis-Installation eines Public Spots für einfache Szenarien* auf Seite 16.
- **Einfacher Gastzugang** – durch die Smart Ticket-Funktion erhält der Client die Zugangsdaten für den Public Spot ganz komfortabel automatisch per SMS oder E-Mail. Alternativ ist auch der Ausdruck eines Vouchers möglich. Genaueres erfahren Sie im Kapitel *Alternative Anmeldeformen* auf Seite 65.

- **Zuverlässig auch unter extremen Bedingungen** – dank der robusten IP66 Outdoor-Gehäuse und ihres erweiterten Temperaturbereichs sind die LANCOM Outdoor-Geräte zuverlässig und trotzen auch extremen Wetterbedingungen von -33 bis +70 °C.



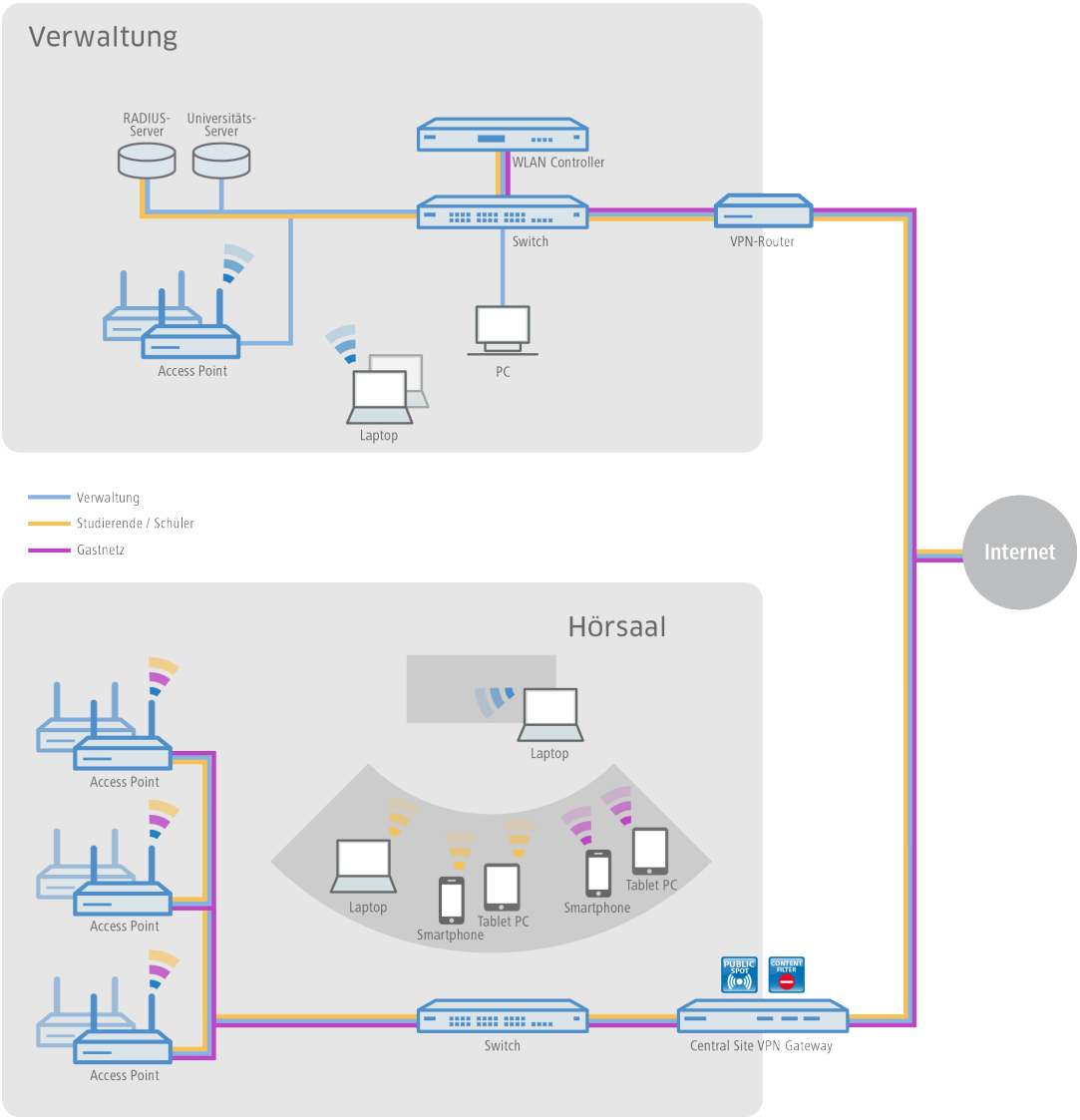
Gastzugänge in Schulen und Universitäten

Für Hausarbeiten recherchieren, für Prüfungen lernen, den Unterricht vorbereiten oder interaktiv gestalten. Die Möglichkeit der Internetnutzung ist für Schüler und Studenten sowie Lehrer und Mitarbeiter an modernen Schulen und Universitäten heute unerlässlich – und das auch in voneinander getrennten Gebäudeteilen, möglichst kabellos und mit den eigenen Endgeräten.

Mit Hilfe von LANCOM WLAN-Lösungen ist dies leicht umsetzbar. Indem separate Netze konfiguriert werden, sind die Internetzugänge der Schüler und Studenten vom Zugang der Verwaltung sicher getrennt. Dank dynamischer VLAN-Zuweisung werden die verschiedenen Benutzergruppen über nur eine SSID den für sie vorgesehenen VLANs zugewiesen. So erhält beispielsweise nur das Personal Zugriff auf den Universitätsserver. Gleichzeitig erhalten die Schüler und Studenten den heute so wichtigen Komfort eines weitreichenden WLAN-Gastzugangs. Die Authentifizierung im Schüler- und Studentennetz (z. B. Eduroam) kann beispielsweise über IEEE 802.1X erfolgen. So ist es auch für Gaststudenten von kooperierenden Unis möglich, sich in das WLAN der Gasthochschule einzuwählen. Und selbst Tagungsgästen kann z. B. mittels eines Vouchers ein temporärer Gastzugang zur Verfügung gestellt werden.

- **Sichere Anmeldung für Universitätsangehörige** – Professoren, Studenten und Angestellte der Universität können über das sicher verschlüsselte WLAN Zugang zum Internet und zu verschiedenen Online-Bibliotheken erhalten.
- **Kein Zugriff von Unbefugten auf interne Daten möglich** – per VLAN oder Layer-3-Tunnel erfolgt innerhalb einer Infrastruktur eine sichere Trennung der Verwaltungs-, Studenten- und Professoren- und Gastnetze. Genaueres erfahren Sie im Kapitel *Virtualisierung und Gastzugang über WLAN Controller mit VLAN* auf Seite 128.

- **Kein Missbrauch des Netzwerks** – durch den LANCOM Content Filter erfolgt eine professionelle, datenbankgestützte Verifizierung von Webseiten. Unerwünschte Websites oder Webinhalte können so für definierte Benutzergruppen unzugänglich gemacht werden.
- **Komfortable, kabellose Internetzugänge** – auch in großen Arealen haben Gäste ohne aufwändige Installation mit ihren mobilen Endgeräten WLAN-Internetzugang.



Gastzugänge in Unternehmen

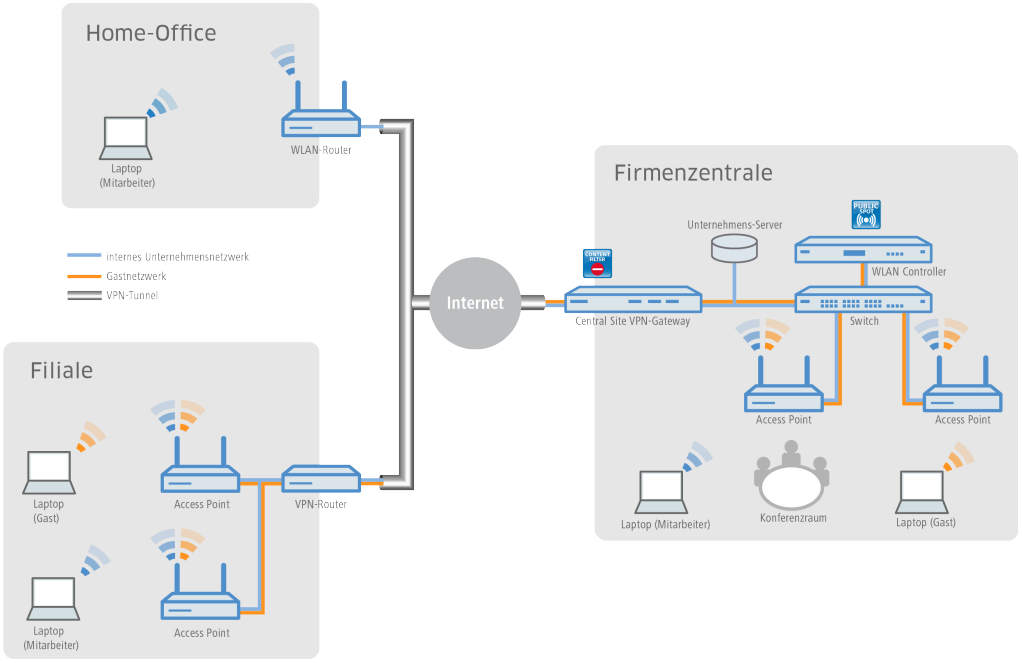
Innerhalb eines Unternehmens mit einer komplexen Netzwerkstruktur ist die Flexibilität und Stabilität des Internetzugangs extrem wichtig. Filialen müssen standortübergreifend auf das Unternehmensnetzwerk zugreifen und Home Office-Mitarbeiter benötigen ebenso Zugriff auf E-Mail-Konten und Datenbanken. Zusätzlich soll Kunden und Besuchern ein separater Gastzugang angeboten werden.

Mit den Geräten von LANCOM und der LANCOM Public Spot Option sind auch diese Szenarien leicht umzusetzen. Über VPN-Tunnel werden dabei die Standorte miteinander verbunden. Unternehmen können ihren externen Gästen durch ein separates Gastnetzwerk in der Firmenzentrale oder auch in angebundenen Filialen Zugriff auf das Internet über die eigenen mobilen Endgeräte gewähren ("Bring Your Own Device"). Dabei bleibt der Zugriff auf unternehmensinterne Daten nur den befugten Mitarbeitern vorbehalten.

- **Sichere Trennung von Unternehmens- und Gastnetz** – durch die sichere Trennung per VLAN oder Layer-3-Tunnel erfolgt innerhalb einer Infrastruktur eine sichere Trennung des Mitarbeiter- und Gastnetzes. Interne Daten sind somit

sicher vor unbefugten Zugriffen. Genaueres erfahren Sie im Kapitel *Virtualisierung und Gastzugang über WLAN Controller mit VLAN* auf Seite 128.

- **Komfortable Inbetriebnahme und Konfiguration** – über LANCOM WLAN Controller können unterschiedliche Benutzerprofile definiert und die Konfigurationen in die verschiedenen WLAN-Geräte – selbst über entfernte Standorte hinweg – eingespielt werden.
- **Einfacher Gastzugang** – über Voucher können den Gästen am Empfang Zugangsdaten für den Public Spot ganz komfortabel für die Nutzung eigener mobiler Clients zur Verfügung gestellt werden ("Bring Your Own Device"). So erhalten nur registrierte Besucher Zugang zum Internet sowie ggf. Zugriff auf weitere Dienste wie E-Mail-Konten.
- **Kein Missbrauch des Netzwerks** – durch den LANCOM Content Filter erfolgt eine professionelle, datenbankgestützte Verifizierung von Webseiten. Unerwünschte Websites oder Webinhalte können so für definierte Benutzergruppen unzugänglich gemacht werden.



Gastzugänge für Provider

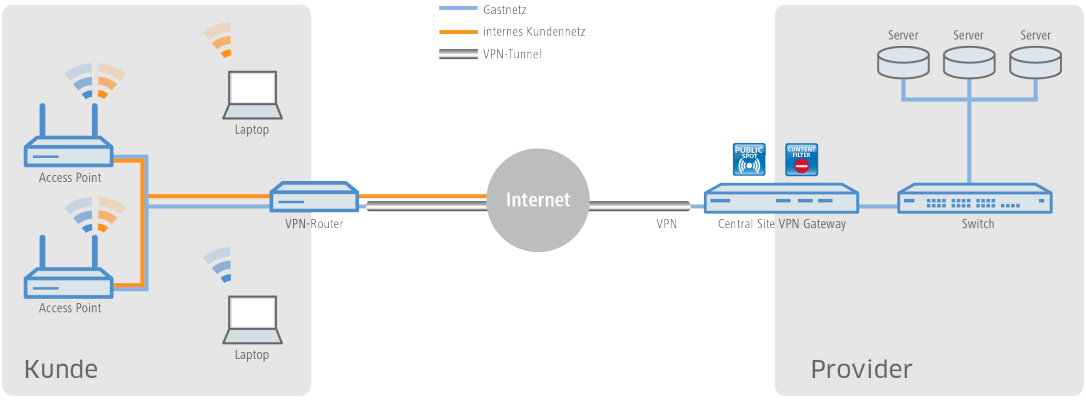
Für Internet-Provider ist es mit den Lösungen von LANCOM sehr einfach, bei ihren Kunden ein Netzwerk mit Gastzugängen anzubieten. Der Provider erhält von LANCOM alle benötigten Netzwerkprodukte aus einer Hand und managt die Netzwerke seiner Kunden zentral und komfortabel – ohne einen Techniker vor Ort.

Für die Umsetzung werden beim Kunden des Providers (beispielsweise ein Hotel, Krankenhaus oder Geschäft) LANCOM Access Points hinter einem LANCOM VPN-Router installiert. Ein separat getrenntes, internes Netz verfügt über einen direkten Internetzugang. Der Gastzugang läuft über einen sicheren VPN-Tunnel zunächst zum Central Site VPN Gateway beim Provider, der auf seinen internen Servern die ankommenden Anfragen protokollieren kann. Ebenfalls kann er mit dem LANCOM Content Filter den Zugang von unerwünschten oder illegalen Websites für die Gastzugänge des Kunden einschränken oder sperren.

- **Einfaches und zentrales Management und Rollout** – auch ohne einen Techniker vor Ort kann der Provider zentral die Netzwerke der Kunden überwachen und konfigurieren. Genaueres erfahren Sie im Kapitel *Basis-Installation eines Public Spots für einfache Szenarien* auf Seite 16.
- **Verschiedene Redirect-Optionen** – durch Netztrennung können verschiedene Gestaltungsmöglichkeiten des Hotspot-Dienstes realisiert werden. So kann den Endkunden z. B. ausschließlich die Verwaltung ihres Hotspots angeboten werden oder auch ein Full-Service bereitgestellt werden, indem der komplette Datenverkehr vom Endkunden zum Provider getunnelt weitergeleitet wird.
- **Anbindung eigener AAA-Systeme** – LANCOM stellt verschiedene Schnittstellen (RADIUS, XML, FIAS) zur Verfügung, mit denen eigene AAA-Server kombiniert werden können. So kann die Authentifizierung und Anmeldung am Hotspot

sowie die Abrechnung providerspezifisch umgesetzt werden. Genaueres erfahren Sie im Kapitel *Alternative Anmeldeformen* auf Seite 65.

- **Multi-Provider-Unterstützung** – LANCOM Geräte sind nicht auf das Zurückgreifen auf einen bestimmten Provider festgelegt. Hotspot-Dienstanbieter, die über Kooperationen mit verschiedenen Providern verfügen, können Ihre Software-Lösungen über verschiedene Schnittstellen mit LANCOM Geräten kombinieren. Genaueres erfahren Sie im Kapitel *Alternative Anmeldeformen* auf Seite 65.
- **Kein Missbrauch des Netzwerks** – durch den LANCOM Content Filter erfolgt eine professionelle, datenbankgestützte Verifizierung von Webseiten. Unerwünschte Websites oder Webinhalte können so für definierte Benutzergruppen unzugänglich gemacht werden.
- **Data Offloading** – WLAN-Hotspots entlasten wirkungsvoll das Mobilfunk-Netz, indem der Datenverkehr auf andere Infrastrukturen ausgelagert wird.

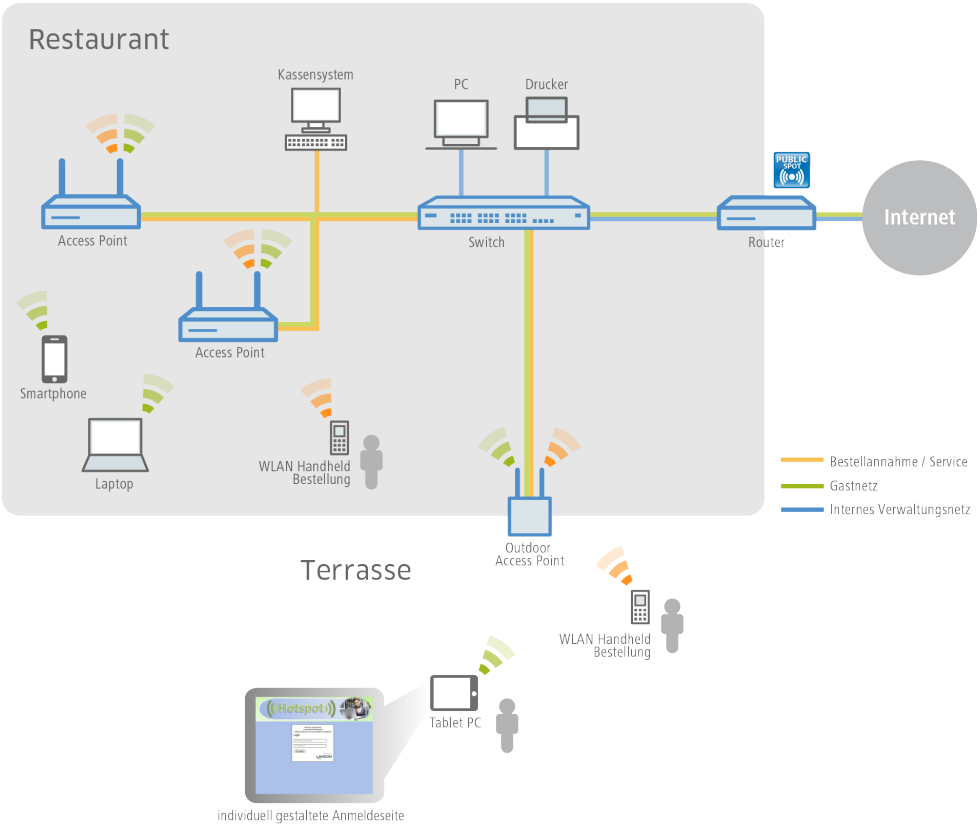


Gastzugänge in der Gastronomie

Den Gästen in einem modernen Restaurant oder Café einen Hotspot zur Verfügung zu stellen, kann die Attraktivität der Location deutlich steigern. Mit den WLAN-Lösungen von LANCOM profitieren die Gäste von einem WLAN-Gastnetz, sodass sie mit ihren mobilen Smartphones, Tablet PCs oder Laptops komfortabel das Internet nutzen können – und das absolut sicher getrennt vom internen Verwaltungsnetz. Für eine deutliche Steigerung der Effizienz im Arbeitsablauf haben die Servicekräfte zudem die Möglichkeit, Bestellungen mithilfe eines WLAN-fähigen Handhelds aufzunehmen und direkt an das Kassensystem, die Küche oder an die Getränketheke zu übertragen. Natürlich ist ein WLAN-Zugang für die Gäste als auch für die Bestellannahme ebenso im Terrassen- oder Außenbereich der Gastronomie verfügbar, denn für Bereiche im Freien eignet sich ideal ein robuster LANCOM Outdoor Access Point

- **Individueller und flexibler Gestaltungsspielraum** – ob eigene Logos, Texte oder Bilder – die Begrüßungsseite des Public Spots kann ganz einfach nach den eigenen Wünschen gestaltet werden. Auch das Aufrufen vordefinierter Websites ist möglich (Walled Garden-Funktion), sodass z. B. die Speisekarte des Restaurants oder die eigene Website ohne vorherige Anmeldung am Hotspot vom Gast besucht werden kann. Genaueres erfahren Sie im Kapitel *Geräteeigene und individuelle Voucher- und Authentifizierungsseiten (Templates)* auf Seite 100.
- **Kein Zugriff von Unbefugten auf interne Daten möglich** – per VLAN oder Layer-3-Tunnel erfolgt innerhalb einer Infrastruktur eine sichere Trennung der Netze. Genaueres erfahren Sie im Kapitel *Virtualisierung und Gastzugang über WLAN Controller mit VLAN* auf Seite 128.
- **Komfortable Inbetriebnahme und Konfiguration** – ein benutzerfreundlicher Einrichtungs- und Konfigurationsassistent garantiert eine einfache Inbetriebnahme von Hotspots. Genaueres erfahren Sie im Kapitel *Basis-Installation eines Public Spots für einfache Szenarien* auf Seite 16.

› **Einfacher Gastzugang** – durch die Smart Ticket-Funktion erhält der Gast die Zugangsdaten für den Public Spot ganz komfortabel automatisch per SMS oder E-Mail. Alternativ ist auch der Ausdruck eines Vouchers möglich. Genaueres erfahren Sie im Kapitel *Alternative Anmeldeformen* auf Seite 65.



1.1.3 Das Public Spot-Modul im Überblick

Die Ansprüche an Geräte im Public Spot-Betrieb sind so unterschiedlich, wie die Umgebungen, in denen sie eingesetzt wird. Ein Public Spot verfügt über Funktionen für die unterschiedlichsten Bedürfnisse, die in den folgenden Abschnitten genauer beschrieben sind.

Open User Authentication (OUA)

Die Open User Authentication (OUA) stellt eine web-basierte Authentisierung über ein Formular bereit und eignet sich deshalb optimal für Public Spot-Installationen.

Typischer Ablauf einer Online-Sitzung mit OUA

1. Der Benutzer eines (W)LAN-fähigen Endgerätes befindet sich in Reichweite eines Access Points bzw. einer Netzwerkdose im Public Spot-Betrieb.

   › WLAN: Nach dem Systemstart meldet sich der WLAN-Adapter automatisch an betreffenden Access Point an.

   › LAN: Nach dem Systemstart stellt der Benutzer über ein geeignetes Kabel den Netzanschluss her und lässt sich vom DHCP-Server eine Adresse zuweisen.

   Ein Internetzugang oder der Zugriff auf einen kostenpflichtigen Service ist in dieser Phase noch nicht möglich.

2. Der Benutzer startet seinen Web-Browser. Das den Public Spot-Service anbietende Gerät führt den Benutzer automatisch auf die Anmeldeseite des Public Spots. Auf dieser Seite findet er detaillierte Informationen zum angebotenen Service.

   Alternativ führt das vom Benutzer verwendete Endgerät automatisch eine Captive-Portal-Erkennung durch und präsentiert direkt nach der Einbuchung in das WLAN die Anmeldeseite des Public Spot.

In der Regel hat der Benutzer seine Anmeldedaten in Form eines Vouchers für einen zeitlich begrenzten Zugang zum Public Spot erhalten. Es sind aber auch andere Anmeldeformen denkbar, wie z. B. die Anmeldung nach Bestätigen der Nutzungsbestimmungen des Betreibers oder die selbstständige Anforderung der Zugangsdaten via E-Mail oder SMS.

3. Im Falle einer Voucher-Anmeldung trägt der Benutzer auf der Anmeldeseite seine Zugangsdaten (Benutzerkennung und Passwort) ein. Je nach Konfiguration prüft entweder der geräteinterne oder ein externer RADIUS-Server die eingegebenen Anmeldedaten. Im Erfolgsfall erhält der Benutzer den Zugang zum Public Spot, ansonsten erscheint eine Fehlermeldung. Falls die Verwendung von Zeitkontingenten gewünscht ist (PrePaid-Modell), überträgt der RADIUS-Server dem Public Spot zusätzlich Informationen zum verfügbaren Zeitguthaben des Benutzers.
4. Der Benutzer kann sich jederzeit beim Public Spot abmelden. Unabhängig davon beendet der Public Spot eine Sitzung selbstständig bei vollständigem Ablauf des Zeitguthabens, bei Erreichen eines festgelegten Ablaufdatums oder bei längerem Kontaktabbruch.

   Während und beim Beenden der Sitzung liefert der Public Spot dem Benutzer eine Übersicht über die Sitzungsdaten. Auf Wunsch meldet der Public Spot parallel dazu alle wichtigen Abrechnungsinformationen des Benutzers an den zuständigen RADIUS-Accounting-Server. Dies kann entweder der geräteinterne oder ein extern konfigurierter Server sein.

Sicherheit im (W)LAN

Bei der Betrachtung von (W)LANs entstehen oft erhebliche Sicherheitsbedenken. Solche Bedenken existieren im Zusammenhang mit Public Spots sowohl beim Betreiber als auch beim Benutzer.

Sicherheit für den Betreiber

Für den Betreiber eines Public Spots steht die Absicherung seiner Netzwerk-Infrastruktur im Vordergrund. Das Public Spot-Modul stellt dem Betreiber deshalb eine Reihe von Sicherungstechnologien und -methoden zur Verfügung:

- **Multi-SSID** (nur WLAN)**, VLAN und virtuelle Router**
  - Die sichere Abgrenzung des öffentlichen Zugangs kann durch eine oder mehrere separate Funkzellen eines Access Points erfolgen (Multi-SSID).
  - VLAN-Technik kann den öffentlichen Zugang vom privaten Netz des Betreibers trennen.
  - Die virtuelle Routing-Technologie ARF (Advanced Routing and Forwarding) von LANCOM Systems versieht eine SSID mit eigenen Sicherheits- und QoS-Einstellungen und routet darüber nur bestimmte Ziele.

  So kann der Gastzugang über einen Public Spot – sicher und effektiv vom Produktivnetz getrennt – die gemeinsame Infrastruktur mitnutzen. Die geräteinterne Firewall kann dabei z. B. die für Public Spot-Nutzer verfügbare Bandbreite im WAN auf max. 50 % begrenzen und nur auf Webseitenzugriffe (HTTP, Port 80) und Namensauflösungen (UDP 53) einschränken.
- **Traffic-Limit**

  Um Denial-of-Service- (DoS-) und Brute-Force-Angriffe auf den Public Spot zu verhindern, können Sie den zulässige Datentransfer noch nicht authentisierter Public Spot-Teilnehmer auf ein ungefährliches Volumen begrenzen.
- **Sperren des Konfigurationszugangs**

  Sie können den Web-Zugriff auf die Gerätekonfiguration (z. B. Ihres Access Points, WLAN Controllers oder Routers) aus dem Public Spot-Netzwerk heraus sperren, so dass der Konfigurationszugang nur über andere festgelegte Management-Schnittstellen möglich ist.

Sicherheit für den Benutzer

Für den Benutzer eines Public Spots steht die Vertraulichkeit der übertragenen Daten im Vordergrund. Zudem wünscht er die Sicherung seiner Benutzerdaten gegen Missbrauch. Ihn schützen folgende Sicherungstechnologien:

- **Intra-Cell Blocking** (nur WLAN)

Unterbinden Sie in Ihrem Public Spot-Netzwerk die Kommunikation der WLAN-Clients untereinander. Diese Maßnahme erschwert – über die nutzerseitig evtl. ohnehin schon bestehenden Schutzmechanismen – den Zugriff auf die Ressourcen Ihrer Public Spot-Benutzer.

› **Verschlüsselung während der Anmeldephase**

Sofern Sie über ein digitales Zertifikat verfügen, können Sie dieses in Ihr Gerät laden, um über das verschlüsselte HTTPS-Verfahren Benutzernamen und Kennwörter sicher zu schützen. Das digitale Zertifikat sollte dabei von einer anerkannten öffentlichen Stelle signiert sein, damit ein Browser es als vertrauenswürdig einstuft und Ihren Nutzern keine Sicherheitswarnung ausgibt. Ohne ein Zertifikat erfolgt die Übertragung der Anmeldedaten unverschlüsselt.

Das Zertifikat sichert lediglich den Anmeldevorgang ab; innerhalb eines Public Spot-Netzwerks werden die Daten in der Regel unverschlüsselt übertragen. Dies gilt sowohl für Verbindungen über LAN als auch über WLAN. Sofern Ihre Nutzer also den normalen Datenverkehr absichern möchten, sind sie auf eigene Verschlüsselungsmechanismen angewiesen!

Ausgenommen davon sind WLAN-Verbindungen, die über Hotspot 2.0 erfolgen: Da der Hotspot-2.0-Standard auf WPA2 (802.1X/802.11i), EAP und 802.11u basiert, werden Datenpakete sowohl bei der Autorisierung als auch während der Sitzung stets verschlüsselt übertragen.

LANCOM empfiehlt dringend, sensitive Nutzdaten immer über verschlüsselte Verbindungen zu übertragen, z. B. durch IPSec-basierte VPN-Tunnel mit dem LANCOM Advanced VPN Client oder durch normale HTTPS-gesicherte Datenverbindungen. Außerdem sollte der Public Spot-Benutzer auf die Aktivierung einer Personal Firewall auf seinem Endgerät achten.

Assistent zur Einrichtung eines Public Spots

Der Setup-Assistent **Public Spot einrichten** unterstützt Sie bei der Einrichtung und ersten Konfiguration Ihres Public Spots. Mit seiner Hilfe gelingt es Ihnen, mit wenigen Klicks ein funktionsfähiges Public Spot-Netzwerk bereitzustellen. Der Assistent gruppiert dazu die dafür notwendigen Einstellungen (z. B. Zuweisen einer Schnittstelle, Vergeben eines IP-Bereichs, Festlegen von Zugangform und Anmeldungsverfahren, Protokollierung) und bietet Ihnen darüber hinaus die Option, einen Administrator mit beschränkten Rechten anzulegen, dem ausschließlich die Einrichtung und ggf. Verwaltung von Public Spot-Nutzern erlaubt ist.

Assistent zum Einrichten und Verwalten von Benutzern

Mit Hilfe des Setup-Wizards **Public-Spot-Benutzer einrichten** (Benutzer-Erstellungs-Assistent) erstellen Sie über WEBconfig zeitlich begrenzte Zugänge zu einem Public Spot-Netzwerk mit wenigen Mausklicks. Dabei bestimmen Sie im einfachsten Fall lediglich die Dauer des Zugangs; der Assistent vergibt Benutzername und Kennwort automatisch und speichert den Zugang in der Benutzerdatenbank des geräteinternen RADIUS-Servers. Der Anwender erhält abschließend ein ausdruckbares, personalisiertes Ticket (Voucher), mit dem er sich im Public Spot-Netzwerk ab sofort bis zur definierten Ablaufzeit anmelden kann.

Alternativ lassen sich Voucher auch auf Vorrat anlegen und ausdrucken, um z. B. in Stoßzeiten die Voucher-Ausgabe zu beschleunigen oder Mitarbeitern ohne Gerätezugriff die Voucher-Ausgabe zu ermöglichen. Hierzu geben Sie im Benutzer-Erstellungs-Assistenten an, dass die Nutzungsdauer erst ab dem ersten Login des Anwenders beginnt. Außerdem definieren Sie eine maximale Gültigkeitsdauer für den Zugang – nach dieser Zeit löscht der Public Spot den Zugang automatisch, auch wenn die Nutzungsdauer noch nicht abgelaufen ist.

Der Setup-Wizard **Public-Spot-Benutzer verwalten** (Benutzer-Verwaltungs-Assistent) stellt alle eingetragenen Public Spot-Zugänge auf einer eigenen Webseite in einer tabellarischen Übersicht dar. So haben Sie mit einem Klick die wichtigsten Daten Ihrer Nutzer im Blick und können auf komfortable Weise die Gültigkeit des Zugangs verlängern / verkürzen oder das betreffende Benutzerkonto komplett löschen. Zusätzlich lassen sich über den Assistenten Informationen zum Benutzerkonto abrufen, wie z. B. das vergebene Passwort im Klartext, der Authentifizierungsstatus, die IP-Adresse, die gesendeten / empfangenen Datenmengen oder etwaige Beschränkungen, die für das Benutzerkonto gelten.

Verwalten mehrere Administratoren die Public Spot-Zugänge, haben Sie die Möglichkeit, die Anzeige der angelegten Accounts auf den jeweiligen Administrator zu beschränken. Als Folge erscheinen in der tabellarischen Übersicht lediglich die angelegten Zugänge des gerade angemeldeten Administrators.

Diese Beschränkung zeigt keine Wirkung, falls ein Administrator-Zugang existiert, dessen kompletter Name Bestandteil der übrigen Administratoren-Accounts ist. "PSpot_Admin" sieht z. B. die Einträge von "PSpot_Admin1" und "PSpot_Admin2". "PSpot_Admin" fungiert in diesem Szenario als Super-Admin. Alle anderen Administratoren ("PSpot_AdminX") dagegen sehen die Einträge der anderen nicht.

1.2 Einrichtung und Betrieb

Dieses Kapitel enthält die wichtigsten Informationen zu Einrichtung und Betrieb eines Public Spots.

- **1. Schritt: Grundkonfiguration**

  Zunächst beschreiben wir die Grundkonfiguration. Nach Abschluss der Grundkonfiguration ist der Public Spot betriebsbereit und für einfaches Anwendungsszenario (Anmeldung über Voucher) vorkonfiguriert.

- **2. Schritt: Sicherheitseinstellungen**

  Dieses Kapitel geht explizit auf sicherheitsrelevanten Einstellungen ein, mit denen Sie Angriffe auf Ihr Public Spot-Netzwerk erschweren und den stabilen Betrieb verbessern. Sofern Sie die hier beschriebenen Einstellungen nicht bereits nicht im Rahmen anderer Einrichtungsschritte getätigt haben, sollten Sie den nachfolgenden Seiten erhöhte Aufmerksamkeit schenken.

- **3. Schritt: Erweiterte Funktionen und Einstellungen**

  Schließlich richtet sich der Blick auf zahlreiche erweiterte Funktionen und Einstellungsoptionen. In detaillierten Beschreibungen erfahren Sie, wie Sie Ihr Gerät individuell an Aufgabe und Umfeld anpassen. Außerdem lernen Sie, wie Sie sich während des Betriebes einen Überblick über Zustand und Aktivitäten des Public-Spots verschaffen.

Bitte beachten Sie, dass der Betrieb eines Public Spots (manchmal auch als "HotSpot" bezeichnet) in Ihrem Land rechtlichen Regulierungen unterliegen kann. Bitte informieren Sie sich vor der Einrichtung eines Public Spots über die jeweils geltenden Vorschriften. Informationen zu diesem Thema finden Sie auch im LANCOM Techpaper "Public Spot", erhältlich unter *www.lancom-systems.de*.

1.2.1 Grundkonfiguration

Die Anleitung der Grundkonfiguration ist in mehrere separate Abschnitte aufgeteilt:

- Der erste Abschnitt beschreibt die Einrichtung eines funktionsfähigen Public Spots am Beispiel eines Wireless Routers.

  Um einen Public Spot für ein einfaches Anwendungsszenario einzurichten, können Sie einen entsprechenden Assistenten starten, der Sie bei der Inbetriebnahme des Public Spots unterstützt.

- Der zweite Abschnitt beschreibt die Konfiguration der Standardwerte für die Benutzer-Assistenten, mit denen auch Mitarbeiter ohne allgemeine Administrator-Rechte neue Public Spot-Benutzer sehr komfortabel anlegen und verwalten können. Hierzu gehört auch das Anlegen eines beschränkten Zugangs, welcher Ihren Mitarbeitern lediglich den Zugriff auf diese Assistenten gewäht.
- Der dritte Abschnitt beschreibt die Benutzerverwaltung im lokalen RADIUS-Server, wahlweise über die Benutzer-Assistenten oder manuell über LANconfig.

Die Abschnitte bauen teilweise aufeinander auf, Sie sollten also idealerweise diese Informationen in der entsprechenden Reihenfolge bearbeiten.

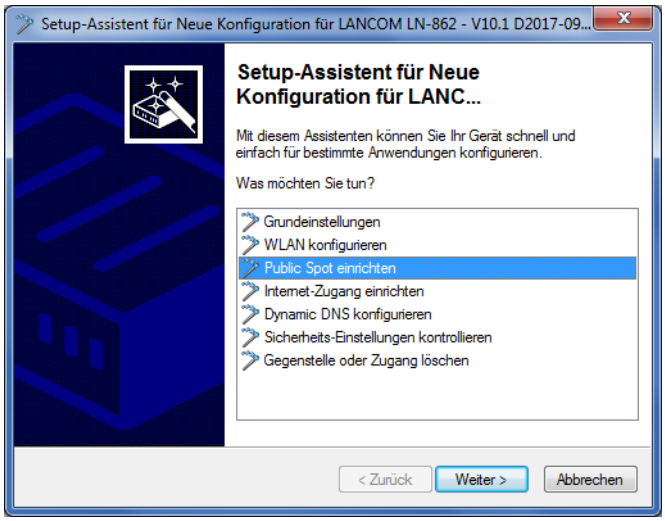
Basis-Installation eines Public Spots für einfache Szenarien

Installation über den Setup-Assistenten

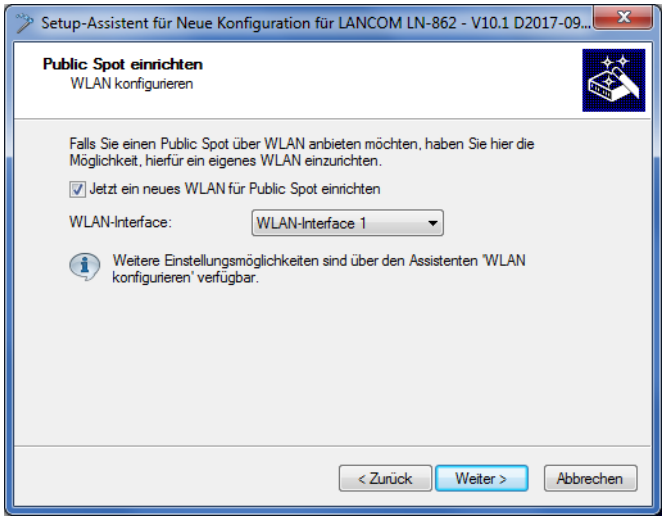
Der folgende Abschnitt beschreibt, wie Sie mit dem Einrichtungs-Assistenten die Basis-Installation eines Public Spots über LANconfig vornehmen.

Der Assistent für die Basis-Konfiguration des Public Spots zeigt je nach Gerätetyp und Verlauf verschiedene Dialoge. Dieses Tutorial stellt nur ein mögliches Beispiel dar.

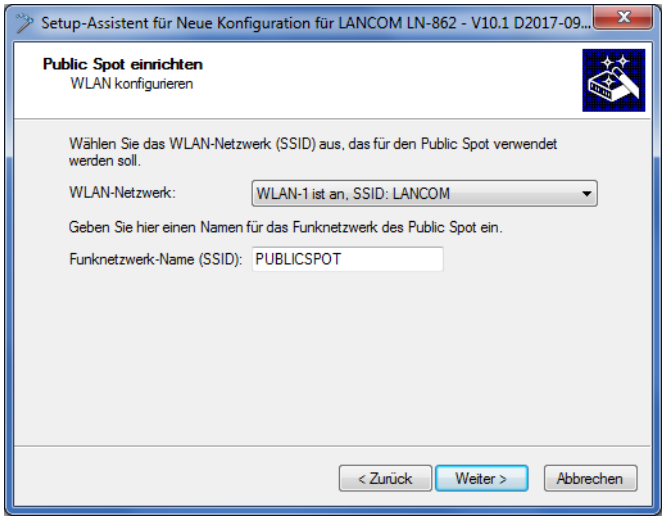
1. Starten Sie dazu LANconfig und markieren Sie das Gerät, für das Sie einen Public Spot einrichten wollen, z. B. einen Access Point.
2. Starten Sie den Setup-Assistenten über **Gerät** > **Setup Assistent**, wählen Sie die Aktion **Public Spot einrichten** und klicken Sie anschließend auf **Weiter**.



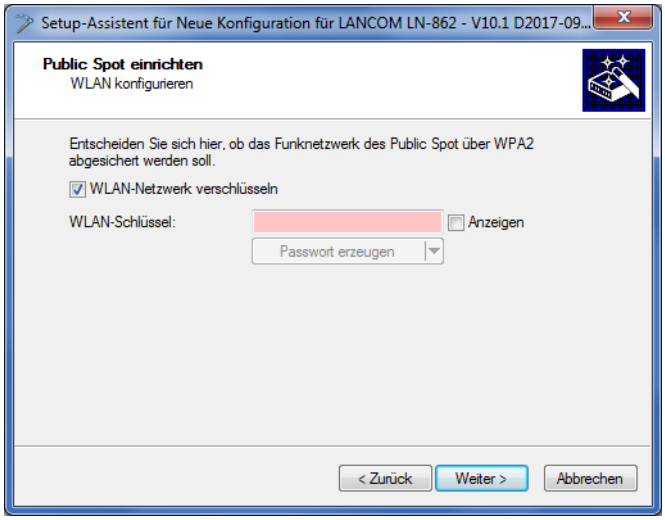
3. Falls Sie die Nutzung des Public Spots über WLAN einrichten möchten, aktivieren Sie die entsprechende Option und klicken Sie auf **Weiter**.



4. Wählen Sie aus dem Auswahlmenü die logische Schnittstelle aus, über die Sie den Public Spot anbieten wollen (z. B. WLAN-1), und geben Sie dem Funknetzwerk einen aussagekräftigen Namen (PUBLICSPOT). Klicken Sie auf **Weiter**.

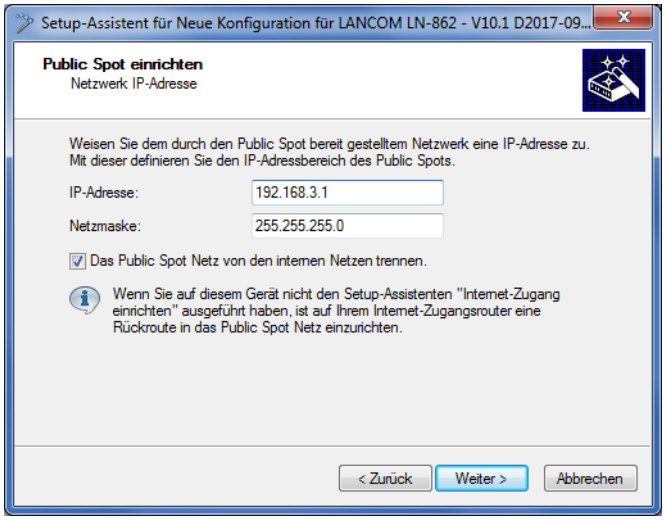


5. Legen Sie fest, ob das Funknetzwerk verschlüsselt werden soll. Geben Sie in diesem Fall einen WLAN-Schlüssel vor oder lassen Sie ihn automatisch generieren.



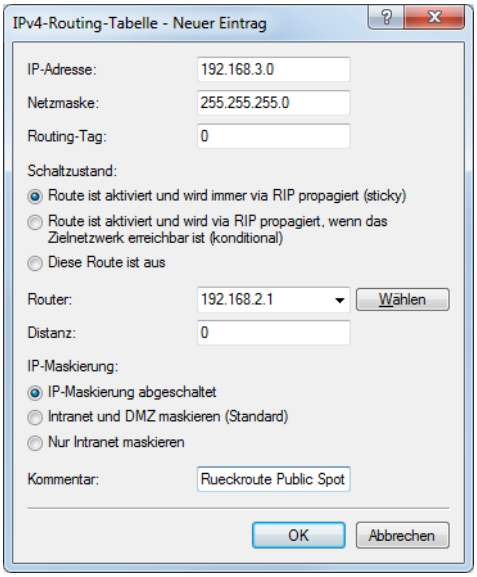
6. Weisen Sie dem Gerät die IP-Adresse und die Netzmaske zu, die Ihr Public Spot-Netzwerk spezifizieren soll, und klicken Sie auf **Weiter**.
   Das Public Spot-Modul enthält in Ihrem Netzwerk eine eigene IP-Adresse, die unabhängig von der Adresse ist, die Sie dem Gerät zugewiesen haben. Haben Sie z. B. ein 192.168.0.0/24-Netzwerk aufgespannt und Ihr Gerät besitzt darin die IP 192.168.2.1, können Sie dem Public Spot-Modul z. B. die IP `192.168.3.1` und die Subnetzmaske `255.255.255.0` vergeben, sofern diese IP nicht anderweitig belegt ist.

Wenn Sie das Public Spot-Netzwerk aus Sicherheitsgründen von den internen Netzwerken trennen möchten, achten Sie darauf, dass die entsprechende Option aktiviert ist.



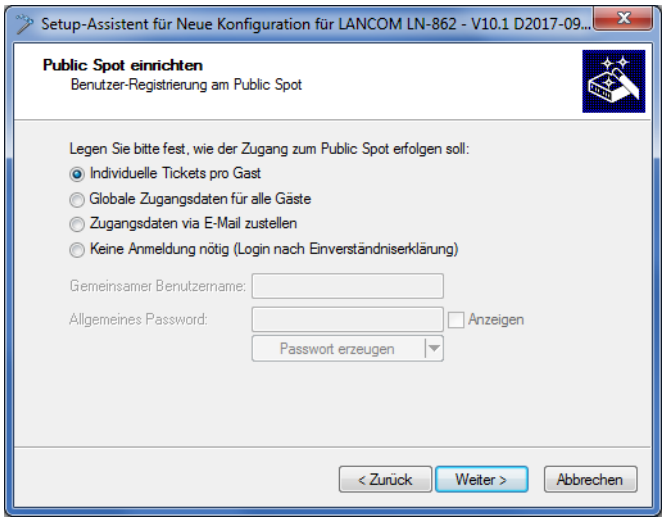
Sofern Ihr Gerät nicht direkt mit dem Internet verbunden ist und Sie für Ihr Public Spot-Netzwerk einen anderen Adresskreis aufgespannt haben, **müssen** Sie in Ihrem Internet-Gateway eine Rückroute in das Public Spot-Netzwerk einrichten. Ohne Rückroute erhalten Public Spot-Nutzer bei der Weiterleitung einen HTTP-Fehler, nachdem sie am Public Spot erfolgreich authentifiziert wurden.

Wie Sie eine Rückroute einrichten, entnehmen Sie bitte der Dokumentation Ihres Internet-Gateways. In LANconfig konfigurieren Sie diese unter **IP-Router** > **Routing** > **IPv4-Routing-Tabelle**. Legen Sie dazu einen neuen Eintrag an und tragen Sie unter **IP-Adresse** die Netzadresse Ihres Public Spot-Netzes ein sowie unter **Router** die Adresse, die der Public Spot in Ihrem lokalen Netz besitzt.

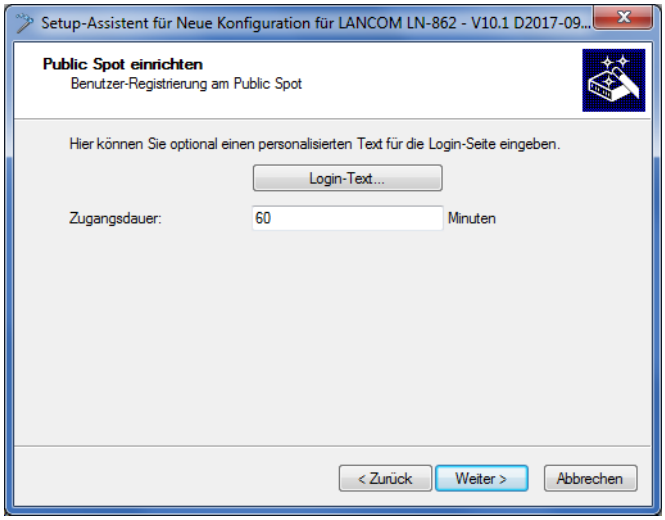


7. Legen Sie fest, mit welchen Zugangsdaten sich Ihre Benutzer am Public Spot anmelden. Außerdem können Sie die Anmeldeseite optional mit einem Login-Text personalisieren. Klicken Sie anschließend auf **Weiter**.

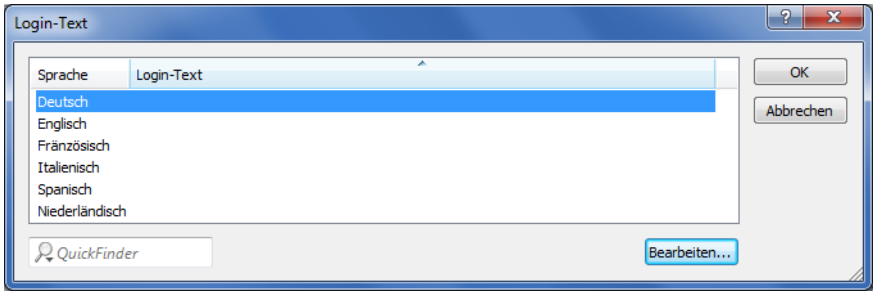
Sie können jedem Benutzer entweder eigene Zugangsdaten aushändigen oder ein allgemeines Konto einrichten, das sämtliche Benutzer für den Zugang zum Public Spot verwenden. Sofern Sie später Voucher ausgeben und feste Benutzerkonten einrichten möchten, wählen Sie die Option **Individuelle Tickets pro Gast**.

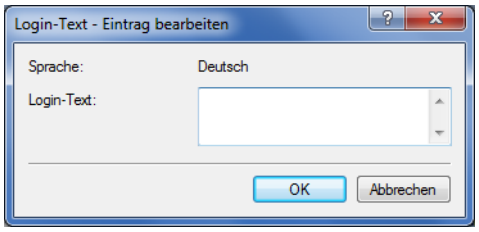


8. Wählen Sie hier optional einen Login-Text, legen Sie die Zugangsdauer fest und klicken Sie **Weiter**.



Login-Text (optional):



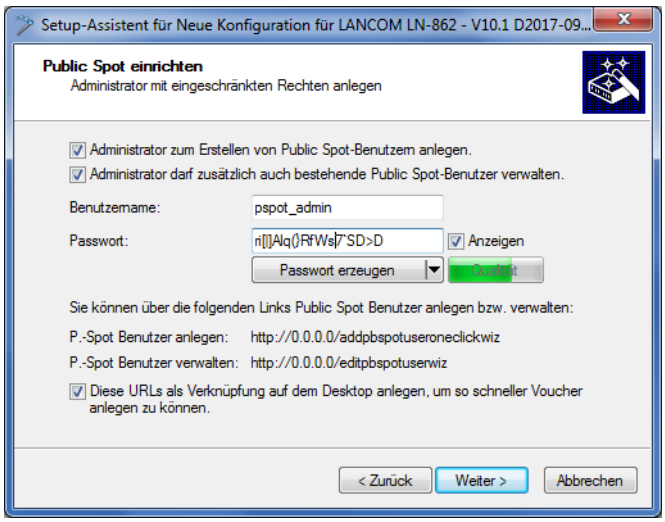


Der Login-Text ist ein individueller Text in HTML-Schreibweise in, welcher auf der Anmeldeseite innerhalb der Box des Anmeldeformulars eingeblendet wird. Sie können diesen Text auch zu einem späteren Zeitpunkt manuell hinzufügen oder ändern (siehe dazu das Kapitel *Individueller Text oder Login-Titel auf der Anmeldeseite* auf Seite 104).

9. Erstellen Sie ggf. einen Administrator mit beschränkten Rechten, der über die Setup-Wizards in WEBconfig Public Spot-Nutzer erstellen und verwalten darf. Klicken Sie anschließend auf **Weiter**.
Ein solcher Administrator ist z. B. dann sinnvoll, wenn Sie Ihren Mitarbeitern eine Möglichkeit an die Hand geben wollen, selbstständig Benutzerkonten zu administrieren, ohne, dass ein Geräte-Administrator in den Prozess eingebunden werden muss. Die die Erstellungsrechte aktivieren im WEBconfig den Benutzer-Erstellungs-Assistenten; die Verwaltungsrechte den Benutzer-Verwaltungs-Assistenten.

   Über den Benutzer-Erstellungs-Assistenten **Public-Spot-Benutzer einrichten** hat ein Administrator die Möglichkeit, zeitliche befristete Benutzerkonten für Public Spot-Benutzer zu erstellen und die dazugehörigen Zugangsdaten auf einem Voucher auszudrucken.

   Über den Benutzer-Verwaltungs-Assistenten **Public-Spot-Benutzer verwalten** hat ein Administrator die Möglichkeit, diese Nutzer zu admistrieren. Dabei kann er die Gültigkeit des Zugangs verlängern oder verkürzen, oder das betreffende Nutzerkonto komplett löschen. Zusätzlich kann er über den Assistenten Informationen zum Benutzerkonto abrufen, wie z. B. das vergebene Passwort im Klartext, den Authentifizierungsstatus, die IP-Adresse, die gesendeten/empfangenen Datenmengen oder etwaige Beschränkungen, die für das Konto gelten.

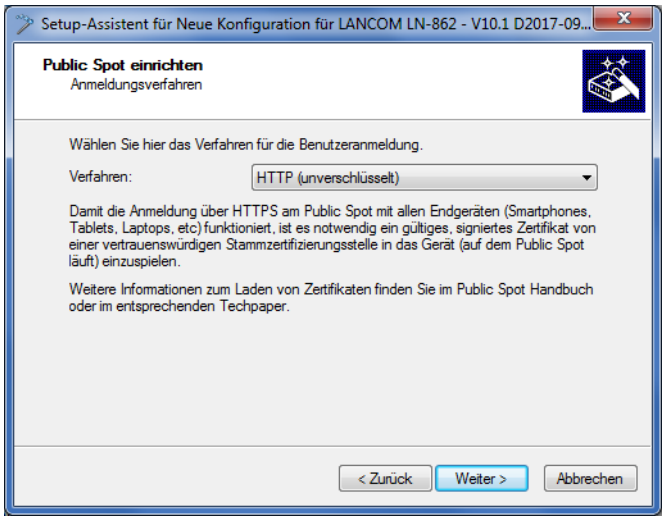


Achten Sie bei der Vergabe eines Passwortes darauf, dass es sicher ist. Der Setup-Assistent prüft während der Eingabe die Qualität des Passwortes. Bei unsicheren Passworten erscheint das Eingabefeld rot, bei erhöhter Sicherheit wechselt es zu gelb, und bei sehr sicheren Passworten erhält es einen grünen Hintergrund.

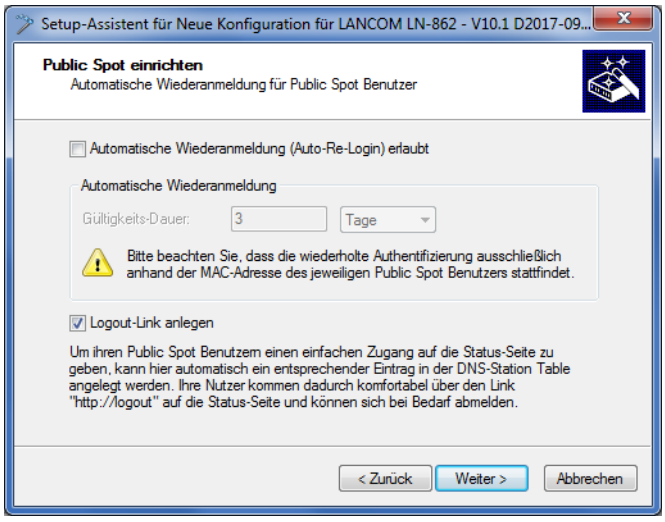
10. Wählen Sie das Verfahren für die Benutzer-Anmeldung. Klicken Sie anschließend auf **Weiter**.

    Sie können in der Drop-Down-Liste zwischen **HTTP** und **HTTPS** wählen, wobei Sie mit einer Verbindung über HTTPS die Sicherheit der Anmeldedaten der Public Spot-Benutzer gewährleisten.

Für die Verwendung von HTTPS sollte anschließend noch ein passendes Server-Zertifikat eingespielt werden. Ansonsten wird dem Benutzer bei der Anmeldung das geräteeigene Zertifikat präsentiert, was im Browser zu einer Zertifikatswarnung führt.

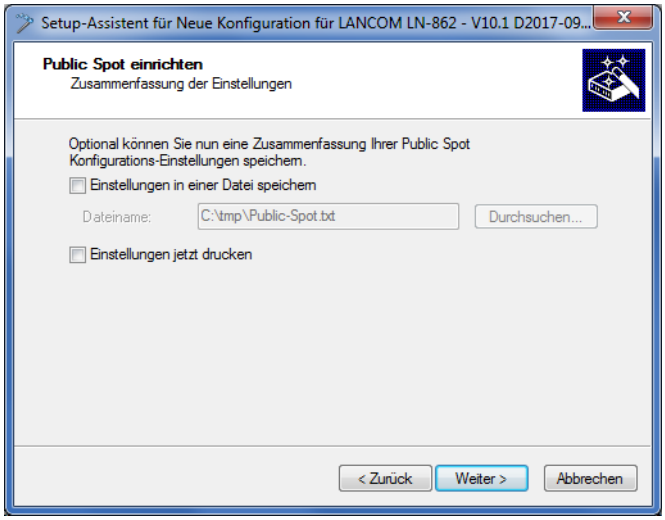


11. Legen Sie fest, ob für sämtliche Public Spot-Nutzer eine automatische Wiederanmeldung erlaubt ist und welche welche maximale Abwesenheit dafür zulässig ist, bevor sich der Nutzer erneut über die Public Spot-Webseite anmelden muss. Klicken Sie anschließend auf **Weiter**.
    Die **Automatische Wiederanmeldung** ist eine Komfort-Option, bei welcher der Public Spot ihm bekannte Nutzer bzw. Geräte automatisch authentifiziert. Da die Erkennung bekannter Geräte jedoch ausschließlich über die MAC-Adresse des Netzwerkadapters erfolgt, welche sich fälschen lässt, stellt dieser Anmeldungsweg ein potentielles Sicherheitsrisiko dar und ist deshalb standardmäßig deaktiviert.



12. Speichern Sie bei Bedarf die vorgenommenen Einstellungen.

Bevor Sie die Konfiguration auf Ihr Gerät übertragen, haben Sie die Möglichkeit, die Einstellungen lokal auf Ihrem PC zu sichern oder eine Zusammenfassung auszudrucken.



13. Klicken Sie abschließend auf **Weiter** und **Fertig stellen**, um die Basis-Installation des Public Spots abzuschließen. Der Setup-Assistent sendet die Einstellungen daraufhin an das Gerät.

Fertig! Damit haben Sie Ihr Public Spot-Modul konfiguriert. Wenn Sie sich nun mit einem WLAN-fähigen Gerät in Reichweite des Public Spots begeben, kann das Gerät die eingerichtete SSID als öffentliches Netzwerk finden und sich an diesem anmelden.

Manuelle Installation

Die nachfolgenden Konfigurationsschritte zeigen Ihnen, wie Sie manuell einen Public Spot für einfache Einsatzszenarien einrichten. Bei dem geschilderten Einsatzszenario aktivieren Sie Public Spot auf einem Interface, über das kein anderer Datenverkehr außer dem des Public Spots läuft; sich z. B. Public Spot- und normale WLAN-Benutzer kein gemeinsames Netzwerk teilen (dedizierte SSID).

Dieses Tutorial stellt nur ein mögliches Beispiel dar. Je nach Geräteart (Access Point, WLAN-Controller, etc.) oder Komplexität der Netzwerkkonfiguration (z. B. Einsatz von VLAN oder ARF) sind abweichende oder zusätzliche Schritte für die Einrichtung eines Public Spots erforderlich! Da derartige Netzwerkkonfigurationen jedoch sehr individuell sind, konzentriert sich das Tutorial bewusst auf ein einfaches Beispiel, damit Sie die notwendigen Schritte bei Bedarf adaptieren können.

1. Starten Sie dazu LANconfig und markieren Sie das Gerät, für das Sie einen Public Spot einrichten wollen, z. B. einen Access Point. Öffnen Sie anschließend den Konfigurationsdialog für das Gerät.
2. Überprüfen Sie die korrekte Uhrzeit.

   Für die Prüfung der Zertifikate und die korrekte Erfassung und Abrechnung der Sitzungsdaten ist die möglichst exakte Uhrzeit im Public Spot wichtig. Bestimmen Sie zunächst Einstellungen wie Zeitzone und Zeitumstellungen (Sommer- und Normalzeit):

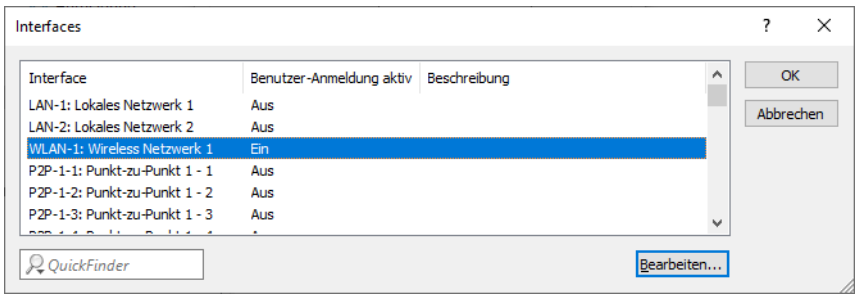
   › LANconfig: **Datum/Zeit** > **Allgemein**

   Damit die Uhrzeit des Public Spots auch später jederzeit korrekt eingestellt bleibt, sollten Sie das Gerät als NTP-Client einrichten. Den dafür notwendigen Zeit-Server tragen Sie unter **Datum/Zeit** > **Synchronisierung** > **Zeit-Server** ein. Öffnen Sie dazu den Hinzufügen-Dialog, um sich eine Liste möglicher Server-Adressen anzeigen zu lassen.
3. Wählen Sie die Schnittstellen für den Public Spot-Betrieb.

   Mit der Auswahl einer Schnittstelle legen Sie fest, auf welchen Schnittstellen die Benutzer-Anmeldung aktiviert wird. Zur Auswahl stehen neben den logischen WLAN-Interfaces, über die sich Public Spot-Benutzer direkt anmelden

können, auch die logischen LAN-Interfaces (LAN-1 etc.) und die Point-to-Point-Strecken (P2P-1 etc.). Über LAN- und P2P-Interfaces können Sie weitere Access-Points in den Public Spot eines anderen Gerätes einbeziehen. Wählen Sie für einen singulären Access-Point hingegen z. B. das logische WLAN-Interface **WLAN-1**.

› LANconfig: **Public-Spot** > **Server** > **Betriebseinstellungen** > **Interfaces**

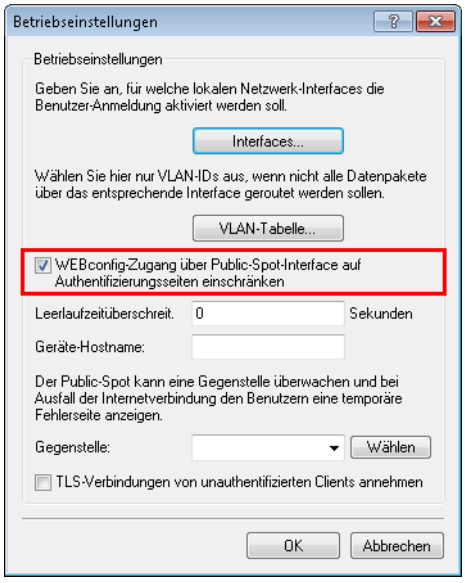


Mit der Aktivierung der Authentifizierung für eine WLAN-Schnittstelle geben Sie automatisch die zugehörige SSID für die Public Spot-Nutzung frei.

Auf einem WLC können Sie bestimmte Ethernet-Interfaces für den Public Spot aktivieren. Dabei können Sie auch eine gezielte Einschränkung auf bestimmte VLANs festlegen.

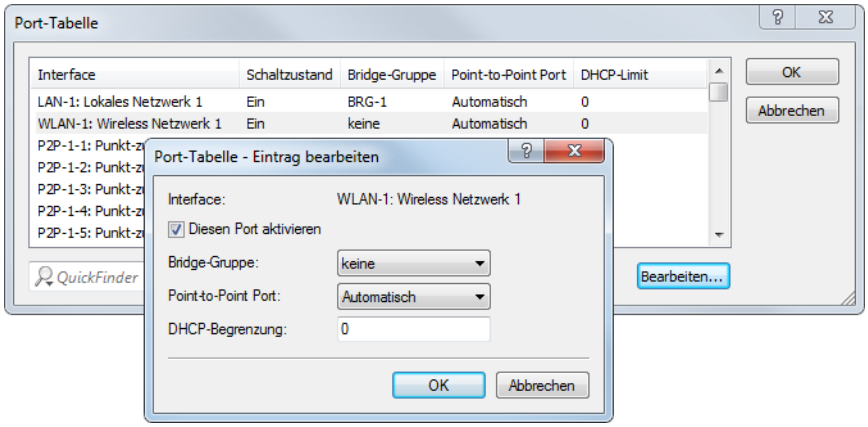
4. Beschränken Sie den Zugriff auf Ihr Gerät aus dem Public Spot-Netzwerk heraus ausschließlich auf die Authentifizierungsseiten.
   Wenn Sie den Zugriff nicht einschränken, sind Public Spot-Nutzer dazu in der Lage, auf die Konfigurationsoberfläche Ihres Gerätes (WEBconfig) zuzugreifen. Aus Sicherheitsgründen sollten Sie diese Möglichkeit jedoch ausschließen.

   › LANconfig: **Public-Spot** > **Server** > **Betriebseinstellungen** > **WEBconfig-Zugang über Public Spot-Interface auf Authentifizierungsseiten einschränken**



5. Trennen Sie die Schnittstelle, über die Sie den Public Spot-Betrieb anbieten wollen, vom übrigen Netzwerkverkehr. Damit Endgeräte über unterschiedliche Interfaces bzw. Schnittstellen eines Public Spot-Gerätes (z. B. zwischen LAN-1 und WLAN-1) miteinander kommunizieren können, sind diese Schnittstellen in Ihrem Gerät logisch miteinander verknüpft (gebridged). In einem Public Spot-Szenario ist solch ein Bridging aus Sicherheitsgründen aber oft nicht erwünscht. Um die Kommunikation zwischen der einem Public Spot zugewiesenen Schnittstelle (z. B. WLAN-1) und dem übrigen Netzwerk zu trennen, müssen Sie das Bridging aufheben. Setzen Sie dazu in der **Port-Tabelle** die **Bridge-Gruppe** für das betreffende Interface auf `keine`.

› LANconfig: **Schnittstellen** > **LAN** > **Port-Tabelle**

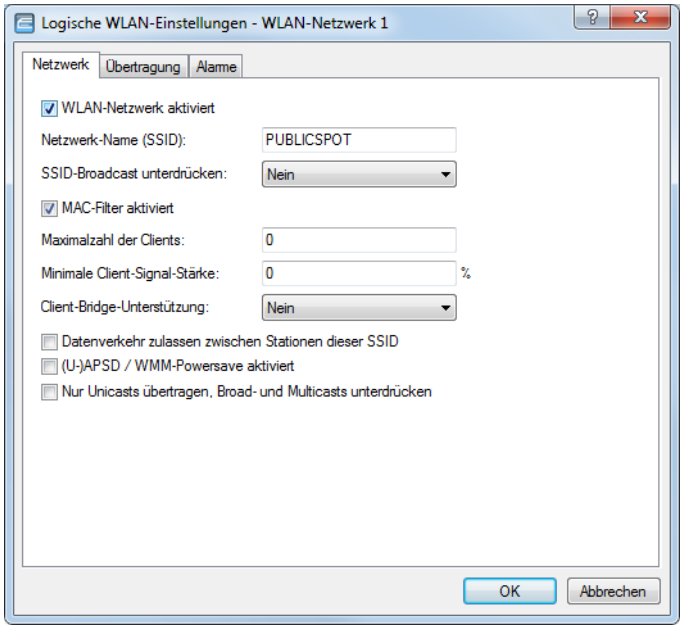


6. Aktivieren Sie WLAN für den Public Spot.

   Diese Einstellung betrifft nicht: Router, WLAN Controller, Central Site Gateways.

   Aktivieren Sie das logische WLAN, welches Sie zuvor für die Public Spot-Anmeldung freigegeben haben, und geben Sie diesem Netzwerk einen aussagekräftigen Namen (SSID).

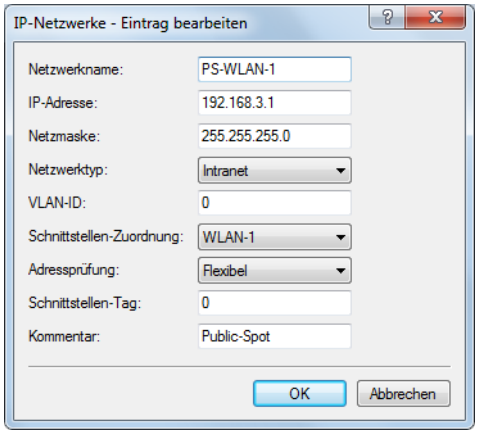
   › LANconfig: **Wireless-LAN** > **Allgemein** > **Logische WLAN-Einstellungen** > **WLAN-Netzwerk <Nummer>** > **Netzwerk**



Sofern Sie kein privates WLAN einrichten, sollten Sie aus Sicherheitsgründen die Einstellung **Datenverkehr zulassen zwischen Stationen dieser SSID** deaktivieren. Dadurch unterbinden Sie die Kommunikation der einzelnen Public Spot-Benutzer untereinander.

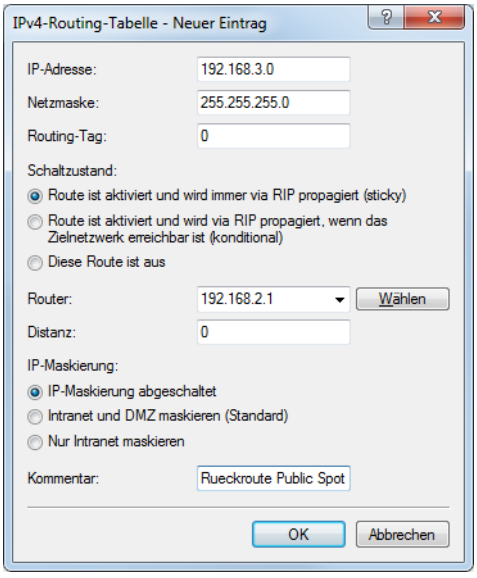
7. Weisen Sie dem Gerät die IP-Adresse und die Netzmaske zu, die Ihr Public Spot-Netzwerk spezifizieren soll.
   Das Public Spot-Modul enthält in Ihrem Netzwerk eine eigene IP-Adresse, die unabhängig von der Adresse ist, die Sie dem Gerät zugewiesen haben. Haben Sie z. B. ein 192.168.0.0/24-Netzwerk aufgespannt und Ihr Gerät besitzt darin die IP 192.168.2.1, können Sie dem Public Spot-Modul z. B. die IP `192.168.3.1` und die Subnetzmaske `255.255.255.0` vergeben, sofern diese IP nicht anderweitig belegt ist. Unter **Schnittstellen-Zuordnung** selektieren Sie die gewählte Schnittstelle, z. B. `WLAN-1`.

› LANconfig: **IPv4** > **Allgemein** > **IP-Netzwerke**



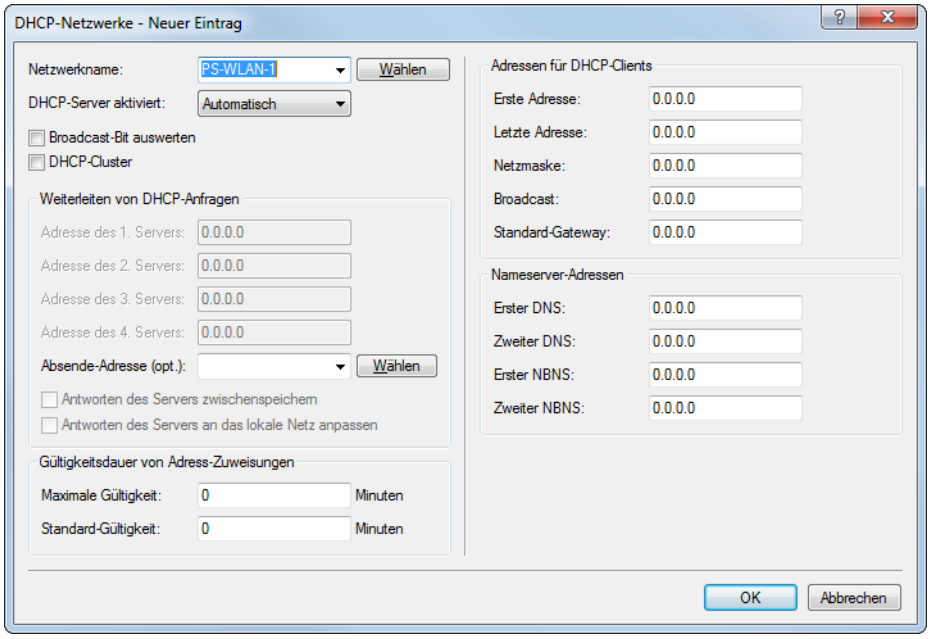
Sofern Ihr Gerät nicht direkt mit dem Internet verbunden ist und Sie für Ihr Public Spot-Netzwerk einen anderen Adresskreis aufgespannt haben, **müssen** Sie in Ihrem Internet-Gateway eine Rückroute in das Public Spot-Netzwerk einrichten. Ohne Rückroute erhalten Public Spot-Nutzer bei der Weiterleitung einen HTTP-Fehler, nachdem sie am Public Spot erfolgreich authentifiziert wurden.

Wie Sie eine Rückroute einrichten, entnehmen Sie bitte der Dokumentation Ihres Internet-Gateways. In LANconfig konfigurieren Sie diese unter **IP-Router** > **Routing** > **IPv4-Routing-Tabelle**. Legen Sie dazu einen neuen Eintrag an und tragen Sie unter **IP-Adresse** die Netzadresse Ihres Public Spot-Netzes ein sowie unter **Router** die Adresse, die der Public Spot in Ihrem lokalen Netz besitzt.



8. Konfigurieren Sie die DHCP-Server-Einstellungen für das Public Spot-Netzwerk.
Da das Gerät ein IP-Netzwerk unabhängig von dem Netzwerk aufspannt, in dem es sich befindet, müssen Sie für dieses Netzwerk einen DHCP-Server konfigurieren. Setzen Sie dazu für das zuvor eingerichtete IP-Netzwerk (z. B. `PS-WLAN-1`) den Wert für **DHCP-Server aktiviert** auf `Ja`.

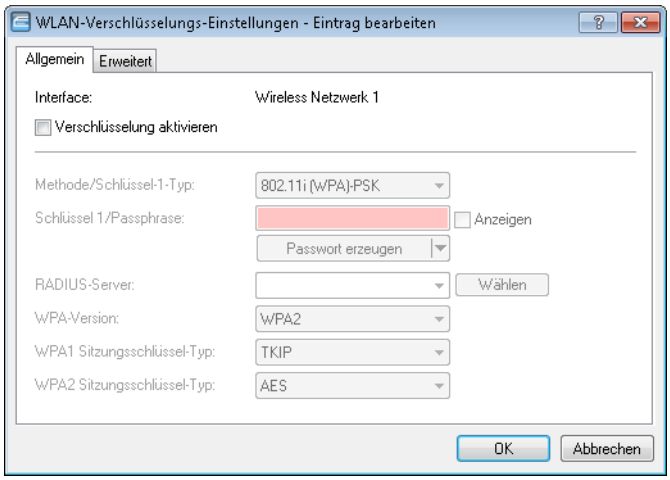
› LANconfig: **IPv4** > **DHCPv4** > **DHCP-Netzwerke**



9. Deaktivieren Sie die Verschlüsselung für das Interface, über das Sie den Public Spot anbieten.

Diese Einstellung betrifft nicht: Router, WLAN Controller, Central Site Gateways.

Standardmäßig ist für alle logischen WLANs eine Verschlüsselung aktiviert. In Public Spot-Anwendungen werden die Nutzdaten zwischen den WLAN-Clients und dem Access Point üblicherweise unverschlüsselt übertragen. Deaktivieren Sie daher unter **Wireless-LAN** > **Verschlüsselung** > **WLAN-Verschlüsselungs-Einstellungen** die Verschlüsselung für das logische WLAN, welches Sie zuvor für die Public Spot-Anmeldung freigegeben haben.

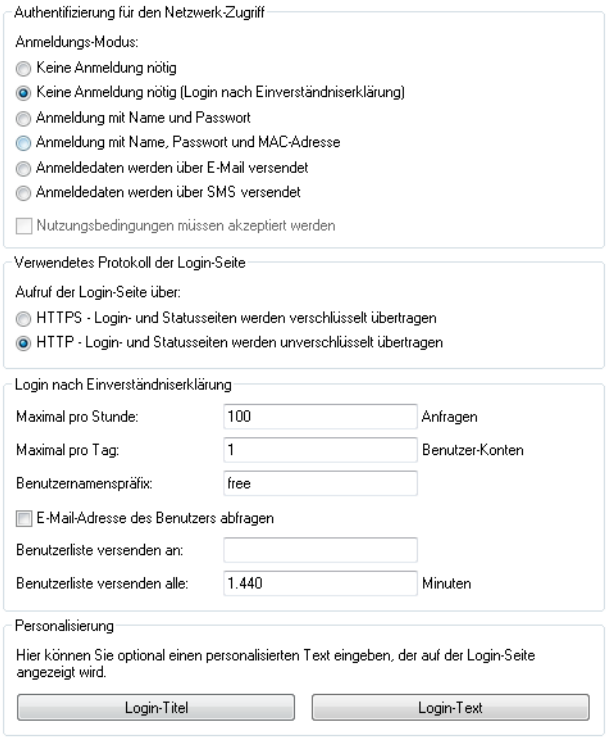


10. Wählen Sie den Anmeldungs-Modus und das verwendete Protokoll für die Benutzeranmeldung aus.

Über den Anmeldungs-Modus legen Sie fest, mit welchen Informationen sich die Benutzer des Public Spot-WLANs anmelden können. Wählen Sie **Anmeldung mit Name und Passwort**, um Ihren Nutzern z. B. die Anmeldung mit einem individuellen Benutzernamen und einem Passwort zu ermöglichen, das Sie diesen vorab zuweisen. Zusätzlich erlaubt Ihnen dieses Einstellung, über sogenannte Voucher (Tickets) kurzfristig Hotspot-Zugänge für Gäste bereitzustellen.

Verwenden Sie als Protokoll **HTTPS**, damit die Zugangsdaten Ihrer Nutzer bei der Anmeldung verschlüsselt übertragen werden.

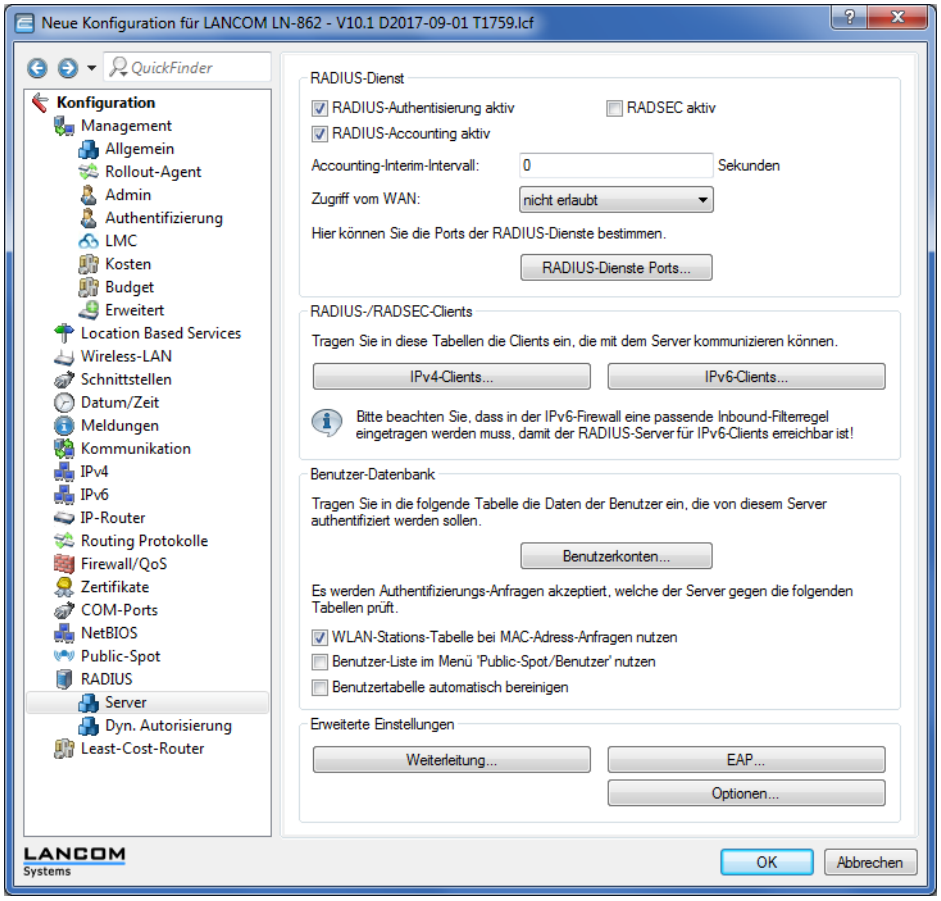
› LANconfig: **Public-Spot** > **Anmeldung** > **Anmeldungs-Modus**



Beachten Sie, dass – wenn Sie die Einstellungen **Keine Anmeldung nötig** wählen –, auch Unbefugte ungehinderten Zugriff auf Ihren Public Spot haben können!

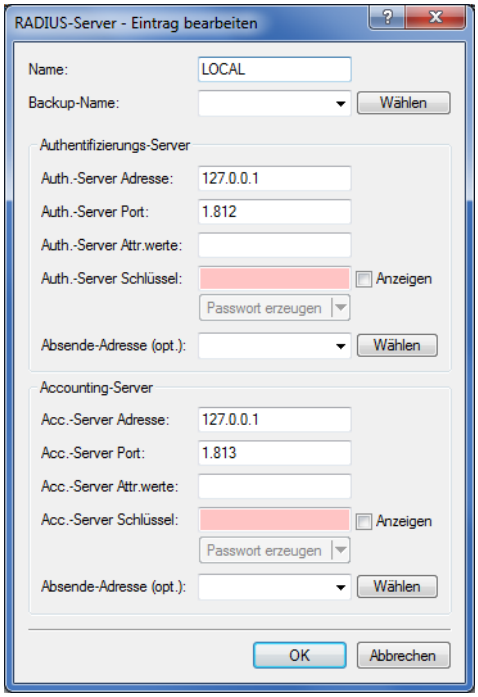
11. Schalten Sie den internen RADIUS-Server für die Benutzerverwaltung und das Accounting ein. Public-Spot-Zugänge speichern Sie in der Benutzer-Datenbank des geräteinternen RADIUS-Servers.

› LANconfig: **RADIUS** > **Server** > **Benutzer-Datenbank**



12. Standardmäßig ist der Public Spot bereits für die Benutzung des internen RADIUS-Servers vorkonfiguriert. Der Listeneintrag ist notwendig, damit der Public Spot die Adresse des RADIUS-Servers kennt und er die Public Spot-Zugänge am internen RADIUS-Server authentifizieren kann.

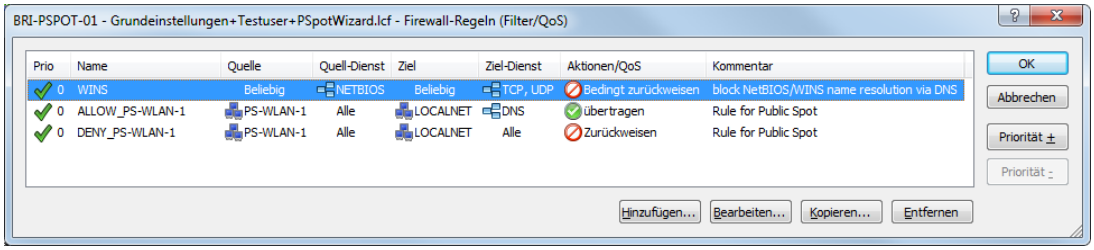
› LANconfig: **Public-Spot** > **Benutzer** > **Benutzer und RADIUS-Server** > **RADIUS-Server**

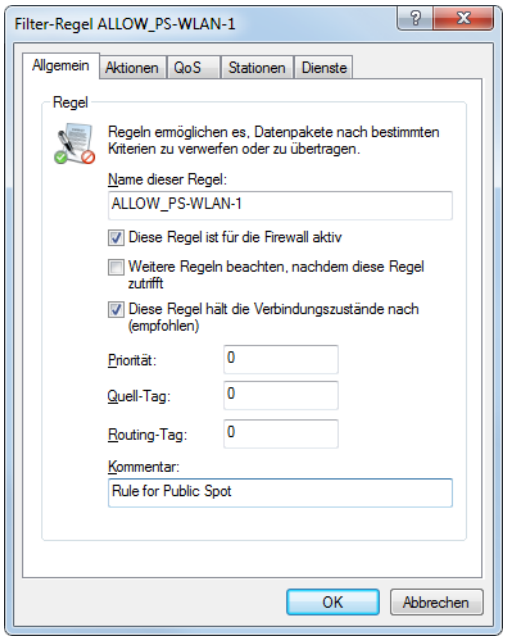


13. Richten Sie zur Absichererung Ihrer lokalen Netzwerke Filterregeln für den Public Spot in der Firewall ein. Erstellen dazu jeweils eine Erlaubnisregel (z. B. `ALLOW_PS-WLAN-1`) und eine Verbotsregel (z. B. `DENY_PS-WLAN-1`).

Über die Erlaubnisregel gestatten Sie Geräten aus dem Public Spot-Netzwerk explizit, DNS-Anfragen in alle lokalen Netzwerke – z. B. Ihr lokales Intranet – zu senden. Über die Verbotsregel hingegen schließen Sie alle übrigen Zugriffe bzw. Anfragen aus dem Public Spot-Netz in Ihre lokalen Netzwerke generell aus. Die Reihenfolge – Erlaubnis vor Verbot – ist dabei essentiell, da die Firewall Regeln nach Priorität von oben nach unten anwendet.

› LANconfig: **Firewall/QoS** > **IPv4-Regeln** > **Regeln…**





› **Einstellungen für die Erlaubnisregel:**

a) Tragen Sie unter **Allgemein** den Namen der Regel ein, z. B. `ALLOW_PS-WLAN-1`.

b) Entfernen Sie alle eventuell voreingestellten Aktions-Objekte aus der Liste und fügen Sie über **Aktionen** > **Hinzufügen…** ein Aktions-Objekt vom Typ **ACCEPT** hinzu.

c) Aktivieren Sie unter **Stationen** > **Verbindungs-Quelle** die Option **Verbindungen von folgenden Stationen** und wählen Sie **Hinzufügen…** > **Benutzerdefinierte Station hinzufügen**.

d) Wählen Sie im sich öffnenden Stations-Dialog die Option **Alle Stationen im lokalen Netzwerk** und wählen Sie unter **Netzwerk-Name** den Namen Ihres Public Spot-IP-Netzwerks, z. B. `PS-WLAN-1`. Schließen Sie den Stations-Dialog mit **OK**.

e) Aktivieren Sie unter **Stationen** > **Verbindungs-Ziel** die Option **Verbindungen an folgende Stationen** und wählen Sie **Hinzufügen…** den Eintrag **LOCALNET**.

f) Aktivieren Sie unter **Dienste** > **Protokolle/Ziel-Dienste** die Option **folgende Protokolle/Ziel-Dienste** und wählen Sie **Hinzufügen…** > **DNS**.

g) Beenden Sie den Filter-Regel-Dialog mit einem abschließenden Klick auf **OK**.
LANconfig trägt die Erlaubnisregel daraufhin in die Regel-Tabelle ein.

› **Einstellungen für die Verbotsregel:**

a) Tragen Sie unter **Allgemein** den Namen der Regel ein, z. B. `DENY_PS-WLAN-1`.

b) Entfernen Sie alle eventuell voreingestellten Aktions-Objekte aus der Liste und fügen Sie über **Aktionen** > **Hinzufügen…** ein Aktions-Objekt vom Typ **REJECT** hinzu.

c) Aktivieren Sie unter **Stationen** > **Verbindungs-Quelle** die Option **Verbindungen von folgenden Stationen** und wählen Sie **Hinzufügen…** > **Benutzerdefinierte Station hinzufügen**.

d) Wählen Sie im sich öffnenden Stations-Dialog die Option **Alle Stationen im lokalen Netzwerk** und wählen Sie unter **Netzwerk-Name** den Namen Ihres Public Spot-IP-Netzwerks, z. B. `PS-WLAN-1`. Schließen Sie den Stations-Dialog mit **OK**.

e) Aktivieren Sie unter **Stationen** > **Verbindungs-Ziel** die Option **Verbindungen an folgende Stationen** und wählen Sie **Hinzufügen…** den Eintrag **LOCALNET**.

f) Beenden Sie den Filter-Regel-Dialog mit einem abschließenden Klick auf **OK**.
LANconfig trägt die Verbotsregel daraufhin in die Regel-Tabelle ein.

14. Speichern Sie die Konfiguation auf Ihrem Gerät.

Fertig! Damit haben Sie Ihr Public Spot-Modul konfiguriert. Wenn Sie sich nun mit einem WLAN-fähigen Gerät in Reichweite des Public Spots begeben, kann das Gerät die eingerichtete SSID als öffentliches Netzwerk finden und sich an diesem anmelden.

Standardwerte für den Public Spot-Assistenten setzen

Der nachfolgende Abschnitt beschreibt, wie Sie die Standardwerte für den **Benutzer-Erstellungs-Assistenten** (Setup-Wizard **Public-Spot-Benutzer einrichten**) an Ihre Bedürfnisse anpassen. Die hier definierten Werte stehen einem Public Spot-Administrator beim Einrichten neuer Benutzer und Voucher-Druck anschließend als Auswahlwerte zur Verfügung (Laufzeiten, Bandbreitenprofile, etc.).

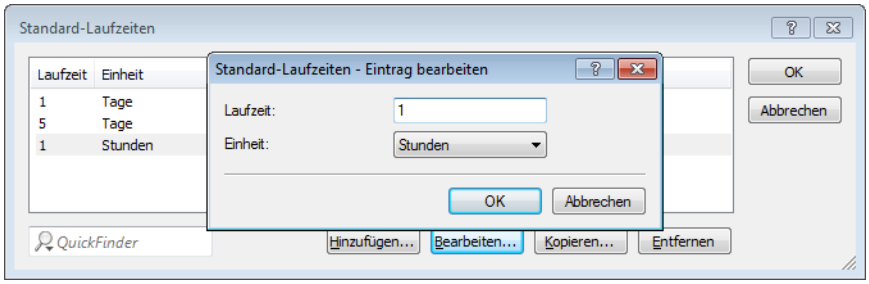
Ausgenommen davon sind die im untenstehenden Dialog abgebildeten Werte für Muster für Benutzernamen und Passwort-Länge, welche ausschließlich dem Gerät als Vorgabewerte dienen.

1. Starten Sie LANconfig und öffnen Sie den Konfigurationsdialog für das Gerät.

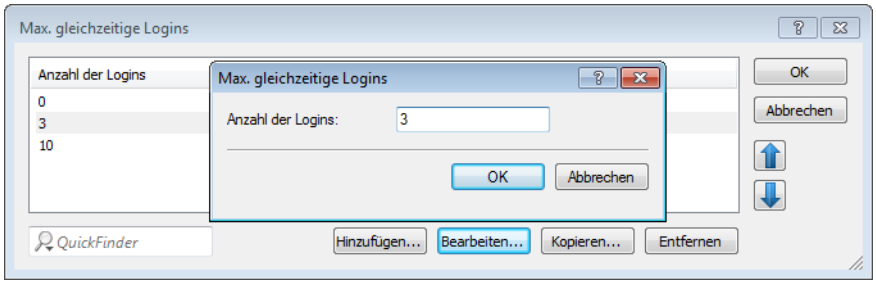
2. Wechseln Sie in die Ansicht **Public-Spot** > **Assistent**.

3. Definieren Sie unter **Standard-Laufzeiten**, welche auswählbaren Gültigkeiten von Benutzerkonten und Vouchern der Assistent standardmäßig anbietet.

Der Benutzer-Erstellungs-Assistent verwendet die kürzeste Laufzeit als Standardwert.



4. Definieren Sie unter **Max. gleichzeitige Logins** die für den jeweiligen Benutzer zutreffende Anzal von Geräten, die maximal gleichzeitig auf das Benutzerkonto zugreifen dürfen.
   Der Wert `0` steht dabei für 'Unbegrenzt'. Ob die mehrfache Anmeldung mit einem oder mehreren Geräten generell erlaubt ist, gibt der Public Spot-Administrator später beim Anlegen eines neues Benutzers über eine gesonderte Einstellung im Assistenten an.

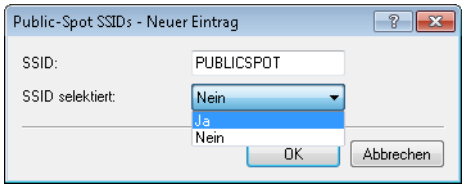


5. Legen Sie unter **Muster für Benutzernamen** fest, nach welchem Muster der Benutzer-Erstellungs-Assistent den Benutzernamen erzeugt.
   Sie können bis zu 19 Zeichen vergeben, wobei der Assistent für die Variable "`%n`" für jeden Benutzer eine eindeutige Nummer vergibt. Für die Standardbezeichnung `user%n` erscheint auf dem Voucher später z. B. `user12345`.

6. Bestimmen Sie unter **Passwort-Länge** die Länge des Passwortes, das der Benutzer-Erstellungs-Assistent für den Public Spot-Zugang generiert.
   Standardmäßig beträgt die Länge 6 Zeichen. Wenn Sie längere Passwörter vergeben möchten, sollten Sie bedenken, dass dem Gast bei deren Eingabe Fehler passieren können, was zu unnötigen Problemen und Rückfragen führt.

7. Optional: Legen Sie unter **Bandbreitenprofile** Grenzen für den Up- und Downlink eines jeden Public Spot-Benutzers fest.
   Mehr zu dieser Einstellung erfahren Sie unter *Bandbreitenprofile verwalten* auf Seite 50.

8. Nur Public Spot über WLAN: Bestimmen Sie unter **Public-Spot SSIDs** die Namen der Public Spot-Netzwerke, für die Sie mit dem Benutzer-Erstellungs-Assistent Benutzerkonten standardmäßig anlegen.



Der Benutzer-Erstellungs-Assistent markiert die als **SSID selektiert** festgelegten Netzwerknamen bei der Einrichtung neuer Public Spot-Benutzer automatisch vor. Sofern Sie beispielsweise einen Access Point oder WLAN Controller einsetzen, können Sie mehrere Netzwerknamen als Vorgabewert auswählen, um den Benutzern standardmäßig den Zugang zu mehreren WLANs zu bereitzustellen. Beim Erstellen eines neuen Benutzers und dem anschließenden Voucher-Druck erscheinen diese SSIDs ebenfalls auf dem ausgedruckten Ticket.

Über die Pfeil-Schaltflächen ändern Sie die Reihenfolge der angezeigten SSIDs. Oft genutzte SSIDs können Sie damit z. B. an die oberen Positionen verschieben.

Fertig! Damit ist die Konfiguration der Standardwerte für den Public Spot-Assistenten abgeschlossen.

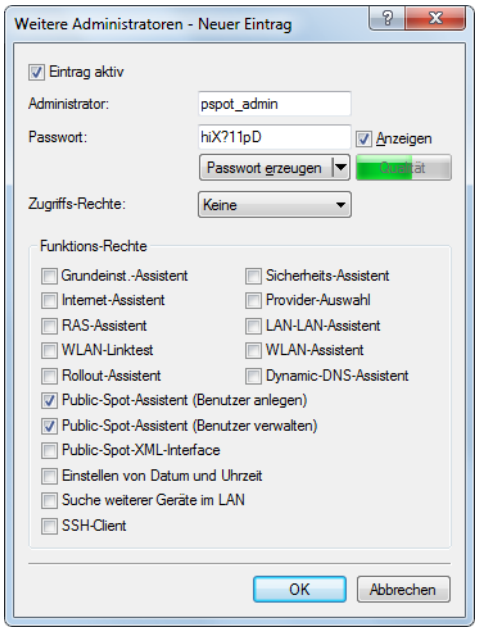
Beschränkten Administrator zur Public Spot-Verwaltung einrichten

Um Mitarbeitern auch ohne Zugriff auf die Gerätekonfiguration die Einrichtung und Verwaltung von Benutzern zu erlauben, haben Sie die Möglichkeit, einen beschränkten Administrator einzurichten, welcher ausschließlich über die Rechte zur Verwendung der *Public Spot-Assistenten* verfügt. Dieses Tutorial beschreibt die dafür erforderlichen Schritte sowie die notwendigen Zugriffs- und Funktionsrechte in LANconfig.

Da die Rechte zur Verwendung der Public Spot-Assistenten getrennt von einander konfigurierbar sind, lässt sich ein beschränkter Administrator auch auf einen einzelnen Assistenten einschränken. Im Falle des Benutzer-Erstellungs-Assistenten leitet das Gerät den beschränkten Administrator nach dem WEBconfig-Login dann automatisch an die entsprechende Eingabemaske weiter.

1. Öffnen Sie in LANconfig den Konfigurationsdialog des Gerätes, für das Sie einen Public Spot-Administrator hinzufügen wollen.
   In diesem Gerät muss das Public Spot-Modul aktiviert sein.
2. Wechseln Sie in die Ansicht **Management** > **Admin**. Klicken Sie im Abschnitt **Geräte-Konfiguration** auf **Weitere Administratoren** und klicken Sie anschließend **Hinzufügen**.

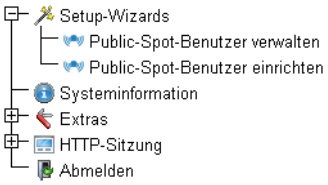
   Wenn Sie einem vorhandenen Administrator die Public Spot-Verwaltung zuweisen möchten, markieren Sie dessen Tabelleneintrag und klicken stattdessen **Bearbeiten**.



3. Aktivieren Sie das Profil, indem Sie die Option **Eintrag aktiv** markieren.
4. Vergeben Sie einen aussagekräftigen Namen im Feld **Administrator**.
5. Bestimmen Sie ein **Passwort** und wiederholen Sie es zur Kontrolle.
6. Setzen Sie die **Zugriffs-Rechte** auf **Keine**.
7. Aktivieren Sie im Abschnitt **Funktions-Rechte** die Optionen **Public-Spot-Assistent (Benutzer anlegen)** für den Benutzer-Erstellungs-Assistenten und **Public-Spot-Assistent (Benutzer verwalten)** für den Benutzer-Verwaltungs-Assistenten.

   Das Funktionsrecht **Public-Spot-XML-Interface** wird von einem Public Spot-Administrator nicht benötigt. Das Recht ist nur relevant, wenn Sie das XML-Interface verwenden und sollte auch dann aus Sicherheitsgründen nicht mit den oben beschriebenen Funktionsrechten kombiniert werden.
8. Speichern Sie das erstellte oder geänderte Administratorprofil mit einem Klick auf **OK**.

Sofern Sie die Funktions-Rechte für mehrere Assistenten gesetzt haben, kann der beschränkte Administrator in WEBconfig über die Navigationsleiste zwischen den Assistenten navigieren.



Sofern Sie ausschließlich das Funktionsrecht **Public-Spot-Assistent (Benutzer anlegen)** gesetzt haben, kann ein beschränkter Administrator lediglich innerhalb des Benutzer-Erstellungs-Assistenten navigieren; die Navigationsleiste bleibt verborgen. Ein manuelles Abmelden über WEBconfig ist in diesem Fall nicht mehr möglich. Aus Sicherheitsgründen ist die Lebensdauer der WEBconfig-Sitzung daher sehr kurz gehalten. Bei entsprechender Inaktivität loggt das Gerät den beschränkten Administrator automatisch aus.

Aus technischen Gründen kann sich der Benutzer-Erstellungs-Assistent nach Verwenden der Schaltfläche **User anlegen und CSV-Export** nicht automatisch aktualisieren. Möchte ein beschränkter Administrator weitere Benutzer einrichten und Voucher ausdrucken, muss er den Assistenten neu aufrufen (z. B. via URL oder Aktualisieren der Webseite, wenn die Navigationsleiste verborgen ist).

Public-Spot-Benutzer für einfache Szenarien einrichten und verwalten

Sie haben die Möglichkeit, Public Spot-Benutzer sowohl von Hand als auch mit Hilfe der Setup-Wizards einzurichten und zu verwalten. Die Einrichtung und Verwaltung von Hand bietet Ihnen umfassendere Konfigurationsmöglichkeiten und erlaubt Ihnen z. B. das Anlegen selbstdefinierter Benutzer von unbegrenzter Lebensdauer.

Über die Setup-Wizards hingegen erstellen Sie generische Public Spot-Benutzer mit automatisch generierten Zugangsdaten von beschränkter Lebensdauer. Der betreffende Setup-Wizard ist ausschließlich über WEBconfig zugänglich, was Ihnen das schnelle Anlegen von Nutzern erlaubt, ohne dass dafür allgemeine Administrationsrechte für das komplette Gerät erforderlich sind. Es wird lediglich ein Administrator mit beschränkten Rechten benötigt.

Es steht Ihnen natürlich auch frei, mit Hilfe des Setup-Wizards zunächst einen generischen Nutzer zu erzeugen und diesen dann manuell Ihren Bedürfnissen (z. B. Änderung des Benutzernamens) entsprechend anzupassen.

Einrichtung und Verwaltung über die Setup-Wizards (WEBconfig)

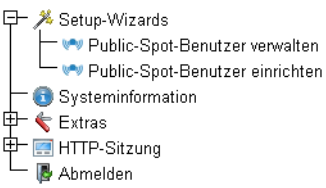
Die Setup-Wizards unterstützen Sie bei der einfachen Verwaltung von Public Spot-Benutzern.

Public-Spot-Benutzer mit einem Klick hinzufügen und Voucher-Druck

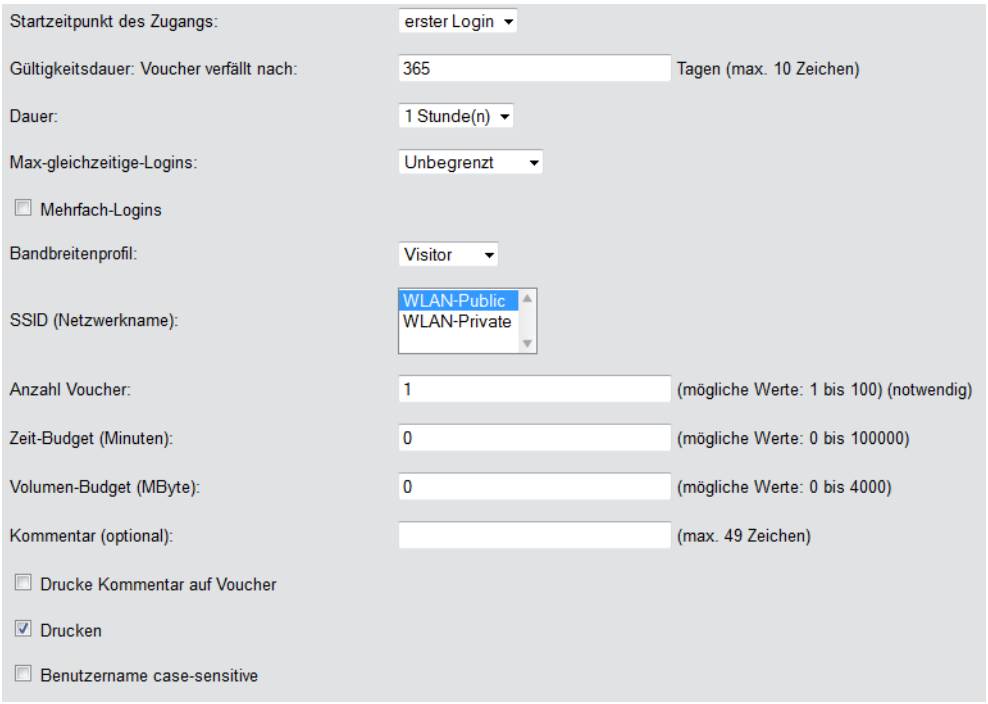
Der folgende Abschnitt beschreibt die Einrichtung eines Public Spot-Benutzers über WEBconfig und den anschließenden Ausdruck des Vouchers. Sie können Voucher dabei auch auf Vorrat anlegen.

Sie benötigen das Zugriffsrecht **Public-Spot-Assistent (Benutzer anlegen)**, um einen neuen Public Spot-Benutzer anzulegen.

1. Melden Sie sich auf der Startseite von WEBconfig als Public Spot-Administrator an.
2. Starten Sie den Setup-Assistenten mit einem Klick auf **Setup-Wizards** > **Public-Spot-Benutzer einrichten**.



3. Der Benutzer-Erstellungs-Assistent startet mit der Eingabemaske. Die Felder sind mit Standardwerten vorbelegt.



Der Assistent vergibt daraufhin automatisch einen Nutzernamen und ein Zugangs-Passwort. Im anschließenden Druck-Dialog können Sie den Voucher-Drucker auswählen und den Voucher ausdrucken.

4. Ändern Sie ggf. vor dem Druck die Standardwerte den Anforderungen entsprechend.

   Die folgenden Einträge beeinflussen sowohl Aussehen als auch Gültigkeit des Vouchers:

   - **Startzeitpunkt des Zugangs**: Legt fest, ab wann der Voucher gültig ist. In der Einstellung **erster Login** gilt der Zugang ab Erstanmeldung; in der Einstellung **sofort** ab Anlegen des Benutzers.

     Um mehrere Vouchers auf Vorrat anzulegen, wählen Sie hier als Gültigkeit des Vouchers `erster Login`. Somit stellen Sie sicher, dass die Vouchers auch nach längerer Vorhaltezeit ihre Gültigkeit behalten.
   - **Gültigkeitsdauer: Voucher verfällt nach**: Geben Sie die Dauer an, nach der der Voucher ungültig wird. Es ist nicht möglich, eine Gültigkeitsdauer einzutragen, wenn der Zugang ab sofort gültig ist.
   - **Dauer**: Wählen Sie die Dauer aus, für die dieser Zugang ab Erstanmeldung oder Anlegen des Benutzers gültig ist. Die hier aufgelisteten Einträge verwalten Sie in der **Default-Laufzeit**-Tabelle.
   - **Max-gleichzeitige-Logins**: Wählen Sie hier die für den jeweiligen Benutzer zutreffende Anzal von Geräten aus, die maximal gleichzeitig auf das Benutzerkonto zugreifen dürfen. Die hier aufgelisteten Einträge verwalten Sie in der **Max-gleichzeitige-Logins-Tabelle**.
   - **Mehrfach-Logins**: Aktivieren Sie diese Option, um dem Benutzer die Anmeldung mehrerer Geräte mit den selben Zugangsdaten generell zu erlauben. Die erlaubte Menge der gleichzeitig angemeldeten Geräte legen Sie über die Auswahlliste **Max-gleichzeitige-Logins** fest.
   - **Bandbreitenprofil**: Wählen Sie aus der Liste ein Bandbreitenprofil, um die dem Nutzer zur Verfügung gestellte Bandbreite (Uplink und Downlink) selektiv zu beschränken. Banbreitenprofile legen Sie in der **Bandbreitenprofile**-Tabelle an.
   - **SSID (Netzwerkname)**: Geben Sie an, für welches WLAN-Netz der Zugang gilt. Die hier aufgelisteten SSIDs verwalten Sie in der **SSID-Tabelle**. Durch drücken der "Strg"-Taste haben Sie die Möglichkeit, mehrere Einträge auszuwählen. Standardeinträge sind bereits vormarkiert.

     Sofern Sie in der Tabelle keinen Eintrag definiert haben, blendet der Assistent diese Einstellungsmöglichkeit aus.

- **Anzahl Voucher**: Geben Sie an, wie viele Vouchers Sie gleichzeitig erstellen möchten. Wenn Sie den ersten Login als Startzeitpunkt des Zugangs festgelegt haben, können Sie hierüber mehrere Vouchers "auf Vorrat" ausdrucken.
- **Zeit-Budget (Minuten)**: Geben Sie an, nach welcher Online-Zeit der Public Spot-Zugang schließt. Je nach gewählter Ablauf-Methode bestimmt entweder dieses Zeit-Budget (inkrementell) oder die eingestellte Voucher-Zugangsdauer (absolut) die Frist für den Zugang.
- **Volumen-Budget (MByte)**: Geben Sie an, nach welcher übertragenen Datenmenge der Zugang schließt.
- **Kommentar (optional)**: Fügen Sie einen Kommentar ein. Dieser Kommentar kann zum Beispiel weitere Hinweise zur Zugangsdauer oder die Telefonnummer der Rezeption bei Zugangsproblemen beinhalten.
- **Drucke Kommentar auf Voucher**: Aktivieren Sie diese Option, damit der Kommentar auf dem Voucher erscheint.
- **Drucken:** Aktivieren Sie diese Option, damit Sie beim Speichern gleichzeitig die registrierten Vouchers ausdrucken.
- **Benutzername case-sensitive**: Aktivieren Sie diese Option, wenn der Public Spot-Nutzer bei der Anmeldung auf die Groß- und Kleinschreibung seines Benutzernamens achten muss.

5. Wenn Sie die Default-Werte unverändert oder die neuen Werte übernehmen möchten, klicken Sie abschließend auf **Speichern und Drucken**.

   Wenn Sie die Option **Drucken** deaktiviert haben, zeigt Ihnen der Assistent nach der Registrierung eine Übersicht der neuen Public Spot-Benutzer. Sie erhalten dann noch einmal die Gelegenheit, die Vouchers auszudrucken.

   Über die Schaltfläche **Benutzerverwaltung aufrufen** gelangen Sie zum Setup-Wizard **Public-Spot-Benutzer verwalten**.

Diese Schaltfläche können Sie wahlweise anzeigen lassen oder ausblenden. Als Default ist sie eingeblendet.

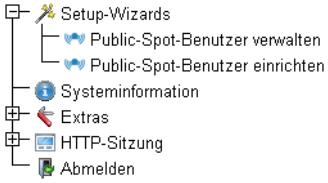
Assistent zum Verwalten von Public Spot-Benutzern

Der folgende Abschnitt beschreibt die Verwaltung von registrierten Public Spot-Benutzern über WEBconfig.

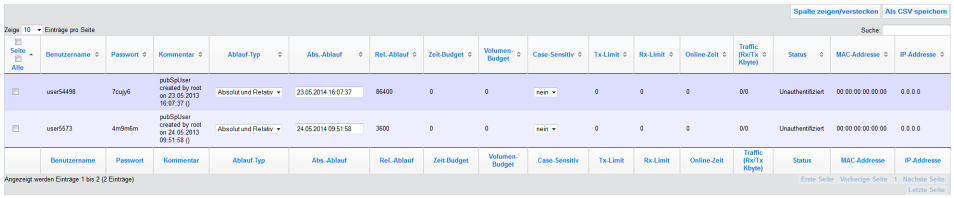
Sie benötigen das Zugriffsrecht **Public-Spot-Assistent (Benutzer verwalten)**, um Public Spot-Benutzer verwalten zu können.

Ungespeicherte Änderungen gehen verloren, sobald Sie diesen Assistenten beenden.

1. Melden Sie sich auf der Startseite von WEBconfig als Public Spot-Administrator an.
2. Starten Sie den Setup-Assistenten mit einem Klick auf **Setup-Wizards** > **Public-Spot-Benutzer verwalten**.



3. Der Public Spot-Assistent startet mit einer Liste der registrierten Public Spot-Benutzer.



In der Auswahlliste **Zeige ... Einträge pro Seite** stellen Sie die Anzahl angezeigter Einträge pro Seite ein. Die entsprechenden Seiten rufen Sie über die Seitennavigation rechts unten auf:

- **Erste Seite**: Zeigt die Seite mit den ersten Einträgen an.
- **Vorherige Seite**: Wechselt eine Seite zurück.
- **Seitennummern (1, 2, 3,...)**: Wechselt direkt zur gewählten Seite.
- **Nächste Seite**: Wechselt eine Seite weiter.
- **Letzte Seite**: Zeigt die Seite mit den letzten Einträgen an.

Über **Suche** filtern Sie die angezeigten Einträge. Der Filter führt eingegebene Zeichenfolgen sofort aus.

Markierte Einträge exportieren Sie über **Als CSV speichern**.

Die Tabellenspalten haben folgende Bedeutungen:

- **Seite/Alle**: In dieser Spalte markieren Sie den Benutzer für die gewünschte Aktion (Drucken, Löschen, Speichern). Um alle Einträge der aktuellen Seite auszuwählen, markieren Sie **Seite**. Um alle Einträge komplett auszuwählen, markieren Sie **Alle**.
- **Benutzername**: Zeigt den manuell oder automatisch vom System vergebenen Benutzernamen an.
- **Passwort**: Zeigt das manuell oder vom System vergebene Passwort an.
- **Kommentar**: Beinhaltet sowohl den bei der Registrierung angegebenen Kommentar (in Klammern) sowie Änderungen an den Benutzer-Daten (automatisch vom System dokumentiert).
- **Ablauf-Typ**: Zeigt an, ob die Gültigkeitsdauer dieses Benutzer-Accounts absolut (fester Zeitpunkt) oder relativ (Zeitspanne ab dem ersten erfolgreichen Login) festgelegt ist.
- **Abs.-Ablauf**: Wenn der Ablauf-Typ "Absolut" aktiviert ist, endet die Gültigkeit dieses Benutzer-Accounts zu dem in diesem Feld angegebenen Zeitpunkt.
- **Rel.-Ablauf**: Wenn der Ablauf-Typ "Relativ" aktiviert ist, endet die Gültigkeit dieses Benutzer-Accounts nach der in diesem Feld angegebenen Zeitspanne nach dem ersten erfolgreichen Login des Benutzers.
- **Zeit-Budget**: Gibt die maximale Nutzungsdauer für diesen Benutzer-Account an. Diese Nutzungsdauer kann der Benutzer bis zum Erreichen einer ggf. definierten relativen oder absoluten Ablaufzeit ausschöpfen.
- **Volumen-Budget**: Gibt das maximale Datenvolumen für diesen Benutzer-Account an. Dieses Datenvolumen kann der Benutzer bis zum Erreichen einer ggf. definierten relativen oder absoluten Ablaufzeit ausschöpfen.
- **Case-Sensitiv**: Gibt an, ob die Anmeldeseite die Groß- und Kleinschreibung des jeweiligen Benutzernamen berücksichtigt.
- **Tx-Limit**: Sofern beim Erstellen des Benutzers ein Bandbreitenprofil vergeben wurde, zeigt dieser Eintrag die maximale Sende-Bandbreite an, die dem Benutzer zur Verfügung steht.
- **Rx-Limit**: Sofern beim Erstellen des Benutzers ein Bandbreitenprofil vergeben wurde, zeigt dieser Eintrag die maximale Empfangs-Bandbreite an, die dem Benutzer zur Verfügung steht.
- **Traffic (Rx/Tx Kbyte)**: Zeigt die Datenmenge in Kilobyte an, die der betreffende Benutzer bisher empfangen (Rx) bzw. gesendet (Tx) hat.
- **Status**: Zeigt den Authentifizierungsstatus der einzelnen Benutzer an, also ob der Benutzer derzeit am Public Spot angemeldet ist (**Authentifiziert**) oder nicht (**Unauthentifiziert**).
- **MAC-Addresse**: Zeigt die physikalische Adresse der Netzwerkkarte des Benutzers, mit der Nutzer derzeit verbunden ist.
- **IP-Addresse**: Zeigt die IPv4-Adresse, die das System dem Benutzer derzeit zugewiesen hat.

Die Schaltflächen am unteren Fensterrand besitzen folgende Funktionen:

- **Drucken**: Drucken Sie die Vouchers der markierten Benutzer aus.
- **Löschen**: Löschen Sie die markierten Benutzer.
- **Speichern**: Speichern Sie die Änderungen.
- **Zurück zur Hauptseite**: Wechseln Sie zur Hauptseite zurück, wobei alle ungespeicherten Änderungen verloren gehen.

Folgende Angaben eines Benutzers passen Sie an, indem Sie die Inhalte der entsprechenden Felder ändern:

- **Ablauf-Typ**
- **Abs.-Ablauf**
- **Rel.-Ablauf**
- **Case-Sensitiv**

4. Markieren Sie den zu ändernden Benutzer in der ersten Spalte.
5. Ändern Sie die entsprechenden Feldinhalte, und klicken Sie auf **Speichern**, um diese Änderungen zu übernehmen. Ungespeicherte Änderungen gehen verloren, sobald Sie diesen Assistenten verlassen.
6. Wenn Sie einen Benutzer löschen möchten, markieren Sie den entsprechenden Eintrag in der ersten Spalte, und klicken Sie auf **Löschen**

Die Löschung eines Eintrags erfolgt ohne vorherige Rückfrage.

Felder mit WEBconfig ausblenden

Im Setup-Assistenten "Public-Spot-Benutzer verwalten" haben Sie über die Schaltfläche **Spalte zeigen/verstecken** die Möglichkeit, Tabellenspalten ein- oder auszublenden. Diese Änderungen sind jedoch nur temporär. Nach einem Seiten-Refresh oder bei einer neuen Sitzung werden die ausgeblendeten Spalten wieder angezeigt.

Um bestimmte Felder dauerhaft zu verbergen, wechseln Sie im LCOS-Menübaum zur Ansicht **Setup** > **Public-Spot-Modul** > **Verwalte-Benutzer-Assistent**. Standardmäßig werden alle Felder angezeigt. Blenden Sie bestimmte Felder aus, um z. B. das Zeit-Budget zu verbergen, bleiben diese Spalten sowohl im Assistenten selbst als auch im Dropdown-Menü unter der Schaltfläche **Spalte zeigen/verstecken** nach einem erneuten Aufrufen der Seite verborgen.

Um einen authentisierten Public Spot-Benutzer zu löschen, müssen die Spalten "Rufende-Station-Id-Maske" und "Gerufene-Station-Id-Maske" im Assistenten sichtbar sein. Nicht authentisierte Benutzer hingegen lassen sich auch löschen, wenn beide Spalten ausgeblendet sind.

Beachten Sie bitte, dass ausgeblendete Felder beim Betätigen der Schaltfläche **Drucken** nicht mit ausgegeben werden. Die Ausgabe als CSV-Datei beinhaltet dagegen alle Daten. Sie haben jedoch die Möglichkeit, die Schaltfläche **Als CSV speichern** zu verbergen. Wechseln Sie dazu im LCOS-Menübaum zur Ansicht **Setup** > **Public-Spot-Modul** > **Neuer-Benutzer-Assistent** > **CSV-Export-verstecken**. Wählen Sie "Ja" und speichern Sie Ihre Eingabe.

Manuelle Einrichtung und Verwaltung

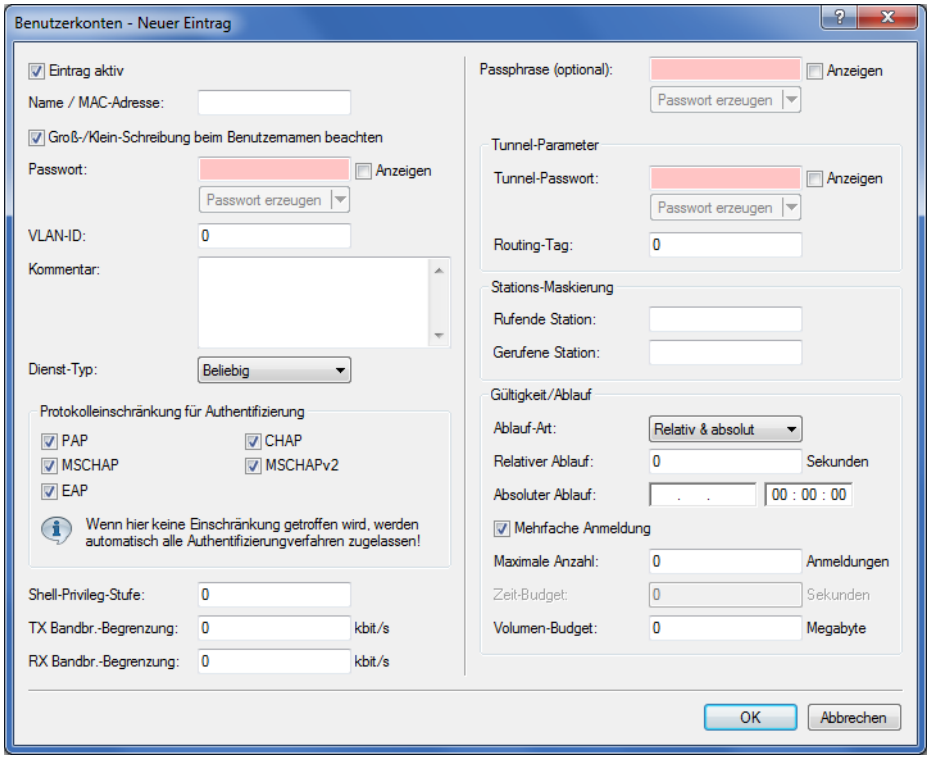
Die nachfolgenden Konfigurationsschritte zeigen Ihnen, wie Sie in LANconfig manuell einen Public Spot-Benutzer für einfache Einsatzszenarien einrichten. Public Spot-Nutzer erstellen und verwalten Sie über die **Benutzer-Datenbank** des geräteinternen RADIUS-Servers, erreichbar unter **RADIUS** > **Server** > **Benutzer-Datenbank**. Hier tragen Sie – aber auch die Setup-Wizards – alle Benutzer ein, die einen Zugang zum Public Spot erhalten sollen.

Das Public Spot-Modul verfügt für die Benutzerverwaltung noch über eine eigene, interne Liste (erreichbar unter **Public-Spot** > **Benutzer** > **Benutzer-Liste**). Im Zuge der technischen Entwicklung ist diese Liste seit LCOS 7.70 durch die Benutzerverwaltung via RADIUS ablöst. Aus Kompatibilitätsgründen wertet das Gerät die interne Benutzer-Liste des Public Spot-Moduls weiterhin aus, sofern Sie dies aktivieren. Für neue Installationen sollten Sie diese Liste jedoch nicht mehr verwenden, da Ihnen sonst zahlreiche Features nicht zur Verfügung stehen (Einrichtung und Verwaltung über die Assistenten, Bandbreiten-Begrenzung, Accounting via RADIUS, VLAN-IDs für Public Spot-Nutzer etc.).

1. Geben Sie unter **Name** den Benutzernamen des zukünftigen Nutzers oder die **MAC-Adresse** seines Endgerätes ein.

   Wenn Sie als Authentifizierungs-Modus **Anmeldung mit Name und Passwort** gewählt haben, tragen Sie hier die Kennung ein, mit welcher sich der Nutzer am Public Spot authentisiert. Die Vergabe eines **Passworts** ist optional, ist für den obigen Authentifizierungs-Modus jedoch zu empfehlen.

   › LANconfig: **RADIUS** > **Server** > **Benutzer-Datenbank** > **Benutzerkonten**



   Sofern die Authentifizierung zusätzlich über die MAC-Adresse erfolgt (Authentifizierungs-Modus **Anmeldung mit Name, Passwort und MAC-Adresse**), definieren Sie die MAC-Adresse über das Feld **Rufende Station** in der Form `12:34:56:78:90:AB`.

2. Setzten Sie den **Dienst-Typ** auf `Anmeldung`.

3. Heben Sie sämtliche Protokolleinschränkungen auf, indem Sie alle Auswahlkästchen deselektieren.
   In einem Public Spot-Szenario findet eine Phase-2-Authentifizierung nicht statt. Diese kann lediglich für direkte WLAN-Verbindungen abseits eines Public Spot-Betriebs und die dazugehörigen RADIUS-Benutzer sinnvoll sein.

   Wenn Sie die Protokolleinschränkungen nicht komplett aufheben, kann sich ein Nutzer nicht über die Login-Webseite Ihres Public Spots anmelden!

4. Optional: Auf Wunsch können Sie z. B. noch

   › im Abschnitt **Gültigkeit/Ablauf** ein relatives oder/und absolutes Ablaufdatum für die Gültigkeit des Benutzerkontos angeben (relativ = Gültigkeit in Sekunden nach erstem Login);
   › unter **TX/RX Bandbr.-Begrenzung Bandbreite** den Uplink/Downlink begrenzen;
   › die **Mehrfache Anmeldung** aktivieren und die **Maximale Anzahl** der Endgeräte angeben, die gleichzeitig über das Benutzerkonto angemeldet sein dürfen.

5. Speichern Sie die Konfiguation auf Ihrem Gerät.

Fertig! Ihre Public Spot-Nutzer können sich nun mit den von Ihnen festgelegten Zugangsdaten am Public Spot anmelden.

1.2.2 Sicherheitseinstellungen

Der Public Spot verfügt über zwei zusätzliche Schutzmechanismen, die ihn wirksam gegen Missbrauch absichern.

Traffic-Limit-Option

Um die Anmeldung am Public Spot über den Browser zu ermöglichen, ist es prinzipiell gestattet, dass auch unangemeldete Benutzer Datenpakete (z. B. DNS-Anfragen) an das Public Spot-Gerät senden. In der Standardeinstellung ist diese Datenmenge unbegrenzt. Daraus ergeben sich folgende Risiken:

- **Unberechtigte Nutzung des Public-Spots:** Mit geeigneten Tools könnte ein Benutzer alle Daten in ein DNS-Paket verpacken (also einen DNS-Tunnel aufbauen) und so einen Public Spot ohne Anmeldung nutzen.
- **Denial-of-Service:** Der Angreifer könnte erhebliche Datenmengen an das angegriffene Gerät senden und auf diese Weise versuchen, das Gerät bzw. den Public Spot zu blockieren.
- **Brute-Force:** Der Angreifer könnte versuchen, Zugang zur Basis-Station zu erhalten, indem er einfach so lange alle denkbaren Anmeldedaten durchprobiert, bis ihm der Zugang schließlich gelingt.

Die Traffic-Limit-Option ermöglicht, diese Risiken wirksam auszuschließen.

Sie aktivieren die Traffic-Limit-Option durch einen Wert ungleich "0". Der Wert bestimmt die maximale Datenmenge in Byte, die eine unangemeldetes Endgerät an den Public Spot senden und von ihm empfangen darf.

- LANconfig: **Public-Spot** > **Server** > **Zugriff ohne Anmeldung ermöglichen** > **Maximales Datenvolumen**

Sobald ein Endgerät dieses Transfervolumen überschreitet, sperrt der Public Sport dieses Gerät und verwirft fortan die von ihm empfangenen Daten ungeprüft. Diese Sperre erlischt erst wieder, wenn der zum Gerät gehörige Eintrag in der Stationstabelle verschwindet.

Bei WLAN-Geräten kann diese Löschung z. B. durch den Ablauf des allgemeinen Idle-Timeouts geschehen:

- WEBconfig: **Extras** > **LCOS-Menübaum** > **Setup** > **WLAN** > **Idle-Timeout**

Bitte beachten Sie, dass bei eingeschalteter Stationsüberwachung die Sperre möglicherweise auch schon früher entfernt wird. Ist eine Mobilstation 60 Sekunden lang unerreichbar, entfernt das Gerät dessen Eintrag aus der Stationstabelle und damit auch die Sperre.

Die Leerlaufzeitüberschreitung für das Public Spot-Modul erfüllt den gleichen Zweck wie der Idle-Timeout für WLAN, beschränkt sich allein auf Verbindungen über Public Spot. Ist die Leerlaufzeitüberschreitung gesetzt und kommen von einem Benutzer keine Datenpakete mehr, loggt das Gerät diesen nach Ablauf der eingetragenen Zeit automatisch aus.

- LANconfig: **Public-Spot** > **Server** > **Leerlaufzeitüberschreitung**

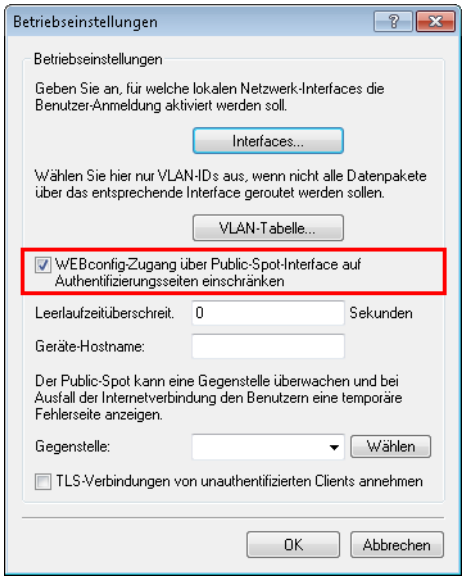
Der optimale Wert des Traffic-Limits hängt zum einen von der Datengröße der Anmeldeseite ab. Zum anderen wirkt sich dieser Wert maßgeblich auf die mögliche Anzahl erfolgloser Anmeldeversuche durch einen Benutzer aus. Im Regelfall bewirkt ein Traffic-Limit von 60.000 Bytes den wirksamen Schutz des Public-Spots, lässt aber gleichzeitig eine ausreichende Anzahl von Anmeldeversuchen zu. Bei Bedarf können Sie diesen Wert den individuellen Bedürfnissen anpassen. Der Default-Wert von "0" Bytes steht für ein unbegrenztes Datenvolumen.

Die Traffic-Limit-Option überwacht ausschließlich den Datenverkehr vor der Anmeldung. Sie berücksichtigt nicht den Datenverkehr von und zu einem ggf. eingerichteten, freien Web-Server. Dieser bleibt zu jeder Zeit unlimitiert.

Konfigurationszugriff einschränken

Der Zugriff aus einem Public Spot-Netzwerk auf die Konfiguration eines Public Spots (WEBconfig) sollte aus Sicherheitsgründen immer ausgeschlossen sein. Mit einem speziellen Schalter besteht die Möglichkeit, den Zugang über Public Spot-Interfaces auf die Public Spot-Authentisierungsseiten zu reduzieren und automatisch alle anderen Konfigurationsprotokolle zu sperren.

- LANconfig: **Public-Spot** > **Server** > **Betriebseinstellungen** > **WEBconfig-Zugang über Public Spot-Interface auf Authentifizierungsseiten einschränken**



Bitte beachten Sie, dass Sie über die Zugriffsrechte unter **Management** > **Admin** > **Konfigurations-Zugriffs-Wege** > **Zugriffs-Rechte** nicht generell den Zugriff über HTTP(S) auf das Gerät einschränken.

1.2.3 Erweiterte Funktionen und Einstellungen

Der Public Spot beinhaltet zahlreiche erweiterte Funktionen, Optionen und Parameter, mit denen Sie ihn individuell an die spezifischen Eigenarten seines Einsatzgebietes anpassen können.

In den folgenden Abschnitten finden Sie Informationen über:

- Multiple Anmeldungen

  Standardmäßig ist die Nutzung von Zugangsdaten auf die Anmeldung mit einem Gerät beschränkt. Erfahren Sie, wie Sie diese Limit heraufsetzen oder die Beschränkung für ein Benutzerkonto komplett aufheben.

- Anmeldungsfreie Netze

  Richten Sie zusätzliche Netze ein, die ein Public Spot-Benutzer auch ohne Anmeldung am Public Spot erreichen kann, um um ihn online mit zusätzlichen Informationen (z. B. Kundenwebseite in einem Unternehmen, Veranstaltungskalender in einem Hotel) zu versorgen.

- Benutzerverwaltung über das Web-API

  Nutzen Sie URLs, um Public Spot-Benutzer über Datei-Verknüpfungen oder Skripte zu anzulegen und zu verwalten.

- Individuelle Begrenzung der Bandbreite

  Begrenzen Sie für jeden Public Spot-Nutzer individuell den ihm zugewiesenen Up- und Downlink.

- Automatische Bereinigung von Benutzerkonten und Mobilstationen

  Nutzen Sie die geräteeigenen Funktionen, um abgelaufene Public Spot-Benutzerkonten und nicht ordnungsgemäß abgemeldetete Mobilstationen (nur WLAN) automatisch aus den geräteinternen Datenbanken zu entfernen.

- Übergabe von WLAN-Sitzungen zwischen Geräten

  Erfahren Sie mehr über die Roaming-Möglichkeiten von Mobilstationen zwischen einzelnen Access Points, und welche besonderen Konfigurationen notwendig sind, um Ihren Benutzern die unterbrechungsfreie Übergabe von WLAN-Sitzungen zu ermöglichen.

- Authentifizierung über RADIUS

Erfahren Sie, wie Sie ein mehrere RADIUS-Server für Authentifizierung und Accounting bereitstellen, und wie Sie Server sinnvoll miteinander verketten, um im Falle der Unerreichbarkeit einzelner Systeme die Nutzerdaten an entsprechende Backup-Systeme weiterzuleiten.

- Abrechnung von Public Spot-Verbindungen im kommerziellen Betrieb

  Erfahren Sie mehr über die Abrechnungsfunktionen, die Ihnen der Public Spot für den kommerziellen Betrieb bereitstellt. Diese Abrechnungsfunktionen lassen sich grob in zwei Modelle unterteilen:

  - Bezahlung tatsächlich genutzter Ressourcen im Nachhinein (Kredit-Abrechnung)
  - Benutzung des Services auf Guthabenbasis (Debit-Abrechnung, PrePaid)

- Verwenden mehrstufiger Zertifikate

  Erfahren Sie, wie Sie SSL-Zertifikatsketten in Ihr Gerät laden.

- Individuelle Zuweisung von VLAN-IDs

  Erfahren Sie, wie Sie einzelnen Public Spot-Nutzern individuelle VLAN-IDs zuweisen.

Mehrfach-Logins

Sie haben die Möglichkeit, Public Spot-Benutzern zu gestatten, sich mit mehreren Geräten gleichzeitig auf ein Benutzerkonto einzuloggen. Dies kann dann erforderlich sein, wenn eine Gruppe von zusammengehörigen Personen (z. B. eine Familie) mehrere Geräte besitzt und diese zur gleichen Zeit für den Zugang ins Netz nutzen möchte.

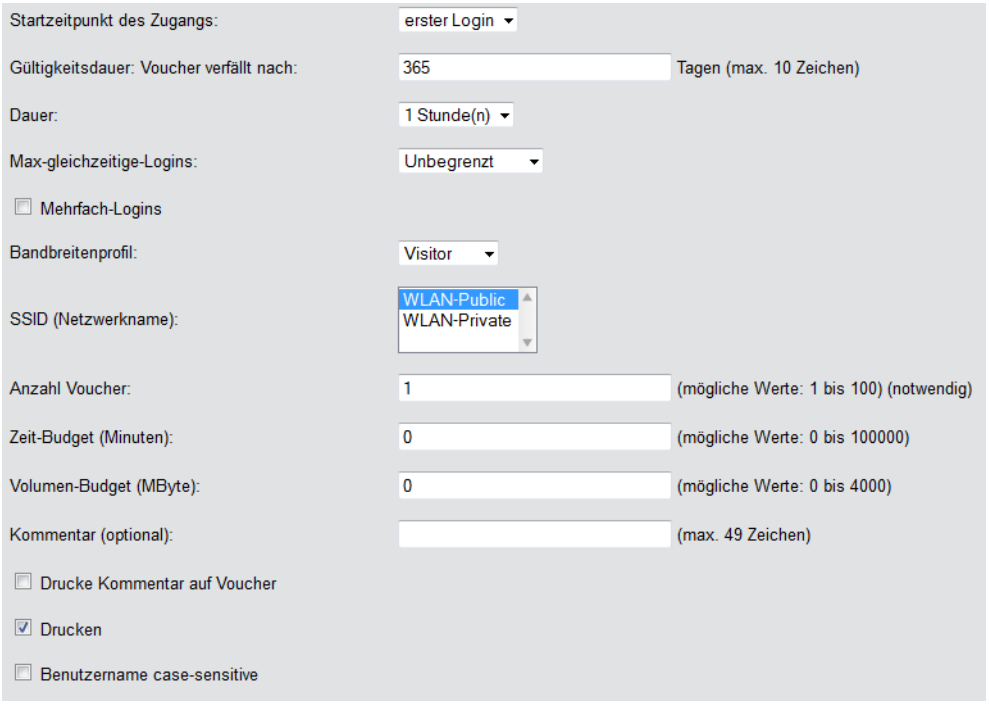
Standardwerte festlegen

Um diese Funktion zu verwenden, definieren Sie im ersten Schritt die mögliche Anzahl der gleichzeitig nutzbaren Geräte im Setup-Menü unter **Public-Spot-Modul** > **Neuer-Benutzer-Assistent** > **Max-gleichzeitige-Logins-Tabelle**. Hier tragen Sie jene Werte ein, die Sie im zweiten Schritt mit Hilfe des Assistenten **Public-Spot-Benutzer einrichten** zuweisen. Der Wert `0` steht dabei für "Unbegrenzt".

Auswahl der Mehrfach-Logins im Benutzer-Erstellungs-Assistenten

Wenn Sie den Assistenten **Public-Spot-Benutzer einrichten** aufrufen, finden Sie das Auswahlmenü **Max-gleichzeitige-Logins** vor. Die hier angezeigten Werte entsprechen den Zahlen, die Sie zuvor in der analog benannten Tabelle festgelegt haben. Die Zahlen werden innerhalb der Phrase "Nur...Gerät(e)" wiedergegeben.

Wählen Sie hier die für den jeweiligen Benutzer zutreffende Anzal von Geräten aus, die maximal gleichzeitig auf das Benutzerkonto zugreifen dürfen. Beachten Sie, dass für die Aktivierung der Funktion zusätzlich noch die Option **Mehrfach-Logins** ausgewählt sein muss.



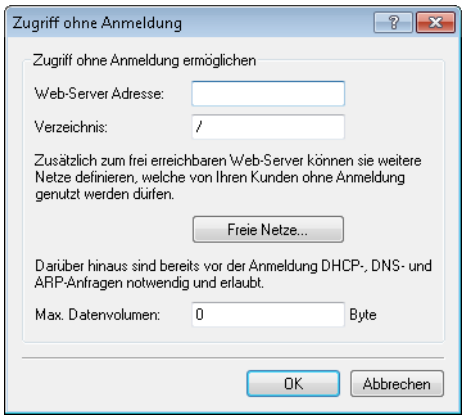
Anmeldungsfreie Netze

Um den Benutzern den Zugang zu wichtigen Informationen auch ohne Anmeldung zu ermöglichen (z. B. wichtige Kontaktinformationen), können Sie einen frei erreichbaren Web-Server definieren.

› LANconfig: **Public-Spot** > **Server** > **Zugriff ohne Anmeldung**

Falls Sie den hier definierten Server nicht vollständig freigegeben wollen, können Sie optional einen abweichenden Pfad auf dem Web-Server angeben:

› LANconfig: **Public-Spot** > **Server** > **Zugriff ohne Anmeldung** > **Verzeichnis**

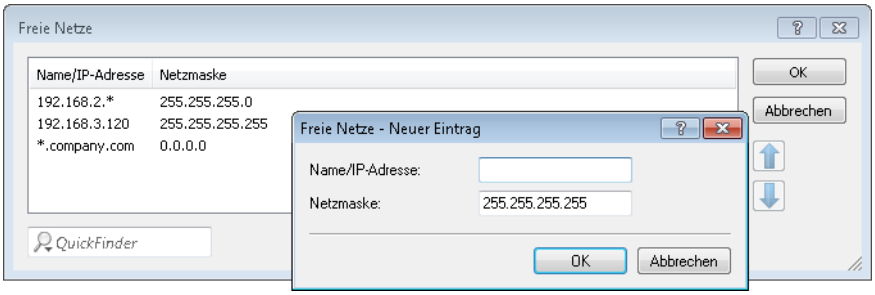


Zusätzlich zum frei erreichbaren Web-Server können Sie weitere Netze und Spezial-Seiten definieren, welche von Ihren Kunden ohne Anmeldung genutzt werden dürfen.

› **Public-Spot** > **Server** > **Zugriff ohne Anmeldung** > **Freie Netze**

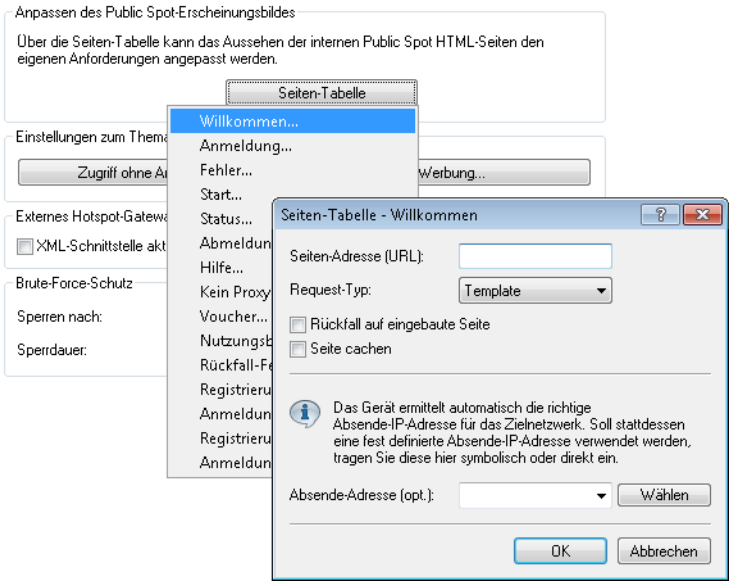
Tragen Sie die IP-Adresse des zusätzlichen Servers oder Netzwerks inklusive Netzmaske ein, auf welche die Public Spot-Benutzer zugreifen dürfen. Alternativ haben Sie auch die Möglichkeit, Domain-Namen (mit oder ohne Wildcard "*") einzutragen. Durch Wildcards können Sie z. B. auch den freien Zugriff auf alle Subdomains einer Domäne erlauben. Der Eintrag `*.company.com` gibt somit auch die Adressen `mail.company.com`, `service.company.com` etc. frei.

Wenn Sie nur eine einzelne Station mit der zuvor benannten Adresse oder eine Domain freischalten wollen, geben Sie als Netzmaske `255.255.255.255` ein. Wenn Sie ein ganzes IP-Netz freigeben wollen, geben Sie dafür die zugehörige Netzmaske an. Sofern Sie keine Netzmaske setzen (Wert `0.0.0.0`), ignoriert das Gerät den betreffenden Tabelleneintrag.



› **Public-Spot** > **Server** > **Seiten-Tabelle**

Tragen Sie die Adressen (URL) der Webseiten ein, die der Public Spot dem Benutzer für die Anmeldung, Fehlermeldungen, Status usw. anzeigen soll. Lesen Sie dazu auch das Kapitel über *geräteeigene und individuelle Authentifizierungsseiten*.



DNS-Snooping

Webdienste mit hohen Nutzerzahlen verteilen die Datenanfragen zur besseren Auslastung auf mehrere Server. So kommt es, dass zwei DNS-Anfragen für denselben Hostnamen (z. B. "www.google.de") zu zwei unterschiedlichen IP-Adressen führen können. Erhält der Public Spot für einen eingegebenen Hostnamen vom zuständigen DNS-Server nun mehrere gültige IP-Adressen, wählt er davon eine aus und speichert sie für zukünftige Anfragen von Public Spot-Benutzern. Bekommt der Benutzer jedoch bei einer weiteren Anfrage für denselben Hostnamen die IP-Adresse eines anderen Servers zugeteilt, sperrt der Public Spot diese Verbindung, weil er diese IP-Adresse nicht als zugangsberechtigt gespeichert hat.

Damit Public Spot-Benutzer sich trotz wechselnder IP-Adressen mit dem angefragten Host verbinden können, analysiert der Public Spot die DNS-Anfragen der Benutzer und speichert die jeweils zurückgegebene IP-Adresse zusammen mit dem Hostnamen, der Gültigkeitsdauer (TTL: "Time to Live"), dem Alter und der Datenquelle fortan als freie Zieladresse in der Tabelle **Status** > **Public-Spot** > **Freie-Hosts**.

Die Einträge in dieser Tabelle verfallen nach der in der DNS-Antwort übertragenen Gültigkeitsdauer (TTL). Um bei sehr niedrigen Werten (z. B. 5 Sekunden) den Public Spot-Benutzer nicht sofort nach einer Anfrage wieder auszusperren, können Sie unter **Setup** > **Public-Spot-Modul** > **Freie-Hosts-Minimal-TTL** eine Mindest-Gültigkeitsdauer festlegen.

Verwaltung von Public Spot-Nutzern über das Web-API

Über die Eingabe einer speziellen URL in der Adresszeile haben Sie die Möglichkeit, Public Spot-Benutzer direkt statt über den Setup-Assistenten anzuzeigen, neu anzulegen oder zu löschen.

URL-Aufbau

Die URL hat folgenden Aufbau:

```
http://<Geräte-URL>/cmdpbspotuser/?action=<action>&parameter1=value1&parameter2=value2
```

Die folgenden Aktionen stehen Ihnen zur Verfügung:

- **action=addpbspotuser**: legt einen oder mehrere neue Public Spot-Benutzer an und druckt anschließend Vouchers in der benötigten Anzahl.
- **action=delpbspotuser**: löscht den Public Spot-Benutzer mit der angegebenen Benutzer-ID.
- **action=editpbspotuser**: zeigt einen Public Spot-Benutzer an, dessen Benutzer-ID Sie mit übergeben haben. Anschließend können Sie den Voucher des Benutzers neu ausdrucken.

Die notwendigen Parameter und deren Werte sind abhängig von der angegebenen Aktion.

Der Assistent ignoriert falsche Parameter-Angaben und übernimmt ausschließlich die korrekten Parameter. Falls Sie einen erforderlichen Parameter falsch angegeben oder ausgelassen haben, zeigt der Assistent eine Eingabemaske. Tragen Sie in diese den korrekten Parameter-Wert ein.

Hinzufügen eines Public Spot-Benutzers

Über die folgende URL registrieren Sie einen neuen Public Spot-Benutzer:

```
http://<Geräte-URL>/cmdpbspotuser/
   ?action=addpbspotuser&parameter1=value1&parameter2=value2&...
```

Ihnen stehen folgende Parameter zur Verfügung:

`comment`

Kommentar zum registrierten Benutzer

Sind für einen Public Spot-Benutzer mehrere Kommentare möglich, geben Sie die Kommentare und die entsprechenden Kommentarfeld-Namen wie folgt an:

```
&comment=<Inhalt1>:<Feldname1>,<Inhalt2>:<Feldname2>,…,<Inhalt5>:<Feldname5>,
```

Existiert ausschließlich ein Kommentarfeld pro Benutzer, genügt die Angabe des Kommentars:

```
&comment=<Kommentar>
```

Deutsche Umlaute werden nicht unterstützt.

Die maximale Zeichenanzahl des Kommentar-Parameters beträgt 191 Zeichen.

`print`

Automatischer Ausdruck des Vouchers.

Fehlt dieser Parameter, zeigt der Assistent anschließend eine entsprechende Schaltfläche, über die Sie den Voucher ausdrucken können.

`printcomment`

Kommentar auf den Voucher drucken.

Fehlt dieser Parameter, erscheint der Kommentar nicht auf dem Voucher (Default-Einstellung).

`nbGuests`

Anzahl der anzulegenden Public Spot-Benutzer.

Fehlt dieser Parameter, legt der Assistent ausschließlich einen Benutzer an (Default-Einstellung).

`defaults`

Default-Werte verwenden

Der Assistent ersetzt fehlende oder falsche Parameter durch Default-Werte.

`expirytype`

Kombinierte Angabe von Ablauf-Typ und ggf. Verfallsdauer des Vouchers.

Geben Sie diesen Parameter wie folgt an:

```
&expirytype=<Wert1>+validper=<Wert2>
```

Die Parameter-Werte haben folgende Bedeutung:

- `Wert1`: Ablauf-Typ. Mögliche Werte sind `absolute`, `relative`, `both`und `none`.
- `Wert2`: Verfallsdauer des Vouchers, wenn `expirytype` den Wert `both` besitzt. In diesem Fall definieren Sie mittels `validper` die maximale Gültigkeit des Vouchers in Tagen für den absoluten Ablauf. Für alle anderen Ablauf-Typen wird der Parameter `validper` nicht gesetzt.

Fehlt ein Parameter oder geben Sie falsche Werte ein, setzt der Assistent die Default-Werte ein.

`ssid`

Netzwerk-Name

Fehlt dieser Parameter, verwendet der Assistent den Standard-Netzwerk-Namen (Default-Einstellung).

`unit`

Zugangsdauer

Geben Sie diesen Parameter wie folgt an:

```
&unit=<Wert1>+runtime=<Wert2>
```

Die Parameter-Werte haben folgende Bedeutung:

- `Wert1`: Einheit der Laufzeit. Mögliche Werte sind: Minute, Stunde, Tag
- `Wert2`: Laufzeit

`timebudget`

Zeit-Budget

Fehlt dieser Parameter, verwendet der Assistent den Default-Wert.

`volumebudget`

Volumen-Budget

Die folgenden Angaben sind möglich:

- `k` oder `K`: Angabe in Kilobytes (kB), z. B. `volumebudget=1000k`.
- `m` oder `M`: Angabe in Megabytes (MB), z. B. `volumebudget=100m`.
- `g` oder `G`: Angabe in Gigabytes (GB), z. B. `volumebudget=1g`.

Ohne Einheit entspricht die Angabe einem Wert in Byte (B).

Fehlt dieser Parameter komplett, verwendet der Assistent den Default-Wert.

`multilogin`

Mehrfach-Logins

Wenn Sie diesen Parameter angeben, kann sich der Benutzer mehrfach mit seinem Benutzer-Account anmelden. Fehlt dieser Parameter, sind Mehrfach-Logins standardmäßig deaktiviert.

`maxconclogin`

Anzahl der maximal gleichzeitigen Logins

Mit diesem Parameter legen Sie fest, mit wie vielen Endgeräten parallel sich ein Nutzer am Public Spot anmelden kann. Gültige Werte sind Ganzzahlen wie z. B. `0, 1, 2, ...`.

Fehlt dieser Parameter oder der Parameter hat den Wert `0`, ist dies gleichbedeutend mit einer unbegrenzten Anzahl von Endgeräten.

Dieser Parameter erfordert, dass Mehrfach-Logins erlaubt sind. Das Setzen dieses Parameters allein hat keine Auswirkungen.

`casesensitive`

Benutzername case-sensitive

Wenn Sie diesen Parameter angeben, muss der Public Spot-Nutzer bei der Anmeldung auf die Groß- und Kleinschreibung seines Benutzernamens achten. Gültige Werte sind:

- `0`: Benutzername case-sensitive ist deaktiviert
- `1`: Benutzername case-sensitive ist aktiviert

Fehlt dieser Parameter, verwendet der Assistent den Default-Wert.

`bandwidthprof`

Bandbreitenprofil

Mit diesem Parameter weisen Sie einem Public Spot-Nutzer ein existierendes Bandbreitenprofil zu. Als gültigen Wert für diesen Parameter geben Sie die Zeilennummer eines unter **Setup** > **Public-Spot-Modul** > **Neuer-Benutzer-Assistent** > **Bandbreitenprofile** angelegten Profilnamens an; z. B.

```
&bandwidthprof=1
```

für den ersten Eintrag in der Tabelle.

Fehlt dieser Parameter oder die Zeilennummer ist ungültig (die Tabelle ist z. B. leer), nimmt der Assistent kein Begrenzung der Bandbreite vor.

Sind für fehlende Parameter in der Public Spot-Verwaltung keine Default-Werte angegeben, öffnet Ihnen der Assistent einen entsprechenden Dialog. Tragen Sie in diesen die fehlenden Werte ein.

Bearbeiten eines Public Spot-Benutzers

Über die folgende URL bearbeiten Sie einen oder mehrere Public Spot-Benutzer:

```
http://<Geräte-URL>/cmdpbspotuser/
   ?action=editpbspotuser&parameter1=value1&parameter2=value2&...
```

Ihnen stehen folgende Parameter zur Verfügung:

`pbspotuser`

Name des Public Spot-Benutzers

Mehrere Benutzer geben Sie in der Form `&pbspotuser=<Benutzer1>+<Benutzer2>+...` an.

Findet der Assistent den angegebenen Benutzer nicht, haben Sie die Möglichkeit nach einem Benutzer suchen.

Nach der Änderung übernehmen Sie diese und drucken Sie diese ggf. zusätzlich aus.

`expirytype`

Kombinierte Angabe von Ablauf-Typ und ggf. Verfallsdauer des Vouchers.

Geben Sie diesen Parameter wie folgt an:

```
&expirytype=<Wert1>+validper=<Wert2>
```

Die Parameter-Werte haben folgende Bedeutung:

- `Wert1`: Ablauf-Typ. Mögliche Werte sind `absolute`, `relative`, `both` und `none`.
- `Wert2`: Verfallsdauer des Vouchers, wenn `expirytype` den Wert `both` besitzt. In diesem Fall definieren Sie mittels `validper` die maximale Gültigkeit des Vouchers in Tagen für den absoluten Ablauf. Für alle anderen Ablauf-Typen wird der Parameter `validper` nicht gesetzt.

Fehlt ein Parameter oder geben Sie falsche Werte ein, setzt der Assistent die Default-Werte ein.

`unit`

Zugangsdauer

Geben Sie diesen Parameter wie folgt an:

```
&unit=<Wert1>+runtime=<Wert2>
```

Die Parameter-Werte haben folgende Bedeutung:

- `Wert1`: Einheit der Laufzeit. Mögliche Werte sind: Minute, Stunde, Tag
- `Wert2`: Laufzeit

`timebudget`

Zeit-Budget

Fehlt dieser Parameter, verwendet der Assistent den Default-Wert.

`volumebudget`

Volumen-Budget

Fehlt dieser Parameter, verwendet der Assistent den Default-Wert.

`print`

Automatischer Ausdruck des Vouchers.

Fehlt dieser Parameter, zeigt der Assistent anschließend eine entsprechende Schaltfläche. Über diese haben Sie die Möglichkeit den Voucher auszudrucken.

bandwidthprof

Bandbreitenprofil

Mit diesem Parameter weisen Sie einem Public Spot-Nutzer ein existierendes Bandbreitenprofil zu. Als gültigen Wert für diesen Parameter geben Sie die Zeilennummer eines unter **Setup** > **Public-Spot-Modul** > **Neuer-Benutzer-Assistent** > **Bandbreitenprofile** angelegten Profilnamens an; z. B.

```
&bandwidthprof=1
```

für den ersten Eintrag in der Tabelle.

Fehlt dieser Parameter oder die Zeilennummer ist ungültig (die Tabelle ist z. B. leer), nimmt der Assistent kein Begrenzung der Bandbreite vor.

Sind für fehlende Parameter in der Public Spot-Verwaltung keine Default-Werte angegeben, öffnet Ihnen der Assistent einen entsprechenden Dialog. Tragen Sie in diesem die fehlenden Werte ein.

Löschen eines Public Spot-Benutzers

Über die folgende URL löschen Sie einen oder mehrere Public Spot-Benutzer:

```
http://<Geräte-URL>/cmdpbspotuser/
   ?action=delpbspotuser&pbSpotuser=<Benutzer1>+<Benutzer2>+...
```

Findet der Assistent den angegebenen Benutzer in der Benutzer-Liste, löscht er ihn und gibt eine entsprechende Meldung aus.

Findet der Assistent den angegebenen Benutzer nicht, zeigt er Ihnen eine Tabelle der registrierten Public Spot-Benutzer. Markieren Sie in dieser die zu löschenden Einträge.

Public Spot-Benutzer auf einem entfernten Public Spot-Gateway anlegen

Bei der Verwendung von Smart Ticket erhält der Benutzer im RADIUS-Server des lokalen Public Spot-Gateways einen entsprechenden Public Spot-Account.

Sind jedoch mehrere Public Spot-Gateways im Einsatz und soll nur ein Gateway die Benutzerkonten in seinem RADIUS-Server vorhalten, wird der Public Spot-Account bei der Verwendung von Smart Ticket auf dem zentralen RADIUS-Server angelegt. Dazu ist es notwendig, das entfernte Public Spot-Gateway im LCOS-Menübaum unter **Setup** > **Public-Spot-Modul** > **Authentifizierungs-Module** festzulegen.

Sofern kein entferntes Public Spot-Gateway definiert wird, werden Public Spot-Benutzerkonten auf dem lokalen Public Spot-Gateway angelegt.

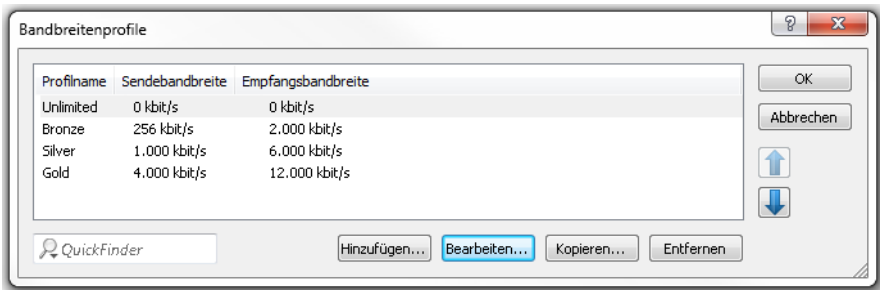
Bandbreitenprofile

Bandbreitenprofile verwalten

Über den Dialog **Public-Spot** > **Assistent** > **Bandbreitenprofile** haben Sie die Möglichkeit, Profile zur Beschränkung der Bandbreite (Uplink und Downlink) für Public Spot-Benutzer einzurichten. Wählen Sie je nach Bedarf zwischen vordefinierten Profilen oder erstellen Sie eigene Bandbreitenprofile. Diese Profile lassen sich neuen Benutzern beim Erstellen eines Zugangs für den Public Spot zuweisen, indem Sie im WEBconfig den Setup-Assistenten **Public-Spot-Benutzer einrichten** aufrufen.

Integration fertiger Bandbreitenprofile

Wählen Sie aus vier vordefinierten Profilen das Ihren Anforderungen entsprechende Bandbreitenprofil aus:



Unlimited

Keine Beschränkung in der Sende- und Empfangsbandbreite.

Diese Werte beziehen sich auf die Sendebandbreite (TX) und Empfangsbandbreite (RX) aus Sicht des Clients.

Bronze

Die Sendebandbreite (TX) beträgt 256 KBit/s, die Empfangsbandbreite (RX) 2 MBit/s.

Silver

Die Sendebandbreite (TX) beträgt 1 MBit/s, die Empfangsbandbreite (RX) 6 MBit/s.

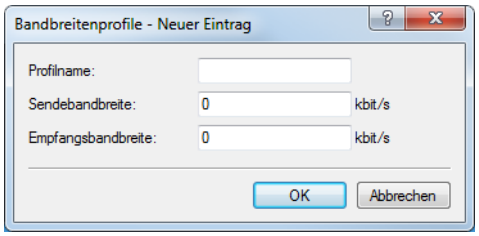
Gold

Die Sendebandbreite (TX) beträgt 4 MBit/s, die Empfangsbandbreite (RX) 12 MBit/s.

Sie haben die Möglichkeit, die fertigen Einträge Ihren Anforderungen entsprechend anzupassen. Markieren Sie dazu das zu bearbeitende Profil und klicken Sie auf die Schaltfläche **Bearbeiten**. Alternativ erstellen Sie eigene Profile.

Erstellen eigener Bandbreitenprofile

Um der Tabelle **Bandbreitenprofile** manuell Einträge hinzuzufügen, klicken Sie auf die Schaltfläche **Hinzufügen**.



Die Einträge im Bearbeitungsfenster haben folgende Bedeutung:

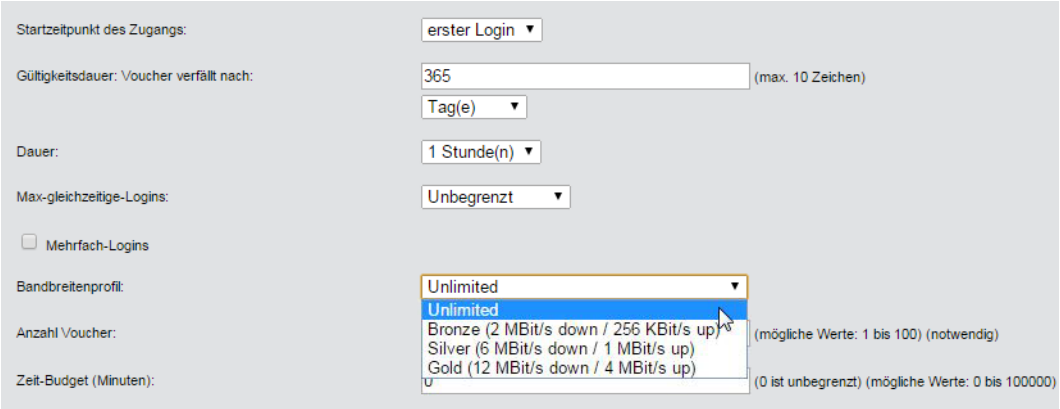
- **Profilname**: Geben Sie hier den Namen für das Bandbreitenprofil ein.
- **Sendebandbreite**: Geben Sie hier die maximale Bandbreite (in KBit/s) ein, die einem Public Spot-Benutzer im Uplink zur Verfügung stehen soll. Um die Bandbreite auf z. B. 1 MBit/s zu beschränken, tragen Sie den Wert `1024` ein.
- **Empfangsbandbreite**: Geben Sie hier die maximale Bandbreite (in KBit/s) ein, die einem Public Spot-Benutzer im Downlink zur Verfügung stehen soll. Um die Bandbreite auf z. B. 1 MBit/s zu beschränken, tragen Sie den Wert `1024` ein.

Bandbreitenprofile zuweisen

Die nachfolgenen Schritte erläutern, wie sie einem Public Spot-Nutzer eingerichtete Bandbreitenprofile zuweisen.

1. Öffnen Sie WEBconfig.

2. Starten Sie über **Setup-Wizards** > **Public Spot-Benutzer einrichten** den Benutzer-Erstellungs-Assistenten.
3. Weisen Sie dem neuen Benutzer aus der Auswahlliste **Bandbreitenprofil** ein entsprechendes Profil zu.



Beim Anlegen eines neuen Benutzers weist der RADIUS-Server dem dazugehörigen Konto automatisch die Ober- und Untergrenzen des betreffenden Bandbreitenprofils zu (nicht das Bandbreitenprofil an sich).

Benutzertabelle automatisch bereinigen

Das Gerät bietet Ihnen die Möglichkeit, abgelaufene Konten von Public Spot-Benutzern automatisch zu löschen.

Die Anwender des Public Spot-Assistenten haben als Administratoren in der Regel stark eingeschränkte Rechte und können Einträge in der Benutzertabelle daher nicht selbst löschen. Da die Benutzertabelle nur eine bestimmte Anzahl von Einträgen umfasst, können veraltete Einträge die Kapazität des Public Spot ggf. einschränken. Die Aktivierung dieser Option ist somit dringend zu empfehlen.

Sofern Sie den internen RADIUS-Server für die Verwaltung der Benutzerkonten verwenden, aktivieren Sie die automatische Bereinigung unter **RADIUS** > **Server** > **Benutzer-Datenbank** > **Benutzertabelle automatisch bereinigen**.

Diese Einstellung hat keine Auswirkungen auf die Benutzertabelle eines externen RADIUS-Servers!

Die nachfolgende Liste bietet Ihnen eine grobe Orientierung, welche Kapazitätsgrenzen für bestimmte Modellreihen gelten. Sollten Sie Ihr Gerät darin nicht wiederfinden, entnehmen Sie die genauen Angaben bitte der Produktbeschreibung.

Tabelle 1: Größe der Benutzertabelle bei ausgewählten LANCOM Modellen

LANCOM Modell	Größe der Benutzertabelle
mit Option **Public Spot**: › LANCOM LN-17xx-Serie › LANCOM L(N)-8xx › LANCOM LN-630acn › LANCOM L-3xx-Serie › LANCOM IAP-4G+ › LANCOM IAP-8xx-Serie › LANCOM IAP-5G › LANCOM OAP-8xx-Serie › LANCOM OAP-5G	64
› LANCOM vRouter 50 › LANCOM 178x-Serie › LANCOM 179x-Serie › LANCOM 18xx-Serie	128
› LANCOM 19xx-Serie	256

LANCOM Modell	Größe der Benutzertabelle
› LANCOM WLC-4006(+) › LANCOM vRouter 250 › LANCOM 2100 › LANCOM WLC-30 › LANCOM WLC-60	
› LANCOM vRouter 500 › LANCOM vRouter 1000 › LANCOM vRouter unlimited mit Option **Public Spot XL**: › LANCOM ISG-1000 › LANCOM ISG-4000 › LANCOM ISG-5000 › LANCOM ISG-8000 › LANCOM WLC-1000 › LANCOM WLC-2000	unbegrenzt*

*) Keine Limitierung der Tabelle, eine Obergrenze von max. 2.500 Benutzern ist jedoch empfehlenswert.

Stationsüberwachung

Bei eingeschalteter Stationsüberwachung überprüft der Public Spot regelmäßig alle angemeldeten Endgeräte daraufhin, ob sie auch tatsächlich erreichbar sind. Verschollene Endgeräte löscht er automatisch aus seiner lokalen Benutzertabelle. Bei ausgeschalteter Stationsüberwachung wird ein Benutzer erst dann abgemeldet, wenn die Gültigkeit seiner Authentifizierung abläuft.

Für kommerziell auf Zeitbasis betriebene Public-Spots ist die Stationsüberwachung außerordentlich wichtig. Bei solchen Installationen muss jederzeit gewährleistet sein, dass Benutzer nur für diejenigen Zeiten bezahlen, in denen sie die Dienste des Public-Spots auch tatsächlich in Anspruch genommen haben.

Konfiguration

Die Stationsüberwachung des Public Spot-Moduls ist standardmäßig deaktiviert. Sie aktivieren sie, indem Sie unter **Public-Spot** > **Server** > **Interface-Auswahl** > **Leerlaufzeitüberschreitung** einen Wert größer `0` – dieser Wert deaktiviert die Funktion – eintragen. Fortan werden alle Endgeräte nach einer bestimmten Zeit der Inaktivität automatisch vom Public Spot getrennt.

Sofern Ihr Public-Spot-Gerät über Wireless LAN verfügt, haben Sie zusätzlich die Möglichkeit, eine Stationsüberwachung global für alle WLAN-Schnittstellen zu aktivieren. Die dazugehörige Einstellung finden Sie unter **Wireless LAN** > **Security** > **Stationen überwachen, um inaktive Stationen zu erkennen**. Hierbei meldet das Gerät Mobilstationen nach spätestens 60 Sekunden ab (Vorgabewert); bei deaktivierter WLAN-Stationsüberwachung kann dies hingegen in der Standardeinstellung bis zu 15 Minuten dauern.

Sofern Sie Public-Spot über WLAN anbieten, beachten Sie bitte, dass die Stationsüberwachung für WLAN der für Public Spot übergeordnet ist, und eine Trennung früher erfolgen kann, wenn die Leerlaufzeitüberschreitung für WLAN (im Setup-Menü einstellbar unter **WLAN** > **Idle-Timeout**) geringer ist als die für Public Spot.

Überwachung

Im laufenden Betrieb können Sie den Public Spot via WEBconfig überwachen. Die Stations-Tabelle im Benutzer-Authentifizierungs-Menü gibt eine Aufstellung der

- aktuell am Public Spot angemeldeten Benutzer und der
- nicht angemeldeten Endgeräte im Netzwerk.

Sie erreichen die Stations-Tabelle im Status-Menü unter **Public-Spot** > **Stations-Tabelle**. Mit der Schaltfläche **Diese Tabelle beobachten** erneuern Sie die Ansicht der Tabelle automatisch und regelmäßig.

Übergabe von WLAN-Sitzungen zwischen Geräten

Wann immer der mit Hotspots zu versorgende Bereich größer wird, kann es erforderlich sein, mehr als nur einen Access Point einzusetzen. Eine mögliche Variante ist dann, ein zentrales Gerät für die Authentifizierung einzurichten, allein auf diesem Gerät das Public Spot-Modul zu aktivieren, und alle anderen Access Points dazu aufzufordern, die entsprechenden Anfragen an das zentrale Gerät weiterzuleiten. Damit fungieren alle übrigen Access Points als einfache, transparente Bridges, welche sich über das Ethernet-Backbone mit diesem zentralen Gateway verbinden. Das versetzt Benutzer in die Lage, sich mit Ihren Clients frei zwischen den Access Points zu bewegen, da alle Session-Informationen in dem zentralen Gateway gespeichert werden.

Diese Variante hat allerdings auch zwei Nachteile:

- Das zentrale Gateway ist ein "single point of failure" und skaliert zudem nicht mit den Anforderungen. Durch den Einsatz von VRRP zum Aufbau einer Redundanz-Lösung lässt sich das Ausfallrisiko minimieren.

  Da über VRRP keine Konfigurationen – wie z. B. die Benutzerdatenbank – abgeglichen werden, bedarf diese Lösung eines externen RADIUS-Servers. Dadurch stehen Ihnen jedoch auch bestimmte Funktionen (wie z. B. die Public Spot-Assistenten in WEBconfig) nicht mehr zur Verfügung.
- Roaming ist nur dann notwendig, wenn das Public Spot-Modul in den Access Points selbst eingerichtet ist. Wenn Sie einen WLAN-Controller verwenden, kann die Authentifizierung zum zentralen Gateway weitergeleitet werden. In diesem Fall ist das Roaming zwischen den Access Points für den WLAN-Controller transparent.

Eine Alternative zu diesem zentralisierten Aufbau ist das Aktivieren des Public Spot-Moduls in allen Access Points. Die Authentifizierung und Seiten-Ablaufsteuerung ist dadurch auf alle Geräte verteilt, und es existiert kein "single point of failure".

Inter Access Point Protocol (IAPP)

Da das Public Spot-Modul als eine "schaltbare" transparente Brigde implementiert ist, benötigen Clients keine neue IP-Adresse, wenn sie zu einem neuem Access Point roamen; offene Verbindungen werden daher auch nicht getrennt. Daraus ergibt sich allerdings die Anforderung, dass sich ein einmal authentifizierter Client nach dem Roamen zu einem anderen Access Point nicht erneut authentifizieren braucht. Die Authentifizierungsinformationen sollten also vom alten zum neuen Access Point mitgenommen werden.

Um Informationen über die roamenden Clients auszutauschen, verwenden Access Points deshalb das sogenannte Inter Access Point Protocol (IAPP): Wann immer ein WLAN-Client zu einem anderen Access Point wechselt, hat er die Möglichkeit, dem neuen Access Point mitzuteilen, mit welchem Access Point er vorher verbunden war. Diese Information erlauben – zusammen mit den regulären Hello-Paketen aus dem Ethernet-Backbone – dem neuen Access Point, den alten Access Point über den Wechsel zu informieren. Der alte Access Point kann daraufhin den Client aus seiner Stationstabelle austragen und die Übergabe bestätigen.

Sollte ein Client für die Verbindung zum neuen Access Point das entsprechende Reassociate-Paket nicht verwenden, sendet der neue Access Point eine Multicast-Übergabeanfrage über den Backbone, statt die Anfrage direkt an den alten Access Point zu richten. Daher funktioniert eine Übergabe auch für Clients, die das IAPP nicht unterstützen.

Die Hauptaufgabe des IAPPs in einem WLAN ist, den alten Access Point anzuweisen, keine Pakete mehr an den entsprechenden Client in seinem Funkbereich zu senden, weil dieser sie nicht mehr empfängt. Ein solches Verhalten könnte andernfalls (aufgrund der Beschaffenheit des 802.11-Frame-Austausch-Protokolls) zu Beeinträchtigungen der anderen mit ihm verbundenen Clients führen.

Wenn das Public Spot-Modul verwendet wird, dient der Kommunikationskanal, den das IAPP liefert, als Übertragungsmedium für Sitzungsinformationen über die WLAN-Clients. Immer dann, wenn ein Access Point eine Übergabeanfrage für einen seiner Clients erhält und für diesen Client über Sitzungsinformationen in seiner Stationstabelle verfügt, leitet er diese Informationen an den anfragenden Access Point weiter. Diese Information beinhalten:

- Den aktuellen Zustand des Clients (authentifiziert oder nicht authentifiziert)

  Für den Fall, dass der Client authentifiziert ist, zusätzlich noch:

- Den zur Authentifizierung verwendeten Benutzernamen
- Den bisher vom Client erzeugten Datenverkehr
- Die bisher verstrichene Sitzungsdauer
- Die IP-Adresse des Clients
- Mögliche Limits zu Sitzungsdauer und Datenvolumen
- Mögliche Angaben zur Leerlauf-Zeitüberschreitung

- Wenn RADIUS-Accounting für die Sitzung verwendet wurde:
  - Den für das RADIUS-Accounting verwendeten Eintrag in der Anmelde-Server-Liste, referenziert durch den Namen
  - Den für die Interim-Updates verwendeten Accounting-Zyklus

Nach erfolgreicher Übergabe beendet der alte Access Point die Sitzung; d. h. er sendet im Falle von RADIUS-Accounting eine Accounting-Stop-Anfrage an den RADIUS-Accounting-Server. Diese ist erforderlich, da ein RADIUS-Server die NAS-Identifizierung nutzen kann, um Anfragen bestimmten Sitzungen zuzuordnen, und er diese Anfragen nicht mehr der richtigen Sitzung zuordnen kann, sobald er die Datenpakete zu einer Sitzung von mehreren Geräten bekommt. Wenn ein Access Point diese Informationen in einer Übergabeantwort erhält, markiert er den Client sofort als authentifiziert und startet nach Möglichkeit eine neue RADIUS-Accounting-Session.

Beachten Sie, dass der neue Access Point einen entsprechenden Eintrag in seiner **Anmelde-Server**-Liste benötigt, um die hierfür benötigten Informationen zu erhalten. Der für das Public Spot-Modul spezifische Teil einer Übergabeantwort ist durch ein "shared secret" geschützt, welches im Setup-Menü unter **Public-Spot-Modul** > **Roaming-Schluessel**. Diese Sicherheitsmaßnahme soll das Fälschen von Übergabeantworten verhindern. Ohne ein konfiguriertes Passwort hängt ein Access Point die oben angeführten Informationen nicht an eine Übergabeantwort an, was den Client zwingt, sich erneut zu authentifizieren.

Authentifizierung über RADIUS

RADIUS ist ein weitläufig anerkanntes Protokoll, um auch größeren Benutzergruppen den Zugang zu einem Server bereitzustellen. Ursprünglich für den Dial-in-Serverzugang über Telefonleitungen entwickelt, eignet sich das Konzept ebenfalls für den Authentifizierungsprozess eines Hotspots. In einem komplexeren Provider-Netzwerk lässt sich dadurch z. B. dieselbe Benutzerbasis sowohl für Zugänge über Dial-in als auch via Hotspot verwenden. RADIUS-Server und ihre Zugangsparameter konfigurieren Sie im Dialog **Public-Spot** > **Benutzer** > **Benutzer und RADIUS-Server** unter **RADIUS-Server**.

In bestimmten Szenarien kann es sinnvoll sein, mehr als nur einen RADIUS-Server einzusetzen. Generell wird ein RADIUS-Server durch seine IP-Adresse, den UPD-Port (typischerweise Port 1645 oder 1812) und das sogenannte "shared secret" spezifiziert. Dies ist eine beliebige Zeichenfolge, welche als Passwort für den Zugang zum Server fungiert. Nur Clients, die das shared secret kennen, können mit dem RADIUS-Server interagieren, da das Passwort des Benutzerkontos mit dem shared secret gehashed wird, anstatt es im Klartext zu übermitteln.

Bei Verwendung eines eigenen externen Hotspot-Gateways ist es möglich, Public Spot-Sessions anzupassen, nachdem die Anmeldung des Benutzers bereits erfolgt ist. Dies ist durch die dynamische Autorisierung durch RADIUS CoA realisierbar (siehe *Dynamische Autorisierung durch RADIUS CoA (Change of Authorization)* auf Seite 178 und *Annahme von RADIUS-CoA-Requests im Public Spot aktivieren* auf Seite 55).

Die einfachste Transaktion zwischen einem RADIUS-Server und einem Client besteht aus dem Übermitteln der eingegebenen Benutzerdaten durch das Gerät und der Antwort des Server mit "ja" oder "nein". Das RADIUS-Protokoll erlaubt allerdings auch komplexere Antworten und Anfragen, bei denen die Kommunikationspartner für Anfragen und Anworten eine variable Liste von Werten – sogenannte "Attribute" – verwenden.

Im *Anhang* finden Sie eine Liste, welche Attribute Ihr Gerät an einen RADIUS-Server senden kann und welche Attribute einer RADIUS-Antwort Ihr Gerät versteht.

Annahme von RADIUS-CoA-Requests im Public Spot aktivieren

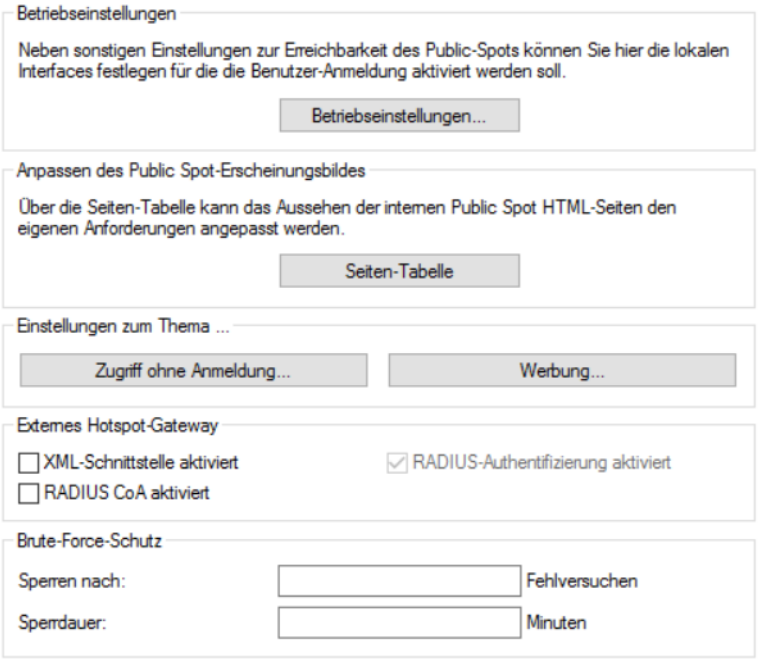
- Die nachfolgenden Handlungsschritte setzen einen funktionierenden Public Spot voraus, welcher an ein externes Hotspot-Gateway angebunden werden kann.

› Das externe Hotspot-Gateway befindet sich entweder in einem frei zugänglichen Netz des Public Spots oder seine Adresse gehört zur Liste der freien Hosts.

Alternativ zu einem XML-basierten `RADIUS_COA_REQUEST`s über das XML-Interface kann der Public Spot auch CoA-Requests über das RADIUS-Protokoll von einem externen Hotspot-Gateway oder einem externen RADIUS-Server entgegen nehmen. Sie haben jedoch auch die Möglichkeit, beide Formen der Befehlsübermittlung parallel zu nutzen.

Der folgende Abschnitt erläutert, wie Sie die RADIUS-CoA-Unterstützung nach RFC3576 im Public Spot aktivieren.

1. Öffnen Sie die Gerätekonfiguration in LANconfig und wechseln Sie in die Ansicht **Public-Spot** > **Server**.



2. Wählen Sie **RADIUS CoA aktiviert** an.
3. Schreiben Sie die Konfiguration zurück in das Gerät.

Der Public Spot verarbeitet fortan RADIUS-CoA-Requests, die von einem externen Hotspot-Gateway eingehen.

Multiple Anmelde-Server

Wie erwähnt, kann die Liste der Anmelde-Server mehr als nur einen Eintrag beinhalten. Es sind Szenarios denkbar, in denen ein Hotspot den Internetzugang für Kunden verschiedener Service-Provider (Anbieter) bereitstellt. Diese Anbieter haben möglicherweise getrennte Benutzerdatenbanken und eigene RADIUS-Server. Das Gerät muss dann anhand des Benutzernamens entscheiden, welcher Anbieter zum betreffenden Benutzer gehört.

Immer, wenn das Gerät für einen zu authentifizierenden Benutzer keinen Eintrag in eigenen, internen Benutzerliste vorfindet, geht es die Liste der Anmelde-Server durch und versucht den Anbieter zu finden, der zu dem betreffenden Benutzer gehört. Der Eintrag `Max.Mustermann@mydomain.de` enthält beispielsweise den Anmelde-Server-Eintrag `MYDOMAIN`. Scheitert diese erste Zuordnung, versucht das Gerät, dem Benutzer den Eintrag `DEFAULT` zuzuordnen.

Sofern auch dieser Eintrag nicht existiert, wählt das Gerät den Anmelde-Server, in der Liste an erster Stelle steht. Findet das Gerät auch hier keinen Eintrag (d. h. die Liste ist leer), schlägt die Benutzerauthentifizierung fehl.

Unabhängig von der Zuordnung eines Benutzers zum Anmeldeserver übermittelt Ihr Gerät stets den vollen Benutzername an den ausgewählten RADIUS-Server. Der ausgewählte RADIUS-Server wird als Anbieter für die anschließende Sitzung gespeichert und für das optionale RADIUS-Accounting verwendet.

Verkettung von Backup-Servern

Internetanbieter wünschen sich eine hohe Verfügbarkeit ihres Angebots und eine übliche Methode, dies zu erreichen, ist Redundanz. Diese Redundanz wird über Backup-Servers erreicht, welche immer dann angefragt werden, wenn die Anfrage auf den primären Server eine Zeitüberschreitung erzeugt hat, z. B. weil der Server selbst oder andere Netzwerkkomponenten auf dem Weg dahin unerreichbar sind.

Der Bedarf an Backup-Servern variiert dabei stark zwischen den unterschiedlichen Anbietern, weshalb die Liste der Anmeldeserver keine fixe Anzahl von Eingabefeldern vorgibt. Stattdessen bietet Ihnen das Gerät eine Verkettung von Backup-Servern an (Backup-Chaining). Hierbei werden zwei oder mehr Einträge der Anmelde-Server-Liste miteinander verkettet, um eine Abfolge von RADIUS-Servern zu erstellen. Das Gerät arbeitet diese Liste Glied für Glied ab, bis es das Ende erreicht hat (Scheitern der Authentifizierung wegen Nicht-Erreichbarkeit des Servers) oder eine Antwort erhält (entweder Positiv oder Negativ).

Sie verketten Backup-Server über das Eingabefeld **Backup-Name** im Hinzufügen-/Bearbeiten-Dialog unter **Public-Spot** > **Server** > **Anmelde-Server**. Wann immer eine RADIUS-Anfrage scheitert (also eine Zeitüberschreitung erzeugt), prüft das Gerät das Backup-Feld und versucht, den darin referenzierten Server zu erreichen. Grundsätzlich lässt sich damit eine beliebige Anzahl von Servern miteinander verketten, wodurch auch die Möglichkeit besteht, mehreren Providern denselben Fallback-Server zuzuweisen. Die Kette von Backup-Servern wird dann abgebrochen, wenn eines der folgenden Ereignisse auftritt:

- Das Anfragen eines RADIUS-Servers ist fehlgeschlagen und der dazugehörige Eintrag der Anmelde-Server-Liste hat ein leeres Backup-Feld.
- Das Anfragen eines RADIUS-Servers ist fehlgeschlagen und der dazugehörige Eintrag der Anmelde-Server-Liste hat ein ungültiges Backup-Feld, der referenzierte Eintrag lässt sich also nicht in der Anmelde-Server-Liste finden.
- Das Anfragen eines RADIUS-Servers ist fehlgeschlagen und der dazugehörige Eintrag der Anmelde-Server-Liste referenziert einen Eintrag, den das Gerät bereits zu erreichen versucht hat. Dadurch werden endlose RADIUS-Anfragen durch Kreisverkettungen verhindert. Es ist möglich, dass zwei RADIUS-Server einander als Backup angeben, während der primäre Server durch den Benutzernamen gewählt wird.

Während das Gerät eine RADIUS-Anfrage sendet, bleibt die TCP/HTTP-Verbindung zum Client weiterhin bestehen. Überschreitet die Laufzeit der Verkettung irgendwann die Laufzeit der TCP/HTTP-Verbindung, bricht der Client den Anmeldeversuch ab. Es kann daher empfehlenswert sein, die Zahl der Anfrage-Wiederholungen an die einzelnen Backup-Server sowie die Zeitspanne zwischen Anfragen zu verringern. Sie tätigen diese Einstellungen im Dialog **RADIUS** > **Server** > **Erweiterte Einstellungen** > **Optionen**.

Abrechnung ohne RADIUS-Accounting-Server

Sofern die Benutzerverwaltung über die interne Benutzer-Liste des Public Spot-Moduls stattfindet und Sie keinen RADIUS-Accounting-Server einsetzen wollen, können Sie lediglich das Ablaufdatum der Benutzerkonten für Abrechnungszwecke verwenden.

Die Verwendung der internen Benutzer-Liste wird nicht mehr empfohlen. Verwenden Sie für neue Installationen stattdessen den internen RADIUS-Server zur Benutzerverwaltung und zum Accouting, um vom vollen Funktionsumfang des Public Spots zu profitieren.

Für Abrechnungsmodelle auf Kredit-Basis kann der Public Spot per SYSLOG detaillierte Verbindungsinformationen an beliebige Rechner im Netzwerk ausgeben. Bei Einsatz entsprechender Software auf dem Zielrechner können Sie die tatsächlich verwendeten Ressourcen (Verbindungszeiten oder Transfervolumen) exakt abrechnen.

Abrechnung über RADIUS-Accounting-Server

Bei Abrechnung über einen RADIUS-Server können Sie den Public Spot so einstellen, dass er regelmäßig aktuelle Verbindungsinformationen über jeden aktiven Benutzer an den angegebenen Accounting-Server ausgibt. Ein Accounting wird immer dann gestartet, wenn ein Client über RADIUS authentifiziert wurde und in der **Anmelde-Server**-Liste für den betreffenden **Authentifizierungs-Server** auch ein gültiger **Accounting-Server** konfiguriert ist. Es ist daher auch möglich, verschiedene RADIUS-Server für Accounting und Authentifizierung zu verwenden.

Jedes der regelmäßigen Meldepakete an den Accounting-Server enthält Angaben darüber, welche Ressourcen (Zeit, übertragene Datenmenge, etc.) der Benutzer seit der letzten Meldung verbraucht hat. So gehen bei einem Ausfall eines Public Spots (etwa durch Stromausfall o. ä.) auch im schlimmsten Fall nur wenige Abrechnungsinformationen verloren.

Die regelmäßige Meldung der Abrechnungsinformationen an den Accounting-Server (Interim-Updates) ist in der Voreinstellung ausgeschaltet. Die Aktivierung erfolgt, wenn Sie den Meldezyklus größer 0 festlegen.

› LANconfig: **Public-Spot** > **Benutzer** > **Update-Zyklus**

Der Meldezyklus wird in Sekunden angegeben. Er bestimmt den Zeitabstand, in dem Ihr Gerät regelmäßig Verbindungsinformationen an den Accounting-Server sendet. Ein Meldezyklus von `0` Sekunden deaktiviert die Funktion. In diesem Fall sendet Ihr Gerät nur zu Beginn und am Ende einer Sitzung Abrechnungsinformationen.

Bei Einsatz von Abrechnungsmodellen auf Guthabenbasis (PrePaid) übernimmt der RADIUS-Server die Überwachung der festgelegten Nutzungsbeschränkungen (Kontingente für Verbindungszeit oder Transfervolumen, Ablaufdatum). Sobald ein Benutzer sein Guthaben aufgebraucht hat, sperrt der RADIUS-Server das Benutzerkonto. Ihr Gerät weist künftige Anmeldeversuche des Benutzers daraufhin ab.

Zeitkontingente für PrePaid-Modelle kann der Public Spot auch während der aktiven Sitzungen überwachen. Wird ein Zeitguthaben vollständig aufgebraucht, so beendet der Public Spot automatisch die betreffende Sitzung. Die Guthabenüberwachung wird eingeschaltet, indem der RADIUS-Server zum Sitzungsbeginn eines Benutzers dessen Zeitguthaben als Attribut "Session Timeout" an den Public Spot übermittelt.

Anfragetypen

Ihr Gerät ist in der Lage, verschiedene Typen von RADIUS-Anfragen an einen Accounting-Server zu senden. Diese Anfragen unterscheiden sich nach je nach Sitzungsstatus eines Benutzers:

› Ein Accounting-Start wird nach einer erfolgreichen Authentifizierung gesendet.
› Ein Accounting-Stop wird nach Beenden einer Public Spot-Sitzung gesendet.
› Optional: Zwischenzeitliche Aktualisierungen (Interim-Updates) werden während der Sitzung gesendet.

Es gibt zwei Arten von Interim-Updates: Ein initiales Update wird im direkten Anschluss an die Start-Anfrage gesendet, da einige RADIUS-Server dieses benötigen, um eine Sitzung in ihrer Accounting-Datenbank anzulegen. Alle weiteren Updates sind davon abhängig, ob ein Accounting-Zyklus für die jeweilige Sitzung definiert wurde (unter **Public-Spot** > **Benutzer** > **Update-Zyklus**).

Alternativ kann dieser Wert auch Bestandteil einer RADIUS-Authentifizierungs-Antwort sein: Dabei bietet der RADIUS-Server einem RADIUS-Client (also z. B. Ihrem Public Spot) ein Accounting-Interim-Intervall an, welches der Client bei entsprechender Unterstützung übernimmt, sofern für ihn lokal kein eigenes Intervall definiert wurde.

Sofern ein lokaler Wert gesetzt wurde, wird dieser immer höher priorisiert als der von einem RADIUS-Server gelieferte Wert, welchen die RADIUS RFCs standardmäßig fordern!

Im *Anhang* finden Sie eine Liste, welche Attribute Ihr Gerät an einen RADIUS-Server senden kann und welche Attribute einer RADIUS-Antwort Ihr Gerät versteht.

Accounting-Backup

Die Backup-Lösung für das RADIUS-Accounting entspricht der für die RADIUS-Authentifizierung, d. h. Ihr Gerät arbeitet die in der Anmelde-Server-Liste angelegten Einträge nach und nach ab (siehe Kapitel *Verkettung von Backup-Servern*). Die Backup-Einträge für die Accouting-Server sollten dabei mit derselben Umsicht gewählt werden wie die für die Authentifizierungs-Server: Sofern Sie mehrere Backup-Server verwenden, müssen sie ggf. Werte für Wiederholung und Zeitüberschreitung der Anfragen anpassen, um eine gute Erreichbarkeit des Gesamtsystems zu erreichen.

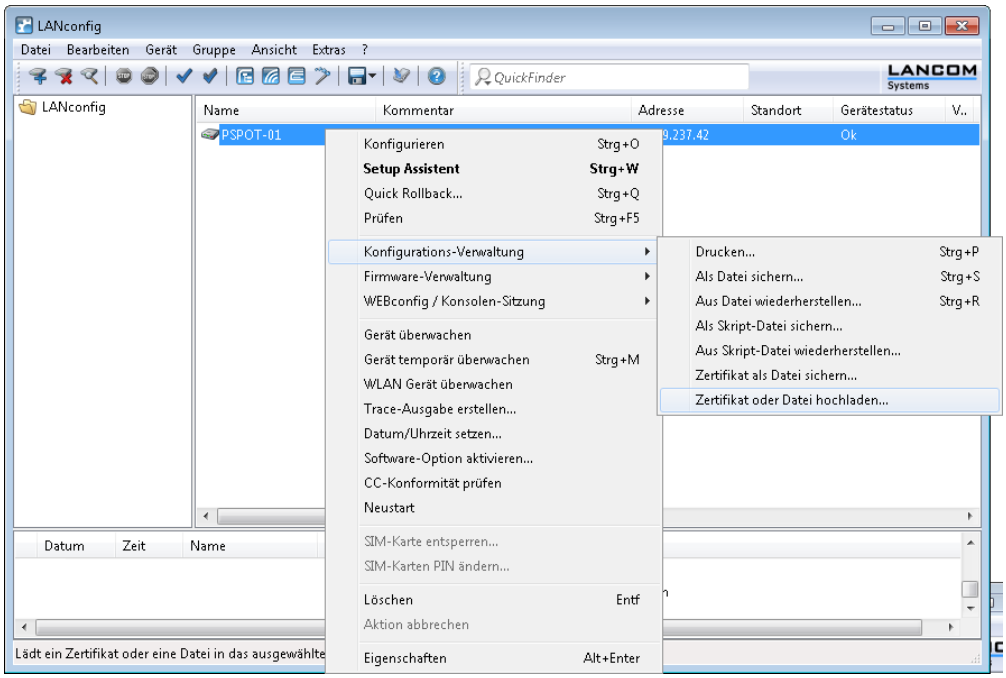
Während das Gerät Accounting-Anfragen sendet, werden laufende Benutzersitzungen nicht angehalten, was – im Gegensatz zur Authentifizierung – zusätzliche Ressourcen im Gerät verbraucht. Bitte achten Sie darauf, dass der Zeitbedarf für die Auswahl eines Accounting-Servers* geringer ausfällt als die Länge eines Accounting-Zyklusses bei Interim-Update-Anfragen. Somit vermeiden Sie einen Anfragestau und daraus resultierenden Stapelüberlauf.

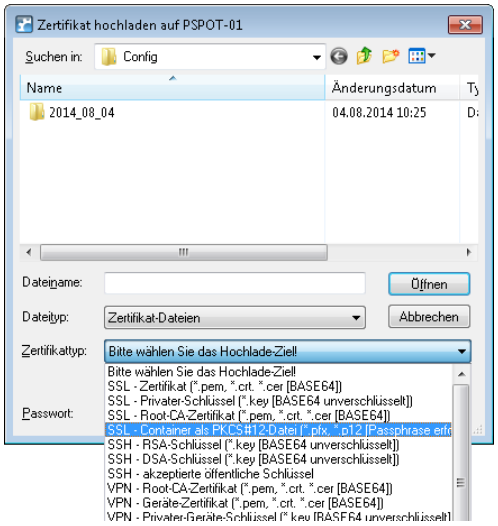
**Anzahl Backups x (Leerlaufzeit-Überschreitung + Anzahl Wiederholungen)*

Mehrstufige Zertifikate für Public Spots

SSL-Zertifikatsketten können in Form eines PKCS#12-Containers in das Gerät geladen werden. Diese Zertifikatsketten können für die Public Spot-Authentifizierungsseiten über den im Gerät implementierten HTTPS-Server verwendet werden. Zertifikate von allgemein anerkannten Trust-Centern sind üblicherweise mehrstufig. Offiziell signierte Zertifikate im Public Spot sind notwendig, um Zertifikatsfehlermeldungen des Browsers bei Public Spot-Authentifizierungen zu vermeiden.

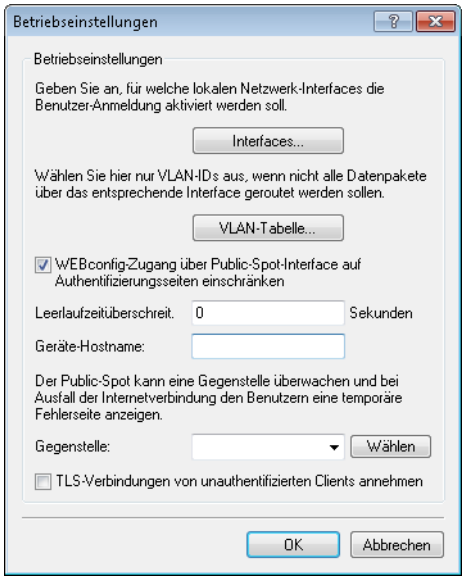
Das Zertifikat laden Sie über LANconfig im Dateimanagement mit den einzelnen Dateien des Root-CA-Zertifikats oder als PKCS#12-Container in das Gerät:





Da Zertifikate üblicherweise auf DNS-Namen ausgestellt werden, muss der Public Spot anstelle einer internen IP-Adresse den DNS-Namen des Zertifikats als Ziel angeben (einzugeben unter **Public-Spot** > **Server** > **Betriebseinstellungen**

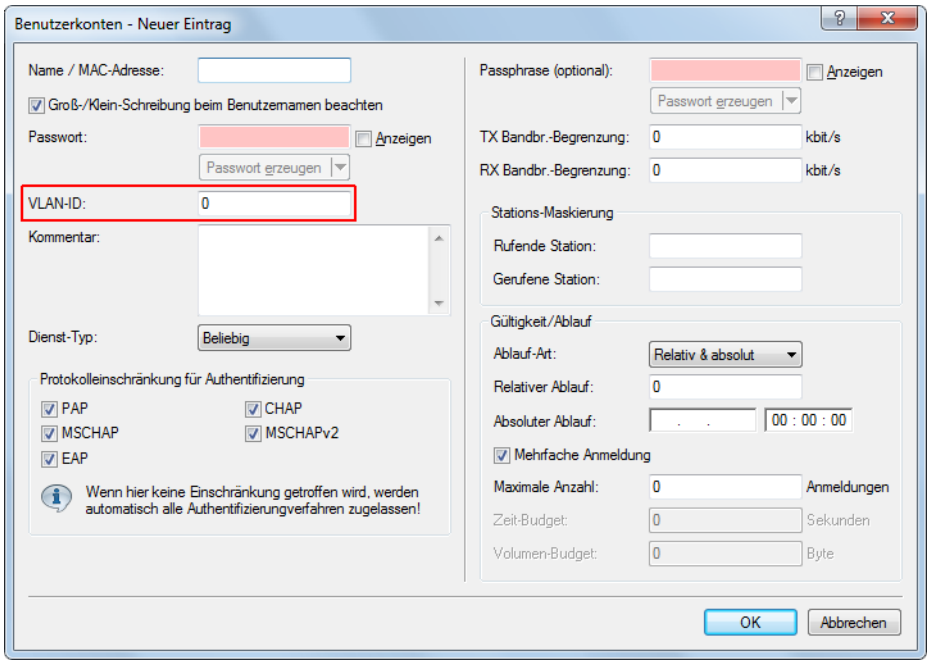
bei **Geräte-Hostname**). Dieser Name muss im DNS-Server auf die entsprechende IP-Adresse des Public Spots aufgelöst werden.



Benutzern individuelle VLANs zuweisen

Unabhängig von der Zuweisung einer VLAN-ID für das gesamte Public Spot-Modul bietet Ihnen das Gerät die Möglichkeit, individuelle VLAN-IDs für einzelne Public Spot-Benutzer zu vergeben. Diese ID wird Ihren Benutzern im Anschluss an eine erfolgreiche Authentifizierung automatisch vom RADIUS-Server zugewiesen. Auf diese Weise ist es z. B. möglich, unterschiedliche Public Spot-Nutzer in getrennte Netze mit verschiedenen Rechten und Zugriffsmöglichkeiten einzuordnen, ohne dass sich diese an getrennten SSIDs anmelden oder Sie die Verfügbarkeit verschiedener Netze öffentlich aussenden müssen (z. B. Netze für unterschiedliche Kunden-Typen). Die entsprechenden Regeln lassen sich über die Firewall realisieren, indem Sie als Quell-Tag die VLAN-ID des betreffenden Nutzers / der betreffenden Nutzergruppe angeben.

Vorraussetzung für die oben beschrieben Funktionen ist ein aktiviertes VLAN-Modul.



- Öffnen Sie die Tabelle **Benutzerkonten** im Dialog **RADIUS** > **Server** > **Benutzer-Datenbank** und klicken Sie auf **Hinzufügen...**, um einen neuen Benutzer zu erstellen.
- Weisen Sie dem neuen Benutzer eine individuelle VLAN-ID über das Eingabefeld **VLAN-ID** zu. Die individuelle VLAN-ID überschreibt nach der Authentifizierung durch den RADIUS-Server eine globale VLAN-ID, die ein Nutzer ansonsten über das Interface erhalten würde. Der Wert `0` deaktiviert die Zuweisung einer individuellen VLAN-ID.

Die Vergabe einer VLAN-ID erfordert technisch bedingt die erneute Adresszuweisung durch den DHCP-Server. Solange ein Client nach der erfolgreichen Authentifizierung noch keine neue Adresse zugewiesen bekommen hat, befindet sich er sich nachwievor in seinem bisherigen (z. B. ungetaggten) Netz. Damit der Client möglichst rasch in das neue Netz überführt wird, ist es notwendig, die Lease-Time des DHCP-Servers unter **IPv4** > **DHCPv4** möglichst gering einzustellen. Mögliche Werte (in Minuten) sind z. B.:

- **Maximale Gültigkeit:** `2`
- **Standard-Gültigkeit:** `1`

Berücksichtigen Sie dabei, dass eine derart starke Verkürzung der globalen Lease-Time Ihr Netz bedingt mit DHCP-Nachrichten flutet und bei größeren Nutzerzahlen zu einer gesteigerten Netzlast führt! Alternativ haben Sie die Möglichkeit, einen externen DHCP-Server einzusetzen oder Ihre Nutzer manuell – über ihren Client – eine neue Adresse anfordern zu lassen. In der Windows-Kommandozeile erfolgt dies z. B. über die Befehle `ipconfig /release` und `ipconfig /renew`.

Durch die Zuweisung einer VLAN-ID verliert ein Nutzer nach Ablauf des initialen DHCP-Leases seine Verbindung! Erst ab dem zweiten Lease – also nach erfolgter Zuweisung der VLAN-ID – bleibt die Verbindung konstant.

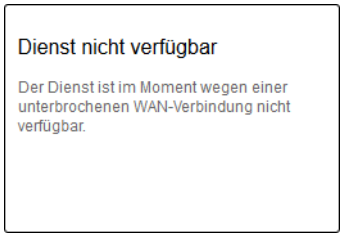
Fehlerseite bei Wegfall der WAN-Verbindung einrichten

Sie haben die Möglichkeit, das Public Spot-Modul gegenüber noch nicht authentifizierten Benutzern – zusätzlich zu den allgemeinen Anmeldefehlern – auch WAN-Verbindungsfehler ausgeben zu lassen. Dadurch werden mögliche Benutzer bereits vorab über die fehlende Verfügbarkeit des Netzwerks informiert. Die entsprechende Variante der **Fehler**-Seite erscheint immer dann, wenn das Public Spot-Modul einen Wegfall der WAN-Verbindung registriert.

Damit die Anzeige der Fehlerseite für diesen Fall korrekt funktioniert, **muss** eine entsprechende Gegenstelle benannt sein, deren Verbindungsstatus das Public Spot-Modul überwacht. Tragen Sie dazu im Dialog **Public-Spot** > **Server** eine entsprechende **Gegenstelle** ein. Über die Schaltfläche **Wählen** können Sie dem Auswahl-Eingabefeld bequem eine bereits eingerichtete oder neue Gegenstelle zuweisen.

Ohne Benennung einer zu überwachenden Gegenstelle deaktiviert das Public Spot-Modul die Ausgabe von Verbindungsfehlern auf der Fehlerseite. Ein Wegfall der WAN-Verbindung führt dann bei unauthentifizierten Benutzern stattdessen zu einem Verbindungs-Timeout in ihrem Browser.

Innerhalb einer individuellen Fehlerseite verwenden Sie den Bezeichner `LOGINERRORMSG`, um die Fehlermeldung des LCOS bei Wegfall der WAN-Verbindung einzufügen. Im Falle eines WAN-Verbindungsfehlers wird dann die folgende Fehlermeldung ausgegeben:



Bereits authentifizierte Benutzer hingegen erhalten unabhängig von der Fehlerseite immer eine entsprechende Fehlermeldung von ihrem Browser.

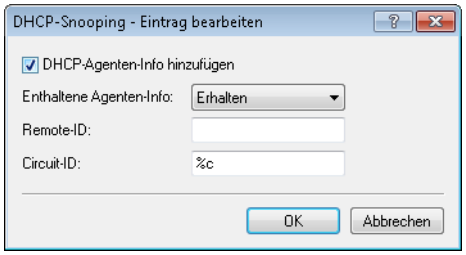
AP-spezifische Anmeldung an einem zentralen Public Spot

Ein zentraler WLC verwaltet in einer verteilten Infrastruktur einen Public Spot, dessen Konfiguration (Public Spot-SSID, Sicherheitsstandards) auf allen beteiligten APs entsprechend identisch ist. Auf diesem Weg kann ein Public Spot-Anbieter z. B. in allen seinen räumlich getrennten Filialen einen identischen Public Spot zur Verfügung stellen.

Die Kunden hätten also nach dem Erhalt eines Vouchers in jeder Filiale Zugriff auf diesen Public Spot. Um dennoch die Nutzung auf die Filiale zu beschränken, in der der Kunde den Voucher erhalten hat, überträgt der AP zusätzlich zu Username und Passwort auch seine Kennung. Diese Kennung ermöglicht die Zuordnung des Vouchers zu diesem AP. Der AP nutzt für die Übertragung der Kennung die Circuit-ID (DHCP-Option 82), die er den DHCP-Requests anhängt. Diese DHCP-Pakete durchlaufen den zentralen Public Spot, der die Kennung anhand der Einträge in der RADIUS-User-Tabelle überprüft.

Der Public Spot lässt diese Anfrage nur zu, wenn diesem Voucher in der RADIUS-User-Tabelle auch dieser AP zugeordnet ist. Kunden, die einen Voucher in Filiale A erhalten haben, können sich also nicht in der Filiale B am gleichen Public Spot anmelden, da beide Filial-APs unterschiedliche Kennungen übertragen.

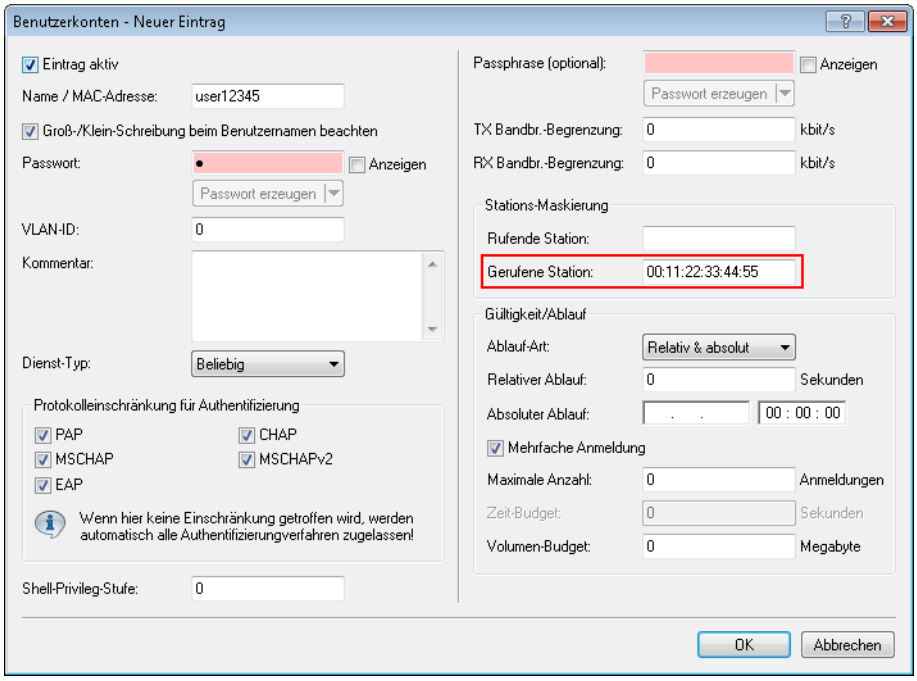
Die AP-Kennung konfigurieren Sie als Circuit-ID unter **Schnittstellen** > **Snooping** > **DHCP-Snooping** bei der entsprechenden Schnittstelle ein.



Sie können die folgenden Variablen verwenden:

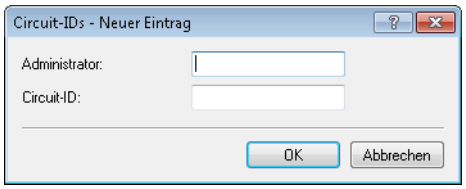
- **%%**: fügt ein Prozent-Zeichen ein.
- **%c**: fügt die MAC-Adresse der Schnittstelle ein, auf der sich der Public Spot-User anmeldet. Handelt es sich um eine WLAN-SSID, ist das die entsprechende BSSID.
- **%i**: fügt den Namen der Schnittstelle ein, auf der sich der Public Spot-User anmeldet.
- **%n**: fügt den Namen des APs ein, wie er z. B. unter **Management** > **Allgemein** festgelegt ist.
- **%v**: fügt die VLAN-ID des DHCP-Request-Paketes ein. Diese VLAN-ID stammt entweder direkt aus dem VLAN-Header des DHCP-Datenpakets oder aus der VLAN-ID-Zuordnung für diese Schnittstelle.
- **%p**: fügt den Namen der Ethernet-Schnittstelle ein, die das DHCP-Datenpaket empfangen hat. Diese Variable ist hilfreich bei Geräten mit eingebautem Ethernet-Switch oder Ethernet-Mapper, da diese mehr als eine physikalische Schnittstelle auf eine logische Schnittstelle mappen können. Bei anderen Geräten sind **%p** und **%i** identisch.
- **%s**: fügt die WLAN-SSID ein, wenn die Anmeldung über einen WLAN-Client erfolgt. Bei anderen Clients enthält diese Variable einen leeren String.
- **%e**: fügt die Seriennummer des APs ein, wie sie z. B. unter **Management** > **Allgemein** zu finden ist.

Im WLC konfigurieren Sie diese Kennung in der RADIUS-User-Tabelle unter **RADIUS** > **Server** > **Benutzer-Datenbank** > **Benutzerkonten**.



Als „Gerufene Station" fügen Sie die Kennung des APs ein, der den entsprechenden Voucher-Zugriff ermöglichen soll.

Der Public Spot-Setup-Assistent kann bei der Einrichtung neuer Public Spot-Nutzer automatisch die Kennung des Gerätes übernehmen, wenn diese unter **Public-Spot** > **Assistent** > **Circuit-IDs** konfiguriert ist.



Der Setup-Assistent prüft beim Anlegen eines neuen Public Spot-Nutzers, ob für den angemeldeten **Administrator** ein Eintrag in dieser Tabelle hinterlegt ist. Ist das der Fall, übernimmt der Setup-Assistent die entsprechende **Circuit-ID** als „gerufene Station" in die RADIUS-User-Tabelle.

Redirect für HTTPS-Verbindungen

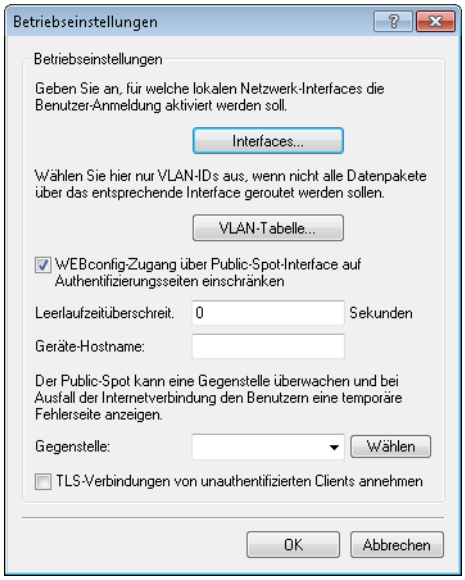
Versucht ein nicht angemeldeter Client über eine Schnittstelle, für die der Public Spot aktiv ist, via HTTPS auf eine Webseite zuzugreifen, wird diese Verbindungsanfrage an das Public Spot-Gateway selber umgeleitet, um dem Nutzer die Anmeldeseite zu präsentieren (ist bei HTTP auch der Fall). In diesem Fall wird dem Benutzer normalerweise eine Zertifikatswarnung seines Browsers präsentiert, da Name oder IP der ursprünglich angesurften Seite nicht dem Namen oder der IP des Public Spot entspricht. Um dies und die Erzeugung von erhöhter Last durch die aufgebauten HTTPS-/TLS-Verbindungen auf dem Public Spot Gateway zu verhindern, können Sie mit dieser Einstellung der Verbindungsaufbau über HTTPS für unangemeldete Clients verhindern.

Ist der Client einmal angemeldet, findet keinerlei Umleitung mehr statt und es können beliebig HTTP- und HTTPS-Verbindungen durch den Client aufgebaut werden.

Heutzutage übliche Clients führen eine "Captive Portal Detection" via HTTP durch. Dabei wird versucht, auf eine bestimmte URL via HTTP zuzugreifen, um das Vorhandensein einer Anmeldeseite (durch Public Spot oder andere Lösungen) zu überprüfen. Dieser Mechanismus wird durch das Ausschalten der HTTPS-Umleitung nicht beeinflusst, da die Erkennung normalerweise über HTTP stattfindet.

Ist es in einem Public Spot-Szenario jedoch nicht vorgesehen, dass unbekannte WLAN-Clients eine Verbindungsanfrage auch über HTTP ausführen sollen, würde dieser wirkungslose HTTPS-Redirect das Public Spot-Gateway unnötig belasten. Entsprechend ist es möglich, diesen HTTPS-Redirect prinzipiell zu deaktivieren. In diesem Fall würde der Benutzer vom Browser eine leere Seite erhalten.

Das Redirect für HTTPS-Verbindungen konfigurieren Sie im LANconfig unter **Public-Spot** > **Server** > **Betriebseinstellungen**.



Um das HTTPS-Redirect einzuschalten, aktivieren Sie die Option **TLS-Verbindungen von unauthentifizierten Clients annehmen**. In der Standardeinstellung ist diese Option deaktiviert.

Schutz vor Brute Force-Angriffen

Brute-Force-Angriffe sind die bekanntesten Angriffe auf ein Netzwerk. Diese Art von Angriff besteht darin, eine Menge an möglichen Passwörtern innerhalb kurzer Zeit auszuprobieren, bis das richtige Passwort gefunden wird. Ein möglicher Schutz vor Brute-Force-Angriffen besteht darin, nach einem oder mehreren aufeinander folgenden fehlgeschlagenen Eingabeversuchen die Zeit bis zur nächsten möglichen Eingabe zu verzögern.

Den Schutz vor Brute-Force-Angriffen konfigurieren Sie mit LANconfig unter **Public-Spot** > **Server** im Abschnitt **Brute-Force-Schutz**.

Sperren nach

Bestimmen Sie, nach wie vielen Fehlversuchen die Eingabesperre für weitere Versuche eingreifen soll.

Sperrdauer

Bestimmen Sie, für wie lange die Eingabesperre gelten soll.

Über die Konsole zeigt der Befehl `show pbbruteprotector` den aktuellen Status des Brute-Force-Schutzes:

`show pbbruteprotector`

Zeigt eine Übersicht über alle am Public Spot angemeldeten MAC-Adressen.

`show pbbruteprotector [MAC-Adresse[ MAC-Adresse[ ...]]]`

Die Angabe einer oder mehrerer durch Leerzeichen getrennter MAC-Adressen zeigt den Status der jeweiligen MAC-Adressen an.

Die Angabe von MAC-Adressen erfolgt in den Formaten `11:22:33:44:55:66`, `11-22-33-44-55-66` oder `112233445566`.

1.2.4 Alternative Anmeldeformen

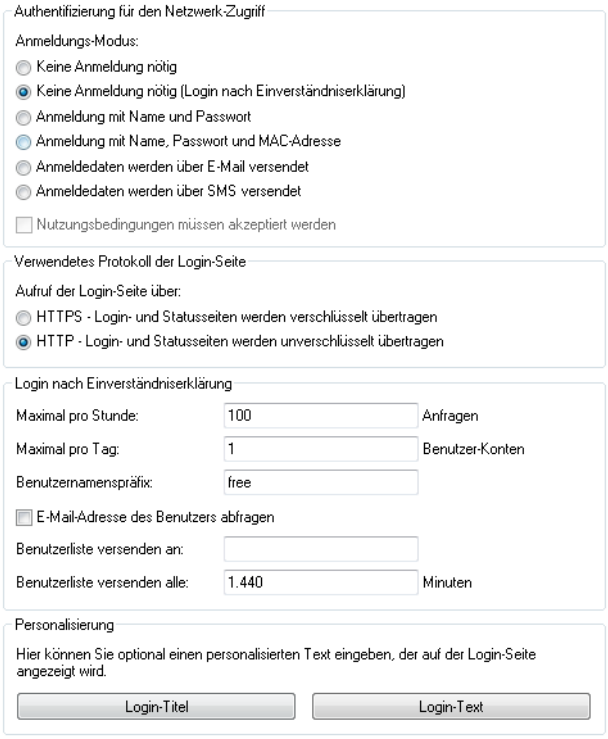
Neben der Anmeldung über vorab mitgeteilte Zugangsdaten können Ihre Nutzer die Zugangsdaten auch selbstständig per E-Mail oder SMS anfordern, oder den schnellen Public Spot-Zugang durch Akzeptieren einer Einverständniserklärung erlangen. Alternativ können Sie über die XML- oder die PMS-Schnitstelle (Modul als Option erhältlich) Ihren Public Spot auch mit anderen Software-Systemen verknüpfen, um so umfassendere oder mehrstufige Anmeldeszenarien zu realisieren.

Ebenso können Sie Ihren Nutzern einen zusätzlichen Komfort bieten, indem Sie z. B. automatisierte Anmeldeverfahren erlauben (Automatische Anmeldung sowie Re-Login über die MAC-Adresse, Anmeldung über WISPr, Hotspot 2.0) und Ihren Nutzern – darauf aufbauend – entsprechende Roaming-Dienste anbieten.

Die Hotspot-2.0- und Roaming-Funktionalitäten sind nur im Zusammenhang mit WLAN verfügbar.

Übersicht der Anmeldemodi

Die Anmeldung am Public Spot kann auf verschiedenen Wegen erfolgen. Diese Einstellungen für die Authentifizierung am Netzwerk legen Sie im Dialog **Public-Spot** > **Anmeldung** fest.



Folgende Anmeldungsmodi stehen Ihnen zur Auswahl:

- **Keine Anmeldung nötig**

  Nutzer erhalten freien Zugang zum Public Spot, eine Anmeldung ist nicht erforderlich.

Verwenden Sie diese Einstellung nicht, wenn Ihr Gerät uneingeschränkten Zugriff auf das Internet bietet!

- **Keine Anmeldung nötig (Login nach Einverständniserklärung)**

  Nutzer erhalten freien Zugang zum Public Spot, nachdem sie die Einverständniserklärung des Betreibers akzeptiert haben. Die Anmeldung erfolgt dabei für die Nutzer völlig transparent über einen RADIUS-Server. Voraussetzung dafür ist, dass Sie eine individuelle Seitenvorlage (Willkommensseite mit Einverständniserklärung) eingerichtet haben: In diesem Fall leitet der Public Spot einen neuen Nutzer zunächst auf die Willkommensseite weiter. Nach Zustimmung der Einverständniserklärung legt das Gerät entsprechend der unter **Public-Spot** > **Assistent** gesetzten Standardwerte automatisch ein Benutzerkonto an und gibt den Zugriff auf das angeschlossene Netzwerk frei.

  Darüber hinaus ist bei Anwählen dieses Anmeldungsmodus der Dialog-Abschnitt **Login nach Einverständniserklärung** verfügbar, in dem Sie zusätzliche Rahmenbedingungen für das Erstellen von freien Benutzerkonten durch den RADIUS-Server festlegen:

  - **Maximal pro Stunde**: Geben Sie an, wie viele Benutzer sich pro Stunde am Gerät automatisch ein Konto erstellen können. Verringern Sie diesen Wert, um Leistungseinbußen durch übermäßig viele Nutzer zu reduzieren.
  - **Maximal pro Tag**: Geben Sie an, wie viele Konten ein Nutzer pro Tag anlegen darf. Ist dieser Wert erreicht und die Nutzer-Sitzung abgelaufen, kann sich ein Benutzer für den Rest des Tages nicht mehr automatisch am Public Spot anmelden und authentifizieren lassen.
  - **Benutzernamenspräfix**: Geben Sie hier einen Präfix an, anhand dessen Sie Benutzer in der RADIUS-Benutzertabelle erkennen, die das Gerät automatisch nach Bestätigen der Nutzungsbedinungen angelegt hat. Dieser Präfix wird dem unter **Public-Spot** > **Assistent** spezifizierten **Muster für den Benutzernamen** unmittelbar vorangestellt.
  - **E-Mail-Adresse des Benutzers abfragen**: Aktivieren Sie diese Checkbox, um die E-Mail-Adresse des Nutzers für die Verwendung des Public Spot abzufragen. Die hier angegebene E-Mail-Adresse trägt das Gerät automatisch im Kommentarfeld des neu angelegten RADIUS-Benutzers ein. Eine Liste aller vorhandenen Adressen wird täglich einmal im Flash-Speicher des Gerätes abgelegt und bleibt auch im Falle eines Neustartes bestehen.
  - **Benutzerliste versenden an**: Geben Sie hier die E-Mail-Adresse an, an die die Adressliste gesendet werden soll. Es werden nur Informationen gesendet, die seit der letzten Übermittlung neu hinzugekommen sind. Die Übermittlung der Adressliste erfolgt als CSV-Datei.
  - **Benutzerliste versenden alle**: Legen Sie fest, in welchem Intervall die aktualisierte Adressliste an die angegebene E-Mail-Adresse übermittelt werden soll. Der Wert wird in Minuten angegeben.

  Die in der Willkommensseite hinterlegten Einverständniserklärung ist nicht mit der Nutzungsbedingungsseite zu verwechseln. Die Seite **Nutzungsbedingungen** ist eine Sonderseite, die nach gesonderter Aktivierung bei anderen Anmeldungsmodi zur Verfügung steht (siehe *Mögliche Authentifizierungsseiten* auf Seite 101). Sofern Sie keine Willkommensseite einrichten (siehe *Konfiguration benutzerdefinierter Seiten* auf Seite 107), zeigt das Gerät beim Zugriff auf den Public Spot eine Fehlermeldung an.

- **Anmeldung mit Name und Passwort**

  Nutzer melden sich am Public Spot mit ihrem Namen und ihrem Passwort an. Die Login-Daten erhalten Nutzer von einem Netzwerk-Administrator über einen Voucher.

- **Anmeldung mit Name, Passwort und MAC-Adresse**

  Nutzer melden sich am Public Spot mit ihrem Namen und ihrem Passwort an. Die Login-Daten erhalten Nutzer von einem Netzwerk-Administrator über einen Voucher. Zusätzlich muss bei diesem Anmeldungs-Modus die MAC-Adresse des Client mit der in der Benutzer-Liste vom Administrator hinterlegten Adresse übereinstimmen.

- **Anmeldedaten werden über E-Mail versendet**

  Nutzer melden sich am Public Spot mit ihrem Namen und ihrem Passwort an. Die Login-Daten generieren sich die Nutzer selbst; zugestellt werden die Daten per E-Mail. Die Aktivität eines Administrators ist nicht erforderlich. Mehr zu diesem Anmeldungsmodus erfahren Sie unter *Selbständige Benutzeranmeldung (Smart Ticket)* auf Seite 67.

- **Anmeldedaten werden über SMS versendet**

Nutzer melden sich am Public Spot mit ihrem Namen und ihrem Passwort an. Die Login-Daten generieren sich die Nutzer selbst; zugestellt werden die Daten per SMS. Die Aktivität eines Administrators ist nicht erforderlich. Mehr zu diesem Anmeldungsmodus erfahren Sie unter *Selbständige Benutzeranmeldung (Smart Ticket)* auf Seite 67.

Durch aktivieren der Option **Nutzungsbedingungen müssen akzeptiert werden** haben Sie in bestimmten Anmeldungsmodi außerdem die Möglichkeit, die Anmeldung an die Anerkennung von Nutzungsbedingungen zu koppeln. In diesem Fall zeigt der Public Spot auf der Anmeldeseite ein zusätzliches Optionsfeld an, welches die Benutzer vor Registrierung bzw. Anmeldung zum Akzeptieren der Nutzungsbedingungen auffordert. Stimmt ein Nutzer diesen Nutzungsbedingungen nicht explizit zu, bleibt ihm eine Anmeldung am Public Spot verwehrt.

Denken Sie daran, vorab eine Seite mit Nutzungsbedingungen in das Gerät zu laden, bevor Sie diese Option aktivieren. Andernfalls zeigt das Gerät dem Benutzer lediglich einen Platzhalter an Stelle der Nutzungsbedingungen an.

Selbständige Benutzeranmeldung (Smart Ticket)

Geräte mit Public Spot bieten Anwendern einen zeitlich begrenzten Zugang zu bestimmten Netzwerken, klassischerweise dem Internet. In vielen Szenarien wird für das Anlegen eines Zugangs ein beschränkter Administrations-Account eingesetzt: Ein Mitarbeiter an einer Hotel-Rezeption z. B. erhält hierbei einen Account, der ausschließlich über die Funktionsrechte zum Anlegen und ggf. Verwalten von Public Spot-Benutzern verfügt. Mit wenigen Mausklicks kann der Mitarbeiter dann den Hotelgästen einen Voucher für den Netzzugang ausdrucken.

Da allerdings auch die komfortable Lösung mit Vouchern immer die Aktivität eines Administrators erfordert, können Sie Ihren Nutzern alternativ die Möglichkeit einräumen, die Zugangsdaten zum drahtlosen Netzwerk eigenständig zu generieren und sich die Zugangsdaten per E-Mail oder SMS zusenden zu lassen (Anmeldung über "Smart Ticket").

Login nach Einverständniserklärung

Alternativ bietet das Gerät Ihnen die Möglichkeit, die Anmeldung für Public Spot-Nutzer völlig transparent über einen RADIUS-Server abzuwickeln. Der Benutzeranmeldung ist in diesem Fall eine Abfrage vorangestellt, bei der ein Nutzer zunächst der im Gerät hinterlegten Einverständniserklärung zustimmen muss, bevor er automatisch Zugang zum Public Spot erhalten. Ein nutzerseitiges Erstellen eigener Zugangsdaten via E-Mail oder SMS entfällt bei dieser Authentifizierungsmethode. Mehr hierzu erfahren Sie im betreffenden Abschnitt unter *Übersicht der Anmeldemodi* auf Seite 65, da der "Login nach Einverständniserklärung" kein Bestandteil der Smart-Ticket-Funktion ist.

E-Mail-Anmeldung konfigurieren

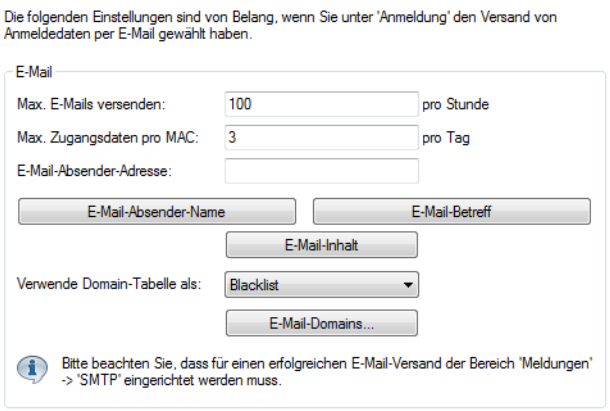
Die Einstellungen für den Versand der Anmeldedaten an das vom Benutzer angegebene E-Mail-Konto nehmen Sie im Dialog **Public-Spot** > **E-Mail** vor. Die nachfolgenden Schritte zeigen Ihnen, wie Sie die E-Mail-Anmeldung korrekt konfigurieren.

Für den erfolgreichen Versand der Anmeldedaten als E-Mail muss unter **Meldungen** > **SMTP-Konto** sowie **Meldungen** > **SMTP-Optionen** ein gültiges SMTP-Konto eingerichtet sein.

Darüber hinaus haben Sie in dem Dialog auch die Möglichkeit, individuelle Texte festzulegen, die das Gerät für den Versand der Anmeldedaten nutzt; siehe *Nachrichtentexte anpassen* auf Seite 71. Standardmäßig setzt das Gerät vordefinierte Textbausteine ein; eine Übersicht dieser Standardtexte finden Sie unter *Standardtexte für E-Mail-Absender, -Betreff und -Inhalt* auf Seite 72.

1. Starten Sie LANconfig und öffnen Sie den Konfigurationsdialog für das Gerät.
2. Wechseln Sie in die Ansicht **Public-Spot** > **Anmeldung**.
3. Ändern Sie den Anmeldungsmodus auf **Anmeldedaten werden über E-Mail versendet**.

4. Wechseln Sie in die Ansicht **Public-Spot** > **E-Mail**.



5. Tragen Sie im Eingabefeld **Max. E-Mails versenden** die maximale Anzahl an E-Mails ein, die das Public Spot-Modul innerhalb einer Stunde an Benutzer für die E-Mail-Anmeldung verschicken darf. Reduzieren Sie den Wert, um die Anzahl der neuen Benutzer pro Stunde zu verringen.
6. Geben Sie im Eingabefeld **Max. Zugangsdaten pro MAC** an, wie viele verschiedene Zugangsdaten das Gerät für eine MAC-Adresse innerhalb eines Tages bereitstellen darf.
7. Geben Sie im Eingabefeld **E-Mail-Absender-Adresse** die E-Mail-Adresse an, die dem zukünftigen Public Spot-Benutzer bei der Zustellung der E-Mail als Absenderadresse angezeigt wird, z. B. `support@providerX.org`.
8. Geben Sie über das Auswahlmenü **Verwende Domain-Tabelle als** an, ob das Gerät die Tabelle **E-Mail-Domains** als Blacklist oder Whitelist verwendet.

   Diese Definition bestimmt, welche E-Mail-Adressen bzw. Domains Ihre Public Spot-Benutzer zur Registrierung angeben dürfen.

   - **Blacklist**: Die Registrierung ist über alle E-Mail-Domains erlaubt bis auf diejenigen, die in dieser Tabelle stehen.
   - **Whitelist**: Die Registrierung ist ausschließlich über die E-Mail-Domains möglich, die in dieser Tabelle stehen.

   Bitte beachten Sie, dass der Public Spot bei einer leeren Domain-List als Whitelist alle Domains ablehnt.

9. Definieren Sie über die Tabelle **E-Mail-Domains** alle E-Mail-Domains, die Sie im Falle einer Anmeldung Ihrer Public Spot-Benutzer via E-Mail erlauben bzw. verbieten wollen. Geben Sie die Domains im Format `web-domain.de` an.
10. Schreiben Sie die Konfiguration zurück auf das Gerät.

SMS-Anmeldung konfigurieren

Die Einstellungen für den Versand der Anmeldedaten als Kurznachricht (SMS) an die vom Benutzer angegebene Rufnummer nehmen Sie im Dialog **Public-Spot** > **SMS** vor. Dabei können Sie – je nach Gerätetyp – zwischen mehreren Varianten wählen:

- Versand der Anmeldedaten als SMS über das geräteeigene 3G/4G WWAN-Modul;
- Versand der Anmeldedaten als SMS über das 3G/4G WWAN-Modul eines anderen Gerätes;
- Versand der Anmeldedaten als E-Mail an ein externes E-Mail2SMS-Gateway, welches die Umwandlung der E-Mail in eine SMS übernimmt.

LCOS überprüft die eingegebene Rufnummer auf ungültige Zeichen. Erlaubt sind ausschließlich Zahlen zwischen 0 und 9. Der Nutzer muss 5 bis 15 Zahlen (exklusive Landesvorwahl) eingeben.

Die nachfolgenden Schritte zeigen Ihnen, wie Sie die einzelnen Varianten der SMS-Anmeldung korrekt konfigurieren.

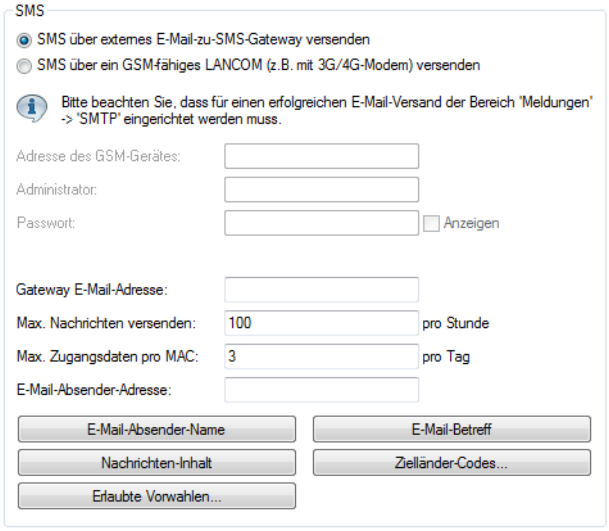
Für den erfolgreichen Versand der Anmeldedaten als Kurznachricht durch ein 3G/4G WWAN-fähiges Gerät muss unter **Meldungen** > **SMS-Nachrichten** dessen internes SMS-Modul eingerichtet sein, siehe *Basiskonfiguration des SMS-Moduls* auf Seite 188.

Der SMS-Versand eignet sich für Installationen mit einem maximalen Durchsatz von 10 SMS pro Minute.

Für den erfolgreichen Versand der Anmeldedaten als E-Mail muss unter **Meldungen** > **SMTP-Konto** sowie **Meldungen** > **SMTP-Optionen** ein gültiges SMTP-Konto eingerichtet sein.

Darüber hinaus haben Sie in dem Dialog auch die Möglichkeit, individuelle Texte festzulegen, die das Gerät für den Versand der Anmeldedaten nutzt; siehe *Nachrichtentexte anpassen* auf Seite 71. Standardmäßig setzt das Gerät vordefinierte Textbausteine ein; eine Übersicht dieser Standardtexte finden Sie unter *Standardtexte für E-Mail-Absender, -Betreff und -Inhalt* auf Seite 72.

1. Starten Sie LANconfig und öffnen Sie den Konfigurationsdialog für das Gerät.
2. Wechseln Sie in die Ansicht **Public-Spot** > **Anmeldung**.
3. Ändern Sie den Anmeldungsmodus auf **Anmeldedaten werden über SMS versendet**.
4. Wechseln Sie in die Ansicht **Public-Spot** > **SMS**.



5. Legen Sie fest, auf welche Art und Weise der SMS-Versand erfolgt:

   - Für den Versand der Anmeldedaten als SMS über das geräteeigene 3G/4G WWAN-Modul, wählen Sie die Einstellung **SMS über internes GSM-Modem versenden** und fahren anschließend mit dem nächsten Konfigurations-Hauptschritt fort.
   - Für den Versand der Anmeldedaten als SMS über das 3G/4G WWAN-Modul eines anderen Gerätes, führen Sie zunächst die Schritte im Abschnitt *Geräte mit 3G/4G WWAN-Modul als SMS-Gateway einsetzen* auf Seite 70 aus und fahren anschließend mit dem nächsten Konfigurations-Hauptschritt fort.
   - Für Versand der Anmeldedaten als E-Mail an ein externes E-Mail2SMS-Gateway, wählen Sie die Einstellung **SMS über externes E-Mail-zu-SMS-Gateway versenden** und fahren im Anschluss an die nachstehenden Unterschritte mit dem nächsten Konfigurations-Hauptschritt fort.

   a) Tragen Sie im Eingabefeld **Gateway E-Mail-Adresse** die IP-Adresse oder den Host-Namen des Gateway-Servers ein, der die E-Mail in eine SMS umwandelt. Erwartet der Provider die Mobilfunknummer im lokalen Teil der E-Mail, können Sie dafür die Variable `$PSpotUserMobileNr` verwenden.

   b) Geben Sie im Eingabefeld **E-Mail-Absender-Adresse** die E-Mail-Adresse an, die dem zukünftigen Public Spot-Benutzer bei der Zustellung der SMS als Absenderadresse angezeigt wird, z. B. `support@providerX.org`.

6. Tragen Sie im Eingabefeld **Max. Nachrichten versenden** die maximale Anzahl an Kurznachrichten ein, die das Public Spot-Modul innerhalb einer Stunde an Benutzer für die SMS-Anmeldung verschicken darf. Reduzieren Sie den Wert, um die Anzahl der neuen Benutzer pro Stunde zu verringen.
7. Geben Sie im Eingabefeld **Max. Zugangsdaten pro MAC** an, wie viele verschiedene Zugangsdaten das Gerät für eine MAC-Adresse innerhalb eines Tages bereitstellen darf.
8. Tragen Sie in die Tabelle **Zielländer-Codes** sämtliche Rufnummern ein, die der Public Spot für den Versand der Anmeldedaten über SMS akzeptiert.
   Die Eingabe eines Länder-Codes kann direkt oder mit vorangestellter Doppel-Null erfolgen, zum Beispiel für Deutschland `49` oder `0049`.

   Diese Tabelle agiert als Whitelist. Sie müssen Länder-Codes definieren, damit ein Versand der Login-Daten erfolgt.
9. Um den SMS-Versand auf bestimmte landesspezifische Vorwahlen zu beschränken, geben Sie die zulässigen Vorwahlen gefolgt von einem '*' in einer kommaseparierten Liste ein. Ein Beispiel für deutsche Mobilfunkanbieter: `15*, 16*, 17*`.

   Wenn Sie für ein Land hier keine Eintragung vornehmen, so werden alle landesspezifischen Vorwahlen zugelassen. Zu dem jeweiligen Land muss zuvor ein Eintrag in der Tabelle Erlaubte-Landesvorwahlen angelegt worden sein.
10. Schreiben Sie die Konfiguration zurück auf das Gerät.

Geräte mit 3G/4G WWAN-Modul als SMS-Gateway einsetzen

Sie haben bei der Public Spot-Anmeldung via SMS (Smart Ticket) die Möglichkeit, den Versand der Zugangsdaten über das 3G/4G WWAN-Modul eines anderen Gerätes anstelle eines externen E-Mail2SMS-Gateways abzuwickeln. Dazu hinterlegen Sie im Gerät, das den Public Spot bereitstellt, die Adresse und die Zugangsdaten des betreffenden 3G/4G-Gerätes. Für den Versand der SMS schickt das Public Spot-Modul dann via URL-Aufruf die Anmeldedaten und die Kurznachricht an das fremde 3G/4G-Gerät.

Die Option steht Ihnen sowohl auf Geräten ohne als auch mit eigenem 3G/4G WWAN-Modul zur Verfügung. Auf diese Weisen haben Sie z. B. die Möglichkeit, mehrere Geräte miteinander zu verketten und eine eigene Versandeinheit einzurichten, falls Sie Public Spot auf einem Gerät ohne 3G/4G WWAN-Modul und / oder mehrere Public Spots betreiben.

1. Starten Sie LANconfig und richten Sie auf dem 3G/4G-Gerät, das als SMS-Gateway fungieren soll, dass SMS-Modul ein (siehe *Basiskonfiguration des SMS-Moduls* auf Seite 188). Darüber hinaus empfiehlt es sich, für den Zugang einen separaten Administrator ohne Zugriffsrechte (Auswahl **Keine**) mit dem alleinigen Funktionsrecht **Senden von SMS** anzulegen.
2. Öffnen Sie den Konfigurationsdialog für das Gerät, das den Public Spot bereitstellt.

3. Wechseln Sie in die Ansicht **Public-Spot** > **SMS**.

4. Wählen Sie die Einstellung **SMS über ein GSM-fähiges Gerät (z. B. mit 3G/4G-Modem) versenden**.
5. Geben Sie in den Eingabefeldern **Administrator** und **Passwort** den Namen und das Passwort für den Administrator auf dem anderen 3G/4G-Gerät ein.
6. Geben Sie im Eingabefeld **Adresse des GSM-Gerätes** die IP-Adresse ein, unter der das andere 3G/4G-Gerät für den Public Spot erreichbar ist.

Nachrichtentexte anpassen

Standardmäßig setzt das Gerät für den Inhalt der versendeten E-Mails oder Kurznachrichten vordefinierte Textbausteine ein; eine Übersicht dieser Standardtexte finden Sie unter *Standardtexte für E-Mail-Absender, -Betreff und -Inhalt* auf Seite 72. Sie haben aber auch die Möglichkeit, eigene Texte zu definieren.

Sofern Sie für eine Sprache keinen individuellen Text spezifizieren, trägt das Gerät automatisch den geräteinternen Standardtext ein.

1. Starten Sie LANconfig und öffnen Sie den Konfigurationsdialog für das Gerät.
2. Wechseln Sie – je nach gewähltem Anmeldungsmodus – in die Ansicht **Public-Spot** > **E-Mail** bzw. **SMS**.
3. Geben über die Schaltfläche **E-Mail-Absender-Name** zu den verfügbaren Sprachen einen individuellen Absendernamen an, den die vom Public Spot zugestellten E-Mails bzw. Kurznachrichten tragen, z. B. `Provider X`.
4. Geben über die Schaltfläche **E-Mail-Betreff** zu den verfügbaren Sprachen eine individuelle Betreffzeile an, die das Public Spot-Modul für seine E-Mails bzw. Kurznachrichten verwendet. Die dabei zur Verfügungen stehenden Steuerzeichen entnehmen Sie dem Abschnitt *Verfügbare Variablen und Steuerzeichen* auf Seite 71.
5. Geben über die Schaltfläche **E-Mail-Inhalt** bzw. **Nachrichteninhalt** zu den verfügbaren Sprachen einen individuellen Text an, den das Public Spot-Modul für seine E-Mails bzw. Kurznachrichten verwendet. Die dabei zur Verfügungen stehenden Variablen und Steuerzeichen entnehmen Sie dem Abschnitt *Verfügbare Variablen und Steuerzeichen* auf Seite 71.
6. Schreiben Sie die Konfiguration zurück in das Gerät.

Verfügbare Variablen und Steuerzeichen

Für die Individualisierung der Standardtexte von Smart Ticket stehen Ihnen verschiedene Variablen und Steuerzeichen zur Verfügung. Die Variablen werden vom Public Spot-Modul beim Versand der E-Mail an den Benutzer bzw. das SMS-Gateway automatisch mit Werten gefüllt.

Variablen

Folgende Variablen stehen Ihnen im Eingabefeld **E-Mail-Inhalt** zur Verfügung:

`$PSpotPasswd`

Platzhalter für das nutzerspezifische Passwort des Public Spot-Zugangs.

`$PSpotLogoutLink`

Platzhalter für die Abmelde-URL des Public Spots in der Form `http://<IP-Adresse des Public Spots>/authen/logout`. Über diese URL hat ein Public Spot-Benutzer die Möglichkeit, sich vom Public Spot abzumelden, falls nach einem erfolgreichen Login das Sitzungsfenster – welches diesen Link ebenfalls enthält – z. B. vom Browser geblockt oder vom Benutzer geschlossen wird.

Steuerzeichen

Der Text in den Eingabefeldern **E-Mail-Betreff** und **E-Mail-Inhalt** darf auch folgende Steuerzeichen enthalten:

`\n`

CRLF (Carriage Return, Line Feed)

`\t`

Tabulator

`\<ASCII>`

ASCII-Code des entsprechenden Zeichens

Verlangt der E-Mail2SMS-Provider eine Variable, in der ein Backslash ("\") vorkommt, müssen Sie diesem ein weiteres "\" voranstellen. Dies unterbindet die Umwandlung des "\" durch LCOS.

Standardtexte für E-Mail-Absender, -Betreff und -Inhalt

Wenn Sie im Dialog **Public-Spot** > **E-Mail** oder. **SMS** zu einer Sprache für das jeweilige Eingabefeld keinen individuellen Text angeben, greift das Gerät beim Generieren der E-Mail automatisch auf die im LCOS hinterlegten Standardtexte zurück. Die verwendete Sprache ist dabei abhängig von der Spracheinstellung des Browsers, den der Benutzer für die Registrierung verwendet hat. Sofern zu einer Sprache keine geräteinternen Standardtexte vorliegen, setzt das Gerät die englischen Texte ein.

Tabelle 2: Übersicht der geräteinternen Standardtexte für die Anmeldung über E-Mail/SMS

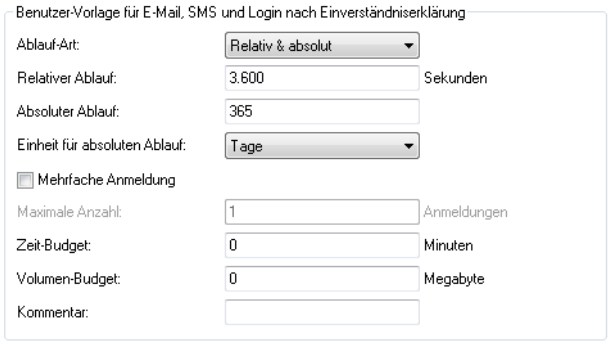
	E-Mail-Absender-Name	E-Mail-Betreff	E-Mail-Inhalt
Deutsch	Public Spot	Ihre Anmeldedaten für den Public Spot	Ihr Passwort für den Public Spot: $PSpotPasswd $PSpotLogoutLink
Englisch	Public Spot	Your Public Spot account	Your password for the Public Spot: $PSpotPasswd $PSpotLogoutLink

Standardwerte für die Benutzer-Vorlage setzen

Der nachfolgende Abschnitt beschreibt, wie Sie die Standardwerte für die **Benutzer-Vorlage** an Ihre Bedürfnisse anpassen. Das Gerät verwendet die hier definierten Werte als Vorgabewerte beim Anlegen neuer Benutzer über Smart-Ticket und dem Login nach Einverständniserklärung. Sofern Sie also den Versand der Anmeldedaten über E-Mail/SMS oder den Login nach Einverständniserklärung als Anmeldungsmodus gewählt haben, enthält jeder neue Benutzer-Account die von der Benutzer-Vorlage vorgegebenen Befugnisse und Einschränkungen.

1. Starten Sie LANconfig und öffnen Sie den Konfigurationsdialog für das Gerät.

2. Wechseln Sie in die Ansicht **Public-Spot** > **Assistent**.



3. Füllen Sie die Eingabefelder im Abschnitt **Benutzer-Vorlage** entsprechend Ihren Vorstellungen aus:

Ablauf-Art

Über diesen Eintrag definieren Sie, auf welche Art ein automatisch angelegtes Public Spot-Benutzerkonto abläuft. Sie können festlegen, ob die Gültigkeitsdauer eines Benutzer-Accounts absolut (fester Zeitpunkt) und / oder relativ (Zeitspanne ab dem ersten erfolgreichen Login) ist. Wenn Sie beide Werte auswählen, hängt der Ablaufzeitpunkt davon ab, welcher Fall als Erstes eintritt.

Relativer Ablauf

Über diesen Eintrag definieren Sie die relative Ablaufzeit eines automatisch angelegten Benutzerkontos (in Sekunden). Der von Ihnen gewählte **Ablauf-Typ** muss ein `relativ` beinhalten, damit diese Einstellung greift. Die Gültigkeit des Kontos endet nach der in diesem Feld angegebenen Zeitspanne nach dem ersten erfolgreichen Login des Benutzers.

Absoluter Ablauf

Über diesen Eintrag definieren Sie die absolute Ablaufzeit eines automatisch angelegten Benutzerkontos (in Tagen). Die von Ihnen gewählte **Ablauf-Art** muss ein `absolut` beinhalten, damit diese Einstellung greift.

Die Gültigkeit des Kontos endet zu dem in diesem Feld angegebenen Zeitpunkt, hochgerechnet vom Tag der Kontoerstellung.

Einheit für absoluten Ablauf

Um kürzere Ablaufzeiten zu konfigurieren, wählen Sie im Dropdown-Menü die Einheit für den absoluten Ablauf aus. Passen Sie ggf. den Wert des absoluten Ablaufes an.

Mehrfache Anmeldung

Über diesen Eintrag erlauben bzw. verbieten Sie ganz allgemein, ob Nutzer eines automatisch erstellten Accounts mehrere Geräte gleichzeitig mit den selben Zugangsdaten am Public Spot anmelden dürfen. Die erlaubte Menge der gleichzeitig angemeldeten Geräte legen Sie über das Eingabefeld **Maximale Anzahl** fest.

Maximale Anzahl

Über diesen Eintrag legen Sie die maximale Anzahl der Geräte fest, die gleichzeitig unter einem automatisch erstellten Account angemeldet sein dürfen. Der Wert `0` steht dabei für 'unbegrenzt'. Damit diese Einstellung greift, muss gleichzeitig der Parameter **Mehrfache Anmeldung** aktiviert sein.

Zeit-Budget

Über diesen Eintrag definieren Sie das Zeit-Budget, welches automatisch angelegte Benutzer erhalten. Der Wert `0` deaktiviert die Funktion.

Volumen-Budget

Über diesen Eintrag definieren Sie das Volumen-Budget, welches automatisch angelegte Benutzer erhalten. Der Wert `0` deaktiviert die Funktion.

Kommentar

Über diesen Eintrag vergeben Sie einen Kommentar oder Infotext, mit dem der RADIUS-Server ein automatisch erstelltes Benutzerkonto versieht.

4. Optional: Verändern Sie bei Bedarf das **Muster für Benutzernamen** sowie die **Passwort-Länge**. Das Gerät benutzt in den o. g. Anmeldungsmodi die betreffenden *Vorgabewerte des Benutzer-Erstellungs-Assistenten*, um automatisch einen Benutzernamen und ein Passwort zu generieren.
5. Schreiben Sie die Konfiguration zurück auf das Gerät.

Automatisches Re-Login

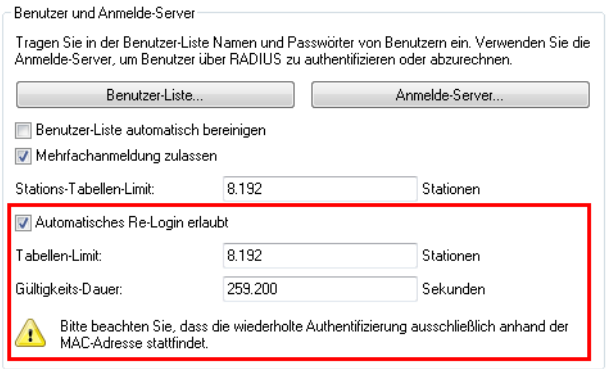
Mobile WLAN-Clients (z. B. Smartphones und Tablett-PCs) buchen sich automatisch in bekannte WLAN-Netze (SSID) ein, wenn sie erneut deren Funkzelle erreichen. Viele Apps greifen in diesem Fall automatisch ohne Umweg über den Webbrowser auf Webinhalte zu, um aktuelle Daten abzufragen (z. B. E-Mails, Soziale Netzwerke, Wetterbericht, etc.). Ähnliches gilt für mobile LAN-Clients (z. B. Notebooks), welche für einen Ortswechsel (z. B. in einer Hochschule dem Wechsel zwischen Hörsaal und Bibliothek) kurzzeitig vom Netz getrennt werden müssen. In allen Fällen ist es unpraktisch, wenn der Benutzer sich zunächst erneut im Browser manuell an einem Public Spot autorisieren muss.

Mit dem automatischen Re-Login genügt es, wenn der Benutzer sich einmalig am Public Spot identifiziert. Nach einer temporären Abwesenheit kann der Benutzer anschließend nahtlos weiter den Public Spot nutzen.

Der Public Spot protokolliert sowohl die manuelle An- und Abmeldung sowie einen Re-Login im SYSLOG. Dabei speichert er für einen Re-Login dieselben Anmeldedaten, die der Benutzer für die erstmalige Authentifizierung verwendet hat.

Die Authentifizierung erfolgt ausschließlich über die MAC-Adresse des Clients, wenn Re-Login aktiviert ist. Da das zu Sicherheitsproblemen führen kann, ist Re-Login standardmäßig deaktiviert.

Die Einstellungen für das automatische Re-Login finden sich bei LANconfig in der Geräte-Konfiguration unter **Public-Spot** > **Benutzer** im Abschnitt **Benutzer und Anmelde-Server**.



Das Auswahlkästchen **Automatische Wiederanmeldung (Auto-Re-Login) erlaubt** aktiviert diese Funktion.

Im Feld **Auto-Re-Login-Tabellen-Limit** bestimmen Sie die Anzahl der Clients (maximal 65536), die die Funktion Re-Login nutzen dürfen.

Im Feld **Auto-Re-Login-Gültigkeitsdauer** bestimmen Sie, wie lange der Public Spot die Anmeldedaten eines Clients für ein Re-Login in der Tabelle speichert. Nach Ablauf dieser Frist muss sich der Public Spot-Benutzer erneut über den Browser auf der Anmeldeseite des Public Spots anmelden.

Automatische Authentifizierung mit der MAC-Adresse

Ein Public Spot gewährt einem Benutzer nach erfolgreicher Authentifizierung den Zugang zu bestimmten Diensten. Zur Authentifizierung zeigt der Public Spot dem Benutzer nach dem Öffnen des Browsers üblicherweise eine Webseite. Der Benutzer gibt in dieser Anmeldeseite seine Benutzerdaten ein, der Public Spot leitet den Benutzer dann auf die erlaubten Webseiten weiter.

In manchen Anwendungsfällen ist die Authentifizierung über eine Webseite nicht erwünscht oder nicht möglich, wie die folgenden Beispiele zeigen:

- Das Endgerät verfügt nicht über einen Browser und kann daher die Anmeldeseite nicht öffnen.
- Der manuelle Aufruf der Anmeldeseite ist z. B. für einen Performance-Test zu langwierig.

Die automatische Authentifizierung am Public Spot mit der MAC-Adresse erlaubt die Nutzung des Public Spot ohne den vorherigen Aufruf der Anmeldeseite. Dazu trägt der Administrator alle MAC-Adressen der entsprechenden Endgeräte in die Tabelle der erlaubten MAC-Adressen unter **Public-Spot** > **Benutzer** > **MAC-authentifizierte Benutzer** ein.

Ablauf der MAC-Adress-Prüfung

Wenn das Gerät die Anfrage eines Clients empfängt, vollzieht der Public Spot bei der automatischen Authentifizierung mit der MAC-Adresse folgende Schritte:

- Wenn der Public Spot die MAC-Adresse der empfangenen Datenpakete bereits authentifiziert hat, leitet das Gerät die zugehörigen Datenpakete weiter.
- Wenn die MAC-Adresse in der Liste der erlaubten Clients enthalten ist, startet der Public Spot eine neue Sitzung für diesen Benutzer und leitet die zugehörigen Datenpakete weiter.
- Wenn ein Provider für die Prüfung der MAC-Adressen über RADIUS definiert und eine positive, noch gültige Authentifizierung für die MAC-Adresse im Public Spot-Cache gespeichert ist, startet der Public Spot eine neue Sitzung für diesen Benutzer und leitet die zugehörigen Datenpakete weiter.
- Wenn ein Provider für die Prüfung der MAC-Adressen über RADIUS definiert, jedoch keine gültige Authentifizierung für die MAC-Adresse im Cache des Public Spot gespeichert ist, leitet der Public Spot die Authentifizierung der MAC-Adresse bei dem entsprechenden RADIUS-Server ein. Nach einer positiven Antwort startet der Public Spot eine neue Sitzung für diesen Benutzer und leitet die zugehörigen Pakete weiter.
- Sind alle zuvor beschriebenen Prüfungen erfolglos, leitet der Public Spot den Benutzer an die Anmeldeseite weiter.

Authentifizierung der MAC-Adresse über RADIUS

Wenn die MAC-Adresse eines anfragenden WLAN-Clients nicht in der Liste der erlaubten Adressen enthalten ist, kann der Public Spot die Adresse alternativ über einen RADIUS-Server authentifizieren.

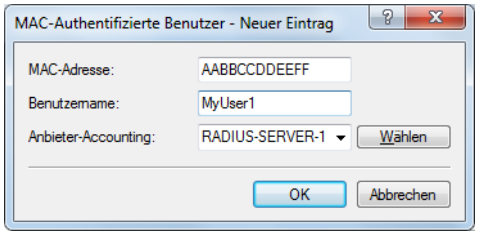
Zur Aktivierung dieser RADIUS-Authentifizierung wählt der Administrator einen der im Gerät definierten RADIUS-Server aus der Anbieter-Liste aus.

Zusätzlich definiert der Administrator eine Lebensdauer für die abgelehnten MAC-Adressen. Mit dieser Lebensdauer verhindert der Public Spot das Fluten des RADIUS-Servers mit wiederholten Anfragen nach MAC-Adressen, die weder über die MAC-Adress-Tabelle noch über den RADIUS-Server ohne Anmeldung authentifiziert werden können.

Wenn eine MAC-Adresse bei einer Anfrage zur Authentifizierung über den RADIUS-Server abgelehnt wird, speichert der Public Spot diese Ablehnung für die definierte Lebensdauer. Weitere Anfragen für die gleiche MAC-Adresse beantwortet der Public Spot innerhalb der Lebensdauer direkt ohne Weiterleitung an den RADIUS-Server.

Konfiguration in LANconfig

Bei der Konfiguration mit LANconfig finden Sie die Parameter für die Authentifizierung der Clients über die MAC-Adresse im Dialog **Public-Spot** > **Benutzer** > **MAC-Authentifizierte Benutzer**.



Automatische Anmeldung über WISPr

Ihr Gerät stellt eine Schnittstelle für die Anmeldung über WISPr bereit. Der **WISPr**-Standard ist der technologische Vorläufer der 802.11u- und Hotspot-2.0-Spezifikation. Die Abkürzung steht für **Wireless Internet Service Provider Roaming** und bezeichnet sowohl ein Verfahren als auch Protokoll, welches Nutzern von WLAN-fähigen Endgeräten dazu ermöglicht, zwischen den WLANs unterschiedlicher Betreiber – respektive deren Internet-Service-Provider – unterbrechungsfrei zu roamen. Die Idee dahinter ähnelt somit der von 802.11u und Hotspot 2.0, erfordert allerdings eine umfassendere Betreuung durch den jeweiligen Nutzer.

Über das WISPr-Protokoll können Sie Endgeräten, für die herstellerseitig keine Unterstützung für Hotspot 2.0 mehr angeboten wird, eine Hotspot-2.0-ähnliche Anmeldung und Netzwerknutzung über Ihren Hotspot ermöglichen. Voraussetzung ist, dass Ihr Service-Provider die dazugehörige Infrastruktur bereitstellt. Nutzerseitig erfolgt die Unterstützung entweder über das verwendete Betriebssystem oder eine geeignete App (Smart-Client). Dieser Client übernimmt für den Nutzer die Authentifizierung am Hotspot; liegen für das betreffende Netzwerk keine Authentifizierungsdaten vor, fragt der Client den Nutzer auf Systemebene nach gültigen Zugangsdaten. Für den Nutzer entfällt somit in jedem Fall die Anmeldung über eine Login-Seite in seinem Browser.

Aufgrund seines Alters unterstützen fast alle aktuelle Endgeräte mit iOS, Android und Windows 8 das WISPr-Protokoll. Darüber hinaus bieten größere WLAN-Internet-Service-Provider häufig auch eigene Apps an, um Ihren Kunden die Anmeldung zu erleichtern: Diese Apps beeinhalten eine vorkonfigurierte Datenbank der Provider-eigenen Hotspots und – optional – der Hotspots seiner Roaming-Partner. Der Ablauf der Authenifizierung entspricht dann dem folgenden Schema:

1. Ein Kunde installiert als Client die Hotspot-App seines Providers, welche in einer Datenbank vorkonfigurierte Hotspot-SSIDs bereitstellt.
2. Der Client verbindet sich automatisch mit einem dieser Hotspots und sendet einen HTTP-GET-Request an eine beliebige URL, um zu testen, ob ein direkter Internetzugriff besteht oder der Public Spot eine Authentifizierung anfordert.
3. Der Hotspot sendet im HTTP-Redirect ein WISPr-XML-Tag mit der Login-URL.
4. Der Client sendet in einem HTTP-Post seine Anmeldedaten an die Login-URL.

Beispiel für XML-Tag im Redirect:

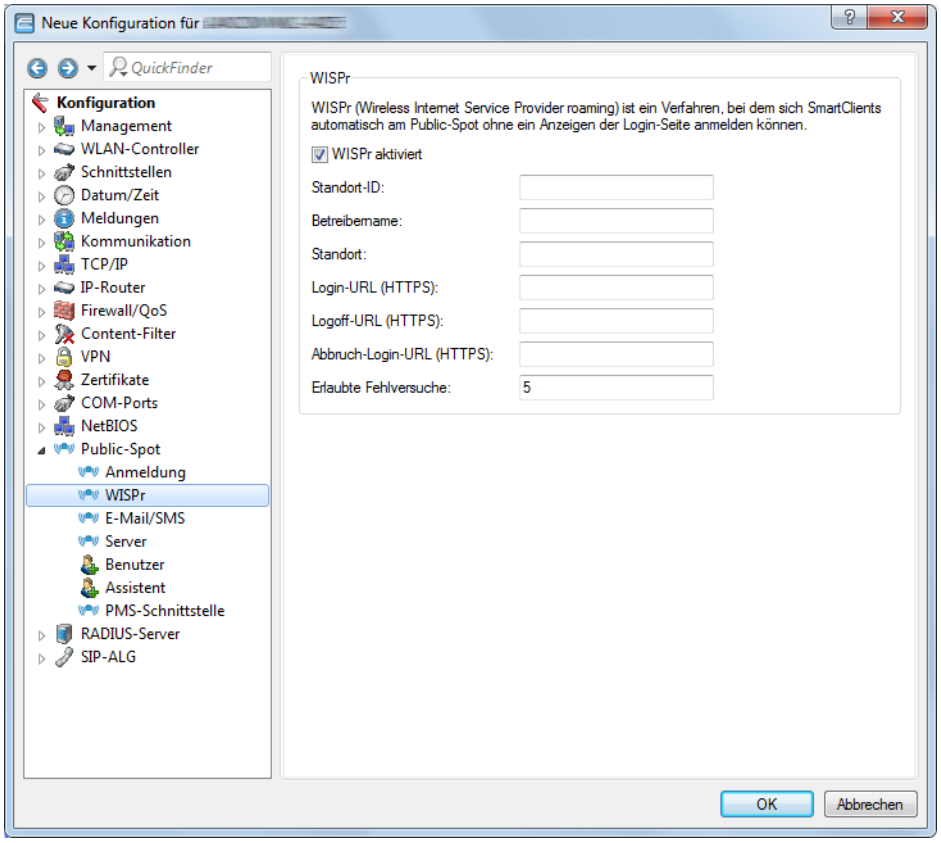
```
<HTML>
<?xml version="1.0" encoding="UTF-8"?>
  <WISPAccessGatewayParam xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xsi:noNamespaceSchemaLocation="http://www.acmewisp.com/WISPAccess GatewayParam.xsd">
    <Redirect>
      <AccessProcedure>1.0</AccessProcedure>
      <AccessLocation>Hotel Contoso Guest Network</AccessLocation>
      <LocationName>Hotel Contoso</LocationName>
      <LoginURL>https://captiveportal.com/login</LoginURL>
      <MessageType>100</MessageType>
      <ResponseCode>0</ResponseCode>
    </Redirect>
   </WISPAccessGatewayParam>
</HTML>
```

Für die Nutzung von WISPr sind zwingend ein SSL-Zertifikat und ein Private-Key im Gerät erforderlich. Das Zertifikat muss entweder von einer vertrauenswürdigen Stelle signiert oder – sofern Sie ein selbst-signiertes

Zertifikat verwenden – im Client als vertrauenswürdig importiert sein. Ansonsten verweigert ein Client das Login via WISPr. Weitere Informationen zum Laden dieser Objekte in Ihr Gerät finden Sie im LANCOM Techpaper "Zertifikatsmanagement im Public Spot", erhältlich unter *www.lancom-systems.de*.

WISPr konfigurieren

Die WISPr-Funktion Ihres Gerätes konfigurieren Sie über den Dialog **Public-Spot** > **WISPr**.



In diesem Dialog haben Sie folgende Einstellungsmöglichkeiten:

- **WISPr aktiviert**: Aktivieren oder deaktivieren Sie die WISPr-Funktion für das Gerät.
- **Standort-ID**: Vergeben Sie hierüber eine eindeutige Standort-Nummer oder -Kennung für Ihr Gerät, z. B. in der Form `isocc=<ISO_Country_Code>,cc=<E.164_Country_Code>,ac=<E.164_Area_Code>,network=<SSID/ZONE>`.
- **Betreibername**: Geben Sie hier den Namen des Hotspot-Betreibers ein, z. B. `providerX`. Diese Angabe hilft dem Nutzer bei der manuellen Auswahl eines Internet-Service-Providers.
- **Standort**: Beschreiben Sie den Standort Ihres Gerätes, z. B. `CafeX_Markt3`. Diese Angabe dient einem Nutzer zur besseren Identifizierung Ihres Hotspots.
- **Login-URL (HTTPS)**: Geben Sie die HTTPS-Adresse ein, an die die WISPr-Client die Zugangsdaten für Ihren Internet-Service-Provider übermittelt. Es kann hier eine beliebige externe URL angegeben werden oder der Public Spot selbst. Falls der Public Spot selbst Benutzer über WISPr authentifizieren soll geben Sie die URL an in der Form `https://<Device-FQDN>/wisprlogin`. Für "wisprlogin" im Beispiel kann eine beliebige, frei definierbare Sub-URL verwendet werden.
- **Logoff-URL (HTTPS)**: Geben Sie die HTTPS-Adresse ein, über die sich ein WISPr-Client von Ihrem Internet-Service-Provider abmeldet. Es gelten die gleichen Regeln wie bei der Login-URL.

- **Abbruch-Login-URL (HTTPS)**: Geben Sie die HTTPS-Adresse ein, an die das Gerät einen WISPr-Client weiterleitet, wenn die Authentifizierung fehlschlägt. Es gelten die gleichen Regeln wie bei der Login-URL.

  Die drei URLs müssen unterschiedlich sein, falls der Public Spot im Gerät verwendet wird, z. B.:

  - Login-URL: https://<Device-FQDN>/wisprlogin
  - Logoff-URL: https://<Device-FQDN>/wisprlogoff
  - Abbruch-Login-URL: https://<Device-FQDN>/wisprabort

  Ausschließlich zu Testzwecken können Sie auch eine URL mit IP-Adressen konfigurieren. In einem Produktiv-System wird ein Client den FQDN des Zertifikates prüfen!

- **Erlaubte Fehlversuche**: Geben Sie hier die Anzahl der Fehlversuche ein, welche die Login-Seite Ihres Internet-Service-Providers maximal erlaubt. Wenn der Public Spot verwendet wird, verweigert der Public Spot nach dieser Anzahl der Fehlversuche weitere Logins vom betreffenden Client.

IEEE 802.11u und Hotspot 2.0

Ihr Gerät unterstützt WLAN-Verbindungen nach dem IEEE-Standard 802.11u und – darauf aufbauend – die Hotspot-2.0-Spezifikation. Über 802.11u haben Sie die Möglichkeit, in einem lokalen WLAN-Netzwerk (z. B. innerhalb Ihrer Firma) oder einem Public Spot-Netzwerk die automatische Authentisierung und Authentifizierung Ihrer Nutzer zu realisieren. Voraussetzung dafür ist, dass die betreffenden Stationen (Smartphones, Tablet-PCs, Notebooks, usw.) Verbindungen nach 802.11u und Hotspot 2.0 auch unterstützen. Folgende Funktionen bieten sich Ihnen im Detail:

- **Automatische Netzwerkwahl**

  In einer 802.11u-fähigen Umgebung entfällt für einen Benutzer die manuelle Suche und Auswahl einer SSID. Stattdessen übernehmen die Stationen eigenständig die Suche und Auswahl eines geeigneten Wi-Fi-Netzwerks, indem sie selbstständig die Betreiber- und Netzwerkdaten aller 802.11u-fähigen Access Points in Reichweite erfragen und auswerten. Eine vorangehende Anmeldung am Access Point ist dabei nicht erforderlich.

  Mit Hotspot 2.0 erhalten Stationen überdies die Möglichkeit, Informationen über die in einem Wi-Fi-Netzwerk verfügbaren Dienste abzurufen. Sind spezifische, für einen Benutzer aber relevante Dienste (z. B. Verbindungen via HTTP, VPN oder VoIP) für ein Wi-Fi-Netzwerk nicht verfügbar, werden alle Netzwerke, die die Kriterien nicht erfüllen, von der weiteren Suche ausgeschlossen. Somit ist sichergestellt, dass Nutzer immer das für sie optimale Netzwerk erhalten.

- **Automatische Authentisierung und Authentifizierung**

  In einer 802.11u-fähigen Umgebung übernimmt die Station automatisch die Anmeldung des Benutzers, sofern die notwendigen Zugangsdaten vorliegen. Die Authentifizierung kann z. B. anhand einer SIM-Karte, eines Benutzernamens und Passworts, oder eines digitalen Zertifikats erfolgen. Ein manuelles und wiederholtes Eingeben der Zugangsdaten in eine Anmeldemaske durch den Benutzer entfällt. Nach erfolgreicher Authentifizierung kann der Nutzer die benötigten Dienste unmittelbar nutzen.

- **Unterbrechungsfreie Verbindungsübergabe (Seamless Handover)**

  Verbindungen nach 802.11u ermöglichen im Zusammenspiel mit 802.21 die unterbrechungsfreie Übergabe von Datenverbindungen über verschiedene Netzwerktypen hinweg. Dies erlaubt es Nutzern, mit ihren Stationen aus dem Mobilfunknetz unterbrechungsfrei in ein WLAN-Netz zu wechseln, sobald sie in den Empfangsbereich einer entsprechenden Hotspot-2.0-Zone kommen – und umgekehrt. Gleiches gilt für den Wechsel zwischen verschiedenen Betreibern, wenn Nutzer z. B. während einer Busfahrt von einem homogenen Netzwerk in ein anderes wechseln.

- **Automatisches Roaming**

  Verbindungen nach 802.11u ermöglichen das Roaming über unterschiedliche Betreibernetzwerke hinweg. Gelangt ein Benutzer in die Hotspot-2.0-Zone eines Betreibers, für den er keine Authentifizierungsdaten besitzt, besteht für seine Station dennoch die Option, in das Heimnetzwerk zu roamen. Die Authentifizierung an der fremden Hotspot-2.0-Zone erfolgt dann durch den Roaming-Partner des Betreibers, was den Nutzer schließlich zur Nutzung des fremden Wi-Fi-Netzwerks berechtigt. Neben Gebieten, in denen nur einzelne Netzwerkbetreiber mit Acess Points präsent sind, gewinnt diese Möglichkeit vor allem auch für Auslandsreisende an Attraktivität.

Beispiel: Angenommen, ein Nutzer ist mit seinem 802.11u-fähigen Smartphone (seiner Station) in der Stadt unterwegs und aktiviert die WLAN-Funktion, um im Internet zu surfen. Die Station beginnt daraufhin damit, alle verfügbaren Wi-Fi-Netzwerke in der Umgebung zu suchen. Bietet ein Teil der dazugehörigen Access Points 802.11u an, wählt die Station anhand der vorab erhaltenen Betreiber- und Netzinformationen dasjenige Netzwerk aus, welches am besten zum benötigten Dienst passt – z. B. einen Hotspot der eigenen Mobilfunkgesellschaft mit Internetfreigabe. Die anschließende Authentifizierung kann in diesem Fall automatisch über die SIM-Karte erfolgen, sodass der Benutzer während des gesamten Vorgangs nicht mehr einzugreifen braucht. Die für die Verbindung gewählte Verschlüsselungsmethode – z. B. WPA2 – bleibt davon unberührt.

Zusammengefasst verknüpfen Datenverbindungen nach 802.11u und mit aktiviertem Hotspot 2.0 die Sicherheitsmerkmale und Leistungsfähigkeit klassischer Wi-Fi-Hot-Spots mit der Flexibilität und Einfachheit von Datenverbindungen über Mobilfunk. Zeitgleich entlasten sie die Mobilfunknetzwerke, indem sie den Datenverkehr (und ggf. auch die Telefonie) auf die Netzstrecken und Frequenzbänder der Access Points umverteilen.

Passpoint® Release 2

Ab LCOS 10.40 ist die erweiterte Hotspot 2.0-Funktionalität Ihres WLAN-Gerätes nach dem von der Wi-Fi Alliance spezifizierten Passpoint® Release 2 konfigurierbar. Der im LCOS integrierte RADIUS-Server beinhaltet ab Version 10.32 RU4 die benötigten Features.

Passpoint® Release 2 vereinfacht das Onboarding von Geräten in ein Netz mit der Verschlüsselungsmethode WPA2-Enterprise (802.1X). Mittels eigener Onboarding-SSID kann ein Benutzer sich ein Profil auf Passpoint® Release 2-fähige Endgeräte installieren und dann automatisch mit den hinterlegten Anmeldedaten ins verschlüsselte Netz wechseln. Somit lassen sich Hotspots realisieren, die verschlüsselte drahtlose Kommunikation ermöglichen. Hierbei können die Gäste über eine offene Onboarding-SSID mit zeitlich begrenzten Zugangsdaten ausgestattet werden.

Ebenso kann ein Mobilfunkanbieter sein Mobilfunknetz entlasten, indem er Wi-Fi Offloading einführt und mobile Endgeräte, die mit einer SIM-Karte ausgestattet sind, automatisch in sein WLAN-Netz einbuchen lässt. Die Endgeräte der Kunden finden das WLAN-Netz des Mobilfunkanbieters automatisch und buchen sich mit den hinterlegten Benutzerdaten der SIM-Karte automatisch in das WLAN-Netz des Betreibers ein.

Mit Passpoint® Release 2 wird die Hotspot 2.0-Funktionalität um die folgenden Features erweitert:

- Online Sign-Up (OSU) – Mit Passpoint® Release 2 bekommen Unternehmen und Netzbetreiber die Möglichkeit, Benutzerprofile über einen so genannten „Online Sign-Up"-Server (OSU-Server) zur Verfügung zu stellen. Über eine offene OSU-SSID hat der Benutzer die Möglichkeit, verschiedene OSU-Server anhand von hinterlegten Icons zu identifizieren und somit den für ihn passenden auszuwählen. Der OSU-Server kann ggf. Benutzerdaten abfragen, bevor er ein passendes Profil für das Endgerät des Benutzers bereitstellt. Neben der offenen OSU-SSID kann auch eine verschlüsselte SSID genutzt werden, welche mittels „anonymous EAP-TLS" die Benutzerdaten verschlüsselt abfragt und bereitstellt. Hierfür wird ein entsprechender RADIUS-Server mit „anonymous EAP-TLS" Unterstützung benötigt.

  Ein OSU-Server ist kein Bestandteil des LCOS. Es gibt allerdings Lösungen von LANCOM Partnern.

- OSU-Icons – Für die unterstützten OSU-Server können im LCOS über die WEBconfig im Bereich **Dateimanagement** entsprechende Icons als Datei hochgeladen werden. Als Dateiformat empfehlen wir PNG.
- Benachrichtigungsmöglichkeit – Auf Netzseite gibt es die Möglichkeit, den Benutzer zu benachrichtigen, wenn eine Abmeldung seitens RADIUS-Server kurz bevor steht. Dies kann z. B. der Fall sein, wenn die Benutzerdaten nicht mehr länger gültig sind oder die festgelegte Verbindungsdauer erreicht wurde.
- QoS Map – Ein Access Point kann über die Funktion „QoS Map Set" seine Clients anweisen, eine bestimmte QoS Map zu verwenden. Hierbei werden die Werte für das Contention Window (Medienzugriff via EDCA) der verschiedenen Access Categories für Voice, Video, Best Effort und Background-Datenpakete und deren zugehörige DSCP-Werte definiert. Gleichzeitig nutzt auch der Access Points die in der QoS Map hinterlegten Werte.

  Aktuell stehen neben den zwei durch die Wi-Fi Alliance vorgegebenen QoS Maps nur die Standard-QoS-Map des LCOS zur Verfügung.

Hotspot-Betreiber und -Service-Provider

Die Hotspot-2.0-Spezifikation der Wi-Fi Alliance unterscheidet zwischen Hotspot-Betreibern und Hotspot-Service-Providern: Ein **Hotspot-Betreiber** unterhält lediglich ein Wi-Fi-Netzwerk, während ein **Hotspot-Service-Provider** (SP) die Verbindung der Nutzer ins Internet oder Mobilfunknetz realisiert. Natürlich ist es möglich, dass ein Betreiber gleichzeitig ein SP ist. In allen anderen Fällen jedoch benötigt ein Hotspot-Betreiber entsprechende Roaming-Vereinbarungen mit einem SP oder einem Zusammenschluss mehrerer SP (Roaming-Konsortium genannt). Erst wenn ein Betreiber diese Vereinbarungen getroffen hat, sind Kunden der entsprechenden Roaming-Partner dazu in der Lage, sich am Hotspot des Betreibers zu authentifizieren. Jeder Service-Provider betreibt dazu seine eigene AAA-Infrastruktur. Die Liste der möglichen Roaming-Partner und der Name des Hotspot-Betreibers teilt ein Hotspot den Stationen über ANQP mit (siehe Funktionsbeschreibung).

Funktionsbeschreibung

Bei 802.11u handelt es sich um den Basis-Standard der IEEE. Dieser Standard erweitert Access Points bzw. Hotspots im Wesentlichen um die Fähigkeit, sogenannte „ANQP-Datenpakete" (Advanced Message Queuing Protocol) in seinen Funksignalen auszustrahlen. ANQP ist ein Query / Response-Protokoll, mit dem ein Gerät eine Reihe von Informationen über den Hotspot abfragen kann. Hierzu gehören sowohl Metadaten, wie z. B. Angaben zum Betreiber und dem Standort, als auch Angaben zum dahinterliegenden Netzwerk, wie z. B. Angaben zu Betreiber-Domänen, Roaming-Partnern, den Authentifizierungsmethoden, Weiterleitungsadressen, usw. Alle 802.11u-fähigen Geräte in Reichweite haben die Möglichkeit, diese Datenpakete ohne vorangehende Anmeldung am Access Point abzufragen, um anhand ihrer die Netzwerkwahl und den -beitritt zu entscheiden.

Die Wi-Fi Alliance hat dem Standard weitere ANQP-Elemente hinzugefügt und vermarktet diese Spezifikation als **Hotspot 2.0**. Die Hotspot-2.0-Funktion ist somit lediglich eine Erweiterung des Standards um zusätzliche Elemente, die Geräte bei ihrer Netzwerkwahl als Kriterien heranziehen können. Hierzu gehören z. B. Angaben zu den am Hotspot verfügbaren Diensten und WAN-Metriken. Das dazugehörige Zertifizierungsprogramm heisst Passpoint®, welches in verschiedenen Ausbaustufen gibt. Bestimmte LANCOM Access Points sind von der Wi-Fi Alliance Passpoint® CERTIFIED (Release 1 und / oder 2).

ANQP-Datenpakete stellen also das zentrale Informationselement des 802.11u-Standards dar. Um die Unterstützung für 802.11u zu signalisieren und die Datenpakete zu übertragen, bedarf es allerdings noch weiterer Elemente, die für den Betrieb von 802.11u essentiell sind:

- Die Signalisierung der 802.11u-Unterstützung in den Beacons und Probes eines Hotspots erfolgt durch das sogenannte „Interworking-Element". In ihm sind bereits erste grundlegende Netzwerkinformationen – wie z. B. die Netzklassifikation, die Internetverfügbarkeit (Internet-Bit) und die OI des Roaming-Konsortiums und / oder des Betreibers – enthalten. Zugleich dient es 802.11u-fähigen Geräten als erstes Filterkriterium bei der Netzsuche.
- Die Übertragung der ANQP-Datenpakete erfolgt innerhalb der sogenannten GAS-Container. GAS steht für Generic Advertisement Service und bezeichnet generische Container, welche einem Gerät erlauben, vom Hotspot – ergänzend zu den Informationen in den Beacons – erweiterte interne und externe Informationen für die Netzwahl abzufragen. Die GAS-Container werden ihrerseits durch sogenannte Public Action Frames auf Layer 2 übermittelt.

Anmeldung eines 802.11u-fähigen Clients an einem Hotspot 2.0

Diese Funktionsbeschreibung erläutert schematisch Auswahl und Anmeldevorgang eines 802.11u-fähigen Geräts an einem Hotspot 2.0.

Anmeldung via Benutzername / Passwort oder digitalem Zertifikat

1. Die Hotspots antworten daraufhin mit einem ANQP-Response, der u. a. jeweils den Namen des Hotspot-Betreibers sowie eine Liste der NAI-Realms enthält, welche alle verfügbaren Roaming-Partner (Service-Provider, kurz SP) auflistet.
2. Das Gerät lädt die auf ihm lokal abgespeicherten Zugangsdaten aus den vom Benutzer eingerichten WLAN-Profilen oder installierten Zertifikaten, und gleicht die dortigen Realms mit den unter (2) erhaltenen NAI-Realm-Listen ab.
   a. Erzielt das Gerät hierbei einen Treffer, weiß es, dass es sich bei betreffenden Wi-Fi-Netzwerk erfolgreich authentisieren kann.

b. Erzielt das Gerät mehrere Treffer, erfolgt die Auswahl eines Wi-Fi-Netzwerks anhand einer vom Benutzer eingerichteten Präferenzliste. Diese Liste legt die Reihenfolge der bevorzugten Betreiber im Zusammenhang mit den möglichen Roaming-Partnern fest. Das Gerät vergleicht hierbei die unter (2) erhaltenen Betreiber-Namen mit der Liste und wählt jenen Betreiber aus, der die höchste Priorität besitzt.

3. Das Gerät authentisiert sich mit seinen lokalen Zugangsdaten am Hotspot des bevorzugten Betreibers für den passenden SP. Der Access Point übermittelt diese Daten seinerseits über die SSPN-Schnittstelle (Subscription Service Provider Network) an ein für die Authentifizierung zuständiges AAA-System. Die Authentisierung erfolgt dabei über die vom SP festgelegte Authentifizierungsmethode; bei der Authentisierung via Benutzername / Passwort umfasst dies EAP-TTLS, bei der Authentisierung via digitalem Zertifikat EAP-TLS.

Anmeldung via (U)SIM

1. Im Unterschied zur Anmeldung via Benutzername / Passwort oder digitalem Zertifikat fragt ein Gerät bei vorliegen einer (U)SIM in seinen ANQP-Requests nicht nach der Liste der NAI-Realms, sondern der 3GPP Cellular Network Information. In den ANQP-Responses beinhaltet diese Cellular-Netzwerk-Informations-Liste alle Mobilfunkanbieter, für die der Access Point eine Authentisierung ermöglicht.

2. Das Gerät lädt aus seiner lokalen (U)SIM-Karte die Kennwerte für das Mobilfunknetzwerk und gleicht diese Daten mit den erhaltenen Cellular-Netzwerk-Informations-Listen ab. Der Listenabgleich sowie die Auswahl eines bevorzugten Betreibernetzwerkes erfolgen synonym zur Anmeldung via Benutzername/Passwort oder digitalem Zertifikat.

3. Das Gerät authentisiert sich mit seinen lokalen Zugangsdaten am Hotspot des bevorzugten Betreibers für die passende Mobilfunkgesellschaft. Der Hotspot übermittelt diese Daten seinerseits über die SSPN-Schnittstelle (Subscription Service Provider Network) an ein für die Authentifizierung zuständiges AAA-System. Durch das Vorhandensein einer (U)SIM-Karte ändert sich die mögliche Authentifizierungsmethode für das Gerät zu EAP-SIM oder EAP-AKA.

4. Das AAA-System erkundigt sich für die Authentifizierung über die MAP-Schnittstelle (Mobile Application Part) beim HLR-Server (Home Location Register) der Mobilfunkgesellschaft, um die Zugangsdaten zu verifizieren.

Im Falle einer erfolgreichen Authentisierung erhält das Gerät den Zugriff auf das WLAN-Netzwerk entweder via Hotspot (Zugangsdaten für das Betreiber-Netzwerk liegen vor) oder automatischem Roaming (Zugangsdaten für das Betreiber-Netzwerk liegen nicht vor).

Stehen dem Gerät mehrere Authentifizierungsmöglichkeiten zur Auswahl (z. B. SIM-Karte und Benutzername / Passwort), hat es die Möglichkeit, anhand der NAI-Realm- bzw. Cellular-Netzwerk-Informations-Liste die bevorzugte EAP-Authentifizierungsmethode und damit die bevorzugten Zugangsdaten auszuwählen.

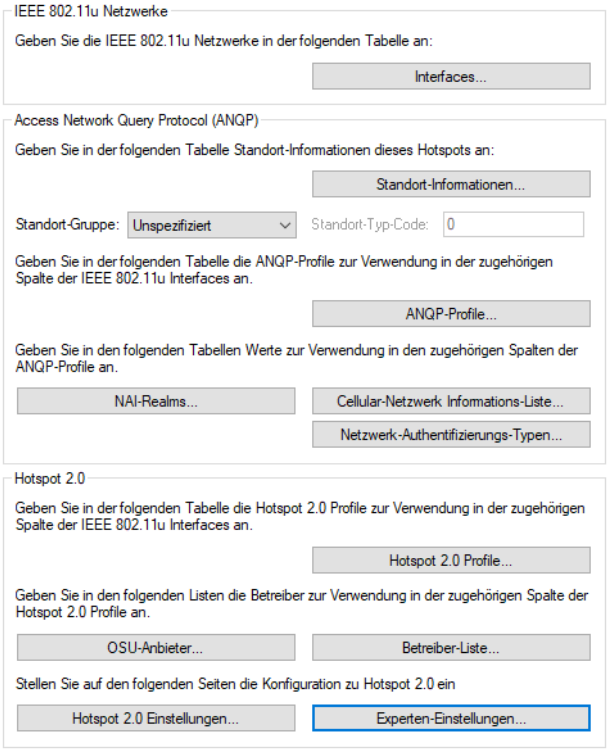
Empfohlene allgemeine Einstellungen

Die Hotspot-2.0-Spezifikation empfiehlt für den 802.11u-Betrieb folgende allgemeine Einstellungen:

- Aktivierte WPA2-Enterprise Sicherheit (802.1X)
- Authentifizierung via EAP mit der entsprechenden Variante:
  - EAP-SIM/EAP-AKA bei Authentifizierung mit SIM/USIM-Karte
  - EAP-TLS bei Authentifizierung mit digitalem Zertifikat
  - EAP-TTLS bei Authentifizierung mit Benutzername und Passwort
- Aktiviertes und eingerichtetes Proxy-ARP
- Deaktivierte Multicast- und Broadcasts in Funkzellen
- Nicht-zugelassener Datenverkehr zwischen den einzelnen mobilen Endgeräten (Layer-2 Traffic-Inspection & Filtering). Die dazugehörigen Schalter finden Sie im LANconfig unter **Wireless-LAN** > **Securtity** > **Datenverkehr zwischen SSIDs**.
- Aktivierte und eingerichtete Firewall auf dem Access-Router, welcher den Internetzugang zur Verfügung stellt

Konfigurationsmenü für IEEE 802.11u / Hotspot 2.0

Das Konfigurationsmenü für IEEE 802.11u und Hotspot 2.0 finden Sie unter **Wireless-LAN** > **IEEE 802.11u**.



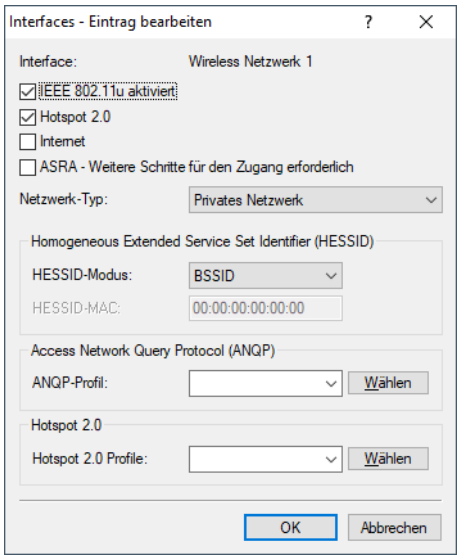
Das Gerät bietet Ihnen über die Schaltfläche **Interfaces** die Möglichkeit, die Unterstützung für den IEEE-802.11u-Standard sowie die Hotspot-2.0-Funktionalität für jede logische WLAN-Schnittstelle separat zu aktivieren bzw. zu deaktivieren sowie zu konfigurieren.

Ein Teil der zu konfigurierenden Parameter ist in sogenannte „Profile" ausgelagert. Über Profile gruppieren Sie Reihen unterschiedlicher Parameter in Listen, auf die Sie aus den einzelnen Dialogen lediglich referenzieren. Im Wesentlichen handelt es sich dabei um Profile für ANQP-Datenpakete sowie Hotspot 2.0. Die Beziehungen zwischen den Profillisten untereinander stellen sich wie folgt dar:

```
|-- Interfaces
  |-- ANQP-Profile
    |-- NAI-Realms
    |-- Cellular-Netzwerk Informations-Liste
    |-- Netzwerk-Authentifizierungs-Typen
  |-- Hotspot 2.0 Profile
    |-- Betreiber-Liste
    |-- OSU-Anbieter
```

Aktivierung für Interfaces

Die Tabelle **Interfaces** ist die höchste Verwaltungsebene für IEEE 802.11u und Hotspot 2.0. Hier haben Sie die Möglichkeit, die Funktionen für jede Schnittstelle ein- oder auszuschalten, ihnen unterschiedliche Profile zuzuweisen oder allgemeine Einstellungen vorzunehmen.



Interface

Name der logischen WLAN-Schnittstelle, die Sie gerade bearbeiten.

IEEE 802.11u aktiviert

Aktivieren oder deaktivieren Sie an der betreffenden Schnittstelle die Unterstützung für Verbindungen nach IEEE 802.11u. Wenn Sie die Unterstüzung aktivieren, sendet das Gerät für die Schnittstelle – bzw. für die dazugehörige SSID – das Interworking-Element in den Beacons / Probes. Dieses Element dient als Erkennungsmerkmal für IEEE-802.11u-fähige Verbindungen: Es enthält z. B. das Internet-Bit, das ASRA-Bit, die HESSID sowie den Standort-Gruppen-Code und den Standort-Typ-Code. Diese Einzelelemente nutzen 802.11u-fähige Geräte als erste Filterkriterien bei der Netzsuche.

Hotspot 2.0

Aktivieren oder deaktivieren Sie an der betreffenden Schnittstelle die Unterstützung für Hotspot 2.0 der Wi-Fi Alliance®. Hotspot 2.0 erweitert den IEEE-802.11u-Standard um zusätzliche Netzwerkinformationen, welche Stationen über einen ANQP-Request abfragen können. Dazu gehören z. B. der betreiberfreundliche Name, die Verbindungs-Fähigkeiten, die Betriebsklasse und die WAN-Metriken. Über diese zusätzlichen Informationen sind Stationen dazu in der Lage, die Wahl eines Wi-Fi-Netzwerkes noch selektiver vorzunehmen.

Internet

Wählen Sie aus, ob das Internet-Bit gesetzt wird. Über das Internet-Bit informieren Sie alle Stationen explizit darüber, dass das Wi-Fi-Netzwerk den Internetzugang erlaubt. Aktivieren Sie diese Einstellung, sofern über Ihr Gerät nicht nur interne Dienste erreichbar sind.

Über diese Funktion teilen Sie lediglich die Verfügbarkeit einer Internetverbindung mit. Die entsprechenden Regularien konfigurieren Sie unabhängig von dieser Option über die Firewall!

ASRA – Weitere Schritte für den Zugang erforderlich

Wählen Sie aus, ob das ASRA-Bit (Additional Step Required for Access) gesetzt wird. Über das ASRA-Bit informieren Sie alle Stationen explizit darüber, dass für den Zugriff auf das Wi-Fi-Netzwerk noch weitere Authentifizierungsschritte notwendig sind. Aktivieren Sie diese Einstellung, wenn Sie z. B. eine Online-Registrierung, eine zusätzliche Web-Authentifikation oder eine Zustimmungswebseite für Ihre Nutzungsbedingungen eingerichtet haben.

Denken Sie daran, in der Tabelle **Netzwerk-Authentifizierungs-Typen** eine Weiterleitungsadresse für die zusätzliche Authentifizierung anzugeben und / oder **WISPr** für das Public Spot-Modul zu konfigurieren, wenn Sie das ASRA-Bit setzen.

Netzwerk-Typ

Wählen Sie aus der vorgegebenen Liste einen Netzwerk-Typ aus, der das Wi-Fi-Netzwerk hinter der ausgewählten Schnittstelle am ehesten charakterisiert. Anhand der hier getroffenen Einstellung haben Nutzer die Wahl, die Netzsuche ihrer Geräte auf bestimmte Netzwerk-Typen zu beschränken. Mögliche Werte sind:

Privates Netzwerk

Beschreibt Netzwerke, in denen unauthorisierte Benutzer nicht erlaubt sind. Wählen Sie diesen Typ z. B. für Heimnetzwerke oder Firmennetzwerke, bei denen der Zugang auf die Mitarbeiter beschränkt ist.

Privat mit Gast-Zugang

Wie **Privates Netzwerk**, doch mit Gast-Zugang für unauthorisierte Benutzer. Wählen Sie diesen Typ z. B. für Firmennetzwerke, bei denen neben den Mitarbeitern auch Besucher das Wi-Fi-Netzwerk nutzen dürfen.

Kostenpflichtiges Öffentliches Netzwerk

Beschreibt öffentliche Netzwerke, die für jedermann zugänglich sind und deren Nutzung gegen Entgelt möglich ist. Informationen zu den Gebühren sind evtl. auf anderen Wegen abrufbar (z. B: IEEE 802.21, HTTP/HTTPS- oder DNS-Weiterleitung). Wählen Sie diesen Typ z. B. für Hotspots in Geschäften oder Hotels, die einen kostenpflichtigen Internetzugang anbieten.

Kostenloses öffentliches Netzwerk

Beschreibt öffentliche Netzwerke, die für jedermann zugänglich sind und für deren Nutzung kein Entgelt anfällt. Wählen Sie diesen Typ z. B. für Hotspots im öffentlichen Nah- und Fernverkehr oder für kommunale Netzwerke, bei denen der Wi-Fi-Zugang eine inbegriffene Leistung ist.

Persönliches Geräte-Netzwerk

Beschreibt Netzwerke, die drahtlose Geräte im Allgemeinen verbinden. Wählen Sie diesen Typ z. B. bei angeschlossenen Digital-Kameras, die via WLAN mit einem Drucker verbunden sind.

Netzwerk für Notdienste

Beschreibt Netzwerke, die für Notdienste bestimmt und auf diese beschränkt sind. Wählen Sie diesen Typ z. B. bei angeschlossenen ESS- oder EBR-Systemen.

Test oder experimentell

Beschreibt Netzwerke, die zu Testzwecken eingerichtet sind oder sich noch im Aufbaustadium befinden.

Wildcard

Platzhalter für bislang undefinierte Netzwerk-Typen.

HESSID-Modus

Geben Sie an, woher das Gerät seine HESSID für das homogene ESS bezieht. Als homogenes ESS bezeichnet man den Verbund einer bestimmten Anzahl von Access Points, die alle dem selben Netzwerk angehören. Als weltweit eindeutige Kennung (HESSID) dient die MAC-Adresse eines angeschlossenen Access Points. Die SSID taugt in diesem Fall nicht als Kennung, da in einer Hotspot-Zone unterschiedliche Netwerkbetreiber die gleiche SSID vergeben haben können, z. B. durch Trivialnamen wie „HOTSPOT". Mögliche Werte für den HESSID-Modus sind:

BSSID

Wählen Sie diesen Eintrag, um die BSSID des Gerätes als HESSID für Ihr homogenes ESS festzulegen.

Benutzer

Wählen Sie diesen Eintrag, um eine HESSID manuell zu vergeben.

Keiner

Wählen Sie diesen Eintrag, um die Schnittstelle keinem homogenen ESS zuzuordnen und aus dem Geräteverbund zu isolieren.

HESSID-MAC

Sofern Sie als **HESSID-Modus** die Einstellung `Benutzer` gewählt haben, tragen Sie hier die HESSID Ihres homogenen ESS in Form einer 6-oktettigen MAC-Adresse ein. Wählen Sie für die HESSID die BSSID eines beliebigen Access Apoints in Ihrem homogenen ESS in Großbuchstaben und ohne Trennzeichen, z. B. „008041AEFD7E“ für die MAC-Adresse 00:80:41:ae:fd:7e.

Sofern Ihr Gerät nicht in mehreren homogenen ESS vertreten ist, ist die HESSID für alle Schnittstellen identisch!

ANQP-Profil

Wählen Sie aus der Liste ein ANQP-Profil aus. ANQP-Profile legen Sie im Konfigurationsmenü über die gleichnamige Schaltfläche an.

Hotspot 2.0 Profile

Wählen Sie aus der Liste ein Hotspot-2.0-Profil aus. Hotspot-2.0-Profile legen Sie im Konfigurationsmenü über die gleichnamige Schaltfläche an.

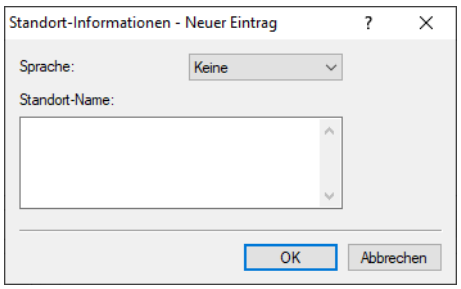
ANQP-Datenpakete konfigurieren

Standort-Informationen und -Gruppe

Über die Tabelle **Standort-Informationen** sowie den nachgelagerten Dialogabschnitt zur **Standort-Gruppe** und zum **Standort-Typ-Code** verwalten Sie die Angaben zum Standort des Access Points.

Mit Angaben zu den **Standort-Informationen** unterstützen Sie einen Nutzer bei der Auswahl des richtigen Hotspots im Falle einer manuellen Suche. Verwenden in einer Hotspot-Zone mehrere Betreiber (z. B. mehrere Cafés) die gleiche SSID, kann der Nutzer mit Hilfe der Standort-Informationen die passende Lokalität eindeutig identifizieren.

Über die **Standort-Gruppe** und den **Standort-Typ-Code** ordnen Sie dagegen Ihr Gerät – im Gegensatz zu den frei definierbaren Standort-Informationen – in eine vorgegebene Kategorie ein.



Sprache

Sie haben die Möglichkeit, für jede Sprache individuelle Informationen zum Standort des Access Points anzugeben. Ihre Nutzer bekommen dann die zur ihrer Sprache passenden Standort-Namen angezeigt. Ist eine Sprache für einen Nutzer nicht vorhanden, entscheidet seine Station, z. B. anhand der Default-Sprache.

Standort-Name

Tragen Sie hier für die ausgewählte Sprache eine kurze Beschreibung zum Standort des Gerätes ein, z. B.

```
Eiscafé Valenzia
Am Markt 3
12345 Musterstadt
```

Die **Standort-Gruppe** beschreibt das Umfeld, in dem Sie den Access Point einsetzen. Sie definieren sie global für alle Sprachen. Die möglichen Werte, festgelegt durch den „Venue Group Code", werden durch den 802.11u-Standard vorgegeben.

Über den **Standort-Typ-Code** haben Sie die Möglichkeit, die Standort-Gruppe weiter zu spezifizieren. Auch hier sind die Werte durch den Standard spezifiziert. Die möglichen Typ-Codes entnehmen Sie bitte der nachfolgenden Tabelle.

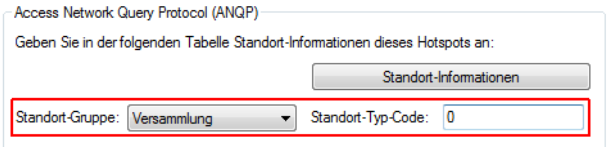


Tabelle 3: Übersicht möglicher Werte für Standort-Gruppen und -Typen

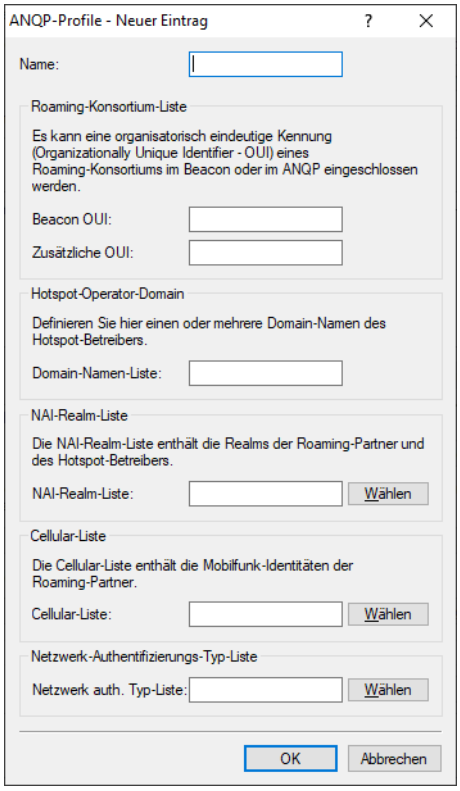
Standort-Gruppe	Standort-Typ-Code
Unspezifiziert	
Versammlung	0 = Unspezifizierte Versammlung 1 = Bühne 2 = Stadion 3 = Passagier-Terminal (z. B. Flughafen, Busbahnhof, Fähranleger, Bahnhof) 4 = Amphitheater 5 = Vergnügungspark 6 = Andachtsstätte 7 = Kongresszentrum 8 = Bücherei 9 = Museum 10 = Restaurant 11 = Schauspielhaus 12 = Bar 13 = Café 14 = Zoo, Aquarium 15 = Notfallleitstelle
Geschäft	0 = Unspezifiziertes Geschäft 1 = Arztpraxis 2 = Bank 3 = Feuerwache 4 = Polizeiwache 6 = Post 7 = Büro 8 = Forschungseinrichtung 9 = Anwaltskanzlei
Ausbildung	0 = Unspezifizierte Ausbildung 1 = Grundschule 2 = Weiterführende Schule 3 = Hochschule

Standort-Gruppe	Standort-Typ-Code
Fabrik und Industrie	› 0 = Unspezifizierte Fabrik und Industrie › 1 = Fabrik
Institutional	› 0 = Unspezifizierte Institution › 1 = Krankenhaus › 2 = Langzeit-Pflegeeinrichtung (z. B. Seniorenheim, Hospiz) › 3 = Entzugsklinik › 4 = Einrichtungsverbund › 5 = Gefängnis
Handel	› 0 = Unspezifizierter Handel › 1 = Ladengeschäft › 2 = Lebensmittelmarkt › 3 = KFZ-Werkstatt › 4 = Einkaufszentrum › 5 = Tankstelle
Wohnheim	› 0 = Unspezifiziertes Wohnheim › 1 = Privatwohnsitz › 2 = Hotel oder Motel › 3 = Studentenwohnheim › 4 = Pension
Lager	› 0 = Unspezifiziertes Lager
Dienste und sonstiges	› 0 = Unspezifizierter Dienst und sonstiges
Fahrzeug	› 0 = Unspezifiziertes Fahrzeug › 1 = Personen- oder Lastkraftwagen › 2 = Flugzeug › 3 = Bus › 4 = Fähre › 5 = Schiff oder Boot › 6 = Zug › 7 = Motorrad
Außen	› 0 = Unspezifizierter Außenbereich › 1 = Städtisches Wi-Fi-Netzwerk (Muni-Mesh-Netzwerk) › 2 = Stadtpark › 3 = Rastplatz › 4 = Verkehrsregelung › 5 = Bushaltestelle › 6 = Kiosk

ANQP-Profile

Über diese Tabelle verwalten Sie die Profillisten für ANQP. **ANQP-Profile** bieten Ihnen die Möglichkeit, bestimmte ANQP-Elemente zu gruppieren und sie in der Tabelle **Interfaces** unabhängig voneinander logischen WLAN-Schnittstellen

zuzuweisen. Zu diesen Elementen gehören z. B. Angaben zu Ihren OIs, Domains, Roaming-Partnern und deren Authentifizierungsmethoden. Ein Teil der Elemente ist in weitere Profillisten ausgelagert.



Name

Vergeben Sie hierüber einen Namen für das ANQP-Profil. Dieser Name erscheint später innerhalb der Interfaces-Tabelle in der Auswahlliste für die ANQP-Profile.

Beacon OUI

Organizationally Unique Identifier, abgekürzt OUI, vereinfacht OI. Als Hotspot-Betreiber tragen Sie hier die OI des Roaming-Partners ein, mit dem Sie einen Vertrag abgeschlossen haben. Sind Sie als Hotspot-Betreiber gleichzeitig der Service-Provider, tragen Sie hier die OI Ihres Roaming-Konsortiums oder Ihre eigene OI ein. Ein Roaming-Konsortium besteht aus einer Gruppe von Service-Providern, die untereinander Vereinbarungen zum gegenseitigen Roaming getroffen haben. Um eine OI zu erhalten, muss sich ein solches Konsortium – ebenso wie ein einzelner Service-Provider – bei der IEEE registrieren lassen.

Es besteht die Möglichkeit, bis zu 3 OIs parallel anzugeben, z. B. für den Fall, dass Sie als Betreiber Verträge mit mehreren Roaming-Partnern haben. Mehrere OIs trennen Sie durch eine kommaseparierte Liste, z. B. `00105E,00017D,00501A`.

Das Gerät strahlt die eingegebene(n) OI(s) in seinen Beacons aus. Soll das Gerät mehr als 3 OIs übertragen, lassen sich diese unter **Zusätzliche OUI** konfigurieren. Zusätzliche OIs werden allerdings erst nach dem GAS-Request einer Station übertragen; sie sind für die Stationen also nicht unmittelbar sichtbar!

Zusätzliche OUI

Tragen Sie hier die OI(s) ein, die das Gerät nach dem GAS-Request einer Station zusätzlich aussendet. Mehrere OIs trennen Sie durch eine kommaseparierte Liste, z. B. `00105E,00017D,00501A`.

Domain-Namen-Liste

Tragen Sie hier eine oder mehrere Domains ein, über die Sie als Hotspot-Betreiber verfügen. Mehrere Domain-Namen trennen Sie durch eine kommaseparierte Liste, z. B. `providerX.org,provx-mobile.com,wifi.mnc410.provX.com`. Für Subdomains reicht es aus, lediglich den obersten gültigen Domain-Namen anzugeben. Hat ein Nutzer z. B. providerX.org als Heimat-Provider in seinem Gerät konfiguriert, werden dieser Domain auch Access Points mit dem Domain-Namen wi-fi.providerX.org zugerechnet. Bei der Suche nach passenden Hotspots bevorzugt eine Station immer den Hotspot seines Heimat-Providers, um mögliche Roaming-Kosten über den Access Point eines Roaming-Partners zu vermeiden.

NAI-Realm-Liste

Wählen Sie aus der Liste ein NAI-Realm-Profil aus. Profile für NAI-Realms legen Sie im Konfigurationsmenü über die Schaltfläche **NAI-Realms** an.

Cellular-Liste

Wählen Sie aus der Liste eine Mobilfunk-Identität aus. Identitäten für Mobilfunknetzwerke legen Sie – wie bei einem Profil – im Konfigurationsmenü über die Schaltfläche **Cellular-Netzwerk Informations-Liste** an.

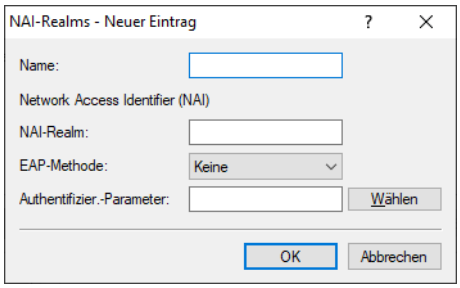
Netzwerk auth. Typ-Liste

Wählen Sie aus der Liste einen Authentifizierungs-Profil aus. Profile zur Netzwerk-Authentifizierung legen Sie im Konfigurationsmenü über die Schaltfläche **Netzwerk-Authentifizierungs-Typen** an.

Zusätzlich haben Sie über die Konsole die Möglichkeit, Ihren Nutzern auch den Typ der verfügbaren IP-Adresse anzuzeigen, den diese nach einer erfolgreichen Authentifizierung vom Netzwerk erhalten können. Sie erreichen die betreffenden Parameter **IPv4-Addr-Type** und **IPv6-Addr-Type** über den Pfad **Setup** > **IEEE802.11u** > **ANQP-General**.

NAI-Realms

Über diese Tabelle verwalten Sie die Profillisten für die NAI-Realms. Mit diesen Listen haben Sie die Möglichkeit, bestimmte ANQP-Elemente zu gruppieren. Hierzu gehören die Realms des Hotspot-Betreibers und seiner Roaming-Partner mitsamt der zugehörigen Authentifizierungs-Methoden und -Parameter. Stationen nutzen diese Liste, um anhand der hier hinterlegten Angaben festzustellen, ob sie für den Hotspot-Betreiber oder einen seiner Roaming-Partner über gültige Anmeldedaten verfügen.



Name

Vergeben Sie hierüber einen Namen für das NAI-Realm-Profil, z. B. den Namen des Service-Providers oder Dienstes, zu dem der NAI-Realm gehört. Dieser Name erscheint später im ANQP-Profil in der Auswahl für die **NAI-Realm-Liste**.

NAI-Realm

Geben Sie hier den Realm für das Wi-Fi-Netzwerk an. Der NAI-Realm selbst ist ein Identifikationspaar aus einem Benutzernamen und einer Domäne, welches durch reguläre Ausdrücke erweitert werden kann. Die Syntax für einen NAI-Realm wird in *RFC 2486* definiert und entspricht im einfachsten Fall

`<username>@<realm>`; für `user746@providerX.org` lautet der entsprechende Realm also `providerX.org`.

EAP-Methode

Wählen Sie aus der Liste eine Authentifizierungsmethode für den NAI-Realm aus. EAP steht dabei für das Authentifizierungs-Protokoll (Extensible Authentication Protocol), gefolgt vom jeweiligen Authentisierungsverfahren. Mögliche Werte sind:

EAP-TLS

Authentifizierung via Transport Layer Security (TLS). Wählen Sie diese Einstellung, wenn die Authentifizierung über den betreffenden NAI-Realm durch ein digitales Zertifikat erfolgt, das der Nutzer installiert.

EAP-SIM

Authentifizierung via Subscriber Identity Module (SIM). Wählen Sie diese Einstellung, wenn die Authentifizierung über den betreffenden NAI-Realm durch das GSM Subscriber Identity Module (die SIM-Karte) der Station erfolgt.

EAP-TTLS

Authentifizierung via Tunneled Transport Layer Security (TTLS). Wählen Sie diese Einstellung, wenn die Authentifizierung über den betreffenden NAI-Realm durch einen Benutzernamen und ein Passwort erfolgt. Zur Sicherheit wird die Verbindung bei diesem Verfahren getunnelt.

EAP-AKA

Authentifizierung via Authentication and Key Agreement (AKA). Wählen Sie diese Einstellung, wenn die Authentifizierung über den betreffenden NAI-Realm durch das UTMS Subscriber Identity Module (die USIM-Karte) der Station erfolgt.

Keine

Wählen Sie diese Einstellung, wenn der betreffende NAI-Realm keine Authentifizierung erfordert.

Authentifizierungs-Parameter

Klicken Sie die zur EAP-Methode passenden Authentifizierungs-Parameter, z. B. für EAP-TTLS

`NonEAPAuth.MSCHAPV2,Credential.UserPass`

oder für EAP-TLS `Credentials.Certificate`.

Mögliche Werte sind:

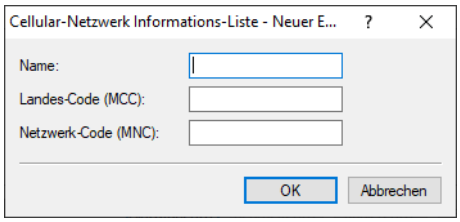
Tabelle 4: Übersicht der möglichen Authentifizierungs-Parameter

Parameter	Sub-Parameter	Erläuterung
NonEAPAuth.		Bezeichnet das Protokoll, welches der Realm für die Phase-2-Authentifizierung erfordert:
	PAP	Password Authentication Protocol
	CHAP	Challenge Handshake Authentication Protocol, ursprüngliche CHAP-Implementierung, spezifiziert im *RFC 1994*
	MSCHAP	CHAP-Implementierung von Microsoft v1, spezifiziert im *RFC 2433*
	MSCHAPV2	CHAP-Implementierung von Microsoft v2, spezifiziert im *RFC 2759*
Credentials.		Beschreibt die Art der Authentifizierung, die der Realm akzeptiert:

Parameter	Sub-Parameter	Erläuterung
	SIM	SIM-Karte
	USIM	USIM-Karte
	NFCSecure	NFC-Chip
	HWToken*	Hardware-Token
	SoftToken*	Software-Token
	Certificate	Digitales Zertifikat
	UserPass	Benutzername und Passwort
	None	Keine Zugangsdaten erforderlich
TunnelEAPCredentials.*		
	SIM*	SIM-Karte
	USIM*	USIM-Karte
	NFCSecure*	NFC-Chip
	HWToken*	Hardware-Token
	SoftToken*	Software-Token
	Certificate*	Digitales Zertifikat
	UserPass*	Benutzername und Passwort
	Anonymous*	Anonyme Anmeldung

Cellular-Netzwerk Informations-Liste

Über diese Tabelle verwalten Sie die Identitätslisten für die Mobilfunknetze. Mit diesen Listen haben Sie die Möglichkeit, bestimmte ANQP-Elemente zu gruppieren. Hierzu gehören die Netzwerk- und Landes-Codes des Hotspot-Betreibers und seiner Roaming-Partner. Stationen mit SIM- oder USIM-Karte nutzen diese Liste, um anhand der hier hinterlegten Angaben festzustellen, ob der Hotspot-Betreiber zu ihrer Mobilfunkgesellschaft gehört oder einen Roaming-Vertrag mit ihrer Mobilfunkgesellschaft hat.



Name

Vergeben Sie hierüber einen Namen für die Mobilfunk-Identität, z. B. ein Kürzel des Netzanbieters in Kombination mit dem verwendeten Mobilfunkstandard. Dieser Name erscheint später im ANQP-Profil in der Auswahl für die **Cellular-Liste**.

Landes-Code (MCC)

Geben Sie hier den Mobile Country Code (MCC) des Hotspot-Betreibers oder seiner Roaming-Partner ein, bestehend aus 2 oder 3 Zeichen, z. B. `262` für Deutschland.

* Der betreffende Parameter oder Sub-Parameter ist im Rahmen der Passpoint™-Zertifizierung für zukünftige Einsatzzwecke reserviert worden, findet gegenwärtig jedoch keine Verwendung.

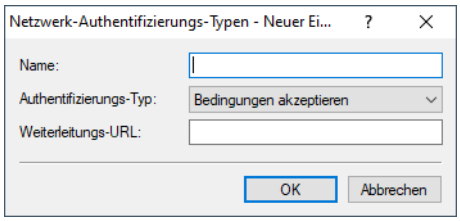
Netzwerk-Code (MNC)

Geben Sie hier den Mobile Network Code (MNC) des Hotspot-Betreibers oder seiner Roaming-Partner ein, bestehend aus 2 oder 3 Zeichen.

Netzwerk-Authentifizierungs-Typen

Über diese Tabelle verwalten Sie Adressen, an die das Gerät Stationen für einen zusätzlichen Authentifizierungsschritt weiterleitet, nachdem sich die Station bereits beim Hotspot-Betreiber oder einem seiner Roaming-Partner erfolgreich authentisiert hat. Pro Authentifizierungs-Typ ist nur eine Weiterleitungsangabe erlaubt.

Denken Sie daran, das ASRA-Bit in der Tabelle **Interfaces** zu setzen, wenn Sie einen zusätzlichen Authentifizierungsschritt einrichten!



Name

Vergeben Sie hierüber einen Namen für den Listeneintrag, z. B. `AGB akzeptieren`. Dieser Name erscheint später im ANQP-Profil in der Auswahl für die **Netzwerk auth. Typ-Liste**.

Authentifizierungs-Typ

Wählen Sie aus der Auswahlliste den Kontext, vor dem die Weiterleitung gilt. Mögliche Werte sind:

Bedingungen akzeptieren

Es ist ein zusätzlicher Authentifizierungsschritt eingerichtet, bei dem ein Benutzer die Nutzungsbedingungen des Betreibers akzeptieren muss.

Online Registrierung

Es ist ein zusätzlicher Authentifizierungsschritt eingerichtet, bei dem sich ein Benutzer erst online registrieren muss.

HTTP-Weiterleitung

Es ist ein zusätzlicher Authentifizierungsschritt eingerichtet, zu dem ein Benutzer via HTTP weitergeleitet wird.

DNS-Weiterleitung

Es ist ein zusätzlicher Authentifizierungsschritt eingerichtet, zu dem ein Benutzer via DNS weitergeleitet wird.

Weiterleitungs-URL

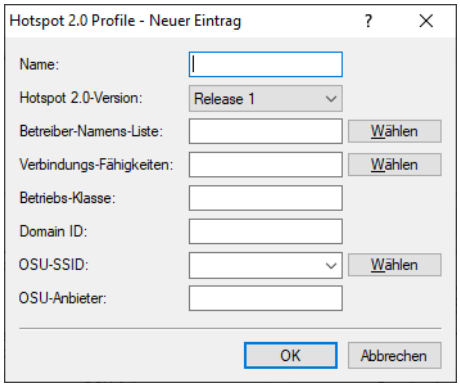
Geben Sie die Adresse an, an die das Gerät Stationen für den zusätzlichen Authentifizierungsschritt weiterleitet.

Hotspot 2.0 konfigurieren

Hotspot 2.0 Profile

Über diese Tabelle verwalten Sie die Profillisten für Hotspot 2.0. **Hotspot 2.0 Profile** bieten Ihnen die Möglichkeit, bestimmte ANQP-Elemente (die der Hotspot-2.0-Spezifikation) zu gruppieren und sie in der Tabelle **Interfaces** unabhängig voneinander logischen WLAN-Schnittstellen zuzuweisen. Zu diesen Elementen gehören z. B. der betreiberfreundliche

Name, die Verbindungs-Fähigkeiten, die Betriebsklasse und die WAN-Metriken. Ein Teil der Elemente ist in weitere Profillisten ausgelagert.



Name

Vergeben Sie hierüber einen Namen für das Hotspot-2.0-Profil. Dieser Name erscheint später innerhalb der Interfaces-Tabelle in der Auswahlliste für die Hotspot-2.0-Profile.

Hotspot 2.0 Version

Stellen Sie das in diesem Profil unterstützte Release von Hotspot 2.0 ein.

Ein Client muss das entsprechende Release beherrschen, um sich verbinden zu können.

Betreiber-Namens-Liste

Wählen Sie aus der Liste das Profil eines Hotspot-Betreibers aus. Profile für Hotspot-Betreiber legen Sie im Konfigurationsmenü über die Schaltfläche **Betreiber-Liste** an.

Verbindungs-Fähigkeiten

Wählen Sie für jeden Dienst die Verbindungs-Fähigkeit aus. Stationen nutzen diese Liste, um anhand der hier hinterlegten Angaben vor einem Netzbeitritt festzustellen, ob Ihr Hotspot die benötigten Dienste (z. B. Internetzugang, SSH, VPN) überhaupt erlaubt. Aus diesem Grund sollten so wenig Einträge wie möglich den Status „unbekannt" tragen. Mögliche Statuswerte für die einzelnen Dienste sind „closed" (`-C`), „open" (`-O`) oder „unknown" (`-U`):

- `ICMP`: Geben Sie an, ob Sie den Austausch von Informations- und Fehlermeldungen via ICMP erlauben.
- `TCP-FTP`: Geben Sie an, ob Sie Dateiübertragungen via FTP erlauben.
- `TCP-SSH`: Geben Sie an, ob Sie verschlüsselte Verbindungen via SSH erlauben.
- `TCP-HTTP`: Geben Sie an, ob Sie Internetverbindungen via HTTP/HTTPS erlauben.
- `TCP-TLS`: Geben Sie an, ob Sie verschlüsselte Verbindungen via TLS erlauben.
- `TCP-PPTP`: Geben Sie an, ob Sie das Tunneln von VPN-Verbindungen via PPTP erlauben.
- `TCP-VOIP`: Geben Sie an, ob Sie Internettelefonie via VoIP (TCP) erlauben.
- `UDP-IPSEC-500`: Geben Sie an, ob Sie IPsec via UDP und Port 500 erlauben.
- `UDP-VOIP`: Geben Sie an, ob Sie Internettelefonie via VoIP (UDP) erlauben.
- `UDP-IPSEC-4500`: Geben Sie an, ob Sie IPsec via UDP und Port 4500 erlauben.
- `ESP`: Geben Sie an, ob Sie ESP (Encapsulating Security Payload) für IPsec erlauben.

Wenn Sie nicht wissen, ob in Ihrem Netzwerk ein Dienst verfügbar und seine Ports offen oder geschlossen sind, oder Sie gegenüber einer Station bewusst keine Angabe zum Status machen wollen, wählen Sie eine `-U`-Einstellung.

Über diesen Dialog legen Sie keine Berechtigungen fest! Die Angaben dienen den Stationen lediglich dazu, den Netzbeitritt über Ihr Gerät zu entscheiden. Spezifische Zugangsberechtigungen für Ihr Netzwerk konfigurieren Sie über andere Gerätefunktionen, wie z. B. die Firewall / QoS.

Betriebs-Klasse

Geben Sie hier den Code für die globale Betriebsklasse des Access Points an. Über die Betriebs-Klasse teilen Sie einer Station mit, auf welchen Frequenzbändern und Kanälen Ihr Access-Point verfügbar ist. Beispiel:

- `81`: Betrieb bei 2,4 GHz mit Kanälen 1–13
- `116`: Betrieb bei 40 MHz mit Kanälen 36 und 44

Die für Ihr Gerät passende Betriebsklasse entnehmen Sie bitte dem IEEE Standard 802.11-2012, Anhang E, Tabelle E-4: Global operating classes; erhältlich unter *standards.ieee.org*.

Domain ID

Die Domain-ID gibt an, welcher ANQP-Server verwendet wird. Alle Access Points bzw. SSIDs mit gleicher Nummer / Domain-ID (16-Bit-Wert) verwenden den gleichen ANQP-Server.

Ein Client würde somit auf eine ANQP-Anfrage auf Access Points / SSIDs mit identischer Domain-ID immer die gleiche Antwort erhalten. Um unterschiedliche Antworten zu erhalten, müsste der Client nach unterschiedlichen Domain-IDs Ausschau halten.

OSU-SSID

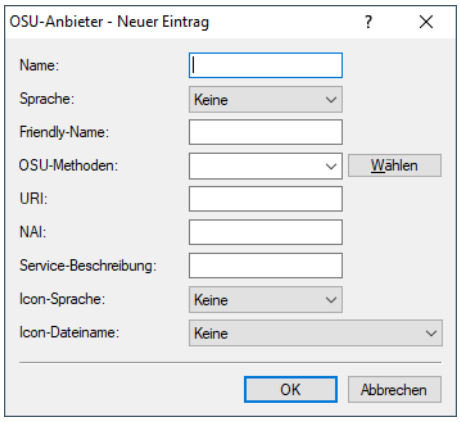
Name der SSID, die Zugang zum OSU-Server bietet.

OSU-Anbieter

Liste der OSU-Providernamen aus *OSU-Anbieter* auf Seite 94, die im Profil unterstützt werden.

OSU-Anbieter

In dieser Tabelle konfigurieren Sie die OSU-Provider für Online Sign-Up bei Passpoint® Release 2.



Name

Geben Sie diesem OSU-Provider einen Namen, über den Sie ihn später referenzieren können. Wenn der gleiche Name erneut verwendet wird, dann kann dieser Provider z. B. für mehrere Spachen verwendet werden.

Sprache

Stellen Sie die von diesem OSU-Provider unterstützte Sprache ein.

Friendly-Name

Geben Sie diesem OSU-Provider einen sprechenden Namen.

OSU-Methoden

Stellen Sie hier die von diesem OSU-Provider verwendeten OSU-Methoden ein. Möglich sind „OMA-DM“ oder „SOAP-XML-SPP“.

Mögliche Methoden innerhalb des Online Sign-Up-Servers bei Passpoint® Release 2:

- OMA – Open Mobile Alliance
- DM – Device Management
- SOAP – Simple Object Access Protocol
- XML – eXtended Markup Language
- SPP – Subscription Provisioning Protocol

URI

Geben Sie eine URI ein, unter der ein Client den OSU-Server erreicht.

NAI

Geben Sie den Network Access Identifier (NAI) für diesen OSU-Provider ein.

Service-Beschreibung

Geben Sie hier einen Beschreibungstext für diesen Dienst ein.

Icon-Sprache

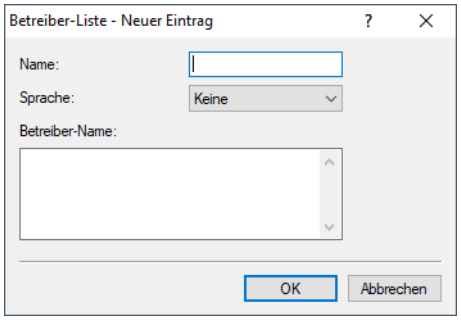
Stellen Sie hier die Sprache des ausgewählten Icons ein.

Icon-Dateiname

Wählen Sie ein Icon für diesen OSU-Provider aus. Die Icons können über die WEBconfig als Datei hochgeladen werden. Als Dateiformat empfehlen wir PNG.

Betreiber-Liste

Über diese Tabelle verwalten Sie die Klartext-Namen der Hotspot-Betreiber. Ein Eintrag in dieser Tabelle bietet Ihnen die Möglichkeit, einen benutzerfreundlichen Betreiber-Namen an die Stationen zu senden, den diese dann anstelle der Realms anzeigen können. Ob sie das allerdings tatsächlich tun, ist abhängig von der Implementierung.



Name

Vergeben Sie hierüber einen Namen für den Eintrag, z. B. eine Indexnummer oder Kombination aus Betreiber-Name und Sprache.

Sprache

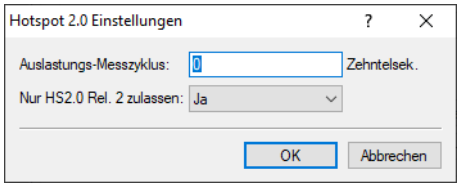
Wählen Sie aus der Liste eine Sprache für den Hotspot-Betreiber aus.

Betreiber-Name

Geben Sie hier den Klartext-Namen des Hotspot-Betreibers ein.

Hotspot 2.0 Einstellungen

In dieser Tabelle konfigurieren Sie spezielle Einstellungen für Hotspot 2.0.



Auslastungs-Messzyklus

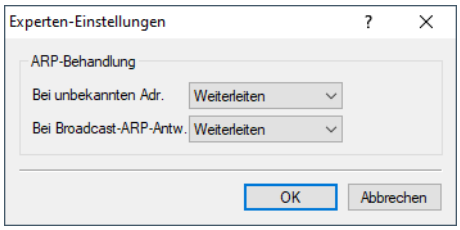
Messzyklus der WAN-Down- / Uplink-Geschwindigkeiten in Zehntelsekunden.

Nur Hotspot 2.0 Release 2 zulassen

Für HotSpot 2.0 Release 2 wird gefordert, nur Release 2-Clients zuzulassen. Dies kann durch diesen Schalter ausgeschaltet werden.

Experten-Einstellungen

In dieser Tabelle konfigurieren Sie Experten-Einstellungen für Hotspot 2.0. Die Einstellungen in diesem Menü dienen der Unterdrückung von ARP (IPv4) bzw. Neighbor Solicitation (IPv6) innerhalb der SSID zwischen den Clients. Alternativ kann dies i.d.R. auch durch die Unterdrückung von Broad- / Multicasts via **Nur Unicasts übertragen, Broad- und Multicasts unterdrücken** in den logischen WLAN-Netzwerkeinstellungen gelöst werden.



Bei unbekannten Adressen

Bei unbekannten Adressen wird das Paket entweder weitergeleitet oder verworfen.

Bei Broadcast-ARP-Antworten

Bei Broadcasts wird das Paket entweder weitergeleitet oder verworfen.

Schnittstelle für Property-Management-Systeme

Sofern Sie ein Property Management System (PMS) einsetzen, bieten Ihnen bestimmte Gerätetypen und -serien die Möglichkeit, das Public Spot-Modul über die PMS-Schnittstelle mit Ihrer PMS-Datenbank zu verknüpfen. Als Hotelbetreiber erhalten Sie so z. B. die Möglichkeit, einem Gast bereits bei der Registrierung automatisch einen Zugang zu Ihrem Public Spot bereitzustellen. Dieser Zugang kann wahlweise kostenlos oder kostenpflichtig (über Prepaid erworbenes Zeitguthaben) erfolgen, wobei anfallende Gebühren auf die Zimmerrechnung des Gastes gebucht werden. Als Zugangsdaten dienen

ihm dabei sein Nachname, seine Zimmernummer sowie optional eine weitere Sicherheitskennung (z. B. seine Registrierungsnummer oder das Abreisedatum).

Gegenüber einer Voucher-Lösung bietet Ihnen die aktivierte PMS-Schnittstelle den Vorteil, dass keine weiteren administrativen Schritte für die Einrichtung und Verwaltung eines Public Spot-Benutzerkontos mehr notwendig sind: Das Gerät legt für einen Gast selbstständig ein Benutzerkonto an, sobald dieser Ihren Public Spot aufruft und sich mit seinen Registrierungsdaten authentifiziert. Registrierungsänderungen, die diesen Gast zukünftig betreffen (Zimmerwechsel, Änderung des Abreisedatums, Check-out, etc.), übernimmt das Gerät eigenständig von Ihrem PMS.

Folgende Anmeldemethoden werden derzeit unterstützt:

1. Voucher
2. PMS-Anmeldung
3. PMS-Anmeldung und Voucher
4. E-Mail
5. SMS

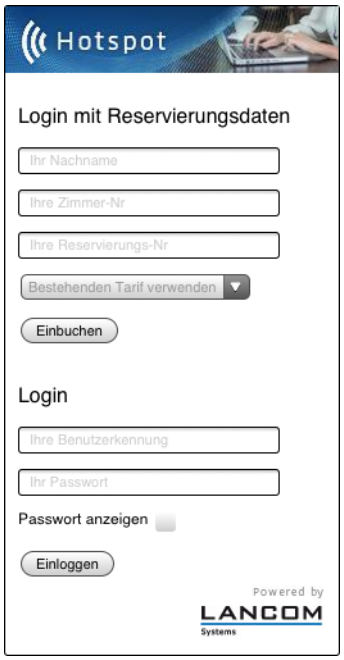
Mit Anmeldemethode (2) kann z. B. für Hotelgäste die Anmeldung anhand der Zimmernummer und des Nachnamen erfolgen, während Sie für Gäste im Restaurant Voucher verkaufen (1). Natürlich haben Sie trotz aktivierter PMS-Schnittstelle auch weiterhin die Möglichkeit, Voucher – z. B. für Tagungsgäste oder Besucher – auszugeben (3).

Die Anmeldemethode konfigurieren Sie global pro Gerät; sie ist somit für alle SSIDs bzw. Netze gleich.

Die PMS-Schnittstelle beinhaltet zur Zeit zur Zeit ausschließlich die Unterstützung für das Hotel-Property-Management-System von Micros Fidelio über TCP/IP.

Funktionsbeschreibung

Wenn Sie die PMS-Schnittstelle aktivieren und eine kostenlose oder kostenpflichtige Login-Seite einstellen, erscheinen auf der Public Spot-Portalseite neue Eingabefelder, über die sich der Gast mit seinem Nachnamen, seiner Zimmernummer und ggf. einer weiteren Sicherheitskennung authentisiert. Die Art dieser Kennung legen Sie über das Setup-Menü fest; möglich sind z. B. die Registrierungsnummer oder das An-/Abreisedatum des Gastes. Sofern Sie den Zugang zu Ihrem Hotspot als kostenpflichtig markiert haben, erscheint überdies ein Auswahlmenü, über welches der Gast das Zeitkontingent bzw. den Tarif auswählt, den er via Prepaid erwerben will (z. B. 1 min für 0,20 EUR oder 1 h für 1 EUR). Die dabei entstehenden Kosten bucht das im Hintergrund arbeitende PMS automatisch auf die Zimmerrechnung.



Bei jeder Anmeldung eines Hotelgastes am Public Spot führt das Gerät einen Abgleich der eingegebenen Registrierungsdaten mit den im PMS hinterlegten Registrierungsdaten durch. Erkennt das PMS in den übermittelten Daten eine gültige Übereinstimmung, meldet es diese Information an das Gerät zurück. Das Gerät legt daraufhin eine neue Sitzung für den Hotelgast an und trägt die dazugehörigen Daten die dazugehörige Accounting-Tabelle (WEBconfig: **Status** > **PMS-Interface** > **Accounting**) ein. In dieser Tabelle erfasst das Gerät – neben den Tarifen – sämtliche Hotelgäste, die sich über die PMS-Schnittstelle eingeloggt haben; ganz egal, ob sie dabei eine kostenlose oder kostenpflichtige Verbindung verwenden. Anschließend gibt das Gerät dem Benutzer den Zugang ins Internet frei.

Hat ein Benutzer für einen kostenpflichtigen Zugang ein Zeitkontingent erworben, kann er dieses verlängern, indem er im angemeldeten Zustand weitere Kontingente erwirbt. Meldet sich vor Ablauf seines Kontingents vom Public Spot ab, kann er seine Sitzung zu einem späteren Zeitpunkt wieder aufnehmen, indem er auf der Login-Seite das entsprechende Feld auswählt. Das Gerät speichert seine Sitzung solange zwischen, bis diese ungültig wird; d. h. das Zeitkontingent aufgebraucht ist oder das PMS dem Gerät die Ausbuchung des Hotelgastes meldet. Bei einem erneuten Login und Abgleich mit dem PMS erkennt das Gerät das immer noch gültige Benutzerkonto und führt dieses fort, anstatt ein neues anzulegen.

Ändern sich zwischenzeitlich die Registrierungsinformationen (z. B. die Zimmernummer), bleibt eine bestehende Sitzung davon zunächst unbeeinflusst. Erst, wenn der Hotelgast seine aktuelle Sitzung beendet und sich erneut am Public Spot anmeldet, muss er sich mit seinen geänderten Zugangsdaten authentisieren. Eine Ausnahme bildet die Ausbuchung eines Gastes aus Ihrem PMS (Check-out): Hierbei beendet das Gerät eine bestehende Sitzung sofort.

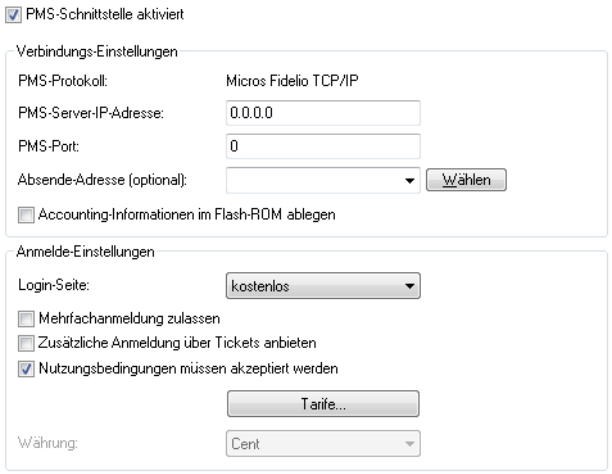
Ihre Nutzer sollten darauf achten, sich ordnungsgemäß vom Public Spot abzumelden. Ohne ordnungsgemäße Abmeldung (hervorgerufen durch einfaches Schließen des Browsers, Trennen der Netzwerkverbindung, Ausschalten des Gerätes, usw.) gilt ein Benutzer als nach wie vor eingeloggt. Dies kann für die Nutzer zu Problemen bei der Wiederanmeldung führen, wenn Sie als Public Spot-Betreiber z. B. keine Mehrfach-Logins erlauben.

Durch die *Stationsüberwachung* haben Sie die Möglichkeit, solche Benutzer nach einer festgelegten Leerlaufzeit automatisch auszuloggen. Dieses Feature ist standardmäßig ausgeschaltet. Für einen kostenpflichtigen Zugang sollten Sie es jedoch unbedingt aktivieren. Andernfalls erfolgt der automatische, geräteinterne Logout erst nach ablaufen des Benutzerkontos, d. h wenn das eingekaufte Zeitkontingent vollständig aufgebraucht ist.

Eine temporäre Abmeldung vom Public Spot verschiebt nicht den Ablaufzeitpunkt eines eingekauften Zeitkontingents! Es nicht möglich, ein bereits gekauftes Zeitguthaben zu "pausieren", um es zu einem späteren Zeitpunkt erneut aufzunehmen. Die Herunterzählung der Zeit beginnt unabhängig vom Anmeldestatus ab Kauf des Kontingents.

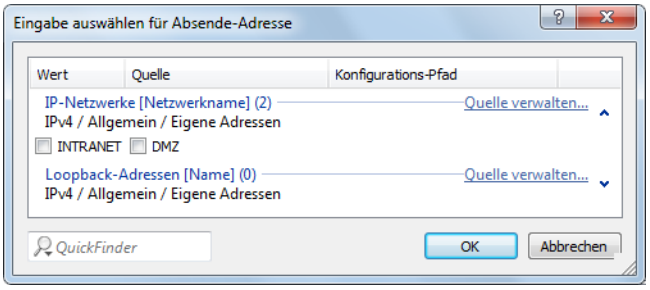
PMS-Schnittstelle konfigurieren

Die PMS-Schnittstelle Ihres Gerätes konfigurieren Sie über den Dialog **Public-Spot** > **PMS-Schnittstelle**.



In diesem Dialog haben Sie folgende Einstellungsmöglichkeiten:

- **PMS-Schnittstelle aktiviert**: Aktivieren oder deaktivieren Sie die PMS-Schnittstelle für das Gerät.
- **PMS-Protokoll**: Bezeichnet das von Ihrem Property-Management-System verwendete Protokoll. Zur Zeit besteht ausschließlich Unterstützung für das Hotel-Property-Management-System von Micros Fidelio über TCP/IP.
- **PMS-Server-IP-Adresse**: Geben Sie hier die IPv4-Adresse Ihres PMS-Servers ein.
- **PMS-Port**: Geben Sie hier den TCP-Port ein, über den Ihr PMS-Server erreichbar ist.
- **Absende-Adresse**: Klicken Sie auf die Schaltfläche **Wählen**, um optional eine andere Adresse zu konfigurieren, an die der PMS-Server seine Antwort-Nachrichten schickt. Standardmäßig schickt der PMS-Server seine Antworten zurück an die IP-Adresse Ihres Gerätes, ohne dass Sie diese hier angeben müssen.



Mögliche Eingabeformen einer Adresse sind:

- Name des IP-Netzwerks (ARF-Netz), dessen Adresse eingesetzt werden soll
- `INT` für die Adresse des ersten Intranets
- `DMZ` für die Adresse der ersten DMZ

  Wenn eine Schnittstelle namens "DMZ" existiert, wählt das Gerät stattdessen deren Adresse!

- `LB0`...`LBF` für eine der 16 Loopback-Adressen oder deren Name

  Das Gerät verwendet Loopback-Adressen auch auf maskiert arbeitenden Gegenstellen stets **unmaskiert**!

- Beliebige IPv4-Adresse

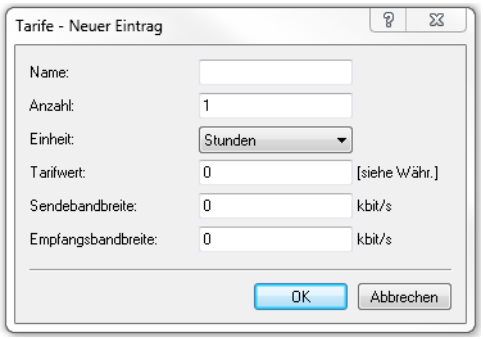
- **Accounting-Informationen im Flash-ROM ablegen**: Aktivieren oder deaktivieren Sie, ob Ihr Gerät die Abrechnungsinformationen in regelmäßigen Abständen im internen Flash-ROM speichert. Dies geschieht standardmäßig stündlich, Sie können das betreffende Intervall aber über das Setup-Menü verändern. Aktivieren Sie diese Option, um bei einem Stromausfall den Komplettverlust von Accounting-Informationen zu vermeiden.

  Beachten Sie, dass ein häufiges Beschreiben dieses Speichers die Lebendauer Ihres Gerätes reduziert!

- **Login-Seite**: Wählen Sie aus der Liste, welche Anmeldemaske die Portalseite für Ihre PMS-Schnittstelle anzeigt. Mögliche Werte sind:
  - `kostenlos`: Wählen Sie diese Einstellung, wenn Sie Ihren Hotelgästen einen kostenlosen Internetzugang anbieten. Ihre Hotelgäste werden auf der Portalseite dennoch dazu aufgefordert, sich mit ihrem Benutzernamen, ihrer Zimmernummer und ggf. einer weiteren Kennung am Hotspot zu authentisieren, um eine Internetnutzung durch Unbefugte zu erschweren.
  - `kostenpflichtig`: Wählen Sie diese Einstellung, wenn Sie Ihren Hotelgästen einen kostenpflichtig Internetzugang anbieten. Ihre Hotelgäste werden auf der Portalseite dazu aufgefordert, sich mit ihrem Benutzernamen, ihrer Zimmernummer und ggf. einer weiteren Kennung am Hotspot zu authentisieren und einen Tarif auszuwählen.

- **Mehrfachanmeldung zulassen**: Aktivieren oder deaktivieren Sie, ob Sie einem Hotelgast erlauben, mehrere WLAN-Geräte mit den selben Zugangsdaten am Hotspot anzumelden.

- **Zusätzliche Anmeldung über Tickets anbieten**: Aktivieren oder deaktivieren Sie, ob Sie zusätzlich zur Anmeldung über die Kombination Benutzername/Zimmernummer auch die Anmeldung über Voucher erlauben.
- **Nutzungsbedingungen müssen akzeptiert werden**: Aktivieren Sie diese Checkbox, um Hotelgäste die Nutzungsbedingungen zur Verwendung Ihres Hotspots bestätigen zu lassen.
- **Tarife**: Sofern Sie einen kostenpflichtigen Internetzugang anbieten, verwalten Sie über diese Tabelle die Tarife für das Accounting.



  - **Name**: Legen Sie hier einen aussagekräftigen Tarifnamen fest.
  - **Anzahl**: Geben Sie hier die Höhe des Zeitkontingents ein, z. B. `1`. In Kombination mit der Einheit entspricht dies im oben gezeigten Screenshot z. B. 1 Stunde.
  - **Einheit**: Wählen Sie aus der Liste eine Einheit für das Zeitkontingent aus. Mögliche Werte sind: `Minuten`, `Stunden`, `Tage`
  - **Tarifwert**: Geben Sie hier die Höhe des Betrags ein, mit dem Sie die Zeitkontingente vergelten. In Kombination mit der in den Anmelde-Einstellungen gewählten Währung entspricht dies z. B. 50 Cent.
  - **Sendebandbreite**: Definieren Sie hier die maximal zulässige Sendebandbreite für diesen Tarif.
  - **Empfangsbandbreite**: Definieren Sie hier die maximal zulässige Empfangsbandbreite für diesen Tarif.

  Eine temporäre Abmeldung vom Public Spot verschiebt nicht den Ablaufzeitpunkt eines eingekauften Zeitkontingents! Es nicht möglich, ein bereits gekauftes Zeitguthaben zu "pausieren", um es zu einem späteren Zeitpunkt erneut aufzunehmen. Die Herunterzählung der Zeit beginnt unabhängig vom Anmeldestatus ab Kauf des Kontingents.

- **Währung**: Sofern Sie einen kostenpflichtigen Internetzugang anbieten, wählen Sie hier die Währungseinheit aus, mit der Sie die angebotenen Zeitkontingente (einstellbar über die Tarif-Tabelle) abrechnen. Diese Einheit erscheint ebenfalls auf der Portalseite. Achten Sie darauf, dass sie mit der Währung des PMS-Servers übereinstimmt. Mögliche Werte sind:
  - `Cent`
  - `Penny`

Erweiterte Einstellungsmöglichkeiten

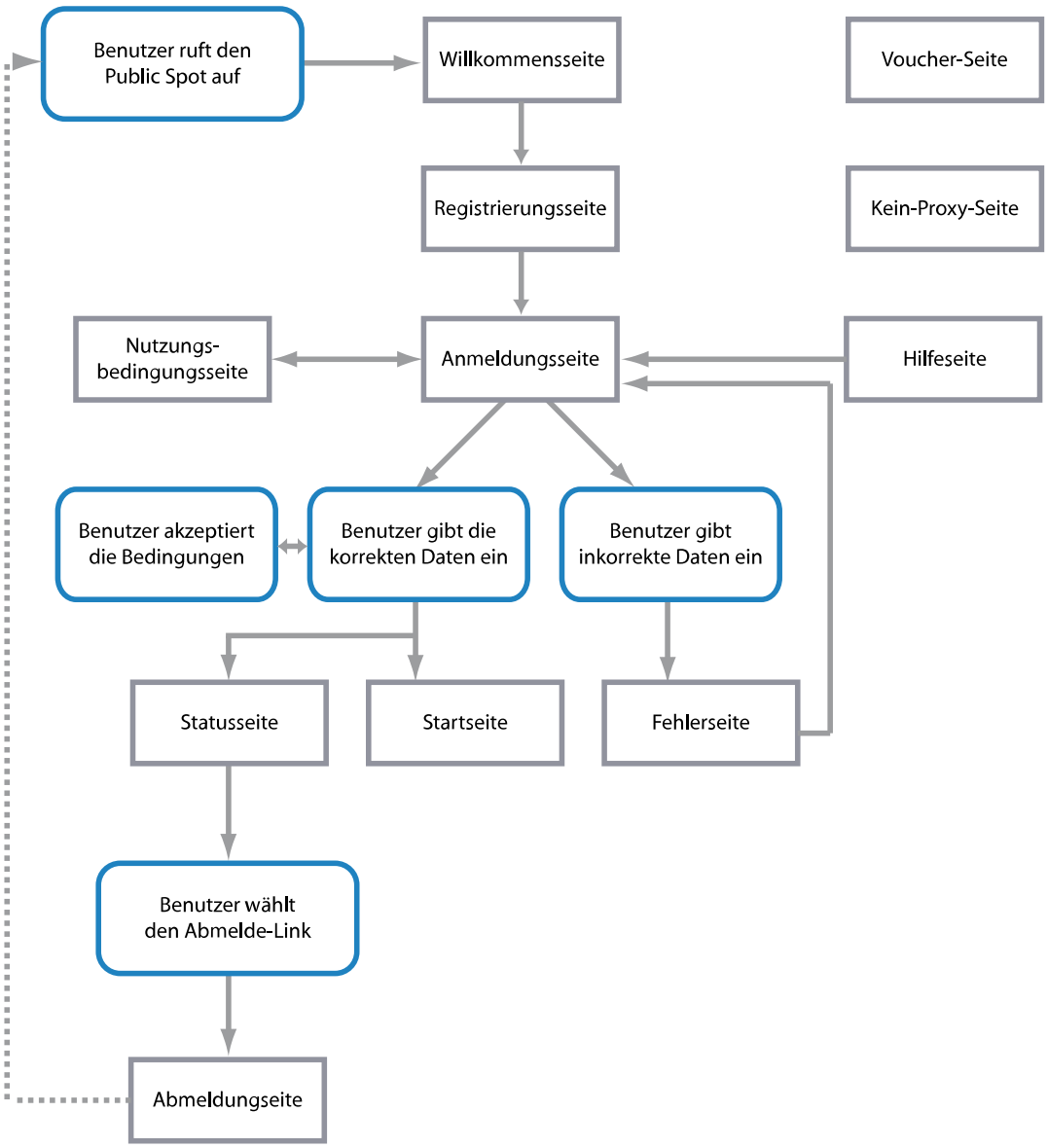
Erweiterte Einstellungen der PMS-Schnittstelle nehmen Sie auf der Konsole bzw. im Setup-Menü vor. Eine Übersicht aller zusätzlichen Parameter finden Sie im *Anhang*.

1.2.5 Geräteeigene und individuelle Voucher- und Authentifizierungsseiten (Templates)

Standardmäßig greift Ihr Gerät für die Anmeldeseite und alle übrigen Authentifizierungsseiten, die Ihre Benutzer vor, während und nach einer Public Spot-Sitzung angezeigt bekommen, auf geräteintern vorinstallierte Standardseiten (Templates) zurück. Sie haben jedoch auch die Möglichkeit, die einzelnen Webseiten Ihren Bedürfnissen entsprechend anzupassen und individuell zu gestalten. Sie benötigen dazu grundlegende HTML-Kenntnisse im Umgang mit DIV-Containern und Cascading Style Sheets (CSS), um die Struktur und das Layout der einzelnen Seiten gezielt zu verändern.

Mögliche Authentifizierungsseiten

Das nachfolgende Flussdiagramm zeigt Ihnen eine Übersicht und das Zusammenspiel aller vorhandenen Authentifizierungsseiten des Public Spot-Moduls. Die Abbildung orientiert sich dabei am Beispiel der Authentisierung mittels Zugangsdaten. Je nach Anmeldungsmodus und eventuell auftretender Fehler kann das Zusammenspiel von dem nachfolgend Gezeigten jedoch leicht abweichen:



Die Seiten **Willkommen** bzw. **Anmeldung** sind jene Seiten, die ein Benutzer angezeigt bekommt, wenn er erstmalig auf das Internet bzw. den Public Spot zugreift.

› Die Seite **Willkommen** ist dabei der Anmeldungsseite vorangestellt und in fast allen Anmeldungsmodi optional: Sie können diese Seite z. B. dafür verwenden, um einen Benutzer zu begrüßen, auf Informationen zum lokalen Angebot zu verweisen oder ihm eine Kurzanleitung zur Verwendung des Public Spot bereitzustellen, bevor er auf die Startseite mit dem Anmeldeformular gelangt. Nur wenn Sie den "Login nach Einverständniserklärung" als Anmeldungsmodus gewählt haben, ist eine individuelle Willkommensseite – welche die Einverständniserklärung beinhaltet – Pflicht, da sie an die Stelle des Anmeldeformulars auf der Anmeldungsseite tritt.

Die Standardseiten, die in Ihrem Gerät vorinstalliert sind, umfassen keine Willkommensseite. Wenn Sie eine solche Seite einrichten, ohne zuvor eine entsprechende Vorlage ins Gerät oder auf einen externen Server zu

laden, gelangt der Benutzer entweder direkt auf die Anmeldungsseite oder erhält eine Fehlermeldung (je nach Anmeldungsmodus).

- Die **Anmeldung** beinhaltet das Anmeldeformular, sofern für die Anmeldung am Public Spot die Authentisierung mittels Zugangsdaten und ggf. Anforderung der selben erforderlich ist.
- Die Seite mit den **Nutzungsbedingungen** ist nur dann zugänglich, wenn Sie die Bestätigung Ihrer Nutzungsbedingungen für den ausgewählten Anmeldungsmodus erforderlich gemacht haben. In diesem Fall erscheint unterhalb des Anmeldeformulars eine Checkbox mit einem zusätzlichen Link, der die Nutzungsbedingungen in einem Pop-Up öffnet.

Die Standardseiten, die in Ihrem Gerät vorinstalliert sind, umfassen für die Nutzungsbedingungs-Seite lediglich einen Platzhalter und keine generischen Nutzungsbedingungen.

Nachdem sich der Benutzer mit seinen Zugangsdaten (sofern erforderlich) autorisiert hat, überprüft das Gerät die Korrektheit der Angaben und stellt daraufhin entweder eine **Fehler**-Seite, die den Benutzer wieder auf die Anmeldeseite zurückführt, oder die **Start**-Seite dar.

- Die **Fehler**-Seite wird dabei lediglich gegenüber unauthentifizierten Public Spot-Benutzern ausgegeben und ist damit mehr oder weniger direkt mit dem Anmeldevorgang verknüpft. Typische Situationen, in denen ein Benutzer die Fehlerseite erhält, sind z. B. der unauthorisierte Zugriff auf den Public Spot, ein erreichtes Benutzerlimit sowie die fehlgeschlagene Authentifizierung durch Eingabe falscher Zugangsdaten oder Fehler beim Authentifizierungsserver. Sofern Sie eine zu überwachende Gegenstelle eingerichtet haben, erscheint die Seite außerdem immer dann, wenn das Public Spot-Modul einen Wegfall der WAN-Verbindung registriert, um einen mögliche Benutzer über die fehlende Verfügbarkeit des Netzwerks vorab zu informieren (siehe *Fehlerseite bei Wegfall der WAN-Verbindung einrichten* auf Seite 61).

  Bereits authentifizierte Benutzer hingegen erhalten unabhängig von der Fehlerseite immer eine entsprechende Fehlermeldung von ihrem Browser.
- Sofern bei der Anmeldung keine Fehler auftraten, verifiziert die **Start**-Seite die erfolgreiche Anmeldung und leitet den Benutzer nach einigen Sekunden Wartezeit auf diejenige Internetseite weiter, die er ursprünglich erreichen wollte.

Zusätzlich öffnet sich nach einer erfolgreichen Anmeldung ein kleines Pop-Up, die **Status**-Seite:

- Die **Status**-Seite zeigt dem Benutzer aktuelle Informationen zu seiner Sitzung an (z. B. die bisherige Nutzungszeit, die gesendeten und empfangenen Datenmenge sowie Gültigkeitsdauer seines Kontos). Sie beinhaltet auch einen Link zum Schließen der aktuellen Sitzung und Beenden des Accountings. Klickt ein Benutzer auf diesen Link, gelangt er auf die Seite **Abmeldung**.
- Die Seite **Abmeldung** bestätigt einem Benutzer die erfolgreiche Abmeldung vom Public Spot.

Die verbleibenden Seiten **Rückfall-Fehler**, **Kein Proxy** und **Hilfe** sind isoliert und nicht unmittelbar mit dem Anmeldevorgang verknüpft.

- Die **Rückfall-Fehler**-Seite erscheint immer dann, wenn das Gerät eine benutzerdefinierte Template-Seite nicht ausliefern kann und der Rückfall auf die LCOS-interne Standardseite fehlt. Die Auslieferung scheitert z. B., wenn Sie innerhalb der Seiten-Tabelle einen falschen Datei-Pfad angegeben haben oder die Template-Seite noch nicht im Gerät vorhanden ist.
- Die **Kein-Proxy**-Seite erscheint immer dann, wenn ein Benutzer versucht, eine HTTP-Verbindung über den Port 8080 an Stelle des normalen HTTP-Ports 80 aufzubauen. Der Port 8080 wird in Intranets typischerweise für HTTP-Proxies verwendet. Da Proxies aber als statische IP-Adresse in den Browsereinstellungen hinterlegt werden, diese sich jedoch nicht über DHCP konfigurieren lassen, liesse sich der Proxy nicht erreichen. Die Seite hat daher nur den Zweck, dem Benutzer eine Anleitung zum Deaktivieren seiner Proxy-Einstellungen zu bieten, bevor er fortfahren kann.
- Die **Hilfe**-Seite ist lediglich ein Platzhalter, um bestimmte Informationen (z. B. Details zur Anmeldung oder Erhaltbarkeit von Vouchern) in die übrigen Authentifizierungsseiten (z. B. die Willkommensseite) einzubetten. Die vorinstallierten Seiten beinhalten keine Hilfe-Seite und auch keinen Link, der auf diese Seite verweist. Um die Hilfe-Seite zu nutzen, müssen Sie demnach eine individuelle Vorlagenseite einrichten.

Keine Authentifizierungsseite stellt die Seite **Voucher** dar: Hierbei handelt es sich um die grafische Vorlage für den Voucher-Druck. Indem Sie dafür eine eigene Vorlage hochladen, können Sie Tickets z. B. im Corporate Design Ihres Unternehmens ausgeben.

Vorinstallierte Standardseiten

Ihr Gerät enthält im Lieferzustand bereits einen Satz vorinstallierter Seiten, mit denen sich ein funktionsfähiger Public Spot-Betrieb bereitstellen lässt.

Die nachfolgende Tabelle gibt Ihnen eine schnellen Überblick über die im LCOS enthaltenen Standardseiten:

Tabelle 5: Übersicht aller vorinstallierten Standardseiten

Seitenbezeichnung	Vorinstalliert?
Willkommen…	nein
Anmeldung…	ja
Fehler…	ja
Start…	ja
Status…	ja
Abmeldung…	ja
Hilfe…	nein
Kein Proxy…	nein
Voucher…	ja
Nutzungsbedingungen…	nein
Rückfall-Fehler…	ja
Anmeldung(E-Mail)…	ja
Registrierung(E-Mail)…	ja
Anmeldung(E-Mail zu SMS)…	ja
Registrierung(E-Mail zu SMS)…	ja

Die Seiten wurden mit der Absicht entwickelt, so simpel wie möglich zu sein, und verwenden daher keine komplexen Techniken wie z. B. Java Skript oder dynamisches HTML. Durch die Verwendung von schlichtem XHTML und CSS für allein die notwendigen Elemente ist sichergestellt, dass sie auf einer Vielzahl von Browsern und Bildschirmgrößen korrekt angezeigt werden.

Als Betreiber eines Hotspots möchten Sie ggf. aber etwas anspruchsvollere Seiten darstellen oder eine möglichst neutrale Seite ohne Herstellerbezug anzeigen. Das Public Spot-Modul bietet Ihnen daher die Möglichkeit, einzelne Standardseiten wahlweise zu Personalisieren oder durch selbstgestaltete Seiten zu ersetzen. Letzteres erreichen Sie entweder mittels HTTP-Umleitungen oder Vorlagen, die Sie in das Gerät laden, und welche das Gerät dann wie ein intelligenter HTML-Preprozessor bearbeitet. Diese Seitenvorlagen lassen sich direkt in den Flash-Speicher laden, wodurch Sie auf einen externen HTTP-Server verzichten können.

Zusätzliche Sprachen für die Authentifizierungsseiten

LCOS 8.84 erweitert die vom Public Spot-Modul ausgegeben Authentifizierungsseiten (d. h. alle vorinstallierten Standardseiten bis auf die Voucher-Seite) um die Sprachunterstützung für Französisch, Spanisch, Italienisch und Niederländisch. Somit haben Sie die Möglichkeit, einem breiteteren internationalen Nutzerspektrum einen Public Spot-Zugang in der jeweiligen Landessprache anzubieten. Die Ausgabe der entsprechenden Sprache erfolgt wie bisher über die Spracheinstellungen des Webbrowsers, mit denen der Nutzer den Public Spot aufruft.

Die Mehrsprachigkeit bezieht sich ausschließlich auf die 8.84-internen Standardseiten. Mehrsprachige inidividuelle Vorlagenseiten lassen sich jedoch unter Zuhilfenahme eines externen Servers realisieren.

Personalisierung der Standardseiten

Als Alternative zu den benutzerdefinierten Seiten bietet Ihnen das Gerät die Möglichkeit, die vorinstallierten Standardseiten in begrenztem Umfang zu personalisieren. Hierzu gehören z. B. die Eingabe eines Login-Textes, welcher Ihren Benutzern innerhalb des Anmeldeformulars angezeigt wird, oder das Austauschen der Header-Grafik (dem sogenannten Kopfbild). Auf diese Weise können Sie schnell einen individuellen Public Spot-Betrieb bereitstellen, ohne sich eingehend mit dem Thema der Webseitenerstellung zu beschäftigen.

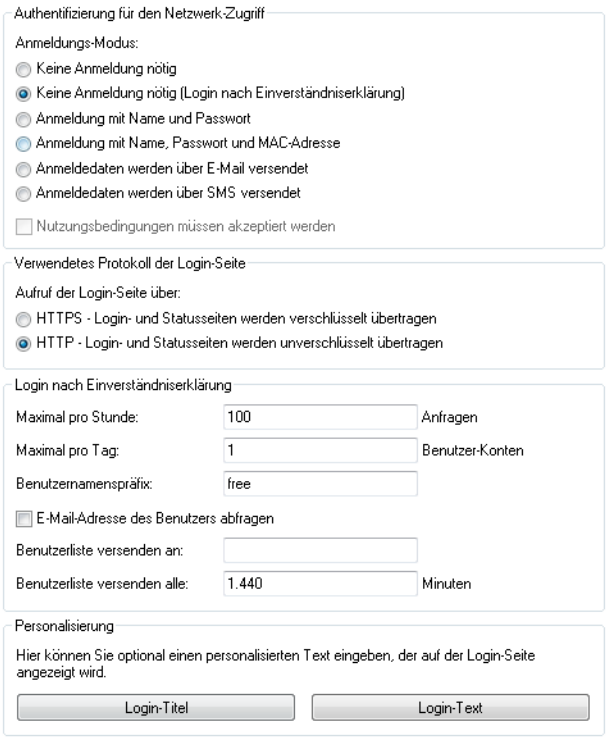
Individueller Text oder Login-Titel auf der Anmeldeseite

Sie haben innerhalb des Public Spot-Moduls die Möglichkeit, einen individuellen **Login-Text** und einen **Login-Titel** anzugeben, welche auf der Anmeldeseite innerhalb der Box des Anmeldeformulars eingeblendet wird. Sowohl Text als auch Titel sind in mehreren Sprachen definierbar (Deutsch, Englisch, Französisch, Italienisch, Spanisch und Niederländisch). Welche Sprache das Gerät letztlich ausgibt, hängt von den Spracheinstellungen des vom Benutzer verwendeten Webbrowsers ab. Wenn Sie für eine Sprache keinen individuellen Login-Text oder Titel spezifizieren, greift das Gerät auf den englischen Login-Text zurück (sofern vorhanden).

Bitte beachten Sie, dass es sich bei Login-Text und Login-Titel um unterschiedliche Elemente handelt!

Um einen individuellen Text oder einen Login-Titel auf der Anmeldeseite einzurichten, führen Sie die nachfolgenden Schritte aus.

1. Öffnen Sie in LANconfig den Konfigurationsdialog für das betreffende Gerät.
2. Wechseln Sie in den Dialog **Public Spot** > **Anmeldung**, klicken Sie auf die Schaltfläche **Login-Text** (alternativ **Login-Titel)** und wählen Sie eine Sprache aus.



3. Tragen Sie in dem sich öffnenden Dialog den Text ein, den Sie Ihren Public Spot-Nutzern anzeigen möchten. Erlaubt ist ein HTML-String mit max. 254 Zeichen, bestehend aus:

```
[Leerzeichen][0-9][A-Z[a-z] @{|}~!$%&amp;'()+-,/:;&lt;=>?[\]^_.#*
```

LANconfig transformiert eingegebene Umlaute automatisch in ihre entsprechenden Umschreibungen (`ü` zu `ue`; `ß` zu `ss`; usw.). Um Umlaute einzugeben, müssen Sie deren HTML-Äquivalente verwenden (z. B. `&uuml;` für `ü`), da

der Text unmittelbar in die Webseite eingebunden wird. Über HTML-Tags haben Sie außerdem die Möglichkeit, den Text zusätzlich zu strukturieren und zu formatieren. Beispiel:

```
Herzlich Willkommen!<br/><i>Bitte f&uuml;llen Sie das Formular aus.</i>
```

4. Klicken Sie **OK**, um die Eingabe abzuschließen, und laden Sie die Konfiguration zurück in das Gerät.

Nach dem erfolgreichen Schreiben der Konfiguration erscheinen Login-Text und Login-Titel beim nächsten Aufruf der Public Spot-Seite.

Individuelle Kopfbilder für variable Bildschirmbreiten

Bestandteil der im Gerät vorinstallierten Seiten ist eine Header-Grafik (Kopfbild genannt), die Ihren Benutzern beim Aufruf des Public Spots oberhalb des Anmelde-Formulars anzeigt wird. Sie können dieses Kopfbild nach Belieben ändern, um z. B. eine dem Einsatzumfeld oder Ihrem Corporate Design angemessene Grafik einzubinden. Sie benötigen dafür keine externen Webserver, sondern können über das Dateimanagement in WEBconfig bzw. die Konfigurationsverwaltung in LANconfig die Grafik direkt ins Gerät laden.

Eine Besonderheit des Kopfbildes ist dabei, dass es im Gerät in zwei unterschiedlichen Varianten vorliegt: Einmal als Großbild für Bildschirme bzw. Browser-Fenster mit einer horizontalen Auflösung >800 px (normale Monitore, Laptops, Tablet-PCs usw.) und einmal als Kleinbild für Bildschirme mit einer geringeren horizontalen Auflösung (PDAs, Mobiltelefone

usw.). Auf diese Weise haben Sie die Möglichkeit, Kopfbilder für unterschiedliche Zielgruppen bereitzustellen und diesen stets ein für Ihr Gerät geeignetes Anmelde-Formular anzubieten.

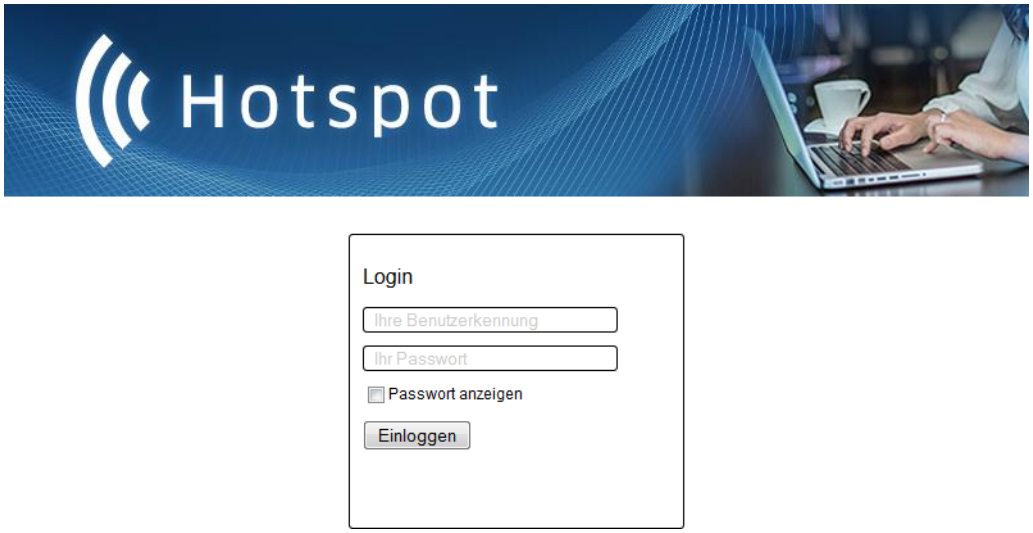


Abbildung 1: Anmeldeseite für breite Bildschirme

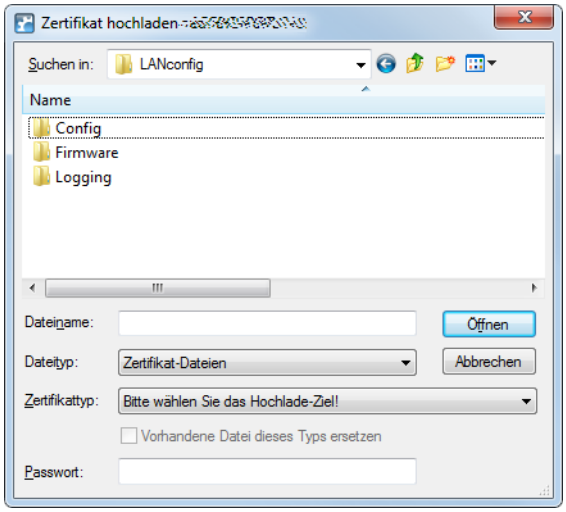
Abbildung 2: Anmeldeseite für schmale Bildschirme

Die möglichen Auflösungen werden durch die CSS-Datei des Gerätes vorgegeben. Für die vorinstallierten Standardgrafiken betragen sie 800x150 px für das Großbild und 258x52 px für das Kleinbild. Der Dateityp muss entweder JPG, GIF oder PNG sein.

Um ein neues Kopfbild als Groß- oder Kleinvariante ins Gerät zu laden, führen Sie die nachfolgenden Schritte aus.

1. Starten Sie LANconfig und markieren Sie das betreffende Gerät.

2. Klicken in der Menüleiste auf **Gerät** > **Konfigurations-Verwaltung** > **Zertifikat oder Datei hochladen**. Der Dialog **Zertifikat hochladen** öffnet sich.



3. Stellen Sie den **Dateityp** auf **Alle Dateien** und wählen Sie den **Zertifikattyp**, den Sie hochladen möchten.
   - **Public Spot – Kopfbild Seiten**: Zertifikattyp für das Großbild
   - **Public Spot – Kopfbild Box**: Zertifikattyp für das Kleinbild

4. Wählen Sie Ihr individuelles Kopfbild aus und klicken Sie auf **Öffnen**. LANconfig beginnt daraufhin mit dem Dateiupload.

Nach dem erfolgreichen Upload erscheint das neue Kopfbild beim nächsten Aufruf der Public Spot-Seite.

Sie können das Zusammenspiel von großem und kleinen Kopfbild überprüfen, indem Sie den Public Spot mit einem Browserfenster >800 px aufrufen und dann die Fensterbreite verkleinern. Durch die eingesetzten CSS-Techniken schaltet die Webseite automatisch zwischen Groß- und Kleinbild um.

Hersteller-Logo und -Kopfbild im Voucher ein-/ausblenden

Ein vom Gerät ausgegebener Voucher enthält standardmäßig das von der Public Spot-Startseite bekannte Kopfbild und Logo. Sie haben die Möglichkeit, die Einbindung dieser Grafiken über die Option **Public-Spot** > **Assistent** > **Kopfbild und Logo mitdrucken** direkt im Gerät zu deaktivieren, ohne dafür ein individuell angepasstes Vouchers-Template einzusetzen, welches diese Grafiken entfernt. In dem Fall gibt das Gerät lediglich einen textneutralen Voucher aus.

Konfiguration benutzerdefinierter Seiten

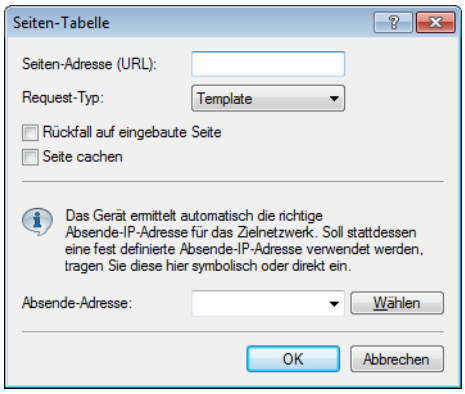
Sofern Sie die vorinstallierten Seiten durch selbstgestaltete Webseiten ersetzen möchten, können Sie diese entweder direkt im Gerät oder auf einem externen HTTP-Server ablegen. Anspruchsvollere HTML-Seiten benötigen ggf. mehr Speicherplatz, als im Gerät zur Verfügung steht. Darüber hinaus bietet Ihnen die Bereitstellung der Webseiten durch einen externen Server noch weitere Vorteile:

- Änderungen lassen sich zentral durchführen. Dadurch reduziert sich der Aufwand, die Anmeldeseiten bei Einsatz mehrerer Geräte in jedem Gerät ändern zu müssen.
- Der Server kann dynamische Seiten bereitstellen, deren Erscheinungsbild davon beeinflusst wird, welche Informationen ihm das Gerät liefert. Auf diese Informationen wird in den folgenden Kapiteln noch näher eingegangen.

Der Speicherort der Vorlagenseiten geben Sie im LANconfig unter **Public-Spot** > **Server** > **Seiten-Tabelle** > **<Name der Vorlagenseite>** > **Seiten-Adresse (URL)** ein. Es stehen Ihnen drei Protokolle für die URL zur Auswahl:

- `http://`...: Lädt die Seite über HTTP von einem externen Server herunter. Das Überschreiben des Standard-TCP-Ports sowie das Angeben von Benutzerdaten ist möglich
- `https://`...: Verhält sich genau wie HTTP, aber verwendet SSL um die Verbindung zu verschlüsseln.

› `file://...`: Verwendet eine Vorlage aus dem lokalen Speicher des Geräts.



Sie können beliebige Dateinamen verwenden. Sofern Sie sich für die Ablage der Templateseiten im lokalen Speicher des Geräts entscheiden, verwendeten Sie die speziell für den jeweiligen Zweck reservierten URLs. Durch Angabe der lokalen URL als **Seiten-Adresse (URL)** z. B. wird eine geräteeigene Standardseite durch eine ins Gerät geladene Seite ersetzt.

Tabelle 6: Übersicht der reservierten Dateinamen für Vorlagenseiten

Lokale URL im Gerät	Seitenbezeichnung
file://pbspot_template_welcome	Willkommen…
file://pbspot_template_login	Anmeldung…
file://pbspot_template_error	Fehler…
file://pbspot_template_start	Start…
file://pbspot_template_status	Status…
file://pbspot_template_logoff	Abmeldung…
file://pbspot_template_help	Hilfe…
file://pbspot_template_noproxy	Kein Proxy…
file://pbspot_template_voucher	Voucher…*
file://pbspot_template_agb	Nutzungsbedingungen…
file://pbspot_template_fallback	Rückfall-Fehler…
file://pbspot_template_reg_email	Registrierung(E-Mail)…
file://pbspot_template_login_email	Anmeldung(E-Mail)…
file://pbspot_template_reg_sms	Registrierung(E-Mail zu SMS)…
file://pbspot_template_login_sms	Anmeldung(E-Mail zu SMS)…

*) Vorlagenseite für den Voucher-Druck, keine Authentifizierungsseite

Durch das Hochladen benutzerdefinierter Webseiten werden die im Geräte vorinstallierten Webseiten nur ersetzt, nicht jedoch überschrieben. Sie können durch Löschen der lokalen URL jederzeit wieder zu den geräteeigenen Standardseiten zurückkehren.

Um eine Möglichst hohe Kompatibilität mit den verschienenen Anzeigegeräten und Web-Browsern zu erreichen, sollten Sie nach Möglichkeit auf den Einsatz von Frames verzichten. Auch spezielle Inhalte (JavaScript, Plug-In-Elemente) können zu einer fehlerhaften Anzeige führen.

Login-Seiten in Abhängigkeit vom Anmeldungsmodus

Die nachfolgende Tabelle liefert Ihnen darüber hinaus eine Übersicht, welche Login-Seite das Gerät in welchem Anmeldungsmodus ausgibt. Sofern für einen Anmeldungsmodus keine individuelle Seitenvorlage eingerichtet ist; verwendet das Public Spot-Modul dafür die 8.84-interne Standardseite:

Tabelle 7: Übersicht der Login-Seiten der einzelnen Anmeldungsmodi

Anmeldungsmodus	Seitenbezeichnung
Keine Anmeldung nötig	–
Keine Anmeldung nötig (Login nach Einverständniserklärung)	Willkommen…
Anmeldung mit Name und Passwort	Anmeldung…
Anmeldung mit Name, Passwort und MAC-Adresse	Anmeldung…
Anmeldedaten werden über E-Mail versendet	› Registrierung(E-Mail)… › Anmeldung(E-Mail)…
Anmeldedaten werden über SMS versendet	› Registrierung(E-Mail zu SMS)… › Anmeldung(E-Mail zu SMS)…

Besondere Template-Seiten für Smart Ticket

Während das Public Spot-Modul in LCOS-Versionen vor 8.84 noch eine zentrale Login-Seite für sämtliche Anmeldemodi verwendet, haben Sie ab LCOS 8.84 die Möglichkeit, für die Smart-Ticket-Funktion (die selbstständige Benutzeranmeldung via E-Mail/SMS) gesonderte Template-Seiten ins Gerät zu laden. Dazu konfigurieren Sie für die Anmeldung über E-Mail/SMS je zwei Seiten: **Registrierung(…)** und **Anmeldung(…)**.

- Auf der Registrierungsseite geben Benutzer zunächst ihre persönlichen Daten (E-Mail-Adresse oder Mobilfunknummer) ein, um sich beim Public Spot zu registrieren und dessen Zugangsdaten anzufordern.
- Auf der Anmeldungsseite geben Benutzer die ihnen zugesendeten Zugangsdaten ein, um sich schlussendlich am Public Spot zu authentisieren.

Die nachfolgende Tabelle liefert Ihnen eine Übersicht aller damit in Verbindung stehenden Abhängigkeiten, die Sie für das erstellen eigener Seitenvorlagen (Templates) benötigen:

Tabelle 8: Übersicht der Abhängigkeiten der SmartTicket-Anmeldeseiten

Anmeldungsmodus	Seitenbezeichnung	Lokale URL im Gerät	Seitenvorlagen-Bezeichner
Anmeldedaten werden über E-Mail versendet	Registrierung(E-Mail)…	file://pbspot_template_reg_email	<regemailform>
	Anmeldung(E-Mail)…	file://pbspot_template_login_email	<loginemailform>
Anmeldedaten werden über SMS versendet	Registrierung(E-Mail zu SMS)…	file://pbspot_template_reg_sms	<regsmsform>
	Anmeldung(E-Mail zu SMS)…	file://pbspot_template_login_sms	<loginsmsform>

Einrichten einer individuellen Vorlagenseite

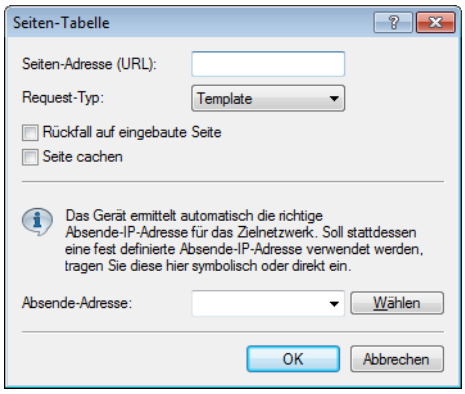
Über eine individuelle Vorlagenseite (auch Template-Seite genannt) haben Sie Möglichkeit, die LCOS-eigenen Vorlagenseiten durch eigene Webseiten zu ersetzen. Die LCOS-eigenen Vorlagenseiten werden dabei nicht überschrieben, sondern lediglich gegen Ihre eigene Seite ausgetauscht, sodass Sie bei Bedarf auf diese standardmäßig installierten Seiten zurückgreifen können.

Die nachfolgenden Schritte zeigen Ihnen am Beispiel einer **Login**-Seite, wie Sie mit Hilfe von LANconfig eine individuelle Vorlagenseite korrekt einrichten.

1. Laden Sie Ihre individuell erstellte Fehlerseite wahlweise auf einen externen HTTP(S)-Server oder als **Public Spot – Login-Seite (*.html, *.htm)** in den Speicher des Gerätes.

Weitere Informationen zum Hochladen eigener Templates sowie entsprechende Beispieldateien finden Sie im Internet in der *LANCOM Support Knowledgebase* unter *Implementierung eigener Webseiten für die LANCOM Public Spot Option*.

2. Öffnen Sie den Konfigurationsdialog des Gerätes in LANconfig, wechseln Sie in den Dialog **Public-Spot** > **Server** und wählen Sie **Seiten-Tabelle** > **Anmeldung**.



3. Tragen Sie unter **Seiten-Adresse (URL)** wahlweise die URL der Anmeldungsseite auf dem externen Server oder den gerätelokalen Dateiverweis ein (`file://pbspot_template_login`).

4. Nehmen Sie bei Bedarf weitere optionale Einstellungen vor.

   - **Request-Typ**: Sofern Sie einen externen Server einsetzen, haben Sie die Möglichkeit die Art des Seitenaufrufs verändern. Standardmäßig (in der Einstellung **Template)** lädt das Gerät eine extern gespeicherte HTM(L)-Seite von der angegebenen URL zur weiteren Verarbeitung durch den internen HTTP-Server. Wenn Sie die Einstellung zu **Redirect** ändern, lagert das Gerät die Seiten-Erzeugung an den externen Server aus (siehe auch *Benutzerdefinierte Seiten via HTTP Redirect* auf Seite 112).
   - **Rückfall auf eingebaute Seite**: Sofern Sie einen externen Server einsetzen und als Template-Typ **Request** gewählt haben, besteht die Möglichkeit, dass das Public Spot-Modul im Falle von HTTP(S)-Fehlern (z. B. Unerreichbarkeit des Servers) die LCOS-eigene Vorlagenseite benutzt, um ggf. einen Weiterbetrieb des Public Spots zu ermöglichen (siehe auch *Auto-Fallback* auf Seite 112. Wenn Sie diese Einstellung nicht aktivieren, zeigt der Public Spot stattdessen die Rückfall-Fehler-Seite an.
   - **Seite cachen**: Auf einigen Geräten haben Sie die Möglichkeit, lokale und externe Templates zu cachen. Mehr dazu erfahren Sie unter *Template Caching* auf Seite 111.
   - **Absende-Adresse**: Über diese Einstellung definieren Sie optional die Loopback-Adresse, die das Gerät benutzt, um sich mit dem externen HTTP(S)-Server zu verbinden. Standardmäßig schickt der Server seine Antworten zurück an die IP-Adresse Ihres Gerätes, ohne dass Sie diese hier angeben müssen. Durch Angabe einer optionalen Loopback-Adresse verändern Sie die Quelladresse bzw. Route, mit der das Gerät den Server anspricht. Dies kann z. B. dann sinnvoll sein, wenn der Server über verschiedene Wege erreichbar ist und dieser einen bestimmten Weg für seine Antwort-Nachrichten wählen soll.

5. Schließen Sie den Dialog sowie den allgemeinen Konfigurationsdialog mit jeweils einem Klick auf **OK**. LANconfig schreibt die getätigten Einstellungen daraufhin zurück in das Gerät.

Fertig!

Grafiken in benutzererstellte Vorlagenseiten einbinden

Für Ihre Seiten stehen Ihnen weitere fünf Bilder-Slots (Voucher-Bild 1 bis Voucher-Bild 5) zur Verfügung, mit denen Sie Bilder für Ihre Voucher ins Gerät laden können. Diese werden im Flash-Speicher abgelegt und verleiben im Gerät.

Übertragen Sie dazu die gewünschten Bilder in das Gerät wie im Abschnitt *Individuelle Kopfbilder für variable Bildschirmbreiten* beschrieben. Wählen Sie beim Upload als **Zertifikattyp** "Public Spot – Voucher-Bild 1" bis "Public Spot – Voucher-Bild 5".

Modifizieren Sie das jeweilige HTML-Template des betreffenden Vouchers (z. B. mit einem Texteditor wie Notepad++) und referenzieren Sie die hochgeladenen Bilder, indem Sie diese als `<img src="/images/voucherimg1">` bis `<img src="/images/voucherimg5">` in die Vorlage einbauen. Wie Sie eine individuelle Vorlagenseite einrichten, lesen Sie im Abschnitt *Einrichten einer individuellen Vorlagenseite*.

Template Caching

Bei der Konfiguration benutzerdefinierter Template-Seiten haben Sie auf Geräten mit hinreichend großem Arbeitsspeicher (z. B. Public Spot-Gateways) die Möglichkeit, Templates im Gerät zu cachen. Das Caching verbessert die Performance des Public Spot-Moduls insbesondere in größeren Szenarien, indem das Gerät einmal geladene Templates und daraus erzeugte HTML-Seiten intern zwischenspeichert.

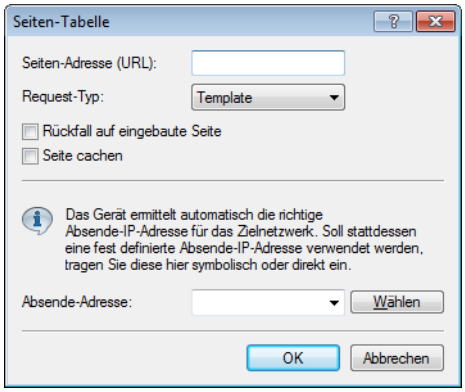
Das Caching ist möglich für:

- Templates abgelegt im lokalen Dateisystem
- Templates abgelegt auf externen HTTP(S)-Servern über statische URLs

Templates auf externen Servern, die mittels Template-Variablen referenziert werden, werden vom Gerät nicht gecached.

Template Caching aktivieren

Um das Caching für eine Seitenvorlage zu aktivieren, setzen Sie in LANconfig unter **Public-Spot** > **Server** > **Seiten-Tabelle** > **<Name der Vorlagenseite>** die Einstellung **Seite cachen**.



Im Setup-Menü finden Sie den dazugehörigen Paramter unter **Public-Spot-Modul** > **Seitentabelle** > **Template-Cache** .

Template Cache löschen

Das Gerät löscht bzw. aktualisiert im Cache gespeicherte Templates automatisch, sobald Sie eine neue Template-Datei in das Dateisystem Ihres Gerätes laden (bei lokaler Speicherung) bzw. die Cache-Zeit für ein HTTP(S)-Template abläuft (bei Speicherung auf externem einem Server). Hierzu wertet das Gerät den `Cache-Control`-Header eines HTTP(S)-Templates aus, um die maximale Cache-Zeit zu erfahren.

Sofern kein `Cache-Control`-Header gesetzt ist, wird die Webseite nicht gecached und direkt wieder verworfen. Achten Sie beim Einrichten eines individuellen Templates somit darauf, das entsprechende META-Tag in Verbindung mit einer sinnvollen Cache-Zeit (in Sekunden) zu setzen, z. B. `<meta http-equiv="cache-control" content="max-age=60">`. Die Dauer der Cache-Zeit ist dabei vom Szenario abhängig; es gibt keine konkreten Empfehlungen.

Sie haben aber auch die Möglichkeit, den Template Cache über eine Aktion manuell zu löschen. Starten Sie dazu im Status-Menü unter **Public-Spot** die Aktion **Flush-Template-Cache**.

Benutzerdefinierte Seiten via HTTP Redirect

Sofern Sie benutzerdefinierte Seiten als Umleitung realisieren (Request-Typ: Redirect), setzt Ihr Gerät diese wie folgt um: Immer, wenn Ihr Gerät eine betreffende Seite an einen Client liefern muss, erweitert es die URL gemäß der im vorangegangenen Kapitel vorgestellten Platzhalter und sendet eine HTTP-Antwort 307 (temporäre Umleitung) mit dieser URL an den Client.

Umleitungen sind besonders dann sinnvoll, wenn Sie eine Willkommensseite verwenden und alle Authentifizierungen auf einem externen Gateway erfolgen sollen. In diesem Fall können die Clients sofort zu diesem Gateway umgeleitet werden. Dieses Feature wird oft gemeinsam mit der externen Gerätekontroller verwendet.

Benutzerdefinierte Seiten über Seitenvorlagen

Alternativ kann das Gerät auch selbst als Client auftreten und die erweiterte URL verwenden um, um über eine HTTP-Verbindung die benutzerdefinierte Seite herunterzuladen. Der interne Preprozessor übernimmt die Bearbeitung der Seite und sendet das Ergebnis anschließend an den Public Spot-Nutzer. Diese Vorverarbeitung erlaubt es, Session-spezifische Daten zu verarbeiten, obwohl der Server eine statische Seite bereithält. Das Gerät verwendet Syntax-Befehle, wie sie bei Web-Browsern bekannt sind. Allerdings beherrscht es allerdings nur eine Teilmenge der möglichen Befehle:

- Die Benutzer-Authentifizierung erfolgt über die Form `user:password@host/...`
- Das Gerät kann nicht-fatale HTTP-Fehler, wie z. B. Redirects, nicht automatisch bereinigen. Stellen Sie also sicher, dass der Zugriff auf die Seite diese Seite auch direkt ausgibt.

Sie können symbolische Namen anstatt IP-Adressen für die Server-Hosts verwenden, solange der DNS korrekt konfiguriert ist. Dieser Mechanismus lässt sich daher in vielerlei Hinsicht als ein Proxy begreifen, der HTML-Seiten einholt und dann an die Clients weiterreicht. Der größte Unterschied ist dabei, dass die URL der Seiten im Gerät und nicht vom Client des Public Spot-Benutzers festgelegt werden.

Auto-Fallback

Für jeden Eintrag in der Seiten-Tabelle lässt sich individuell festlegen, ob eine Fallback-Funktion benutzt werden soll oder nicht. Diese Fallback-Funktion hat nur dann eine Bedeutung, wenn eine Seite als Vorlage (Request-Typ: Template) und nicht als Umleitung (Request-Typ: Redirect) definiert ist. Beim Herunterladen einer Seite über HTTP können eine Reihe von Fehlern auftreten:

- Das Nachschlagen eines Hosts beim DNS kann fehlschlagen.
- Die TCP/HTTP-Verbindung zum Server kann fehlschlagen.
- Der HTTP-Server kann eine Fehlermeldung ausgeben (wie z. B. 404, wenn eine ungültige URL angefragt wurde).

Standardmäßig gibt das Gerät solche Fehler an den Benutzer weiter, damit dieser eine erneute Anfrage starten oder den Betreiber des Public Spots davon in Kenntnis setzen kann. Alternativ kann das Konfigurieren einer Fallback-Funktion sicherstellen, dass der Hotspot weiter funktioniert, indem das Gerät stattdessen die standardmäßig installierten Seiten verwendet. Sie aktivieren die Fallback-Funktion im LANconfig über die Einstellung **Rückfall auf eingebaute Seite**.

Weitergegebene HTTP-Attribute

Wie bereits erwähnt kann das Gerät in einige Punkten als eine Art HTTP-Proxy gesehen werden, dass die Anmelde- und Status-Seite einholt. HTTP-Proxies sollten bestimmte Attribute intakt lassen, wenn Sie Anfragen des Clients weiterleiten:

- Das Gerät leitet Cookies zwischem dem Client und dem Server weiter. Cookie-Werte des Clients können also den Server transparent erreichen, und der Server kann Cookies auf dem Client setzen. Der Einsatz von Cookies ist notwendig, wenn die vom Server gesendeten Dateien aus ASP-Skripten stammen, da ASP die Session-ID in einem Cookie hinterlegt.
- Das Gerät wird den `User-Agent`-Wert des Clients unverändert weiterleiten. Dadurch kann der Server verschiedene Seiten je nach Browser und Betriebssystem ausgeben. PDAs und Mobiltelephone erwarten für kleine Bildschirme optimierte Seiten.
- Das Gerät wird eine `X-Forwarded-For`-Zeile in die HTTP-Anfrage anfügen um die IP-Adresse des Clients zu übermitteln..

› WEBconfig versucht die eigene Sprache anhand der durch `Accept-Languages` gelieferten Sprachpräferenz auszurichten und dann anhand der internen Datenbank auszugeben (momentan nur Englisch und Deutsch). Die gewählte Sprache wird dem Server durch ein weiteres `Accept-Languages`-Tag gemeldet, damit dieser eine Seite in der korrekten Sprache anbieten kann. Beim Übertragen der Seite prüft das Gerät, ob die Seite ein Language-Tag enthält. Wird es nicht gefunden, ersetzt das Gerät die Spracheinstellungen in der Vorlage mit der tatsächlich genutzten Sprache.

URL-Platzhalter (Template-Variablen)

Die URLs in der Seiten-Tabelle brauchen keine konstante Adresse darstellen. Sie haben die Möglichkeit, bestimmte Platzhalter – auch Template-Variablen genannt – in die Adresse zu integrieren, die dann mit den Parametern einer Public Spot-Sitzung gefüllt werden, wenn das Gerät die Seiten vom Server anfordert. Die Platzhalter haben dabei ein ähnliches Format wie in der Programmiersprache C; also ein Prozentzeichen, welchem unmittelbar ein einzelner, kleingeschriebener Buchstabe folgt. Folgende Platzhalter sind definiert:

%a

Fügt die IP-Adresse des Geräts ein. Dieser Platzhalter liefert nur dann einen Wert, wenn der **Request-Typ** in der **Seiten-Tabelle** auf `Template` gesetzt ist.

Bitte beachten Sie, dass dieser Platzhalter keine erreichbare Adresse erzeugt, wenn das Gerät sich hinter einem Router mit aktiviertem NAT befindet.

%c

Fügt die LAN-MAC-Adresse des Public Spot-Gerätes als 12-stelligen Hexadezimal-String ein. Die Ausgabe erfolgt im Format 'aa:bb:cc:dd:ee:ff'.

%d

Geben Sie den URL-Parameter "%d" als Circuit-ID an, z. B. `http://ipaddress/?circuit=%d&nas=%i`. Diese Variable ersetzt das Public Spot Modul mit der Circuit-ID, die im DHCP-Request des Clients erkannt wurde.

Dafür ist es erforderlich, dass auf dem AP "DHCP Snooping" so konfiguriert ist, dass der AP die Circuit-ID in der Public Spot-Stationstabelle des WLCs abfragen kann.

Somit ist es möglich, die Public Spot-Willkommensseite auf den angemeldeten Clients je nach Standort zu verändern.

%e

Fügt die Seriennummer des Geräts ein.

%i

Fügt die NAS-Port-Id ein. 'NAS' steht in diesem Zusammenhang für 'Network Access Server'. Diese Variable überträgt das Interface des Gerätes, über das sich ein Client anmeldet. Bei einem WLC oder Router ohne WLAN entspräche dies einer physischen Schnittstelle wie z. B. `LAN-1`, bei einem Standalone-Access-Point hingegen der SSID.

%l

Fügt den Hostnamen des Geräts ein.

%m

Fügt die MAC-Adresse des Clients als 12-stelligen Hexadezimal-String ein. Die individuellen Bytes werden durch zwei Doppelpunkte getrennt.

%n

Fügt den Namen des Geräts ein, wie er im Setup-Menü unter **Name** konfiguriert ist.

%o

Fügt die URL der Internetseite ein, die der Benutzer ursprünglich angefordert hat. Nach erfolgreicher Authentifizierung leitet das Gerät den Benutzer an diese URL weiter.

%p

Fügt die IP-Adresse des Public Spot-Gerätes in dem ARF-Kontext des jeweiligen Clients ein.

Sofern Ihr Gerät also in verschiedenen IP-Netzwerken aktiv ist, können Sie über diese Variable die IP-Adresse angeben, welche das Gerät in dem Netz benutzt, in dem auch der Client anzutreffen ist.

%r

Fügt die IP-Adresse des Clients ein (aus Sicht des Public Spot-Gerätes in dem jeweiligen ARF-Kontext).

%s

Fügt die WLAN SSID des Netzwerks ein, über das sich der Client verbunden hat. Diese Funktion ist besonders dann interessant, wenn sie MultiSSID verwenden, da der Server hierüber die Möglichkeit erhält, in Abhängigkeit von der SSID verschiedene Seiten auszugeben. Sollte der Client über einen anderen Access Point, welcher sich mit dem Gerät über ein Punkt-zu-Punkt-WLAN verbindet, verbunden sein, fügt dieser Platzhalter die SSID des ersten WLANs ein. Wenn der Client über Ethernet verbunden ist, produziert dieser Platzhalter einen leeren Wert.

%t

Fügt das Routing-Tag ein, mit dem die Datenpakete des Clients versehen werden.

%v

Sofern dem anfragenden Client eine individuelle VLAN-ID zugewiesen wurde, überträgt diese Variable die Quell-VLAN-ID.

%0-9

Fügt eine einzelne Zahl im Bereich von 0 bis 9 ein.

%%

Fügt ein einzelnes Prozentzeichen ein.

Um die Variablen für ein Template zu verwenden, ergänzen Sie in der Seiten-Tabelle die angegebene **Seiten-Adresse (URL)** um die betreffemden Parameter. In den nachfolgenden URLs würde `%i` gemäß dem o. g. Beispielwert durch `LAN-1` ersetzt werden:

Beispiel: `http://192.168.1.1/willkommen.php?nas=%i`

Beispiel: `http://192.168.1.1/%i_willkommen.html`

Seitenvorlagen-Tags und Syntax

Nachdem das Gerät die Seite vom Server empfangen hat, führt es einige Transformationen an den Seitenvorlagen durch, bevor es die Seite an den Client weitergibt. Diese Transformationen ersetzen die vordefinierten HTML-Tag-Platzhalter mit Daten der aktuellen Session (z. B. der aktuelle Ressourcenverbrauch in der Status-Seite). Eine vom Server bereitgestellte Seite sollte daher eher als eine Vorlage für eine HTML-Seite betrachtet werden. Die HTML-Syntax wurde deshalb für die Platzhalter gewählt, weil dadurch das Erstellen der Seiten mit Hilfe handelsüblicher HTML-Editoren möglich ist, ohne die Syntax zu verletzen.

Insgesamt sind drei Platzhalter-Tags definiert:

› `<pblink **identifier**>**text**</pblink>`

Markiert **text** als einen klickbaren Link zu **identifier**, typischerweise um eine andere Seite zu verknüpfen. Bitte beachten Sie, dass `</pblink>` nur ein Alias für `</a>` ist, da eine solch symetrische Definition zu weniger Probleme mit den gängigen HTML-Editoren führt. Das folgende Fragment definiert z. B. einen Link zur Hilfe-Seite:

```
Bitte klicken Sie <pblink helplink>hier</pblink> um weitere Hilfe aufzurufen.
```

› `<pbelem **identifier**>`

Fügt den unter **identifier** als Bezeichner angegebenen Wert an diesem Ort ein. Zum Beispiel fügt die folgende Zeile das Zeitguthaben des Benutzers ein:

```
Session wird in <pbelem sesstimeout> Sekunden beendet.
```

› `<pbcond **identifier(s)**>**code**</pbcond>`

Fügt nur dann **code** in die Seite ein, wenn alle Bezeichner TRUE sind, dass heisst numerische Werte sind nicht Null und Zeichenfolgen sind nicht leer. Bitte beachten Sie, dass sich diese Abhängigkeiten nicht ineinander verschachteln lassen. Vom vorherigen Beispiel ausgehend, zeigt die folgende Zeile nur dann an, wieviel Zeit einem Benutzer noch bleibt, wenn dieser ein Limit hat:

```
<pbcond sesstimeout>Session wird in <pbelem sesstimeout> Sekunden beendet.</pbcond>
```

Ein Satz von Beispiel-Seitenvorlagen ist bei LANCOM Systems verfügbar. Diese Beispiele sollen als reine Illustration und Anregung zum Erstellen eigener Seiten dienen.

Seitenvorlagen-Bezeichner

Für die Gestaltung benutzerdefinierter Template-Seiten stehen Ihnen die nachfolgenden Bezeichner zur Verfügung. Das Gerät unterscheidet dabei nicht zwischen Groß- und Kleinschreibung.

Bitte beachten Sie, dass nicht alle Bezeichner für alle Ausdrücke verfügbar sind. Nicht alle Bezeichner stehen auf allen Seiten zur Verfügung.

ACCOUNTEND

Gültig für: `<pbelem>`

Dieser Bezeichner fügt auf einem Voucher Informationen zur Gültigkeit des Vouchers ein, d. h. ab wann und bis wann der erstellte Zugang gültig ist.

APADDR

Gültig für: `<pbelem>`

Dieser Bezeichner beinhaltet die IP-Adresse des Public Spots aus Sicht des Clients. Kann für benutzerdefinierte Anmeldeseiten verwendet werden, wenn das `LOGINFORM`-Element nicht benutzt wird.

AUTOPRINT

Gültig für: `<pbelem>`

Dieser Bezeichner fügt ein Java-Skript in die Seite ein mit der Anweisung, den Druck-Dialog zu öffnen, um die angezeigte Seite auszudrucken. Beachten Sie, dass Sie den `pbelem`-Tag in diesem Fall mit einem separaten `script` abschließen **müssen**, also `<pbelem autoprint></script>`.

BANDWIDTHPROFNAME

Gültig für: `<pbelem>`

Dieser Bezeichner beinhaltet das Bandbreiten-Profil, mit dem der Benutzer verknüpft ist.

Dieser Bezeichner ist ab LCOS-Version 9.18 RU1 verfügbar. Templates mit diesem Bezeichner sind für LCOS-Versionen vor 9.18 RU1 nicht geeignet.

COMMENT

Gültig für: `<pbelem>`

Dieser Bezeichner beinhaltet auf einem Voucher den optionalen Kommentar, sofern Sie im Setup-Wizard dafür einen entsprechenden Text eingetragen haben.

HELPLINK

Gültig für: `<pblink>`

Dieser Bezeichner beinhaltet die URL der Hilfeseite.

LOGINEMAILFORM

Gültig für: `<pbelem>`

Dieser Bezeichner beinhaltet für die Anmeldung über Smart-Ticket das HTML-Formular zur Authentisierung am Public Spot mit den via E-Mail erhaltenenen Zugangsdaten.

LOGINERRORMSG

Gültig für: `<pbelem>`

Dieser Bezeichner liefert die Fehlermeldung des LCOS im Falle einer gescheiterten Anmeldung sowie bei Wegfall der WAN-Verbindung. Dieser Bezeichner steht nur auf der allgemeinen Fehlerseite und der Rückfall-Fehlerseite zur Verfügung.

Um die Fehlermeldung des RADIUS-Servers im Falle einer gescheiterten Anmeldung abzurufen, verwenden Sie den Bezeichner **SERVERMSG**.

LOGINFORM

Gültig für: `<pbelem>`

Dieser Bezeichner beinhaltet für die Anmeldung über Benutzername und Passwort (und ggf. MAC-Adresse) das HTML-Formular zur Authentisierung am Public Spot.

LOGINLINK

Gültig für: `<pblink>`

Dieser Bezeichner beinhaltet die URL der Anmeldungsseite.

LOGINSMSFORM

Gültig für: `<pbelem>`

Dieser Bezeichner beinhaltet für die Anmeldung über Smart-Ticket das HTML-Formular zur Authentisierung am Public Spot mit den via SMS erhaltenenen Zugangsdaten.

LOGOFFLINK

Gültig für: `<pblink>`

Dieser Bezeichner beinhaltet die URL der Abmeldungsseite.

ORIGLINK

Gültig für: `<pbelem>` `<pblink>` `<pbcond>`

Dieser Bezeichner beinhaltet die URL, die vom Benutzer angefordert wurde, bevor der Authentifizierungsprozess begonnen wurde. Ist diese Adresse nicht bekannt, ist der Bezeichner leer.

PASSWORD

Gültig für: `<pbelem>`

Dieser Bezeichner beinhaltet auf einem Voucher das Password für den Public Spot-Zugang.

REDIRURL

Gültig für: `<pbelem>` `<pblink>` `<pbcond>`

Dieser Bezeichner hält eine mögliche Umleitungs-URL aus der Authentifizierungsantwort des RADIUS-Servers bereit (sofern es diese gab). Lässt sich nur auf Fehler- und Startseite verwenden.

REGEMAILFORM

Gültig für: `<pbelem>`

Dieser Bezeichner beinhaltet für die Anmeldung über Smart-Ticket das HTML-Formular zum Anfordern der Zugangsdaten via E-Mail (Registrierung).

REGSMSFORM

Gültig für: `<pbelem>`

Dieser Bezeichner beinhaltet für die Anmeldung über Smart-Ticket das HTML-Formular zum Anfordern der Zugangsdaten via SMS (Registrierung).

RXBANDWIDTH

Gültig für: `<pbelem>`

Dieser Bezeichner beinhaltet die maximale Empfangsbandbreite des Bandbreitenprofils.

Dieser Bezeichner ist ab LCOS-Version 9.18 RU1 verfügbar. Templates mit diesem Bezeichner sind für LCOS-Versionen vor 9.18 RU1 nicht geeignet.

RXBYTES

Gültig für: `<pbelem>`

Dieser Bezeichner gibt an, wieviele Daten in Bytes das Gerät in dieser Session vom Client empfangen hat.

RXTXBYTES

Gültig für: `<pbelem>`

Dieser Bezeichner gibt an, wieviele Daten in Bytes das Gerät in dieser Session vom Client empfangen und wieviele Daten es an den Client gesendet hat. Er gibt somit die Summe aus TXBYTES und RXBYTES aus.

SERVERMSG

Gültig für: `<pbelem>` `<pbcond>`

Dieser Bezeichner hält die Authentifizierungsantwort des RADIUS-Servers bereit (sofern es diese gab). Lässt sich nur auf der Fehler- und der Startseite verwenden. Im Falle einer gescheiterten Anmeldung enthält dieser Bezeichner die Fehlermeldung des RADIUS-Servers.

Um die Fehlermeldung des LCOS-Servers im Falle einer gescheiterten Anmeldung abzurufen, verwenden Sie den Bezeichner **LOGINERRORMSG**.

SESSIONSTATUS

Gültig für: `<pbelem>`

Dieser Bezeicher gibt eine Text-Repräsentation über das aktuelle Verhältnis des Clients zum Gerät aus (ob authentifiziert oder nicht).

SESSIONTIME

Gültig für: `<pbelem>`

Dieser Bezeichner gibt die Zeit in Sekunden an, die seit der Anmeldung am Public Spot verstrichen ist.

SESSTIMEOUT

Gültig für: `<pbelem>` `<pbcond>`

Dieser Bezeichner gibt die noch verbleibende Zeit der aktuellen Sitzung an. Nach Ablauf dieser Zeit beendet das Gerät die aktuelle Sitzung automatisch. Für eine Sitzung ohne Zeitlimit ist dieser Bezeichner gleich Null.

SSID

Gültig für: `<pbelem>` `<pbcond>`

Dieser Bezeichner enthält auf einem Voucher die SSID, für die der Public Spot-Zugang erstellt wurde.

STATUSLINK

Gültig für: `<pbelem>` `<pblink>`

Dieser Bezeichner beinhaltet die URL der Abmeldeseite. Innerhalb des `<pblink>`-Elements wird automatisch eine Referenz generiert, die ein neues Browser-Fenster öffnet.

TXBANDWIDTH

Gültig für: `<pbelem>`

Dieser Bezeichner beinhaltet die maximale Sendebandbreite des Bandbreitenprofils.

Dieser Bezeichner ist ab LCOS-Version 9.18 RU1 verfügbar. Templates mit diesem Bezeichner sind für LCOS-Versionen vor 9.18 RU1 nicht geeignet.

TXBYTES

Gültig für: `<pbelem>`

Dieser Bezeichner gibt an, wieviele Daten in Bytes das Gerät während der aktuellen Sitzung zum Client gesendet hat.

USER NAME

Gültig für: `<pbcond>`

Über diesen Bezeichner haben Sie die Möglichkeit, auf der Voucher-Seite konditionalen HTML-Code einzufügen, den das Gerät nur bei bestimmten Benutzern bzw. Administratoren ausgibt. `USER` gilt dabei als Präfix und **muss** dem Benutzernamen (`NAME`) mit einem Leerzeichen vorangestellt werden. Um also bei Aufruf der Voucher-Seite eine HTML-Ausgabe speziell für den Benutzer 'root' zu erzeugen, verwenden Sie die folgende Syntax:

```
<pbcond USER root>Conditional HTML Code</pbcond>
```

In größeren Public Spot-Szenarien mit zentraler Verwaltung – z. B. auf einem WLAN-Controller – lässt sich diese Abhängigkeit auch zur Standortlokalisierung einsetzen: Dazu erstellen Sie für jeden der betreffenden Access Points einen eigenen Public Spot-Admin und spezifizieren für die einzelnen Administratoren einen konditionalen Voucher-Text.

USERID

Gültig für: `<pbelem>`

Dieser Bezeichner beinhaltet die User-ID (in Form des Benutzernamens), mit der die aktuelle Sitzung gestartet wurde. Der Bezeichner ist undefiniert, wenn der Client (noch) nicht eingeloggt ist.

VOLLIMIT

Gültig für: `<pbelem>` `<pbcond>`

Dieser Bezeichner gibt die verbleibende Datenmenge an, die dem Benutzer noch zur Verfügung steht, bevor das Gerät die aktuelle Sitzung automatisch beendet. Für eine Sitzung ohne Datenlimit ist dieser Bezeichner gleich Null.

VOUCHERIMG

Gültig für: `<pbelem>`

Dieser Bezeichner fügt das Seitenbanner Bild (in Groß) in die Seite ein.

Neue Platzhalter ab LCOS-Version 9.20:

Mit diesen Platzhaltern ist eine detailliertere Anpassung der Seitenvorlagen möglich. Im Unterschied zu den oben genannten Platzhaltern wird bei Nutzung dieser Platzhalter kein zusätzlicher beschreibender Text ausgegeben, sondern nur die reinen Werte.

${SSID}

Gibt den Netzwerknamen / die SSID aus.

${USERID}

Gibt den Benutzernamen aus.

${PASSWORD}

Gibt das Benutzerpasswort aus.

${COMMENT}

Gibt den Kommentar aus.

${BandwidthProfName}

Gibt den Namen des Bandbreitenprofils aus.

${TxBandwidth}

Gibt die vorgegebene Maximalbandbreite (Senderichtung) aus.

${RxBandwidth}

Gibt die vorgegebene Maximalbandbreite (Empfangsrichtung) aus.

${ACCOUNTEND}

Dieser Bezeichner gibt das Ticket-Ende (Datum und Uhrzeit) aus.

Zur Verwendung dieser Platzhalter ist es erforderlich, in der Vorlage die jquery-Bibliothek einzubinden. Dazu fügen Sie in der Vorlage folgendes ein:

```
<script src="/jquery/jquery.js" type="text/javascript"></script>

<script src="/jquery/jquery.tmpl.min.js" type="text/javascript"></script>
```

Verwenden Sie außerdem die neuen Platzhalter innerhalb eines <script>-Blocks:

```
<script id="voucherTemplate" type="text/x-jquery-tmpl">

[... Inhalt ...]

</script>
```

Grafiken in benutzererstellten Seiten

Beinahe alle Webseiten beinhalten Bilder, die vom Browser des Clients unabhängig von der eigentlichen HTML-Seite heruntergeladen werden. Bei den vorinstallierten Seiten sind auch die dazugehörigen Grafikdateien im Gerät gespeichert. Das Gerät passt dabei automatisch die notwendigen Rechte an, damit auch nicht-authentifizierte Clients problemlos auf die Bilder zugreifen können. Bei benutzerdefinierten Seiten wird jedoch jeder Zugriff auf die referenzierten (geräteexternen) Bilder wie ein normaler Internetzugriff behandelt, und würde Benutzer daher automatisch wieder auf die Willkommens- oder Startseite führen.

Um dieses Verhalten zu verhindern, sollten Sie darauf achten, dass die Server, die die Grafikdateien bereithalten, zu den **Freien Servern** gehören. Freie Server sind Adressen, deren Zugang nicht beschränkt ist; die also auch von nicht-authentifizierten Clients aufrufbar sind und die von der Accounting-Funktion nicht mit dem übrigen Datenverkehr verrechnet werden.

Das Kapitel *Anmeldungsfreie Netze* auf Seite 44 erhält weitere Informationen, wie Sie einen freien Server konfigurieren. Bitte beachten Sie, dass, wenn eine benutzererstellte Seite als eine Umleitung definiert ist, das Ziel dieser Umleitung ebenfalls zu den Freien Servern gehören sollte.

Template-Vorschau über WEBconfig

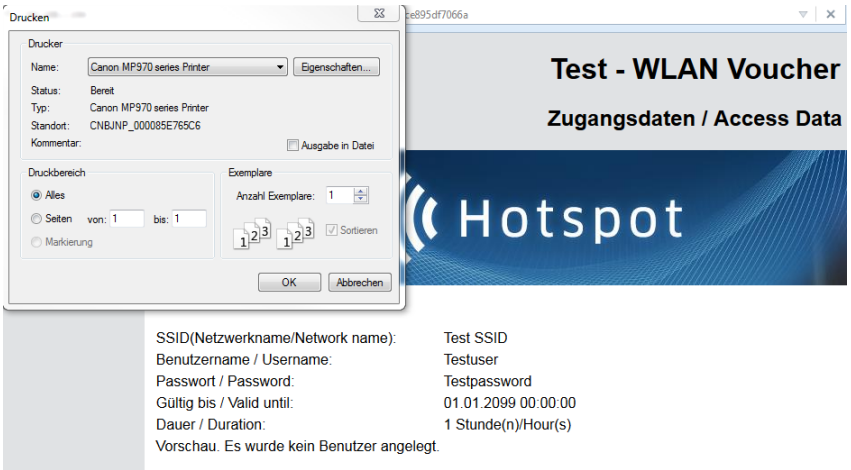
Um Änderungen an den Public Spot-Vorlagen verfolgen zu können, wechseln Sie in WEBconfig zur Ansicht **Extras** > **Public-Spot Template-Vorschau**.

Wählen Sie ein Template zum Anzeigen aus der Liste aus.

Das ausgewählte Template wird im gleichen Browserfenster angezeigt. Über die "Zurück"-Funktion Ihres Browsers gelangen Sie zum WEBconfig zurück.

Einige Templates beinhalten einen Javascript-Code. Dieser Code wird beim Aufrufen des jeweiligen Templates ausgeführt. So enthält das Template "Voucher-Seite" z. B. den Code zum Ausdrucken, sobald die Seite angezeigt wird.

Auf dieser Seite sind Testdaten hinterlegt. Es wird jedoch kein entsprechender Benutzer angelegt. Sie haben also die Möglichkeit, das Template zu testen und auszudrucken.



Sofern kein Template vorliegt oder gefunden werden kann, erscheint eine Fehlermeldung im WEBconfig.

Public Spot Captive Portal API

Der Public Spot unterstützt den neuen Standard der Captive Portal API nach *RFC 8908*. Der Standard erlaubt es WLAN-Clients in einem Hotspot ein Captive Portal bzw. eine Login-Seite automatisch zu finden.

Der Client erhält per DHCP die URL der Portal-Seite und kann dann per API-Anfrage an den Hotspot prüfen, ob ein Login erforderlich ist oder der Zugriff für den Client schon erlaubt ist. Das beschleunigt die Benutzererfahrung in einem Hotspot deutlich und stellt durch die Definition eines Standards nun eine bessere Herstellerinteroperabilität zwischen Hotspot und Clients her.

Folgende Schritt sind dazu erforderlich:

1. Die Verwendung von TLS-Zertifikaten im Public Spot ist zwingend erforderlich. Ohne HTTPS-Login stellt der Client an das Portal keine Anfrage.
2. Der DHCP-Server muss die Captive Portal DHCP-Option an den Client ausliefern.

Die Konfiguration finden sie in LANconfig unter **Public-Spot** > **Server** > **Captive Portal API (RFC 8908)**.

Captive Portal API aktiviert

Aktiviert bzw. deaktiviert die Funktion der Captive Portal API im Public Spot.

Benutzerportal-URL

(Optional) Die Captive Portal API unterstützt laut Standard nur die Betriebsart über TLS. Deshalb muss das Gerät über ein vertrauenswürdiges Zertifikat sowie einen DNS-Namen verfügen. Im Default kann der Parameter leer gelassen werden und wird automatisch vom System eingefügt. Dazu muss der Gerätename in den Public Spot Betriebseinstellungen konfiguriert werden und mit dem TLS-Zertifikat übereinstimmen. Wird ein externer Hotspot-Server verwendet, kann auch eine URL des externen Servers eingetragen werden. Als weitere Voraussetzung gilt, dass die Clients im Hotspot das Captive Portal per DHCP-Option finden müssen. Dazu muss die entsprechende DHCP-Option nach *RFC 8910* für das Hotspot-Netzwerk konfiguriert werden.

Venue-URL

(Optional) URL (TLS), über die der Betreiber dem Benutzer zusätzliche Informationen über die Lokation des Hotspots bereitstellen kann, z. B. die Webseite des Hotels des Hotspots.

DHCPv4-Option konfigurieren(laut RFC 8910)

Legen Sie in LANconfig einen neuen Tabelleneintrag unter **IPv4** > **DHCPv4** > **DHCP-Optionen** an.

Options-Nummer

Nummer der Option, die an die DHCP-Clients übermittelt werden soll. Hier 114.

Netzwerkname

Name des Public Spot-Netzwerks (siehe IPv4-Netzwerke)

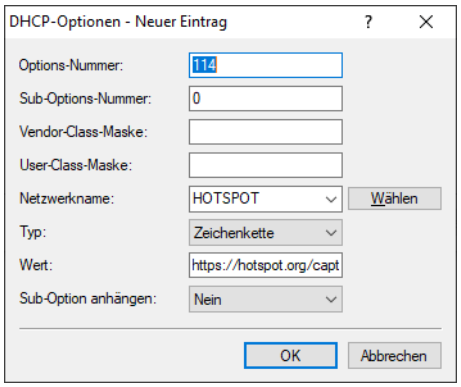
Typ

Typ des Eintrags. Hier Zeichenkette.

Wert

HTTPS-URL des LANCOM Routers im Hotspot, z. B. „https://hotspot.org/captive-portal-api“. Der DNS-Name, z. B. „hotspot.org“, ist der Gerätename des Routers im TLS-Zertifikat ergänzt um den internen Pfad der Public Spot Login-Seite „captive-portal-api“. Der DNS-Name muss durch den Hotspot-Clients auflösbar sein. Ebenso

muss der Gerätename in den Public Spot-Betriebseinstellungen konfiguriert werden und mit dem TLS-Zertifikat übereinstimmen.



DHCPv6-Option konfigurieren (laut RFC8910)

Legen Sie in LANconfig einen neuen Tabelleneintrag unter **IPv6** > **DHCPv6** > **DHCPv6-Server** > **Weitere Optionen** an.

Interface-Name / Relay-IP

Name des Public Spot Netzwerks (siehe IPv6-Netzwerke)

Optionscode

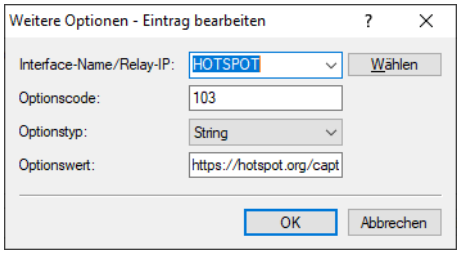
103

Optionstyp

String

Optionswert

HTTPS-URL des LANCOM Routers im Hotspot, z. B. „https://hotspot.org/captive-portal-api". Der DNS-Name, z. B. „hotspot.org", ist der Gerätename des Routers im TLS-Zertifikat ergänzt um den internen Pfad der Public Spot Login-Seite „captive-portal-api". Der DNS-Name muss durch den Hotspot-Clients auflösbar sein. Ebenso muss der Gerätename in den Public Spot-Betriebseinstellungen konfiguriert werden und mit dem TLS-Zertifikat übereinstimmen.

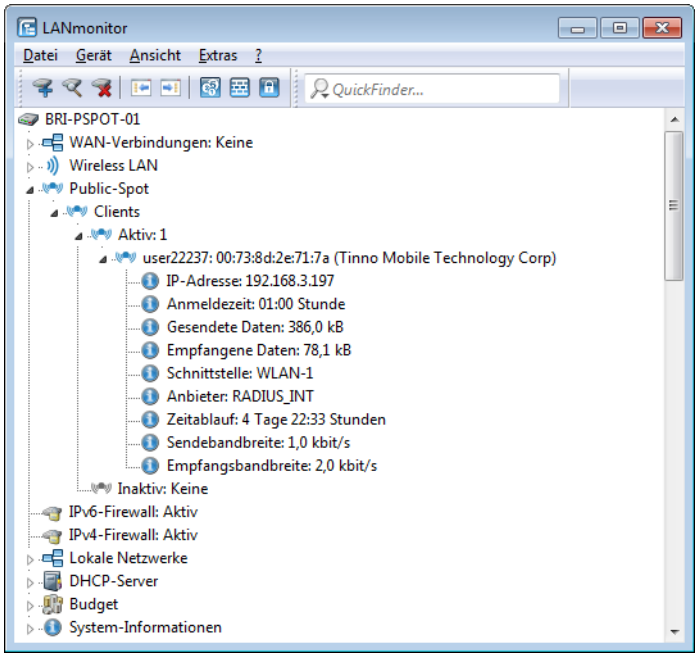


1.2.6 Public Spot-Clients anzeigen

Sie haben die Möglichkeit, sich im LANmonitor detaillierte Informationen zu Public Spot-Clients anzeigen zu lassen.

1. Öffnen Sie den Menüzweig **Public-Spot** > **Clients**.
2. Doppelklicken Sie auf **Aktiv**, um aktive Clients anzuzeigen, oder auf **Inaktiv**, um inaktive Clients anzuzeigen.

3. Doppelklicken Sie auf einen Client, um detaillierte Informationen zu diesem abzurufen.



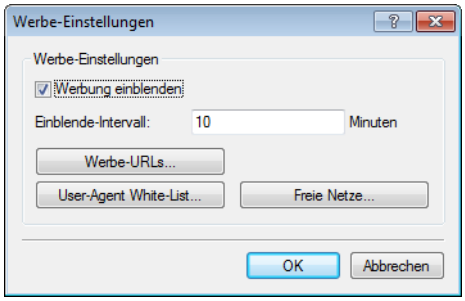
1.2.7 Public Spot-Benutzern Werbung einblenden

Sie haben die Möglichkeit, Public Spot-Benutzern in konfigurierbaren Zeitabständen Werbung einzublenden. Der Public Spot zeigt die Werbung im normalen Browser-Fenster des Benutzers an und nicht über Pop-ups, da alle modernen Browser Pop-ups in der Regel blocken. In der Public Spot-Stationstabelle gibt es somit drei Zustände für einen Client:

- Authentifiziert: Der Client ist angemeldet und darf surfen.
- Unauthentifiziert: Der Client ist nicht angemeldet und darf nicht surfen.
- Werbung: Der Client wird beim nächsten Aufruf einer URL auf eine Werbeseite umgeleitet.

Dabei haben Sie die Möglichkeit, über eine Whitelist bestimmte Netze und User-Agents von den Werbe-Einblendungen auszunehmen.

1. Wählen Sie in der Geräte-Konfiguration den Menüzweig **Public-Spot** > **Server** aus und klicken Sie dort auf **Werbe-Einstellungen**.
2. Aktivieren Sie das Kontrollkästchen **Werbung einblenden**.



Sie haben jetzt die Möglichkeit, den Einblende-Intervall zu verändern und weitere Einstellungen vorzunehmen.

3. Geben Sie unter **Einblende-Intervall** ein Intervall in Minuten, nach dem der Public Spot einen Benutzer auf eine Werbe-URL umleitet. Bei einem Intervall von 0 erfolgt die Umleitung direkt nach der Anmeldung.
4. Klicken Sie auf **Werbe-URLs**, um eine Werbe-URL hinzuzufügen. Wenn Sie mehrere Werbe-URLs hinzufügen, blendet der Public Spot diese im festgelegten Intervall nacheinander ein.

5. Optional: Klicken Sie auf **User-Agent White-List**, um User-Agents hinzuzufügen, die der Public Spot von Werbe-Einblendungen ausnimmt.
6. Optional: Klicken Sie auf **Freie Netze**, um Netze hinzuzufügen, die der Public Spot von Werbe-Einblendungen ausnimmt. Hier besteht beispielsweise die Möglichkeit, die automatischen Such-URLs der Browser eingeben, z. B. `*.google.com`. Normalerweise sendet ein Browser jede Tastatureingabe in der Adressleiste an eine Suchmaschine; durch das Setzen der Ausnahme reagiert die Werbeseite aber nicht auf diesen Zugriff.

   Anmeldungsfreie Netze sind generell werbefrei. Eine explizite Aufnahme derartiger Netze in die Whitelist ist somit nicht erforderlich.
7. Schließen Sie alle Dialoge durch einen Klick auf **OK**.

Public Spot-Benutzer werden nach Ablauf des Einblende-Intervalls auf eine Werbe-URL umgeleitet, sofern ihr User-Agent nicht auf der White-List steht oder sie sich innerhalb eines Freien Netzes bewegen.

Der Zeitpunkt der Werbe-Einblendungen bezieht sich auf die Session-Zeit eines aktiven Public Spot-Clients. Sendet ein Client eine bestimmte Zeit keine Daten, so verschiebt sich auch der Zeitpunkt, zu dem der Public Spot das nächste Mal Werbung einblendet.

1.3 Zugriff auf den Public Spot

1.3.1 Voraussetzungen für die Anmeldung

- Gerät mit Netzwerkadapter
- Betriebssystem mit TCP/IP-Protokoll (automatischer Bezug der IP-Adresse per DHCP ist eingeschaltet)
- Web-Browser (Unterstützung von JavaScript und Frames)
- Direkter Internetzugriff (Proxy-Verwendung ausgeschaltet)
- Notwendige Informationen zum Zugriff auf das WLAN (Netzwerkname, Verschlüsselungs-Informationen)
- Gültige Benutzerdaten (Kennung und Passwort)

Informationen für den WLAN-Zugang

Für den Zugang zum WLAN sind maximal zwei Angaben erforderlich:

- **Netzwerkname des WLAN (SSID)**

  Wenn die Basis-Stationen des Public-Spots für den Betrieb als Closed-Network konfiguriert sind, muss ein Benutzer den exakten Netzwerknamen des WLANs (die SSID) kennen.
- **WLAN-Verschlüsselung**

  Obwohl Gastzugänge auch mit aktivierter WLAN-Verschlüsselung wie z. B. WPA denkbar sind, werden Public-Spots in der Regel ohne WLAN-Verschlüsselung betrieben. Für den Zugriffsschutz sorgt dabei die Benutzeranmeldung mit Username und Passwort. Die Datensicherheit bei der Übertragung über den Public Spot muss vom Endanwender selbst bereitgestellt werden (z. B. über einen VPN-Client).

Informationen für den LAN-Zugang

Sofern Sie die IP-Adressen in Ihrem Netzwerk automatisch (z. B. via DHCP) vergeben, benötigen Benutzer lediglich:

- eine Anschlussdose, auf welcher der Public Spot aufgelegt ist.
- ein LAN-Kabel, um Ihren LAN-Adapter mit der Anschlussdose zu verbinden.

Informationen für die Authentifizierung

Folgende Daten müssen dem Benutzer für die Anmeldung vorliegen:

- Benutzerkennung
- Passwort
- MAC-Adresse

Wenn Sie an den Basis-Stationen des Public-Spots den Authentifizierungs-Modus "MAC+Benutzer+Passwort" gewählt haben, müssen Sie als Betreiber zusätzlich die MAC-Adressen der Endgeräte Ihrer Benutzer kennen. Ein Endgerät übermittelt seine eigene MAC-Adresse automatisch während der gesamten Kommunikation mit dem Public Spot. Der Benutzer muss sie daher nicht bei jeder Anmeldung manuell eingeben, sondern dem Betreiber nur einmal vor der Benutzung mitteilen.

1.3.2 Anmelden am Public Spot

1. Wählen Sie sich in das WLAN des Public-Spots ein (für WLAN-Verbindungen) oder verbinden Sie sich über das Ethernet-Kabel mit dem Netzwerk (für LAN-Verbindungen).
   Die notwendigen Einstellungen für diese Einwahl erfolgen je nach Mobilgerät bzw. WLAN-Adapter auf mehr oder weniger komfortable Art und Weise. Bei vielen Geräten wird der Netzwerkname (SSID) des gewünschten WLANs in einem Konfigurationsprogramm des WLAN-Adapters angegeben. Bei einigen Produkten ist auch die Ansicht aller Access Points in Funkreichweite möglich, aus denen Sie einfach die gewünschte auswählen können.

   Die notwendigen Einstellungen für die Verbindung über einen LAN-Adapter erhält ein Nutzer – je nach Konfiguration – automatisch durch das Netzwerk bzw. einen angeschlossenen DHCP-Server oder vom Netzwerk-Administrator.

2. Starten Sie Ihren Web-Browser.

   Sobald der Web-Browser auf eine beliebige Internet-Seite zugreift, schaltet sich automatisch der Public Spot dazwischen und präsentiert seine Anmeldeseite. Je nachdem, welche Firmware-Version Sie verwenden und welchen Anmeldemodus Sie gewählt haben, besitzt die Anmeldeseite bzw. das darin angezeigte Anmeldeformular ein unterschiedliches Erscheinungsbild. Im Nachfolgenden wird die Anmeldung über einen Vouchers (bzw. mittels Benutzername und Passwort) angenommen.

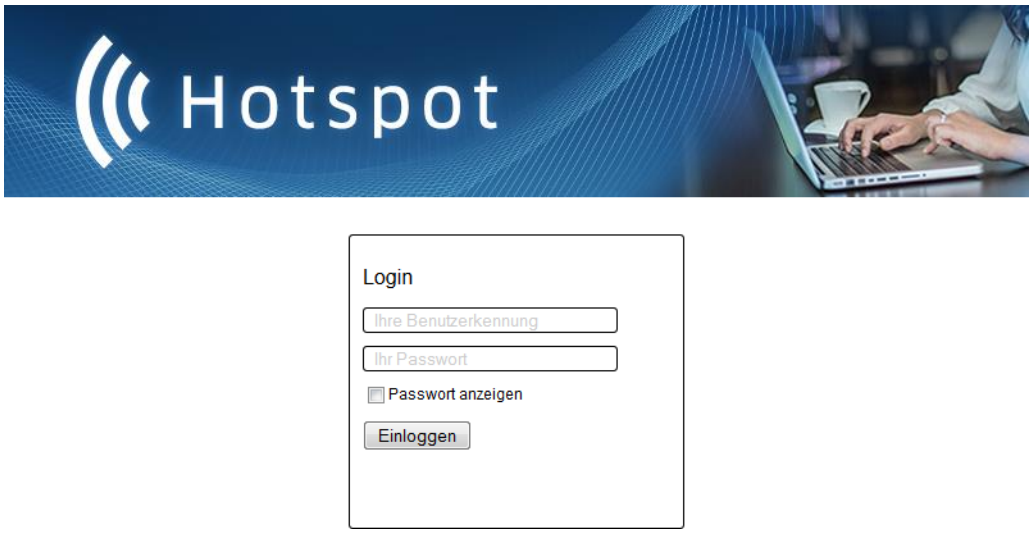


Abbildung 3: Anmeldeseite für breite Bildschirme

3. Geben Sie die vollständige **Benutzerkennung** und das **Passwort** in die entsprechenden Felder ein und bestätigen Sie Ihre Eingabe mit **Einloggen**.

   Für die Anmeldung sollten Sie einen Web-Browser mit aktivierter JavaScript-Unterstützung verwenden, damit das Popup-Fenster mit den Statusmeldungen über die Sitzung geöffnet werden kann.

   Bei erfolgreicher Anmeldung am Public Spot öffnet sich ein zusätzliches Fenster, das die wichtigsten Informationen der aktuellen Sitzung anzeigt. Auch die Abmeldung erfolgt über dieses Fenster. Daher sollte es während der gesamten Sitzung nach Möglichkeit geöffnet bleiben (z. B. in minimierter Darstellung).

Schlägt die Anmeldung fehl, öffnet sich eine Fehlerseite mit der Aufforderung, zur Anmeldeseite zurückzukehren und die Authentisierung zu wiederholen. Das Eingabeformular übernimmt dabei einen Teil der zuvor eingegebenen Daten, um dem Benutzer z. B. im Falle von Tippfehlern die Eingabe zu erleichtern.

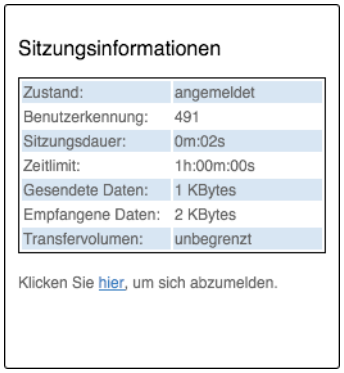
1.3.3 Informationen zur Sitzung

Das Fenster mit den Sitzungsinformationen aktualisiert sich automatisch regelmäßig. Neben Zustand und verwendeter Benutzerkennung sind vor allem die angebotenen Informationen über Verbindungszeit und übertragenes Datenvolumen von Interesse.

Falls das Sitzungsinformations-Fenster nicht geöffnet ist, können Sie es durch Eingabe folgender Adresszeile im Web-Browser öffnen:

```
http://<IP-Adresse des Public Spots>/authen/status
```

Alternativ können Sie auch über die Kurz-URL `http://logout` die Sitzungsseite öffnen.



1.3.4 Abmelden vom Public Spot

Im Sitzungsinformations-Fenster können Sie sich vom Public Spot abmelden. Klicken Sie dazu auf **hier** in der unteren Textzeile des Fensters.

Falls das Sitzungsinformations-Fenster nicht geöffnet ist, können Sie sich auch durch Eingabe folgender Adresszeile im Web-Browser abmelden:

```
http://<IP-Adresse des Public Spots>/authen/logout
```

Alternativ können Sie auch über die Kurz-URL `http://logout` die Sitzungsseite öffnen und sich darüber vom Public Spot abmelden.

Der Betreiber kann seinen Public Spot so einstellen, dass dieser einen Benutzer nach 60 Sekunden Unerreichbarkeit automatisch abmeldet. Fragen Sie im Zweifel beim Betreiber des Public-Spots nach, ob er die automatische Abmeldung (*Stationsüberwachung*) aktiviert hat.

1.3.5 Rat und Hilfe

Im folgenden Abschnitt finden Sie Lösungen für die häufigsten Probleme, die bei der Benutzung eines Public Spots auftreten können.

Die Anmeldeseite des Public Spots erscheint nicht

› Der Internet-Zugang muss so eingestellt sein, dass er direkt über den Netzwerkadapter und nicht über eine DFÜ-Einwahlverbindung erfolgt. Prüfen Sie daher die Verbindungseinstellungen in Ihrem Web-Browser. Wenn Sie den Microsoft Internet Explorer verwenden, so müssen unter **Extras** > **Internetoptionen** > **Verbindungen** die eingetragenen DFÜ-Konfigurationen deaktiviert sein.

- Der Internet-Zugang muss direkt erfolgen, also ohne Umweg über einen Proxy-Server. Beim Microsoft Internet Explorer schalten Sie dazu die Verwendung des Proxy-Servers im Menü **Extras** > **Internetoptionen** > **Verbindungen** > **LAN-Einstellungen…** aus.
- Sofern Sie die Verbindung über einen WLAN-Adapter herstellen: Prüfen Sie, ob Ihr Netzwerkadapter den Public Spot überhaupt finden kann. Für die Suche nach einem Access Point bietet Ihr WLAN-Adapter geeignete Hilfsmittel an.
- Sofern Sie die Verbindung über einen WLAN-Adapter herstellen: Prüfen Sie, ob Sie Ihren Netzwerkadapter ausreichend für den Zugang zum Public Spot-Netz konfiguriert haben.
  - Vermutlich müssen Sie den Netzwerknamen des WLAN angeben.
  - Bei Einsatz eines verschlüsselten Public Spots ist zusätzlich auch die Eingabe des passenden WPA- oder WEP-Schlüssels erforderlich.
- Prüfen Sie, ob Ihr Netzwerkadapter auf den automatischen Bezug einer IP-Adresse (DHCP) eingeschaltet ist. Ihm darf keine feste IP-Adresse zugewiesen sein.

Wenn Ihr Netzwerkadapter auf eine feste IP-Adresse konfiguriert ist, dann kann durch die Umstellung auf den automatischen Adressbezug per DHCP der Verlust wichtiger Konfigurationswerte ausgelöst werden. Notieren Sie sich vor der Umstellung alle Werte, die in den Netzwerkeinstellungen aufgeführt sind (IP-Adresse, Standard-Gateway, DNS-Server usw.).

Die Anmeldung funktioniert nicht

- Achten Sie auf die vollständige und richtige Eingabe der Benutzerdaten. Bei allen Eingaben ist auf korrekte Groß- und Kleinschreibung zu achten.
- Ist die Feststelltaste (CAPS-LOCK) an Ihrem Gerät aktiviert? Dadurch wird die Groß- und Kleinschreibung vertauscht. Deaktivieren Sie die Feststelltaste und wiederholen Sie die Eingabe Ihrer Anmeldedaten.
- Möglicherweise überprüft der Betreiber des Public Spots nicht nur Benutzername und Kennung, sondern auch die sogenannte MAC-Adresse (physikalische Adresse) Ihres Netzwerkadapters. Vergewissern Sie sich in diesem Fall beim Public Spot-Betreiber, dass er Ihre korrekte MAC-Adresse kennt.

Es sind keine weiteren Anmeldeversuche mehr möglich

Wenn der Public Spot nach einer Reihe von erfolglosen Anmeldeversuchen die Kommunikation mit Ihnen abbricht, so deaktivieren Sie für mindestens 60 Sekunden den WLAN-Adapter (oder Ihr komplettes Gerät) bzw. trennen den LAN-Adapter vom Netz, und versuchen Sie es danach erneut.

Das Sitzungsinformations-Fenster wird nicht angezeigt

Zur Anzeige des Sitzungsinformations-Fensters geben Sie in der Adresszeile Ihres Web-Browsers folgende Zeile ein:

```
http://<IP-Adresse des Public Spots>/authen/status
```

Der Public Spot-Betreiber gibt Ihnen die `<IP-Adresse des Public Spots>` auf Nachfrage an.

Der Public Spot fordert ohne Grund die Neuanmeldung (WLAN)

Beim Wechsel in den Funkbereich eines anderen Access Points (Roaming) wird die erneute Anmeldung erforderlich. Wenn Sie sich im Überschneidungsbereich zweier Access Points befinden, kann es sogar zu einem regelmäßigen Verbindungswechsel zwischen beiden Access Points kommen. Die Angabe des Roaming Secret ermöglicht die Übergabe einer Public Spot-Sitzung an anderen Access Point ohne Neuanmeldung.

- LANconfig: **Public-Spot** > **Benutzer** > **Roaming Secret**

1.4 Tutorials zur Einrichtung und Verwendung des Public Spots

Die folgenden Tutorials beschreiben beispielhaft, wie Sie das Public Spot-Modul sinnvoll einsetzen können.

1.4.1 Virtualisierung und Gastzugang über WLAN Controller mit VLAN

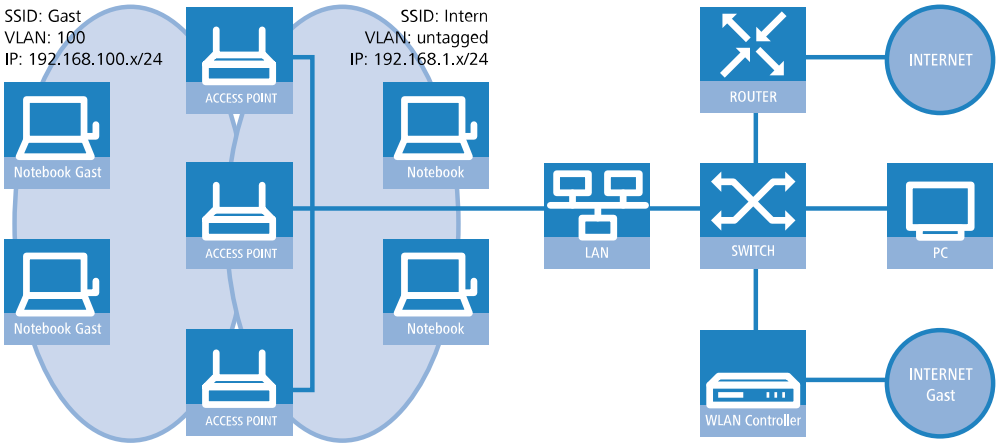
In vielen Unternehmen ist es erwünscht, den Besuchern für die mitgebrachten Notebooks o. ä. einen Internetzugang über WLAN anzubieten. In einem größeren Netzwerk mit mehreren Access Points kann die Konfiguration der nötigen Einstellungen zentral im WLAN Controller erfolgen.

Ziele

- Nutzung der WLAN-Infrastruktur für interne Mitarbeiter und Gäste
- Nutzung der gleichen physikalischen Komponenten (Kabel, Switche, Access Points)
- Trennung der Netzwerke über VLAN und ARF
- Auskopplung der Datenströme zu bestimmten Zielnetzwerken:
  - Gäste: nur Internet
  - Interne Mitarbeiter: Internet sowie alle lokalen Geräte und Dienste
- Gäste melden sich über ein Webformular am WLAN an.
- Interne Mitarbeiter nutzen die WLAN-Verschlüsselung zur Authentifizierung.

Aufbau

- Die Verwaltung der Access Points erfolgt zentral über den WLC.
- Der WLC dient als DHCP-Server für die WLAN-Clients des Gastnetzes.
- Für das Gastnetz wird der Internetzugang vom WLC (z. B. separater DSL Zugang oder Internetzugang über Firmen-DMZ) bereitgestellt.
- Die kabelgebundene Infrastruktur basiert auf gemanagten VLAN-fähigen Switches:
  - Das VLAN-Management der Access Points erfolgt über den WLC.
  - Das VLAN-Management der Switches erfolgt separat über die Switch-Konfiguration.
- Die Access Points werden innerhalb des internen VLANs betrieben.

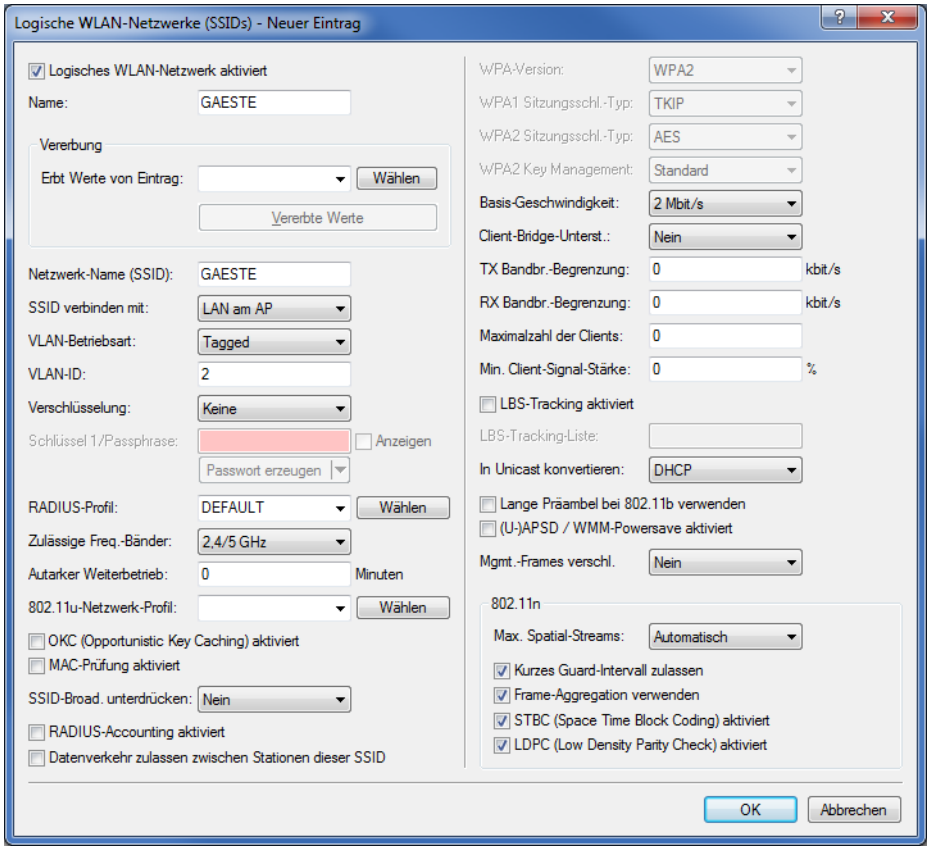


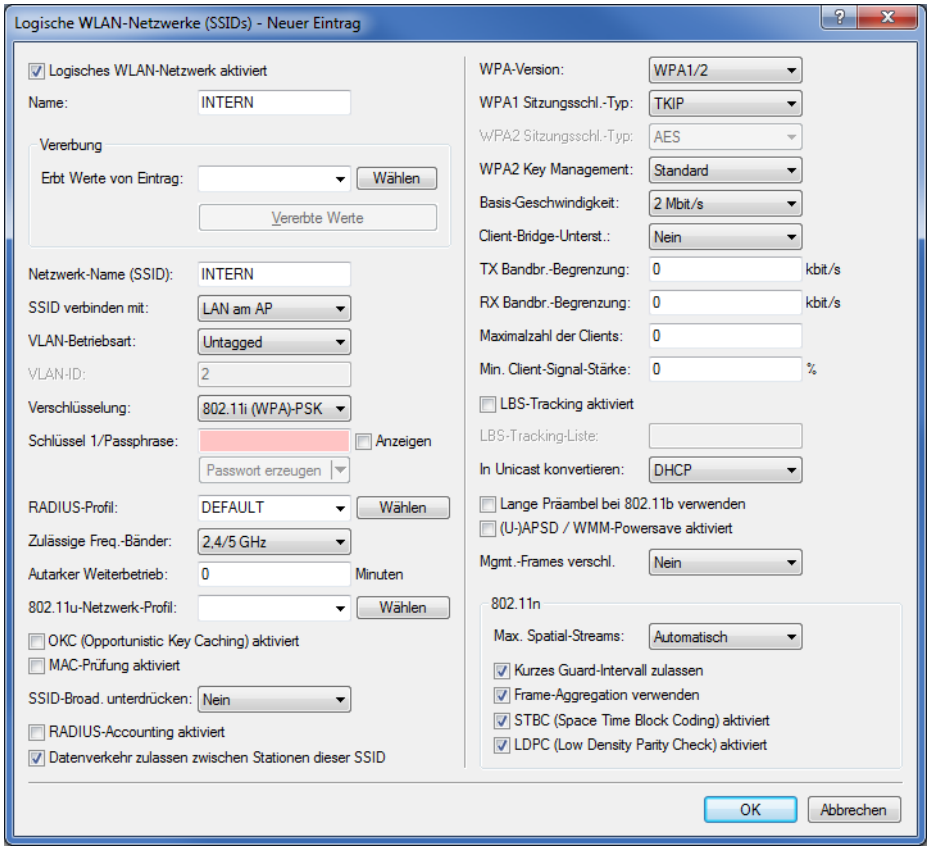
WLAN-Konfiguration des WLAN Controllers

Bei der WLAN-Konfiguration definieren Sie die benötigten WLAN-Netzwerke und weisen sie zusammen mit den physikalischen WLAN-Einstellungen den vom Controller verwalteten Access Points zu.

1. Erstellen Sie ein logisches WLAN für die Gäste und eines für die internen Mitarbeiter.
   - Das WLAN mit der SSID `GAESTE` erhält die VLAN-ID `100` (VLAN-Betriebsart **Tagged**) und verwendet **Keine** Verschlüsselung.
   - Das WLAN mit der SSID `INTERN` erhält keine VLAN-ID (VLAN-Betriebsart **Untagged**, d. h. Datenpakete werden ohne VLAN-Tag in das Ethernet übertragen) und verwendet eine Verschlüsselung nach WPA, z. B. **802.11i (WPA)-PSK**.

› LANconfig: **WLAN-Controller** > **Profile** > **Logische WLAN-Netzwerke (SSIDs)**

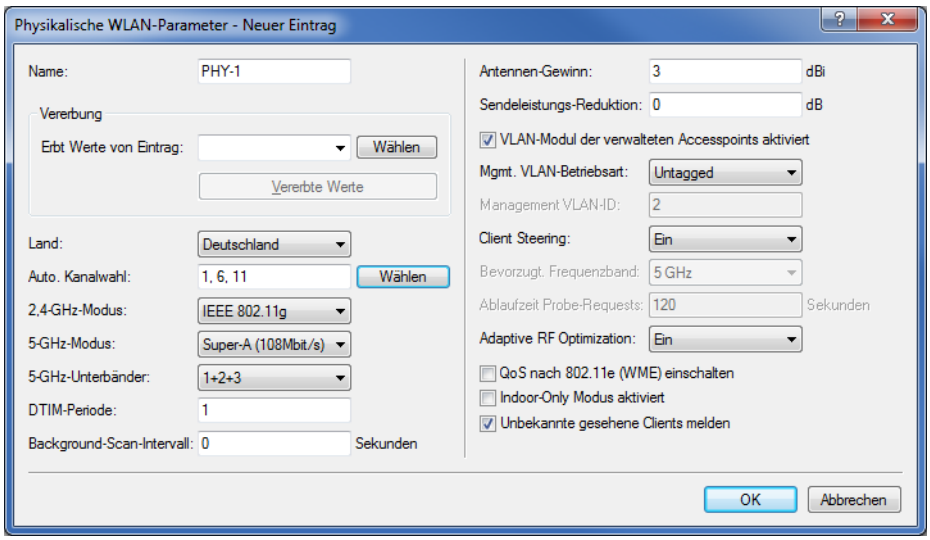




Wenn Sie die **VLAN-Betriebsart** auf **Untagged** stellen, graut LANconfig das Eingabefeld **VLAN-ID** im oben gezeigten Hinzufügen-/Bearbeiten-Dialog aus. Die dazugehörige Tabelle **Logische WLAN-Netzwerke (SSIDs)** zeigt als zugewiesene VLAN aber trotzdem den im ausgegrauten Feld ausgewiesenen Wert an. Dieser Eintrag ist lediglich programmintern, da der zulässige Wertebereich zwischen 2 und 4094 liegt. Letztlich entscheidend ist die VLAN-Betriebsart: Wenn diese auf **Untagged** steht, wird in keinem Fall eine VLAN-ID übertragen.

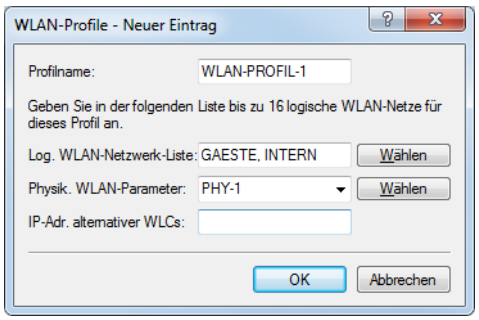
2. Erstellen Sie einen Satz von physikalischen Parametern für die verwendeten Access Points.
Dabei wird die Management-VLAN-ID auf `1` gesetzt, um die VLAN-Nutzung generell zu aktivieren (jedoch ohne separates Management-VLAN für das Gerät; der Management-Datenverkehr wird ungetagged übertragen).

   › LANconfig: **WLAN-Controller** > **Profile** > **Physikalische WLAN-Parameter**



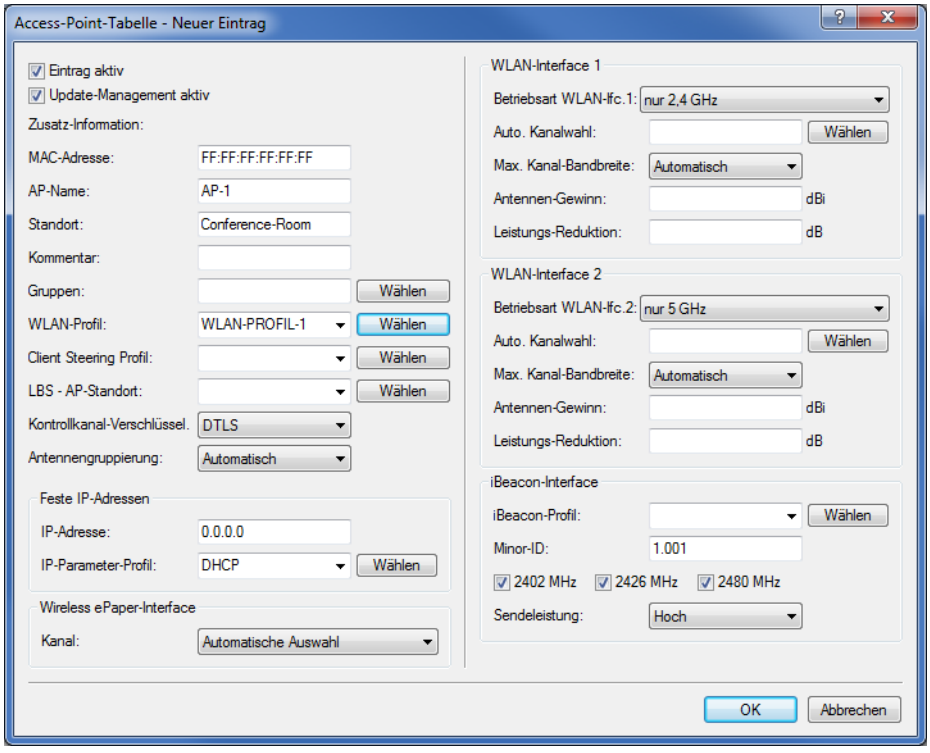
3. Erstellen Sie ein WLAN-Profil, welches Sie den Access Points zuweisen.
   Unter diesem WLAN-Profil vereinen Sie die beiden zuvor erstellten logischen WLAN-Netzwerke und den zuvor erstellten Satz von physikalischen Parametern.

   › LANconfig: **WLAN-Controller** > **Profile** > **WLAN-Profile**



4. Ordnen Sie das WLAN-Profil den vom Controller verwalteten Access Points zu.
   Tragen Sie dazu die einzelnen Access Points mit der MAC-Adresse in die Access-Point-Tabelle ein. Alternativ können Sie über die Schaltfläche **Default** auch ein Standardprofil anlegen, das für alle Access Points gilt.

   › LANconfig: **WLAN-Controller** > **AP-Konfig.** > **Access-Point-Tabelle**



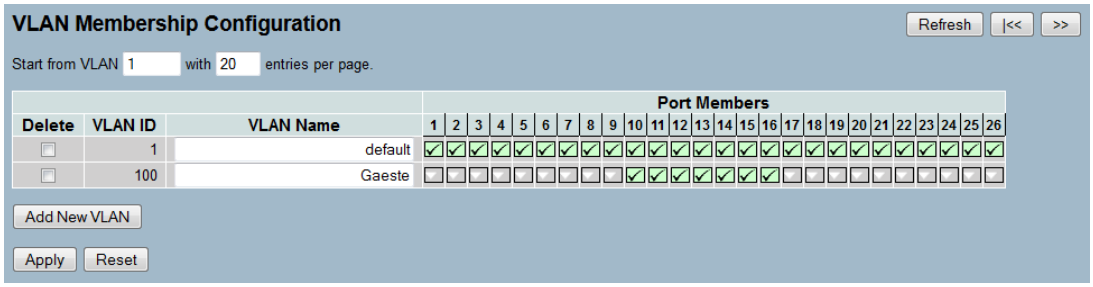
Konfiguration des Switches (LANCOM GS-2326P)

In diesem Kapitel beschreiben die Konfiguration des Switches am Beispiel eines LANCOM GS-2326P.

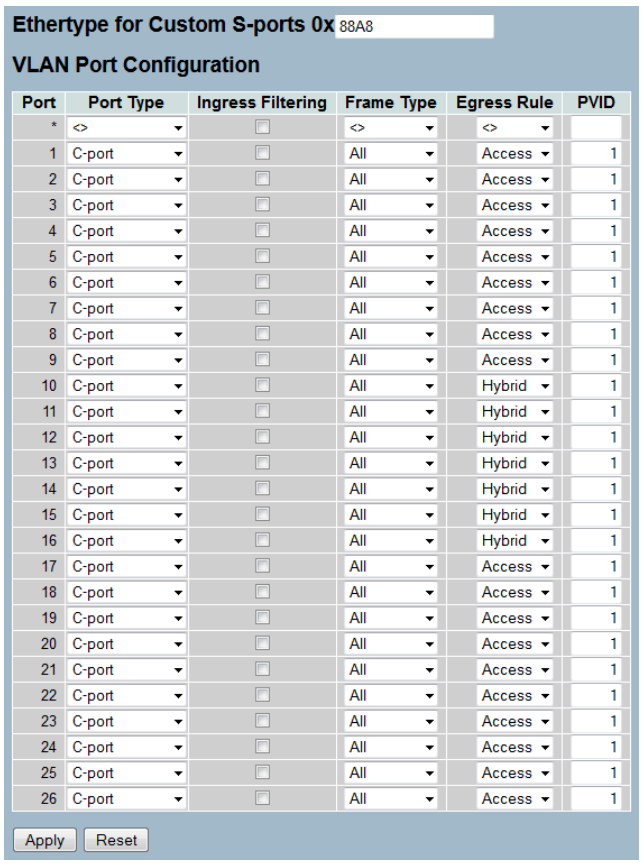
1. Legen Sie unter **Configuration** > **VLAN** > **VLAN-Membership** für das eingerichtete Gäste-Netz eine weitere VLAN-Gruppe an.

   Zur Unterscheidung der VLANs im Switch werden zwei Gruppen verwendet. Das interne Netz für die Mitarbeiter wird in der Gruppe `default` abgebildet, das der Gäste in der Gruppe `Gaeste`.

- Die VLAN-Gruppe für die internen Mitarbeiter verwendet die Default-VLAN-ID `1`. Diese zur internen Verwaltung eingesetzte VLAN-ID gilt auf allen Ports und wird ungetagged betrieben; d. h. alle ungetaggt eingehenden Datenpakete erhalten für das interne Routing die VLAN-ID 1, welche bei ausgehenden Datenpaketen wieder entfernt wird (siehe auch "PVID" im nächsten Schritt).
- Die VLAN-Gruppe für die Gäste verwendet die VLAN-ID `100`, die Sie bereits bei der Konfiguration der WLANs im Controller eingetragen haben. Sie gilt nur auf den Ports, an denen der WLAN-Controller und die Access Points angeschlossen sind (in diesem Beispiel: Port 10 bis 16, grüner Haken unter **Port Members**). Bei ausgehenden Datenpaketen entfernt der Switch die Tags nicht; d. h. alle getaggt eingehenden Datenpakete mit der VLAN-ID 100 behalten diesen Tag und werden nur an die Ports geroutet, die Mitglied der entsprechenden Gruppe sind.



2. Stellen Sie unter **Configuration** > **VLAN** > **Ports** den **Port Type** alle Ports auf **C-port**. Details zu dieser Einstellung finden Sie in der Switch-Dokumentation.
3. Konfigurieren Sie die **Egress Rule** für die einzelnen Ports.
   - Alle Ports außer Port 10 bis 16 erhalten die Regel **Access**. Dadurch leiten diese Ports nur ungetaggte Datenpakete weiter, alle anderen werden verworfen.
   - Die Ports 10 bis 16 erhalten die Regel **Hybrid**. Dadurch leiten diese Ports sowohl ungetaggte als auch getaggte Datenpakete weiter.



Achten Sie darauf, dass die **PVID** (Port-VLAN-ID) für jeden Port den Wert `1` besitzt. Die PVID ist die VLAN-ID, die ein Port eingehenden Datenpaketen ohne VLAN-Tag zuweist; daher entspricht die PVID der VLAN-ID der `default`-Gruppe.

4. OPTIONAL: Sofern Sie den Zugang zum Gäste-Netz auch über Ethernet erlauben möchten, stellen Sie unter **Configuration** > **VLAN** > **Ports** z. B. für die Ports 17 bis 20 die **PVID** auf `100`, und weisen unter **Configuration** > **VLAN** > **VLAN-Membership** diese Ports der Gruppe `Gaeste` zu. Dadurch erhalten alle über diese Ports ungetaggt eingehenden Datenpakete die VLAN-ID 100.

   Beachten Sie, dass die betreffenden Datenpakete den Switch dann lediglich über die Ports des Gäste-Netzes wieder verlassen können!

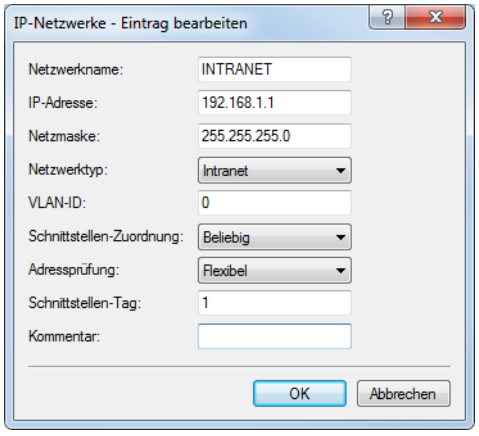
Konfiguration der IP-Netzwerke im WLAN Controller

Für die Trennung der Datenströme auf Layer 3 werden zwei verschiedene IP-Netzwerke verwendet (ARF – Advanced Routing and Forwarding).

1. Stellen Sie für das interne Netzwerk das **INTRANET** auf die Adresse `192.168.1.1` ein.

   Dieses IP-Netzwerk verwendet die **VLAN-ID** `0`. Damit werden alle ungetaggten Datenpakete diesem Netzwerk zugeordnet (das VLAN-Modul des Controllers selbst muss dazu deaktiviert sein). Das **Schnittstellen-Tag** `1` wird für die spätere Auskopplung der Daten im virtuellen Router verwendet.

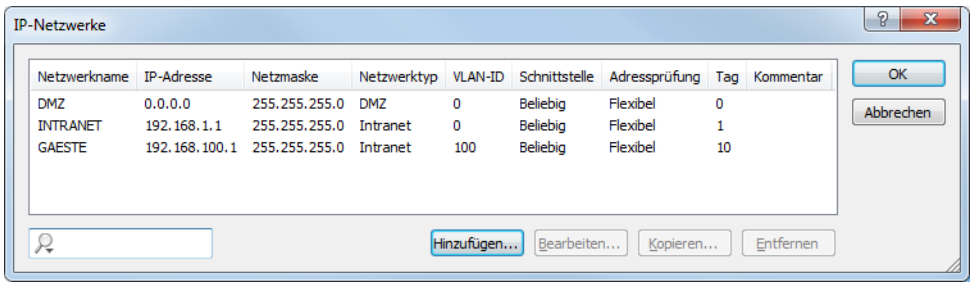
   › LANconfig: **TCP/IP** > **Allgemein** > **IP-Netzwerke**



2. Legen Sie für die Gäste ein neues IP-Netzwerk mit der Adresse `192.168.100.1` an.

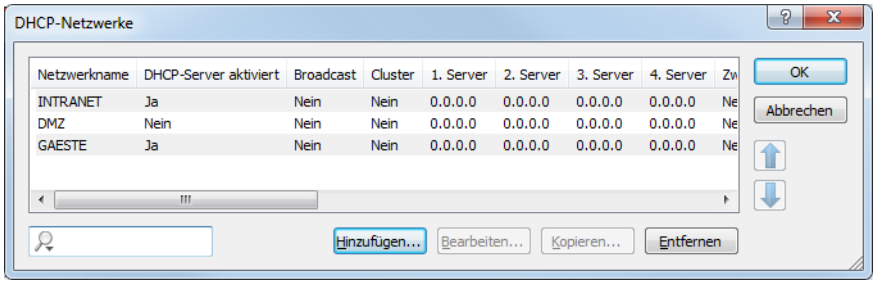
   Dieses Netzwerk verwendet die **VLAN-ID** `100`. Damit werden alle Datenpakete mit dieser ID dem Gäste-Netzwerk zugeordnet. Auch hier dient das **Schnittstellen-Tag** `10` der späteren Verwendung im virtuellen Router.

   › LANconfig: **TCP/IP** > **Allgemein** > **IP-Netzwerke**

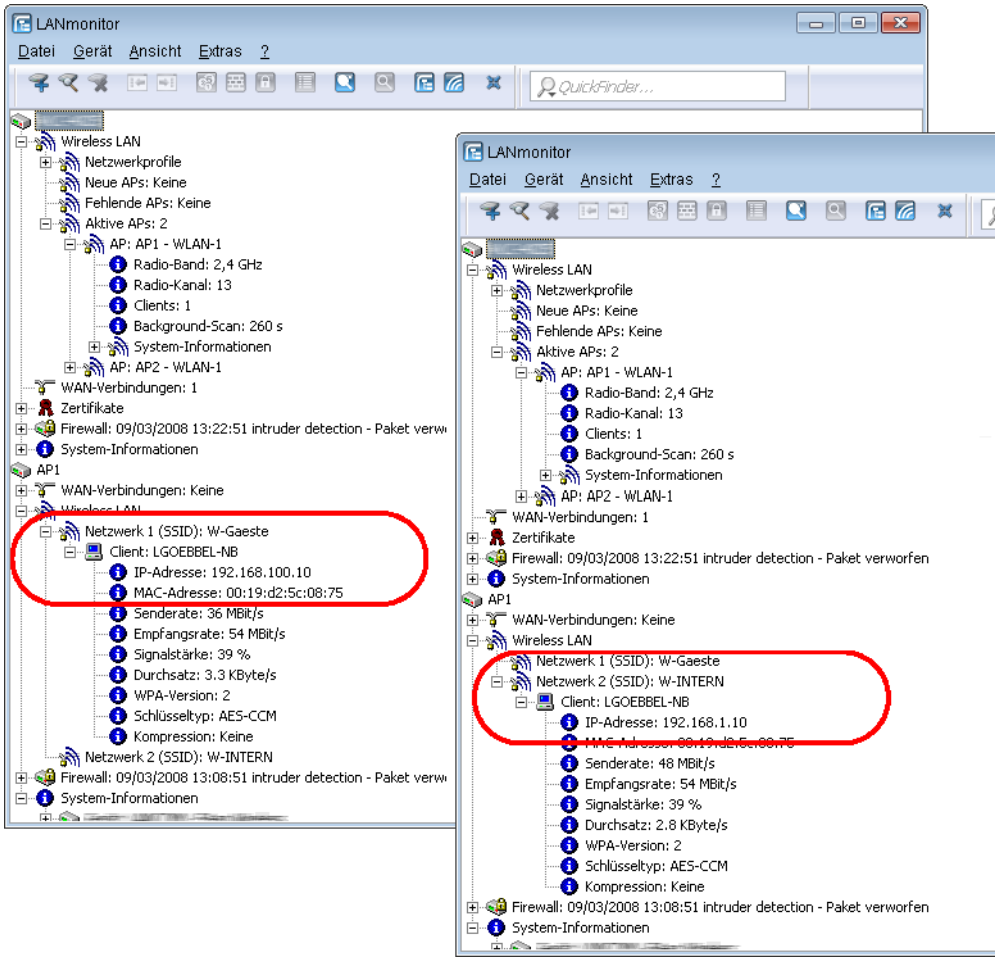


3. Aktivieren Sie für die beiden IP-Netzwerke den DHCP-Server.

› LANconfig: **TCP/IP** > **Allgemein** > **IP-Netzwerke**



Mit diesen Einstellungen können die WLAN-Clients der internen Mitarbeiter und der Gäste gezielt den jeweiligen Netzwerken zugeordnet werden.

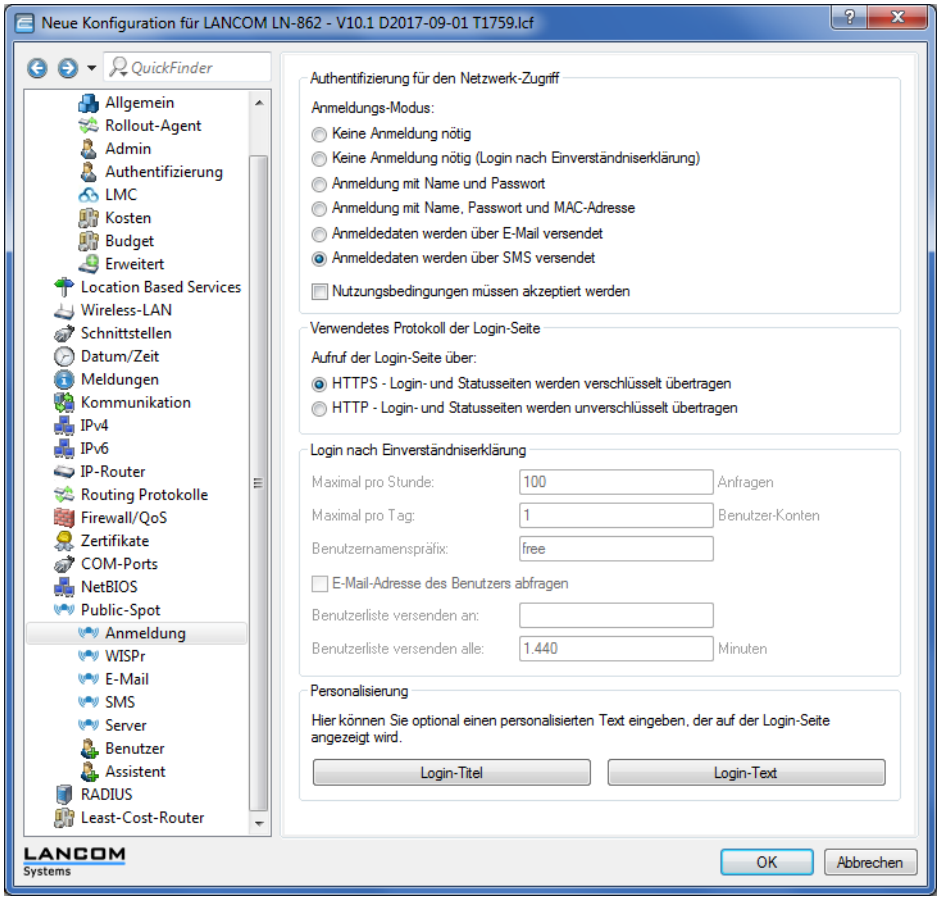


Konfiguration der Public Spot-Zugänge

Mit dem Public Spot bieten Sie einen kontrollierten Zugriffspunkt auf Ihr WLAN. Die Authentifizierung erfolgt durch Benutzerabfrage über ein Webinterface. Bei Bedarf können Sie den Zugang zeitlich begrenzen.

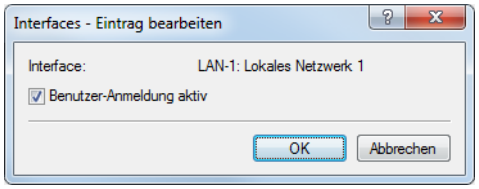
1. Aktivieren Sie die Authentifizierung für den Netzwerk-Zugriff mit Benutzername und Passwort.

› LANconfig: **Public-Spot** > **Anmeldung** > **Authentifizierung für den Netzwerk-Zugriff**



2. Aktivieren Sie die Benutzeranmeldung für das Controller-Interface, über das er mit dem Switch verbunden ist.

› LANconfig: **Public-Spot** > **Server** > **Betriebseinstellungen** > **Interfaces**

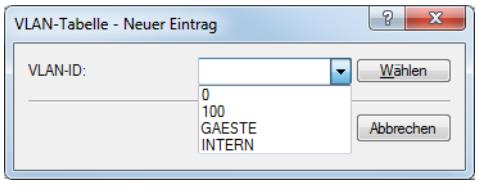


3. Regulieren Sie den Zugang zum Public Spot.

Mit dem Eintrag der VLAN-ID "100" für das Gäste-Netzwerk in der VLAN-Tabelle beschränken Sie die Public Spot-Verwendung auf Datenpakete aus diesem virtuellen LAN. Alle Datenpakete aus anderen VLANs werden ohne Anmeldung am Public Spot weitergeleitet.

Ohne die Einschränkung des Interfaces auf die VLAN-ID ist der Controller auf dem angegebenen physikalischen Ethernet-Port nicht mehr erreichbar!

› LANconfig: **Public-Spot** > **Server** > **VLAN-Tabelle**



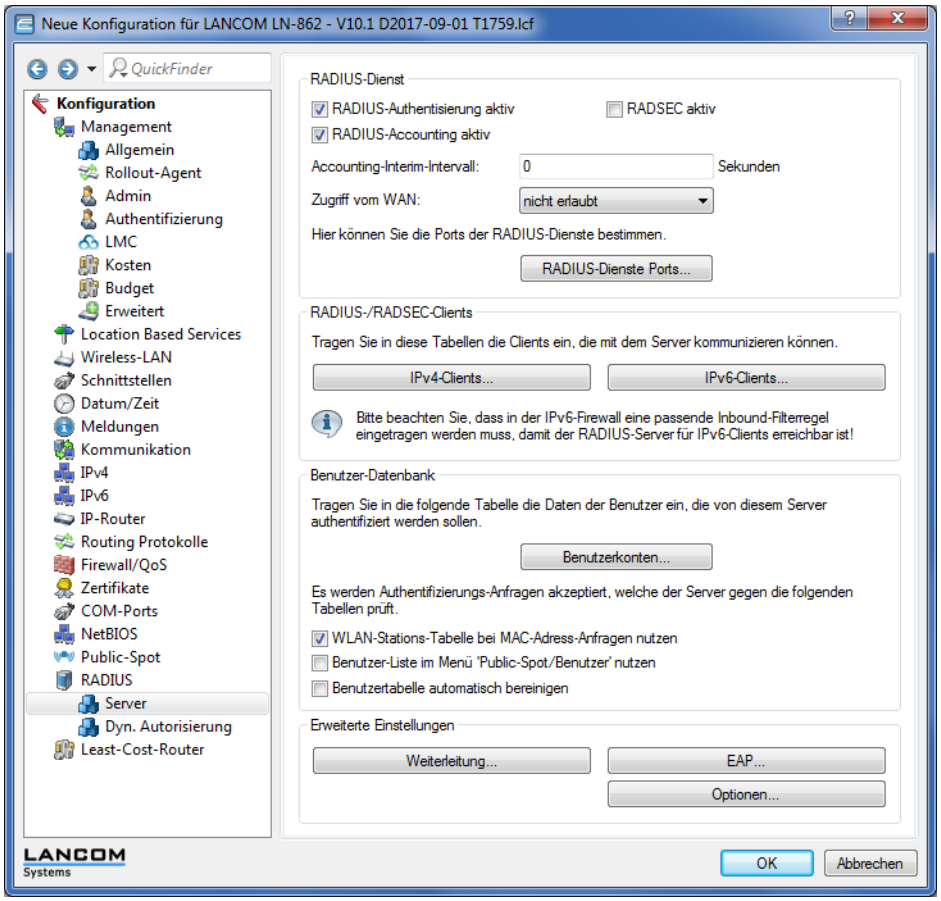
4. Aktivieren Sie die Option zum Bereinigen der Benutzertabelle, damit das Gerät nicht mehr benötigte Einträge automatisch löscht.

   › LANconfig: **RADIUS** > **Server** > **Benutzer-Datenbank** > **Benutzertabelle automatisch bereinigen**

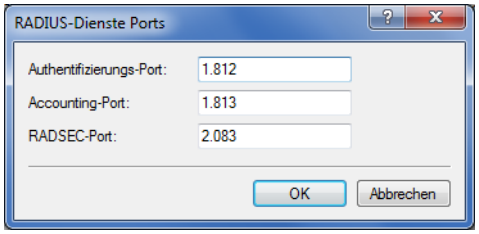
Internen RADIUS-Server für Public Spot-Nutzung konfigurieren

Der Assistent speichert die Public Spot-Zugänge in der Benutzerdatenbank des internen RADIUS-Servers. Damit Sie diese Public Spot-Zugänge nutzen können, wurde der interne RADIUS-Server standardmäßig vorkonfiguriert. Dies können Sie in **LANconfig** wie folgt einsehen:

1. Navigieren Sie zu **RADIUS** > **Server** > **RADIUS-Dienst**.
2. Stellen Sie sicher, dass die Häkchen für **RADIUS-Authentisierung aktiv** und **RADIUS-Accounting aktiv** gesetzt sind.



3. Klicken Sie die Schaltfläche **RADIUS-Dienste Ports**.

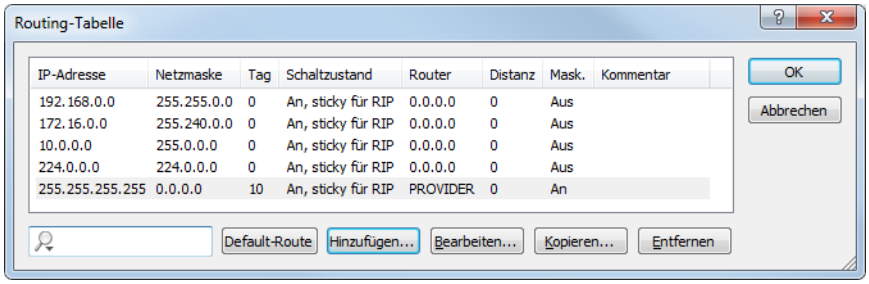


Hier sehen Sie die Default-Einstellungen.

Konfiguration des Internetzugangs für das Gästenetzwerk

1. Um den Benutzern des Gast-Netzes einen Internetzugang bereitzustellen, nutzen Sie z. B. den Assistenten für die Einrichtung eines Zugangs zum Providernetz.
2. Beschränken Sie den Zugang zum Providernetz.
   Damit dieser Zugang nur für die Benutzer im Gästenetzwerk zur Verfügung steht, vergeben Sie der entsprechenden Route das Routing-Tag "10". Damit können nur Datenpakete aus dem IP-Netzwerk "GAESTE" mit dem Schnittstellen-Tag "10" in das Netz des Providers übertragen werden. Das Routing zwischen dem Gäste-Netzwerk und dem internen Netzwerk ist aufgrund der unterschiedlichen Routing-Tags ausgeschlossen.

   › LANconfig: **IP-Router** > **Routing** > **Routing-Tabelle**



3. Optional: Laden Sie im LANconfig ggf. über **Gerät** > **Konfigurations-Verwaltung** > **Zertifikat oder Datei hochladen** eine HTML-Vorlage und ein Bild als Vorlage für die Ausgabe der Vouchers in das Gerät.
   Das Bild kann als GIF, JPEG oder PNG vorliegen und darf maximal 64 KB groß sein.

1.4.2 Virtualisierung und Gastzugang über WLAN Controller ohne VLAN

"Overlay Netzwerk": Netzwerke für Access Points trennen ohne VLAN

Die Trennung von Netzwerken in einer gemeinsam genutzten physikalischen Infrastruktur basiert in vielen Fällen auf dem Einsatz von VLANs. Dieses Verfahren setzt allerdings voraus, dass die eingesetzten Switches VLAN-fähig sind und dass in allen Switches die entsprechenden VLAN-Konfigurationen durchgeführt werden. Der Administrator rollt die VLAN-Konfiguration in diesem Beispiel also über das gesamte Netzwerk aus.

Mit einem WLC können Sie die Netze auch mit minimalem Einsatz von VLANs trennen. Über einen CAPWAP-Datentunnel leiten die APs die Nutzdaten der angeschlossenen WLAN-Clients direkt zum WLC, der die Daten den entsprechenden VLANs zuordnet. Die VLAN-Konfiguration beschränkt sich dabei auf den WLC und einen einzigen zentralen Switch. Alle anderen Switches arbeiten in diesem Beispiel ohne VLAN-Konfiguration.

Mit dieser Konfiguration reduzieren Sie das VLAN auf den Kern der Netzstruktur (in der Grafik blau hinterlegt dargestellt). Darüber hinaus erfordern lediglich 3 der genutzten Switch-Ports eine VLAN-Konfiguration.

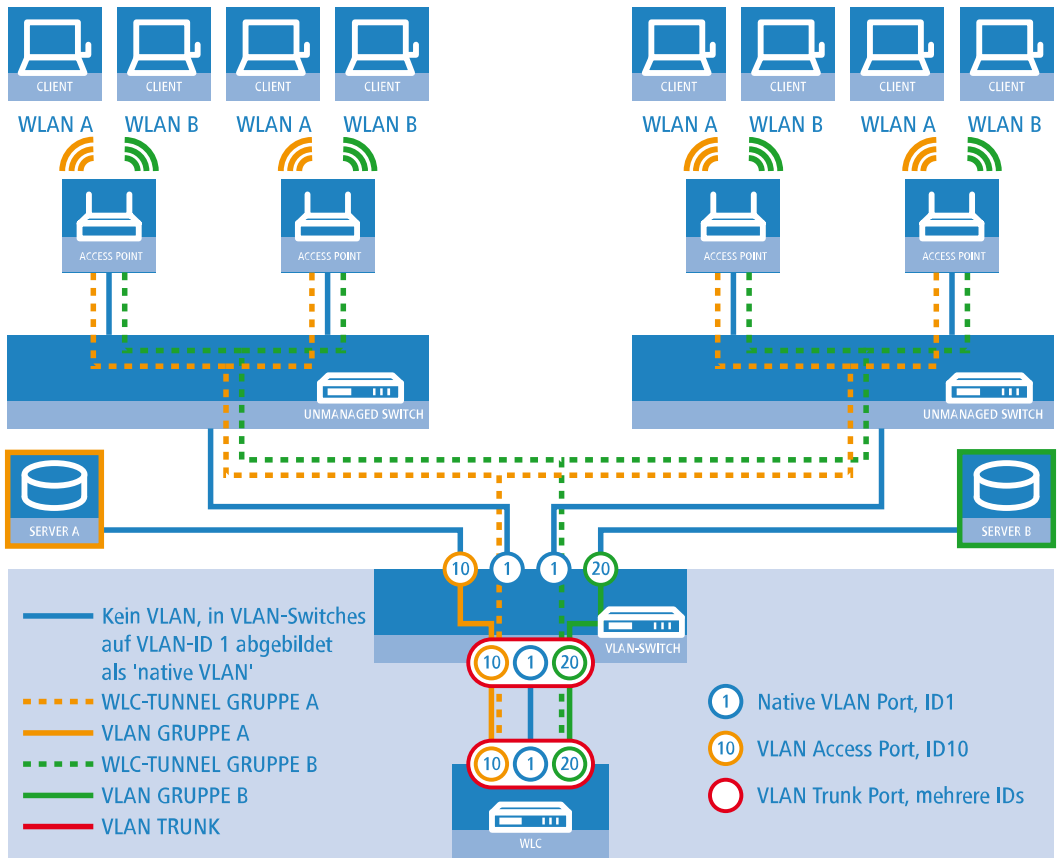


Abbildung 4: Anwendungsbeispiel Overlay-Netz

Die Grafik zeigt ein Anwendungsbeispiel mit den folgenden Komponenten:

- Das Netz besteht aus zwei Segmenten mit jeweils einem eigenen (nicht unbedingt VLAN-fähigen) Switch.
- In jedem Segment stehen mehrere APs, angeschlossen an den jeweiligen Switch.
- Jeder AP bietet zwei SSIDs für die WLAN-Clients aus verschiedenen Benutzergruppen an, in der Grafik dargestellt in Grün und Orange.
- Jede der Benutzergruppen hat Zugang zu einem eigenen Server, der vor dem Zugriff aus anderen Benutzergruppen getrennt ist. Die Server sind nur durch die auf dem Switch konfigurierten Access-Ports über die entsprechenden VLANs erreichbar.
- Ein WLC verwaltet alle APs in Netz.
- Ein zentraler, VLAN-fähiger Switch verbindet die Switches der Segmente, die gruppenbezogenen Server und den WLC.

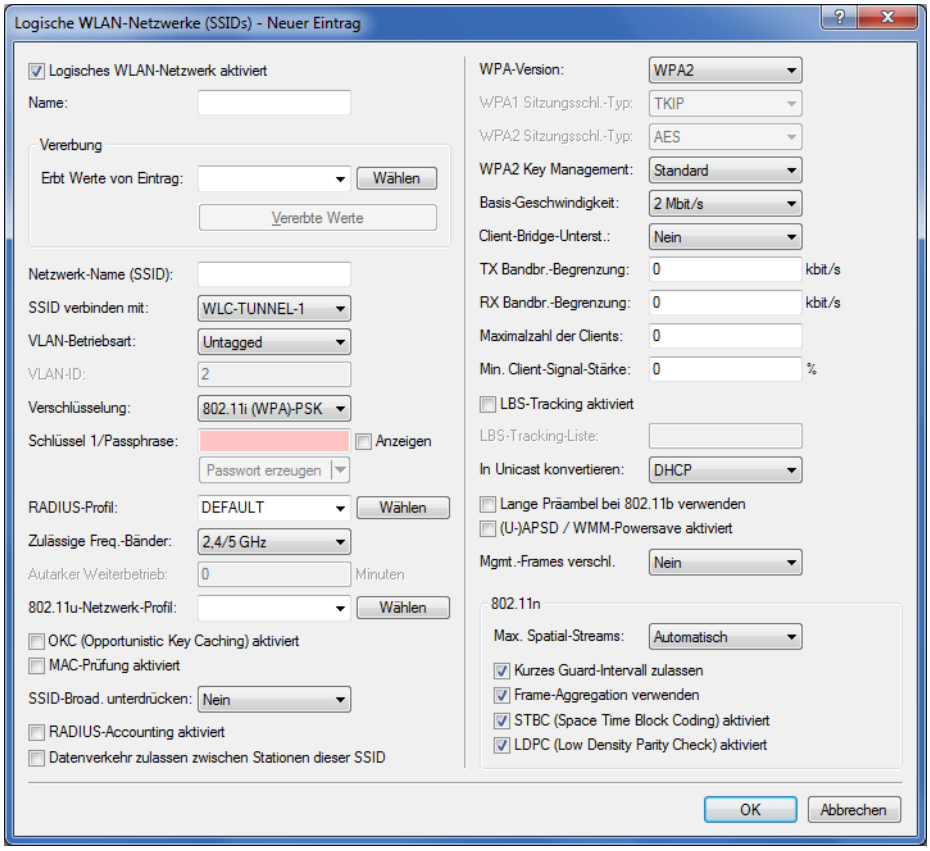
Das Ziel der Konfiguration: Ein WLAN-Client, der sich an einer bestimmten SSID anmeldet, soll Zugang zu "seinem" Server haben – unabhängig vom verwendeten AP und unabhängig vom Segment, in dem er sich gerade befindet.

Die folgende Beschreibung basiert auf einer funktionsfähigen Grundkonfiguration des WLCs. Die Konfiguration des VLAN-Switches ist nicht Bestandteil dieser Beschreibung.

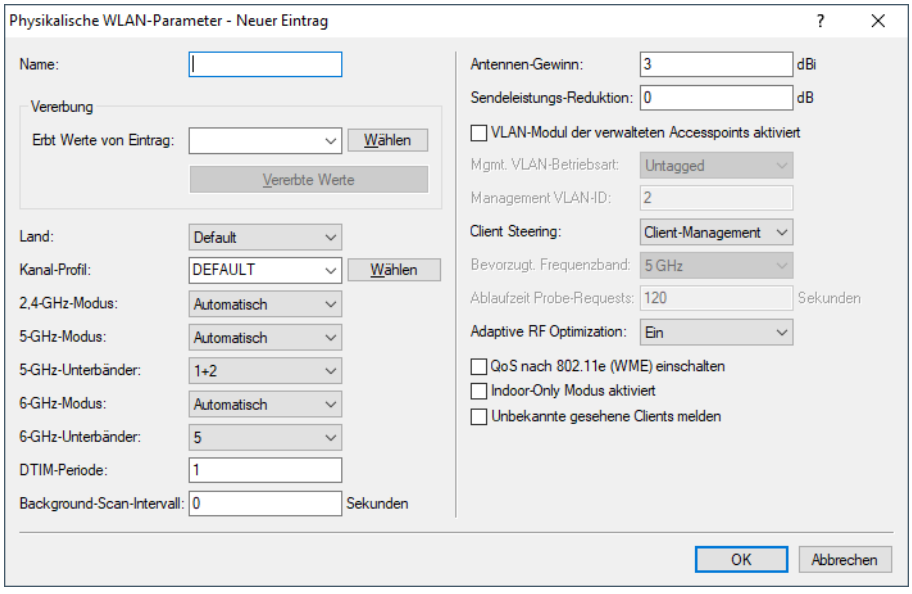
Konfiguration der WLAN-Einstellungen

1. Erstellen Sie für jede SSID einen Eintrag in der Liste der logischen Netzwerke mit einem passenden Namen und der zugehörigen SSID. Verbinden Sie diese SSID mit einem WLC-Tunnel, die erste SSID z. B. mit 'WLC-TUNNEL-1' und die zweite mit 'WLC-TUNNEL-2'. Stellen Sie die VLAN-Betriebsart jeweils auf 'Tagged' mit der VLAN-ID '10' für das

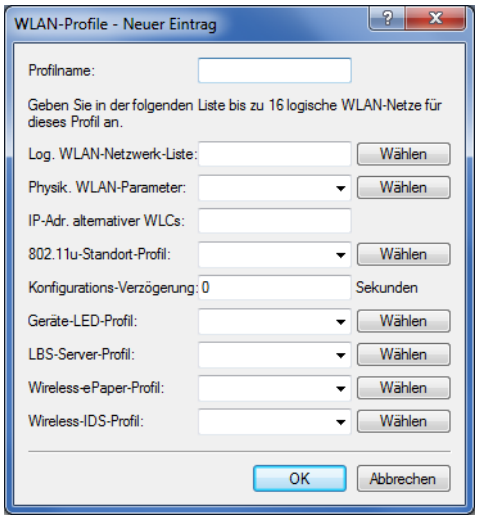
erste logischen Netz und der VLAN-ID '20' für das zweite logischen Netz. In LANconfig finden Sie diese Einstellungen unter **Konfiguration** > **WLAN-Controller** > **Profile** > **Logische WLAN-Netzwerke (SSIDs)**.



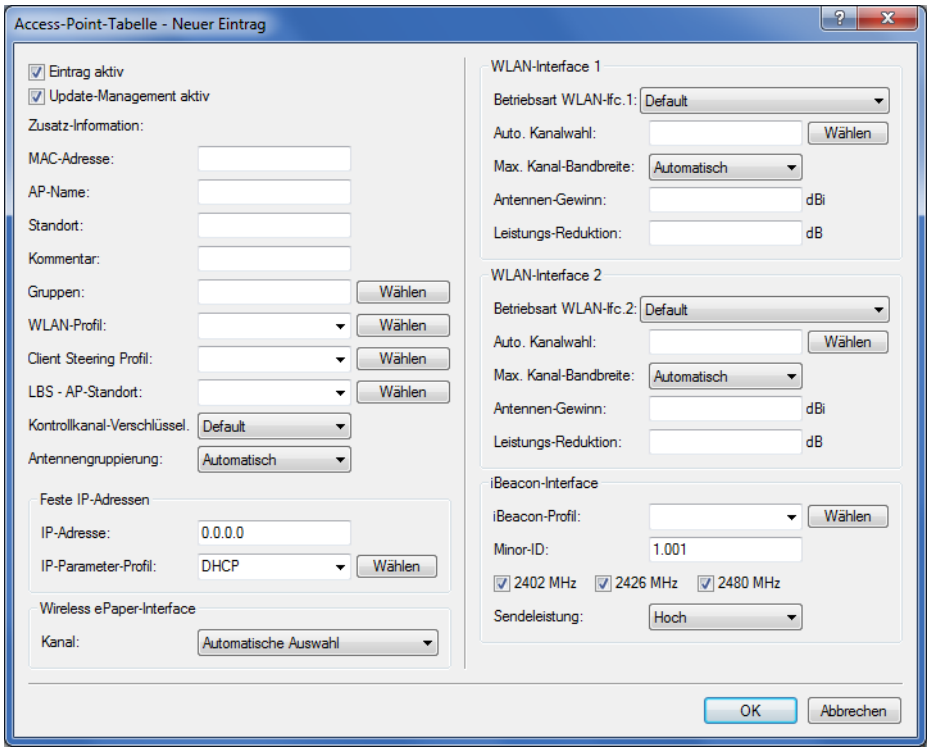
2. Erstellen Sie einen Eintrag in der Liste der physikalischen WLAN-Parameter mit den passenden Einstellungen für Ihre APs, z. B. für das Land 'Europa' mit den Kanälen 1, 6 und 11 im 802.11g/b/n und 802.11a/n gemischten Modus. Aktivieren Sie für dieses Profil der physikalischen WLAN-Parameter die Option, das VLAN-Modul auf den APs einzuschalten. Stellen Sie die Betriebsart für das Management-VLAN in den APs auf 'Ungetagged' ein. In LANconfig finden Sie diese Einstellungen unter **Konfiguration** > **WLAN-Controller** > **Profile** > **Physikalische WLAN-Parameter**.



3. Erstellen Sie ein WLAN-Profil mit einem passenden Namen und ordnen Sie diesem WLAN-Profil die zuvor erstellten logischen WLAN-Netzwerke und die physikalischen WLAN-Parameter zu. In LANconfig finden Sie diese Einstellungen unter **Konfiguration** > **WLAN-Controller** > **Profile** > **WLAN-Profile**.

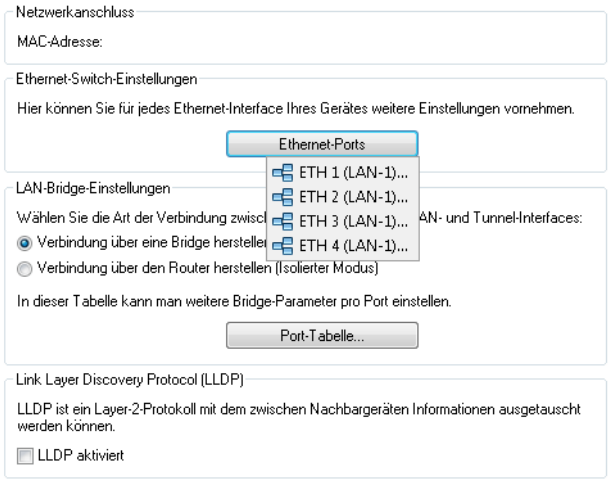


4. Erstellen Sie für jeden verwalteten AP einen Eintrag in der AP-Tabelle mit einem passenden Namen und der zugehörigen MAC-Adresse. Ordnen Sie diesem AP das zuvor erstellte WLAN-Profil zu. In LANconfig finden Sie diese Einstellungen unter **Konfiguration** > **WLAN-Controller** > **AP-Konfig.** > **Access-Point-Tabelle**.

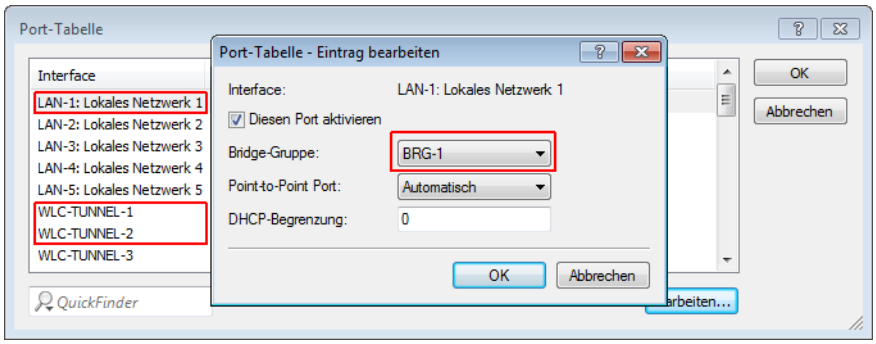


Konfiguration der Schnittstellen am WLC

5. Ordnen Sie jedem physikalischen Ethernet-Port eine separate logische LAN-Schnittstelle zu, z. B. 'LAN-1'. Stellen Sie sicher, dass die anderen Ethernet-Ports nicht der gleichen LAN-Schnittstelle zugeordnet sind. In LANconfig finden Sie diese Einstellungen unter **Konfiguration** > **Schnittstellen** > **LAN** > **Ethernet-Ports**.

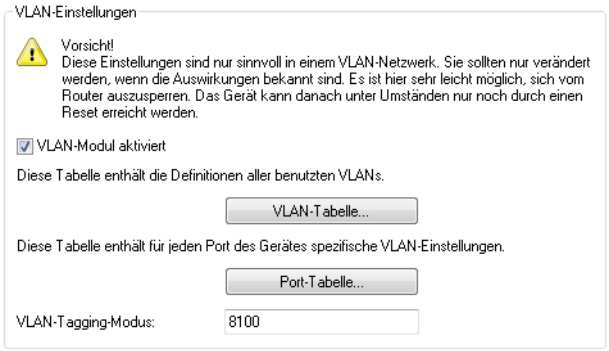


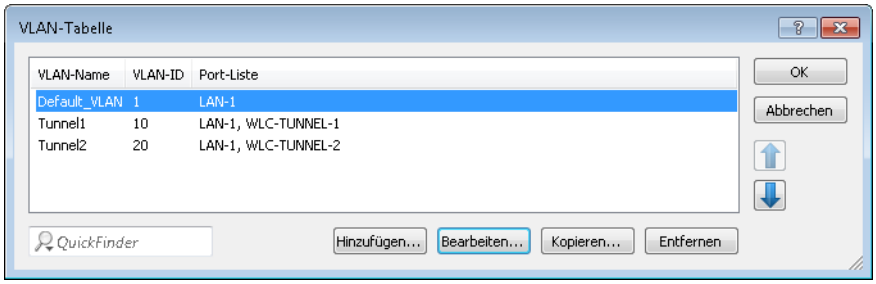
6. Ordnen Sie die logische LAN-Schnittstelle 'LAN-1' und die WLC-Tunnel 'WLC-Tunnel-1' und 'WLC-Tunnel-2' der Bridge-Gruppe 'BRG-1' zu. Stellen Sie sicher, dass die anderen LAN-Schnittstellen nicht der gleichen Bridge-Gruppe zugeordnet sind. In LANconfig finden Sie diese Einstellungen unter **Konfiguration** > **Schnittstellen** > **LAN** > **Port-Tabelle**.



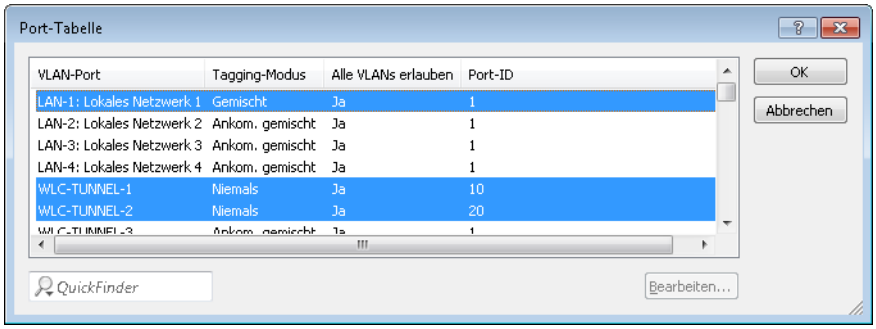
Die LAN-Schnittstellen und WLC-Tunnel gehören standardmäßig keiner Bridge-Gruppe an. Indem Sie die LAN-Schnittstelle 'LAN-1' sowie die beiden WLC-Tunnel 'WLC-Tunnel-1' und 'WLC-Tunnel-2' der Bridge-Gruppe 'BRG-1' zuordnen, leitet das Gerät alle Datenpakete zwischen LAN-1 und den WLC-Tunneln über die Bridge weiter.

7. Aktivieren Sie unter **Schnittstellen** > **VLAN** das VLAN-Modul des WLC und ordnen Sie unter **VLAN-Tabelle** dem gewünschten VLAN den oben gewählten LAN-Port (LAN-1) sowie den passenden WLC-Tunnel zu.





8. Stellen Sie unter **Schnittstellen** > **VLAN** > **Port-Tabelle** den Tagging-Modus der Tunnel-Interfaces sowie des LAN-Interfaces korrekt ein und setzen Sie die passende Port-VLAN-ID.



Je nach Schaltung des Switches konfigurieren Sie den Tagging-Modus des LAN-Interfaces auf 'Gemischt' oder 'Immer'.

Im Normalfall betreibt man die Tunnel-Interfaces im Modus 'Niemals', da Pakete hier (aus dem WLAN) immer ungetaggt ankommen und der WLC sie mit der Port-VLAN-ID versieht.

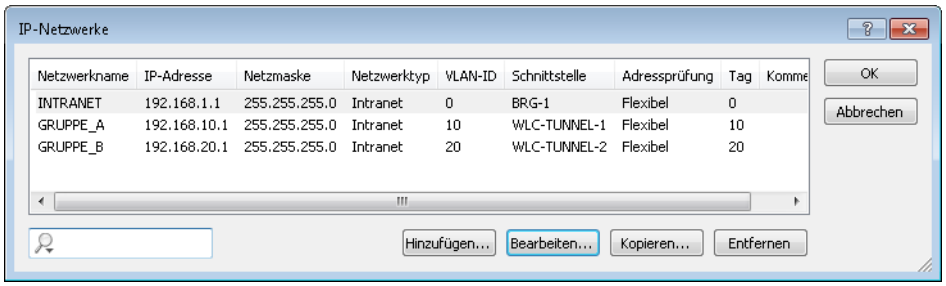
Bitte beachten Sie, dass bei Aktivierung des VLAN-Moduls die auf dem WLC angelegten ARF-Netze eine VLAN-ID erhalten müssen. Soll der WLC das Netz ohne VLAN-Tag erreichen, setzen Sie bei oben stehender VLAN-Konfiguration die '1' als VLAN-ID für das IP-Netz.

Eine ähnliche Konfiguration ist möglich, indem Sie schon am Access Point ein VLAN-Tag für die durch den Tunnel zu leitenden Pakete setzen und das VLAN-Modul des WLC nicht nutzen.

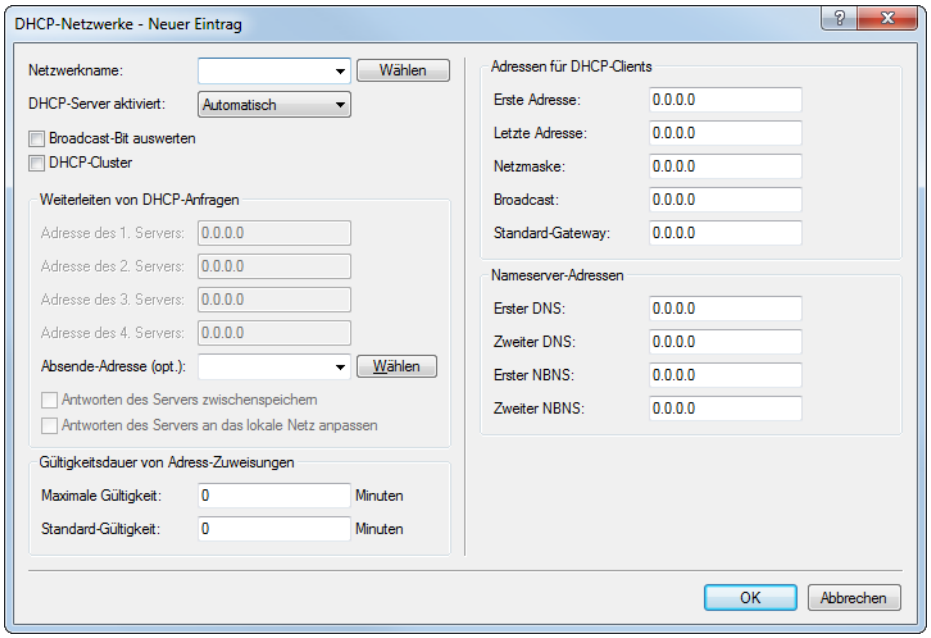
Dabei würde der WLC allerdings durch das Bridgen der verschiedenen WLC-Tunnel untereinander auch Broadcasts in alle Tunnel weiterleiten, was ab einer bestimmten Menge von Tunneln/SSIDs und APs zu Lastproblemen im Netz und auf dem WLC führen kann. Die vorliegende Konfiguration des VLAN-Moduls verhindert das.

9. Ergänzend konfigurieren Sie unter **IPv4** > **Allgemein** > **IP-Netzwerke** für die auf Layer 2 getrennten Netzwerke die IP-Einstellungen.

   Damit das Gerät die Netzwerke nicht wieder auf Layer 3 verbindet, ist auch eine Trennung auf Layer 3 erforderlich, z. B. durch ein Schnittstellen-Tag oder durch die Firewall.



10. Der WLC kann optional als DHCP-Server für die APs fungieren. Aktivieren Sie dazu den DHCP-Server für das 'INTRANET'. In LANconfig finden Sie diese Einstellungen unter **IPv4** > **DHCPv4** > **DHCP-Netzwerke**.



WLAN-Controller mit Public Spot

Dieses Szenario basiert auf dem ersten Szenario (Overlay-Netzwerk) und erweitert es um spezifische Einstellungen für eine Benutzer-Authentifizierung.

Die Durchleitung der Nutzdaten aus den WLANs über WLC-Tunnel bis zum WLC ermöglicht eine besonders einfache Konfiguration von Public Spots z. B. für Gäste parallel zu einem intern genutzten WLAN.

In diesem Beispiel haben die Mitarbeiter einer Firma Zugang zu einem eigenen WLAN (SSID), die Gäste erhalten über einen Public Spot ebenfalls Zugang zum Internet. Die APs in allen Bereichen des Gebäudes bieten die beiden SSIDs 'FIRMA' und 'GAESTE' an.

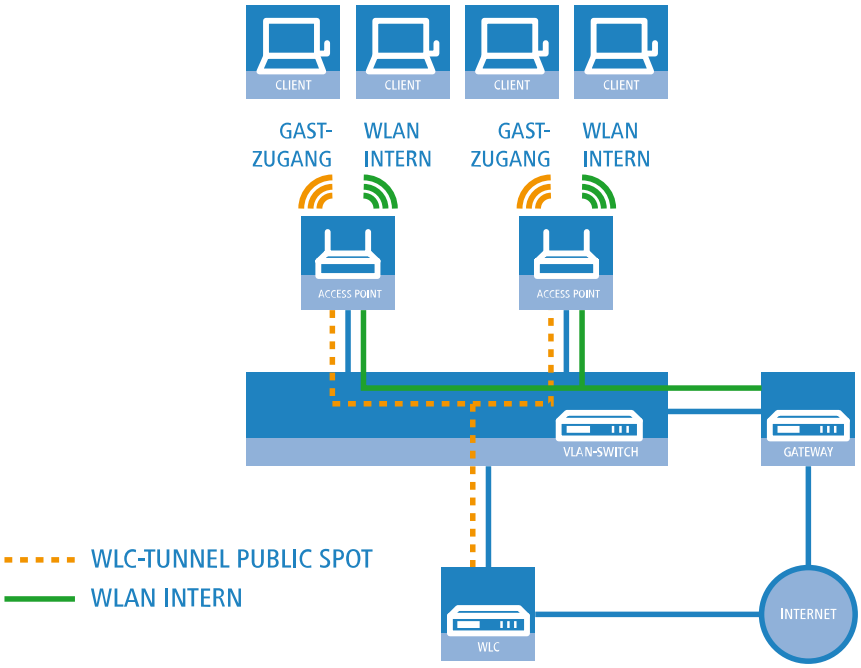
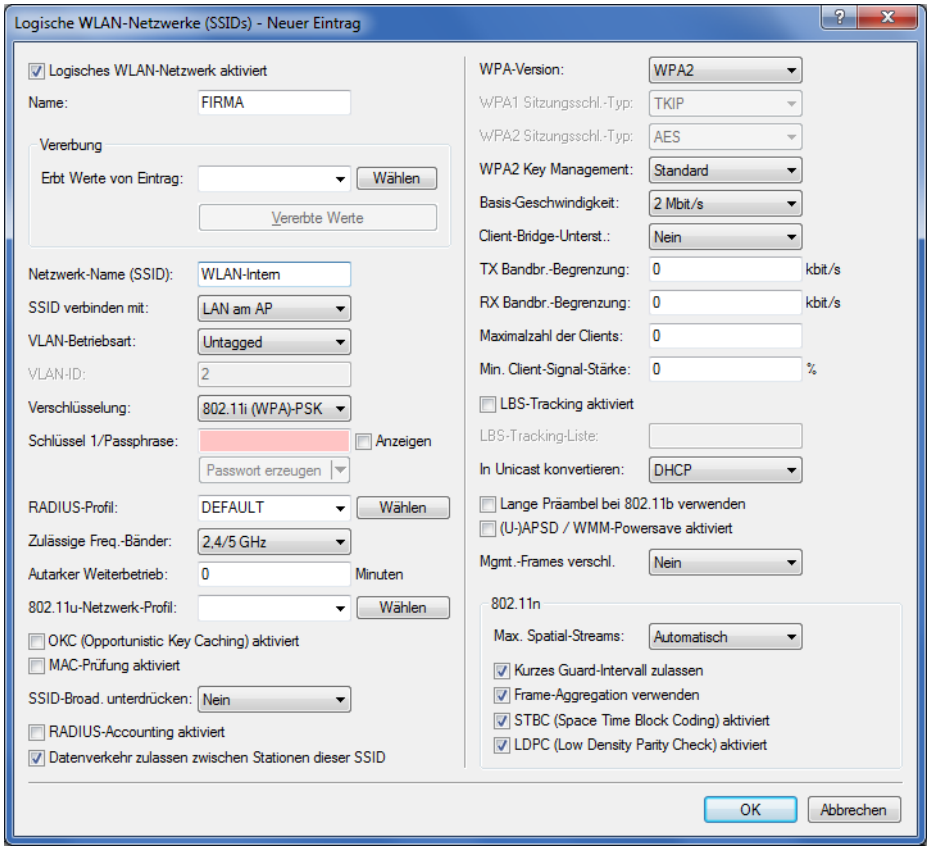


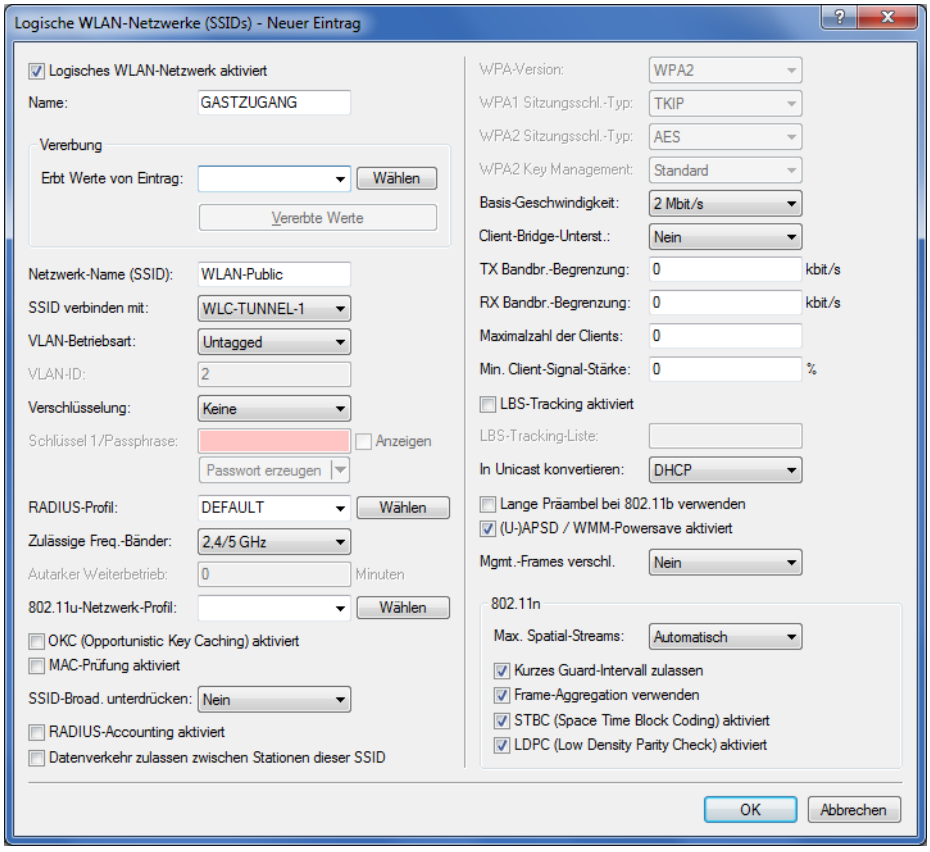
Abbildung 5: Anwendungsbeispiel WLAN-Controller mit Public Spot

Das Ziel der Konfiguration: Ein WLAN-Client, der sich an der internen SSID anmeldet, soll Zugang zu allen internen Ressourcen und zum Internet über das zentrale Gateway erhalten. Die APs koppeln die Nutzdaten der internen Clients lokal aus und leiten sie direkt in das LAN weiter. Die WLAN-Clients der Gäste melden sich am Public Spot an. Die APs leiten die Nutzdaten der Gäste-Clients über einen WLC-Tunnel direkt zum WLC, der über eine separate WAN-Schnittstelle Zugang zum Internet ermöglicht.

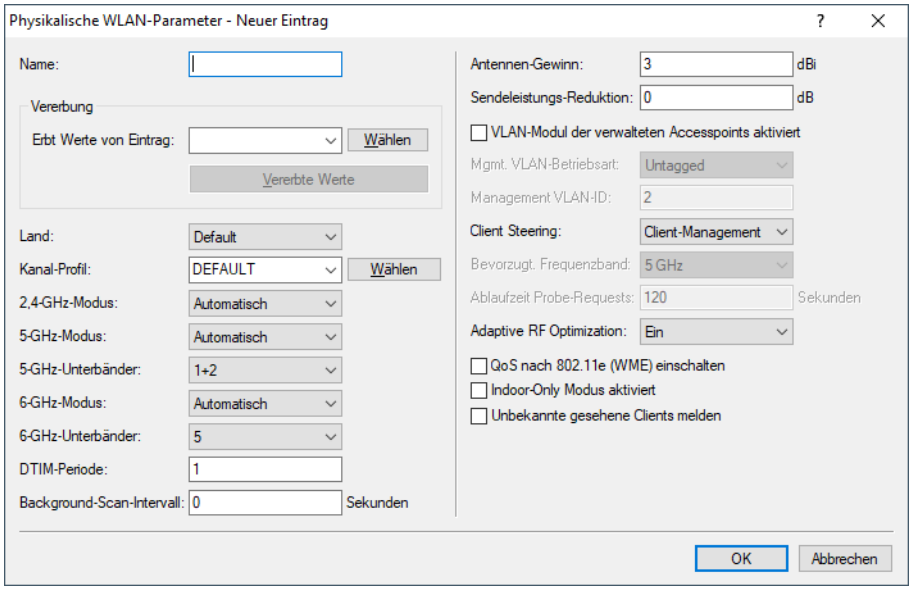
1. Erstellen Sie für das interne WLAN und das Gäste-WLAN jeweils einen Eintrag in der Liste der logischen Netzwerke mit einem passenden Namen und der zugehörigen SSID. Verbinden Sie die SSID für die interne Nutzung mit dem 'LAN am AP', die SSID für die Gäste z. B. mit 'WLC-TUNNEL-1'. Deaktivieren Sie bei der SSID für das Gästenetzwerk die Verschlüsselung, damit sich die WLAN-Clients der Gäste beim Public Spot anmelden können. Unterbinden Sie

für diese SSID außerdem den Datenverkehr der Stationen untereinander (Interstation-Traffic). In LANconfig finden Sie diese Einstellung unter **Konfiguration** > **WLAN-Controller** > **Profile** > **Logische WLAN-Netzwerke (SSIDs)**.

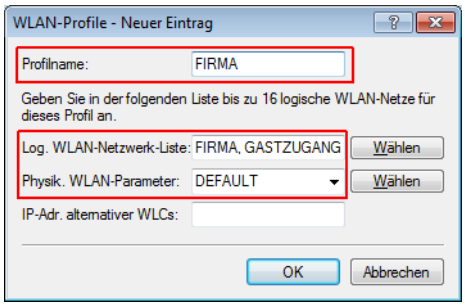




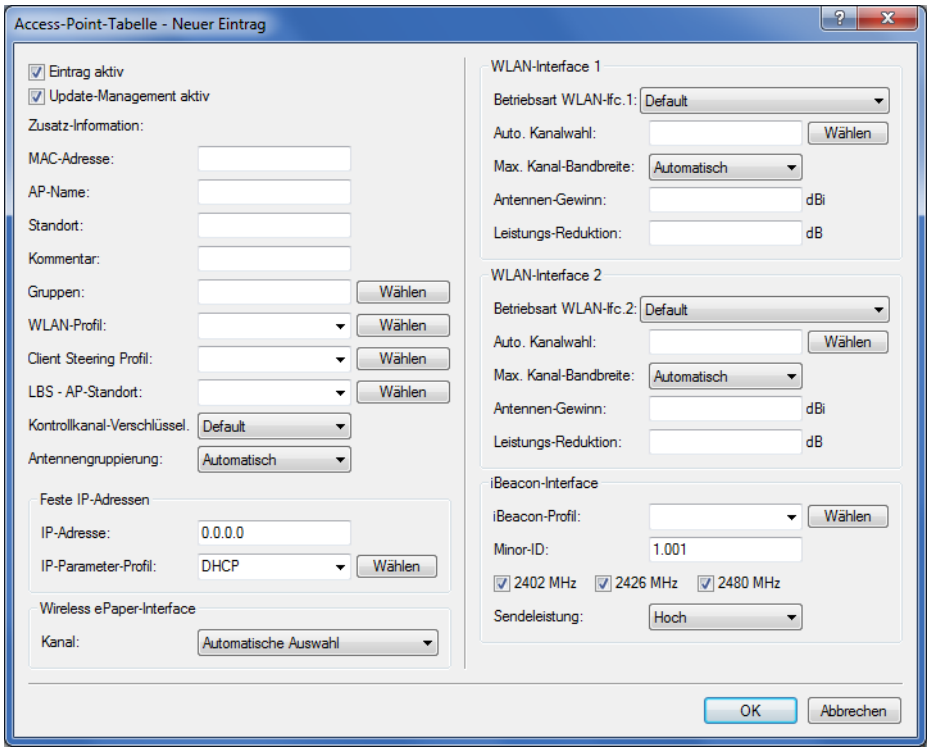
2. Erstellen Sie einen Eintrag in der Liste der physikalischen WLAN-Parameter mit den passenden Einstellungen für Ihre APs, z. B. für das Land 'Europa' mit den Kanälen 1, 6 und 11 im 802.11g/b/n und 802.11a/n gemischten Modus. In LANconfig finden Sie diese Einstellung unter **Konfiguration** > **WLAN-Controller** > **Profile** > **Physikalische WLAN-Parameter**.



3. Erstellen Sie ein WLAN-Profil mit einem passenden Namen und ordnen Sie diesem WLAN-Profil die zuvor erstellten logischen WLAN-Netzwerke und die physikalischen WLAN-Parameter zu. In LANconfig finden Sie diese Einstellung unter **Konfiguration** > **WLAN-Controller** > **Profile** > **WLAN-Profile**.

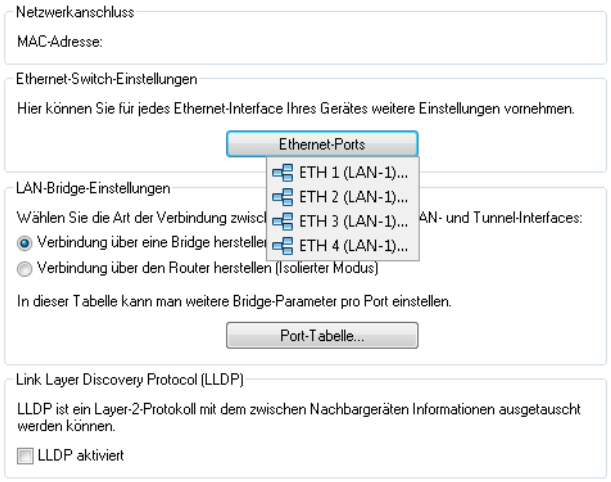


4. Erstellen Sie für jeden verwalteten AP einen Eintrag in der AP-Tabelle mit einem passenden Namen und der zugehörigen MAC-Adresse. Ordnen Sie diesem AP das zuvor erstellte WLAN-Profil zu. In LANconfig finden Sie diese Einstellung unter **Konfiguration** > **WLAN-Controller** > **AP-Konfig** > **Access-Point-Tabelle**.

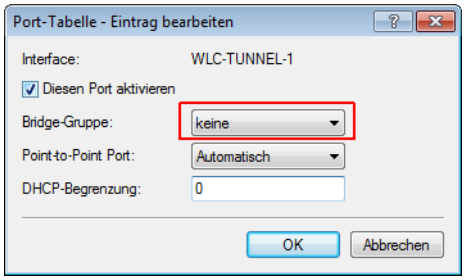


5. Ordnen Sie jedem physikalischen Ethernet-Port eine separate logische LAN-Schnittstelle zu, z. B. 'LAN-1'. Stellen Sie den 4. Ethernet-Port auf die logische LAN-Schnittstelle 'DSL-1' ein. Der WLC verwendet diese LAN-Schnittstelle später

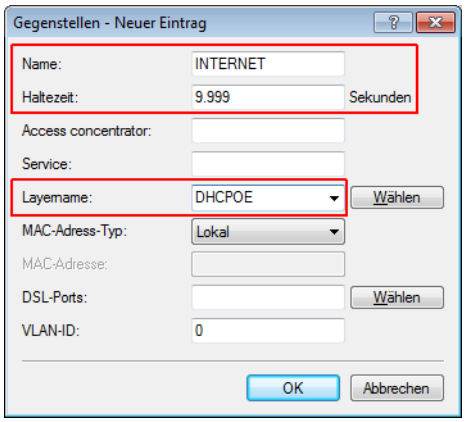
für den Internetzugang des Gästenetzes. In LANconfig finden Sie diese Einstellung unter **Konfiguration** > **Schnittstellen** > **LAN** > **Ethernet-Ports**.



6. Überprüfen Sie, dass die logische LAN-Schnittstelle 'WLC-Tunnel 1' keiner Bridge-Gruppe zugeordnet ist. So stellen Sie sicher, dass die anderen LAN-Schnittstellen keine Daten zum Public Spot-Netzwerk übertragen. In LANconfig finden Sie diese Einstellung unter **Konfiguration** > **Schnittstellen** > **LAN** > **Port-Tabelle**.

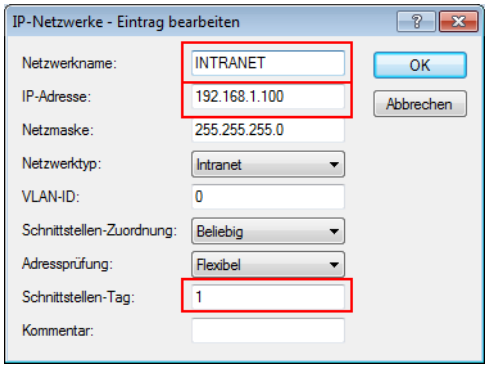


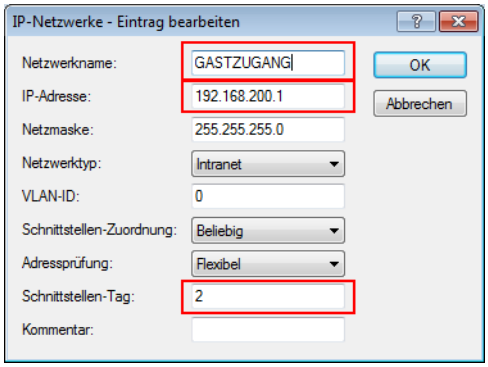
7. Erstellen Sie für den Internetzugang der Gäste einen Eintrag in der Liste der DSL-Gegenstellen mit der Haltezeit '9999' und dem vordefinierten Layer 'DHCPOE'. Dieses Beispiel setzt voraus, dass ein Router mit aktiviertem DHCP-Server den Internetzugang bereitstellt. In LANconfig finden Sie diese Einstellung unter **Konfiguration** > **Kommunikation** > **Gegenstellen** > **Gegenstellen**.



8. Erstellen Sie für die interne Nutzung das IP-Netzwerk 'INTRANET' z. B. mit der IP-Adresse '192.168.1.100' und mit dem Schnittstellen-Tag '1', für die Gäste das IP-Netzwerk 'GASTZUGANG' z. B. mit der IP-Adresse '192.168.200.1' und mit dem Schnittstellen-Tag '2'. Der virtuelle Router im WLC nutzt die Schnittstellen-Tags, um die Routen für die

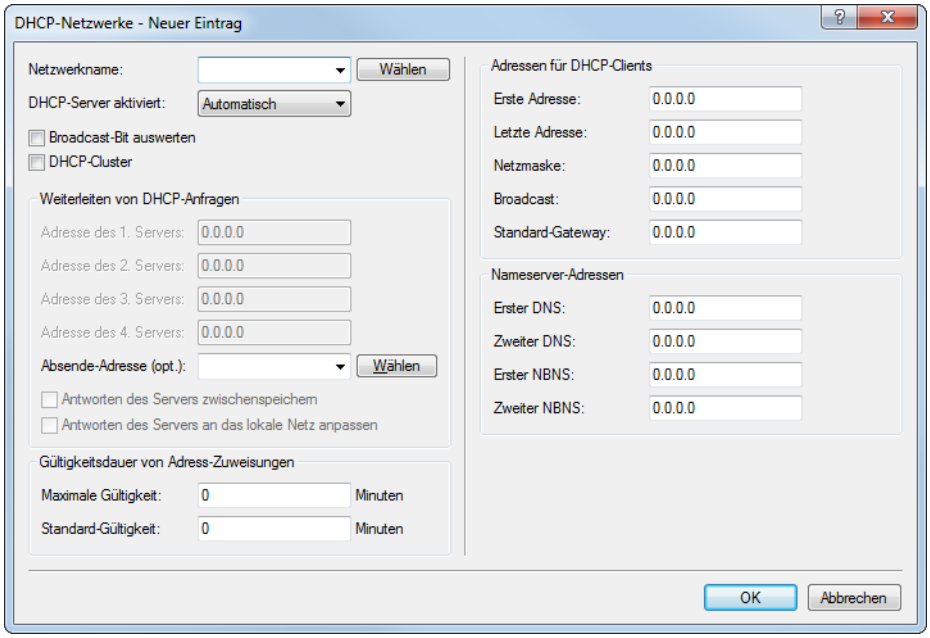
beiden Netzwerke zu trennen. In LANconfig finden Sie diese Einstellung unter **Konfiguration** > **TCP/IP** > **Allgemein** > **IP-Netzwerke**.



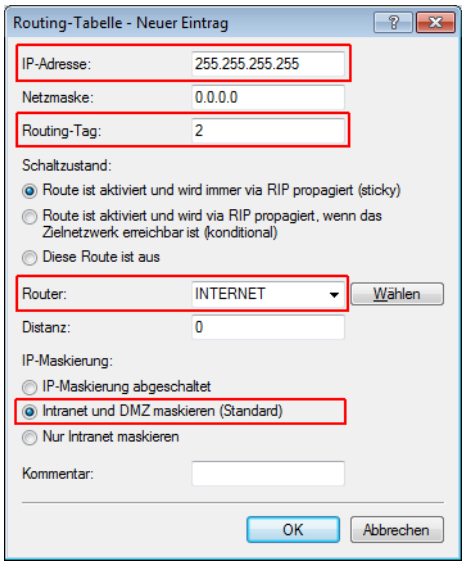


9. Der WLC kann als DHCP-Server für die APs und die angemeldeten WLAN-Clients fungieren. Aktivieren Sie dazu den DHCP-Server für das 'INTRANET' und den 'GASTZUGANG. In LANconfig finden Sie diese Einstellung unter **Konfiguration** > **TCP/IP** > **DHCP** > **DHCP-Netzwerke**.

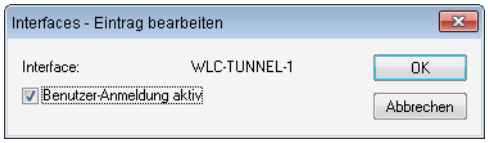
Die Aktivierung des DHCP-Servers ist für das Gästenetz zwingend, für das interne Netz optional. Für das interne Netz können Sie den DHCP Server auch anders realisieren.



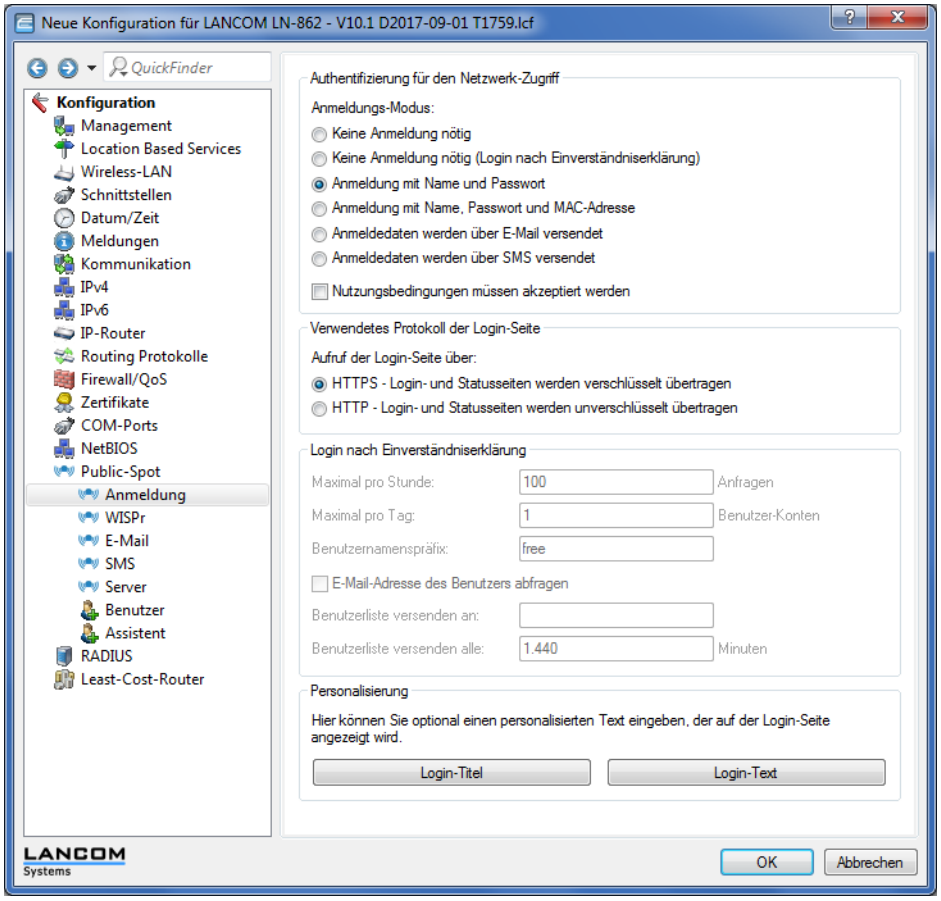
10. Erstellen Sie eine neue Standard-Route in der Routing-Tabelle, welche die Daten aus dem Gästenetzwerk auf den Internet-Zugang des WLCs leitet. Wählen Sie dazu das Routing-Tag '2' und den Router 'Internet'. Aktivieren Sie außerdem die Option 'Intranet und DMZ maskieren (Standard)'. In LANconfig finden Sie diese Einstellung unter **Konfiguration** > **IP-Router** > **Routing** > **Routing-Tabelle**.



11. Aktivieren Sie die Public Spot-Anmeldung für die logische LAN-Schnittstelle 'WLC-Tunnel 1'. In LANconfig finden Sie diese Einstellung unter **Konfiguration** > **Public-Spot** > **Server** > **Betriebseinstellungen** > **Interfaces**.



12. Aktivieren Sie im letzten Schritt die Anmeldung über den Public-Spot für den WLC. In LANconfig finden Sie diese Einstellung unter **Konfiguration** > **Public-Spot** > **Anmeldung**.



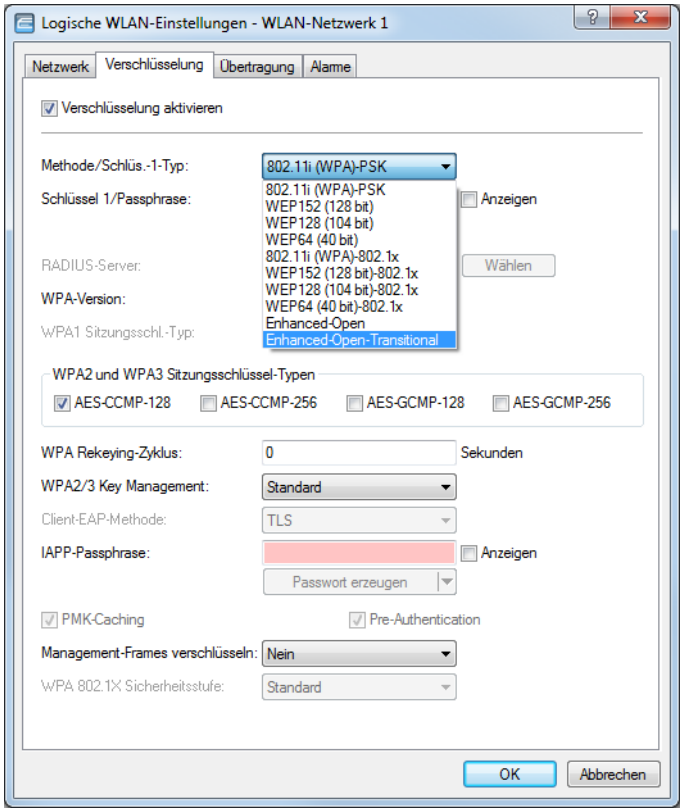
Neben der Konfiguration des WLCs konfigurieren Sie den Public Spot nach Ihren Wünschen entweder für die interne Benutzerliste oder für die Verwendung eines RADIUS-Servers.

1.4.3 Einrichtung eines sicheren Hotspots mit Enhanced Open

Mit Enhanced Open bietet sich erstmals die Möglichkeit, einen sicheren und trotzdem einfach bedienbaren Hotspot anzubieten.

Hierzu wird Enhanced Open mit der LANCOM Public Spot Option kombiniert.

Richten Sie hierzu das für den Hotspot zu nutzende WLAN wie gewohnt ein – wählen Sie allerdings als Verschlüsselungsmethode **Enhanced Open-Transitional**:



Die Eingabe eines Schlüssels ist nicht erforderlich und auch nicht möglich: Ein Enhanced Open-fähiger Client baut ohne Angabe eines Schlüssels eine verschlüsselte Verbindung zum Access Point auf. Die Benutzererfahrung ist damit identisch zu der bei Verwendung eines unverschlüsselten WLANs: Das Eingeben eines vorher erhaltenen Schlüssels wie bei WPA2-PSK entfällt.

Die Nutzung des Transitional-Modus bewirkt, dass die selbe SSID gleichzeitig von Clients verwendet werden kann, die Enhanced Open unterstützen, sowie von Clients, die noch kein Enhanced Open unterstützen. Im letztgenannten Fall kommt allerdings keine Verschlüsselung zum Einsatz, so dass die SSID wie eine ohne Verschlüsselung betriebene SSID funktioniert. Sobald Enhanced Open in der Zukunft eine hohe Marktdurchdringung erreicht hat, kann vom Transitional-Modus in den regulären Enhanced Open-Modus gewechselt werden.

Anschließend kann wie gewohnt mit der Konfiguration des Public Spot-Moduls fortgefahren werden. Da das Public Spot-Modul unabhängig von den Verschlüsselungseinstellungen der WLAN-Schnittstellen ist, können alle Funktionen des Public Spot-Moduls in Zusammenhang mit Enhanced Open ohne Einschränkung verwendet werden.

Zusammenfassend eignet sich Enhanced Open ideal für den Betrieb von Hotspots, da es ein höheres Sicherheitsniveau als die bisher verwendeten, unverschlüsselten Hotspots bietet. Durch den optionalen Transitional-Modus ist sichergestellt, dass auch Clients, welche Enhanced Open noch nicht unterstützen, transparent angebunden werden können.

1.4.4 Einrichtung eines externen RADIUS-Servers für die Benutzerverwaltung

In manchen Anwendungen sollen die Benutzerdaten nicht im Gerät gespeichert werden, sondern in einem externen, zentralen RADIUS-Server. In diesem Fall muss der Public Spot zur Überprüfung der Benutzerdaten mit diesem externen RADIUS-Server kommunizieren.

Beachten Sie, dass Ihnen bestimmte Funktionen (wie z. B. die Public Spot-Assistenten in WEBconfig) nicht zur Verfügung stehen, wenn Sie einen externen RADIUS-Server zur Benutzerverwaltung einsetzen!

Die folgende Anleitung setzt voraus, dass Ihnen die IP-Adresse eines funktionsfähigen RADIUS-Servers im Netzwerk bekannt ist.

Mit den folgenden Konfigurationsschritten richten Sie einen Public Spot für die Nutzung eines externen RADIUS-Servers ein:

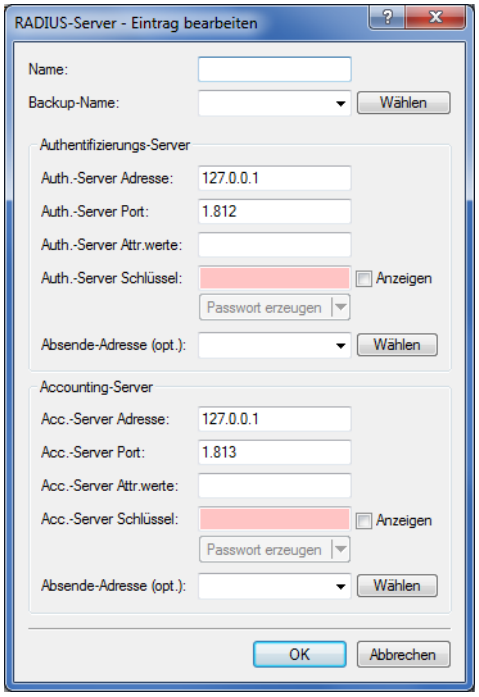
1. Führen Sie die Schritte aus dem Abschnitt *Manuelle Installation* aus.

   Die exakte Uhrzeit im Gerät ist hier u. a. für die korrekte Steuerung von zeitlich begrenzten Zugängen notwendig.

   Wenn die Authentifizierung mit zusätzlicher Prüfung der physikalischen Adresse (MAC-Adresse) eingestellt ist, übermittelt der Public Spot bei der Anmeldung eines Benutzers die MAC-Adresse des Endgerätes an den RADIUS-Server. Dabei bleibt dem Public Spot verborgen, ob der Server die MAC-Adresse auch tatsächlich prüft oder nicht. Die korrekte Überprüfung der MAC-Adresse muss durch entsprechende Konfiguration des RADIUS-Servers gewährleistet sein.

2. Tragen Sie die Angaben zum RADIUS-Server ein.

   Bei der Konfiguration eines Public Spots können die Benutzer-Anmeldedaten an einen oder mehrere RADIUS-Server weitergeleitet werden. Diese Server konfigurieren Sie in LANconfig unter **Public-Spot** > **Benutzer** > **Benutzer und RADIUS-Server** > **RADIUS-Server**. Welche Anmeldedaten die einzelnen RADIUS-Server von den Benutzern benötigen, ist für das den Public Spot bereitstellende Gerät nicht wichtig, da dieses die Daten transparent an den RADIUS-Server weiterreicht.



   Die angegebenen IP-Adressen müssen statisch sein. Außerdem muss der Public Spot die angegebenen Ziel-Adressen erreichen können. Für IP-Adressen außerhalb des eigenen Netzwerkes ist es daher erforderlich, einen Router mit Kontakt zum Ziel-Netzwerk als Gateway in den DHCP-Einstellungen des Public Spots einzutragen. Dieses Gateway müssen Sie als Default-Route in die Routing-Tabelle eintragen.

   Zur Verbuchung der Verbindungsdaten durch den RADIUS-Server ist es erforderlich, die Angaben zum Accounting-Server vollständig einzutragen. Alternativ zur Verwendung eines RADIUS-Accounting-Servers können Sie sich die Verbindungsinformationen vom Public Spot auch per SYSLOG-Funktion ausgeben lassen.

3. Fertig!

   Damit ist Ihr Public Spot betriebsbereit. Alle Benutzer, die über ein gültiges Konto am RADIUS-Server verfügen, können sich über das Web-Interface am Public Spot anmelden.

1.4.5 Interner und externer RADIUS-Server kombiniert

Für die Authentifizierung von Benutzern mit IEEE 802.1X wird in manchen Unternehmen ein externer RADIUS-Server eingesetzt. In einer Anwendung mit einem WLAN Controller und mehreren Access Points fungiert zunächst der WLAN Controller als RADIUS-Server für alle Access Points. Im WLAN Controller definieren Sie dazu die entsprechende Weiterleitung der RADIUS-Anfragen an den externen RADIUS-Server.

Die im folgenden beschriebenen Einstellungen sind nur dann notwendig, wenn Sie in Ihrem Gerät neben dem Public Spot einen externen RADIUS-Server nutzen.

Im Zusammenhang mit einem Public Spot für Gast-Zugänge sind weitere Einstellungen notwendig:

- Die Authentifizierungsanfragen der internen Mitarbeiter sollen an den externen RADIUS-Server weitergeleitet werden.
- Die Authentifizierungsanfragen der Public Spot-Zugänge sollen vom internen RADIUS-Server geprüft werden.

Realm-Tagging für das RADIUS-Forwarding

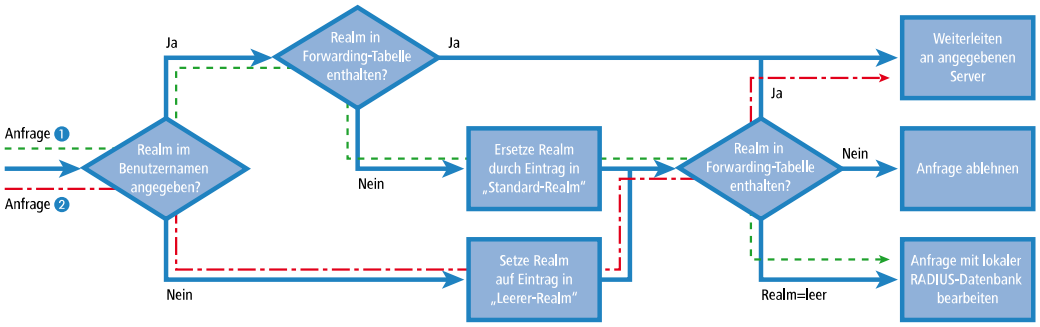
Die Authentifizierungsanfragen der beiden Benutzergruppen müssen separat behandelt werden. Damit der WLAN Controller diese beiden Gruppen unterscheiden kann, nutzt er sogenannte "Realms". Realms dienen der Adressierung von Domänen, innerhalb derer Benutzeraccounts gültig sind. Der WLAN Controller kann die Realms mit der Authentifizierungsanfrage an den internen RADIUS-Server übermitteln. Alternativ kann der RADIUS-Server nach folgenden Regeln die Realms der Benutzernamen verändern, um das RADIUS-Forwarding zu steuern:

- Der als "Standard-Realm" definierte Wert ersetzt einen vorhandenen Realm einer eingehenden Anfrage, wenn für diesen Realm keine Weiterleitung definiert ist.
- Der RADIUS-Server verwendet den unter "Leerer-Realm" definierten Wert **nur dann**, wenn der eingehende Benutzername **noch keinen** Realm enthält.

Über einen Eintrag in der Weiterleitungstabelle leitet der WLAN Controller alle Authentifizierungsanfragen mit einem bestimmten Realm an einen RADIUS-Server weiter. Wenn in der Weiterleitungstabelle kein passender Eintrag vorhanden ist, lehnt er die Anfrage ab.

Stellt der WLAN Controller nach der Ermittlung eines Realms einen leeren Realm fest, so prüft er die Authentifizierungsanfrage **immer** mit der internen RADIUS-Datenbank.

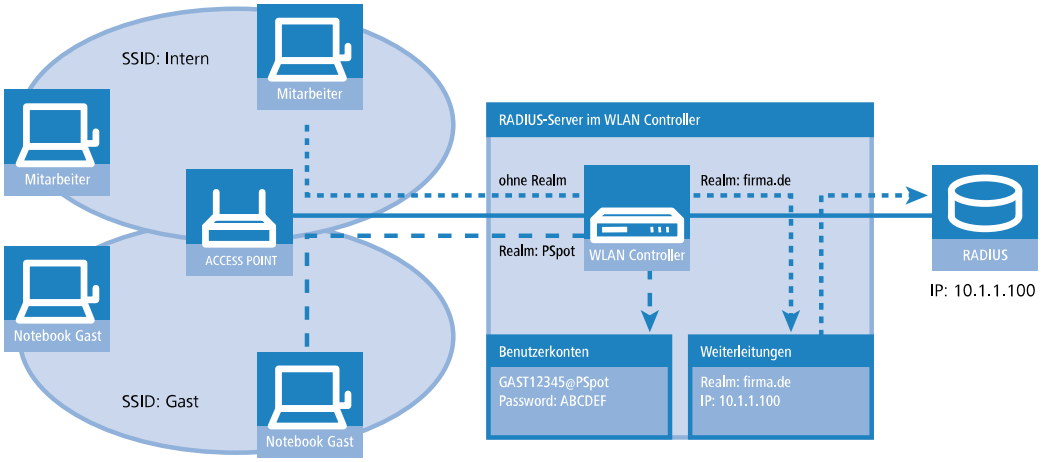
Das folgende Flussdiagramm zeigt schematisch die Arbeitsweise des RADIUS-Server bei der Verarbeitung von Realms:



Durch ein unterschiedliches Realm-Tagging können somit verschiedene RADIUS-Server angesprochen werden. Den Entscheidungsweg im RADIUS-Server des Gerätes können Sie im Diagramm für die beiden Anfragen verfolgen:

1. Da die Benutzernamen für die Gastzugänge automatisch erzeugt werden, wird für diese Benutzernamen der Realm "PSpot" verwendet. Da in der Weiterleitungstabelle kein entsprechender Eintrag vorhanden ist und der Standard-Realm leer ist, leitet der WLAN Controller alle Authentifizierungsanfragen mit diesem Realm an den internen RADIUS-Server weiter.
2. Um den Konfigurationsaufwand zu begrenzen, werden die internen Benutzer weiterhin ohne Realm geführt. Der RADIUS-Server im Gerät kann einen leeren Realm automatisch durch einen anderen Realm ersetzen, mit dem er die internen Benutzer identifiziert. In diesem Beispiel ersetzt er den leeren Realm durch die Domäne der Firma "firma.de".

Mit den Angaben in der Weiterleitungstabelle können alle Authentifizierungsanfragen mit diesem Realm an den externen RADIUS-Server weitergeleitet werden.

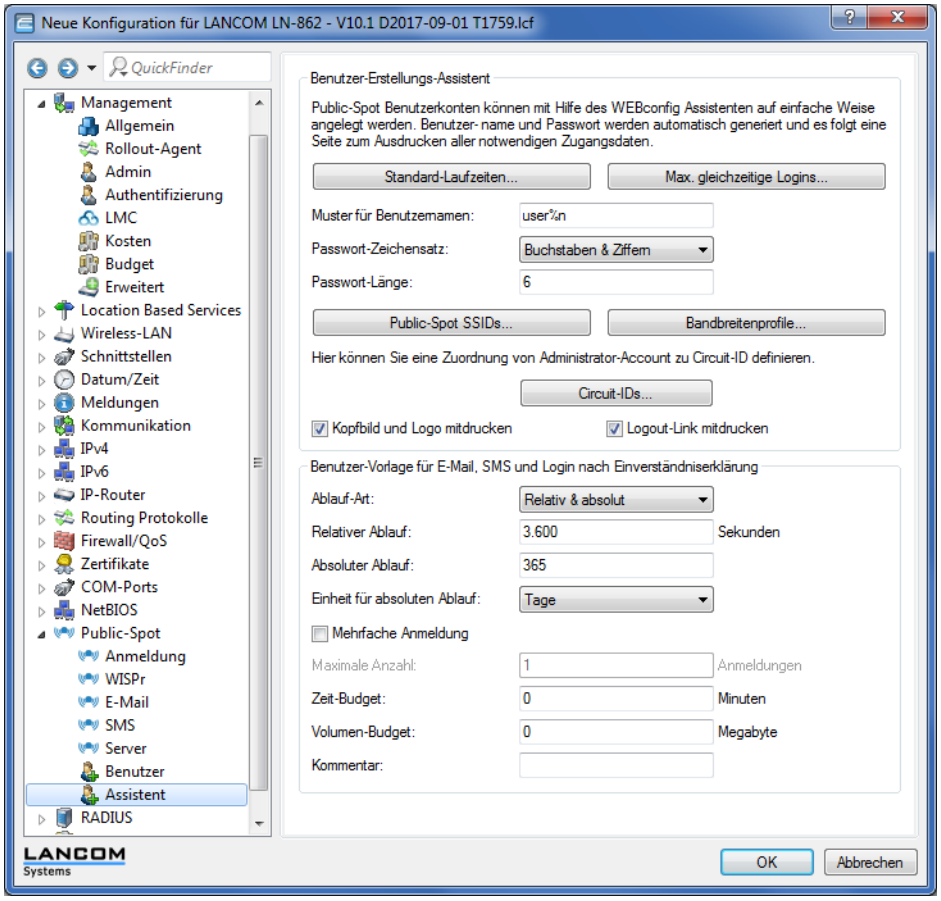


Konfiguration für das RADIUS-Forwarding

Mit den folgenden Konfigurationsschritten können Sie die separate Behandlung der internen Benutzer und der Gastzugänge definieren.

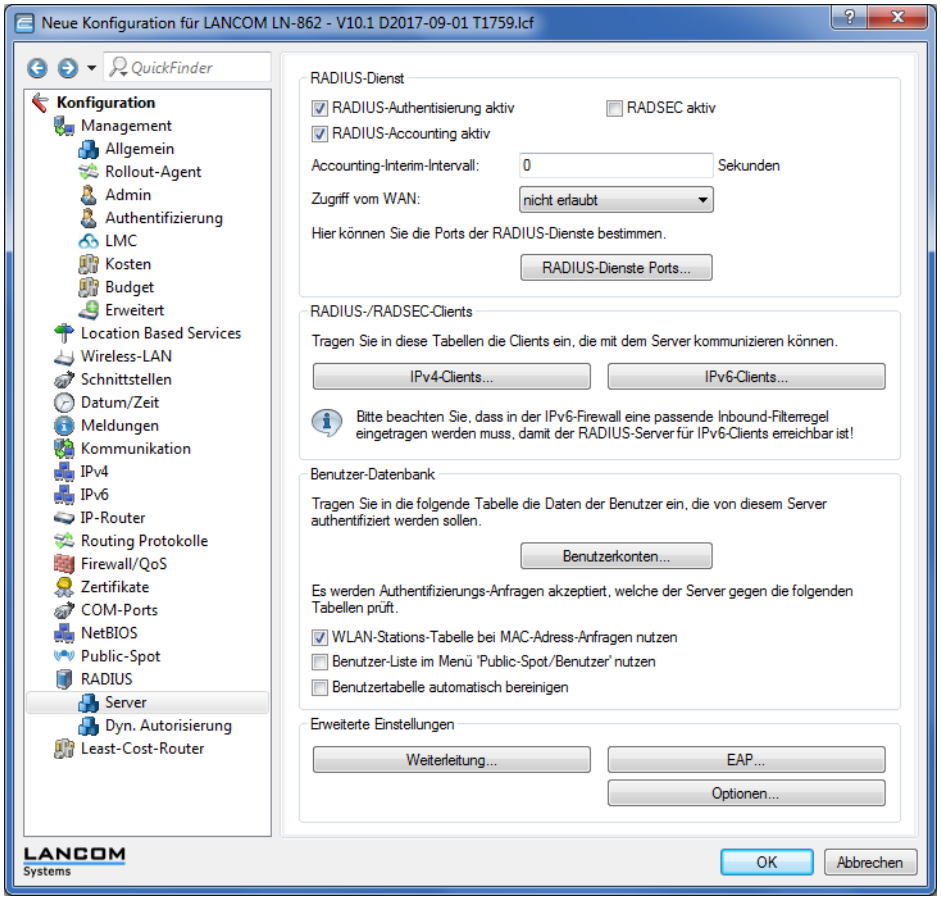
1. Passen Sie im Public Spot das Muster für die Benutzernamen so an, dass ein eindeutiger Realm verwendet wird. Mit dem Muster "user%n@PSpot" generiert der Public-Spot z. B. Benutzernamen der Form "user12345@PSpot".

   › **LANconfig: Public-Spot** > **Assistent** > **Benutzer-Erstellungs-Assistent**



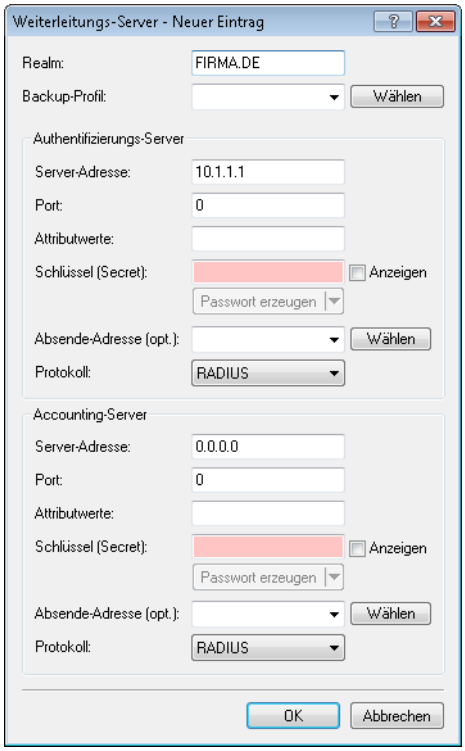
2. Tragen Sie im RADIUS-Server des WLAN Controllers einen "leeren Realm" ein (z. B. "FIRMA.DE").
   Dieser Realm wird für alle Benutzernamen verwendet, die ohne Realm eine Authentifizierungsanfrage bei dem WLAN Controller stellen. Das sind in dieser Anwendung die internen Benutzer, für die kein Realm definiert ist. Damit der RADIUS-Server des WLAN Controllers für diese Benutzernamen auch keinen Realm einsetzt, müssen Sie den "Standard-Realm" unbedingt leer lassen.

   › **LANconfig: RADIUS > Server > Erweiterte Einstellungen > Weiterleitung > RADIUS-Weiterleitungs-Server > Weiterleitungs-Server**



3. Damit der WLAN Controller die Authentifizierungsanfragen der internen Benutzer an den externen RADIUS-Server weiterleiten kann, legen Sie einen passenden Eintrag bei den Weiterleitungen an.

Mit dem Realm "FIRMA.DE" werden alle eingehenden RADIUS-Anfragen an die angegebene IP-Adresse weitergeleitet, die über diesen Realm verfügen.



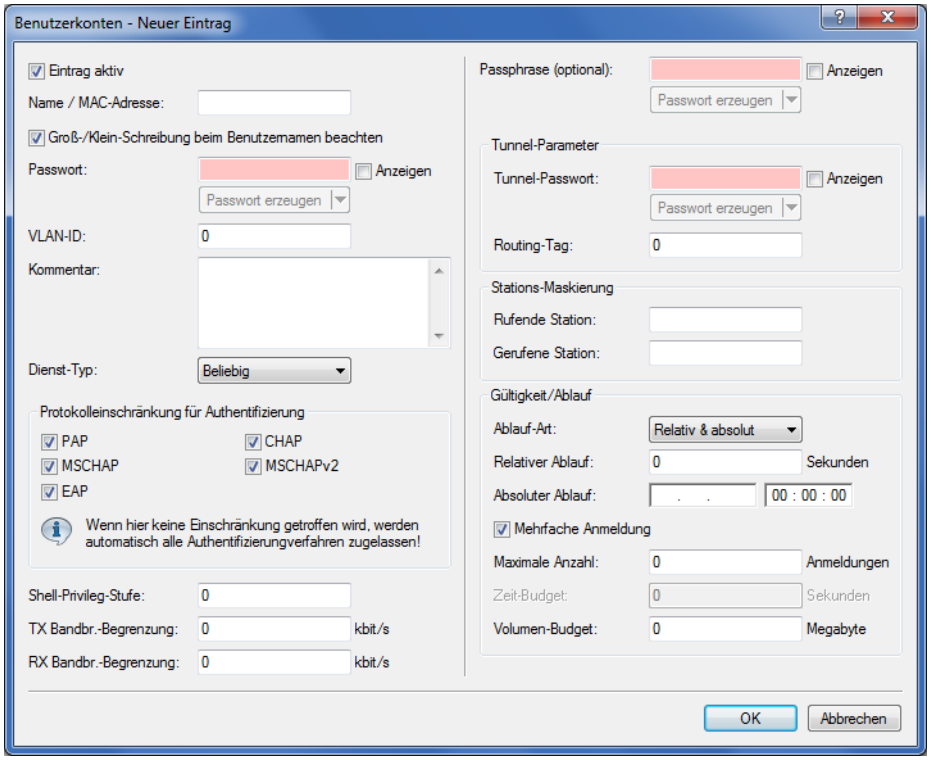
4. Die Authentifizierungsanfragen der Public Spot-Benutzer gehen mit dem Realm "@PSpot" beim WLAN Controller ein. Da für diesen Realm keine Weiterleitung definiert ist, werden die Benutzernamen automatisch in der internen RADIUS-Datenbank geprüft. Da die über den Assistenten angelegten Public Spot-Zugänge in dieser Datenbank gespeichert werden, können diese Anfragen wie gewünscht authentifiziert werden.

1.4.6 Prüfung von WLAN-Clients über RADIUS (MAC-Filter)

Bei der Nutzung von RADIUS zur Authentifizierung von WLAN-Clients können Sie neben einem externen RADIUS-Server auch die interne RADIUS-Benutzerdatenbank eines WLAN Controllers nutzen, um nur bestimmten WLAN-Clients anhand ihrer MAC-Adresse den Zugang zum WLAN zu erlauben.

Tragen Sie die zugelassenen MAC-Adressen über LANconfig in die RADIUS-Datenbank ein und aktivieren Sie alle Authentifizierungsmethoden. Wählen Sie als **Name / MAC-Adresse** und **Passwort** jeweils die MAC-Adresse in der Schreibweise 'AABBCC-DDEEFF'.

› LANconfig: **RADIUS** > **Server** > **Benutzer-Datenbank** > **Benutzerkonten**



1.4.7 Einrichtung eines externen SYSLOG-Servers

Je nach Anwendungsfall, ist für den Betrieb eines Public Spots das Speichern der Nutzungsdaten erforderlich. Diese Daten lassen sich z. B. in einem SYSLOG-Server speichern. SYSLOG-Server sind teilweise als freie Software verfügbar.

Zum Speichern der Nutzungsdaten aus einem Public Spot über SYSLOG wird der externe SYSLOG-Server in dem jeweiligen Public Spot konfiguriert. Daraufhin wird das Anlegen bzw. Löschen von Public Spot-Benutzern sowie der Anfang und das Ende von Public Spot-Sitzungen mit einer Nachricht an den SYSLOG-Server protokolliert. Beim Ende der Sitzung wird in dieser Nachricht – mit der Quelle "Login" und der Priorität "Information" – neben dem übertragenen Datenvolumen auch die verwendete IP-Adresse gemeldet.

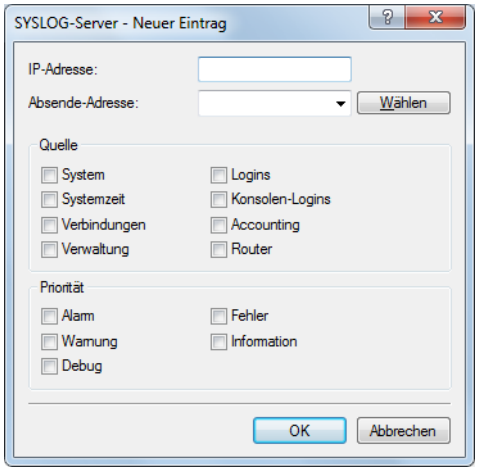
Weitere Informationen über die Konfiguration von SYSLOG entnehmen Sie bitte dem Kapitel *Das SYSLOG-Modul*. Informationen über die rechtlichen Regelungen finden Sie im LANCOM Techpaper "Public Spot", erhältlich unter *www.lancom-systems.de*.

Externen SYSLOG-Server konfigurieren

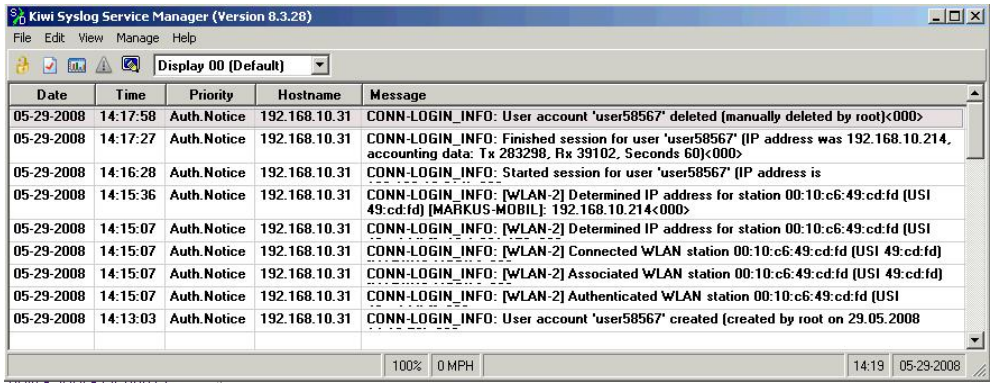
Ihr Gerät ist dazu in der Lage, das Anlegen und Löschen von neuen Public Spot-Benutzern sowie deren An- und Abmeldevorgänge zu protokollieren. Diese intern gespeicherten Informationen können Sie aber auch an einen externen SYSLOG-Server weiterleiten. Die nachfolgenden Schritte zeigen Ihnen, wie Sie die Protokollierung mit einem auf einem externen SYSLOG-Server installierten Programm vornehmen (in diesem Beispiel "Kiwi").

1. Starten Sie LANconfig und öffnen Sie den Konfigurationsdialog Ihres Gerätes.
2. Wechseln Sie in den Dialog **Meldungen** > **Allgemein** und öffnen Sie die Tabelle **SYSLOG-Server**.

3. Fügen Sie einen neuen Eintrag hinzu. Definieren Sie dazu die **IP-Adresse** des Rechners, auf dem der SYSLOG-Client installiert ist (z. B. `192.168.10.237`), und geben Sie die **Quelle** (`Logins`, `Accounting`) sowie die **Priorität** (`Information`) an.



4. Schließen Sie die Dialoge und schreiben Sie die Konfiguration zurück auf Ihr Gerät.
5. Starten Sie das Auswertungsprogramm auf Ihrem SYSLOG Server (z. B. "Kiwi"). Sobald das Programm gestartet ist, zeichnet es das Anlegen und Löschen von neuen Public Spot-Benutzern sowie die An- und Abmeldungen von Public Spot-Benutzers auf.



1.5 XML-Interface

Um eine Vielzahl von Public Spot-Szenarios abdecken zu können, ist die Standard-Authentifizierungsmethode des Public Spots alleine über Name und Passwort nicht ausreichend. Zugriffs- und Abrechnungsmodelle über Social Media, Kreditkarten und weitere Methoden erfordern oft zusätzliche Zugriffsdaten, die der Public Spot in dieser Form nicht verwalten kann.

Die implementierte XML-Schnittstelle verbindet den Public Spot und ein externes Gateway. Sie leitet dabei die Daten des Benutzers nur an das Gateway weiter, das anschließend die Authentifizierung und Abrechnung übernimmt und dem Public Spot nur Informationen über Dauer und Limitierungen des Benutzerzugangs mitteilt.

Der Public Spot übernimmt also dabei nur die folgenden Aufgaben:

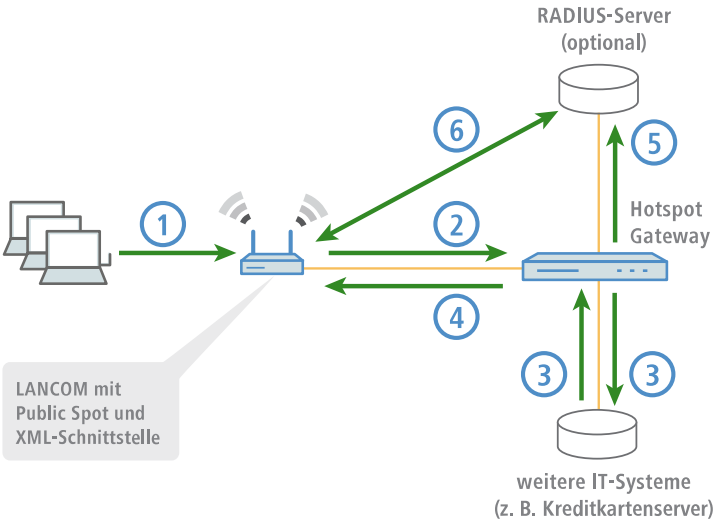
- Weiterleiten der Benutzeranfragen
- Einschränken von unerlaubten Zugangsversuchen
- Annahme der Gateway-Kommandos zum Starten und Beenden einer Sitzung

› ggf. Abrechnen der Sitzungen

Da es nicht sinnvoll ist, alle vorhandenen, teilweise sehr speziellen Szenarios mit den zugehörigen Gateway-Befehlen im Public Spot zu implementieren, ist die XML-Schnittstelle universal und flexibel aufgebaut.

1.5.1 Funktion

Die Kommunikation zwischen XML-Interface und externem Gateway läuft ab wie folgt:



1. Der Benutzer verbindet sich mit dem WLAN auf dem Public Spot und sendet eine HTTP-Anfrage an den Public Spot.
2. Der Public Spot leitet die HTTP-Anfrage für den Login-Vorgang weiter an das externe Hotspot-Gateway. Dazu befindet sich das externe Hotspot-Gateway entweder in einem frei zugänglichen Netz des Public Spots oder seine Adresse gehört zur Liste der freien Hosts.

   Das externe Gateway erhält die MAC-Adresse des anfragenden Public Spot-Clients dabei in der Weiterleitung durch den Public Spot. Unter **Public-Spot-Modul** > **Seitentabelle** wählen Sie dazu bei der entsprechenden Seite den **Typ** "Redirect" aus und ergänzen die **URL** um den Parameter `?myvar=%m`.

   Beispiel: `http://192.168.1.1/?myvar=%m`

   Hierbei ist `myvar` eine beliebig wählbare Variable. Entscheidend ist die Variable `%m`, die der Public Spot beim Weiterleiten der Anfrage durch die MAC-Adresse des Public Spot-Clients ersetzt.

Tabelle 9: Variblen

Variable	Bedeutung
%s	SSID-Name
%v	Quell-VLAN
%i	Interface (gilt für LAN, WLAN, WLC-Tunnel)
%t	Routing-Tag
%m	MAC-Adresse des Clients
%c	MAC-Adresse des Public Spot Gateways
%r	Remote-IP (Client)
%p	lokale IP (Public Spot Gateway)
%o	original durch den Client aufgerufene URL
%n	Gerätename des Public Spot Gateways

Variable	Bedeutung
%e	Seriennummer des Public Spot Gateways
%l	Hostname des Public Spot Gateways
%0-9	Fügt eine einzelne Zahl im Bereich von 0 bis 9 ein
%%	Fügt ein einzelnes Prozentzeichen ein

3. Das Hotspot-Gateway prüft die Anmeldedaten des Benutzers und kontaktiert ggf. weitere IT-Systeme zur Kreditkartenabrechnung o. ä.
4. Das Hotspot-Gateway sendet eine XML-Datei mit den Benutzerdaten an die XML-Schnittstelle des Public Spots. Das externe Hotspot-Gateway kontaktiert das Gerät mit Public Spot-XML-Schnittstelle über die URL `http://<Geräte-URL>/xmlauth`.

   Die XML-Schnittstelle im Public Spot analysiert diese Datei und veranlasst die entsprechenden Aktionen. Bei einer Login-Anfrage übernimmt die XML-Schnittstelle den Benutzer mit seiner MAC-Adresse in die Liste der angemeldeten Public Spot-Benutzer. Bei einer Logout-Anfrage entfernt die XML-Schnittstelle den Benutzer wieder aus dieser Liste. Gleichzeitig bestätigt die XML-Schnittstelle die jeweilige Anfrage, indem sie eine entsprechende XML-Datei an das Hotspot-Gateway sendet.

   Damit der Public Spot die Anweisungen der XML-Datei verarbeiten kann, muss im Gerät ein spezieller Administrator eingerichtet sein, der das Funktionsrecht "Public Spot-XML-Schnittstelle" besitzt. Über dieses Admin-Konto meldet sich das Hotspot-Gateway am Public Spot an.

   Während der Benutzer am Public Spot angemeldet ist, können XML-Schnittstelle und Hotspot-Gateway Statusinformationen in Form von XML-Dateien über die aktuelle Session austauschen.

   Hat der Benutzer sein Online-Kontingent ausgeschöpft, sendet das Hotspot-Gateway einen Stop-Befehl an die XML-Schnittstelle, woraufhin der Public Spot dem Benutzer den weiteren Zugang sperrt. Auch die Sperrung des Zugangs bestätigt das XML-Interface wieder mit einer entsprechenden XML-Datei an das Hotspot-Gateway.
5. Sofern die zusätzliche Nutzung eines RADIUS-Servers aktiviert ist, meldet das Hotspot-Gateway einen Benutzer an einem RADIUS-Server an.
6. Der Public Spot übermittelt während der Sitzung die relevanten Daten an den RADIUS-Server, z. B. für eine spätere Abrechnung der Public Spot-Nutzung (Accounting). Standardmäßig verwendet der Public Spot dazu seinen internen RADIUS-Server. Bei Bedarf konfigurieren Sie auf dem Gerät mit Public Spot die Nutzung eines externen RADIUS-Servers.

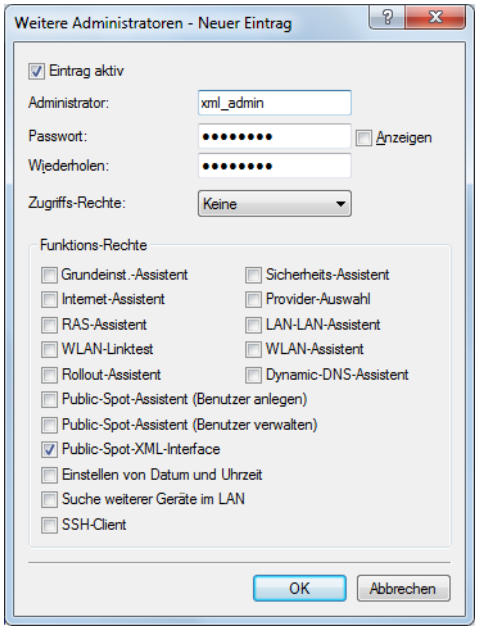
Die Kommunikation zwischen dem Public Spot und einem Hotspot-Gateway über XML ist nicht genormt. Konfigurieren Sie das Hotspot-Gateway entsprechend den Vorgaben im Abschnitt *Befehle*, so dass Public Spot und Hotspot-Gateway die verwendeten XML-Nachrichten in der erforderlichen Form austauschen. Der Austausch der XML-Nachrichten läuft unsichtbar ohne grafische Oberfläche ab. Testen Sie diesen Nachrichtenaustausch z. B. über Tools wie *cURL*.

1.5.2 Einrichtung des XML-Interfaces

Der folgende Abschnitt beschreibt die Einrichtung des XML-Interfaces.

1. Erstellen Sie unter **Management** > **Admin** > **Weitere Administratoren** einen neuen Administrator mit dem Funktionsrecht **Public-Spot-XML-Schnittstelle**.

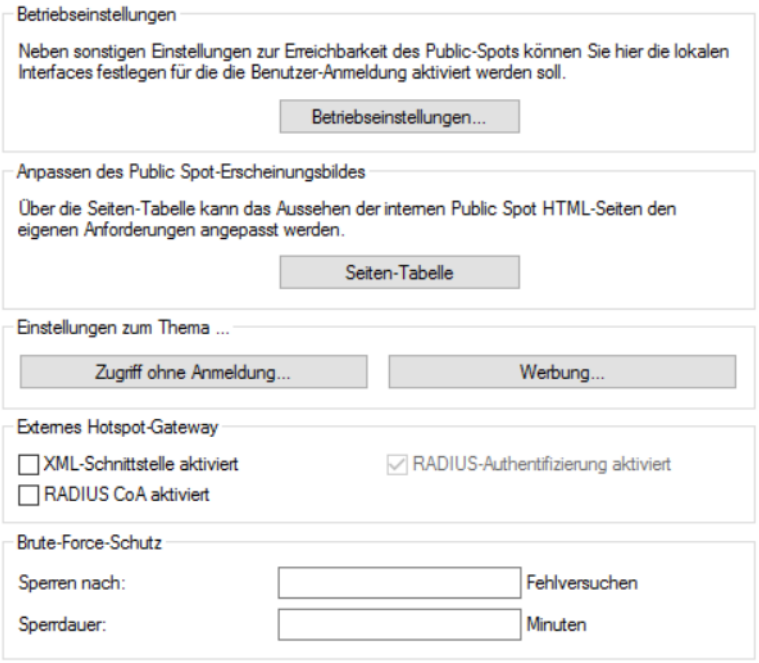
Über dieses Administrator-Konto sendet das (externe) Gateway später seine XML-Anfragen an die XML-Schnittstelle des Public Spots.



Der angelegte Administrator sollte über keine weiteren Public Spot-Funktionsrechte verfügen, da sie das Konto mit bestimmten Konfigurationsrechten ausstatten und dies in Kombination mit dem XML-Interface ein potentielles Sicherheitsrisiko darstellt (z. B. wenn die Kommunikation zwischen XML-Sender und Gerät unverschlüsselt erfolgt).

2. Aktivieren Sie unter **Public-Spot** > **Server** im Abschnitt **Externes Hotspot-Gateway** die XML-Schnittstelle und die RADIUS-Authentifizierung.

   Ankommende XML-Anfragen übergibt das Public Spot-Modul entweder an den internen RADIUS-Server oder – bei Nutzung eines externen RADIUS-Servers über einen Realm – an den externen RADIUS-Server.



3. Klicken Sie im Rahmen **Zugriff ohne Anmeldung ermöglichen** auf die Schaltfläche **Freie Netze** und fügen Sie ein neues Netz hinzu. Für **Name/IP-Adresse** geben Sie den Host-Namen bzw. die IP-Adresse der Anmeldeseite des Gateways ein, dessen Dienste die Public Spot-Benutzer nutzen dürfen. Als **Netzmaske** geben Sie `255.255.255.255` ein.

   Durch die Speicherung als freies Netz können die Benutzer ohne Anmeldung am Public Spot direkt auf die Anmeldeseite des Gateways zugreifen.

4. Konfigurieren Sie das Gateway so, dass es die Sitzungsdaten des Benutzers als XML-Datei an die XML-Schnittstelle des Public Spots sendet.
   Bei Fragen zur Konfiguration des Gateways wenden Sie sich an den zuständigen Service-Provider.

1.5.3 Analyse des XML-Interfaces mit cURL

Der folgende Abschnitt beschreibt die Analyse des XML-Interfaces mit der Open-Source-Software cURL.

cURL (Client for URL) ist eine Kommandozeilen-Anwendung, mit der man Dateien ohne den Einsatz von Web-Browsern oder FTP-Clients in einem Netzwerk übertragen kann. cURL ist Bestandteil von vielen Linux-Distributionen und steht auch für weitere Betriebssysteme zur Verfügung.

Um das XML-Interface mit cURL analysieren zu können, benötigen Sie im Public Spot einen Administrator mit dem Funktionsrecht "Public Spot-XML-Schnittstelle".

1. Laden Sie zunächst cURL herunter und installieren bzw. entpacken Sie es.
2. Starten Sie cURL mit der Befehlszeile `curl -X POST -H "Content-Type:text/xml" -d @filename http://user:pass@myhost/xmlauth/`.

   Die Parameter haben folgende Bedeutung:

   filename

   Pfad und Name der lokalen XML-Datei, z. B. der Login-Request aus den *Beispielen*.

   user

   Benutzername mit Funktionsrecht "Public Spot-XML-Schnittstelle". Ohne diese Authentifizierung funktioniert das XML-Feature nicht.

   pass

   Passwort des Benutzers

   myhost

   IP-Adresse bzw. DNS-Name des Gerätes mit Public Spot-XML-Schnittstelle

3. Über Telnet können Sie mit dem Befehl `trace # XML-Interface-PbSpot` einen Trace aktivieren, um zu überprüfen, ob XML-Anfragen erfolgreich waren bzw. Fehlermeldungen erhalten.

1.5.4 Befehle

Das XML-Interface kann je drei Arten von Anfragen und Antworten verarbeiten:

- Login
- Logout
- Status

Dabei kann eine XML-Datei auch mehrere Anfragen bzw. Antworten enthalten.

Login

Sendet das externe Gateway in einer XML-Datei einen "Login"-Request, schaltet der Public Spot den Online-Zugriff für den entsprechenden Benutzer frei. Ein "Login"-Request enthält das Attribut `COMMAND="RADIUS_LOGIN"`.

Verwendet der Public Spot keinen RADIUS-Server, speichert er bei einem "Login"-Request den Benutzer inkl. seiner MAC-Adresse direkt in der internen Statustabelle. Dadurch kann er den Benutzer zukünftig sofort authentifizieren und muss ihm nicht erst eine Login-Seite anzeigen, auf der er Benutzername und Passwort eingeben muss.

Bei Verwendung eines RADIUS-Servers ist eine erfolgreiche Ausführung des "Login"-Request nur dann möglich, wenn die Anmeldedaten des entsprechende Benutzers schon im RADIUS-Server vorliegen.

Über das Web-API des Public Spots können Sie komfortabel neue Public Spot-Benutzer im internen RADIUS-Server des Gerätes anlegen.

Das XML-Interface kann die folgenden XML-Elemente im **Login-Request** verarbeiten:

`SUB_USER_NAME`

Benutzername

`SUB_PASSWORD`

Benutzerpasswort

`SUB_MAC_ADDR`

MAC-Adresse des Benutzer-Gerätes. Mögliche Formate sind:

- 00164115208c
- 00:16:41:15:20:8c
- 00-16-41-15-20-8c

`VLAN_ID` (optional)

Individuelle VLAN-ID, die das Gerät dem Public Spot-Benutzer beim Login zuweist. Die individuelle VLAN-ID überschreibt nach der Authentifizierung durch den RADIUS-Server eine globale VLAN-ID, die ein Nutzer ansonsten über das XML-Interface erhalten würde.

Der Wert `0` deaktiviert die Verwendung eines VLANs.

`SOURCE_VLAN` (optional, nur in Verbindung mit der Authentifizierung über einen RADIUS-Server)

Die VLAN-ID des Netzes, aus dem sich ein Public Spot-Benutzer anzumelden versucht (Quell-VLAN). Der Public Spot leitet die Quell-VLAN in seinem Access-Request an den internen oder einen externen RADIUS-Server weiter. Dazu verwendet der Public Spot das RADIUS-Attribut 81 (**Tunnel-Private-Group-Id**) im Zusammenspiel mit den RADIUS-Attributen 64 (**Tunnel-Type**) und 65 (**Tunnel-Medium-Type**). Der RADIUS-Server kann auf Basis der Quell-VLAN dann z. B. entscheiden, ob er den Access-Request des Public Spots akzeptiert oder ablehnt.

Hat der RADIUS-Server die Anfrage akzeptiert, überträgt er in seinem Access-Accept die o. g. RADIUS-Attribute zurück an den Public Spot. Anschließend hinterlegt der Public Spot das Quell-VLAN für den jeweiligen Client und dessen Stationsliste und gibt dem Benutzer den Zugriff auf das Public Spot-Netz frei.

Nutzen Sie Quell-VLAN in Verbindung mit dem Setup-Parameter *2.24.47*. Dadurch verhindern Sie, dass sich ein Public Spot-Benutzer in VLAN-getrennten Public Spot-Netzen/SSIDs nach einmaliger Authentisierung durch den RADIUS-Server an sämtlichen verwalteten Public Spot-Netzen/SSIDs anmelden kann.

Die SOURCE_VLAN ist nicht mit der VLAN_ID zu verwechseln. Die VLAN_ID wird nicht an den RADIUS-Server übermittelt, sondern vom Public Spot dazu genutzt, einem Benutzer nach erfolgreicher Authentifizierung eine vom Gateway vorgegebene VLAN-ID zuzuweisen.

PROVIDER (teilweise erforderlich)

Name des RADIUS-Servers, den der Public Spot für den Benutzer verwendet (Authentifizierung und Accounting). Wenn Sie keinen RADIUS-Server angeben, verwendet der Public Spot den für das Modul global konfigurierten Server.

Dieses XML-Element ist zwingend erforderlich, wenn Sie

- für das Public Spot-Modul mehrere RADIUS-Server konfiguriert haben.
- die XML-Schnittstelle ohne RADIUS-Authentifizierung, aber mit RADIUS-Accounting verwenden wollen.

In den übrigen Fällen ist die Angabe dieses XML-Elements optional.

Der referenzierte RADIUS-Server muss in der Konfiguration vorhanden sein.

TXRATELIMIT (optional)

Maximale Bandbreite (in KBit/s), die dem Public Spot-Benutzer im Uplink zur Verfügung steht.

RXRATELIMIT (optional)

Maximale Bandbreite (in KBit/s), die dem Public Spot-Benutzer im Downlink zur Verfügung steht.

SECONDSEXPIRE (optional)

Nutzungsdauer (die maximale Online-Zeit) für einen Benutzer-Account in Sekunden. Diese Nutzungsdauer kann der Benutzer bis zum Erreichen einer ggf. definierten relativen oder absoluten Ablaufzeit ausschöpfen.

Der Wert 0 schaltet die Überwachung der Nutzungsdauer aus.

TRAFFICEXPIRE (optional)

Maximales Datenvolumen für einen Benutzer-Account. Dieses Datenvolumen kann der Benutzer bis zum Erreichen einer ggf. definierten relativen oder absoluten Ablaufzeit ausschöpfen.

Die folgenden Angaben sind möglich:

- k oder K: Angabe in Kilobytes (kB), z. B. <TRAFFICEXPIRE>1000k</TRAFFICEXPIRE>.
- m oder M: Angabe in Megabytes (MB), z. B. <TRAFFICEXPIRE>100m</TRAFFICEXPIRE>.
- g oder G: Angabe in Gigabytes (GB), z. B. <TRAFFICEXPIRE>1g</TRAFFICEXPIRE>.

Ohne Einheit entspricht die Angabe einem Wert in Byte (B).

Der Wert 0 schaltet die Überwachung des Datenvolumens aus.

Das XML-Interface sendet dem Gateway daraufhin eine "Login"-Response, die die folgenden XML-Elemente enthalten kann:

SUB_USER_NAME

Benutzername

SUB_STATUS

Der aktuelle Benutzerstatus. Folgende Werte sind möglich:

- `RADIUS_LOGIN_ACCEPT`: Login erfolgreich
- `RADIUS_LOGIN_REJECT`: Login wird zurückgewiesen

`SUB_MAC_ADDR`

MAC-Adresse des Benutzer-Gerätes. Mögliche Formate sind:

- 00164115208c
- 00:16:41:15:20:8c
- 00-16-41-15-20-8c

`PROVIDER`

Name des RADIUS-Servers der für diesen Benutzer verwendet werden soll.

Im Folgenden finden Sie einige Beispiele für XML-Dateien:

Login-Request

Das externe Gateway sendet die Daten für den Start einer Sitzung an den Public Spot:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<PUBLICSPOTXMLINTERFACE>
  <ACCESS_CUBE COMMAND="RADIUS_LOGIN">
    <SUB_USER_NAME>user2350</SUB_USER_NAME>
    <SUB_PASSWORD>5juchb</SUB_PASSWORD>
    <SUB_MAC_ADDR>00164115208c</SUB_MAC_ADDR>
    <PROVIDER>DEFAULT</PROVIDER>
  </ACCESS_CUBE>
</PUBLICSPOTXMLINTERFACE>
```

Der Public Spot aktiviert den Benutzer 'user2350' in der internen Status-Tabelle.

Login-Response:

Das XML-Interface sendet eine Bestätigung über den Start einer Sitzung an das externe Gateway:

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
<PUBLICSPOTXMLINTERFACE>
 <ACCESS_CUBE ID="WLC_PM" IP="192.168.100.2" COMMAND="USER_STATUS">
    <SUB_STATUS>RADIUS_LOGIN_ACCEPT</SUB_STATUS>
    <SUB_MAC_ADDR>00:16:41:15:20:8b</SUB_MAC_ADDR>
    <SUB_USER_NAME>user2350</SUB_USER_NAME>
    <TXRATELIMIT>0</TXRATELIMIT>
    <RXRATELIMIT>0</RXRATELIMIT>
    <SECONDSEXPIRE>0</SECONDSEXPIRE>
    <TRAFFICEXPIRE>0</TRAFFICEXPIRE>
    <ACCOUNTCYCLE>0</ACCOUNTCYCLE>
    <IDLETIMEOUT>0</IDLETIMEOUT>
    </ACCESS_CUBE>
</PUBLICSPOTXMLINTERFACE>
```

CoA

Für die Anmeldung eines Public Spot-Benutzers ohne Änderungen während des Anmeldezeitraums genügt der Parameter `RADIUS_LOGIN`. Mittels `RADIUS_CoA` hingegen haben Sie die Möglichkeit, die für einen Public Spot-Benutzer geltenden Rahmenbedingungen auch während einer laufenden Sitzung zu verändern. Dazu sendet Ihr externes Hotspot-Gateway einen `RADIUS-CoA-Request` an den Public Spot, welcher die darin enthaltenen Änderungen direkt auf die **Stations-Tabelle** unter **Status** > **Public-Spot** überträgt.

Ein möglicher Anwendungsfall für CoA-Nachrichten ist z. B. die automatische Drosselung der Bandbreite: Hat ein Public Spot-Benutzer sein Volumenbudget verbraucht, kann ein externe Hotspot-Gateway diesen Benutzer drosseln, indem das Hotspot-Gateway nach Auswerten der Accounting-Daten eine entsprechende CoA-Nachricht an den Public Spot schickt

Die XML-Nachrichten für die Verhandlung zwischen Hotspot-Gateway und Public Spot sehen wie folgt aus:

RADIUS-CoA-Request

Das externe Gateway sendet die Daten für die Änderung einer Sitzung an den Public Spot. Der Public Spot ändert daraufhin die Sitzungsdaten des angemeldeten Benutzers 'user2350' in der Stations-Tabelle:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<PUBLICSPOTXMLINTERFACE>
  <ACCESS_CUBE COMMAND="RADIUS_COA_REQUEST">
    <SUB_USER_NAME>user2350</SUB_USER_NAME>
    <SUB_PASSWORD>5juchb</SUB_PASSWORD>
    <SUB_MAC_ADDR>00164115208c</SUB_MAC_ADDR>
    <TXRATELIMIT>100</TXRATELIMIT>
    <RXRATELIMIT>100</RXRATELIMIT>
    <SECONDSEXPIRE>3600</SECONDSEXPIRE>
    <TRAFFICEXPIRE>10000000</TRAFFICEXPIRE>
  </ACCESS_CUBE>
</PUBLICSPOTXMLINTERFACE>
```

Im obigen Beispiel werden dem Benutzer eine Sitzungsdauer von 3.600 Sekunden sowie ein übertragbares Datenvolumen von 10.000.000 Byte bei einer Sende- und Empfangsbandbreite von 100 kBit/s zugewiesen.

RADIUS-CoA-Response:

Das XML-Interface sendet eine Bestätigung über die Änderung der Sitzungsdaten an das externe Hotspot-Gateway:

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
<PUBLICSPOTXMLINTERFACE>
 <ACCESS_CUBE ID="WLC_PM" IP="192.168.100.2" COMMAND="USER_STATUS">
    <SUB_STATUS>RADIUS_COA_ACCEPT</SUB_STATUS>
    <SUB_MAC_ADDR>00:16:41:15:20:8b</SUB_MAC_ADDR>
    <SUB_USER_NAME>user2350</SUB_USER_NAME>
    <TXRATELIMIT>100</TXRATELIMIT>
    <RXRATELIMIT>100</RXRATELIMIT>
    <SECONDSEXPIRE>3600</SECONDSEXPIRE>
    <TRAFFICEXPIRE>10000000</TRAFFICEXPIRE>
    <ACCOUNTCYCLE>0</ACCOUNTCYCLE>
    <IDLETIMEOUT>0</IDLETIMEOUT>
    </ACCESS_CUBE>
</PUBLICSPOTXMLINTERFACE>
```

Im Falle des Drosselungsbeispiels betrifft die Änderung der Benutzersitzung immer das Kontingent, das dem Benutzer ab Änderungszeitpunkt noch zusteht. War der Benutzer z. B. bereits eine Stunde angemeldet, stehen ihm nach der Änderung des Zeitkontingents auf sechs Stunden anschließend noch fünf Stunden zur Verfügung. Fällt das zugewiesene Zeitkontingent dagegen geringer aus als der Benutzer bereits angemeldet ist, loggt der Public Spot den betreffenden Nutzer aus und sendet eine Logout-Nachricht an das Hotspot-Gateway.

Logout

Sendet das externe Gateway in einer XML-Datei einen "Logout"-Request, sperrt der Public Spot den Online-Zugriff für den entsprechenden Benutzer. Ein "Logout"-Request enthält das Attribut `COMMAND="RADIUS_LOGOUT"`.

Das XML-Interface kann die folgenden XML-Elemente einer Anfrage verarbeiten:

`SUB_USER_NAME`

Benutzername

Bekommt das Gerät diesen Request und stellt das Public Spot-Modul fest, dass dieser User mit den passenden MAC online ist, loggt der Public Spot diesen aus.

`SUB_MAC_ADDR`

MAC-Adresse des Benutzer-Gerätes. Mögliche Formate sind:

- 00164115208c
- 00:16:41:15:20:8c

- 00-16-41-15-20-8c

TERMINATION_CAUSE

Grund für das Abmelden des Benutzers

Das XML-Interface sendet dem Gateway daraufhin eine "Logout"-Response, die die folgenden XML-Elemente enthalten kann:

SUB_USER_NAME

Benutzername

SUB_STATUS

Der aktuelle Benutzerstatus. Folgende Werte sind möglich:

- `RADIUS_LOGOUT_DONE`: Logout erfolgreich
- `RADIUS_LOGOUT_REJECT`: Logout wird zurückgewiesen

SUB_MAC_ADDR

MAC-Adresse des Benutzer-Gerätes. Mögliche Formate sind:

- 00164115208c
- 00:16:41:15:20:8c
- 00-16-41-15-20-8c

TERMINATION_CAUSE

Grund für die Sperrung des Zugangs

Im Folgenden finden Sie einige Beispiele für XML-Dateien:

Logout-Request

Das externe Gateway sendet den Befehl für die Beendigung einer Sitzung an den Public Spot:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<PUBLICSPOTXMLINTERFACE>
  <ACCESS_CUBE COMMAND="RADIUS_LOGOUT">
    <SUB_USER_NAME>user2350</SUB_USER_NAME>
    <SUB_MAC_ADDR>00164115208c</SUB_MAC_ADDR>
    <TERMINATION_CAUSE>Check-Out</TERMINATION_CAUSE>
  </ACCESS_CUBE>
</PUBLICSPOTXMLINTERFACE>
```

Logout-Response:

Das XML-Interface sendet eine Bestätigung über den Stopp einer Sitzung an das externe Gateway:

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
<PUBLICSPOTXMLINTERFACE>
   <ACCESS_CUBE ID="WLC_PM" IP="192.168.100.2" COMMAND="USER_STATUS">
     <SUB_STATUS>RADIUS_LOGOUT_DONE</SUB_STATUS>
     <SUB_MAC_ADDR>00:16:41:15:20:8b</SUB_MAC_ADDR>
     <SUB_USER_NAME>user2350</SUB_USER_NAME>
     <TERMINATION_CAUSE>User logout request</TERMINATION_CAUSE>
    </ACCESS_CUBE>
</PUBLICSPOTXMLINTERFACE>
```

Status

Mit einem "Status"-Request erfragt das externe Gateway beim Public Spot den aktuellen Status eines Benutzers. Ein "Status"-Request enthält das Attribut `COMMAND="RADIUS_Status"`.

Das XML-Interface kann die folgenden XML-Elemente einer Anfrage verarbeiten:

`SUB_USER_NAME`

Benutzername

`SUB_MAC_ADDR`

MAC-Adresse des Benutzer-Gerätes. Mögliche Formate sind:

- 00164115208c
- 00:16:41:15:20:8c
- 00-16-41-15-20-8c

Das XML-Interface sendet dem Gateway daraufhin eine "Status"-Response, die die folgenden XML-Elemente enthalten kann:

`SUB_USER_NAME`

Benutzername

`SUB_MAC_ADDR`

MAC-Adresse des Benutzer-Gerätes. Mögliche Formate sind:

- 00164115208c
- 00:16:41:15:20:8c
- 00-16-41-15-20-8c

`SUB_STATUS`

Der aktuelle Benutzerstatus. Folgende Werte sind möglich:

- `RADIUS_STATUS_DONE`: Status Anfrage erfolgreich
- `RADIUS_STATUS_REJECT`: Status Anfrage zurückgewiesen, z. B. unbekannter User oder MAC Adresse

`SESSION_TXBYTES`

Aktuell gesendete Datenmenge

`SESSION_RXBYTES`

Aktuell empfangene Datenmenge

`SESSION_TXPACKETS`

Anzahl der bisher gesendeten Datenpakete

`SESSION_RXPACKETS`

Anzahl der bisher empfangenen Datenpakete

`SESSION_STATE`

Aktueller Status der Sitzung

SESSION_ACTUAL_TIME

Aktuelle Uhrzeit

Im Folgenden finden Sie einige Beispiele für XML-Dateien:

Status-Request

Das externe Gateway sendet den Befehl für die Statusabfrage an den Public Spot:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<PUBLICSPOTXMLINTERFACE>
  <ACCESS_CUBE COMMAND="RADIUS_STATUS">
    <SUB_USER_NAME>user2350</SUB_USER_NAME>
    <SUB_MAC_ADDR>00164115208c</SUB_MAC_ADDR>
  </ACCESS_CUBE>
</PUBLICSPOTXMLINTERFACE>
```

Status-Response:

Das XML-Interface sendet eine Statusmeldung an das externe Gateway:

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
<PUBLICSPOTXMLINTERFACE>
   <ACCESS_CUBE ID="WLC_PM" IP="192.168.100.2" COMMAND="USER_STATUS">
     <SUB_STATUS>RADIUS_STATUS_DONE</SUB_STATUS>
     <SUB_MAC_ADDR>00:16:41:15:20:8b</SUB_MAC_ADDR>
     <SUB_USER_NAME>user2350</SUB_USER_NAME>
     <SESSION_ID>2</SESSION_ID>
     <SESSION_TXBYTES>0</SESSION_TXBYTES>
     <SESSION_RXBYTES>0</SESSION_RXBYTES>
     <SESSION_TXPACKETS>0</SESSION_TXPACKETS>
     <SESSION_RXPACKETS>0</SESSION_RXPACKETS>
     <SESSION_STATE>Authenticated</SESSION_STATE>
     <SESSION_ACTUAL_TIME>0</SESSION_ACTUAL_TIME>
   </ACCESS_CUBE>
</PUBLICSPOTXMLINTERFACE>
```

2 Anhang

2.1 Allgemein übermittelte RADIUS-Attribute

Das RADIUS-Client-Modul wurde auf Basis der RFCs Nr. 2865 und Nr. 2866 implementiert.

Diese Spezifikationen definieren sogenannte Attribute, die teilweise zwingend implementiert werden müssen, teilweise aber auch optional sind. Die folgenden Übersichtsseiten zeigt, welche Attribute bei welchen Meldungen zwischen RADIUS-Server und Ihrem Gerät übertragen bzw. ausgewertet werden.

2.1.1 Meldungen an den und vom Authentifizierungs-Server

Übertragene Attribute

Wie bereits erwähnt, übermittelt Ihr Gerät in einer RADIUS-Anfrage weit mehr als ausschließlich Benutzername und -kennwort. RADIUS-Server können diese zusätzlichen Informationen komplett ignorieren oder lediglich eine Teilmenge davon verarbeiten. Viele dieser Attribute werden auch für den Serverzugang über Dial-in verwendet und sind in den RADIUS RFCs als Standard-Attribute definiert. Einige für den Hotspot-Betrieb wichtige Informationen lassen sich jedoch nicht mit den Standard-Attributen abbilden. Diese zusätzlichen Attribute werden als herstellerspezifisch mit der Herstellerkennung 2356 (LANCOM Systems GmbH) verwendet.

Tabelle 10: Übersicht der vom Gerät an den Authentifizierungs-Server übertragenen RADIUS-Attribute

ID	Bezeichnung	Bedeutung	Mögliche Werte in LCOS
1	User-Name	Der vom Benutzer eingegebene Name.	
2	User-Password	Das vom Benutzer eingegebene Passwort.	
4	NAS-IP-Address	IP-Adresse Ihres Gerätes.	<IPv4-Adresse des Gerätes>
6	Service-Type	Art des Dienstes, den der Benutzer angefragt hat. Der Wert „1“ steht dabei für Login.	
8	Framed-IP-Address	Gibt die dem Client zugewiesene IP-Adresse an.	<IP-Adresse des Clients>
30	Called-Station-Id	MAC-Adresse Ihres Gerätes.	<nn:nn:nn:nn:nn:nn>
31	Calling-Station-Id	MAC-Adresse des Clients. Die Ausgabe erfolgt byte-weise in hexadezimaler Schreibweise mit Trennzeichen.	<nn:nn:nn:nn:nn:nn>
32	NAS-Identifier	Name Ihres Gerätes, sofern konfiguriert.	<Geräte-Name>
61	NAS-Port-Type	Art des physikalischen Ports, über den ein Benutzer eine Authentifizierung angefragt hat.	› **Id 19** kennzeichnet Clients aus dem WLAN. › **Id 15** kennzeichnet Clients aus dem Ethernet.
87	NAS-Port-Id	Bezeichnung des Interfaces, über welches ein Client mit Ihrem Gerät verbunden ist. Dies kann sowohl eine physische als auch logische Schnittstelle sein. Bedenken Sie, dass mehr als nur ein Client über ein Interface verbunden sein kann; die Port-Nummer verweist also im Gegensatz zu Dial-in-Servern nicht eindeutig auf einen Client.	z. B. › LAN-1 › WLAN-1-5 › WLC-TUNNEL-27

Ausgewertete Attribute

Ihr Gerät untersucht die Authentifizierungs-Antwort eines RADIUS-Servers auf Attribute, die es eventuell weiterverarbeiten kann. Die meisten Attribute haben allerdings nur dann eine Bedeutung, wenn die Antwort positiv war, sodass sie die anschließende Sitzung beeinflussen.

Tabelle 11: Übersicht aller unterstützten RADIUS-Attribute

ID	Bezeichnung	Bedeutung	Mögliche Werte in LCOS
18	Reply-Message	Eine beliebige Zeichenfolge des RADIUS-Servers, die entweder ein gescheitertes Anmelden oder eine Willkommensnachricht beinhaltet. Diese Nachricht lässt sich über das `SERVERMSG`-Element in eine benutzerdefinierte Start- oder Fehlerseite integrieren.	
25	Class	Ein beliebiges Oktett oder Achtbitzeichen, das die Daten vom Authentifizerungs- / Accounting-Backend enthält. Jedes Mal, wenn das Gerät eine RADIUS-Accounting-Anfrage stellt, wird dieses Attribut unverändert gesendet. Innerhalb einer Authentifizierungs-Antwort kann dieses Attribut mehrmals vorkommen, um z. B. eine Zeichenfolge zu übertragen, die länger als 255 Bytes ist. Das Gerät behandelt alle Vorkommen dieses Attributes in Accounting-Anfragen in der Reihenfolge, in der sie in der Authentifizierungs-Antwort aufgetreten sind.	
26	Vendor 2356, Id 1 LCS-Traffic-Limit	Definiert eine Datenmenge in Bytes, nach der das Gerät die Sitzung automatisch beendet. Dieser Wert ist nützlich, um Volumen-limitierte Benutzerkonten zu erstellen. Wenn dieses Attribut in der Authentifizierungs-Antwort fehlt, wird kein Volumen-Limit angenomnen. Ein Datenlimit von 0 wird als ein Benutzerkonto interpretiert, das zwar grundsätzlich gültig ist, aber sein Datenvolumen aufgebraucht hat. In diesem Fall startet das Gerät keine Sitzung.	
26	Vendor 2356, Id 3 LCS-Redirection-URL	Kann eine beliebige URL enthalten, die als zusätzlicher Link auf der Startseite angeboten wird. Dies kann die Startseite des Benutzers sein oder eine Seite mit zusätzlichen Informationen zum Benutzerkonto.	
26	Vendor 2356, Id 5 LCS-Account-End	Definiert einen absoluten Zeitpunkt (gemessen in Sekunden seit dem 1. Januar 1970 0:00:00), nach dem der Account ungültig wird. Wenn dieses Attribut in der Authentifizierungs-Antwort fehlt, wird kein Datumslimit angenomnen. Das Gerät startet keine Sitzung, wenn die interne Systemuhr nicht eingestellt ist oder der angegebene Zeitpunkt in der Vergangenheit liegt.	
26	Vendor 2356, Id 7 LCS-Public-Spot-Username	Enthält den Namen eines Public Spot-Benutzers für den Auto-Login. Der Auto-Login bezieht sich dabei auf die Tabelle der MAC-authentifizierten Benutzer, denen der Server automatisch einen Benutzernamen zuweist.	
26	Vendor 2356, Id 8 LCS-TxRateLimit	Definiert eine maximale Downstream-Rate in kbps. Diese Beschränkung lässt sich mit der dazugehörigen Public Spot-Funktion kombinieren.	
26	Vendor 2356, Id 9 LCS-RxRateLimit	Definiert eine maximale Upstream-Rate in kbps. Diese Beschränkung lässt sich mit der dazugehörigen Public Spot-Funktion kombinieren.	
26	Vendor 2356, Id 13 LCS-Advertisement-URL	Definiert eine kommaseparierte Liste von Werbe-URLs.	

ID	Bezeichnung	Bedeutung	Mögliche Werte in LCOS
26	Vendor 2356, Id 14 LCS-Advertisement-Interval	Definiert das Intervall in Minuten, nach dem der Public Spot einen Benutzer an eine Werbe-URL umleitet. Bei einem Intervall von 0 erfolgt die Umleitung direkt nach der Anmeldung.	
27	Session-Timeout	Definiert eine optionale Maximal-Dauer für die Sitzung in Sekunden. Wenn dieses Attribut in der Authentifizierungs-Antwort fehlt, wird kein Zeitlimit angenommen. Ein Zeitlimit von 0 wird als ein Benutzerkonto interpretiert, das zwar grundsätzlich gültig ist, aber seine verfügbare Zeit aufgebraucht hat. In diesem Fall startet das Gerät keine Sitzung.	
28	Idle-Timeout	Definiert einen Zeitraum in Sekunden, nach dem das Gerät die Sitzung beendet, wenn es keine Pakete vom Client mehr empfängt. Dieser Wert überschreibt möglichweise eine unter **Public-Spot** > **Server** > **Leerlaufzeitüberschreitung** lokal definierte Leerlauf-Zeitüberschreitung.	
64	Tunnel-Type	Definiert das Tunneling-Protokoll, welches für die Sitzung verwendet wird.	
65	Tunnel-Medium-Type	Definiert das Transportmedium, über das eine getunnelte Sitzung hergestellt wird.	
81	Tunnel-Private-Group-ID	Definiert die Gruppen-ID, falls die Sitzung getunnelt ist.	
85	Acct-Interim-Interval	Definiert die Zeit zwischen aufeinander folgenden RADIUS-Accounting-Aktualisierungen. Dieser Wert wird nur dann ausgewertet, wenn auf dem RADIUS-Client lokal kein eigenes Accounting-Intervall festgelegt ist, Sie für das Public Spot-Modul also keinen **Update-Zyklus** festgelegt haben.	

Beachten Sie, dass sich die Attribute für LCS-Account-Ende und Session-Zeitüberschreitung gegenseitig ausschließen und daher beide Attribute nicht in einer Antwort auftreten sollten. Sollten dennoch beide Attribute auftreten, wertet das Gerät das zuletzt auftretende Attribut aus.

2.1.2 Meldungen an/vom Accounting-Server

Übertragene Attribute

Der Satz von RADIUS-Attributen der einem RADIUS-Server in einer Accounting-Anfrage übergeben wird ähnelt einer Authentifizierungs-Anfrage. Dennoch werden einige spezifische Accounting-Attribute hinzugefügt. Die folgenden Attribute sind in allen RADIUS-Accounting-Anfragen vorhanden:

Übersicht der vom Gerät an den Accounting-Server übertragenen RADIUS-Attribute

1

User-Name

Name des Benutzerkontos, dass zur Authentifizierung verwendet wurde.

4

NAS-IP-Address

IP-Adresse Ihres Gerätes.

8

Framed-IP-Address

IP-Adresse, die dem Client zugewiesen wurde.

25

Class

Alle Class-Attribut-Werte, die der RADIUS-Authentifizierungs-Server in seiner Antwort geliefert hat.

30

Called-Station-Id

MAC-Adresse Ihres Gerätes

31

Calling-Station-Id

MAC-Adresse des Clients. Die Ausgabe erfolgt byte-weise in hexadezimaler Schreibweise mit Trennzeichen (nn:nn:nn:nn:nn:nn).

32

NAS-Identifier

Name Ihres Gerätes, sofern konfiguriert.

40

Acct-Status-Type

Anfragetyp, welcher den Start oder den Stop des Accountings, oder ein Interim-Update signalisiert. Weitere Erläuterungen finden Sie im Kapitel *Anfragetypen*.

44

Acct-Session-Id

Eine Zeichenfolge, die den Client eindeutig identifiziert. Sie besteht aus der MAC-Adresse des Netzwerkadapters, dem Zeitpunkt der Anmeldung (gemessen in Sekunden seit dem 1. Januar 1970 0:00:00) und der Sitzungszähler, den Ihr Gerät lokal verwaltet.

61

NAS-Port-Type

Art des physikalischen Ports, über den ein Benutzer eine Authentifizierung angefragt hat.

- **Id 19** kennzeichnet Clients aus dem WLAN
- **Id 15** kennzeichnet Clients aus dem Ethernet

87

NAS-Port-Id

Bezeichnung des Interfaces, über welches ein Client mit Ihrem Gerät verbunden ist. Dies kann sowohl eine physische als auch logische Schnittstelle sein, wie z. B. `LAN-1`, `WLAN-1-5` oder `WLC-TUNNEL-27`.

Bedenken Sie, dass mehr als nur ein Client über ein Interface verbunden sein kann; die Port-Nummer also im Gegensatz zu Dial-in-Servern nicht eindeutig auf einen Client verweist.

Im Falle einer Accounting-Stop-Anfrage oder eines Interim-Updates beinhaltet die Anfrage zusätzlich folgendes Attribute:

42

Acct-Input-Octets

Die Summe aller vom Client empfangenen Daten-Bytes in dieser Sitzung, Modulo 2^{32}.

43

Acct-Output-Octets

Die Summe aller zum Client gesendeten Daten-Bytes in dieser Sitzung, Modulo 2^{32}.

46

Acct-Session-Time

Die Gesamtdauer der Sitzung des Clients in Sekunden.

Wurde die Sitzung wegen einer Leerlauf-Zeitüberschreitung beendet, reduziert sich dieser Wert um die Leerlaufzeit.

47

Acct-Input-Packets

Die Anzahl der Datenpakete, die Ihr Gerät während der Sitzung vom Client empfangen hat.

48

Acct-Output-Packets

Die Anzahl der Datenpakete, die Ihr Gerät während der Sitzung zum Client gesendet hat.

49

Acct-Terminate-Cause

Der Grund für den Abbruch oder das Ende der Accounting-Sitzung. Wird gesendet, wenn das der **Acct-Status-Type** den Wert `Start` oder `Stop` besitzt.

52

Acct-Input-Gigawords

Die oberen 32 Bits der Summe aller vom Client empfangenen Daten-Bytes während dieser Sitzung.

53

Acct-Output-Gigawords

Die oberen 32 Bits der Summe aller zum Client gesendeten Daten-Bytes während dieser Sitzung.

55

Event-Timestamp

Der Zeitpunkt, an dem diese Accounting-Anfrage gestartet wurde (gemessen in Sekunden seit dem 1. Januar 1970 0:00:00). Dieses Attribut ist nur dann vorhanden, wenn die Systemuhr Ihres Gerätes eine gültige Zeit aufweist.

Beachten Sie, dass das RADIUS-Accounting erst nach der erfolgreichen Anmeldung eines Clients mit der Abrechnung beginnt; also die für die Authentifizierung benötigte Zeit nicht aufgezeichnet wird. Über die *Traffic-Limit-Option* können Sie den Datenverkehr während der Authentifizierungsphase einschränken. Die finale Accounting-Stop-Anfrage enthält natürlich ebenso das Termination-Cause-Attribute (49). Eine Übersicht der dieser Attribute finden Sie im LANCOM "Public Spot: Implementation Guide", erhältlich unter *www.lancom-systems.de*.

Ausgewertete Attribute

Ihr Gerät wertet die Antworten von RADIUS-Accounting-Servern derzeit nicht aus.

2.2 Durch WISPr übermittelte RADIUS-Attribute

Wenn Sie WISPr aktivieren und einen externen RADIUS-Server verwenden, übermittelt der Public Spot die Attribute (Access-Request):

- **Location-ID**
- **Location-Name**
- **Logoff-URL**

Bei diesen Attributen handelt es sich um einen Auszug der vorangegangenen Abschnitt konfigurierten Werte. Über sie kann ein Provider oder Roaming-Broker den Ort des Clients zu Abrechnungszwecken identifizieren. Es werden Vendor Specific Attributes (VSA) mit der IANA Private Enterprise Number (PEN) 14122 verwendet.

Von einem externen RADIUS-Server verarbeitet der Public Spot die Attribute (Access-Accept):

- **Redirection-URL**: URL, zu der ein Client nach der Anmeldung weitergeleitet werden soll. Diese Funktion wird nicht von allen Smart-Clients unterstützt.
- **Bandwidth-Max-Up**: Maximale Bandbreite der Upload-Geschwindigkeit, die der Client erhalten soll.
- **Bandwidth-Max-Down**: Maximale Bandbreite der Download-Geschwindigkeit die der Client erhalten soll.
- **Session-Terminate-Time**: Zeitpunkt, zu dem der Client automatisch de-authentifiziert werden soll. Dieses Attribut besitzt nach ISO 8601 das Format `YYYY-MM-DDThh:mm:ssTZD`. Falls TZD nicht angegeben wird, wird der Client nach Ortszeit des Public Spots de-authentifiziert.
- **Session-Terminate-End-Of-Day**: Der Wert dieses Attributs kann entweder 0 oder 1 sein. Er gibt an, ob der Client am Ende des Abrechnungstages vom Public Spot de-authentifiziert werden soll.

Für das Accounting verwendet der Public Spot die Attribute:

- **Location-ID**
- **Location-Name**

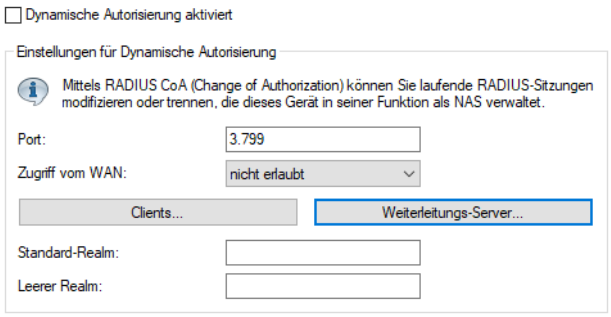
2.3 Dynamische Autorisierung durch RADIUS CoA (Change of Authorization)

Mit der dynamischen Autorisierung ist es möglich, aktuelle RADIUS-Sitzungen zu bearbeiten. Dazu übermittelt der jeweilige CoA Client eine CoA Nachricht an das NAS. Diese Nachricht enthält neben der identifizierenden Merkmale für die Session, die Sie ändern möchten, die zu bearbeitenden Attribute und deren neue Werte.

Zudem besteht die Möglichkeit, die jeweilige Sitzung zu trennen. Dies erfolgt durch eine Disconnect Message (DM), die an das NAS gesendet wird – das NAS trennt daraufhin die gewünschte Verbindung.

2.3.1 Dynamische Autorisierung mit LANconfig konfigurieren

Um die dynamische Autorisierung (CoA) mit LANconfig zu konfigurieren, öffnen Sie die Ansicht **RADIUS** > **Dyn. Autorisierung**.



Dynamische Autorisierung aktiviert

Hier aktivieren oder deaktivieren Sie die dynamische Autorisierung.

Port

Enthält den Standard-Port, auf dem CoA-Nachrichten angenommen werden.

Zugriff vom WAN

Dieser Eintrag legt fest, ob Nachrichten vom WAN zugelassen sind, nur über VPN angenommen werden oder verboten sind.

Clients

Tragen Sie hier alle CoA-Clients ein, die Nachrichten an das NAS senden dürfen.

Weiterleitungs-Server

Sollen CoA-Nachrichten weitergeleitet werden, ist es erforderlich, die Weiterleitungen hier anzugeben.

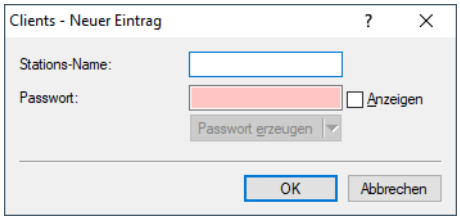
Standard-Realm

Dieser Realm gilt alternativ, wenn der übermittelte Benutzername einen unbekannten Realm verwendet, der nicht in der Liste der Weiterleitungs-Server enthalten ist.

Leerer Realm

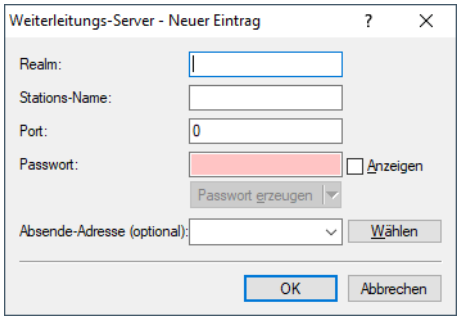
Dieser Realm gilt alternativ, wenn der übermittelte Benutzername keinen Realm enthält.

Um CoA-Clients für die dynamische Autorisierung hinzuzufügen, klicken auf die Schaltfläche **Clients** und fügen Sie der Tabelle einen neuen Eintrag hinzu.



Tragen Sie einen Stationsnamen für den Client ein und definieren Sie ein Passwort, das der Client für den Zugang zum NAS benötigt.

Um neue Weiterleitungs-Server für die dynamische Autorisierung hinzuzufügen, klicken Sie auf die Schaltfläche **Weiterleitungs-Server** und fügen Sie der Tabelle einen neuen Eintrag hinzu.



Realm

Tragen Sie hier den Realm ein, mit dem der RADIUS-Server das Weiterleitungs-Ziel identifiziert.

Verwenden Sie ggf. bereits vorhandene Weiterleitungs-Server, die unter **RADIUS** > **Server** > **Erweiterte Einstellungen** > **Weiterleitung** > **Weiterleitungs-Server** definiert sind.

Stations-Name

Geben Sie den Hostnamen des Weiterleitungs-Servers an.

Port

Legen Sie den Port des Servers fest, über den die Anfragen weitergeleitet werden.

Passwort

Legen Sie ein Passwort fest, das der Client für den Zugang zum RADIUS-Server benötigt.

Absende-Adresse (optional)

Geben Sie optional eine Absendeadresse an.

Legen Sie fest, welche logischen WLAN-Schnittstellen die dynamische Autorisierung verwenden dürfen. Aktivieren oder deaktivieren Sie hierfür im Reiter "Netzwerk" unter **Wireless-LAN** > **Allgemein** > **Logische WLAN-Einstellungen** > **Netzwerk** beim jeweiligen Interface die Checkbox **RADIUS CoA aktiviert**.

2.4 Im- / Export von RADIUS-Benutzerdaten per CSV-Datei

Der interne RADIUS-Server ist im Prinzip eine Benutzerdatenbank. Daher soll hier eine einfache Möglichkeit gezeigt werden, mit der Sie Benutzereinträge im- und exportieren können. Insbesondere ist dies für Public-Spot-Benutzer relevant, die z. B. in größerer Zahl von einem externen System erzeugt werden. Aber auch für LEPS-MAC können Sie hier die Daten vereinfacht importieren. Als Format für den Datenaustausch wird csv (comma separated values) genommen, wobei als Default-Separator der einzelnen Datenfelder ein Semikolon dient.

2.4.1 Export von RADIUS-Benutzerdaten per CSV-Datei

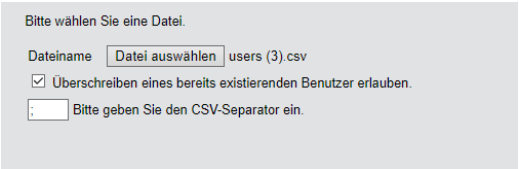
Um die Benutzerdaten des RADIUS-Servers über WEBconfig zu exportieren, gehen Sie folgendermaßen vor.

Klicken Sie auf **Extras** > **RADIUS-Benutzer exportieren**.
Die Benutzerdaten werden als Datei `users.csv` heruntergeladen. Als Trennzeichen dient das Semikolon; in der ersten Zeile sind die Bezeichner der Datenbankfelder.

2.4.2 Import von RADIUS-Benutzerdaten per CSV-Datei

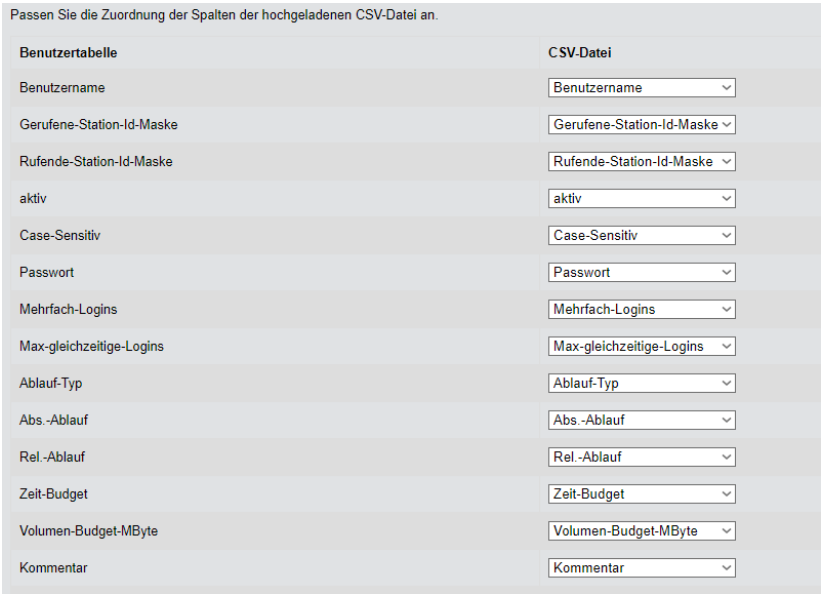
Um die Benutzerdaten des RADIUS-Servers über WEBconfig zu importieren, gehen Sie folgendermaßen vor.

1. Führen Sie wie in *Export von RADIUS-Benutzerdaten per CSV-Datei* auf Seite 180 beschrieben einen Export der Benutzerdaten durch, um die korrekte Kopfzeile mit den Bezeichnern der Datenbankfelder zu erhalten.
2. Erstellen Sie eine CSV-Importdatei mit einer Kopfzeile, welche die im vorigen Schritt ermittelten korrekten Bezeichner der Datenbankfelder beinhaltet. Die Importdatei muss nicht alle Spalten enthalten.
3. Wechseln Sie zum Menüpunkt **Extras** > **RADIUS-Benutzer importieren**.
4. Wählen Sie mit **Datei auswählen** die zu importierende CSV-Datei aus.
5. Geben Sie den CSV-Separator ein. Standardmäßig ist bereits „;“ voreingestellt.



6. Starten Sie den Upload.

7. Kontrollieren Sie nun die Zuordnung der unterstützten Spalten zu den in der CSV-Datei erkannten Spalten. Die Zuordnung kann in diesem Dialog angepasst werden. Wenn Sie die Spaltennamen aus der zuvor exportierten CSV-Datei übernommen haben, ist keine Anpassung notwendig.



8. Wählen Sie **Import starten**, um den Vorgang abzuschließen und die Benutzerdaten zu übernehmen.

2.5 Experteneinstellungen zur PMS-Schnittstelle

Zusätzlich zu den Einstellungsmöglichkeiten, die Ihnen LANconfig für die PMS-Schnittstelle bietet, haben Sie die Möglichkeit, über das Setup-Menü eine Reihe weiterer Parameter zu konfigurieren. Diese Parameter umfassen einerseits Werte, die das Gerät zur internen Synchronisation mit Ihrem PMS-System benötigt und normalerweise nicht verändert werden. Andererseits finden Sie im Setup-Menü auch erweiterte Einstellungen, mit denen Sie das Leistungsspektrum der PMS-Schnittstelle weiter ausbauen können, z. B. durch die kostenfreie Nutzung eines Public Spots für Gäste mit VIP-Status bei einem ansonsten kostenpflichtigen Zugang.

Die nachfolgenden Seiten bieten Ihnen eine Übersicht sämtlicher Parameter für die PMS-Schnittstelle, die nicht über LANconfig konfigurierbar sind.

2.5.1 Accounting

In diesem Menü konfigurieren Sie die Übermittlung der Abrechnungsinformationen vom Gerät an Ihr PMS.

SNMP-ID:

2.64.10

Pfad Konsole:

Setup > **PMS-Interface**

Accounting-Tabelle-Reinigungsintervall

Über diesen Eintrag konfigurieren Sie, in welchem Intervall das Gerät seine interne Accounting-Tabelle im Status-Menü von abgelaufenen Sitzungen befreit.

SNMP-ID:

2.64.10.3

Pfad Konsole:

Setup > **PMS-Interface** > **Accounting**

Mögliche Werte:

0 … 4294967295 Sekunden

Default-Wert:

60

Besondere Werte:

0

Der Wert 0 deaktiviert die automatische Bereinigung.

Flashrom-Speicherintervall

Über diesen Eintrag konfigurieren Sie, in welchem Intervall das Gerät die gesammelten Accounting-Informationen in seinem internen Flash-ROM sichert.

Beachten Sie, dass ein häufiges Beschreiben dieses Speichers die Lebensdauer Ihres Gerätes reduziert!

SNMP-ID:

2.64.10.2

Pfad Konsole:

Setup > **PMS-Interface** > **Accounting**

Mögliche Werte:

0 … 4294967295 Sekunden

Default-Wert:

15

Besondere Werte:

0

Der Wert 0 deaktiviert die Funktion.

Accounting-Tabelle-Updateintervall

Über diesen Eintrag konfigurieren Sie, in welchem Intervall das Gerät seine interne Accounting-Tabelle im Status-Menü aktualisiert.

SNMP-ID:

2.64.10.4

Pfad Konsole:

Setup > **PMS-Interface** > **Accounting**

Mögliche Werte:

0 … 4294967295 Sekunden

Default-Wert:

15

Besondere Werte:

0

Wenn der Wert 0 ist, ist die Aktualisierung deaktiviert und die Status-Tabelle zeigt keine Werte an.

2.5.2 Login-Formular

In diesem Menü nehmen Sie die PMS-spezifischen Einstellungen zur Login-/Portalseite, die Ihren Gäste beim unauthentifizierten Zugriff auf den Hotspot erscheint.

SNMP-ID:

2.64.11

Pfad Konsole:

Setup > **PMS-Interface**

Kostenlos-VIP-Status

In dieser Tabelle verwalten Sie lokal die VIP-Kategorien aus Ihrem PMS.

SNMP-ID:

2.64.11.6

Pfad Konsole:

Setup > **PMS-Interface** > **Login-Formular**

Status

Tragen Sie hier die VIP-Kategorie aus Ihrem PMS ein, deren Mitgliedern Sie einen kostenlosen Internetzugang zur Verfügung stellen wollen.

Haben Sie auf Ihrem PMS-Server z. B. drei mögliche VIP-Stati eingerichtet (VIP1, VIP2, VIP3), wollen allerdings nur den Hotelgästen aus Kategorie VIP2 einen freien Internetzugang anbieten, tragen Sie deren entsprechende Kennung hier ein.

SNMP-ID:

2.64.11.6.1

Pfad Konsole:

Setup > **PMS-Interface** > **Login-Formular** > **Kostenlos-VIP-Status**

Mögliche Werte:

max. 20 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default-Wert:

leer

Fidelio-kostenlos-Sicherheits-Check

Wählen Sie aus, mit welcher weiteren Kennung sich ein Hotelgast – zusätzlich zu seinem Benutzernamen und seiner Zimmernummer – am Public Spot authentisiert, sofern Sie eine kostenlose Internetnutzung anbieten. Wenn Sie `Keiner` wählen, verzichtet das Gerät auf die Abfrage einer weiteren Kennung.

SNMP-ID:

2.64.11.3

Pfad Konsole:

Setup > **PMS-Interface** > **Login-Formular**

Mögliche Werte:

Keiner
Reservierungsnummer
Ankunftsdatum
Abreisedatum
Vorname
Profilnummer

Default-Wert:

Keiner

Fidelio-kostenlos-VIP-Sicherheits-Check

Wählen Sie aus, mit welcher weiteren Kennung sich eine VIP – zusätzlich zu ihrem Benutzernamen und ihrer Zimmernummer – am Public Spot authentisiert, sofern Sie eine kostenlose Internetnutzung für VIPs anbieten. Wenn Sie `Keiner` wählen, verzichtet das Gerät auf die Abfrage einer weiteren Kennung.

SNMP-ID:

2.64.11.5

Pfad Konsole:

Setup > **PMS-Interface** > **Login-Formular**

Mögliche Werte:

Keiner
Reservierungsnummer
Ankunftsdatum
Abreisedatum
Vorname
Profilnummer

Default-Wert:

Keiner

Fidelio-kostenpflichtig-Sicherheits-Check

Wählen Sie aus, mit welcher weiteren Kennung sich ein Hotelgast – zusätzlich zu seinem Benutzernamen und seiner Zimmernummer – am Public Spot authentisiert, sofern Sie eine kostenpflichtige Internetnutzung anbieten. Wenn Sie `Keiner` wählen, verzichtet das Gerät auf die Abfrage einer weiteren Kennung.

SNMP-ID:

2.64.11.4

Pfad Konsole:

Setup > **PMS-Interface** > **Login-Formular**

Mögliche Werte:

Keiner
Reservierungsnummer
Ankunftsdatum
Abreisedatum
Vorname
Profilnummer

Default-Wert:

Reservierungsnummer

PMS-Login-Formular

Wählen Sie aus, welche Anmeldemaske die Portalseite für Ihre PMS-Schnittstelle anzeigt.

SNMP-ID:

2.64.11.2

Pfad Konsole:

Setup > **PMS-Interface** > **Login-Formular**

Mögliche Werte:

kostenlos

Wählen Sie diese Einstellung, wenn Sie Ihren Hotelgästen einen kostenlosen Internetzugang anbieten. Ihre Hotelgäste werden auf der Portalseite dennoch dazu aufgefordert, sich mit ihrem Benutzernamen, ihrer Zimmernummer und ggf. einer weiteren Kennung am Hotspot zu authentisieren, um eine Internetnutzung durch Unbefugte zu erschweren.

kostenpflichtig

Wählen Sie diese Einstellung, wenn Sie Ihren Hotelgästen einen kostenpflichtig Internetzugang anbieten. Ihre Hotelgäste werden auf der Portalseite dazu aufgefordert, sich mit ihrem Benutzernamen, ihrer Zimmernummer und ggf. einer weiteren Kennung am Hotspot zu authentisieren und einen Tarif auszuwählen.

kostenlos-VIP

Wählen Sie diese Einstellung, wenn Sie einen eigentlich kostenpflichtigen Internetzugang für VIPs kostenlos anbieten wollen. Ihre VIPs erhalten dann zwar die Anmeldemaske für den kostenpflichtigen Zugang, es werden ihnen jedoch keine Gebühren in Rechnung gestellt.

Default-Wert:

kostenlos

PublicSpot-Login-Formular

Aktivieren bzw. deaktivieren Sie, ob die Portalseite die Public-Spot-eigenen Anmeldemaske anzeigt. Wenn Sie diese Einstellung deaktivieren, können sich Public-Spot-Nutzer, die eine Kombination aus Benutzername und Passwort als Zugangsdaten verwenden (z. B. fest eingetragene oder über Voucher eingerichtete Nutzer), nicht mehr am Gerät anmelden.

SNMP-ID:

2.64.11.1

Pfad Konsole:

Setup > **PMS-Interface** > **Login-Formular**

Mögliche Werte:

nein
ja

Default-Wert:

nein

2.5.3 Gastname-Case-Sensitiv

Aktivieren oder deaktivieren Sie, ob das Gerät beim Abgleich des beim Login angegebenen Nachnamens mit dem Gastnamen in der PMS-Datenbank auf Groß- und Kleinschreibung achtet. Ist diese Einstellung aktiviert, wird einem Gast der Public-Spot-Zugang verweigert, wenn die Schreibweise seines Namens nicht der dem Hotel mitgeteilten Schreibweise entspricht.

SNMP-ID:

2.64.12

Pfad Konsole:

Setup > **PMS-Interface**

Mögliche Werte:

nein
ja

Default-Wert:

ja

2.5.4 Trennzeichen

Über diesen Eintrag konfigurieren Sie das Trennzeichen, das Ihr PMS benutzt, um Datensätze an eine API weiterzureichen. Die Micros-Fidelio-Spezifikation z. B. verwendet standardmäßig den senkrechten Trennstrich (|, Hex 7C).

Sie sollten diesen Wert nach Möglichkeit nicht verändern. Ein falsches Trennzeichen führt dazu, dass das Gerät die von Ihrem PMS übermittelten Datensätze nicht mehr lesen kann und die PMS-Schnittstelle nicht funktioniert!

SNMP-ID:

2.64.6

Pfad Konsole:

Setup > **PMS-Interface**

Mögliche Werte:

max. 1 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default-Wert:

|

2.5.5 Zeichensatz

Wählen Sie den Zeichensatz aus, in dem Ihr PMS die Nachnamen Ihrer Gäste an das Gerät übermittelt.

SNMP-ID:

2.64.7

Pfad Konsole:

Setup > **PMS-Interface**

Mögliche Werte:

CP850
W1252

Default-Wert:

CP850

2.6 SMS-Empfang und -Versand

Sofern Ihr Gerät über ein 3G/4G WWAN-Modul verfügt, ist Ihr Gerät ebenfalls dazu in der Lage, Kurznachrichten über den Short Message Service (SMS) zu empfangen und zu versenden.

Die SMS-Funktion dient dabei vorwiegend als benachrichtigende und funktionserweiternde Schnittstelle für die LCOS-eigenen Module sowie externe Instanzen wie Router, Management-Lösungen, Accounting-Systeme und Ähnliche. Sie haben jedoch auch als Benutzer die Möglichkeit, über die entsprechende *Funktion im LANmonitor* oder mit dem `smssend`-Kommando auf der Konsole Kurznachrichten zu verschicken. Darüber hinaus haben Sie mit LANmonitor auch die Möglichkeit, gesendete oder empfangene Nachrichten *komfortabel zu verwalten*.

Der SMS-Empfang und -Versand muss ebenfalls Vertragsgegenstand der von Ihnen verwendeten SIM-Karte sein.

2.6.1 Empfang von SMS-Nachrichten

Ihr Gerät ist dazu in der Lage, SMS-Benachrichtungen auf Basis des ETSI-Standards TS 127.005 zu empfangen bzw. abzufragen, zu speichern und auf Wunsch den Erhalt einer SMS im SYSLOG zu protokollieren. Der Eintrag ins SYSLOG erfolgt dabei als "Hinweis", um Sie über ggf. wichtige Meldungen – wie z. B. die Benachrichtigung durch eine externe Instanz – zu informieren. Eine solche Instanz kann beispielsweise das Accounting-System Ihres Providers sein:

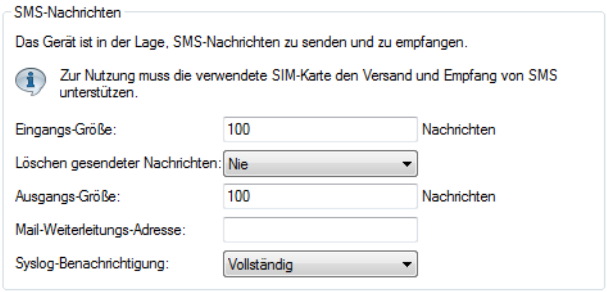
Sofern Sie mit dem Gerät eine Verbindung zum Internet über das 3G/4G WWAN-Modul herstellen und der Vertrag mit Ihrem Internet-Provider eine Volumenbegrenzung umfasst, drosselt oder stoppt Ihr Provider die Datenübertragung bei Erreichen dieser Volumengrenze (je nach Vertrag). In Ländern mit entsprechender Gesetzgebung gilt dies z. B. ebenfalls für das Erreichen bestimmter Gebührengrenzen beim Daten-Roaming. Bevor die Datenübertragung jedoch gedrosselt oder gestoppt wird, versenden viele Provider eine SMS, die Sie als Kunde über das Erreichen der Volumengrenze informiert. Mit einer enstprechenden Benachrichtigungseinstellung im Syslog und / oder per E-Mail informiert Sie das Gerät umgehend über den Empfang der SMS, sodass Sie zeitnah darauf reagieren können.

2.6.2 Basiskonfiguration des SMS-Moduls

Die nachfolgenden Schritte zeigen Ihnen, wie Sie die Basiskonfiguration des SMS-Moduls eines 3G/4G WWAN-fähigen Gerätes vornehmen.

1. Starten Sie LANconfig und öffnen Sie den Konfigurationsdialog für das Gerät.

2. Wechseln Sie in die Ansicht **Meldungen** > **SMS-Nachrichten**.



3. Geben Sie unter **Eingangs-Größe** die maximale Anzahl an Kurznachrichten an, die das Gerät im Nachrichteneingang aufbewahrt.
   Beim Überschreiten der eingestellten Anzahl wird die älteste Nachricht gelöscht. In diesem Fall erfolgt **kein** SYSLOG-Eintrag. Der Wert `0` deaktiviert das Limit, d. h. Nachrichten werden im unbegrenzten Umfang aufbewahrt.

4. Legen Sie unter **Löschen gesendeter Nachrichten** fest, wie das Gerät mit versendeten Kurznachrichten umgeht.
   - **Sofort**: Versendete Kurznachrichten werden nicht gespeichert.
   - **Nie**: Versendete Kurznachrichten werden dauerhaft gespeichert.

5. Geben Sie unter **Ausgangs-Größe** die maximale Anzahl an Kurznachrichten an, die das Gerät im Nachrichtenausgang aufbewahrt.
   Beim Überschreiten der eingestellten Anzahl wird die älteste Nachricht gelöscht. In diesem Fall erfolgt **kein** SYSLOG-Eintrag. Der Wert `0` deaktiviert das Limit, d. h. Nachrichten werden im unbegrenzten Umfang aufbewahrt.

6. Legen Sie unter **Syslog-Benachrichtigung** fest, ob und wie das Gerät eingehende Kurznachrichten im SYSLOG protokolliert.
   - **Nein**: Im SYSLOG erfolgt für eingehende Kurznachrichten kein Eintrag.
   - **Nur Absender/kein Inhalt**: Der Eingang einer Kurznachricht wird zusammen mit der Absender-Rufnummer im SYSLOG erfasst.
   - **Vollständig**: Der Eingang einer Kurznachricht wird zusammen mit der Absender-Rufnummer und dem vollständigen Nachrichtentext im SYSLOG erfasst.

7. Optional: Geben Sie unter **Mail-Weiterleitungs-Adresse** die E-Mail-Adresse an, an die das Gerät eingehende Kurznachrichten weiterleiten soll.

   Damit die E-Mail-Weiterleitung funktioniert, muss ein gültiges SMTP-Konto im Gerät konfiguriert sein.

8. Übertragen Sie die Konfiguration zurück an das Gerät.

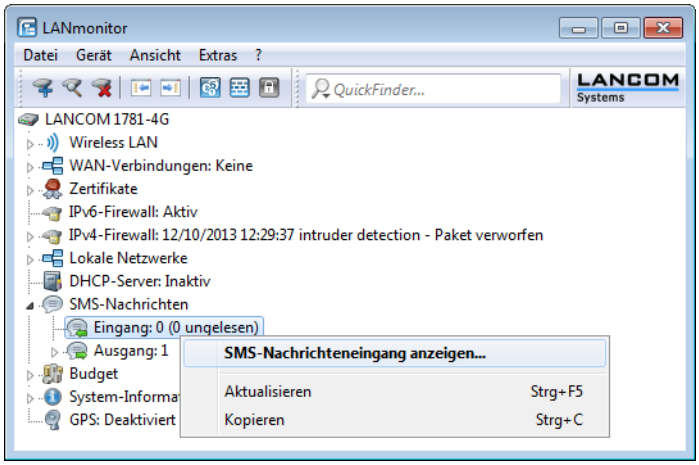
Fertig! Damit ist die Basiskonfiguration des SMS-Moduls abgeschlossen.

2.6.3 SMS-Nachrichten mit LANmonitor verwalten

Der nachfolgende Abschnitt zeigt, wie Sie auf einem 3G/4G WWAN-fähigen Gerät mit LANmonitor eingegangene oder versendete Kurznachrichten einsehen und bei Bedarf löschen.

1. Starten Sie LANmonitor und navigieren Sie im Menübaum des betreffenden Gerätes zu **SMS-Nachrichten** > **Eingang** bzw. **Ausgang**.
   Sofern im Gerät bereits Kurznachrichten vorliegen, zeigt LANmonitor direkt unter **Eingang** die letzten fünf empfangenen und unter **Ausgang** die letzten fünf gesendeten SMS an.

2. Öffnen Sie das Kontextmenü auf dem entsprechenden Eintrag und wählen Sie **SMS-Nachrichteneingang anzeigen** bzw. **SMS-Nachrichtenausgang anzeigen**.



Es öffnet sich ein neues Fenster, in dem LANmonitor alle eingegangenen bzw. versendeten Kurznachrichten und deren Status auflistet. Im **SMS-Nachrichteneingang** haben Sie die Möglichkeit, einzelne oder mehrere ausgewählte Nachrichten wahlweise zu löschen oder als gelesen/ungelesen zu markieren; der Status ist der Lesestatus (entsprechend **Neu** oder **Gelesen**). Im **SMS-Nachrichtenausgang** lassen sich die Nachrichten nur löschen; der Status ist der Sendestatus (**Ungesendet** oder **Gesendet**).

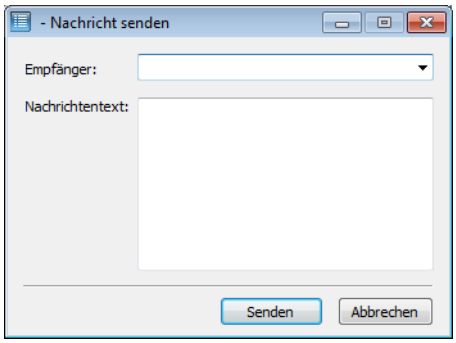
Die angezeigten Nachrichten verwalten Sie über das Kontextmenü. Um den kompletten Nachrichteneingang bzw. -ausgang zu löschen, wählen Sie in der Menüleiste unter **Nachrichten** die betreffende Aktion.

Um zwischen Nachrichteneingang und -ausgang bequem hin- und herzuwechseln, wählen Sie in der Menüleiste unter **Ansicht** die entsprechende Nachrichtenbox aus.

2.6.4 SMS-Nachrichten mit LANmonitor versenden

Der folgende Abschnitt zeigt, wie Sie mit LANmonitor Kurznachrichten über ein 3G/4G WWAN-fähiges Gerät versenden.

1. Starten Sie LANmonitor und navigieren Sie im Menübaum des betreffenden Gerätes zu **SMS-Nachrichten**.
2. Öffnen Sie das Kontextmenü auf dem Eintrag und wählen Sie **Nachricht senden**.
3. Geben Sie in dem sich öffnenden Editorfenster die Rufnummer des Empfängers und den zu versendenden Nachrichtentext ein.
   Die Anzahl der Zeichen ist dabei auf eine Kurznachricht (max. 160 Zeichen) beschränkt. Eine Übersicht der verfügbaren Zeichen finden Sie im Abschnitt *Zeichensatz für den SMS-Versand* auf Seite 191.



4. Klicken Sie **Senden**, um die Nachricht über das geräteinterne SMS-Modul zu verschicken.

2.6.5 URL-Platzhalter für den SMS-Versand

Sie haben die Möglichkeit, das SMS-Modul in seiner Rolle als Schnittstelle auch über eine URL anzusprechen. Dazu integrieren Sie vorgegebene Platzhalter (Parameter) in die URL, was den SMS-Versand über das Gerät per HTTP(S)-Aufruf erlaubt. Somit eignen sich LANCOM Mobilfunk-Router insbesondere auch für den Einsatz als SMS-Gateway.

Der SMS-Versand eignet sich für Installationen mit einem maximalen Durchsatz von 10 SMS pro Minute.

Die Authentifizierung am Gerät erfolgt mit Ihren Zugangsdaten; deren Einbindung in die URL gibt die Credential-Schreibweise Ihres Browsers vor. Typischerweise lautet diese Schreibweise `Benutzername:Passwort@Host`.

Je nach Einsatzszenario (z. B. SMS-Gateway) empfiehlt es sich, für den Zugang einen Administrator ohne Zugriffsrechte (**Keine**) mit dem alleinigen Funktionsrecht **Senden von SMS** anzulegen.

Nicht alle Webbrowser unterstützen die Übermittlung von Zugangsdaten über die URL. Hierzu gehört u. a. der Microsoft Internet Explorer in seinen aktuellen Versionen. Weichen Sie in diesem Fall auf einen anderen Browser aus, um den SMS-Versand über die URL zu nutzen.

Der URL-Aufruf erfolgt über die Syntax:

```
(http|https)://<User>:<Password>@<Host>/sms/?<Param1>=<Value1>&…&oldauth
```

Der Parameter `oldauth` ist dabei **zwingend** erforderlich; andernfalls sendet keiner der von Ihnen verwendeten Browser die Zugangsdaten an das Gerät. Darüber hinaus sind folgende Platzhalter definiert:

`DestinationAddress`

Rufnummer, an die das Gerät die SMS schicken soll. Es gelten die gleichen Konventionen wie für normale Telefonanrufe. Geben Sie den Parameter wie folgt an:

```
&DestinationAddress=01511234567
&DestinationAddress=00491511234567
```

`Content`

Inhalt der Kurznachricht. Die Anzahl der Zeichen ist dabei auf eine Kurznachricht (max. 160 Zeichen) beschränkt. Eine Übersicht der verfügbaren Zeichen finden Sie im Abschnitt *Zeichensatz für den SMS-Versand* auf Seite 191.

Um Leerzeichen und andere Sonderzeichen in die SMS einzubauen, müssen Sie diese in URL-kodierter Form an das Gerät übermitteln. Leerzeichen beispielsweise kodieren Sie mittels `%20` und Punkte mit `%2E`. Geben Sie den Parameter wie folgt an:

```
&Content=Dies%20ist%20eine%20Nachricht%2E
```

Mehr zu dem Thema erfahren Sie im Internet unter dem Stichwort "URL Encoding" sowie unter *www.w3schools.com*.

Manche Browser führen die URL-Kodierung automatisch durch. Generell ist jedoch zu empfehlen, Inhalte eigenständig zu kodieren, um die korrekte Umwandlung aller Zeichen sicherzustellen.

2.6.6 Zeichensatz für den SMS-Versand

Der Umfang der in einer SMS verfügbaren Zeichen (max. 160 Zeichen zu je 7 Bit = 1.120 Bit) ergibt sich aus dem GSM-Basiszeichensatz (ingesamt 128 Zeichen) sowie ausgewählten Zeichen aus dem erweiterten GSM-Zeichensatz. Mit dem erweiterten Zeichensatz lassen sich zusätzliche Zeichen darstellen; diese belegen jedoch den doppelten Speicherplatz und reduzieren die maximale Zeichenanzahl entsprechend. Zeichen, die nicht im SMS-Modul implementiert sind, ignoriert das Gerät beim Versand.

Folgende Zeichen sind im **GSM-Basiszeichensatz** definiert:

@	Δ	SP	0	¡	P	¿	p
£	_	!	1	A	Q	a	q
$	Φ	"	2	B	R	b	r
¥	Γ	#	3	C	S	c	s
è	Λ	¤	4	D	T	d	t
é	Ω	%	5	E	U	e	u
ù	Π	&	6	F	V	f	v
ì	Ψ	'	7	G	W	g	w
ò	Σ	(	8	H	X	h	x
Ç	Θ	)	9	I	Y	i	y
LF	Ξ	*	:	J	Z	j	z
Ø	ESC	+	;	K	Ä	k	ä
ø	Æ	,	<	L	Ö	l	ö
CR	æ	-	=	M	Ñ	m	ñ
Å	ß	.	>	N	Ü	n	ü
å	É	/	?	O	§	o	à

"SP" bezeichnet in der Übersicht das Leerzeichen. "LF", "CR" und "ESC" bezeichnen die Steuerzeichen für den Zeilenvorschub, den Wagenrücklauf und den Escape auf den erweiterten GSM-Zeichensatz.

Folgende Zeichen sind aus dem **erweiterten GSM-Zeichensatz** implementiert:

{	|	}	[	]	~	^	\	€	

2.7 Das SYSLOG-Modul

Mit dem SYSLOG-Modul besteht die Möglichkeit, Zugriffe auf das Gerät protokollieren zu lassen. Diese Funktion ist insbesondere für Systemadministratoren interessant, da sie die Möglichkeit bietet, eine lückenlose Historie aller Aktivitäten aufzeichnen zu lassen.

Um die SYSLOG-Nachrichten empfangen zu können, benötigen Sie einen entsprechenden SYSLOG-Client bzw. -Dämon. Unter UNIX / Linux erfolgt die Protokollierung durch den in der Regel standardmäßig eingerichteten SYSLOG-Dämon. Dieser meldet sich entweder direkt über die Konsole oder schreibt das Protokoll in eine entsprechende SYSLOG-Datei.

Unter Linux wird in der Datei `/etc/syslog.conf` angegeben, welche Facilities (Dienst oder die Komponente, welche die Nachricht ausgelöst hat) in welche Logdatei geschrieben werden sollen. Überprüfen Sie in der Konfiguration des Dämons, ob auf Netzwerkverbindungen explizit gehört wird.

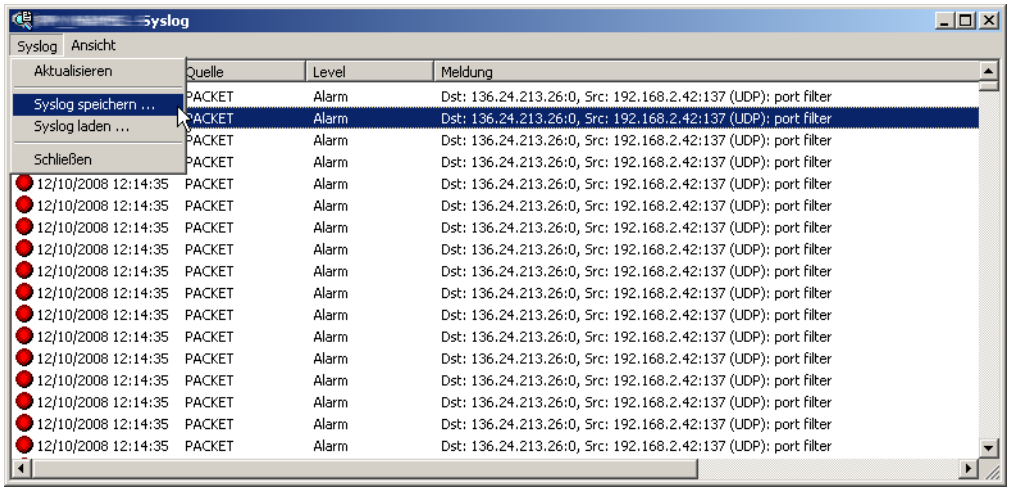
Windows stellt keine entsprechende Systemfunktion bereit. Sie benötigen spezielle Software, die die Funktion eines SYSLOG-Dämons erfüllt.

Als Erweiterung zur Ausgabe der SYSLOG-Informationen über einen entsprechenden SYSLOG-Client werden je nach Speicherausstattung des Gerätes zwischen 100 und 23.000 SYSLOG-Meldungen im RAM gespeichert. Diese internen SYSLOGs können an verschiedenen Stellen eingesehen werden:

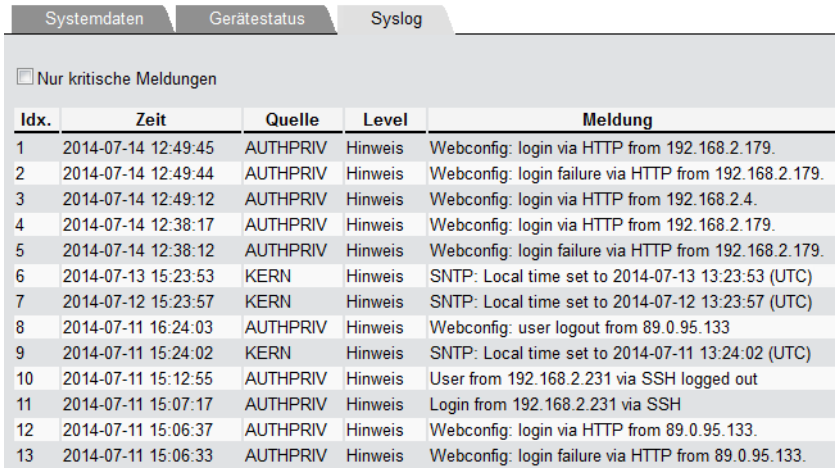
- In der Statistik der Geräte auf der Kommandozeite

- In WEBconfig unter /Systeminformation/Syslog
- In LANmonitor haben Sie zusätzlich die Möglichkeit, das Syslog aus dem Gerät zu exportieren und in einer Datei zu speichern. Klicken Sie dazu mit der rechten Maustaste auf den Namen des Gerätes und wählen Sie im Kontextmenü den Eintrag **Syslog anzeigen**. Die Ansicht ist jeweils ein aktueller Schnappschuss. Mit **Aktualisieren** wird eine Kopie des derzeitigen SYSLOGs vom Gerät exportiert und in der Ansicht dargestellt. **Syslog speichern** speichert die aktuelle Anzeige in eine Datei. Gespeicherte SYSLOGs können mit **Syslog laden** wieder zur Ansicht geöffnet werden.

Die SYSLOG-Meldungen werden nur dann in den geräteinternen Speicher geschrieben, wenn das Gerät als SYSLOG-Client mit der Loopback-Adresse 127.0.0.1 eingetragen wurde oder die bootpersistente Speicherung aktiviert wurde. Siehe *SYSLOG, Eventlog und Bootlog bootpersistent*.



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



Idx.	Zeit	Quelle	Level	Meldung
1	2014-07-14 12:49:45	AUTHPRIV	Hinweis	Webconfig: login via HTTP from 192.168.2.179.
2	2014-07-14 12:49:44	AUTHPRIV	Hinweis	Webconfig: login failure via HTTP from 192.168.2.179.
3	2014-07-14 12:49:12	AUTHPRIV	Hinweis	Webconfig: login via HTTP from 192.168.2.4.
4	2014-07-14 12:38:17	AUTHPRIV	Hinweis	Webconfig: login via HTTP from 192.168.2.179.
5	2014-07-14 12:38:12	AUTHPRIV	Hinweis	Webconfig: login failure via HTTP from 192.168.2.179.
6	2014-07-13 15:23:53	KERN	Hinweis	SNTP: Local time set to 2014-07-13 13:23:53 (UTC)
7	2014-07-12 15:23:57	KERN	Hinweis	SNTP: Local time set to 2014-07-12 13:23:57 (UTC)
8	2014-07-11 16:24:03	AUTHPRIV	Hinweis	Webconfig: user logout from 89.0.95.133
9	2014-07-11 15:24:02	KERN	Hinweis	SNTP: Local time set to 2014-07-11 13:24:02 (UTC)
10	2014-07-11 15:12:55	AUTHPRIV	Hinweis	User from 192.168.2.231 via SSH logged out
11	2014-07-11 15:07:17	AUTHPRIV	Hinweis	Login from 192.168.2.231 via SSH
12	2014-07-11 15:06:37	AUTHPRIV	Hinweis	Webconfig: login via HTTP from 89.0.95.133.
13	2014-07-11 15:06:33	AUTHPRIV	Hinweis	Webconfig: login failure via HTTP from 89.0.95.133.

2.7.1 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-Stufen sind im Gerät auf fünf Stufen reduziert. Die nachfolgende Tabelle zeigt die Zuordnung zwischen dem Alarmlevel, Bedeutung und SYSLOG-Severities.

Priorität	Bedeutung	SYSLOG-Severity
Alarm	Hierunter werden alle Meldungen zusammengefasst, die der erhöhten Aufmerksamkeit des Administrators bedürfen.	PANIC, ALERT, CRIT
Fehler	Auf diesem Level werden alle Fehlermeldungen übermittelt, die auch im Normalbetrieb auftreten können, ohne dass ein Eingriff des Administrators notwendig wird (z. B. Verbindungsfehler).	ERROR
Warning	Dieser Level übermittelt Fehlermeldungen, die den ordnungsgemäßen Betrieb des Geräts nicht beeinträchtigen.	WARNING
Information	Auf diesem Level werden alle Nachrichten übermittelt, die rein informellen Charakter haben (z. B. Accounting-Informationen).	NOTICE, INFORM
Debug	Übertragung aller Debug-Meldungen. Debug-Meldungen erzeugen ein erhebliches Datenvolumen und beeinträchtigen den ordnungsgemäßen Betrieb des Geräts. Sie sollten daher im Regelbetrieb ausgeschaltet sein und nur zur Fehlersuche verwendet werden.	DEBUG

Die folgende Tabelle gibt eine Übersicht über die Bedeutung aller internen Nachrichtenquellen, die Sie im Gerät einstellen können. Zusätzlich gibt Ihnen die letzte Spalte der Tabelle die standardmäßige Zuordnung zwischen den internen Quellen des Geräts und den SYSLOG-Facilities an. Diese Zuordnung kann bei Bedarf verändert werden.

Quelle	Bedeutung	Facility
System	Systemmeldungen (Bootvorgänge, Timersystem etc.)	KERNEL
Logins	Meldungen sowohl über den erfolgreichen Verbindungsauf- und -abbau als auch über Login und Logout eines Users während der PPP-Verhandlung sowie dabei auftretende Fehler	AUTH
Systemzeit	Meldungen über Änderungen der Systemzeit	CRON
Konsolen-Logins	Meldungen über Konsolen-Logins (Telnet, Outband, etc), Logouts und dabei auftretende Fehler	AUTHPRIV
Verbindungen	Meldungen über auftretende Fehler beim Verbindungsauf- und -abbau (Display-Trace)	LOCAL0
Accounting	Accounting-Informationen nach dem Abbau einer Verbindung (User, Onlinezeit, Transfervolumen)	LOCAL1
Verwaltung	Meldungen über Konfigurationsänderungen, remote ausgeführte Kommandos etc.	LOCAL2
Router	Regelmäßige Statistiken über die am häufigsten genutzten Dienste (nach Portnummern aufgeschlüsselt) sowie Meldungen über gefilterte Pakete, Routing-Fehler etc.	LOCAL3

Header

Der Header beinhaltet den Namen oder die IP-Adresse des Gerätes, von dem die SYSLOG-Nachricht empfangen wurde. Für die Auswertung der Nachrichten ist auch die zeitliche Abfolge sehr wichtig. Um die zeitliche Konsistenz der Meldungen nicht durch unterschiedliche Gerätezeiten zu stören, wird die Zeitinformation erst beim SYSLOG-Client in die Nachrichten eingefügt.

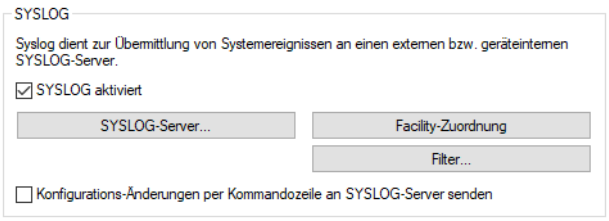
Für die Auswertung der SYSLOG-Meldungen im internen Speicher müssen die Geräte über eine gültige Zeitinformation verfügen.

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.

2.7.2 SYSLOG konfigurieren

In LANconfig konfigurieren Sie SYSLOG unter **Meldungen/Monitoring** > **Protokolle** im Abschnitt **SYSLOG**.



SYSLOG aktiviert

Aktivieren Sie das SYSLOG-Protokoll.

Konfigurations-Änderungen per Kommandozeile an SYSLOG-Server senden

Über das Kommandozeilen-Interface vorgenommene Konfigurations-Änderungen werden per SYSLOG an die eingerichteten Server gesendet.

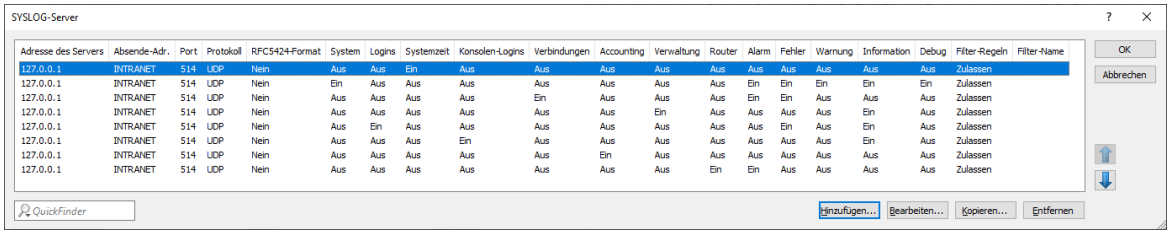
Diese Protokollierung umfasst ausschließlich die an der Konsole ausgeführten Befehle. Konfigurationsänderungen und Aktionen über LANconfig oder Webconfig sind davon nicht erfasst.

SYSLOG-Server

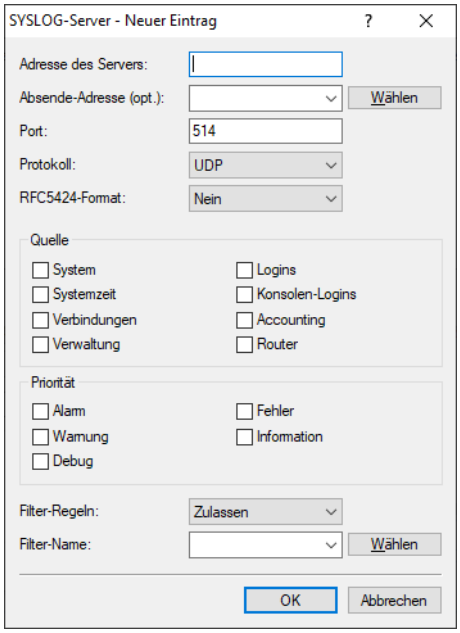
In LANconfig konfigurieren Sie die Einstellungen zum SYSLOG-Server unter **Meldungen/Monitoring** > **Protokolle** > **SYSLOG** über **SYSLOG-Server**.

Klicken Sie auf **SYSLOG-Server**, um die vorhandenen SYSLOG-Einträge anzuzeigen.

Die Tabelle der SYSLOG-Einträge ist im Auslieferungszustand mit sinnvollen Einstellungen vorbelegt, um wichtige Ereignisse für die Diagnose im internen SYSLOG-Speicher abzulegen. Diese Einstellungen entsprechen den Vorgaben aus der UNIX-Welt, aus der SYSLOG ursprünglich kommt. Der folgende Screenshot zeigt diese vordefinierten SYSLOG-Einträge unter LANconfig:



Klicken Sie auf **Hinzufügen** bzw. markieren Sie einen Eintrag und klicken Sie auf **Bearbeiten**.



Adresse des Servers

Legen Sie die IP-Adresse des SYSLOG-Servers fest. Die Angabe ist möglich in Form einer IPv4- / IPv6-Adresse oder eines Hostnamens.

Absende-Adresse (opt.)

Konfigurieren Sie optional eine Absende-Adresse, die der SYSLOG-Client statt der ansonsten automatisch für die Zieladresse gewählten Absende-Adresse verwendet. Falls Sie z. B. Loopback-Adressen konfiguriert haben, können Sie diese hier als Absende-Adresse angeben.

Port

Definiert die Portnummer (z. B. 514 für TCP / UDP).

Protokoll

Definiert das verwendete Protokoll. Mögliche Werte:

UDP

User Datagram Protocol

TCP

Transmission Control Protocol

TLS

Der Syslog-Client unterstützt drei Szenarien im TLS-Modus:

1. Der Syslog-Client akzeptiert alle TLS-Server-Zertifikate des Syslog-Servers. Dazu wird im Router kein vertrauenswürdiges CA-Zertifikat hinterlegt.
2. Der Syslog-Client akzeptiert nur Server-Zertifikate, die von einer vertrauenswürdigen CA signiert wurden. Dazu muss das CA-Zertifikat in den entsprechenden Zertifikatsslot des Routers hochgeladen werden.
3. Der Syslog-Client authentifiziert sich mit einem TLS-Client-Zertifikat beim Syslog-Server und der Syslog-Server authentifiziert sich mit seinem CA-Zertifikat. Dazu muss sowohl das TLS-Client-Zertifikat für den Router und das CA-Zertifikat in den entsprechenden Zertifikatsslot des Routers hochgeladen werden, z. B. in einem Container als PKCS#12-Datei.

Zertifikate für Syslog können entweder über die WEBconfig oder per LANconfig in das Gerät geladen werden.

- **LANconfig**:**Rechtsklick auf das Gerät** > **Konfigurationsverwaltung** > **Zertifikat oder Datei hochladen**
  - **Syslog - Container als PKCS12-Datei** oder
  - **Syslog - Root CA Zertifikat**
- **WEBconfig**: **Extras** > **Dateimanagement** > **Zertifikat oder Datei hochladen** > **Dateityp**
  - **Syslog - Container als PKCS12-Datei** oder
  - **Syslog - Root CA Zertifikat**

RFC5424-Format

Definiert, ob der Syslog-Client Nachrichten im RFC5424-Format an den Syslog-Server senden soll.

Quelle

Die folgende Tabelle gibt eine Übersicht über die Bedeutung aller Nachrichtenquellen, die Sie im Gerät einstellen können. Zusätzlich gibt Ihnen die letzte Spalte der Tabelle die Zuordnung zwischen den internen Quellen des Geräts und den SYSLOG-Facilities an.

Quelle	Bedeutung	Facility
System	Systemmeldungen (Bootvorgänge, Timersystem etc.)	KERNEL
Logins	Meldungen über Login und Logout eines Users während der PPP-Verhandlung sowie dabei auftretende Fehler	AUTH
Systemzeit	Meldungen über Änderungen der Systemzeit	CRON
Konsolen-Logins	Meldungen über Konsolen-Logins (Telnet, Outband, etc), Logouts und dabei auftretende Fehler	AUTHPRIV
Verbindungen	Meldungen über den Verbindungsauf- und -abbau sowie dabei auftretende Fehler (Display-Trace)	LOCAL0
Accounting	Accounting-Informationen nach dem Abbau einer Verbindung (User, Onlinezeit, Transfervolumen)	LOCAL1
Verwaltung	Meldungen über Konfigurationsänderungen, remote ausgeführte Kommandos etc.	LOCAL2
Router	Regelmäßige Statistiken über die am häufigsten genutzten Dienste (nach Portnummern aufgeschlüsselt) sowie Meldungen über gefilterte Pakete, Routing-Fehler etc.	LOCAL3

Priorität

Die im SYSLOG ursprünglich definierten acht Prioritätsstufen sind im Gerät auf fünf Stufen reduziert. Die nachfolgende Tabelle zeigt die Zuordnung zwischen Alarmlevel, Bedeutung und SYSLOG-Prioritäten.

Priorität	Bedeutung	SYSLOG-Priorität
Alarm	Hierunter werden alle Meldungen zusammengefasst, die der erhöhten Aufmerksamkeit des Administrators bedürfen.	PANIC, ALERT, CRIT
Fehler	Auf diesem Level werden alle Fehlermeldungen übermittelt, die auch im Normalbetrieb auftreten können, ohne dass ein Eingriff des Administrators notwendig wird (z. B. Verbindungsfehler).	ERROR
Warnung	Dieser Level übermittelt Fehlermeldungen, die den ordnungsgemäßen Betrieb des Geräts nicht beeinträchtigen.	WARNING
Information	Auf diesem Level werden alle Nachrichten übermittelt, die rein informellen Charakter haben (z. B. Accounting-Informationen).	NOTICE, INFORM
Debug	Übertragung aller Debug-Meldungen. Debug-Meldungen erzeugen ein erhebliches Datenvolumen und beeinträchtigen den ordnungsgemäßen Betrieb des Geräts. Sie	DEBUG

Priorität	Bedeutung	SYSLOG-Priorität
	sollten daher im Regelbetrieb ausgeschaltet sein und nur zur Fehlersuche verwendet werden.	

Filter-Regeln

Werden die Syslog-Meldungen an einen oder mehrere Server übertragen, indem Einstellungen für den Empfang bestimmter Meldungen konfiguriert wurden, so werden alle konfigurierten Meldungen mit der konfigurierten Quelle und Priorität an die Server übertragen. Mitunter ist es jedoch wünschenswert, bestimmte Meldungen für die Server auszufiltern, nur bestimmte Meldungen überhaupt zu schicken oder auch deren Quelle und Priorität zu verändern, falls sie im Serverlog eine andere Gewichtung erhalten sollen. Der Syslog-Filter erlaubt es, Meldungen in Abhängigkeit von Quelle, Priorität und / oder Meldungstext zu filtern. Dabei stellen Sie hier ein, ob die Meldungen, die über den im folgenden Feld eingestellten Filter bestimmt werden, zugelassen oder abgelehnt werden.

Filter-Name

Wählen Sie einen der konfigurierten Filter aus.

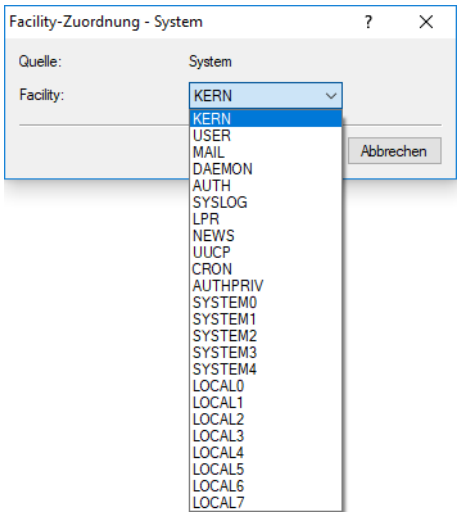
Wenn Sie alle Parameter definiert haben, bestätigen Sie die Eingaben mit **OK**. In der SYSLOG-Tabelle erscheint der SYSLOG-Client mit seinen Parametern.

SYSLOG-Facilities zuordnen

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

Die standardmäßige Zuordnung ist bei Bedarf veränderbar. So lassen sich z. B. alle SYSLOG-Meldungen eines Geräts mit einer bestimmten Facility (Local7) versenden. Mit der entsprechenden Konfiguration des SYSLOG-Clients können Sie so alle Meldungen in einer gemeinsamen Log-Datei sammeln.

Über **Meldungen/Monitoring** > **Protokolle** lassen sich im Abschnitt **SYSLOG** unter **Facility-Zuordnung** die internen Quellen den entsprechenden SYSLOG-Facilities zuordnen.



Hier können Sie alle Meldungen vom Gerät einer Facility zuordnen und dadurch können diese vom SYSLOG-Client ohne zusätzlichen Aufwand in eine spezielle Log-Datei geschrieben werden.

Alle Facilities werden auf 'local7' gesetzt. Unter Linux werden nun in der Datei `/etc/syslog.conf` durch den Eintrag

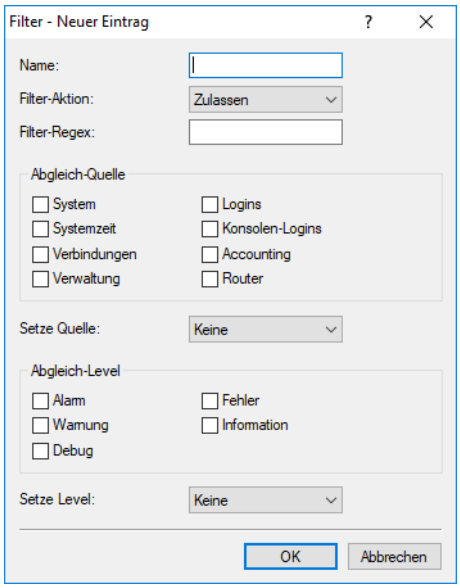
```
local7.* /var/log/lancom.log
```

alle Ausgaben des Geräts in die Datei `/var/log/lancom.log` geschrieben.

Filter

Werden die Syslog-Meldungen an einen oder mehrere Server übertragen, indem Einstellungen für den Empfang bestimmter Meldungen konfiguriert wurden, so werden alle konfigurierten Meldungen mit der konfigurierten Quelle und Priorität an die Server übertragen. Mitunter ist es jedoch wünschenswert, bestimmte Meldungen für die Server auszufiltern, nur bestimmte Meldungen überhaupt zu schicken oder auch deren Quelle und Priorität zu verändern, falls sie im Serverlog eine andere Gewichtung erhalten sollen. Der Syslog-Filter erlaubt es, Meldungen in Abhängigkeit von Quelle, Priorität und / oder Meldungstext zu filtern. Konfigurieren Sie hier diese Filter, die Sie dann bei Einträgen des SYSLOG-Servers verwenden können.

In LANconfig konfigurieren Sie die Filtereinstellungen zum SYSLOG-Server unter **Meldungen/Monitoring** > **Protokolle** > **SYSLOG** über **Filter**.



Name

Geben Sie diesem Filter einen aussagekräftigen Namen. Es können mehrere Regeln mit demselben Filter-Namen angelegt werden. Diese werden dann in der Reihenfolge, in der sie in der Filter-Tabelle angelegt werden, beim Versenden der Nachrichten geprüft. Trifft keine Regel in dieser Filterkette zu, wird die Nachricht gemäß der in der Server-Tabelle eingetragenen Default-Policy für den Server versendet oder verworfen.

Filter-Aktion

Aktion, falls die Regel zutrifft; „Zulassen“ erlaubt das Versenden der Meldung an den Server, „Ablehnen“ verwirft die Meldung.

Filter-Regex

Regulärer Ausdruck in Perl-Syntax (siehe z. B. *Regular expressions in Perl*), auf den der Meldungstext zutreffen muss. Ein leerer String bedeutet, dass der Meldungstext nicht betrachtet wird und daher alle Meldungstexte zutreffen.

Abgleich-Quelle

Quelle der Meldung, für die diese Regel gilt. Der Wert „keine“ steht für eine beliebige Quelle.

Setze Quelle

Neue Quelle der Meldung, falls die Regel zutrifft. Der Wert „Keine“ bedeutet, dass die Quelle nicht verändert wird.

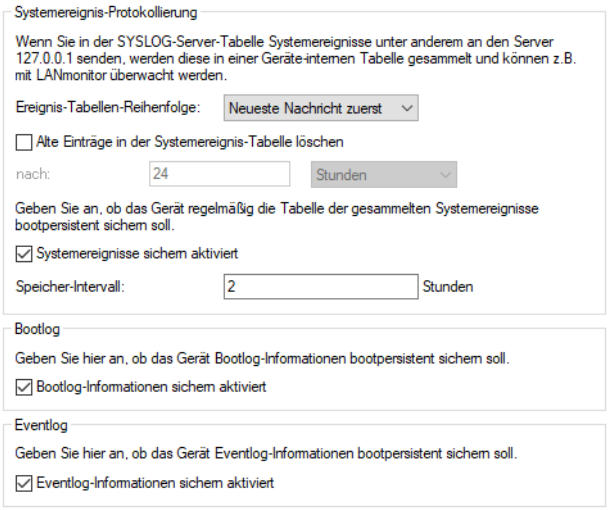
Abgleich-Level

Priorität der Meldung, für die diese Regel gilt. Der Wert „keine“ steht für eine beliebige Priorität.

Setze Level

Neue Priorität der Meldung, falls die Regel zutrifft. Der Wert „Keine“ bedeutet, dass die Priorität nicht verändert wird.

Systemereignis-Protokollierung



Speicherfrist von Systemereignissen festlegen

Unter **Meldungen/Monitoring** > **Systemereignisse** > **Systemereignis-Protokollierung** bestimmen Sie, für wie lange das Gerät Systemereignisse speichert. Markieren Sie dazu die Option **Alte Einträge in der Systemereignis-Tabelle löschen** und defnieren Sie eine Zeit (0-9999) in Stunden, Tagen oder Monaten.

Ein Monat entspricht hierbei 30 Tagen.

SYSLOG, Eventlog und Bootlog bootpersistent

Die Einstellungen für das bootpersistente Speichern von SYSLOG-, Eventlog- und Bootlog-Nachrichten finden Sie (sofern für Ihr Gerät verfügbar) unter **Meldungen/Monitoring** > **Systemereignisse** Aktivieren Sie dazu die folgenden Optionen:

- SYSLOG: **Systemereignisse sichern aktiviert**

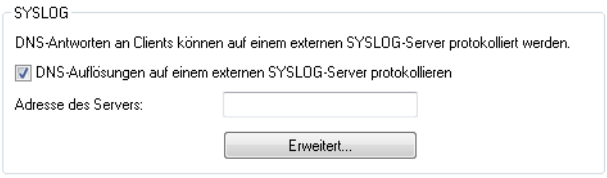
  Über den Eintrag **Speicher-Intervall** geben Sie die Zeitspanne in Stunden an, nach der die SYSLOG-Systemereignisse bootpersistent gesichert werden.
- Bootlog: **Bootlog-Informationen sichern aktiviert**
- Eventlog: **Eventlog-Informationen sichern aktiviert**

DNS-Anfragen und -Antworten an externen Syslog-Servern dokumentieren

Der DNS-Server in LANCOM Geräten löst DNS-Anfragen von Clients auf. Eine Übersicht darüber, welche Clients welche Namen angefragt und welche Antworten sie erhalten haben, steht im Syslog zur Verfügung.

Das Syslog des Routers / Access Points selbst kann nicht genutzt werden. Es ist daher erforderlich, einen externen Syslog-Server einzutragen.

Die Konfiguration des DNS-Loggings erfolgt im LANconfig unter **DNS** > **Allgemein** im Abschnitt **SYSLOG**.



DNS-Auflösungen auf einem externen SYSLOG-Server protokollieren

Markieren Sie diese Option, um das DNS-Logging zu aktivieren.

Diese Option ist unabhängig von der Einstellung im Syslog-Modul. Auch bei aktiviertem DNS-Logging und deaktiviertem Syslog-Modul (Einstellung unter **Meldungen** > **Allgemein** im Abschnitt **SYSLOG**) erfolgt das DNS-Logging.

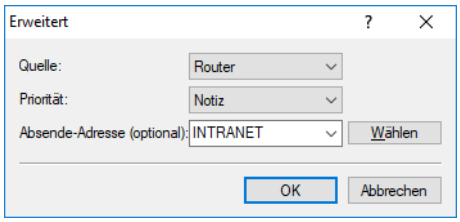
Die entsprechende SYSLOG-Meldung hat den folgenden Aufbau:

```
PACKET_INFO: DNS for <IP-Address>, TID {Hostname}: Resource-Record
```

Adresse des Servers

Enthält die IP-Adresse oder den DNS-Namen des zu nutzenden SYSLOG-Servers.

Die Einstellungen hinter der Schaltfläche **Erweitert** beeinflussen die Inhalte der SYSLOG-Meldungen.



Quelle

Enthält die Log-Quelle, die in den SYSLOG-Meldungen erscheint.

Priorität

Enthält den Log-Level, der in den SYSLOG-Meldungen erscheint.

Absende-Adresse (optional)

Enthält die Absende-Adresse, die in den SYSLOG-Meldungen erscheint.

2.7.3 Bedeutung von SYSLOG-Meldungen

Erweiterte Statusanzeige des Einbuchvorgangs ins Mobilfunknetz

Um Probleme bei der Verbindung in ein Mobilfunknetz schneller analysieren zu können, führen WWAN-fähige Router alle Einbuchvorgänge im SYSLOG auf. Somit kann der Anwender z. B. erkennen, ob und warum der Mobilfunkprovider eine Verbindung ablehnt.

Das Gerät erzeugt bei den folgenden Ereignissen je einen SYSLOG-Eintrag:

Status	Bedeutung	SYSLOG-Severity
WWAN: Currently not searching for network	Das Modem ist nicht eingebucht und sucht derzeit nicht nach einem Funknetz.	INFORM

Status	Bedeutung	SYSLOG-Severity
WWAN: Searching for network	Das Modem ist nicht eingebucht und sucht nach einem Funknetz.	INFORM
WWAN: Registered to home network	Das Modem hat sich erfolgreich ins Funknetz seines Mobilfunkproviders eingebucht.	INFORM
WWAN: Registered to foreign network	Das Modem hat sich erfolgreich ins Funknetz eines Roaming-Partners seines Mobilfunkproviders eingebucht.	INFORM
WWAN: Unknown registration	Initialwert. Das Modem hat noch keine Rückmeldung vom Funkmodul über den Einbuchungsstatus erhalten.	INFORM
WWAN: Network registration denied	Der Mobilfunkprovider hat die Einbuchung ins Funknetz abgelehnt.	ERROR
WWAN: Lost network registration	Das Modem hat die Verbindung zum eingebuchten Funknetz verloren.	NOTICE
WWAN: Failed to set network	Das Modem hat den Befehl zum Setzen des Netzwerks mit einer Fehlermeldung beantwortet. Dieser Fehler tritt z. B. auf, wenn das Netzwerk unerreichbar ist oder nicht existiert, oder ein Fehler im Gerät vorliegt.	ERROR
WWAN: Failed to set network mode	Das Modem hat den Befehl zum Setzen des Netzwerkmodus mit einer Fehlermeldung beantwortet. Dieser Fehler tritt z. B. auf, wenn das Netzwerk unerreichbar ist oder nicht existiert, oder ein Fehler im Gerät vorliegt.	ERROR
WWAN: Using modem '...'.	Zeigt das verwendete Modem an.	INFORM
WWAN: Modem is gone.	Modem ist nicht mehr verfügbar.	INFORM
WWAN: Resetting modem.	Re-Init durch Modem-Reset	WARNING
WWAN: Local disconnect.	D-Kanal-Disconnect	INFORM
WWAN: Local disconnect (Release).	D-Kanal-Release	INFORM
WWAN: Force 2G mode at ... dB.	Modem startet den 2G-Fallback	NOTICE
WWAN: Ending forced 2G mode.	Modem beendet den 2G-Fallback	INFO
WWAN: Forced 2G mode disabled.	Der 2G-Fallback-Modus ist deaktiviert.	INFO
WWAN: PIN missing in profile.	PIN fehlt im Profil.	ERROR
WWAN: PUK required.	Modem fordert PUK.	ERROR
WWAN: Invalid PIN.	Falsche PIN	ERROR
WWAN: Failed to set APN	Fehler beim Setzen des APN. Das Modem hat den Befehl zum Setzen eines APNs mit einer Fehlermeldung beantwortet. Dieser Fehler tritt z. B. auf, wenn das Netzwerk unerreichbar ist bzw. nicht existiert oder ein Fehler im Gerät vorliegt.	ERROR
WWAN: Using profile '...'.	Name des verwendeten Profils.	NOTICE
WWAN: Can not find profile '...'.	Profil nicht vorhanden.	ERROR
WWAN: Disonnected.	Physikalische Verbindung beendet.	INFORM

Status	Bedeutung	SYSLOG-Severity
WWAN: Connected: '...'.	Das Modem hat eine Datenverbindung zum Netzwerk hergestellt und kann ab jetzt Daten über das Mobilfunk-Netzwerk übertragen.	INFORM
WWAN: Cell-ID is ..., Local Area Code is	Funkzellen-ID und Ländercode.	INFORM
WWAN: Current Network is '...'.	Netzwerk (Text)	INFORM
WWAN: Current Network is	Netzwerk (Nummer)	INFORM
WWAN: Mode ..., Band '...'.	Anzeige von Netzwerk-Modus und Band	INFORM
WWAN: Mode ..., Band '...', Bandwith in MHz: ..., Channel (Rx/Tx): .../....	Anzeige von Netzwerk-Modus, Band, Bandbreite sowie Kanal (Empfangs- und Senderichtung).	INFORM
WWAN: Mode ..., Band '...', Channel (Rx/Tx): .../....	Anzeige von Netzwerk-Modus, Band sowie Kanal (Empfangs- und Senderichtung).	INFORM
WWAN: Max. Datarate (Ds/Us): .../....	Aktuelle QoS-Datenrate (Down- und Upstream)	INFORM
WWAN: Network mode is '...'.	Aktueller Modus. Mögliche Werte sind: › GPRS › EDGE › UMTS › HSPA › LTE	INFORM
WWAN: Signal strength is ... dBm.	Aktuelle Signalstärke	INFORM
WWAN: Using stored APN. APN: '...', PDP type:	Aktuell verwendeter Zugangspunkt im Netzwerk.	INFORM
WWAN: Setting new APN. APN: '...', PDP type:	Wechsel des Netzwerk-Zugangspunktes	INFORM
WWAN: Temperature is ...°C.	Aktuelle Modultemperatur	INFORM
WWAN: Temperature status: '...'.	Aktueller Temperaturstatus des Moduls. Mögliche Werte sind: › Normal › High Warning › High Critical › Low Critical	INFORM (Normal), WARNING (High Warning), CRITICAL (High Critical, Low Critical)
WWAN: Closing device: '...'.	Das Gerät, über das die Verbindung ins WAN läuft, fährt herunter.	INFORM
WWAN: Hangup: '...'.	Das Modem beendet die Netzwerk-Verbindung.	INFORM
WWAN: Error in modem init: '___'.	Bei der Initialisierung des Modems ist ein Fehler aufgetreten.	ERROR

Dokumentation von Ereignissen auf den xDSL-Schnittstellen

Das Gerät erzeugt bei den folgenden xDSL-Schnittstellen-Ereignissen je einen SYSLOG-Eintrag:

Status	Bedeutung	SYSLOG-Severity
xDSL: Booting modem: ...	Das Modem startet neu.	NOTICE

Status	Bedeutung	SYSLOG-Severity
xDSL: Set up line to <Leitungsmodus>/<Leitungstyp>	Das xDSL-Modul baut die Verbindung mit dem angegebenen Modus und Typ auf. Folgende Werte sind möglich: › Leitungsmodus: Disabled, Auto sowie alle unter **Setup** > **Schnittstellen** > **ADSL-Interface bzw. VDSL-Interface** konfigurierbaren Modi. › Leitungstyp: POTS, ISDN	INFORM
xDSL: Line is up. DS-Rate: ..., US-Rate: ..., DS-Margin: ..., US-Margin: ..., DS-Attn: ..., US-Attn: ..., Mode: ..., Profile:	Das Modem hat die Verbindung erfolgreich mit angegebenen Werten aufgebaut.	NOTICE
xDSL: Line data update. DS-Rate: ..., US-Rate: ..., DS-Margin: ..., US-Margin: ..., DS-Attn: ..., US-Attn: ..., Mode: ..., Profile: ...	Nach einer Synchronisation nehmen Modem und DSLAM eine Optimierung der xDSL-Verbindung vor. Dadurch können sich ggf. die Leitungswerte ändern. Nach einer Minute gibt das Modem die aktuellen Leitungswerte aus.	NOTICE
xDSL: Line data update.	Nach einer Synchronisation nehmen Modem und DSLAM eine Optimierung der xDSL-Verbindung vor. Nach einer Minute gibt das Modem diese Meldung aus, wenn sich die Leitungswerte nach der Synchronisation nicht geändert haben.	NOTICE
xDSL: Line disconnected due to	Die Verbindung ist aus dem angegebenem Grund abgebrochen. Folgende Werte sind möglich: › modem reboot › retrain › silence › high line error rate › protocol setting › line type setting › automode line type switch › modem timeout › VC parameter change	NOTICE
xDSL: SNR margin (dB, Down/Up): .../...	Der Wert zwischen notwendigem und gemessenem Signal-Rausch-Abstand (SNR) hat sich um mehr als 1dB geändert.	INFORM