Addendum LCOS 8.82

LCOS
[LANCOM OPERATING SYSTEM]

LANCOM
Systems

Inhalt

1 Addendum zur LCOS-Version 8.82

Dieses Dokument beschreibt die Änderungen und Ergänzungen in der LCOS-Version 8.82 gegenüber der vorherigen Version.

2 Routing und WAN-Verbindungen

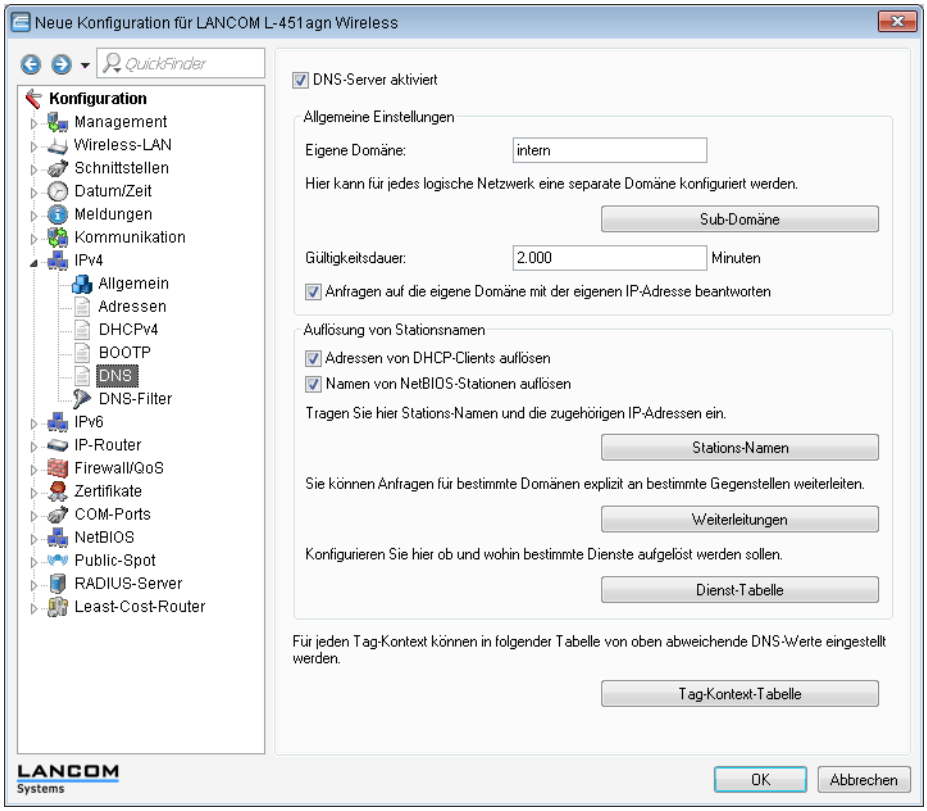
2.1 DNS-Weiterleitung pro ARF-Kontext konfigurierbar

Ab LCOS-Version 8.82 sind bei der DNS-Weiterleitung mehrere voneinander unabhängige Forwarding-Definitionen (insbesondere allgemeine Wildcard-Definitionen mit "*") durch die Kennzeichnung mit eindeutigen Routing-Tags möglich. Abhängig vom Routing-Kontext des anfragenden Clients berücksichtigt der Router nur die passend gekennzeichneten Forwarding-Einträge sowie die allgemeinen, mit "0" gekennzeichneten Einträge.

2.1.1 Advanced Routing and Forwarding (ARF)

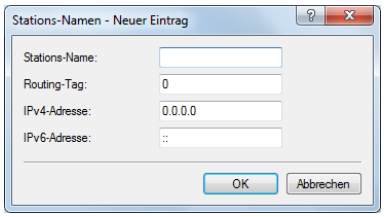
Routing-Tags für DNS-Weiterleitung

Bei der DNS-Weiterleitung sind mehrere voneinander unabhängige Forwarding-Definitionen (insbesondere allgemeine Wildcard-Definitionen mit "*") durch die Kennzeichnung mit eindeutigen Routing-Tags möglich. Abhängig vom Routing-Kontext des anfragenden Clients berücksichtigt der Router nur die passend gekennzeichneten Forwarding-Einträge sowie die allgemeinen, mit "0" gekennzeichneten Einträge.



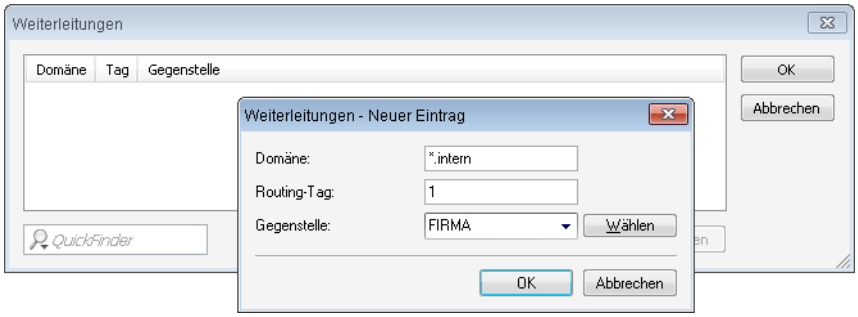
Stations-Namen

Unter **Konfiguration** > **IPv4** > **DNS** > **Stations-Namen** definieren Sie, welche Stations-Namen das Gerät wie und in welchem Tag-Kontext auflöst.



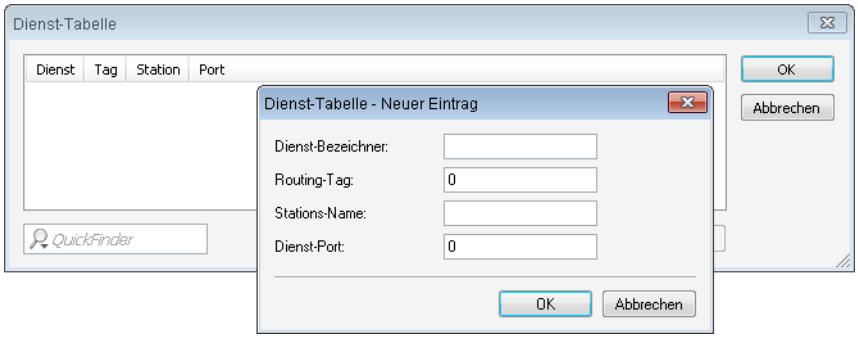
DNS-Weiterleitungen

Unter **Konfiguration** > **IPv4** > **DNS** > **Weiterleitungen** versehen Sie Weiterleitungsregeln mit Routing-Tags, so dass diese nur mit dem korrekten Routing-Tag zur Verfügung stehen.



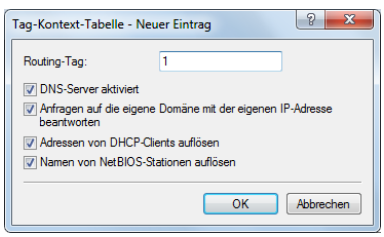
Dienst-Tabelle

Unter **Konfiguration** > **IPv4** > **DNS** > **Dienst-Tabelle** versehen Sie Dienste mit Routing-Tags, so dass diese nur mit dem korrekten Routing-Tag erreichbar sind.



Tag-Kontext-Tabelle

Im LANconfig lassen sich unter **Konfiguration** > **IPv4** > **DNS** > **Tag-Kontext-Tabelle** Tag-Kontexte definieren, die die globalen Einstellungen des DNS-Servers für bestimmte Schnittstellen- und Routing-Tags (Routing-Kontext) überschreiben:



Wenn ein Eintrag für einen Tag-Kontext existiert, dann gelten für diesen Kontext nur die DNS-Einstellungen in dieser Tabelle. Existiert hingegen kein Eintrag in dieser Tabelle, dann gelten die globalen Einstellungen des DNS-Servers.

Folgende Optionen sind je Tag-Kontext möglich:

- **Routing-Tag**: Eindeutiges Schnittstellen- bzw. Routing-Tag im Bereich von 1-65535, dessen folgende Einstellungen die globalen Einstellungen des DNS-Servers überschreiben sollen.
- **DNS-Server aktiviert**: Aktiviert den DNS-Server des Gerätes.
- **Anfragen auf die eigene Domäne mit der eigenen IP-Adresse beantworten**: Wenn aktiviert, werden DNS-Anfragen betreffs der eigenen Domäne mit der IP-Adresse des Routers beantwortet.
- **Adressen von DHCP-Clients auflösen**: Aktiviert die Auflösung von Stations-Namen, die über DHCP eine IP-Adresse angefordert haben.
- **Namen von NetBIOS-Stationen auflösen**: Aktiviert die Auflösung von Stations-Namen, die dem NetBIOS-Router bekannt sind.

2.1.2 Ergänzungen im Setup-Menü

Rtg-Tag

Das Routing-Tag legt bei einer Station fest, in welchem Tag-Kontext das Gerät den Stationsnamen auflöst.

SNMP-ID:

2.17.5.4

Pfad Telnet:

Setup > **DNS** > **DNS-Liste**

Mögliche Werte:

0 bis 65535

Default:

0

Rtg-Tag

Das Routing-Tag legt fest, welche Filter im jeweiligen Tag-Kontext gelten.

SNMP-ID:

2.17.6.6

Pfad Telnet:

Setup > **DNS** > **Filter-Liste**

Mögliche Werte:

0 bis 65535

Default:

0

Rtg-Tag

Das Routing-Tag ermöglicht es, mehrere voneinander unabhängige Forwarding-Definitionen zu bestimmen (insbesondere allgemeine Wildcard-Definitionen mit "*"). Abhängig vom Routing-Kontext des anfragenden Clients berücksichtigt der Router nur die passend gekennzeichneten Forwarding-Einträge sowie die allgemeinen, mit "0" gekennzeichneten Einträge.

SNMP-ID:

2.17.9.3

Pfad Telnet:

Setup > **DNS** > **DNS-Weiterleitungen**

Mögliche Werte:

0 bis 65535

Default:

0

Rtg-Tag

Das Routing-Tag legt fest, ob und wie der Router bestimmte Dienstanfragen im jeweiligen Tag-Kontext auflösen soll.

SNMP-ID:

2.17.10.4

Pfad Telnet:

Setup > **DNS** > **Service-Location-Liste**

Mögliche Werte:

0 bis 65535

Default:

0

2.2 Quell-Tags für Firewall-Regeln

2.2.1 Ergänzungen im Setup-Menü

Quell-Tag

Das Quell-Tag (erwartetes Schnittstellen- bzw. Routing-Tag) dient zur Identifikation des ARF-Kontextes aus dem ein Paket empfangen wurde. Dieses kann zur Einschränkung von Firewall-Regeln auf bestimmte ARF-Kontexte verwendet werden.

SNMP-ID:

2.8.10.2.15

Pfad Telnet:

Setup > **IP-Router** > **Firewall** > **Regel-Tabelle**

Mögliche Werte:

0…65535

Erläuterung:

- 65535: Die betreffende Firewall-Regel wird angewandt, wenn das erwartete Schnittstellen- bzw. Routing-Tag 0 ist.
- 1…65534: Die betreffende Firewall-Regel wird angewandt, wenn das erwartete Schnittstellen- bzw. Routing-Tag 1…65534 ist.
- 0: Wildcard. Die betreffende Firewall-Regel wird auf alle ARF-Kontexte angewandt (erwartetes Schnittstellen- bzw. Routing-Tag 0…65535).

Default:

0

3 VPN

3.1 Hashfunktion SHA2-256 über LANconfig auswählbar

Ab LCOS-Version 8.82 können Sie für entsprechend ausgestattete Geräte bei IKE- und IPsec-Proposals über LANconfig auch den Hash-Algorithmus 'SHA-2-256' auswählen.

3.1.1 LANCOM VPN im Überblick

Funktionen von LANCOM VPN

In diesem Abschnitt sind alle Funktionen und Eigenschaften von LANCOM VPN aufgelistet. Experten im im Bereich VPN bietet er eine stark komprimierte Zusammenfassung über die Leistungsfähigkeit der Funktion. Das Verständnis der verwendeten Fachtermini setzt allerdings solide Kenntnisse über die technischen Grundlagen von VPN voraus. Für die Inbetriebnahme und den Normalbetrieb von LANCOM VPN sind diese Informationen jedoch nicht erforderlich.

- VPN nach dem IPSec-Standard
- VPN-Tunnel über Festverbindung, Wählverbindung und IP-Netzwerk
- IKE Main- und Aggressive Modus
- LANCOM Dynamic VPN: Öffentliche IP-Adresse können statisch oder dynamisch sein (für den Aufbau zu Gegenstellen mit dynamischer IP-Adresse ist eine ISDN-Verbindung erforderlich)
- IPSec-Protokolle ESP, AH und IPCOMP im Transport- und Tunnelmodus
- Hash-Algorithmen:
  - HMAC-MD5-96, Hashlänge 128 Bits
  - HMAC-SHA-1-96, Hashlänge 160 Bits
  - HMAC-SHA-2-256, Hashlänge 256 Bits
- Symmetrische Verschlüsselungsverfahren
  - AES, Schlüssellänge 128, 192 und 256 Bits
  - Triple-DES, Schlüssellänge 168 Bits
  - Blowfish, Schlüssellänge 128-448 Bits
  - CAST, Schlüssellänge 128 Bits
  - DES, Schlüssellänge 56 Bits
- Kompression mit „Deflate“ (ZLIB) und LZS
- IKE Config Mode
- IKE mit Preshared Keys
- IKE mit RSA-Signature und digitalen Zertifikaten (X.509)
- Schlüsselaustausch über Oakley, Diffie-Hellman-Algorithmus mit Schlüssellänge 768 Bits, 1024 Bits, 1536 Bits und 2048 Bits (well known groups 1, 2, 5 und 14)
- Schlüsselmanagement nach ISAKMP

3.1.2 Ergänzungen im Setup-Menü

IKE-Auth-Alg

Hash-Verfahren zur Abbildung der Verschlüsselung

SNMP-ID:

2.19.4.11.4

Pfad Telnet:

Setup > **VPN** > **Proposals** > **IKE**

Mögliche Werte:

MD5

SHA1

SHA2-256

Default:

MD5

ESP-Auth-Alg

ESP-Authentifizierungsverfahren für dieses Proposal

SNMP-ID:

2.19.4.12.5

Pfad Telnet:

Setup > **VPN** > **Proposals** > **IPSEC**

Mögliche Werte:

Keine Authentifizierung

HMAC-MD5

HMAC-SHA1

HMAC-SHA2-256

Default:

Keine Authentifizierung

AH-Auth-Alg

AH-Authentifizierungsverfahren für dieses Proposal

SNMP-ID:

2.19.4.12.6

Pfad Telnet:

Setup > **VPN** > **Proposals** > **IPSEC**

Mögliche Werte:

Keine Authentifizierung

HMAC-MD5

HMAC-SHA1

HMAC-SHA2-256

Default:

Keine Authentifizierung

4 RADIUS

4.1 Eingabelänge für RADIUS-Weiterleitungsziele

Ab LCOS-Version 8.82 können Realms bis zu 64 Zeichen lang sein, um Roaming-Provider mit langen Realms benutzen zu können.

4.1.1 Ergänzungen im Setup-Menü

Realm

Zeichenkette, mit der der RADIUS-Server das Weiterleitungs-Ziel identifiziert.

SNMP-ID:

2.25.10.3.1

Pfad Telnet:

Setup > **RADIUS** > **Server** > **Weiterleit-Server**

Mögliche Werte:

max. 64 Zeichen

Default:

Leer

Backup

Alternativer Weiterleitungs-Server, an den der RADIUS-Server Anfragen weiterleitet, wenn der erste Weiterleitungs-Server nicht erreichbar ist.

SNMP-ID:

2.25.10.3.5

Pfad Telnet:

Setup > **RADIUS** > **Server** > **Weiterleit-Server**

Mögliche Werte:

max. 64 Zeichen

Default:

Leer

Default-Realm

Dieser Realm gilt alternativ, wenn der übermittelte Benutzername einen unbekannten Realm verwendet, der nicht in der Liste der Weiterleitungs-Server enthalten ist.

SNMP-ID:

2.25.10.5

Pfad Telnet:

Setup > **RADIUS** > **Server**

Mögliche Werte:

max. 64 Zeichen

Default:

Leer

Empty-Realm

Dieser Realm gilt alternativ, wenn der übermittelte Benutzername keinen Realm enthält.

SNMP-ID:

2.25.10.6

Pfad Telnet:

Setup > **RADIUS** > **Server**

Mögliche Werte:

max. 64 Zeichen

Default:

Leer

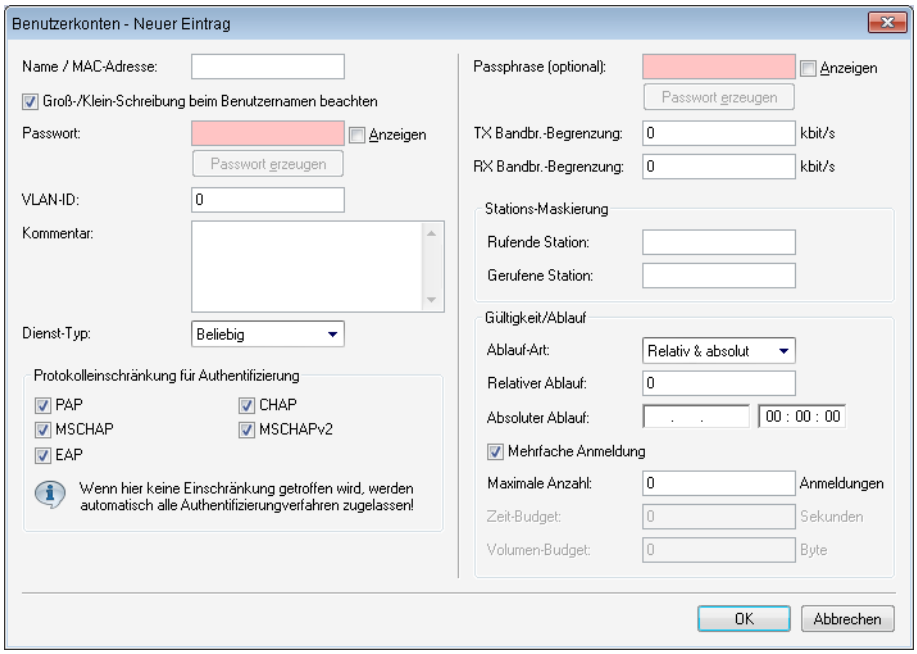
4.2 Bandbreitenzuweisung per RADIUS

Ab LCOS-Version 8.82 kann der RADIUS-Server des LANCOM jedem registrierten Client unabhängig vom verwendeten Interface eine Bandbreitenbegrenzung zuordnen. Bisher war das in Public-Spot-Szenarien immer nur dann möglich, wenn Public-Spot-Gateway und zugehöriges WLAN-Interface auf demselben Gerät aktiv waren.

4.2.1 Erweiterungen im RADIUS-Server

RADIUS-Benutzer

In der Benutzer-Datenbank können Sie bis zu 64 Benutzer eintragen, die der RADIUS-Server ohne weitere Datenbanken authentifizieren kann. Diese Benutzer-Tabelle verwendet der RADIUS-Server für lokale Anfragen, also für Anfragen mit Benutzernamen ohne Realm.



- **Benutzername**: Geben Sie hier den Namen des Benutzers ein
- **Groß-/Kleinschreibung beim Benutzernamen beachten**: Bei aktivierter Option unterscheidet der RADIUS-Server nach Groß- und Kleinschreibung. "User12345" und "user12345" sind somit zwei unterschiedliche Benutzer.
- **Passwort**: Passwort des Benutzers
- **VLAN-ID**: ID des logischen Teilnetzes
- **Kommentar**: Zusätzliche Informationen zum Benutzer
- **Dienst-Typ**: Der Dienst-Typ ist ein spezielles Attribut des RADIUS-Protokolls, welches der NAS (Network Access Server) mit dem Authentication Request übermittelt. Der Request wird nur dann positiv beantwortet, wenn der angefragte Dienst-Typ mit dem Dienst-Typ des Benutzerkontos übereinstimmt. Mögliche Werte sind:
  - `Beliebig`: Der Dienst-Typ kann ein beliebiger Sein.
  - `Framed`: Für Prüfung von WLAN-MAC-Adressen über RADIUS bzw. bei IEEE 802.1x.
  - `Anmeldung`: Für Public-Spot-Anmeldungen.
  - `Nur Authentifizierung` : Für Einwahl-Gegenstellen über PPP, die mit RADIUS authentifiziert werden.

  Beachten Sie, dass in Abhängigkeit vom Gerät die Anzahl der Einträge mit dem Dienst-Typ `Beliebig` oder `Anmeldung` begrenzt sein kann. Ist Ihr Gerät z. B. dazu in der Lage, insgesamt 64 Public-Spot-Benutzer zu verwalten, dann verweigert LANconfig nach dem 64. Benutzerkonto mit dem Dienst-Typ `Beliebig/Anmeldung` die Anlage weiterer Benutzerkonten mit diesen Dienst-Typen.
- **Protokolleinschränkung**: Mit dieser Option können Sie die für den Benutzer erlaubten Authentifizierungsverfahren einschränken. Mögliche Werte sind:
  - PAP
  - CHAP
  - MSCHAP
  - MSCHAPv2

- EAP

- **Passphrase**: zugeordnete WPA-Passphrase des registrierten Benutzers
- **TX-Bandbr.-Begrenzung**: Begrenzung der Bandbreite beim Senden von Daten
- **RX-Bandbr.-Begrenzung**: Begrenzung der Bandbreite beim Empfangen von Daten

  Die Bandbreitenbegrenzung für Senden und Empfangen gilt unabhängig vom verwendeten Interface (LAN und WLAN).
- **Rufende Station**: Diese Maske schränkt die Gültigkeit des Eintrags auf bestimmte IDs ein, die die rufende Station (WLAN-Client) übermittelt. Bei der Authentifizierung über 802.1x wird die MAC-Adresse der rufenden Station im ASCII-Format (nur Großbuchstaben) übertragen, dabei werden Zeichenpaare durch einen Bindestrich getrennt (z. B. "00-10-A4-23-19-C0").
- **Gerufene Station**: Diese Maske schränkt die Gültigkeit des Eintrags auf bestimmte IDs ein, die die gerufende Station (BSSID und SSID des Access-Points) übermittelt. Bei der Authentifizierung über 802.1x werden die MAC-Adresse (BSSID) der gerufenden Station im ASCII-Format (nur Großbuchstaben) übertragen, dabei werden Zeichenpaare durch einen Bindestrich getrennt. Die SSID wird nach einem Doppelpunkt als Trennzeichen angehängt (z. B. "00-10-A4-23-19-C0:AP1").
- **Ablauf-Art**: Diese Option legt die Art der Gültigkeitsdauer des Benutzer-Accounts fest. Mögliche Werte sind:
  - `Relativ & absolut`
  - `Relativ`
  - `Absolut`
  - `Niemals`
- **Relativer Ablauf**: Gültigkeit in Sekunden ab der ersten erfolgreichen Anmeldung
- **Absoluter Ablauf**: Gültigkeit in Stunden, Minuten und Sekunden ab einem bestimmten Datum
- **Mehrfache Anmeldung**: Aktiviert die Möglichkeit für den Client, sich mehrfach anmelden zu können.
- **Maximale Anzahl**: Maximale Anzahl der gleichzeitigen Anmeldungen des Clients.
- **Zeit-Budget**: Legt das Zeit-Budget in Sekunden fest, das dem Client zur Verfügung steht.
- **Volumen-Budget**: Legt das Datenvolumen fest, das dem Client zur Verfügung steht.

4.2.2 Ergänzungen im Status-Menü

Stations-Tabelle

Diese Tabelle enthält Bandbreitenzuweisungen für im RADIUS-Server registrierte Clients, unabhängig davon, über welches Interface diese Clients angeschlossen sind.

SNMP-ID:

1.5.90

Pfad Telnet:

Status > **LAN**

Schnittstelle

Schnittstelle, an der der Client angeschlossen ist.

MAC-Adresse

MAC-Adresse des Clients.

Tx-Limit

Bandbreitenbegrenzung für den Empfang von Daten.

Rx-Limit

Bandbreitenbegrenzung für das Senden von Daten.

VLAN-Id

VLAN-ID des Netzwerkes, über das der Client kommuniziert.

5 WLAN-Management

5.1 Band-Steering über WLAN-Controller

Ab LCOS-Version 8.82 können WLAN-Controller die Einstellung des Band-Steerings der Access-Points in den Radioprofilen verwalten.

5.1.1 Ergänzungen in LANconfig

Konfiguration

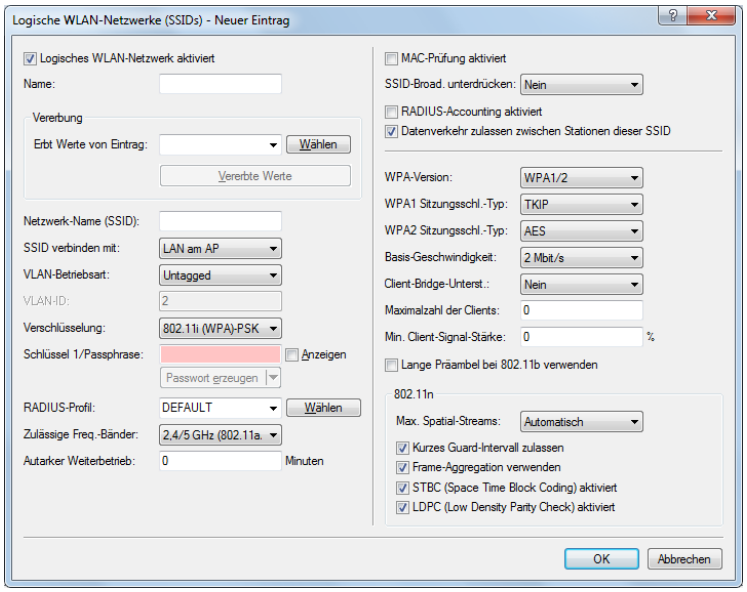
Die meisten Parameter zur Konfiguration der LANCOM WLAN Controller entsprechen denen der Access Points. In diesem Abschnitt werden daher nicht alle WLAN-Parameter explizit beschrieben sondern nur die für den Betrieb der WLAN-Controller erforderlichen Aspekte.

Profile

Im Bereich der Profile definieren Sie die logischen WLAN-Netzwerke, die physikalischen WLAN-Parameter sowie die WLAN-Profile, die eine Kombination aus den beiden vorgenannten Elementen darstellen.

Logische WLAN-Netzwerke

Hier werden die logischen WLAN-Netzwerke eingestellt, die den Access Points zugewiesen werden. Für jedes logische WLAN-Netzwerk können Sie die folgenden Parameter definieren:



LANconfig: **WLAN-Controller** > **Profile** > **Logische WLAN-Netzwerke**

WEBconfig: **LCOS-Menübaum** > **Setup** > **WLAN-Management** > **AP-Konfiguration** > **Netzwerkprofile**

- **Netzwerk-Name (SSID)**

Name des logischen WLAN-Netzwerks, unter dem die Einstellungen gespeichert werden. Dieser Name wird nur für die interne Verwaltung der logischen Netze verwendet.

- **Vererbung**

  Auswahl eines schon definierten logischen WLAN-Netzwerks, von dem die Einstellungen übernommen werden sollen.

- **SSID verbinden mit**

  Service Set Identifier – unter diesem Namen wird das logische WLAN-Netzwerk für die WLAN-Clients angeboten.

- **VLAN-ID**

  VLAN-ID für dieses logische WLAN-Netzwerk.

  Bitte beachten Sie, dass für die Nutzung der VLAN-IDs in einem logischen WLAN-Netzwerk die Einstellung einer Management-VLAN-ID erforderlich ist (siehe Physikalische WLAN Parameter)!

- **Autarker Weiterbetrieb**

  Zeit in Minuten, für die der Access Point im Managed-Modus mit seiner aktuellen Konfiguration weiterarbeitet.

  Die Konfiguration wird dem Access Point vom WLAN-Controller zugewiesen und optional im Flash gespeichert (in einem Bereich, der nicht mit LANconfig oder anderen Tools auszulesen ist). Falls die Verbindung zum WLAN-Controller unterbrochen wird, arbeitet der Access Point für die hier eingestellte Zeit mit seiner Konfiguration aus dem Flash weiter. Auch nach einem eigenen Stromausfall kann der Access Point mit der Konfiguration aus dem Flash weiterarbeiten.

  Wenn die eingestellte Zeit abgelaufen ist und die Verbindung zum WLAN-Controller noch nicht wiederhergestellt wurde, wird die Konfiguration im Flash gelöscht – der Access Point stellt seinen Betrieb ein. Sobald der WLAN-Controller wieder erreichbar ist, wird die Konfiguration erneut vom WLAN-Controller zum Access Point übertragen.

  Durch diese Option kann der Access Point auch dann weiter arbeiten, wenn die Verbindung zum WLAN-Controller kurzfristig unterbrochen wird. Außerdem stellt diese Maßnahme einen wirksamen Schutz gegen Diebstahl dar, da die sicherheitsrelevanten Parameter der Konfiguration nach Ablauf der eingestellten Zeit automatisch gelöscht werden.

  Stellt der Access Point im Backupfall eine Verbindung zu einem sekundären WLAN-Controller her, so wird der Ablauf der Zeit für den autarken Weiterbetrieb unterbrochen. Der Access Point bleibt also mit seinen WLAN-Netzwerken auch über diese eingestellte Zeit hinaus aktiv, solange er eine Verbindung zu einem WLAN-Controller hat.

  Bitte beachten Sie, dass die Konfigurationsdaten im Flash erst nach Ablauf der eingestellten Zeit für den autarken Weiterbetrieb gelöscht werden, nicht jedoch durch die Trennung vom Stromnetz!

- **Min. Client-Signal-Stärke**

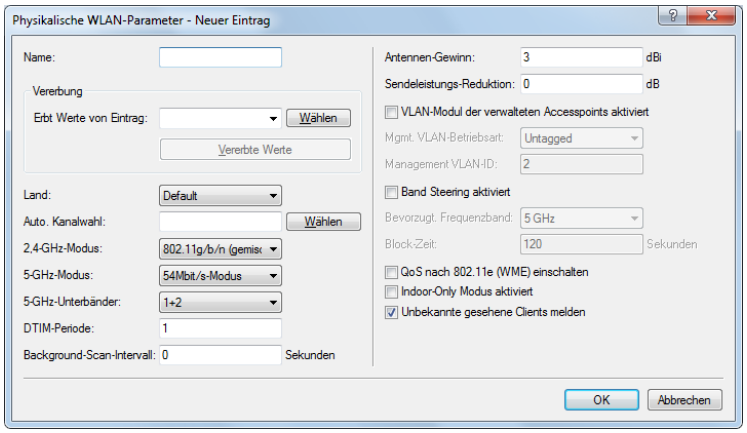
  Dieser Eintrag bestimmt den Schwellwert in Prozent für die minimale Signalstärke für Clients beim Einbuchen. Unterschreitet ein Client diesen Wert, sendet der Access-Point keine Probe-Responses mehr an diesen Client und verwirft die entsprechenden Anfragen.

  Ein Client mit schlechter Signalstärke findet den Access-Point somit nicht und kann sich nicht darauf einbuchen. Das sorgt beim Client für eine optimierte Liste an verfügbaren Access-Points, da die Liste keine Access-Points aufführt, mit denen der Client an der aktuellen Position nur eine schwache Verbindung aufbauen könnte.

Alle weiteren Parameter der WLAN-Netzwerke entsprechen denen der üblichen Konfiguration für Access Points.

Physikalische WLAN-Parameter

Hier werden die physikalischen WLAN-Parameter eingestellt, die den Access Points zugewiesen werden. Für jeden Satz von physikalischen WLAN-Parametern können Sie die folgenden Parameter definieren:



LANconfig: **WLAN-Controller** > **Profile** > **Physikalische WLAN-Parameter**

WEBconfig: **LCOS-Menübaum** > **Setup** > **WLAN-Management** > **AP-Konfiguration** > **Radioprofile**

- **Name**

  Eindeutiger Name für diese Zusammenstellung von physikalischen WLAN-Parametern.

- **Vererbung**

  Auswahl eines schon definierten Satzes von physikalischen WLAN-Parametern, von dem die Einstellungen übernommen werden sollen.

- **Land**

  Land, in dem die Access Points betrieben werden sollen. Aufgrund dieser Information werden landesspezifische Einstellungen wie die erlaubten Kanäle etc. festgelegt.

- **Automatische Kanalwahl**

  Standardmäßig können die Access Points alle Kanäle nutzen, die aufgrund der Ländereinstellung erlaubt sind. Um die Auswahl auf bestimmte Kanäle zu beschränken, können hier die gewünschten Kanäle als kommaseparierte Liste eingetragen werden. Dabei ist auch die Angabe von Bereichen (z. B. '1,6,11') möglich.

- **Management VLAN-ID**

  Die VLAN-ID, die für das Management-Netz der Access Points verwendet wird.

  Die Management-VLAN-ID **muss** auf einen Wert ungleich null eingestellt werden, um VLANs auf den WLAN-Netzwerken nutzen zu können. Das gilt auch dann, wenn das Management-Netz selbst nicht mit VLAN-IDs getaggt werden soll (Mgmt-VLAN-ID = 1).

  Die VLAN-Aktivierung gilt jeweils nur für logischen WLAN-Netzwerke, die mit diesen physikalischen WLAN-Parametern verbunden sind.

- **Band Steering aktiviert**

  Dieser Eintrag bestimmt, ob der Access-Point das Band-Steering aktivieren soll. In diesem Fall kann ein Dual-Port-Access-Point einen WLAN-Client auf ein bevorzugtes Frequenzband umleiten.

Alle weiteren physikalischen WLAN-Parameter entsprechen denen der üblichen Konfiguration für Access Points.

Für denn erfolgreichen Profilbezug ist es erforderlich, dass der HTTP-Zugriff auf den WLAN-Controller aus dem lokalen Netz erlaubt ist.

5.1.2 Ergänzungen im Setup-Menü

Melde-gesehene-Clients

Dieser Eintrag bestimmt, ob der Access-Point im WLAN-Netz erkannte Clients melden soll.

SNMP-ID:

2.37.1.2.20

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **Radioprofile**

Mögliche Werte:

Ja

Nein

Default:

Ja

Client-Steering

Dieser Eintrag bestimmt, ob der Access-Point das Band-Steering aktivieren soll.

SNMP-ID:

2.37.1.2.21

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **Radioprofile**

Mögliche Werte:

Ja

Nein

Default:

Nein

Bevorzugtes-Band

Dieser Eintrag bestimmt, in welches Frequenzband der Access-Point den WLAN-Client bevorzugt leiten soll.

SNMP-ID:

2.37.1.2.22

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **Radioprofile**

Mögliche Werte:

5GHz

2,4GHz

Default:

5GHz

Proberequest-Herausaltern-Sekunden

Dieser Eintrag bestimmt die Zeit in Sekunden, für die die Verbindung eines WLAN-Clients im Access-Point gespeichert bleiben soll. Nach Ablauf dieser Zeit löscht der Access-Point den Eintrag in der Tabelle.

Wenn Sie Clients im WLAN benutzen, die z. B. oft von Dual-Band- auf Single-Band-Modus umschalten, sollten Sie diesen Wert entsprechen niedrig ansetzen.

SNMP-ID:

2.37.1.2.23

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **Radioprofile**

Mögliche Werte:

max. 10 Zeichen aus 0 bis 9

Besondere Werte:

0: Der Access-Point betrachtet gesehene Probe-Requests sofort als ungültig.

Default:

120

Minimal-Stations-Staerke

Dieser Eintrag bestimmt den Schwellwert in Prozent für die minimale Signalstärke für Clients beim Einbuchen. Unterschreitet ein Client diesen Wert, sendet der Access-Point keine Probe-Responses mehr an diesen Client und verwirft die entsprechenden Anfragen.

Ein Client mit schlechter Signalstärke findet den Access-Point somit nicht und kann sich nicht darauf einbuchen. Das sorgt beim Client für eine optimierte Liste an verfügbaren Access-Points, da die Liste keine Access-Points aufführt, mit denen der Client an der aktuellen Position nur eine schwache Verbindung aufbauen könnte.

SNMP-ID:

2.37.1.1.36

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **Netzwerkprofile**

Mögliche Werte:

max. 3 Zeichen aus 0 bis 9

Default:

0

6 WLAN

6.1 Erweitertes ARP-Handling

Ab LCOS-Version 8.82 können Access-Points mehr als eine IP-Adresse je WLAN-Client speichern.

6.1.1 Ergänzungen im Status-Menü

ARP-Handling

Dieses Menü zeigt IPv4- und IPv6-Informationen über die in der WLAN-Funkzelle erkannten WLAN-Clients.

Der Access-Point kann in diesen Tabellen, speziell bei IPv6-Netzwerken, mehrere IP-Adressen pro WLAN-Client speichern. Der Eintrag in der WLAN-Stationstabelle (**Setup** > **WLAN** > **Stationstabelle**) zeigt bei mehreren IP-Adressen pro WLAN-Client immer auf die zuletzt erkannte IP-Adresse.

SNMP-ID:

1.3.62

Pfad Telnet:

Status > **WLAN**

ARP-Tabelle

Diese Tabelle enthält IPv4-Informationen über die in der WLAN-Funkzelle erkannten WLAN-Clients.

SNMP-ID:

1.3.62.1

Pfad Telnet:

Status > **WLAN** > **ARP-Behandlung**

Adresse

Enthält die gespeicherte IPv4-Adresse des WLAN-Clients.

MAC-Adresse

Enthält die zugehörige MAC-Adresse des WLAN-Clients.

Schnittstelle

Enthält die SSID, über die der WLAN-Client verbunden ist.

VLAN-Id

Enthält die VLAN-ID, über die der WLAN-Client verbunden ist.

Alter

Enthält die Zeitdauer in Sekunden, vor der der Access-Point den WLAN-Client zuletzt erkannt hat.

Der Access-Point löscht Einträge in dieser Tabelle nur dann, wenn er den entsprechenden WLAN-Client nicht mehr in der WLAN-Funkzelle erkennt.

Es ist möglich, dass der Access-Point in dieser Tabelle mehrere IP-Adressen für einen WLAN-Client (bzw. mehrere WLAN-Clients mit identischer IP-Adresse) speichert, um z. B. Adresskonflikte aufzuzeigen.

ND-Tabelle

Diese Tabelle enthält IPv6-Informationen über die in der WLAN-Funkzelle erkannten WLAN-Clients.

SNMP-ID:

1.3.62.2

Pfad Telnet:

Status > **WLAN** > **ARP-Behandlung**

Adresse

Enthält die gespeicherte IPv6-Adresse des WLAN-Clients.

MAC-Adresse

Enthält die zugehörige MAC-Adresse des WLAN-Clients.

Schnittstelle

Enthält die SSID, über die der WLAN-Client verbunden ist.

VLAN-Id

Enthält die VLAN-ID, über die der WLAN-Client verbunden ist.

Alter

Enthält die Zeitdauer in Sekunden, vor der der Access-Point den WLAN-Client zuletzt erkannt hat.

Der Access-Point löscht Einträge in dieser Tabelle nur dann, wenn er den entsprechenden WLAN-Client nicht mehr in der WLAN-Funkzelle erkennt.

Es ist möglich, dass der Access-Point in dieser Tabelle mehrere IP-Adressen für einen WLAN-Client (bzw. mehrere WLAN-Clients mit identischer IP-Adresse) speichert, um z. B. Adresskonflikte aufzuzeigen.

ARP-Anfragen-beantwortet

Dieser Eintrag zeigt die Anzahl der direkt vom Access-Point erfolgreich beantworteten ARP-Requests, ohne die Anfrage zuvor an die WLAN-Funkzelle weitergeleitet zu haben.

SNMP-ID:

1.3.62.11

Pfad Telnet:

Status > **WLAN** > **ARP-Behandlung**

ARP-Anfragen-nicht-beantwortet

Dieser Eintrag zeigt die Anzahl der nicht vom Access-Point direkt beantworteten ARP-Requests. Stattdessen musste der Access-Point diese Anfrage zunächst an die WLAN-Funkzelle weiterleiten.

SNMP-ID:

1.3.62.12

Pfad Telnet:

Status > **WLAN** > **ARP-Behandlung**

ARP-Anfragen-verworfen

Dieser Eintrag zeigt die Anzahl der vom Access-Point verworfenen ARP-Requests. Gründe hierfür können sein:

- Der Access-Point hat diese Anfrage bereits über eine andere Schnittstelle beantwortet.
- Der Access-Point hat diese Anfrage als überflüssige ARP-Abfrage eingestuft.
- Die Anfrage entspricht nicht dem VLAN-Override des WLAN-Clients.

SNMP-ID:

1.3.62.13

Pfad Telnet:

Status > **WLAN** > **ARP-Behandlung**

ND-Suchen-beantwortet

Dieser Eintrag zeigt die Anzahl der direkt vom Access-Pont erfolgreich beantworteten ND-Requests, ohne die Anfrage zuvor an die WLAN-Funkzelle weitergeleitet zu haben.

SNMP-ID:

1.3.62.14

Pfad Telnet:

Status > **WLAN** > **ARP-Behandlung**

ND-Suchen-nicht-beantwortet

Dieser Eintrag zeigt die Anzahl der nicht vom Access-Point direkt beantworteten ND-Requests. Stattdessen musste der Access-Point diese Anfrage zunächst an die WLAN-Funkzelle weiterleiten.

SNMP-ID:

1.3.62.15

Pfad Telnet:

Status > **WLAN** > **ARP-Behandlung**

ND-Suchen-verworfen

Dieser Eintrag zeigt die Anzahl der vom Access-Point verworfenen ND-Requests. Gründe hierfür können sein:

- Der Access-Point hat diese Anfrage bereits über eine andere Schnittstelle beantwortet.
- Der Access-Point hat diese Anfrage als eine DAD-Abfrage (Duplicate Address Detection) eingestuft.
- Die Anfrage entspricht nicht dem VLAN-Override des WLAN-Clients.

SNMP-ID:

1.3.62.16

Pfad Telnet:

Status > **WLAN** > **ARP-Behandlung**

Werte-loeschen

Diese Aktion löscht alle gespeicherten Werte in den ARP- bzw. ND-Tabellen.

SNMP-ID:

1.3.62.99

Pfad Telnet:

Status > **WLAN** > **ARP-Behandlung**

6.2 Multi- und Broadcasts in Funkzellen abschaltbar

Ab LCOS-Version 8.82 besteht gemäß der HotSpot-2.0-Spezifikation die Möglichkeit, Multi- und Broadcasts in Funkzellen abzuschalten.

6.2.1 Ergänzungen im Setup-Menü

Nur-Unicasts-senden

Multi- und Broadcast-Sendungen innerhalb einer WLAN-Funkzelle bedeuten eine Belastung für die Bandbreite dieser Funkzelle, zumal die WLAN-Clients mit diesen Sendungen oft nichts anfangen können. Der Access-Point fängt durch ARP-Spoofing bereits einen Großteil der Multi- und Broadcast-Sendungen in die Funkzelle ab. Mit der Beschränkung auf Unicast-Sendungen filtert er z. B. überflüssige IPv4-Broadcasts wie Bonjour oder NetBIOS aus den Anfragen heraus.

Die Unterdrückung von Multi- und Broadcast-Sendungen ist zudem eine Forderung der HotSpot-2.0-Spezifikation.

SNMP-ID:

2.23.20.1.19

Pfad Telnet:

Pfad Telnet: Setup > **Schnittstellen** > **WLAN** > **Netzwerk**

Mögliche Werte:

Ja

Nein

Default:

Nein

6.2.2 Ergänzungen in LANconfig

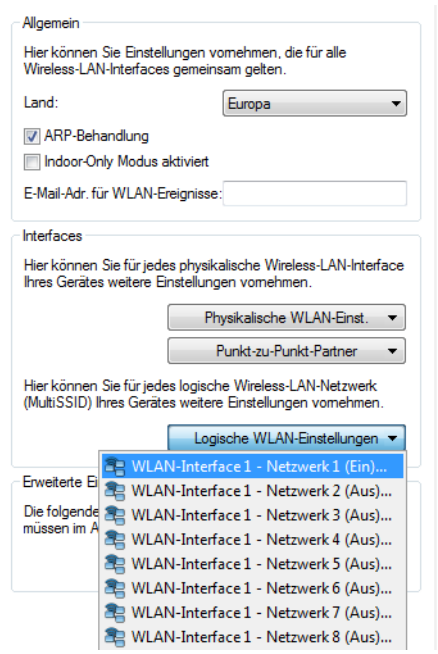
Konfiguration der WLAN-Parameter

Die Einstellungen für die Funknetzwerke erfolgen an verschiedenen Stellen in der Konfiguration:

- Manche Parameter betreffen die physikalische WLAN-Schnittstellen. Einige LANCOM-Modelle verfügen über eine WLAN-Schnittstelle (Single Radio Access Point), andere Modelle haben ein zweites WLAN-Modul integriert (Dual Radio Access Point). Die Einstellungen für die physikalischen WLAN-Schnittstellen gelten für alle logischen Funknetzwerke, die mit diesem Modul aufgespannt werden. Zu diesen Parametern gehören z. B. die Sendeleistung der Antenne und die Betriebsart des WLAN-Moduls (Access Point oder Client).
- Andere Parameter beziehen sich nur auf die jeweiligen logischen Funknetze, die mit einem physikalischen Interface aufgespannt werden. Dazu gehört z. B. die SSID oder die Aktivierung der Verschlüsselung, z. B. 802.11i mit AES.
- Eine dritte Gruppe von Parametern hat zwar Auswirkungen auf den Betrieb des Funknetzwerks, ist aber nicht nur für WLANs von Bedeutung. Dazu gehören z. B. die Protokollfilter in der LAN-Bridge.

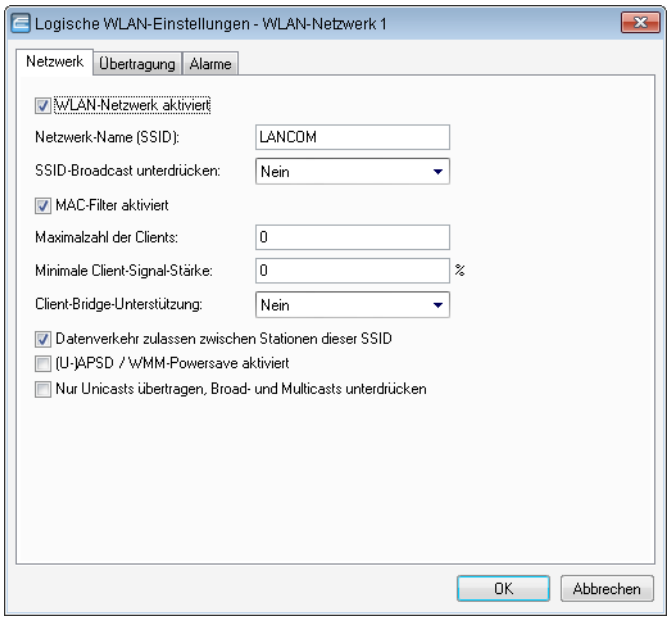
Die logischen WLAN-Schnittstellen

Jede physikalische WLAN-Schnittstelle kann bis zu acht verschiedene logische Funknetzwerke aufspannen (Multi-SSID). Für jedes dieser Funknetze können bestimmte Parameter speziell definiert werden, ohne dass zusätzliche Access Points benötigt werden.



Netzwerkeinstellungen

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



- **WLAN-Netzwerk aktiviert**

  Mit diesem Schalter aktivieren bzw. deaktivieren Sie das entsprechende logische WLAN.

- **Netzwerk-Name** (SSID)

Bestimmen Sie für jedes benötigte logische Funknetzwerk eine eindeutige SSID (den Netzwerknamen). Nur solche Netzwerkkarten, die über die gleiche SSID verfügen, können sich in diesem Funknetzwerk anmelden.

- **SSID-Broadcast unterdrücken**

  Sie können Ihr Funk-LAN entweder in einem öffentlichen oder in einem privaten Modus betreiben. Ein Funk-LAN im öffentlichen Modus kann von Mobilstationen in der Umgebung ohne weiteres kontaktiert werden. Durch Aktivieren der Closed-Network-Funktion versetzen Sie Ihr Funk-LAN in einen privaten Modus. In dieser Betriebsart sind Mobilstationen ohne Kenntnis des Netzwerknamens (SSID) von der Teilnahme am Funk-LAN ausgeschlossen.

  Schalten Sie den "Closed-Network-Modus" ein, wenn Sie verhindern möchten, dass sich WLAN-Clients mit der SSID "Any" oder einer leeren SSID in Ihrem Funknetzwerk anmelden.

  Die Option **SSID-Broadcast unterdrücken** ermöglicht folgende Einstellungen:

  - **Nein**: Der Access Point veröffentlicht die SSID der Funkzelle. Sendet ein Client einen Probe Request mit leerer oder falscher SSID, antwortet der Access Point mit der SSID der Funkzelle (öffentliches WLAN).
  - **Ja**: Der Access Point veröffentlicht die SSID der Funkzelle nicht. Sendet ein Client einen Probe Request mit leerer SSID, antwortet der Access Point ebenfalls mit einer leeren SSID.
  - **Verschärft**: Der Access Point veröffentlicht die SSID der Funkzelle nicht. Sendet ein Client einen Probe Request mit leerer oder falscher SSID, antwortet der Access Point überhaupt nicht.

  Das einfache Unterdrücken der SSID bietet keinen ausreichenden Zugriffsschutz, da der Access Point diese bei der Anmeldung berechtigter WLAN-Clients im Klartext überträgt und sie somit für alle im WLAN-Netz befindlichen WLAN-Clients kurzfristig sichtbar ist.

- **MAC-Filter aktiviert**

  In der MAC-Filterliste (**Wireless-LAN** > **Stationen** > **Stationen**) sind die MAC-Adressen der Clients hinterlegt, die sich bei einem Access Point einbuchen dürfen. Mit dem Schalter **MAC-Filter aktiviert** können Sie die Verwendung der MAC-Filterliste gezielt für einzelne logische Netzwerke ausschalten.

  Die Verwendung der MAC-Filterliste ist auf jeden Fall erforderlich für logische Netzwerke, in denen sich die Clients mit einer individuellen Passphrase über LEPS anmelden. Die bei LEPS verwendete Passphrase wird ebenfalls in der MAC-Filterliste eingetragen. Für die Anmeldung mit einer individuellen Passphrase beachtet der Access Point daher immer die MAC-Filterliste, auch wenn Sie diese Option hier deaktivieren.

- **Maximale Client-Anzahl**

  Legen Sie hier die maximale Anzahl der Clients fest, die sich bei diesem Access Point einbuchen dürfen. Weitere Clients, die sich über diese Anzahl hinaus anmelden wollen, lehnt der Access Point ab.

- **Minimale Client-Signal-Stärke**

  Mit diesem Eintrag bestimmen Sie den Schwellwert in Prozent für die minimale Signalstärke für Clients beim Einbuchen. Unterschreitet ein Client diesen Wert, sendet der Access Point keine Probe-Responses mehr an diesen Client und verwirft die entsprechenden Anfragen.

  Ein Client mit schlechter Signalstärke findet den Access Point somit nicht und kann sich nicht darauf einbuchen. Das sorgt beim Client für eine optimierte Liste an verfügbaren Access Points, da keine Access Points aufgeführt werden, mit denen der Client an der aktuellen Position nur eine schwache Verbindung aufbauen könnte.

- **Client-Bridge-Unterstützung**

  Aktivieren Sie diese Option für einen Access Point, wenn Sie im WLAN-Client-Modus für eine Client-Station die Client-Bridge-Unterstützung aktiviert haben.

  Sie können den Client-Bridge-Modus ausschließlich zwischen zwei LANCOM-Geräten verwenden.

- **Datenverkehr zulassen zwischen Stationen dieser SSID**

  Aktivieren Sie diese Option, wenn alle Stationen, die an dieser SSID angemeldet sind, untereinander kommunizieren dürfen.

- **(U-)APSD / WMM-Powersave aktiviert**

Aktivieren Sie diese Option, um Stationen die Unterstützung für den Stromsparmechanismus (U-)APSD ([Unscheduled] Automatic Power Save Delivery) zu signalisieren.

(U-)APSD ist im Standard 802.11e verankert und hilft VoWLAN-Geräten dabei, ihre Akkulaufzeit zu erhöhen. Die betreffenden Geräte schalten dafür nach der Anmeldung an einem (U-)APSD-fähigen Access Point in den Energiesparmodus um. Erhält der Acess Point nun Datenpakete für das betreffende Gerät, speichert es die Daten kurz zwischen und wartet, bis das VoWLAN-Gerät wieder verfügbar ist. Erst dann leitet er die Daten weiter. (U-)APSD erhöht demnach die Latenzzeit des Funkmoduls, wodurch es letztlich weniger Strom verbraucht. Die einzelnen Ruhezeiten können dabei so kurz ausfallen, dass ein VoWLAN-Gerät selbst im Gesprächszustand noch den Stromsparmechanismus benutzen kann. Die betreffenden Geräte müssen (U-)APSD allerdings ebenfalls unterstützen.

Bei WWM (Wi-Fi Multimedia) Power Save handelt es sich um einen Stromsparmechanismus der Wi-Fi Alliance, welcher auf U-APSD basiert. Bestimmte LANCOM Access Points sind von der Wi-Fi Alliance WMM® Power Save CERTIFIED.

- **Nur Unicasts übertragen, Broad- und Multicasts unterdrücken**

  Multi- und Broadcast-Sendungen innerhalb einer WLAN-Funkzelle bedeuten eine Belastung für die Bandbreite dieser Funkzelle, zumal die WLAN-Clients mit diesen Sendungen oft nichts anfangen können. Der Access-Point fängt durch ARP-Spoofing bereits einen Großteil der Multi- und Broadcast-Sendungen in die Funkzelle ab. Mit der Beschränkung auf Unicast-Sendungen filtert er z. B. überflüssige IPv4-Broadcasts wie Bonjour oder NetBIOS aus den Anfragen heraus.

  Die Unterdrückung von Multi- und Broadcast-Sendungen ist zudem eine Forderung der HotSpot-2.0-Spezifikation.

6.3 IEEE 802.11u und Hotspot 2.0

Ab LCOS 8.82 unterstützt Ihr Gerät 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.

- **Unterbrechnungsfreie 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 des 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.

6.3.1 Hotspot-Betreiber und -Service-Provider

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

6.3.2 Funktionsbeschreibung

Bei **802.11u** handelt es sich um den Basis-Standard der IEEE. Dieser Standard erweitert Access Points bzw. Hotspots im Wesentlichen um die Fähigkeit, sogenannte **ANQP-Datenpakete** (Advanced Message Queuing Protocol) in seinen Funksignalen auszustrahlen. ANQP ist ein Query/Response-Protokoll, mit dem ein Gerät eine Reihe von Informationen über den Hotspot abfragen kann. Hierzu gehören sowohl Meta-Daten, 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™. Bestimmte LANCOM Access Points sind von der Wi-Fi Alliance Passpoint™ CERTIFIED.

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 802.11-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.

6.3.3 Empfohlene allgemeine Einstellungen

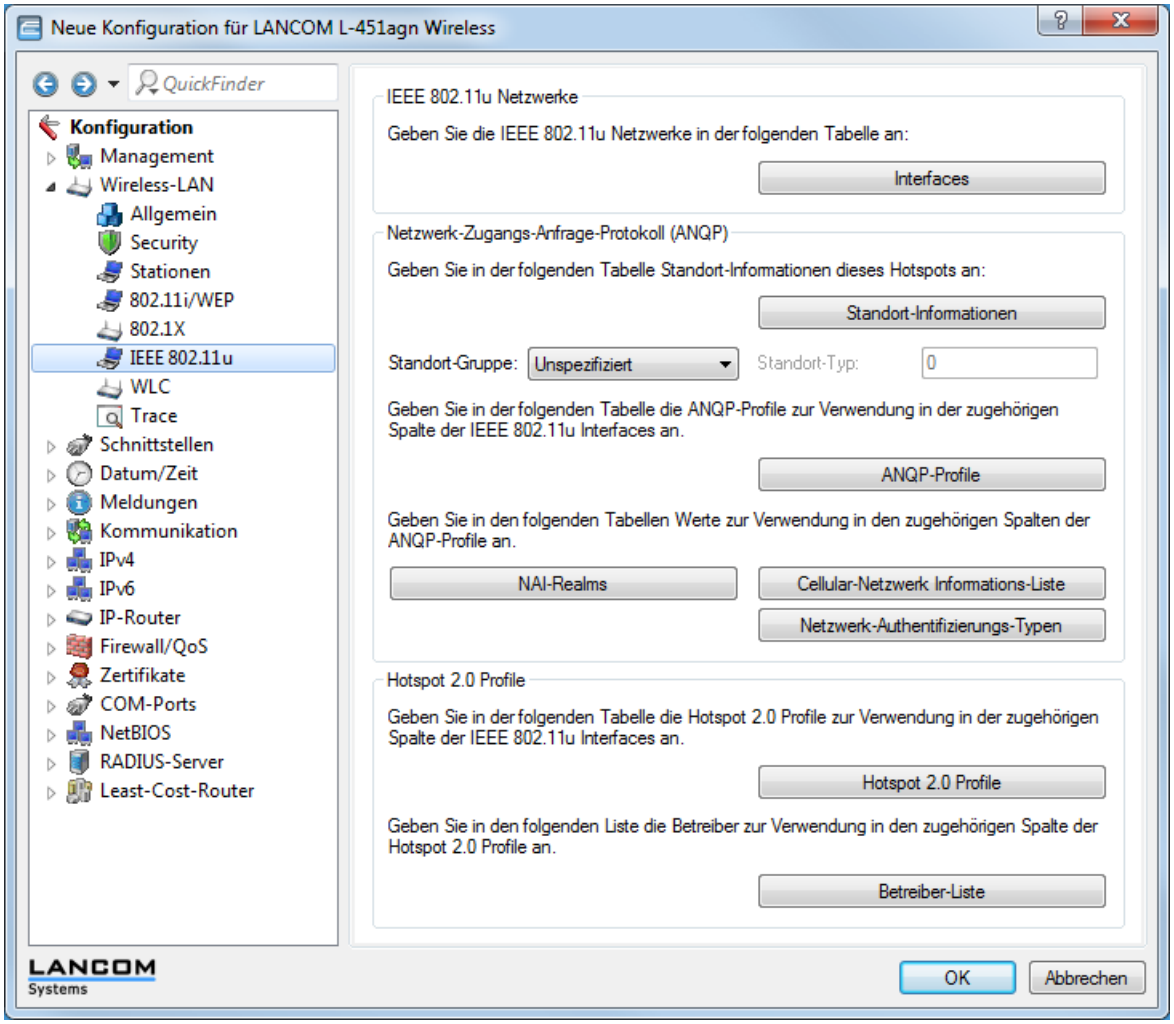
Die Hotspot-2.0-Spezifikation empfiehlt für den 802.11u-Betrieb folgende allgemeine Einstellungen:

- Aktivierte WPA2-Enterprise Sicherheit (802.1x)
- Authentifizierung via EAP mit der entsprechenden Variante:
  - EAP-SIM/EAP-AKA bei Authentifizierung mit SIM/USIM-Karte
  - EAP-TLS bei Authentifizierung mit digitalem Zertifikat
  - EAP-TTLS bei Authentifizierung mit Benutzername und Passwort
- Aktiviertes und eingerichtetes Proxy-ARP
- Deaktivierte Multicast- und Broadcasts in Funkzellen (neu in LCOS 8.82)
- Nicht-zugelassener Datenverkehr zwischen den einzelnen mobilen Endgeräten (Layer-2 Traffic-Inspection & Filtering). Die dazugehörigen Schalter finden Sie im LANconfig unter **Wireless-LAN** > **Securtity**.
- Aktivierte und eingerichtete Firewall auf dem Access-Router, welcher den Internetzugang zur Verfügung stellt

6.3.4 Ergänzungen in LANconfig

Konfigurationsmenü für IEEE 802.11u / Hotspot 2.0

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



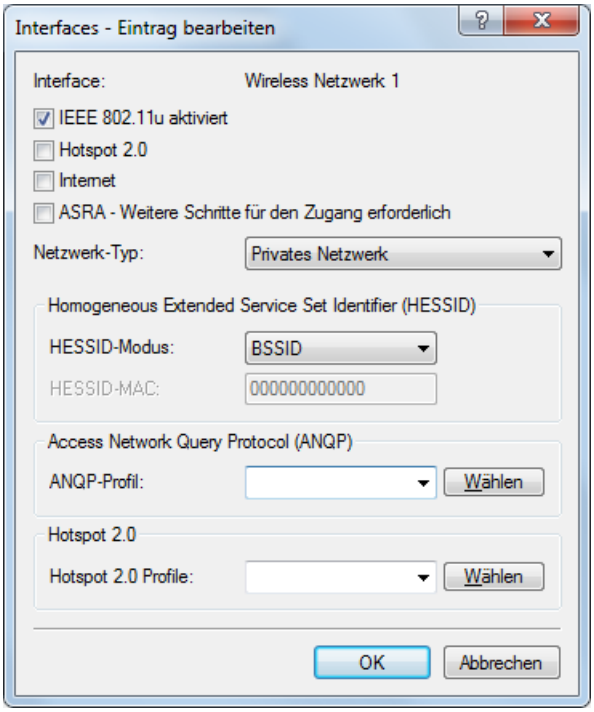
Das Gerät bietet Ihnen über die Schaltfläche **Interfaces** die Möglichkeit, die Unterstützung für den IEEE-802.11u-Standard sowie die Hotspot-2.0-Funktionalität für jede logische WLAN-Schnittstelle separat zu aktivieren bzw. deaktivieren sowie zu konfigurieren.

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
```

Aktivierung für Interfaces

Die Tabelle **Interfaces** ist die höchste Verwaltungsebene für 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.



Um die Einträge in der Tabelle **Interfaces** zu bearbeiten, klicken Sie auf die Schaltfläche **Bearbeiten…**. Die Einträge im Bearbeitungsfenster haben folgende Bedeutung:

- **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 – respektiv 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 802.11-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 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.

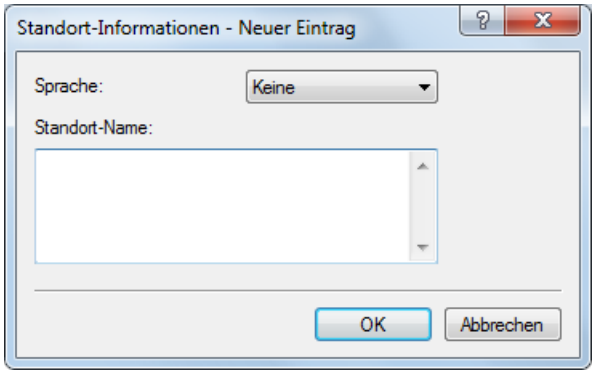
ANQP-Datenpakete konfigurieren

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.



Um die Einträge in der Tabelle **Standort-Informationen** zu bearbeiten, klicken Sie auf die Schaltfläche **Hinzufügen…**. Die Einträge im Bearbeitungsfenster haben folgende Bedeutung:

- **Sprache**: Sie haben die Möglichkeit, für jede Sprache individuelle Informationen zum Standort des Access Points zu 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 vom 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.

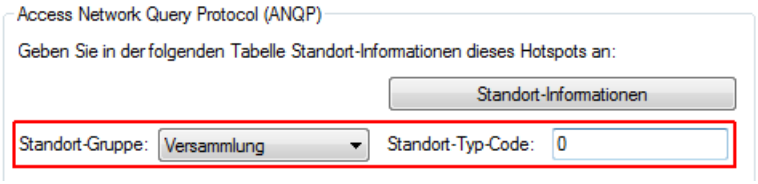


Tabelle 1: Übersicht möglicher Werte für Standort-Gruppen und -Typen

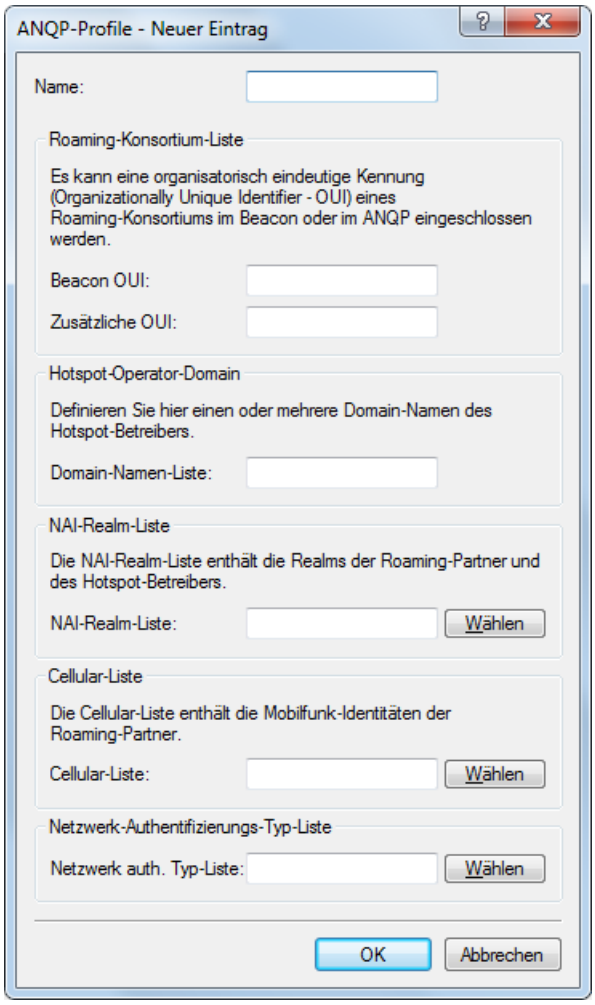
Standort-Gruppe	Code = Standort-Typ-Code
Unspezifiziert	
Versammlung	■ 0 = Unspezifizierte Versammlung ■ 1 = Bühne ■ 2 = Stadion ■ 3 = Passagier-Terminal (z. B. Flughafen, Busbahnhof, Fähranleger, Bahnhof) ■ 4 = Amphitheater ■ 5 = Vergnügungspark ■ 6 = Andachtsstätte ■ 7 = Kongresszentrum ■ 8 = Bücherei ■ 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
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

Standort-Gruppe	Code = Standort-Typ-Code
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.



Um die Einträge in der Tabelle **ANQP-Profile** zu bearbeiten, klicken Sie auf die Schaltfläche **Hinzufügen…**. Die Einträge im Bearbeitungsfenster haben folgende Bedeutung:

- **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!

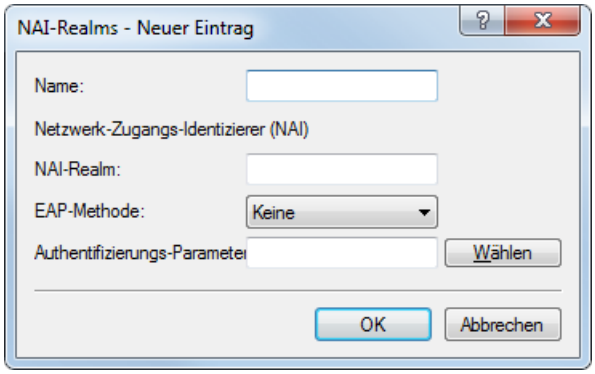
- **Zusätzliche OUI**: Tragen Sie hier die OI(s) ein, die das Gerät nach dem GAS-Request einer Station zusätzlich aussendet. Mehrere OIs trennen Sie durch eine kommaseparierte Liste, z. B. `00105E,00017D,00501A`.

- **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 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 Hostpot 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.

Zusätzliche haben Sie über die Telnet-Konsole bzw. das Setup-Menü 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 Telnet-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.

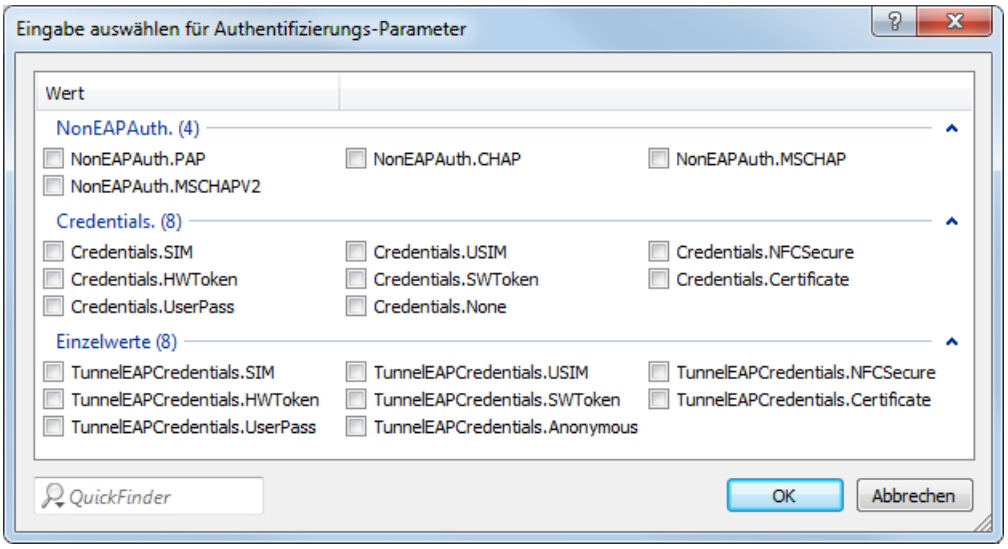


Um die Einträge in der Tabelle **NAI-Realms** zu bearbeiten, klicken Sie auf die Schaltfläche **Hinzufügen…**. Die Einträge im Bearbeitungsfenster haben folgende Bedeutung:

- **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 IETF 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 Schaltfläche **Wählen** und selektieren Sie in dem sich öffnenden Eingabedialog 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 2: Übersicht der möglichen Authentifizierungs-Parameter

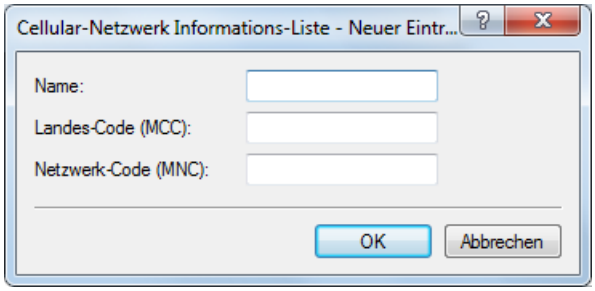
Parameter	Sub-Parameter	Erläuterung
NonEAPAuth.		Bezeichnet das Protokoll, welches der Realm für die Phase-2-Authentifizierung erfordert:
	PAP	Password Authentication Protocol
	CHAP	Challenge Handshake Authentication Protocol, ursprüngliche CHAP-Implementierung, spezifiziert im RFC 1994
	MSCHAP	CHAP-Implementierung 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:
	SIM	SIM-Karte
	USIM	USIM-Karte
	NFCSecure	NFC-Chip
	HWToken*	Hardware-Token

Parameter	Sub-Parameter	Erläuterung
	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

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

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.



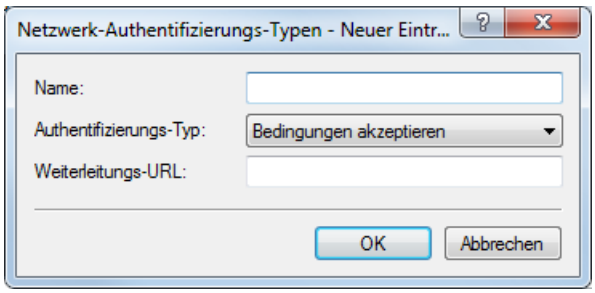
Um die Einträge in der Tabelle **Cellular-Netzwerk Informations-Liste** zu bearbeiten, klicken Sie auf die Schaltfläche **Hinzufügen…**. Die Einträge im Bearbeitungsfenster haben folgende Bedeutung:

- **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.
- **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!



Um die Einträge in der Tabelle **Netzwerk-Authentifizierungs-Typen** zu bearbeiten, klicken Sie auf die Schaltfläche **Hinzufügen…**. Die Einträge im Bearbeitungsfenster haben folgende Bedeutung:

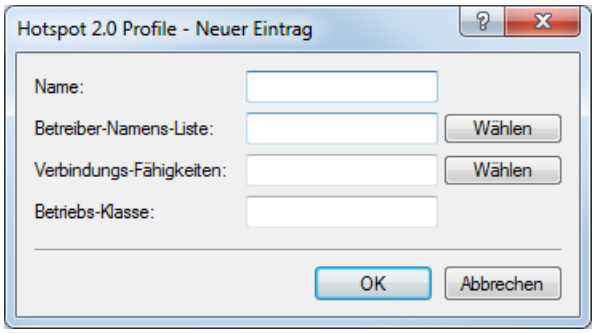
- **Name**: Vergeben Sie hierüber einen Namen für den Listeneintrag, z. B. `AGB akzeptieren`. Dieser Name erscheint später im ANQP-Profil in der Auswahl für die **Netzwerk auth. Typ-Liste**.
- **Authentifizierungs-Typ**: Wählen Sie aus der Auswahlliste den Kontext, vor dem die Weiterleitung gilt. Mögliche 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 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

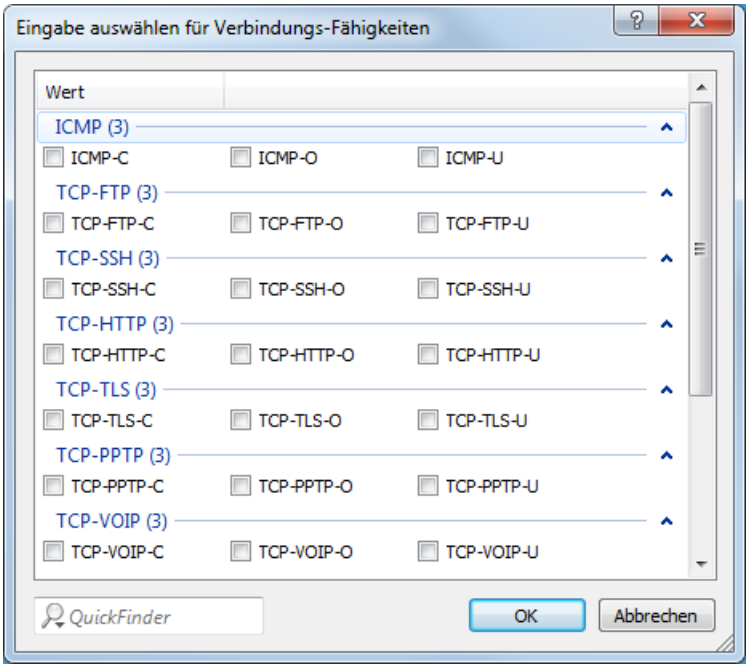
Über diese Tabelle verwalten Sie die Profillisten für Hotspot 2.0. **Hotspot 2.0 Profile** bieten Ihnen die Möglichkeit, bestimmte ANQP-Elemente (die der Hotspot-2.0-Spezifikation) zu gruppieren und sie in der Tabelle **Interfaces** unabhängig voneinander logischen WLAN-Schnittstellen zuzuweisen. Zu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



Um die Einträge in der Tabelle **Hotspot 2.0 Profile** zu bearbeiten, klicken Sie auf die Schaltfläche **Hinzufügen…**. Die Einträge im Bearbeitungsfenster haben folgende Bedeutung:

- **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.
- **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**:



Klicken Sie die Schaltfläche **Wählen** und geben Sie in dem sich öffnenden Eingabedialog für jeden Dienst die Verbindungs-Fähigkeit an. 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.

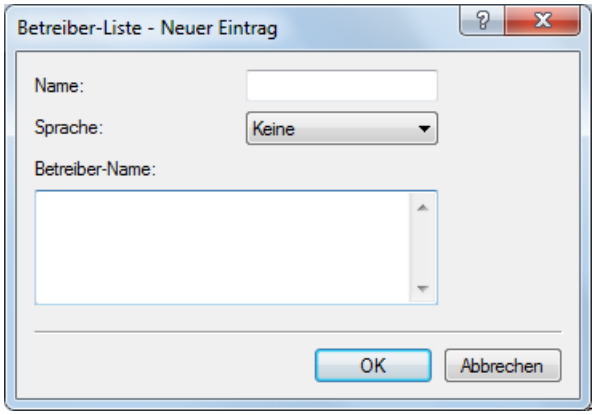
Über diesen Dialog legen Sie keine Berechtigungen fest! Die Angaben dienen den Stationen lediglich dazu, den Netzbeitritt über Ihr Gerät zu entscheiden. Spezifische Zugangsberechtigungen für Ihr Netzwerk konfigurieren Sie über andere Gerätefunktionen, wie z. B. die Firewall/QoS.

- **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*.

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.



Um die Einträge in der Tabelle **Betreiber-Liste** zu bearbeiten, klicken Sie auf die Schaltfläche **Hinzufügen…**. Die Einträge im Bearbeitungsfenster haben folgende Bedeutung:

- **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.

6.3.5 Ergänzungen im Setup-Menü

IEEE802.11u

Über die Tabellen und Parameter in diesem Menü nehmen Sie sämtliche Einstellungen für Verbindungen nach IEEE 802.11u und Hotspot 2.0 vor.

SNMP-ID:

2.71

Pfad Telnet:

Setup

ANQP-General

In diesem Menü nehmen die Sie allgemeine Einstellungen zu ANQP vor.

SNMP-ID:

2.71.6

Pfad Telnet:

Setup > **IEEE802.11u**

IPv4-Addr-Type

Über diesen Eintrag teilen Sie einer IEEE-802.11u-fähigen Station mit, ob diese nach erfolgreicher Authentifizierung am Hotspot des Betreibers eine IP-Adresse vom Typ IPv4 erhält.

SNMP-ID:

2.71.6.5

Pfad Telnet:

Setup > **IEEE802.11u** > **ANQP-General**

Mögliche Werte:

Not-Available

IPv4-Adresstyp ist nicht verfügbar.

Public-Addr-Available

Öffentliche IPv4-Adresse ist verfügbar.

Port-Restr-Addr-Avail

Port-beschränkte IPv4-Adresse ist verfügbar.

Single-Nat-Priv-Addr-Avail

Private, einfach NAT maskierte IPv4-Adresse ist verfügbar.

Double-Nat-Priv-Addr-Avail

Private, doppelt NAT maskierte IPv4-Adresse ist verfügbar.

Port-Restr-Single-Nat-Addr-Avail

Port-beschränkte IPv4-Adresse und einfach NAT maskierte IPv4-Adresse ist verfügbar.

Port-Restr-Double-Nat-Addr-Avail

Port-beschränkte IPv4-Adresse und doppelt NAT maskierte IPv4-Adresse ist verfügbar.

Availability-not-known

Die Verfügbarkeit eines IPv4-Adresstyps ist unbekannt.

Default:

Single-Nat-Priv-Addr-Avail

IPv6-Addr-Type

Über diesen Eintrag teilen Sie einer IEEE-802.11u-fähigen Station mit, ob diese nach erfolgreicher Authentifizierung am Hotspot des Betreibers eine IP-Adresse vom Typ IPv6 erhält.

SNMP-ID:

2.71.6.6

Pfad Telnet:

Setup > **IEEE802.11u** > **ANQP-General**

Mögliche Werte:

Not-Available

IPv6-Adresstyp ist nicht verfügbar.

Available

IPv6-Adresstyp ist verfügbar.

Availability-not-known

Die Verfügbarkeit eines IPv6-Adresstyps ist unbekannt.

Default:

Not-Available

Venue-Group

Die Standort-Gruppe (Venue Group) 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 vom 802.11u-Standard vorgegeben.

SNMP-ID:

2.71.6.1

Pfad Telnet:

Setup > **IEEE802.11u** > **ANQP-General**

Mögliche Werte:

- `Unspecified`: Unspezifiziert
- `Assembly`: Versammlung
- `Business`: Geschäft
- `Educational`: Ausbildung
- `Factory-and-Industrial`: Fabrik und Industrie
- `Institutional`: Institutional
- `Mercantile`: Handel
- `Resindential`: Wohnheim
- `Storage`: Lager
- `Utility-and-Miscellaneous`: Dienste und sonstiges
- `Vehicular`: Fahrzeug
- `Outdoor`: Außen

Default:

Unspecified

Venue-Type

Über den Standort-Typ-Code (Venue-Type) 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.

SNMP-ID:

2.71.6.2

Pfad Telnet:

Setup > **IEEE802.11u** > **ANQP-General**

Mögliche Werte:

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

Standort-Gruppe	Code = 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
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

Standort-Gruppe	Code = Standort-Typ-Code
	■ 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

Default:

0

Hotspot2.0

In diesem Menü nehmen die Sie allgemeine Einstellungen zu Hotspot 2.0 vor.

SNMP-ID:

2.71.7

Pfad Telnet:

Setup > **IEEE802.11u**

Connection-Capability

Diese Tabelle beinhaltet eine festgelegte Liste der Verbindungsfähigkeiten, auf die Sie in der Tabelle **Hotspot2.0-Profile** im Eingabefeld **Connection-Capabilities** (SNMP-ID 2.71.7.9.3) als kommaseparierte Liste referenzieren. Mögliche Statuswerte für die einzelnen Dienste sind 'closed' (**-C**), 'open' (**-O**) oder 'unknown' (**-U**).

SNMP-ID:

2.71.7.2

Pfad Telnet:

Setup > **IEEE802.11u** > **Hotspot2.0**

Hotspot2.0

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 **Setup** > **Schnittstellen** > **WLAN** > **IEEE802.11u** unter **HS20-Profil** 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.

SNMP-ID:

2.71.7.9

Pfad Telnet:

Setup > **IEEE802.11u** > **Hotspot2.0**

Name

Vergeben Sie hierüber einen Namen für das Hotspot-2.0-Profil. Diesen Namen geben Sie später in der Tabelle **Setup** > **Schnittstellen** > **WLAN** > **IEEE802.11u** unter **HS20-Profil** an.

SNMP-ID:

2.71.7.9.1

Pfad Telnet:

Setup > **IEEE802.11u** > **Hotspot2.0** > **Hotspot2.0**

Mögliche Werte:

String, max. 32 Zeichen

Default:

Operator-Name

Geben Sie in diesem Feld ein gültiges Profil für den Hotspot-Betreiber an.

SNMP-ID:

2.71.7.9.2

Pfad Telnet:

Setup > **IEEE802.11u** > **Hotspot2.0** > **Hotspot2.0**

Mögliche Werte:

Name aus Tabelle **Setup** > **IEEE802.11u** > **Hotspot2.0** > **Operator-List**, max. 65 Zeichen

Default:

Connection-Capabilities

Geben Sie in diesem Feld einen oder mehrere gültige Einträge aus zu den Verbindungs-Fähigkeiten an. 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.

SNMP-ID:

2.71.7.9.3

Pfad Telnet:

Setup > **IEEE802.11u** > **Hotspot2.0** > **Hotspot2.0**

Mögliche Werte:

Name aus Tabelle **Setup** > **IEEE802.11u** > **Hotspot2.0** > **Connection-Capability**, max. 252 Zeichen.
Mehrere Namen trennen Sie durch eine kommaseparierte Liste.

Default:

Operating-Class

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*.

SNMP-ID:

2.71.7.9.4

Pfad Telnet:

Setup > **IEEE802.11u** > **Hotspot2.0** > **Hotspot2.0**

Mögliche Werte:

Betriebsklassen-Code, max. 32 Zeichen

Default:

Operator-List

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.

SNMP-ID:

2.71.7.1

Pfad Telnet:

Setup > **IEEE802.11u** > **Hotspot2.0**

Name

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

SNMP-ID:

2.71.7.1.1

Pfad Telnet:

Setup > **IEEE802.11u** > **Hotspot2.0** > **Operator-List**

Mögliche Werte:

String, max. 32 Zeichen

Default:

Language

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

SNMP-ID:

2.71.7.1.4

Pfad Telnet:

Setup > **IEEE802.11u** > **Hotspot2.0** > **Operator-List**

Mögliche Werte:

Keine

Englisch

Deutsch

Chinesisch

Spanisch

Franzoesisch

Italienisch

Russisch

Niederlaendisch

Tuerkisch

Portugiesisch

Polnisch

Tschechisch

Arabisch

Default:

Keine

Operator-Name

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

SNMP-ID:

2.71.7.1.2

Pfad Telnet:

Setup > **IEEE802.11u** > **Hotspot2.0** > **Operator-List**

Mögliche Werte:

String, max. 252 Zeichen

Default:

leer

Uplink-Speed

Über diesen Eintrag geben Sie den Nominalwert der Sende-Bandbreite (Uplink) an, die einem angemeldeten Client an Ihrem Hotspot maximal zur Verfügung steht. Die Bandbreite selbst definieren Sie z. B. über das Public-Spot-Modul.

SNMP-ID:

2.71.7.8

Pfad Telnet:

Setup > **IEEE802.11u** > **Hotspot2.0**

Mögliche Werte:

0 bis 4294967295, in kBit/s

Default:

0

Link-Status

Über diesen Eintrag geben Sie den Konnektivitäts-Status Ihres Gerätes mit dem Internet an.

SNMP-ID:

2.71.7.4

Pfad Telnet:

Setup > **IEEE802.11u** > **Hotspot2.0**

Mögliche Werte:

- `Auto`: Das Gerät ermittelt den Statuswert für diesen Parameter automatisch.
- `Link-Up`: Die Verbindung zum Internet ist herstellt.
- `Link-Down`: Die Verbindung zum Internet ist unterbrochen.
- `Link-Test`: Die Verbindung zum Internet befindet sich im Aufbau oder wird geprüft.

Default:

Auto

Downlink-Speed

Über diesen Eintrag geben Sie den Nominalwert der Empfangs-Bandbreite (Downlink) an, die einem angemeldeten Client an Ihrem Hotspot maximal zur Verfügung steht. Die Bandbreite selbst definieren Sie z. B. über das Public-Spot-Modul.

SNMP-ID:

2.71.7.7

Pfad Telnet:

Setup > **IEEE802.11u** > **Hotspot2.0**

Mögliche Werte:

0 bis 4294967295, in KBit/s

Default:

0

Auth-Parameter

Diese Tabelle beinhaltet eine festgelegte Liste der möglichen Authentifizierungsparameter für die NAI-Realms, auf die Sie in der Tabelle **NAI-Realms** im Eingabefeld **Auth-Parameter** (SNMP-ID 2.71.9.4) als kommaseparierte Liste referenzieren.

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:
	SIM	SIM-Karte

Parameter	Sub-Parameter	Erläuterung
	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

SNMP-ID:

2.71.8

Pfad Telnet:

Setup > **IEEE802.11u**

Cellular-Network-Information-List

Über diese Tabelle verwalten Sie die Profillisten 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.

Im Setup-Menü weisen Sie diese Liste über die Tabelle **Setup** > **IEEE802.11u** > **IEEE802.11u** einem IEEE802.11u-Profil zu.

SNMP-ID:

2.71.4

Pfad Telnet:

Setup > **IEEE802.11u**

Name

Vergeben Sie hierüber einen Namen für das Mobilfunknetz-Profil, z. B. ein Kürzel des Netzanbieters in Kombination mit dem verwendeten Mobilfunkstandard. Diesen Namen geben Sie später in der Tabelle **Setup** > **IEEE802.11u** > **IEEE802.11u** unter **Cellular-List** an.

SNMP-ID:

2.71.4.1

Pfad Telnet:

Setup > **IEEE802.11u** > **Cellular-Network-Information-List**

Mögliche Werte:

String, max. 32 Zeichen

Default:

Country-Code

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.

SNMP-ID:

2.71.4.2

Pfad Telnet:

Setup > **IEEE802.11u** > **Cellular-Network-Information-List**

Mögliche Werte:

String, max. 3 Zeichen

Default:

Network-Code

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

SNMP-ID:

2.71.4.3

Pfad Telnet:

Setup > **IEEE802.11u** > **Cellular-Network-Information-List**

Mögliche Werte:

String, max. 3 Zeichen

Default:

ANQP-Profile

Über diese Tabelle verwalten Sie die Profillisten für IEEE802.11u bzw. ANQP. IEEE802.11u-Profile bieten Ihnen die Möglichkeit, bestimmte ANQP-Elemente zu gruppieren und sie in der Tabelle **Setup** > **Schnittstellen** > **WLAN** > **IEEE802.11u** unter **IEEE802.11u-Profil** 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.

SNMP-ID:

2.71.1

Pfad Telnet:

Setup > **IEEE802.11u**

Name

Vergeben Sie hierüber einen Namen für das IEEE802.11-Profil. Diesen Namen geben Sie später in der Tabelle **Setup** > **Schnittstellen** > **WLAN** > **IEEE802.11u** unter **IEEE802.11u-Profil** an.

SNMP-ID:

2.71.1.1

Pfad Telnet:

Setup > **IEEE802.11u** > **ANQP-Profile**

Mögliche Werte:

String, max. 32 Zeichen

Default:

Include-in-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 **Additional-OUI** konfigurieren. Zusätzliche OIs werden allerdings erst nach dem GAS-Request einer Station übertragen; sie sind für die Stationen also nicht unmittelbar sichtbar!

SNMP-ID:

2.71.1.2

Pfad Telnet:

Setup > **IEEE802.11u** > **ANQP-Profile**

Mögliche Werte:

OI, max. 65 Zeichen. Mehrere OIs trennen Sie durch eine kommaseparierte Liste.

Default:

Additional-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`.

SNMP-ID:

2.71.1.3

Pfad Telnet:

Setup > **IEEE802.11u** > **ANQP-Profile**

Mögliche Werte:

OI, max. 65 Zeichen. Mehrere OIs trennen Sie durch eine kommaseparierte Liste.

Default:

Domain-List

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 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 Hostpot seines Heimat-Providers, um mögliche Roaming-Kosten über den Access Point eines Roaming-Partners zu vermeiden.

SNMP-ID:

2.71.1.4

Pfad Telnet:

Setup > **IEEE802.11u** > **ANQP-Profile**

Mögliche Werte:

String, max. 65 Zeichen. Mehrere Domains trennen Sie durch eine kommaseparierte Liste.

Default:

NAI-Realm-List

Geben Sie in diesem Feld ein gültiges NAI-Realm-Profil an.

SNMP-ID:

2.71.1.5

Pfad Telnet:

Setup > **IEEE802.11u** > **ANQP-Profile**

Mögliche Werte:

Name aus Tabelle **Setup** > **IEEE802.11u** > **NAI-Realms**, max. 65 Zeichen

Default:

Cellular-List

Geben Sie in diesem Feld ein gültiges Mobilfunknetzwerk-Profil an.

SNMP-ID:

2.71.1.6

Pfad Telnet:

Setup > **IEEE802.11u** > **ANQP-Profile**

Mögliche Werte:

Name aus Tabelle **Setup** > **IEEE802.11u** > **Cellular-Network-Information-List**, max. 65 Zeichen

Default:

Network-Auth-Type-List

Geben Sie in diesem Feld ein oder mehrere gültiges Authentifizierungs-Parameter an.

SNMP-ID:

2.71.1.7

Pfad Telnet:

Setup > **IEEE802.11u** > **ANQP-Profile**

Mögliche Werte:

Name aus Tabelle **Setup** > **IEEE802.11u** > **Network-Authentication-Type**, max. 65 Zeichen. Mehrere Namen trennen Sie durch eine kommaseparierte Liste.

Default:

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.

Im Setup-Menü weisen Sie diese Liste über die Tabelle **Setup** > **IEEE802.11u** > **IEEE802.11u** einem IEEE802.11u-Profil zu.

SNMP-ID:

2.71.9

Pfad Telnet:

Setup > **IEEE802.11u**

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. Diesen Namen geben Sie später in der Tabelle **Setup** > **IEEE802.11u** > **IEEE802.11u** unter **NAI-Realm-List** an.

SNMP-ID:

2.71.9.1

Pfad Telnet:

Setup > **IEEE802.11u** > **NAI-Realms**

Mögliche Werte:

String, max. 32 Zeichen

Default:

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 IETF RFC 2486 definiert und entspricht im einfachsten Fall `<username>@<realm>`; für `user746@providerX.org` lautet der entsprechende Realm also `providerX.org`.

SNMP-ID:

2.71.9.2

Pfad Telnet:

Setup > **IEEE802.11u** > **NAI-Realms**

Mögliche Werte:

String, max. 32 Zeichen

Default:

EAP-Method

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

SNMP-ID:

2.71.9.3

Pfad Telnet:

Setup > **IEEE802.11u** > **NAI-Realms**

Mögliche Werte:

- `Kein`: Wählen Sie diese Einstellung, wenn der betreffende NAI-Realm keine Authentifizierung erfordert.
- `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 installieren muss.
- `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.

Default:

Kein

Auth-Parameter

Geben Sie in das Feld die zur EAP-Methode passenden Authentifizierungs-Parameter durch eine kommaseparierte Liste ein, z. B. für EAP-TTLS `NonEAPAuth.MSCHAPV2`,`Credential.UserPass` oder für EAP-TLS `Credentials.Certificate`.

SNMP-ID:

2.71.9.4

Pfad Telnet:

Setup > **IEEE802.11u** > **NAI-Realms**

Mögliche Werte:

Name aus Tabelle **Auth-Parameter**, max. 65 Zeichen. Mehrere Namen werden durch Kommas separiert.

Default:

Network-Authentication-Type

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.

SNMP-ID:

2.71.5

Pfad Telnet:

Setup > **IEEE802.11u**

Name

Vergeben Sie hierüber einen Namen für den Tabelleneintrag, z. B. `AGB akzeptieren`.

SNMP-ID:

2.71.5.3

Pfad Telnet:

Setup > **IEEE802.11u** > **Network-Authentication-Type**

Mögliche Werte:

String, max. 32 Zeichen

Default:

Network-Auth-Type

Wählen Sie aus der Liste den Kontext, vor dem die Weiterleitung gilt.

SNMP-ID:

2.71.5.1

Pfad Telnet:

Setup > **IEEE802.11u** > **Network-Authentication-Type**

Mögliche Werte:

- `Accept-Terms-Cond`: Es ist ein zusätzlicher Authentifizierungsschritt eingerichtet, bei dem ein Benutzer die Nutzungsbedingungen des Betreibers akzeptieren muss.
- `Online-Enrollment`: Es ist ein zusätzlicher Authentifizierungsschritt eingerichtet, bei dem ein Benutzer erst online registrieren muss.
- `Http-Redirection`: Es ist ein zusätzlicher Authentifizierungsschritt eingerichtet, zu dem ein Benutzer via HTTP weitergeleitet wird.
- `DNS-Redirection`: Es ist ein zusätzlicher Authentifizierungsschritt eingerichtet, zu dem ein Benutzer via DNS weitergeleitet wird.

Default:

Accept-Terms-Cond

Redirect-URL

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

SNMP-ID:

2.71.5.2

Pfad Telnet:

Setup > **IEEE802.11u** > **Network-Authentication-Type**

Mögliche Werte:

URL, max. 65 Zeichen

Default:

Venue-Name

In diese Tabelle geben Sie allgemeine Informationen zum Standort des Access Points ein.

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.

SNMP-ID:

2.71.3

Pfad Telnet:

Setup > **IEEE802.11u**

Name

Tragen Sie einen Namen für den Listeneintrag in die Tabelle ein, z. B. ein Sprach-Beschreibungspaar oder eine Indexnummer.

SNMP-ID:

2.71.3.1

Pfad Telnet:

Setup > **IEEE802.11u** > **Venue-Name**

Mögliche Werte:

String, max. 32 Zeichen

Default:

leer

Language

Wählen Sie hier die Sprache aus, in der Sie die Informationen zum Standort hinterlegen.

SNMP-ID:

2.71.3.3

Pfad Telnet:

Setup > **IEEE802.11u** > **Venue-Name**

Mögliche Werte:

Keine

Englisch

Deutsch

Chinesisch

Spanisch

Franzoesisch

Italienisch

Russisch

Niederlaendisch

Tuerkisch

Portugiesisch

Polnisch

Tschechisch

Arabisch

Default:

Keine

Venue-Name

Tragen Sie für die ausgewählte Sprache eine kurze Beschreibung zum Standort des Gerätes ein.

SNMP-ID:

2.71.3.2

Pfad Telnet:

Setup > **IEEE802.11u** > **Venue-Name**

Mögliche Werte:

String, max. 252 Zeichen

Default:

leer

IEEE802.11u

Die Tabelle **IEEE802.11u** ist die höchste Verwaltungsebene für 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.

SNMP-ID:

2.23.20.16

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN**

Ifc

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

SNMP-ID:

2.23.20.16.1

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **IEEE802.11u**

Operating

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 – respektiv 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 802.11-fähige Geräte als erste Filterkriterien bei der Netzsuche.

SNMP-ID:

2.23.20.16.2

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **IEEE802.11u**

Mögliche Werte:

ja

nein

Default:

nein

Hotspot2.0

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.

Diese Funktion setzt die aktivierte Unterstützung für Verbindungen nach IEEE 802.11u voraus!

SNMP-ID:

2.23.20.16.3

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **IEEE802.11u**

Mögliche Werte:

ja

nein

Default:

nein

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.

SNMP-ID:

2.23.20.16.4

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **IEEE802.11u**

Mögliche Werte:

ja

nein

Default:

nein

Network-Typ

Wählen Sie aus der vorgegebenen Liste einen Netzwerk-Typ aus, der das Wi-Fi-Netzwerk hinter der ausgewählten Schnittstelle am ehesten charakterisiert.

SNMP-ID:

2.23.20.16.5

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **IEEE802.11u**

Mögliche Werte:

- `Private`: 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.

- `Private-GuestAcc`: Wie `Private`, 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.
- `Public-Charge`: 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.
- `Public-Free`: 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.
- `Personal-Dev`: 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.
- `Emergency`: Beschreibt Netzwerke, die für Notdienste bestimmt und auf diese beschränkt sind. Wählen Sie diesen Typ z. B. bei angeschlossenen ESS- oder EBR-Systemen.
- `Experimental`: Beschreibt Netzwerke, die zu Testzwecken eingerichtet sind oder sich noch im Aufbaustadium befinden.
- `Wildcard`: Platzhalter für bislang undefinierte Netzwerk-Typen.

Default:

Private

Asra

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.

SNMP-ID:

2.23.20.16.6

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **IEEE802.11u**

Mögliche Werte:

ja

nein

Default:

nein

HESSID

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 (seine BSSID). 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".

SNMP-ID:

2.23.20.16.7

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **IEEE802.11u**

Mögliche Werte:

BSSID

user

none

Default:

BSSID

HESSID-MAC

Sofern Sie als **HESSID-Modus** die Einstellung `user` 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!

SNMP-ID:

2.23.20.16.8

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **IEEE802.11u**

Mögliche Werte:

MAC-Adresse, in Großbuchstaben und ohne Trennzeichen

Default:

000000000000

ANQP-Profil

Wählen Sie aus der Liste ein ANQP- bzw. 802.11u-Profil aus. 802.11u-Profile legen Sie im Setup-Menü über die Tabelle **Setup** > **IEEE802.11u** > **ANQP-Profile** an.

SNMP-ID:

2.23.20.16.10

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **IEEE802.11u**

Mögliche Werte:

Name aus Tabelle **Setup** > **IEEE802.11u** > **ANQP-Profile**, max. 32 Zeichen

Default:

HS20-Profil

Wählen Sie aus der Liste ein Hotspot-2.0- bzw. HS20-Profil aus. HS20-Profile legen Sie im Setup-Menü über die Tabelle **Setup** > **IEEE802.11u** > **Hotspot2.0** an.

SNMP-ID:

2.23.20.16.13

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **IEEE802.11u**

Mögliche Werte:

Name aus Tabelle **Setup** > **IEEE802.11u** > **Hotspot2.0**, max. 32 Zeichen

Default:

7 Public Spot

7.1 Template-Variablen

An einem Public Spot haben Sie die Möglichkeit, ausgewählte Variablen über die URL an die Templates – also die einem Benutzer angezeigten Webseiten des Public-Spot-Moduls – zu übergeben. Auf diesem Wege lassen sich z. B. SSID- oder VLAN-ID-abhängige Anmeldeseiten realisieren oder dem Benutzer zusätzliche Verbindungsinformationen auf der Anmeldeseite anzeigen.

Folgende Variablen stehen Ihnen zur Auswahl:

%i

Platzhalter für die **NAS-Port-Id**. "NAS" steht in diesem Zusammenhäng 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.

%s

Platzhalter für die **SSID**. Wenn das genutzte Gerät ein Access Point ist, übertragt diese Variable die SSID, z. B. `PUBLICSPOT`.

%v

Platzhalter für die **Quell-VLAN**. Sofern dem anfragenden Client eine VLAN zugewiesen wurde, überträgt diese Variable die Quell-VLAN-ID.

Um die Variablen für ein Template zu verwenden, legen Sie unter **Public-Spot-Modul** > **Seitentabelle** für die jeweilige Seite den **Request-Typ** fest und ergänzen die **Seiten-Adresse (URL)**, unter der sich die angepassten Templates befinden, um die einzelnen 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`

7.2 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.

7.2.1 Individueller Text auf der Anmeldeseite

Sie haben innerhalb des Public Spot-Moduls die Möglichkeit, einen individuelle Text anzugeben, welcher auf der Anmeldeseite innerhalb der Box des Anmeldeformulars eingeblendet wird. Führen Sie dazu die nachfolgenden Schritte aus.

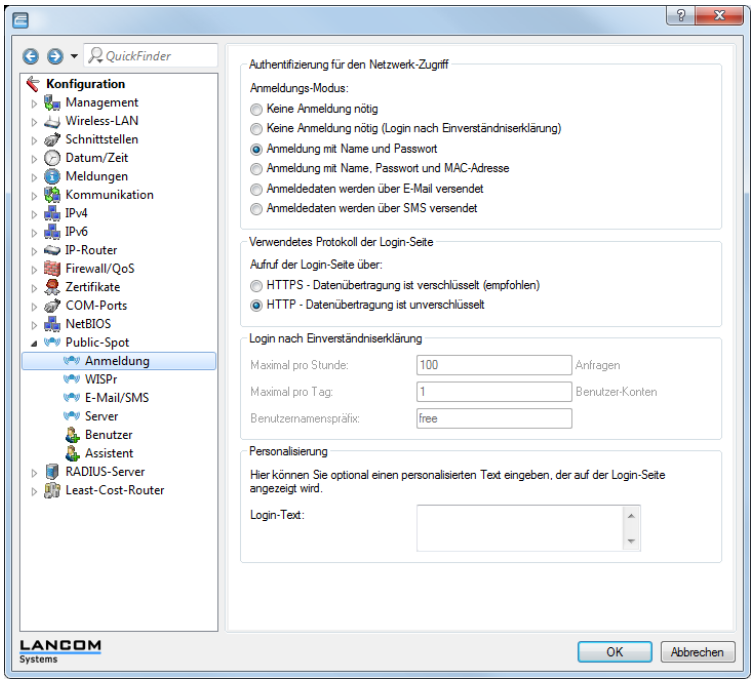
1. Öffnen Sie in LANconfig den Konfigurationsdialog für das betreffende Gerät.

2. Wechseln Sie in den Dialog **Public Spot** > **Anmeldung** und tragen Sie im Abschnitt **Personalisierung** 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. Um Umlaute einzugeben, müssen Sie deren HTML-Äquivalente verwenden (z. B. `&uuml;` für ü). 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>)
```



3. Klicken Sie **OK**, um den Login-Text in das Gerät zu laden.

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

7.2.2 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 Coporate 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 Variaten 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.

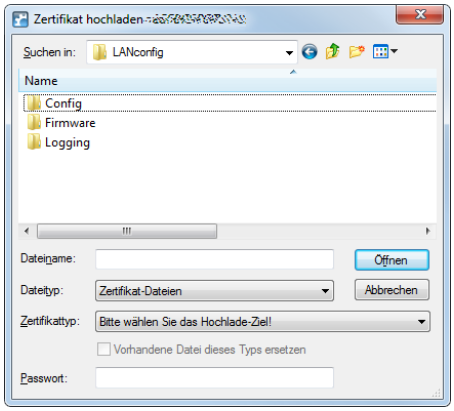
Abbildung 1: Anmeldeseite für breite Bildschirme

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.

7.2.3 Ergänzungen im Setup-Menü

Login-Text

Die Einstellung bietet Ihnen die Möglichkeit, einen individuelle Text anzugeben, den das Gerät auf der Anmeldeseite des Public Spot-Moduls innerhalb der Box des Anmeldeformulars einblendet. Um Umlaute einzugeben, sollten 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>)
```

SNMP-ID:

2.24.33

Pfad Telnet:

Setup > **Public-Spot-Modul**

Mögliche Werte:

Beliebiger String, max. 254 Zeichen aus

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

Default:

7.3 Selbstständige Benutzeranmeldung – Einfacher Login

Als Alternative zur selbständigen Benutzeranmeldung via E-Mail oder SMS haben Sie ab LCOS 8.82 die Möglichkeit, das Anlegen und Authentifizieren von Public-Spot-Nutzern automatisch über einem RADIUS-Server abzuwickeln, nachdem die Nutzer die Nutzungsbedingungen für das WLAN-Netzwerk akzeptiert haben.

7.3.1 Selbständige Benutzeranmeldung (Smart Ticket)

Geräte mit Public Spot bieten Anwendern einen zeitlich begrenzten Zugang zu drahtlosen Netzwerken. Für das Anlegen eines solchen Zugangs war bisher ein Administrations-Account auf dem Gerät mit Public Spot erforderlich. Für die Mitarbeiter an der Rezeption in einem Hotel legen Sie dazu z. B. einen speziellen Administrations-Account an, der ausschließlich über die Funktionsrechte zum Anlegen von Public Spot-Benutzern verfügt. Mit wenigen Mausklicks kann der Mitarbeiter dann den Hotelgästen einen Voucher für den Zugang zum drahtlosen Netzwerk ausdrucken.

Da allerdings auch die komfortable Lösung mit Vouchers immer die Aktivität eines Administrators erfordert, können Sie den Nutzern alternativ die Möglichkeit einräumen, auf der Startseite des Public Spot selbst Zugangsdaten zum drahtlosen Netzwerk zu generieren und sich die Zugangsdaten per E-Mail oder SMS zusenden zu lassen. Voraussetzung für die Zusendung per E-Mail ist ein in den Geräteeinstellungen vollständig eingerichtetes SMTP-Konto. Für die Zusendung per SMS nutzt das Gerät einen externen SMS-Dienstanbieter, der je nach Wunsch den Betreiber oder den Benutzer des Public Spots mit den Gebühren der SMS belastet.

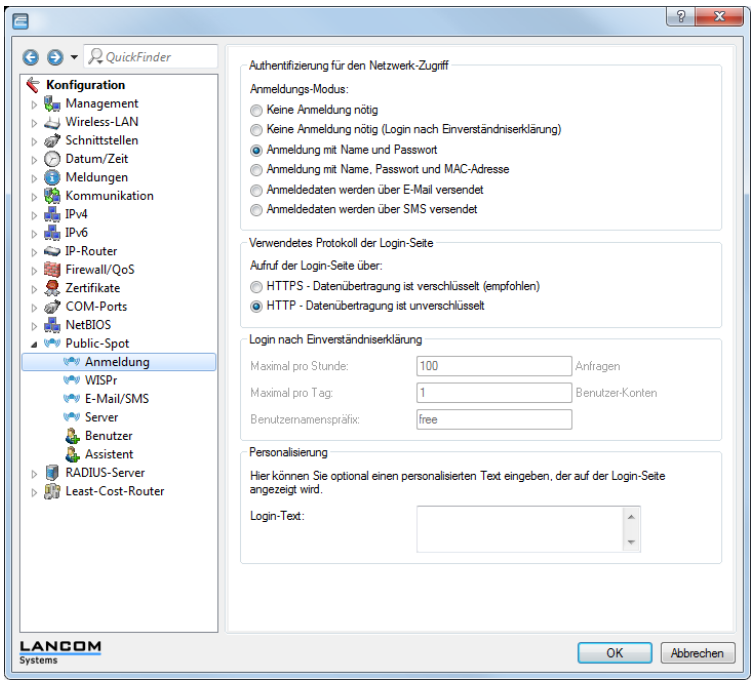
Alternativ bietet das Gerät Ihnen die Möglichkeit, die Anmeldung für Public Spot-Nutzer völlig transparent über einen Radius-Server abzuwickeln. Der Benutzeranmeldung ist in diesem Fall eine Abfrage vorangestellt, bei der die Nutzer zunächst den im Gerät hinterlegten Nutzungsbestimmungen zustimmen müssen, bevor sie automatisch Zugang zum

Public Spot erhalten (Ein-Klick-Anmeldung). Ein nutzerseitiges Erstellen eigener Zugangsdaten via E-Mail oder SMS entfällt bei dieser Authentifizierungsmethode.

7.3.2 Ergänzungen in LANconfig

Übersicht der Anmeldemodi

In diesem Dialog legen Sie die Einstellungen für die Authentifizierung am Netzwerk fest.



Folgende Anmeldungs-Modi 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 Nutzungsbestimmungen des Betreibers akzeptiert haben (Ein-Klick-Anmeldung). Die Anmeldung erfolgt dabei für die Nutzer völlig transparent über einen Radius-Server. Voraussetzung dafür ist, dass Sie eine individuelle Willkommensseite inklusive eigener Nutzungsbestimmungen eingerichtet haben: In diesem Fall leitet der Public Spot einen neuen Nutzer zunächst auf die Willkommensseite weiter, deren Nutzungsbestimmungen er zustimmen muss. Nach der Bestätigung legt das Gerät entsprechend der Standardwerte für den **Benutzer-Erstellungs-Assistent** (unter **Public-Spot** > **Assistent**) automatisch ein Benutzerkonto an und gibt den Zugriff auf das angeschlossene Netzwerk frei.

  Im Rahmen **Login nach Einverständniserklärung** legen Sie die Rahmenbedingungen für das Erstellen von freien Benutzerkonten durch den RADIUS-Server fest:

  - **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.

Um eine eigene Willkommensseite (htm, html) in das Gerät zu laden, nutzen Sie die Upload-Funktion unter **Gerät** > **Konfigurations-Verwaltung** > **Zertifikat oder Datei hochladen** und referenzieren unter **Public-Spot** > **Server** > **Seiten-Tabelle** > **Willkommen** im Eingabefeld **Seiten-Adresse (URL)** mit `file://pbspot_template_welcome` auf diese Datei. Vorlagen für eine Willkommensseite sowie detailliertere Informationen zum Hochladen eigener Templates finden Sie im Internet in der LANCOM Support Knowledgebase unter *Implementierung eigener Webseiten*.

Die in der Willkommensseite hinterlegten Nutzungsbedingungen sind nicht mit der Nutzungsbedingungsseite zu verwechseln. Die Seite **Nutzungsbedingungen** ist eine Sonderseite, die nach gesonderter Aktivierung nur im Zusammenhang mit der Anmeldung via E-Mail/SMS angezeigt wird.

Ist keine Willkommensseite eingerichtet, 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**

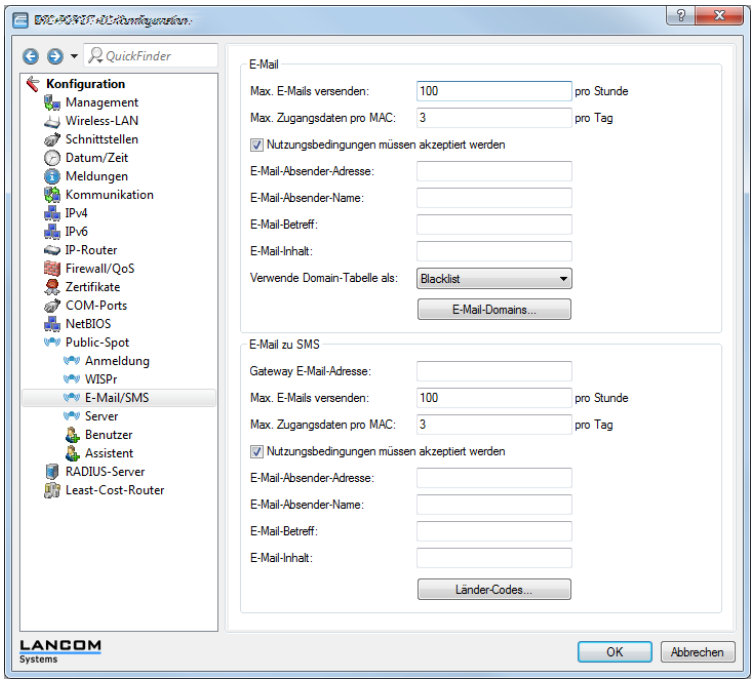
  Nutzer melden sich am Public Spot mit ihrem Namen und ihrem Passwort an. Die Login-Daten generieren sich die Nutzer selbst; zugestellt werden die Daten per E-Mail. Die Aktivität eines Administrators ist nicht erforderlich.

- **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.

Konfiguration der E-Mail/SMS-Anmeldung

Sie definieren die Einstellungen für den Versand der Anmeldedaten über E-Mail oder SMS im Dialog **Public-Spot** > **E-Mail/SMS**.



Dabei haben Sie folgende Konfigurationsmöglichkeiten:

- **Max. E-Mails versenden**: Tragen Sie hier die maximale Anzahl an E-Mails ein, die das Public Spot-Modul innerhalb einer Stunde an Benutzer für die Anmeldung über E-Mail verschicken darf. Reduzieren Sie den Wert, um die Anzahl der neuen Benutzer pro Stunde zu verringen.
- **Max. Zugangsdaten pro MAC**: Geben Sie an, wie viele verschiedene Zugangsdaten das Gerät für eine MAC-Adresse innerhalb eines Tages bereitstellen darf.
- **Nutzungsbedingungen müssen akzeptiert werden**: Wenn Sie diese Option aktivieren, zeigt der Public Spot auf der Anmeldeseite ein zusätzliches Optionsfeld an, welches die Benutzer vor der Registrierung via E-Mail/SMS zum Akzeptieren der Nutzungsbedingungen auffordert.

  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.
- **E-Mail-Absender-Adresse**: Geben Sie die E-Mail-Adresse an, die Ihren Nutzern bei der Zustellung der E-Mail als Absendeadresse angezeigt wird, z. B. `support@providerX.org`.
- **E-Mail-Absender-Name**: Geben Sie den Namen an, der Ihren Nutzern bei der Zustellung der E-Mail als Absender angezeigt wird, z. B. `Provider X`. Wenn Sie dieses Feld leer lassen, trägt das Gerät automatisch den im Folgekapitel beschriebenen Standardtext ein.
- **E-Mail-Betreff**: Geben Sie die Betreffzeile für die E-Mail an. Wenn Sie dieses Feld leer lassen, trägt das Gerät automatisch den im Folgekapitel beschriebenen Standardtext ein.
- **E-Mail-Inhalt:** Geben Sie den Nachrichtentext für die E-Mail an. Sie können darin die folgenden Variablen nutzen:
  $PSpotPasswd

  Platzhalter für das nutzerspezifische Passwort des Public Spot-Zugangs.s

  $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.

Wenn Sie dieses Feld leer lassen, trägt das Gerät automatisch den im Folgekapitel beschriebenen Standardtext ein.

- **Verwende Domain-Tabelle als**: Geben Sie 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.
- **Gateway E-Mail-Adresse**: Tragen Sie hier 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.
- **Länder-Codes**: In dieser Tabelle tragen Sie die vom Gerät akzeptierten Länder-Codes ein. Die Eingabe eines Länder-Codes kann direkt oder mit vorangestellter Doppel-Null erfolgen, zum Beispiel für Deutschland `49` oder `0049`.

  Diese Tabelle agiert Whitelist. Sie **müssen** Länder-Codes definieren, damit ein Versand der Login-Daten erfolgt!

7.3.3 Ergänzungen im Setup-Menü

Authentifizierungs-Modus

Ihr Gerät unterstützt unterschiedliche Arten der Authentifizierung für den Netzwerk-Zugriff im Public Spot. Sie können zunächst festlegen, ob sich ein Benutzer überhaupt anmelden muss. Der Public Spot speichert die Zugangsdaten in der Benutzer-Tabelle. Falls Sie sich für ein Anmeldeverfahren entscheiden, haben Sie drei Möglichkeiten:

- Die Anmeldung erfolgt mit Benutzername und Passwort oder zusätzlich mit der physikalischen bzw. MAC-Adresse. In diesem Fall teilt der Adminstrator den Benutzern die Zugangsdaten z. B. über einen Ausdruck mit.
- Die Anmeldung erfolgt mit Benutzername und Passwort, welche sich der Benutzer selber generiert. Der Versand der Zugangsdaten bei erstmaliger Anmeldung automatisch entweder per E-Mail oder per SMS.
- Die Anmeldung erfolgt automatisiert über einen RADIUS-Server, nachdem der Benutzer die Nutzungsbedingungen auf der vom Administrator eingerichteten Willkommensseite akzeptiert hat. Die Zugangsdaten selbst bleiben dem Benutzer verborgen; sie werden von ihm auch nicht benötigt. Die Anlage eines Benutzerkontos über den RADIUS-Server erfolgt lediglich zur internen Verwaltung der betreffenden Nutzer.

SNMP-ID:

2.24.1

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Modus**

Mögliche Werte:

keine

Benutzer+Passwort

MAC+Benutzer+Passwort

E-Mail

E-Mail2SMS

Login-nach-Einverstaendniserklaerung

Default:

keine

Authentifizierungs-Module

In diesem Menüpunkt definieren Sie einzelne Parameter zur Benutzung des Netzwerk-Zugriffs und legen fest, wie und mit welchen Parametern die Authentifizierung und der Versand der Anmeldedaten erfolgt.

SNMP-ID:

2.24.41

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module**

Login-nach-Einverstaendniserklaerung

In diesem Menü nehmen Sie die Einstellungen für die automatische Anmeldung und Authentifizierung via RADIUS vor.

SNMP-ID:

2.24.41.4

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module**

Benutzer-Konto-Pro-Tag

Dieser Eintrag zeigt für den bezeichneten Anmeldungs-Modus die Anzahl der Konten, die ein Nutzer am Tag anlegen kann. Ist dieser Wert erreicht und die Nutzer-Session abgelaufen, kann sich ein Benutzer für den betreffenden Tag nicht mehr automatisch am Public Spot anmelden und authentifizieren lassen.

SNMP-ID:

2.24.41.4.2

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **Login-nach-Einverstaendniserklaerung**

Mögliche Werte:

0 bis 65535

Default:

1

Benutzername-Prefix

Dieser Eintrag enthält den Prefix, der automatisch generierten Public-Spot-Benutzernamen vorangestellt wird, wenn Sie vom Gerät im Anmeldungs-Modus "Kein-Authentifizierung" (automatische Anmeldung und Authentifizierung) erstellt wurden.

SNMP-ID:

2.24.41.4.3

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **Login-nach-Einverstaendniserklaerung**

Mögliche Werte:

String, max. 10 Zeichen

Default:

free

Max-Request-Pro-Stunde

Dieser Eintrag zeigt die maximale Anzahl der Benutzer pro Stunde an, die sich am Gerät automatisch ein Konto erstellen können. Verringern Sie diesen Wert, um Leistungseinbußen durch übermäßig viele Nutzer zu reduzieren.

SNMP-ID:

2.24.41.4.1

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **Login-nach-Einverstaendniserklaerung**

Mögliche Werte:

0 bis 65535

Default:

100

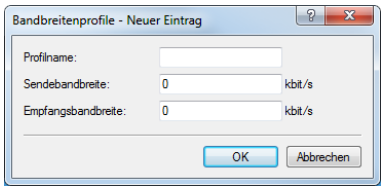
7.4 Bandbreitenprofile

Ab LCOS 8.82 haben Sie die Möglichkeit, Bandbreitenprofile für Public Spot-Nutzer einzurichten.

7.4.1 Ergänzungen in LANconfig

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. 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.



Um die Einträge in der Tabelle **Bandbreitenprofile** zu bearbeiten, klicken Sie auf die Schaltfläche **Hinzufügen…**. Die Einträge im Bearbeitungsfenster haben folgende Bedeutung:

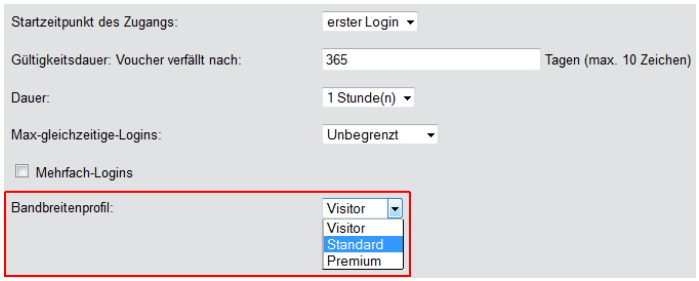
- **Profilname**: Geben Sie hier den Namen für das Bandbreitenprofil ein.
- **Sendebandbreite**: Geben Sie hier die maximale Bandbreite (in KBit/s) ein, die einem Public Spot-Benutzer im Uplink zur Verfügung stehen soll. Um die Bandbreite auf z. B. 1 MBit/s zu beschränken, tragen Sie den Wert `1024`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



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

7.4.2 Ergänzungen im Setup-Menü

Bandbreitenprofile

In dieser Tabelle verwalten Sie die einzelnen Bandbreitenprofile. Über ein Bandbreitenprofil haben Sie die Möglichkeit, die Public-Spot-Benutzern zur Verfügung gestellte Bandbreite (Uplink und Downlink) bei der Kontoerstellung selektiv zu beschränken.

SNMP-ID:

2.24.19.17

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Neuer-Benutzer-Assistent**

Profilename

Geben Sie hier den Namen für das Bandbreitenprofil ein.

SNMP-ID:

2.24.19.17.1

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Neuer-Benutzer-Assistent** > **Bandbreitenprofile**

Mögliche Werte:

String, max. 255 Zeichen

Default:

TX-Bandbreite

Geben Sie hier die maximale Bandbreite (in Bit/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.

SNMP-ID:

2.24.19.17.2

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Neuer-Benutzer-Assistent** > **Bandbreitenprofile**

Mögliche Werte:

0 bis 4294967295

Default:

0

RX-Bandbreite

Geben Sie hier die maximale Bandbreite (in Bit/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.

SNMP-ID:

2.24.19.17.3

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Neuer-Benutzer-Assistent** > **Bandbreitenprofile**

Mögliche Werte:

0 bis 4294967295

Default:

0

7.5 Dynamische VLAN-Zuweisung via RADIUS

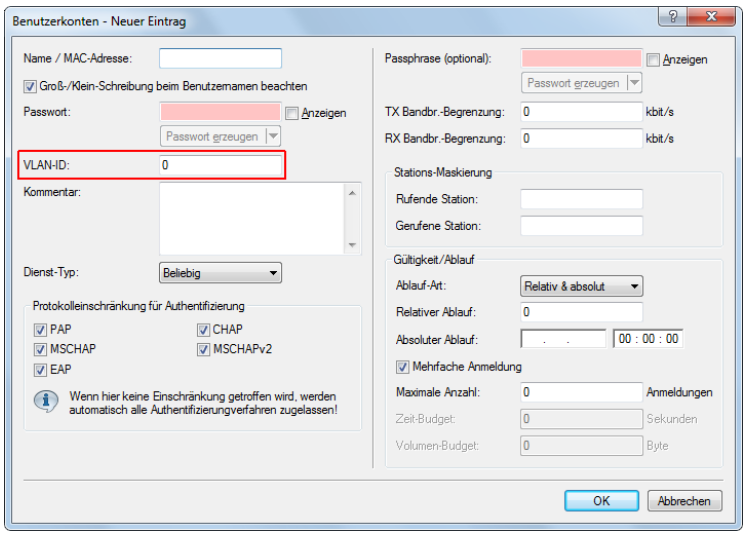
Ab LCOS 8.82 haben Sie die Möglichkeit, einzelnen Public-Spot-Nutzern bei der Anmeldung eine individuelle VLAN-ID zuzuweisen. Anhand dieser ID können Sie dann z. B. über die Firewall weitere Rechte und Regeln festlegen, die für den verschiedenen Nutzer gelten.

7.5.1 Ergänzungen in LANconfig

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-ServerAllgemein** 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.

7.5.2 Ergänzungen im Setup-Menü

VLAN-Id

Über dieses Eingabefeld weisen Sie dem Benutzer eine individuelle 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 – im Setup-Menü unter **Setup** > **DHCP** – möglichst gering einzustellen. Mögliche Werte (in Minuten) sind z. B.:

- **Max.-Gueltigkeit-Minuten**: 2
- **Default-Gueltigkeit-Minuten**: 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 anderen 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.

SNMP-ID:

2.24.42.8

Pfad Telnet:

Setup > **RADIUS** > **Server** > **Benutzer**

Mögliche Werte:

0 bis 4094

Default:

4

7.6 Automatisches Re-Login

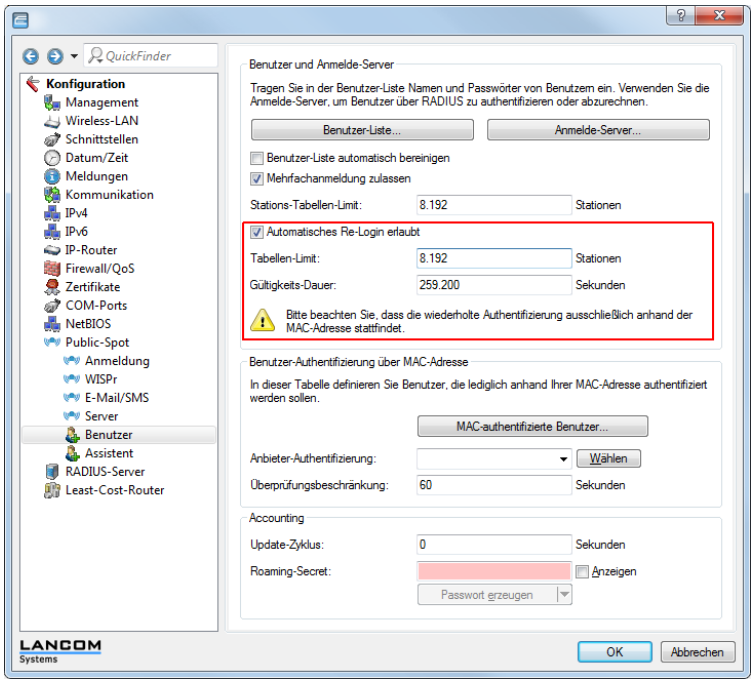
Mobile WLAN-Clients (z. B. Smartphones und Tablett-PCs) buchen sich automatisch in bekannte WLAN-Netze (SSID) ein, wenn sie erneut deren Funkzelle erreichen. Viele Apps greifen in diesem Fall automatisch ohne Umweg über den Webbrowser auf Webinhalte zu, um aktuelle Daten abzufragen (z. B. E-Mails, Soziale 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.

7.6.1 Ergänzungen im Setup-Menü

Auto-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. Emails, soziale Netzwerke, Wetterbericht etc.). In diesen Fällen ist es unpraktisch, wenn der Benutzer sich zunächst erneut im Browser manuell an einem Public Spot authentifizieren muss.

Mit dem automatischen Re-Login genügt es, wenn der Benutzer sich beim erstmaligen Aufenthalt in der Funkzelle am Public Spot identifiziert. Nach einer zwischenzeitlichen 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.

Bitte beachten Sie, dass die Authentifizierung ausschließlich anhand der MAC-Adresse stattfindet, wenn Auto-Re-Login aktiviert ist.

In diesem Menüpunkt konfigurieren Sie die Parameter für das automatische Re-Login.

SNMP-ID:

2.24.50

Pfad Telnet:

Setup > **Public-Spot-Modul**

Aktiv

Mit dieser Aktion aktivieren bzw. deaktivieren sie das automatische Re-Login.

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

SNMP-ID:

2.24.50.1

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Auto-Re-Login**

Mögliche Werte:

ja

nein

Default:

nein

Stations-Tabellen-Limit

Sie können die maximale Anzahl der Clients, die die Funktion Re-Login nutzen dürfen, auf bis zu 65536 Teilnehmer vergrößern.

Während des Betriebs wird ausschließlich eine Vergrößerung der Stationstabelle sofort übernommen. Starten Sie den Access-Point neu, damit eine Reduzierung der Stationstabelle wirksam wird.

SNMP-ID:

2.24.50.2

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Auto-Re-Login**

Mögliche Werte:

16 bis 65536

Default:

8192

Exist-Timeout

Dieser Wert gibt an, wie lange der Public Spot die Anmeldedaten eines WLAN-Clients für ein Re-Login in der Tabelle speichert. Nach Ablauf dieser Frist (in Sekunden) muss sich der Public-Spot-Benutzer erneut über den Browser auf der Anmeldeseite des Public Spots anmelden.

Sofern ein Public-Spot-Nutzer über ein Zeitkontingent verfügt, welches kleiner ist als der hier eingestellte Timeout-Wert, ist dieser Parameter für ihn wirkungslos. Ein automatisches Re-Login findet nicht statt, sobald ein Benutzer den Status "Unauthentifiziert" trägt.

SNMP-ID:

2.24.50.3

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Auto-Re-Login**

Mögliche Werte:

max. 10 Zeichen

Default:

259200

7.6.2 Ergänzungen im Status-Menü

Auto-Re-Login

Dieses Menü enthält die Statuswerte für das automatische Re-Login der Public-Spot-Benutzer.

SNMP-ID:

1.44.8

Pfad Telnet:

Status > **Public-Spot**

Stations-Tabelle

Diese Tabelle enthält die Anmeldedaten der am Public Spot angemeldeten Benutzer. Anhand dieser Tabelle kann der Public Spot den Benutzern ein automatisches Re-Login ermöglichen.

SNMP-ID:

1.44.8.1

Pfad Telnet:

Status > **Public-Spot** > **Auto-Re-Login**

MAC-Adresse

Enthält die MAC-Adresse, mit der der WLAN-Client zuletzt am Public Spot angemeldet war.

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

IP-Adresse

Enthält die IP-Adresse, mit der der WLAN-Client zuletzt am Public Spot angemeldet war.

Benutzername

Enthält den Benutzernamen, mit dem der Benutzer zuletzt am Public Spot angemeldet war.

Exist-Timeout

Gibt die Dauer in Sekunden an, für die sich der Benutzer automatisch am Public Spot anmelden kann, ohne sich erneut authentifizieren zu müssen.

7.7 Anmeldung über WISPr

Zusätzlich zur Unterstützung von IEEE 802.11u und Hotspot 2.0 bietet Ihnen LCOS 8.82 eine Schnittstelle zum WISPr-Protokoll, um auch Smart- bzw. Legacy-Clients, die kein 802.11u unterstützen, eine automatische, Hotspot-2.0-ähnliche Anmeldung an Ihrem Hotspot anzubieten. Beachten Sie als Betreiber dabei, dass sowohl Ihr Internet-Service-Provider als auch das Gerät des Nutzers eine entsprechende technische Infrastruktur bereitstellen muss.

7.7.1 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:

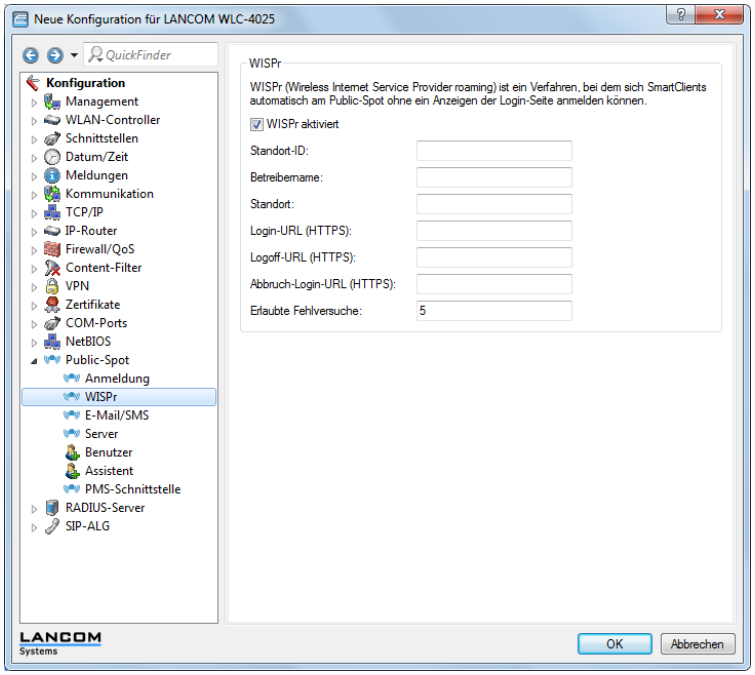
```
<HTML>
<?xml version=”1.0” encoding=”UTF-8”?>
  <WISPAccessGatewayParam
xmlns:xsi=”http://www.w3.org/2001/XMLSchema-instance”
   xsi:noNamespaceSchemaLocation=”http://www.acmewisp.com/WISPAccess
GatewayParam.xsd”>
    <Redirect>
      <AccessProcedure>1.0</AccessProcedure>
      <AccessLocation>Hotel 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. Weitere Informationen zum Laden dieser Objekte in Ihr Gerät finden Sie im LANCOM-Techpaper "Zertifikatsmanagement im Public Spot". 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.

7.7.2 Ergänzungen in LANconfig

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 LANCOM Public Spot selbst. Falls der LANCOM Public Spot selbst Benutzer über WISPr authentifizieren soll geben Sie die URL an in der Form `https://<FQDN-des-LANCOMs>/wisprlogin`. Für "wisprlogin" im Bespiel 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 LANCOM verwendet wird, z. B.:

- Login-URL: https://<FQDN-des-LANCOMs>/wisprlogin
- Logoff-URL: https://<FQDN-des-LANCOMs>/wisprlogoff
- Abbruch-Login-URL: https://<FQDN-des-LANCOMs>/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.

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**

7.7.3 Ergänzungen im Setup-Menü

Abbruch-Login-URL

Geben Sie die HTTPS-Adresse ein, an die das Gerät einen WISPr-Client weiterleitet, wenn die Authentifizierung fehlschlägt.

SNMP-ID:

2.24.42.7

Pfad Telnet:

Setup > **Public-Spot-Modul** > **WISPr**

Mögliche Werte:

HTTPS-URL, max. 255 Zeichen

Default:

In-Betrieb

Aktivieren oder deaktivieren Sie die WISPr-Funktion für Ihr Gerät.

SNMP-ID:

2.24.42.1

Pfad Telnet:

Setup > **Public-Spot-Modul** > **WISPr**

Mögliche Werte:

nein

ja

Default:

nein

Login-URL

Geben Sie die HTTPS-Adresse ein, an die die WISPr-Client die Zugangsdaten für Ihren Internet-Service-Provider übermittelt.

SNMP-ID:

2.24.42.5

Pfad Telnet:

Setup > **Public-Spot-Modul** > **WISPr**

Mögliche Werte:

HTTPS-URL, max. 255 Zeichen

Default:

Logout-URL

Geben Sie die HTTPS-Adresse ein, über die sich ein WISPr-Client von Ihrem Internet-Service-Provider abmeldet.

SNMP-ID:

2.24.42.6

Pfad Telnet:

Setup > **Public-Spot-Modul** > **WISPr**

Mögliche Werte:

HTTPS-URL, max. 255 Zeichen

Default:

Max-Authen-Fehler

Geben Sie hier die Anzahl der Fehlversuche ein, welche die Login-Seite Ihres Internet-Service-Providers maximal erlaubt.

SNMP-ID:

2.24.42.8

Pfad Telnet:

Setup > **Public-Spot-Modul** > **WISPr**

Mögliche Werte:

0 bis 65535

Default:

5

Operator-Name

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.

SNMP-ID:

2.24.42.3

Pfad Telnet:

Setup > **Public-Spot-Modul** > **WISPr**

Mögliche Werte:

String, max. 255 Zeichen, mit folgenden Zeichenbeschränkungen:

```
Alphanummerische Zeichen:  [0-9][A-Z][a-z]
Sonderzeichen:             @{|}~!$%&'()+-,/:;<=>?[\]^_`.
```

Default:

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>`.

SNMP-ID:

2.24.42.2

Pfad Telnet:

Setup > **Public-Spot-Modul** > **WISPr**

Mögliche Werte:

String, max. 255 Zeichen, mit folgenden Zeichenbeschränkungen:

```
Alphanummerische Zeichen:  [0-9][A-Z][a-z]
Sonderzeichen:             @{|}~!$%&'()+-,/:;<=>?[\]^_`.
```

Default:

Standort-Name

Beschreiben Sie den Standort Ihres Gerätes, z. B. `CafeX_Markt3`. Diese Angabe dient einem Nutzer zur besseren Identifizierung Ihres Hotspots.

SNMP-ID:

2.24.42.4

Pfad Telnet:

Setup > **Public-Spot-Modul** > **WISPr**

Mögliche Werte:

String, max. 255 Zeichen, mit folgenden Zeichenbeschränkungen:

```
Alphanummerische Zeichen:  [0-9][A-Z][a-z]
Sonderzeichen:             @{|}~!$%&'()+-,/:;<=>?[\]^_`.
```

Default:

7.8 PMS-Schnittstelle

Ab LCOS 8.82 haben Sie die Möglichkeit, das Public-Spot-Modul mit dem Hotel-Property-Management-System von Micros Fidelio zu verknüpfen, um Ihren Gästen bereits bei der Registrierung automatisch einen Zugang zu Ihrem Hotspot bereitzustellen. Die Aktivität eines zusätzlichen Public-Spot-Administrators (z. B. für das Erstellen von Vouchern) entfällt hierbei.

Die PMS-Schnittstelle ist derzeit ausschließlich für die folgenden Geräteypen und -serien verfügbar:

- LANCOM 1780-Serie
- LANCOM 1781-Serie
- LANCOM WLC-4006
- LANCOM WLC-4006+
- LANCOM WLC-4025
- LANCOM WLC-4025+
- LANCOM WLC-4100
- LANCOM 7100 VPN
- LANCOM 7100+ VPN
- LANCOM 9100 VPN
- LANCOM 9100+ VPN

7.8.1 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.

Die PMS-Schnittstelle ist derzeit ausschließlich für die folgenden Geräteypen und -serien verfügbar:

- LANCOM 1780-Serie
- LANCOM 1781-Serie
- LANCOM WLC-4006
- LANCOM WLC-4006+
- LANCOM WLC-4025
- LANCOM WLC-4025+

- LANCOM WLC-4100
- LANCOM 7100 VPN
- LANCOM 7100+ VPN
- LANCOM 9100 VPN
- LANCOM 9100+ VPN

7.8.2 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.

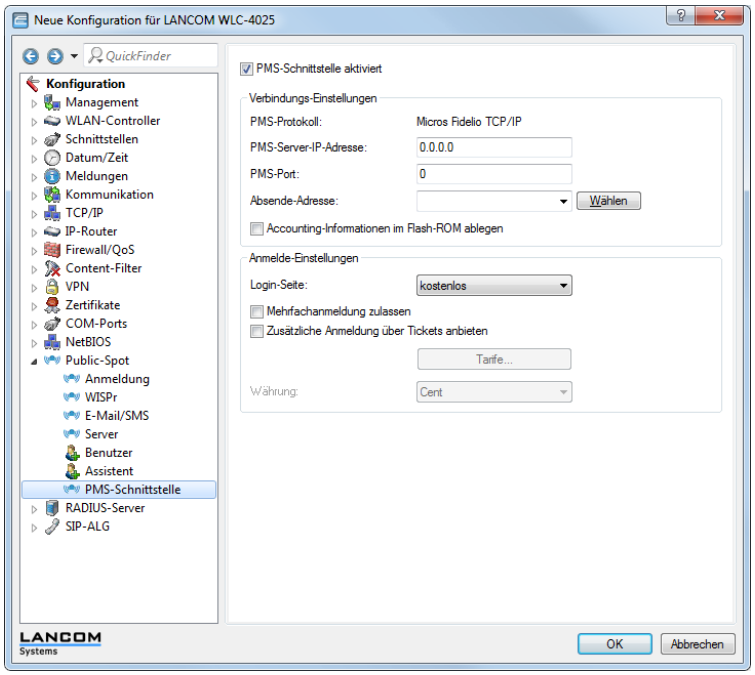
Durch die *Stationsüberwachung* haben Sie die Möglichkeit, solche Benutzer nach einer festgelegten Leerlaufzeit automatisch auszuloggen. Dieses Feature ist standardmäßig ausgeschaltet. Für einen kostenpflichtigen Zugang sollten Sie es jedoch unbedingt aktivieren. Andernfalls erfolgt der automatische, 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.

7.8.3 Ergänzungen in LANconfig

PMS-Schnittstelle konfigurieren

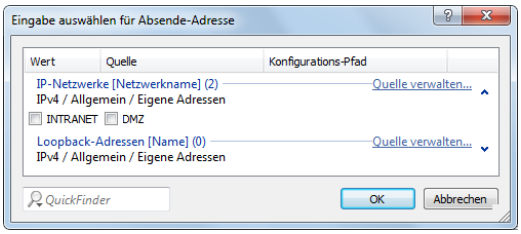
Die PMS-Schnittstelle Ihres Gerätes konfigurieren Sie über den Dialog **Public-Spot** > **PMS-Schnittstelle**.



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**!

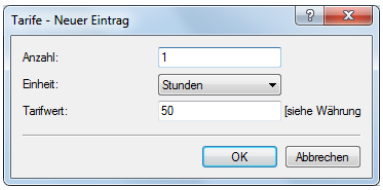
  - Beliebige IPv4-Adresse

- **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.

- **Tarife**: Sofern Sie eine kostenpflichtigen Internetzugang anbieten, verwalten Sie über diese Tabelle die Tarife für das Accounting.



  - **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 gewählten Währung entspricht dies in den oben gezeigten Screenshots z. B. 50 Cent.

  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 eine 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`

7.8.4 Ergänzungen im Status-Menü

PMS-Interface

Dieses Menü beinhaltet die Statuswerte für die PMS-Schnittstelle (PMS = Property-Management-System).

SNMP-ID:

1.78

Pfad Telnet:

Status

Accounting

Diese Tabelle zeigt eine Übersicht der Abrechnungsinformationen, die zu sämtlichen Hotelgästen vorliegen, welche den Public Spot über die PMS-Schnittstelle benutzt haben. Das Gerät erfasst Abrechnungsinformationen unabhängig davon, ob die betreffenden Nutzer eine kostenlose oder kostenpflichtige Verbindung verwenden. Somit bietet Ihnen diese Tabelle gleichzeitig auch eine Übersicht aller am Public Spot aktiven und inaktiven Hotelgäste.

SNMP-ID:

1.78.2

Pfad Telnet:

Status > **PMS-Interface**

Reservierungsnummer

Reservierungsnummer, die der Hotelgast in Ihrem PMS erhalten hat

Benutzername

Nachname des Hotelgastes, wie er in Ihrem PMS hinterlegt ist

Raumnummer

Nummer des Zimmers, das der Hotelgast bewohnt

MAC-Adresse

MAC-Adresse des Gerätes, für das Accounting-Daten gesammelt wurden

Kommentar

Vom Gerät automatisch generierter Kommentar

Zeitbudget

Prepaid-Zeitkontingent, das der Hotelgast gekauft hat

Volumenbudget

Prepaid-Volumenkontingent, das der Hotelgast gekauft hat

Diese Spalte ist ein Platzhalter. Das Setzen von Volumenkontingenten ist zur Zeit nicht möglich.

Gesamtvolumen

Datenvolumen, das der Nutzer in allen seinen Sitzungen (vergangene und aktuelle) verbraucht hat. Das Gesamtvolumen gibt somit den Echtzeitwert des seit seiner Registrierung insgesamt vom Hotelgast erzeugten Datenverkehrs wieder.

Die Subtraktion des Initial-Gesamtvolumen vom Gesamtvolumen ergibt das Datenvolumen, das der Nutzer in seiner letzten aktiven Sitzung verbraucht hat.

Gesamtzeit

Dauer aller Sitzungen (vergangene und aktuelle) eines Hotelgastes am Public Spot

Die Subtraktion der Initial-Gesamtzeit von der Gesamtzeit ergibt die Dauer, die der Nutzer während seiner letzten aktiven Sitzung am Public Spot angemeldet war.

Aktiv

Zeigt an, ob das Endgerät des betreffenden Hotelgastes gerade am Public Spot angemeldet ist und Accounting-Daten gesammelt werden

zuletzt aktualisiert

Zeigt an, wann das Gerät die Accounting-Daten zuletzt aktualisiert hat. Das Aktualisierungsintervall bestimmen Sie im Setup-Menü über den Parameter **Accounting-Tabelle-Updateintervall**.

Initial-Gesamtvolumen

Datenvolumen, das der Nutzer in seinen vergangenen Sitzungen insgesamt verbraucht hat

Die Subtraktion des Initial-Gesamtvolumen vom Gesamtvolumen ergibt das Datenvolumen, das der Nutzer in seiner letzten aktiven Sitzung verbraucht hat.

Initial-Gesamtzeit

Dauer aller vergangenen Sitzungen eines Hotelgastes am Public Spot

Die Subtraktion der Initial-Gesamtzeit von der Gesamtzeit ergibt die Dauer, die der Nutzer während seiner letzten aktiven Sitzung am Public Spot angemeldet war.

Verbindung

Dieser Statuswert zeigt die Aktivität der PMS-Schnittstelle an.

SNMP-ID:

1.78.1

Pfad Telnet:

Status > **PMS-Interface**

Mögliche Werte:

An

Aus

7.8.5 Ergänzungen im Setup-Menü

PMS-Interface

Über die Tabellen und Parameter in diesem Menü nehmen Sie sämtliche Einstellungen für die PMS-Schnittstelle vor (PMS = Property-Management-System).

SNMP-ID:

2.64

Pfad Telnet:

Setup

Accounting

In diesem Menü konfigurieren Sie die Übermittlung der Abrechnungsinformationen vom Gerät an Ihr PMS.

SNMP-ID:

2.64.10

Pfad Telnet:

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. Wenn der Wert `0` ist, ist die automatische Bereinigung deaktiviert.

SNMP-ID:

2.64.10.3

Pfad Telnet:

Setup > **PMS-Interface** > **Accounting**

Mögliche Werte:

0…4294967295 Sekunden

Default:

60

Flashrom-Speichern

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!

SNMP-ID:

2.64.10.1

Pfad Telnet:

Setup > **PMS-Interface** > **Accounting**

Mögliche Werte:

nein

ja

Default:

nein

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 Lebendauer Ihres Gerätes reduziert!

SNMP-ID:

2.64.10.2

Pfad Telnet:

Setup > **PMS-Interface** > **Accounting**

Mögliche Werte:

0…4294967295 Sekunden

Default:

15

Accounting-Tabelle-Updateintervall

Über diesen Eintrag konfigurieren Sie, in welchem Intervall das Gerät seine interne Accounting-Tabelle im Status-Menü aktualisiert. Wenn der Wert `0` ist, ist die Aktualisierung deaktiviert und die Status-Tabelle zeigt keine Werte an.

SNMP-ID:

2.64.10.4

Pfad Telnet:

Setup > **PMS-Interface** > **Accounting**

Mögliche Werte:

0…4294967295 Sekunden

Default:

15

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 Telnet:

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 Telnet:

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 Telnet:

Setup > **PMS-Interface** > **Login-Formular** > **Kostenlos-VIP-Status**

Mögliche Werte:

String, max. 20 Zeichen

Default:

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 Telnet:

Setup > **PMS-Interface** > **Login-Formular**

Mögliche Werte:

Keiner

Reservierungsnummer

Ankunftsdatum

Abreisedatum

Vorname

Profilnummer

Default:

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 Telnet:

Setup > **PMS-Interface** > **Login-Formular**

Mögliche Werte:

Keiner

Reservierungsnummer

Ankunftsdatum

Abreisedatum

Vorname

Profilnummer

Default:

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 Telnet:

Setup > **PMS-Interface** > **Login-Formular**

Mögliche Werte:

Keiner

Reservierungsnummer

Ankunftsdatum

Abreisedatum

Vorname

Profilnummer

Default:

Reservierungsnummer

PMS-Login-Formular

Wählen Sie aus, welche Anmeldemaske die Portalseite für Ihre PMS-Schnittstelle anzeigt.

SNMP-ID:

2.64.11.2

Pfad Telnet:

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:

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 Telnet:

Setup > **PMS-Interface** > **Login-Formular**

Mögliche Werte:

nein

ja

Default:

nein

Tarif

Sofern Sie eine kostenpflichtigen Internetzugang anbieten, verwalten Sie über diese Tabelle die Tarife für das Accounting.

SNMP-ID:

2.64.9

Pfad Telnet:

Setup > **PMS-Interface**

Anzahl

Geben Sie hier die Höhe des Zeitkontingents ein, z. B. `1`. In Kombination mit der Einheit entspricht dies dann z. B. 1 Stunde.

SNMP-ID:

2.64.9.1

Pfad Telnet:

Setup > **PMS-Interface** > **Tarif**

Mögliche Werte:

0…9999999999999999999

Default:

Einheit

Wählen Sie aus der Liste eine Einheit für das Zeitkontingent aus.

SNMP-ID:

2.64.9.2

Pfad Telnet:

Setup > **PMS-Interface** > **Tarif**

Mögliche Werte:

Stunde(n)

Tag(e)

Minute(n)

Default:

Stunde(n)

Tarifwert

Geben Sie hier die Höhe des Betrags ein, mit dem Sie die Zeitkontingente vergelten. In Kombination mit der gewählten Währung entspricht dies dann z. B. 50 Cent

SNMP-ID:

2.64.9.3

Pfad Telnet:

Setup > **PMS-Interface** > **Tarif**

Mögliche Werte:

0…9999999999999999999

Default:

Aktiv

Aktivieren oder deaktivieren Sie die PMS-Schnittstelle für das Gerät.

SNMP-ID:

2.64.1

Pfad Telnet:

Setup > **PMS-Interface**

Mögliche Werte:

nein

ja

Default:

nein

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 Telnet:

Setup > **PMS-Interface**

Mögliche Werte:

nein

ja

Default:

ja

Loopback-Address

Geben Sie hier optional eine andere Adresse (Name oder IP) an, an die der PMS-Server seine Antwort-Nachrichten schickt.

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.

SNMP-ID:

2.64.4

Pfad Telnet:

Setup > **PMS-Interface**

Mögliche Werte:

- 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
- Beliebige IPv4-Adresse

Sofern die hier eingestellte Absendeadresse eine Loopback-Adresse ist, wird diese auch auf maskiert arbeitenden Gegenstellen **unmaskiert** verwendet!

Default:

Multi-Login

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

SNMP-ID:

2.64.13

Pfad Telnet:

Setup > **PMS-Interface**

Mögliche Werte:

nein

ja

Default:

nein

PMS-Port

Geben Sie hier den TCP-Port ein, über den Ihr PMS-Server erreichbar ist.

SNMP-ID:

2.64.5

Pfad Telnet:

Setup > **PMS-Interface**

Mögliche Werte:

0…65535

Default:

0

PMS-Server-IP-Adresse

Geben Sie hier die IPv4-Adresse Ihres PMS-Servers ein.

SNMP-ID:

2.64.3

Pfad Telnet:

Setup > **PMS-Interface**

Mögliche Werte:

IPv4-Adresse

Default:

nein

PMS-Typ

Bezeichnet das von Ihrem Property-Management-System verwendete Protokoll. Zur Zeit besteht ausschließlich die Unterstützung für das Hotel-Property-Management-System von Micros Fidelio über TCP/IP.

SNMP-ID:

2.64.2

Pfad Telnet:

Setup > **PMS-Interface**

Mögliche Werte:

TCP/IP

Default:

TCP/IP

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 Telnet:

Setup > **PMS-Interface**

Mögliche Werte:

String, max. 1 Zeichen

Default:

|

Waehrung

Sofern Sie eine 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.

SNMP-ID:

2.64.8

Pfad Telnet:

Setup > **PMS-Interface**

Mögliche Werte:

CENT

PENNY

Default:

CENT

Zeichensatz

Wählen Sie den Zeichensatz aus, in dem Ihr PMS die Nachnamen Ihrer Gäste an das Gerät übermittelt.

SNMP-ID:

2.64.7

Pfad Telnet:

Setup > **PMS-Interface**

Mögliche Werte:

CP850

W1252

Default:

CP850

8 LCMS

8.1 SSH-Konfigurationsprotokoll in LANconfig

Im Rahmen der CC-Compliance (Common Criteria) unterstützt LANconfig ab der Version LCOS 8.82 die Konfiguration von LANCOM CC-Produkten über SSH bzw. Datentransfer per SCP.

8.1.1 Ergänzungen in LANconfig

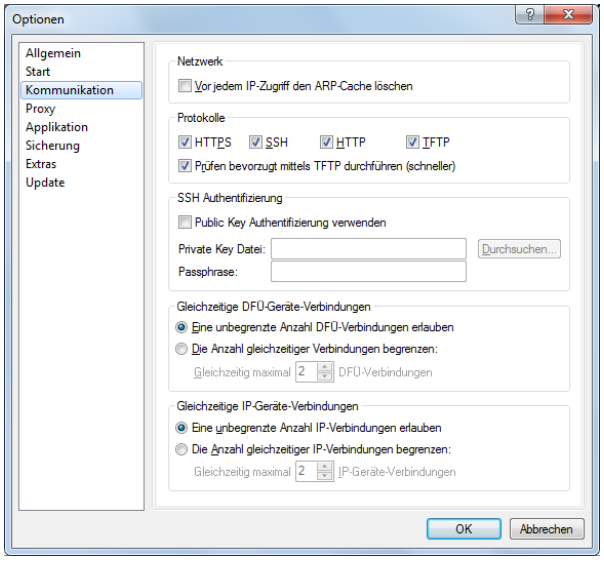
Gerätespezifische Einstellung der Kommunikationsprotokolle

Zur Übertragung der Daten bei der Konfiguration mit LANconfig stehen wahlweise die Protokolle HTTPS, SSH, HTTP oder TFTP Verfügung. Deren Konfiguration erfolgt im Dialog **Extras** > **Optionen** > **Kommunikation**.

Die allgemein angebotenen Protokolle werden global definiert. Zusätzlich ist es möglich, Protokolle für bestimmte Geräte zu unterbinden. Es ist jedoch nicht möglich ein global deaktiviertes Protokoll für einzelne Geräte wieder zu aktivieren.

Konfiguration der globalen Kommunikationseinstellungen

Die Konfiguration der Kommunikationsprotokolle unterscheidet zwischen dem Protokoll für das reine Prüfen des Gerätes und den Protokollen für andere Operationen wie z. B. einen Firmware-Upload etc.:



- **HTTPS**, **SSH**, **HTTP**, **TFTP**

  Mit dieser Auswahl aktivieren Sie die einzelnen Protokolle für die Operationen Firmware-Upload sowie Konfigurations- und Script-Upload und -Download. Bei diesen Operationen versucht LANconfig, diese Protokolle in der Reihenfolge HTTPS, SSH, HTTP und TFTP zu verwenden. Schlägt die Übertragung mit einem der gewählten Protokolle fehl, versucht LANconfig automatisch das nächste Protokoll.

- **Prüfen bevorzugt mittels TFTP durchführen**

  Eine Prüfung der Geräte überträgt mit den Systeminformationen nur geringe Datenmengen. Gerade im LAN ist also die Geräteprüfung durchaus mit dem TFTP-Protokoll sinnvoll. Wenn diese Option aktiviert ist, verwendet LANconfig zum Prüfen der Geräte zunächst das TFTP-Protokoll, unabhängig von den zuvor eingestellten

Kommunikationsprotokollen. Schlägt die Prüfung über TFTP fehl, versucht LANconfig im Anschluss die Protokolle HTTPS, SSH und HTTP.

- **Public Key Authentifizierung verwenden**

  Sofern Sie als Protokoll SSH ausgewählt haben, können Sie die Authentifizierung alternativ über einen privaten Schlüssel durchführen. In diesem Fall entfällt die Authentifizierung über eine Dialog zur Kenntworteingabe. Tragen Sie in die Eingabefelder den Pfad zu Ihrer privaten Schlüsseldatei und ggf. die Passphrase ein, mit der Sie die Datei zusätzlich verschlüsselt haben. Den dazugehörigen öffentlichen Schlüssel laden Sie über LANconfig oder WEBconfig in die einzelnen Geräte.

Die globalen Kommunikationseinstellungen sind den gerätespezifischen Einstellungen übergeordnet, um z. B. die Verwendung eines Protokolls zentral unterbinden zu können.

Die Menüstruktur in LANconfig

Über die Menüleiste können Sie Geräte und deren Konfigurationen verwalten sowie das Aussehen und die Funktionsweise von LANconfig anpassen.

Datei

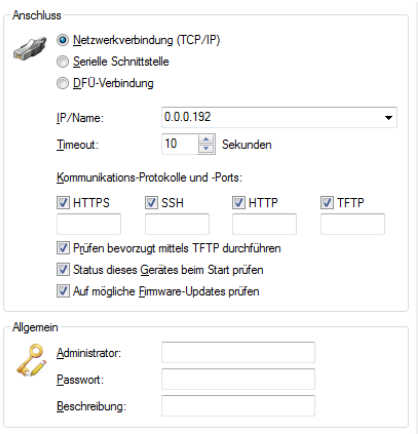
Unter dem Menüpunkt **Datei** verwalten Sie Geräte allgemein und beenden bei Bedarf LANconfig.

Gerät hinzufügen

Über **Datei** > **Gerät hinzufügen** können Sie ein neues Gerät hinzufügen. Es öffnet sich ein Dialog, in dem Sie Einstellungen für das Gerät, die Verbindung und die Sicherung vornehmen können.

Allgemein

Auf dieser Seite legen Sie – abweichend von den globalen Einstellungen – fest, wie sich LANconfig mit dem Gerät verbindet. Zudem können Sie Zugangsdaten hinterlegen, um nicht bei jedem Start von LANconfig beim ersten Verbindungsaufbau die Daten manuell einzugeben.



Anschluss

Im Bereich **Anschluss** können Sie die Anschluss-Einstellungen für ein Gerät vornehmen.

Wählen Sie hier aus, wie das Gerät erreichbar ist:

- **Netzwerkverbindung (TCP/IP)**: Wählen Sie diese Option, wenn das Gerät über ein IP-Netzwerk zu erreichen ist.
- **Serielle Schnittstelle**: Wählen Sie diese Option, wenn das Gerät an die serielle Schnittstelle dieses Computers angeschlossen ist.

- **DFÜ-Verbindung**: Wählen Sie diese Option aus, wenn Sie das Gerät über das DFÜ-Netzwerk erreichen wollen.

  Bitte beachten Sie, dass nicht jeder Router die Fernkonfiguration über eine DFÜ-Verbindung unterstützt.
- **IP/Name:**: Geben Sie die IP-Adresse des Gerätes an. Sie können auch einen Domain-Namen (DN oder FQDN) oder einen NetBIOS-Namen angeben. Dieser Name wird bei jedem Zugriff überprüft. LANconfig speichert und verwendet die dabei aufgelöste IP-Adresse. Sollte die Überprüfung einmal nicht möglich sein, greift LANconfig auf die letzte erfolgreich aufgelöste IP-Adresse zurück.
- **Timeout**: Geben Sie hier an, wieviele Sekunden das Programm auf Antworten von diesem Gerät warten soll.
- **HTTPS**, **SSH**, **HTTP**, **TFTP**: Mit dieser Auswahl aktivieren Sie die einzelnen Protokolle für die Operationen Firmware-Upload sowie Konfigurations- und Script-Upload und -Download. Bei diesen Operationen versucht LANconfig, diese Protokolle in der Reihenfolge HTTPS, SSH, HTTP und TFTP zu verwenden. Schlägt die Übertragung mit einem der gewählten Protokolle fehl, versucht LANconfig automatisch das nächste Protokoll.
- **Prüfen bevorzugt mittels TFTP durchführen**: Diese Option bewirkt, dass LANconfig ungeachtet der ausgewählten Protokolle bevorzugt mit TFTP prüft. Dies ist vorteilhaft bei Geräten, die im LAN erreichbar sind. Die Prüfung erfolgt schneller und belastet den Rechner weniger, was sich bei der Bearbeitung einer größeren Anzahl von Geräten bemerkbar macht. Die fehlende HTTPS-Verschlüsselung stellt im LAN keinen Nachteil dar.
- **Status dieses Gerätes beim Start prüfen**: Markieren Sie die Option, wenn LANconfig den Status des Gerätes beim Start prüfen soll.
- **Auf mögliche Firmware-Updates prüfen**: Markieren Sie die Option, wenn LANconfig auf mögliche Firmware-Updates prüfen soll.

Wie im Abschnitt 'Kommunikationsprotokolle und Ports' erwähnt, testet LANconfig andere Protokolle und führt sie aus, wenn TFTP nicht verfügbar ist. Auch hier sind die globalen Einstellungen den gerätespezifischen übergeordnet.

Nachdem Sie die Einstellungen vorgenommen haben, versucht das Programm das Gerät zu erreichen und dessen Namen und Version abzufragen. Wenn dies fehlschlägt, zeigt LANconfig eine kurze Fehlermeldung in der Spalte **Status**.

Allgemein

In diesem Bereich können Sie Zugangsdaten zum Gerät und eine Beschreibung eingeben.

- **Administrator**: Geben Sie hier den Benutzernamen eines Administrators ein.
- **Passwort**: Geben Sie hier das zugehörige Passwort ein.
- **Beschreibung**: Geben Sie hier die Beschreibung des Gerätes ein, die LANconfig im Hauptfenster anzeigen soll.

  LANconfig speichert die hier eingegebenen Zugangsdaten dauerhaft, so dass Sie diese beim erstmaligen Zugriff auf das Gerät in einer LANconfig-Sitzung nicht mehr eingeben müssen.

  Wenn Sie Benutzernamen und Passwort dauerhaft speichern, erhält jeder Nutzer Zugang zu dem Gerät, der auch LANconfig ausführen darf.

Kommunikationsprotokolle und Ports

Das Prüfen, also die Übertragung der Systeminformationen, führt LANconfig in Abhängigkeit der hier ausgewählten Kommunikations-Protokolle durch.

LANconfig führt auch die Geräte-Aktionen Script-, Firmware-, Konfigurations-Upload und Konfigurations-Download über die hier ausgewählten Kommunikationsprotokolle aus.

Bei Geräten mit LCOS-Versionen kleiner als 5.20 verwendet LANconfig unabhängig von den hier gewählten Protokollen bei allen Aktionen das TFTP-Protokoll.

LANconfig versucht in der Reihenfolge HTTPS, SSH, HTTP und TFTP und SSH, mit jedem gewählten Protokoll die oben aufgeführten Geräte-Aktionen auszuführen. Endet eine Aktion aufgrund des verwendeten Protokolls fehlerhaft, wiederholt LANconfig sie mit dem nächsten ausgewählten Protokoll.

Damit die Aktion überhaupt funktionieren kann, muss mindestens ein Protokoll ausgewählt sein.

Bei Verwendung von HTTP(S) und einem Proxyserver kann es notwendig sein, diesen Proxyserver zu umgehen, damit LANconfig die Geräte erreichen kann. In den Internetoptionen der Systemsteuerung von Windows können Sie den Proxyserver für lokale Adressen umgehen. In den erweiterten Einstellungen der Internetoptionen können Sie außerdem weitere Adressen definieren, die nicht über den Proxyserver kontaktiert werden sollen.

Zum Einstellen der Protokolle gibt es jeweils eine gerätespezifische und eine globale Einstellmöglichkeit. Die globalen Einstellungen im Options-Menü sind den gerätespezifischen übergeordnet. Dadurch ist es möglich, die einzelnen Protokolle mit Hilfe eines globalen Schalters für alle Geräte auszuschalten.

Tipps

- Wenn sich das Gerät noch im Auslieferungszustand befindet, hat es noch keine eigene IP-Adresse. In diesem Fall geben Sie die IP-Adresse Ihres Computers ein und ersetzen Sie den letzten Abschnitt der Ziffernfolge durch '254': Wenn ihr Computer die IP-Adresse '192.168.1.1' hat, dann weisen Sie dem Gerät die IP-Adresse '192.168.1.254' zu.
- Wenn Sie nicht wissen, welche Adresse ein Gerät hat, können Sie auch danach über **Datei** > **Geräte** suchen.

Mögliche für Probleme beim Herstellen einer Verbindung mit einem neuen Gerät

Wenn LANconfig ein Gerät nicht erreicht, erscheint unter Status eine der unten aufgeführten Fehlermeldungen.

Um ein Gerät erneut zu überprüfen, markieren Sie es in der Liste, und klicken Sie dann auf in der Menüleiste auf **Gerät** > **Prüfen**.

- **Serieller Fehler**: LANconfig konnte die serielle Schnittstelle nicht öffnen. Schließen Sie alle Programme, die möglicherweise darauf zugreifen.
- **IP-Fehler**: Überprüfen Sie, ob die IP-Adresse des Gerätes richtig ist und ob Ihr Computer korrekt mit dem Netzwerk verbunden ist. Stellen Sie außerdem sicher, dass das TCP/IP-Protokoll installiert und richtig konfiguriert ist.
- **Keine Antwort**: Überprüfen Sie, ob die IP-Adresse des Gerätes richtig ist. Möglicherweise ist auch die Netzwerkverbindung zwischen Ihrem Rechner und dem Gerät zu langsam oder unzuverlässig.
- **Status unbekannt**: LANconfig hat das Gerät zwar über die angegebene IP-Adresse erreicht, konnte jedoch keine weiteren Informationen abfragen. Möglicherweise unterstützt LANconfig dieses Gerät nicht.
- **Zugriff verweigert:** Das Gerät ist für den Zugriff von Ihrem Rechner aus gesperrt.

Gerät

Unter dem Menüpunkt **Gerät** können Sie die Konfiguration von am Netzwerk angeschlossenen Geräten bearbeiten, Firmware-Updates verwalten und Geräteverbindungen überwachen.

Die Funktionen im Menü **Gerät** können Sie nur auswählen, wenn Sie mindestens ein Gerät in der Geräteliste markiert haben. Dieses Menü können Sie ebenfalls über die rechte Maustaste für ein markiertes Gerät aufrufen.

WEBconfig / Konsolen-Sitzung

Unter **Gerät** > **WEBconfig / Konsolen-Sitzung** können Sie die folgenden Aktionen wählen:

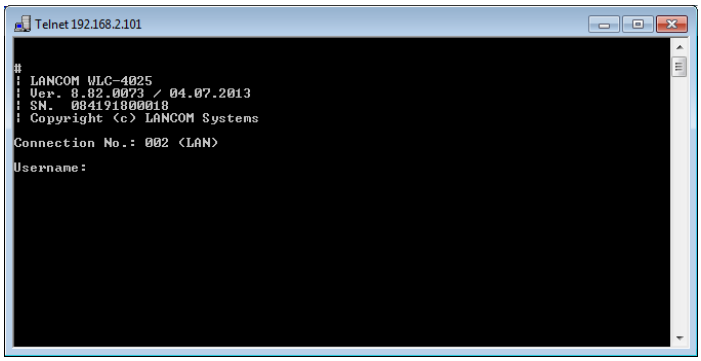
Web-Browser starten

Öffnet die WEBconfig-Oberfläche für das markierte Gerät.

Unter **Extras** > **Optionen** > **Extras** > **Browser zur Darstellung von WEBconfig** können Sie auswählen, ob LANconfig zur Anzeige den Standardbrowser des Systems oder den internen Browser verwenden soll.

Telnet-Sitzung öffnen

Öffnet eine Verbindung zum Gerät mit dem in den Einstellungen konfigurierten Telnet-Client.



SSH-Sitzung öffnen

Öffnet eine Verbindung zum Gerät mit dem in den Einstellungen konfigurierten SSH-Client.

Extras

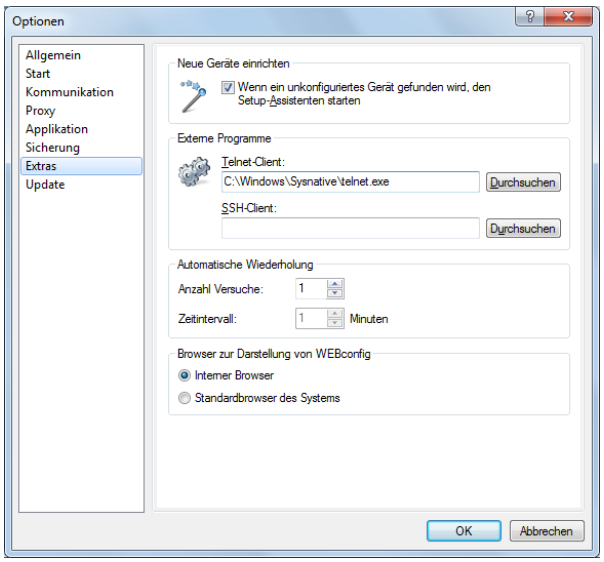
Wenn Sie in der Menüleiste auf **Extras** > **Optionen** klicken, öffnet sich die Dialogbox für weitere Einstellungsmöglichkeiten. (Sie erreichen diese Dialogbox auch, indem Sie F7 drücken.)

Optionen

Unter dem Menüpunkt **Optionen** können Sie zusätzliche Funktionen von LANconfig aufrufen, z. B. für die Kommunikation mit angeschlossenen Geräten, den Aufruf externer Anwendungen oder die automatische Suche nach Firmware-Updates.

Extras

In diesem Dialog können Sie **zusätzliche Einstellungen** vornehmen.



Neue Geräte einrichten

Wenn diese Option markiert ist, startet LANconfig bei jedem gefundenen, aber noch nicht konfigurierten Gerät den Setup-Assistenten.

Externe Programme

Bestimmen Sie hier jeweils die Programmdatei des Telnet-Clients und des SSH-Clients, die LANconfig für Verbindungen zu den Geräten benutzen soll.

Automatische Wiederholung

Anzahl Versuche

Geben Sie hier die Anzahl der Versuche für einen Firmware- oder Konfigurations-Upload an. Die Anzahl können Sie im Bereich von 1 bis 9999 einstellen. Einen Verbindungsversuch führt LANconfig immer durch. Schlägt dieser fehl, erfolgt eine Wiederholung der Aktion nach abgelaufener Intervall-Zeit. Es erfolgen so viele Wiederholungen, bis LANconfig entweder die eingestellte Anzahl von Versuchen durchgeführt hat oder die Aktion erfolgreich war. Es ist jedoch auch möglich, dass LANconfig die Wiederholungen vorzeitig abbricht, wenn eine Situation eintritt, die voraussichtlich nicht ohne weitere Einflussnahme zum Erfolg führt. Dies kann z. B. eine Datei sein, die das Gerät nicht öffnen kann.

Zeitintervall

Geben Sie hier die Intervalldauer in Minuten an, die zwischen zwei Firmware- oder Konfigurations-Upload-Versuchen verstreichen soll. Die Intervalldauer können Sie im Bereich von 1 bis 9999 einstellen.

Browser zur Darstellung von WEBconfig

Bestimmen Sie hier, welchen Browser LANconfig standardmäßig für die Anzeige von WEBconfig verwenden soll. Zur Auswahl stehen der Standard-Browser des Betriebssystems und der LANconfig-interne Browser LCCEF (LANCOM Chromium Embedded Framework).

9 IPv6

9.1 Reconfigure-Funktion des DHCPv6-Servers

Jede IPv6-Adresse bzw. jedes IPv6-Präfix hat eine vom Server vorgegebene Lebenszeit. In gewissen Intervallen fragt ein Client beim Server an, um seine Adresse zu verlängern (sogenannte Renew/Rebind-Zeiten).

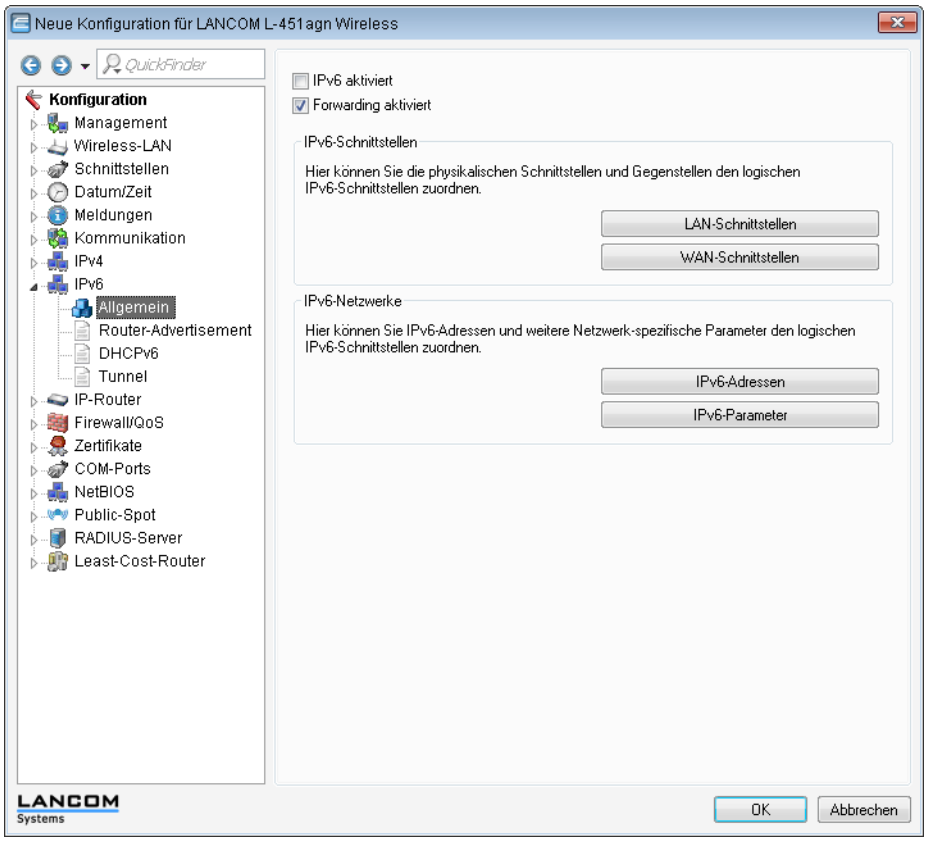
Ändert sich aber z. B. durch Trennung und Wiederaufbau der Internetverbindung oder Anforderung eines neuen Präfixes (Telekom-Privcay-Funktion) das WAN-Präfix, so hat der Server keine Möglichkeit, die Netzwerkgeräte darüber zu informieren, dass sich Präfix bzw. Adresse geändert haben. Das bedeutet, dass ein Client noch eine alte Adresse oder ein altes Präfix verwendet und damit nicht mehr mit dem Internet kommunizieren kann.

Ab der Version LCOS 8.82 kann der DHCPv6-Server in IPv6-fähigen LANCOM-Geräten durch eine Reconfigure-Funktion die Clients im Netzwerk auffordern, ihre Leases/Bindings zu erneuern.

9.1.1 Ergänzungen in LANconfig

IPv6-Konfigurationsmenü

Im Gegensatz zu früheren Versionen, in denen es im Konfigurationsmenü die Konfigurationsmöglichkeit TCP/IP für IPv4 gab, finden Sie nun an dieser Stelle die Optionen **IPv4** und **IPv6**.



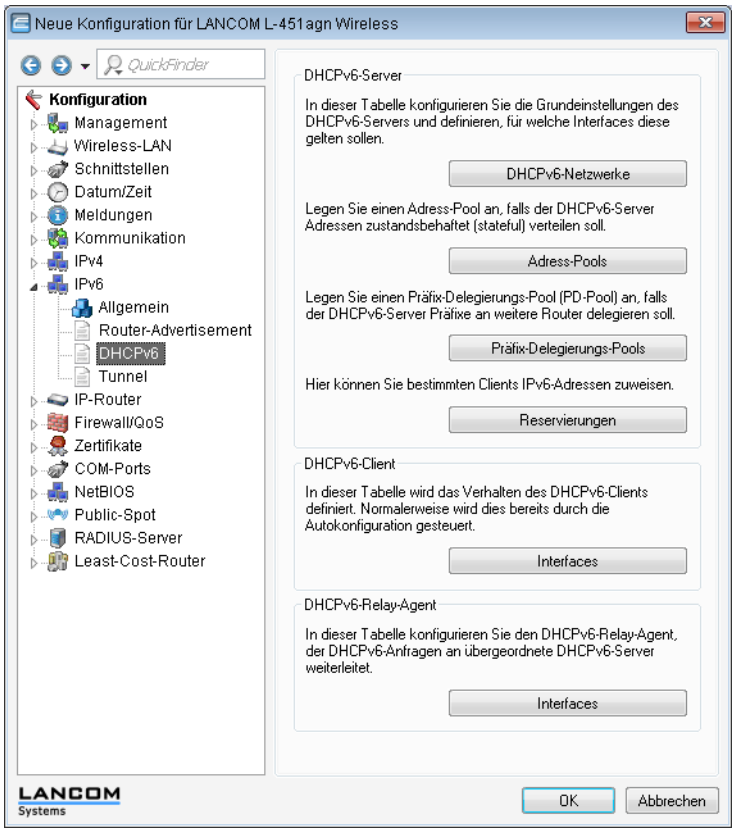
Klicken Sie auf **IPv6**, um die Einstellungen für dieses Protokoll vorzunehmen. Die Konfiguration **IPv6** ist unterteilt in die Optionen

- **Allgemein**,
- **Router-Advertisement**,
- **DHCPv6** und
- **Tunnel**.

Standardmäßig befinden Sie sich nach dem Klick auf **IPv6** in der Option **Allgemein**.

DHCPv6

Hier konfigurieren Sie DHCPv6-Server, den DHCPv6-Client und den DHCPv6-Relay-Agent.

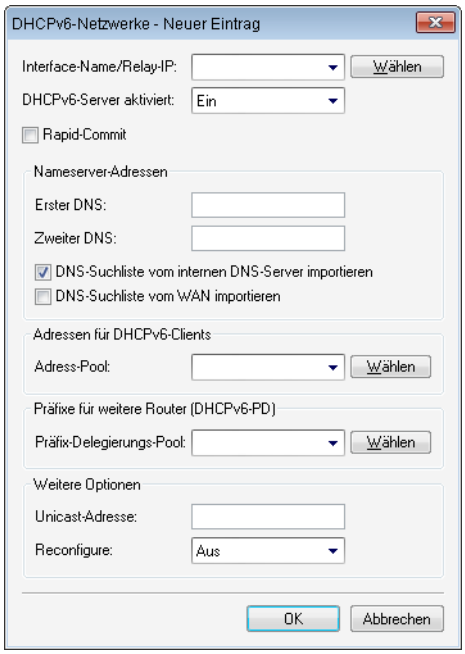


DHCPv6-Server

Öffnen Sie mit den folgenden Schaltflächen die Tabellen zur Einstellung der jeweiligen Funktionen:

DHCPv6-Netzwerke

In dieser Tabelle konfigurieren Sie die Grundeinstellungen des DHCPv6-Servers und definieren, für welche Interfaces diese gelten sollen.



Interface-Name-or-Relay

Name des Interfaces, auf dem der DHCPv6-Server arbeitet, z. B. "INTRANET". Alternativ hinterlegen Sie hier die IPv6-Adresse des entfernten DHCPv6 Relay-Agenten.

DHCPv6-Server aktiviert

Aktiviert bzw. deaktiviert den Eintrag.

Rapid-Commit

Bei aktiviertem Rapid-Commit antwortet der DHCPv6-Server direkt auf eine Solicit-Anfrage mit einer Reply-Nachricht.

Der Client muss explizit die Rapid-Commit-Option in seiner Anfrage setzen.

Erster DNS

IPv6-Adresse des ersten DNS-Servers.

Zweiter DNS

IPv6-Adresse des zweiten DNS-Servers.

DNS-Suchliste vom internen DNS-Server importieren

Gibt an, ob die DNS-Suchliste (DNS Search List) bzw. die eigene Domäne für dieses logische Netzwerk vom internen DNS-Server eingefügt werden soll, z. B. "intern". Die eigene Domäne ist unter **IPv4** > **DNS** > **Allgemeine Einstellungen** konfigurierbar. Die Default-Einstellung ist "aktiviert".

DNS-Suchliste vom WAN importieren

Gibt an, ob die vom Provider übertragende DNS-Suchliste (z. B. provider-xy.de) in diesem logischen Netzwerk angekündigt werden soll. Die Default-Einstellung ist "deaktiviert".

Adress-Pool

Name des für dieses Interface verwendeten Adress-Pools.

Verteilt der DHCPv6-Server seine Adressen 'stateful', müssen Sie entsprechende Adressen in die Tabelle **Adress-Pools** eintragen.

Präfix-Delegierungs-Pool

Name des Präfix-Pools, den der DHCPv6-Server verwenden soll.

Soll der DHCPv6-Server Präfixe an weitere Router delegieren, müssen Sie entsprechende Präfixe in der Tabelle **Präfix-Delegierungs-Pools** eintragen.

Unicast-Adresse

Standardmäßig reagiert der DHCPv6-Server ausschließlich auf Multicast-Anfragen. Wenn der DHCPv6-Server auf eine Unicast-Anfragen reagieren soll, so kann hier diese IPv6-Adresse konfiguriert werden. In der Regel reicht Multicast zur Kommunikation aus.

Reconfigure

Jede IPv6-Adresse bzw. jedes IPv6-Präfix hat eine vom Server vorgegebene Lebenszeit. In gewissen Intervallen fragt ein Client beim Server an, um seine Adresse zu verlängern (sogenannte Renew/Rebind-Zeiten).

Ändert sich aber z. B. durch Trennung und Wiederaufbau der Internetverbindung oder Anforderung eines neuen Präfixes (Telekom-Privcay-Funktion) das WAN-Präfix, so hat der Server keine Möglichkeit, die Netzwerkgeräte darüber zu informieren, dass sich Präfix bzw. Adresse geändert haben. Das bedeutet, dass ein Client noch eine alte Adresse oder ein altes Präfix verwendet und damit nicht mehr mit dem Internet kommunizieren kann.

Die Reconfigure-Funktion ermöglicht dem DHCPv6-Server, die Clients im Netzwerk zu einer Erneuerung der Leases/Bindings aufzufordern. Wenn der Client mit dem Server beim ersten Kontakt erfolgreich ein Re-Konfiguration (Reconfigure) ausgehandelt hat, dann kann der Server den Client jederzeit auffordern, seine Adresse oder andere Informationen zu aktualisieren. Der Mechanismus wird durch den sogenannten *Reconfigure Key* geschützt, so dass nur der ursprüngliche Server mit dem richtigen Schlüssel den Client auffordern kann. Erhält der Client eine Reconfigure-Nachricht ohne gültigen Reconfigure-Key, so verwirft der Client diese Aufforderung zur Re-Konfiguration.

Unterstützt wird das *Reconfigure Key Authentication Protocol* nach RFC 3315 für die Optionen *Renew* und *Information-Request*, sowie *Rebind* nach RFC 6644. Das Auslösen der Rekonfiguration erfolgt auf der Konsole des Gerätes durch einen do-Befehl im Status-Baum (siehe Beschreibung im Status-Baum).

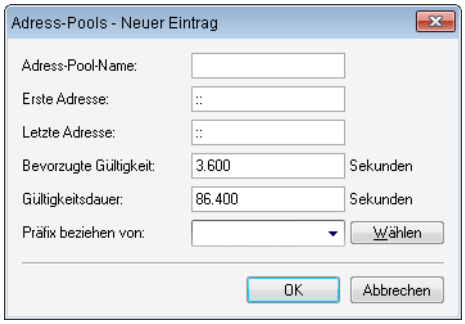
Den Status eines Clients in Bezug auf Reconfigure finden Sie unter **Status** > **IPv6** > **DHCPv6** > **Server** > **Clients**.

Folgende Einstellungen stehen Ihnen zur Auswahl:

- **Aus**: Deaktiviert die Reconfigure-Funktion.
- **Zurückweisen**: Clients, die die Reconfigure-Option in Anfragen gesetzt haben, werden vom Server abgelehnt und erhalten keine Adressen, Präfixe oder andere Optionen.
- **Erlauben**: Hat ein Client die Reconfigure-Option in Anfragen gesetzt, so verhandelt der Server mit dem Client die nötigen Parameter, um zu einem späteren Zeitpunkt ein Reconfigure zu starten.
- **Erforden**: Clients müssen die Reconfigure-Option in ihren Anfragen setzen, sonst lehnt der Server diese Clients ab. Dieser Modus ist dann sinnvoll, wenn Sie sichergehen wollen, dass der Server ausschließlich Clients bedient, die Reconfigure unterstützen. Dadurch ist gewährleistet, dass alle Clients zu einem späteren Zeitpunkt erfolgreich durch Reconfigure ihre Adressen, Präfixe oder weiteren Informationen aktualisieren können.

Adress-Pools

In dieser Tabelle definieren Sie einen Adress-Pool, falls der DHCPv6-Server Adressen stateful verteilen soll:



Adress-Pool-Name

Name des Adress-Pools

Erste Adresse

Erste Adresse des Pools, z. B. "2001:db8::1"

Letzte Adresse

Letzte Adresse des Pools, z. B. "2001:db8::9"

Bevorzugte Gültigkeit

Bestimmen Sie hier die Zeit in Sekunden, die der Client diese Adresse als 'bevorzugt' verwenden soll. Nach Ablauf dieser Zeit führt ein Client diese Adresse als 'deprecated'.

Gültigkeitsdauer

Bestimmen Sie hier die Zeit in Sekunden, die der Client diese Adresse als 'gültig' verwenden soll.

Wenn Sie ein Präfix eines WAN-Interfaces zu dynamischen Bildung der Adressen verwenden, ist das Konfigurieren der Werte `Bevorzugte Gültigkeit` und `Gültigkeitsdauer` gesperrt. In diesem Fall ermittelt das Gerät diese Werte automatisch aus den vorgegebenen Werte des delegierten Präfixes des Providers.

Präfix beziehen von

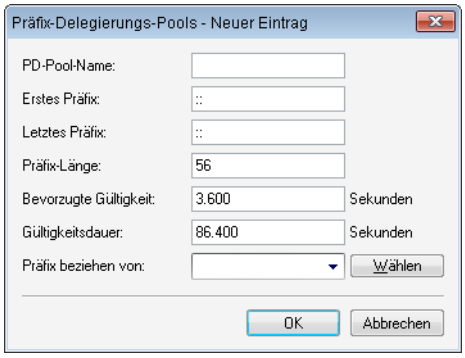
Mit diesem Parameter können Sie den Netzwerk-Clients Adressen aus dem Präfix zuteilen, das der Router vom WAN-Interface per DHCPv6-Präfix-Delegation vom Provider bezogen hat. Wählen Sie hier das entsprechende WAN-Interface aus. Hat der Provider beispielsweise das Präfix "2001:db8::/64" zugewiesen, dann können Sie beim Parameter **Erste Adresse** den Wert "::1" und bei **Letzte Adresse** den Wert "::9" eingeben. Zusammen mit dem vom Provider delegierten Präfix "2001:db8::/64" erhalten Clients dann Adressen aus dem Pool "2001:db8::1" bis "2001:db8::9". Ist das Provider-Präfix größer als "/64", z. B. "/48" oder "56", so müssen Sie das Subnetting für das logische Netzwerk in den Adressen berücksichtigen. **Beispiel:**

- Zugewiesenes Provider-Präfix: "2001:db8:abcd:aa::/56"
- "/64" als Präfix des logischen Netzwerks (Subnetzt-ID 1): "2001:db8:abcd:aa01::/64"
- Erste Adresse: "0:0:0:0001::1"
- Letzte Adresse: "0:0:0:0001::9"

Sie sollten diesen Mechanismus nur verwenden, wenn der Provider ein festes Präfix zuweist. Ansonsten kann es passieren, dass der Provider dem Router ein neues Präfix delegiert hat, aber der Client noch eine Adresse aus dem Pool mit dem alten Präfix besitzt. Dazu muss der Client seine Adresse beim Server aktualisieren.

Präfix-Delegierungs-Pools

In dieser Tabelle bestimmen Sie Präfixe, die der DHCPv6-Server an weitere Router delegieren soll:



PD-Pool-Name

Name des PD-Pools

Erstes Präfix

Erstes zu delegierendes Präfix im PD-Pool, z. B. "2001:db8:1100::"

Letztes Präfix

Letztes zu delegierendes Präfix im PD-Pool, z. B. "2001:db8:FF00::"

Präfix-Länge

Länge der Präfixe im PD-Pool, z. B. "56" oder "60"

Bevorzugte Gültigkeit

Bestimmen Sie hier die Zeit in Sekunden, die der Client dieses Präfix als 'bevorzugt' verwenden soll. Nach Ablauf dieser Zeit führt ein Client diese Adresse als 'deprecated'.

Gültigkeitsdauer

Bestimmen Sie hier die Zeit in Sekunden, die der Client dieses Präfix als 'gültig' verwenden soll.

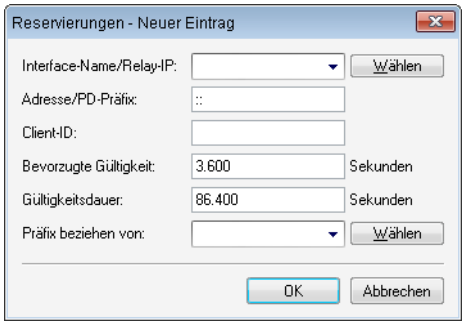
Wenn Sie ein Präfix eines WAN-Interfaces zu dynamischen Bildung der Adressen verwenden, ist das Konfigurieren der Werte `Bevorzugte Gültigkeit` und `Gültigkeitsdauer` gesperrt. In diesem Fall ermittelt das Gerät diese Werte automatisch aus den vorgegebenen Werte des delegierten Präfixes des Providers.

Präfix beziehen von

Name des WAN-Interfaces, von dem der Client das Präfix zur Adress- bzw. Präfixbildung verwenden soll.

Reservierungen

Wenn Sie Clients feste IPv6-Adressen oder Routern feste Präfixe zuweisen wollen, können Sie in dieser Tabelle pro Client eine Reservierung vornehmen:



Interface-Name-oder Relay

Name des Interfaces, auf dem der DHCPv6-Server arbeitet, z. B. "INTRANET". Alternativ können Sie auch die IPv6-Adresse des entfernten Relay-Agenten eintragen.

Adresse/PD-Präfix

IPv6-Adresse oder PD-Präfix, das Sie statisch zuweisen wollen.

Client-ID

DHCPv6-Unique-Identifier (DUID) des Clients.

Bei DHCPv6 lassen sich Clients nicht mehr wie bei DHCPv4 anhand ihrer MAC-Adresse, sondern anhand der DUID identifizieren. Die DUID lässt sich auf dem jeweiligen Client auslesen, unter Windows beispielsweise mit dem Kommandozeilen-Befehl `show dhcpv6-client` oder im WEBconfig unter **Status** > **IPv6** > **DHCPv6** > **Client** > **Client-ID**.

Arbeitet das Gerät als DHCPv6-Server, finden sich die Client-IDs der Clients mit aktuellem Bezug von IPv6-Adressen unter **Status** > **IPv6** > **DHCPv6** > **Server** > **Adress-Zuteilungen**, bzw. mit aktuellem Bezug von IPv6-Präfixen unter **Status** > **IPv6** > **DHCPv6** > **Server** > **PD-Zuteilungen**.

Der LANmonitor zeigt die Client-IDs der Clients unter **DHCPv6-Server** an.

Bevorzugte Gültigkeit

Bestimmen Sie hier die Zeit in Sekunden, die der Client diese Adresse als 'bevorzugt' verwenden soll. Nach Ablauf dieser Zeit führt ein Client diese Adresse als 'deprecated'.

Gültigkeitsdauer

Bestimmen Sie hier die Zeit in Sekunden, die der Client diese Adresse als 'gültig' verwenden soll.

Wenn Sie ein Präfix eines WAN-Interfaces zu dynamischen Bildung der Adressen verwenden, ist das Konfigurieren der Werte `Bevorzugte Gültigkeit` und `Gültigkeitsdauer` gesperrt. In diesem Fall ermittelt das Gerät diese Werte automatisch aus den vorgegebenen Werte des delegierten Präfixes des Providers.

Präfix beziehen von

Name des WAN-Interfaces, von dem der Client das Präfix zur Adress- bzw. Präfixbildung verwenden soll.

9.1.2 Ergänzungen im Setup-Menü

Reconfigure

Jede IPv6-Adresse bzw. jedes IPv6-Präfix hat eine vom Server vorgegebene Lebenszeit. In gewissen Intervallen fragt ein Client beim Server an, um seine Adresse zu verlängern (sogenannte Renew/Rebind-Zeiten).

Ändert sich aber z. B. durch Trennung und Wiederaufbau der Internetverbindung oder Anforderung eines neuen Präfixes (Telekom-Privcay-Funktion) das WAN-Präfix, so hat der Server keine Möglichkeit, die Netzwerkgeräte darüber zu informieren, dass sich Präfix bzw. Adresse geändert haben. Das bedeutet, dass ein Client noch eine alte Adresse oder ein altes Präfix verwendet und damit nicht mehr mit dem Internet kommunizieren kann.

Die Reconfigure-Funktion ermöglicht dem DHCPv6-Server, die Clients im Netzwerk zu einer Erneuerung der Leases/Bindings aufzufordern.

SNMP-ID:

2.70.3.1.4.13

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Server** > **Interface-Liste**

Mögliche Werte:

Aus: Deaktiviert die Reconfigure-Funktion.

Verbieten: Clients, die die Reconfigure-Option in Anfragen gesetzt haben, werden vom Server abgelehnt und erhalten keine Adressen, Präfixe oder andere Optionen.

Erlauben: Hat ein Client die Reconfigure-Option in Anfragen gesetzt, so verhandelt der Server mit dem Client die nötigen Parameter, um zu einem späteren Zeitpunkt ein Reconfigure zu starten.

Erzwingen: Clients müssen die Reconfigure-Option in ihren Anfragen setzen, sonst lehnt der Server diese Clients ab. Dieser Modus ist dann sinnvoll, wenn Sie sichergehen wollen, dass der Server ausschließlich Clients bedient, die Reconfigure unterstützen. Dadurch ist gewährleistet, dass alle Clients zu einem späteren Zeitpunkt erfolgreich durch Reconfigure ihre Adressen, Präfixe oder weiteren Informationen aktualisieren können.

Default:

Aus

9.1.3 Ergänzungen im Status-Menü

Reconfigure

Diese Aktion veranlasst die Clients im Netz, ihre Leases/Bindings zu erneuern. Es kann entweder ein Reconfigure für Renew-, Rebind- oder Information-Request ausgelöst werden.

Die Reconfigure-Funktion erwartet im Anschluss folgende Parameter:

- `renew`: (optional, Default) Fordert den Client auf, ein Renew für seine Adresse und/oder sein Präfix durchzuführen.
- `rebind`: (optional) Fordert den Client auf, ein Rebind für seine Adresse und/oder sein Präfix durchzuführen.
- `info`: (optional) Fordert den Client auf, ein Information-Request zu senden, um z. B. seinen DNS-Server zu aktualisieren.
- `-c <Client-ID>`: Die Reconfigure-Funktion gilt für den Client mit der angegebenen Client-ID.
- `-b <Adresse/Präfix>`: Die Reconfigure-Funktion gilt für den Client mit der angegebenen Adresse bzw. dem angegebenen Präfix.
- `-i <Interface/Relay>`: Die Reconfigure-Funktion gilt allen Clients, die am angegebenen Interface bzw. Relay angeschlossen sind.
- `-a`: Die Reconfigure-Funktion gilt für alle Clients.

SNMP-ID:

1.77.3.1.7

Pfad Telnet:

Status > **IPv6** > **DHCPv6** > **Server**

10 Diagnose

10.1 SYSLOG: Konfiguration der Speicherfrist von Systemereignissen

Ab der Version LCOS 8.82 können Sie die Speicherfrist für Systemereignisse auch komfortabler in Stunden, Tagen und Monaten eingeben.

10.1.1 Ergänzungen im Setup-Menü

Nachrichtenalter-Einheit

Dieser Parameter bestimmt, ob das angegebene Nachrichtenalter in Stunden, Tagen oder Monaten gilt.

Ein Monat entspricht hierbei 30 Tagen.

SNMP-ID:

2.22.11

Pfad Telnet:

Setup > **SYSLOG**

Mögliche Werte:

Stunde

Tag

Monat

Default:

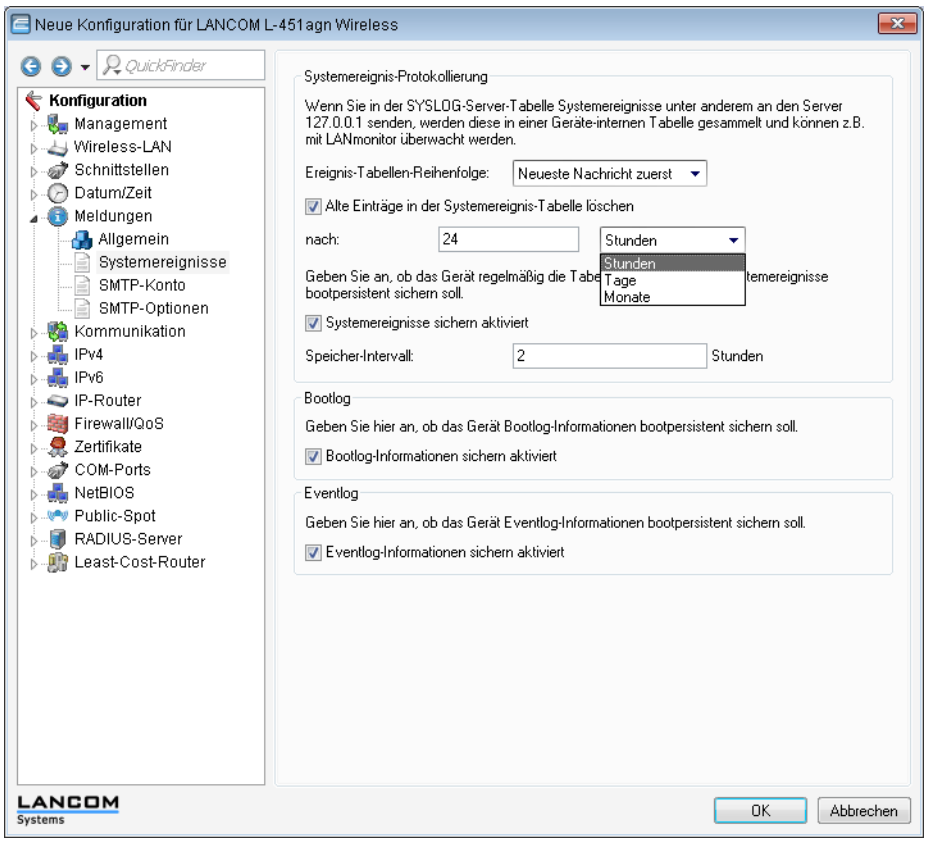
Stunde

10.1.2 Ergänzungen in LANconfig

Konfiguration der Speicherfrist von Systemereignissen

Unter **Meldungen** > **Systemereignisse** können Sie im Abschnitt **Systemereignisse-Protokollierung** bestimmen, für wie lange das Gerät Systemereignisse speichern soll. Sie können sowohl Menge (0–9999) als auch Einheit (Stunde, Tag, Monat) festlegen.

Ein Monat entspricht hierbei 30 Tagen.



10.2 SYSLOG: Erweiterung der Einträge des internen SYSLOG-Servers

Ab der Version LCOS 8.82 kann der interne SYSLOG-Server bestimmter Geräte bis zu 23.000 Einträge speichern.

Diese Änderung umfasst derzeit die folgenden Gerätetypen und -Serien:

- LANCOM 17xx+-Serie
- LANCOM 1781-Serie
- LANCOM 1780EW-4G
- LANCOM L-460agn dual Wireless
- LANCOM L-451agn Wireless
- LANCOM L-452agn dual Wireless
- LANCOM 7100+ VPN
- LANCOM 9100+ VPN
- LANCOM WLC-4006+

10.3 SYSLOG: Erweiterte Statusanzeige des Einbuchvorgangs ins Mobilfunknetz

Ab LCOS-Version 8.82 zeigt das SYSLOG detaillierte Informationen über den Status des Einbuchvorgangs in ein Mobilfunknetz (UMTS, GPRS, LTE) an.

10.3.1 Erweiterte Statusanzeige des Einbuchvorgangs ins Mobilfunknetz

Um Probleme bei der Verbindung in ein Mobilfunknetz schneller analysieren zu können, führen WWAN-fähige LANCOM-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:

Änderung oder Problem beim Setzen des Registrierungsstatus

Status	Bedeutung	SYSLOG-Severity
not searching for network	Das Modem ist nicht eingebucht und sucht derzeit nicht nach einem Funknetz.	INFORM
searching for network	Das Modem ist nicht eingebucht und sucht nach einem Funknetz.	INFORM
registered to home network	Das Modem hat sich erfolgreich ins Funknetz seines Mobilfunkproviders eingebucht.	INFORM
registered to foreign network	Das Modem hat sich erfolgreich ins Funknetz eines Roaming-Partners seines Mobilfunkproviders eingebucht.	INFORM
unknown registration	Initialwert. Das Modem hat noch keine Rückmeldung vom Funkmodul über den Einbuchungsstatus erhalten.	INFORM
network registration denied	Der Mobilfunkprovider hat die Einbuchung ins Funknetz abgelehnt.	ERROR
lost network registration	Das Modem hat die Verbindung zum eingebuchten Funknetz verloren.	NOTICE
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
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

Problem beim Setzen des Netzwerkmodus

Status	SYSLOG-Severity
Auto	ERROR
UMTS	ERROR

Status	SYSLOG-Severity
GPRS	ERROR
LTE	ERROR

Problem beim Setzen des APN

Status	Bedeutung	SYSLOG-Severity
failed to set 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 oder nicht existiert, oder ein Fehler im Gerät vorliegt.	ERROR

10.3.2 Ergänzungen im Status-Menü

Netzregistrierung

Dieser Eintrag zeigt den Statuswert der Netzregistrierung an. Jede Statusänderung erzeugt jeweils eine SNMP-Trap-Nachricht zur weiteren Auswertung und Verarbeitung (z. B. durch einen SNMP-Manager).

Mögliche Werte sind:

- **No_Network**: Das Modem ist nicht eingebucht und sucht derzeit nicht nach einem Funknetz.
- **Home_Network**: Das Modem hat sich erfolgreich ins Funknetz seines Mobilfunkproviders eingebucht.
- **Searching**: Das Modem ist nicht eingebucht und sucht nach einem Funknetz.
- **Searching(Denied)**: Das Modem ist nicht eingebucht und sucht nach einem Funknetz, wurde im Verlauf der Suche aber mindestens einmal abgewiesen. Dieser Zusatz verschwindet, sobald das Modem sich erfolgreich einbucht.
- **Unknown**: Initialwert. Das Modem hat noch keine Rückmeldung vom Funkmodul über den Einbuchungsstatus erhalten.
- **Roaming**: Das Modem hat sich erfolgreich ins Funknetz eines Roaming-Partners seines Mobilfunkproviders eingebucht.
- **Denied**: Der Mobilfunkprovider hat die Einbuchung ins Funknetz abgelehnt.

SNMP-ID:

1.49.7

Pfad Telnet:

Status > **Modem-Mobilfunk**