connecting your business

Addendum

LCOS 8.84

LANCOM
Systems

Inhalt

1 Addendum zur LCOS-Version 8.84

Dieses Dokument beschreibt die Änderungen und Ergänzungen in der LCOS-Version 8.84 gegenüber der vorherigen Version.

2 Konfiguration

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

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

2.1 Default-Rollout-Assistent

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

Beim Aufruf des Default-Rollout-Assistenten fragt der Assistent alle Informationen ab, die er für einen erfolgreichen Verbindungsaufbau zum LSR benötigt. Hierzu gehören:

- das für den Verbindungsaufbau verwendete Protokoll (HTTP oder HTTPS);
- die IP-Adresse oder den DNS-Namen des LSR-Servers;
- den Benutzernamen und das Passwort für die Authentisierung am LSR;
- der Name oder die Nummer des Rollout-Projektes;
- die Geräte-ID (optional); sowie
- die zum Gerät gehörende Rollout-TAN.

Dieser Prozess lässt sich auch teilweise bis vollständig automatisieren, indem Sie die betreffenden Angaben dauerhaft im Gerät hinterlegen. Die dazugehörige Tabelle finden Sie im Setup-Menü unter **HTTP** > **Rollout-Wizard** > **Vorbelegungen**. Standardmäßige Vorbelegungen sind der vom Assistenten verwendete Port sowie die Loopback-Adresse.

Sofern Ihr Gerät über einen USB-Anschluss verfügt, lässt sich dessen automatische Ladefunktion auch dafür nutzen, um ein beliebiges unkonfiguriertes Gerät per USB-Stick mit den relevanten Basisinformationen für den Rollout-Wizard zu versorgen.

Bevor das Gerät mit dem Rollout-Vorgang beginnt, zeigt Ihnen der Assistent die verwendeten Verbindungsdaten in einer Zusammenfassung noch einmal an. Außerdem überprüft das Gerät mit einem ICMP Echo Request (Ping), ob der angegebene Server erreichbar ist. Schlägt diese Prüfung fehl, haben Sie die Möglichkeit, den Assistenten neu zu konfigurieren oder den Rollout-Vorgang trotzdem fortzusetzen. Ist der angegebene Host erreichbar, beginnt das Gerät im weiteren Verlauf damit, seine Zielkonfiguration beim LSR abzufragen.

Sofern der LSR-Server über das Internet erreichbar ist, Sie den Rollout-Wizard aber auf einem Gerät ausführen, auf dem noch keine Internet-Verbindung eingerichtet ist, müssen Sie zunächst den Einrichtungsassistenten für das Internet durchlaufen.

2.1.1 Ergänzungen im Setup-Menü

Vorbelegungen

Über diese Tabelle haben Sie die Möglichkeit, alle Parameter, die der Default-Rollout-Assistent standardmäßig abfragt, mit vorgegebenen Werten zu belegen. So konfigurierte Parameter werden beim Ausführen des Default-Rollout-Assistenten anschließend übergangen und nicht mehr abgefragt.

Eine 'leere' Vorbelegung bei den Werten **Port** und **Quell-Loopback-Adresse** wertet das Gerät als Eintrag 'Auto'. In diesem Fall benutzt der Default-Rollout-Assistent den entsprechenden HTTP(S)-Standard-Port sowie als Loopback-Adresse die zum Ziel passende Adresse Ihres Gerätes. Wenn Sie mit verschiedenen ARF-Netzen arbeiten, müssen Sie über die Loopback-Adresse das ARF angeben, in dem der LSR-Server erreichbar ist.

SNMP-ID:

2.21.20.9

Pfad Telnet:

Setup > **HTTP** > **Rollout-Wizard**

Name

Dieser Eintrag zeigt den Namen des Parameters, der sich mit vorbelegten Werten füllen lässt.

SNMP-ID:

2.21.20.9.1

Pfad Telnet:

Setup > **HTTP** > **Rollout-Wizard** > **Vorbelegungen**

Vorbelegung

Dieser Eintrag zeigt den Wert, mit dem der betreffende Parameter im Rollout-Assistenten vorbelegt wird.

SNMP-ID:

2.21.20.9.2

Pfad Telnet:

Setup > **HTTP** > **Rollout-Wizard** > **Vorbelegungen**

Mögliche Werte:

Beliebiger String, max. 127 Zeichen aus

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

Default:

Benutze-Vorbelegung

Über diesen Eintrag legen Sie fest, ob das Gerät den vom Rollout-Wizard abgefragten Parameter automatisch mit dem hier konfigurierten Inhalt vorbelegt. Dieser Parameter wird dann nicht mehr im Rollout-Wizard abgefragt.

SNMP-ID:

2.21.20.9.2

Pfad Telnet:

Setup > **HTTP** > **Rollout-Wizard** > **Vorbelegungen**

Mögliche Werte:

nein

ja

Default:

(zeilenabhängig)

Loesche-Assistent

Über diese Aktion löschen Sie einen benutzerdefinierten Rollout-Assistenten. Das Gerät verwendet dann den LCOS-internen Default-Assistenten, wenn Sie den Rollout-Assistenten aktivieren.

SNMP-ID:

2.21.20.10

Pfad Telnet:

Setup > **HTTP** > **Rollout-Wizard**

Mögliche Parameter:

Keine Parameter vorhanden

2.2 Automatische Erzeugung gerätespezifischer SSH-Schlüssel

Sämtliche Geräte auf LCOS-Basis, die mit einer LCOS-Version kleiner als 8.84 ausgeliefert werden, sind ab Werk mit einem Satz vordefinierter Kryptographie-Schlüssel mit 1024 Bit Länge ausgestattet, die folgende Fingerprints abbilden:

```
SSH
    ssh-dss 27:c5:1d:9f:be:27:3d:50:d7:bf:c1:68:0b:18:97:d7
    ssh-rsa 03:56:e6:52:ee:d2:da:f0:73:b5:df:3d:09:08:54:b7
```

Sofern Sie ein Gerät mit LCOS 8.84 oder höher einsetzen und keinen individuellen Schlüssel ins Gerät geladen haben, versucht der interne SSH-Server nach einem Konfigurations-Reset direkt beim Systemstart eigene gerätespezifische SSH-Schlüssel zu kompilieren. Dazu gehören

- ein SSH-2-RSA-Schlüssel mit 2048 Bit Länge;
- ein SSH-2-DSS-Schlüssel mit 1024 Bit Länge (Definition nach FIPS 186-2);

welche das Gerät als **ssh_rsakey** und **ssh_dsakey** in seinem internen Dateisystem ablegt.

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

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

```
sshkeygen -t rsa -b 2048 -f ssh_rsakey
sshkeygen -t dsa -b 1024 -f ssh_dsakey
```

2.3 Sicherheitsabfrage bei der SSH-Schlüsselerzeugung unterdrücken

Ab LCOS 8.84 haben Sie die Möglichkeit, mit einem speziellen Parameter eventuelle Sicherheitsabfragen bei der SSH-Schlüsselerzeugung im LCOS zu unterdrücken:

```
sshkeygen [-?|-h] [-t (dsa|rsa)] [-b <Bits>] -f <OutputFile> [-q]
```

-q

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

2.4 Mehrere SNMP-Communities einrichten

Ab LCOS 8.84 haben Sie die Möglichkeit, mehrere schreibgeschützte Communities für den SNMP-Zugriff zu definieren. Die Einträge in der Tabelle *2.9.22 Read-Only-Communities* auf Seite 10 ergänzen dazu den bereits bestehenden Parameter *2.9.15 Read-Only-Community* auf Seite 10. Das Gerät wertet die hinterlegten Einträge gleichberechtigt aus.

2.4.1 Ergänzungen im Setup-Menü

Passw.Zwang-fuer-SNMP-Lesezugriff

Über diese Einstellung legen Sie fest, ob das Lesen von SNMP-Meldungen über einen SNMP-Agenten (z. B. LANmonitor) die Eingabe eines Passwort erfordert.

SNMP-ID:

2.9.10

Pfad Telnet:

Setup > **SNMP**

Mögliche Werte:

nein

In dieser Einstellung lassen sich Informationen über den Zustand des Gerätes, aktuelle Verbindungen, Reports, etc. öffentlich via SNMP auslesen (Ready-Only Community 'public' aktiviert).

ja

In dieser Einstellung lassen sich Informationen über den Zustand des Gerätes, aktuelle Verbindungen, Reports, etc. erst dann via SNMP auslesen, nachdem sich der betreffende Benutzer am Gerät authentisiert hat (Ready-Only Community 'public' daktiviert). Die Authorisierung kann wahlweise über die Zugangsdaten für den Administrator-Account oder über den in der individuellen SNMP-Community definierten Zugang derfolgen.

Default-Wert:

nein

Read-Only-Community

Über diesen Parameter definieren Sie eine individuelle SNMP-Community für den Lesezugriff. Geben Sie dazu entweder ein Master-Passwort oder ein Benutzername:Passwort-Paar ein. Lassen Sie das Feld leer, um keine weitere schreibgeschützte Community ausser 'public' zu verwenden (sofern aktiviert).

Das deaktivieren der Community 'public' hat keine Auswirkung auf den Zugriff über die hier angelegte Community. Eine individuelle SNMP Read-Only Community bleibt stets ein alternativer Zugangsschlüssel, welcher nicht an ein Administratorkonto gebunden ist.

SNMP-ID:

2.9.15

Pfad Telnet:

Setup > **SNMP**

Mögliche Werte:

Keine direkte Abhängigkeit von anderen Werten. **Read-Only-Community** aus **Setup** > **SNMP** > **Read-Only-Communities** erweitert jedoch den hier definierten Parameter um weitere schreibgeschützte Communities.

max. 31 Zeichen aus `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default-Wert:

leer

Read-Only-Communities

In dieser Tabelle definieren Sie weitere schreibgeschützte Communities für den SNMP-Zugriff.

SNMP-ID:

2.9.22

Pfad Telnet:

Setup > **SNMP**

Read-Only-Community

Über diesen Parameter definieren Sie eine zusätzliche individuelle SNMP-Community für den Lesezugriff. Geben Sie dazu entweder ein Master-Passwort oder ein Benutzername:Passwort-Paar ein.

Das deaktivieren der Community 'public' hat keine Auswirkung auf den Zugriff über die hier angelegte Community. Eine individuelle SNMP Read-Only Community bleibt stets ein alternativer Zugangsschlüssel, welcher nicht an ein Administratorkonto gebunden ist.

SNMP-ID:

2.9.22.1

Pfad Telnet:

Setup > **SNMP** > **Read-Only-Communities**

Mögliche Werte:

Keine direkte Abhängigkeit von anderen Werten. Dieser Parameter erweitert jedoch die **Read-Only-Community** aus **Setup** > **SNMP** um weitere schreibgeschützte Communities.

max. 31 Zeichen aus `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default-Wert:

leer

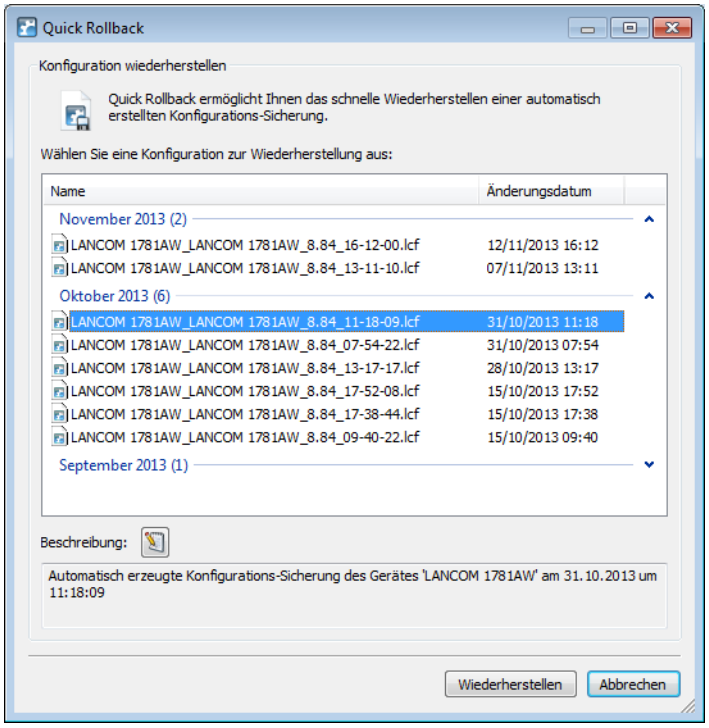
3 LCMS

3.1 Ergänzungen in LANconfig

3.1.1 Quick Rollback

Als Ergänzung zur automatischen Sicherung der Gerätekonfiguration haben Sie die Möglichkeit, die gesicherte Konfigurationen mit nur einem Klick wiederherzustellen. Dazu markieren Sie in der Geräteansicht das gewünschte Gerät und wählen **Gerät** > **Quick Rollback**, um die Funktion für das Quick Config Rollback aufzurufen. LANconfig listet Ihnen daraufhin alle geeigneten Gerätekonfigurationen auf, die sich unter dem Pfad für die automatischen Sicherung der Gerätekonfiguration befinden. Sofern LANconfig für das ausgewählte Gerät keine Sicherungsdatei finden kann, bricht diese Aktion mit einer Warnmeldung ab.

LANconfig nutzt für die Zuordnung von Konfigurationssicherungen zum betreffenden Gerät die in den Meta-Daten hinterlegte Seriennummer. Ab LCOS 8.84 wird diese bei der automatischen Sicherung miterfasst; in älteren Konfigurationssicherungen ohne Seriennummer müssen Sie diese jedoch manuell ergänzen, damit Quick Rollback die Dateien erkennt. Lesen Sie dazu auch *Erweiterte Meta-Daten für Konfigurationsdateien* auf Seite 13.



Um eine Konfigurationssicherung wiederherzustellen, markieren Sie einen Eintrag und klicken auf **Wiederherstellen**.

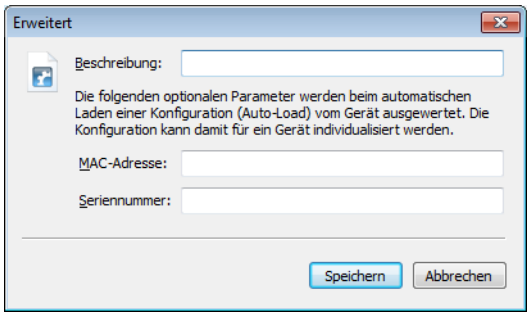
Darüber hinaus haben Sie die Möglichkeit, die Konfigurationssicherungen mit zusätzlichen Kommentaren zu versehen bzw. die darin enthaltenen Kommentare zu bearbeiten und ggf. zu ergänzen: Über die Schaltfläche **Beschreibung bearbeiten** ( ) aktivieren Sie das darunterliegende Kommentarfeld, um den darin enthaltenen Text zu bearbeiten. Über die Schaltfläche **Beschreibung speichern** ( ) schreiben Sie den Text des Kommentarfeldes anschließend in die Sicherungsdatei.

Quick Rollback ist nicht für LANCOM Switches verfügbar.

Erweiterte Meta-Daten für Konfigurationsdateien

LANconfig bietet beim (manuellen) Speichern einer Geräte-Konfiguration die Möglichkeit, zusätzlich zu den üblichen Meta-Daten erweiterte Meta-Daten – bestehend aus MAC-Adresse und/oder Geräte-Seriennummer – in der Konfigurationsdatei (*.lcf) zu erfassen. Diese erweiterten Meta-Daten werden dann z. B. beim Quick Config Rollback oder Laden einer Gerätekonfiguration via USB berücksichtigt.

Um die erweiterten Meta-Daten in eine Konfigurationsdatei mit aufzunehmen, klicken Sie im Datei-speichern-Dialog von LANconfig auf die Schaltfläche **Erweitert** und geben die Daten – sofern nicht bereits vorausgefüllt – in die jeweiligen Felder ein.



Alternativ haben Sie auch die Möglichkeit, eine lcf-/lcs-Datei in einem Texteditor zu öffnen und die erweiterten Meta-Daten nachträglich von Hand zu ergänzen. Ergänzen Sie dazu die Zeile `(<Firmware>) (<Feature-Mask>;<Feature-IDs>;<Hardware-Mask>)` um die Klammer `(MAC:<MAC-Address>;SERIAL:<Serialnumber>)`.

Beispiel, evtl. Zeilenumbrüche sind dem Anzeigeformat geschuldet:

```
(Konfiguration von 'DEVICE-01' vom 12.11.2013)
(8.84.0081) (0x0000c010,IDs:4,e,f,2b;0x0c000002) (MAC:00a0571d12fc;SERIAL:4002578718100036)
```

3.1.2 Firmware über das Kontextmenü freischalten

Sie haben die Möglichkeit, die im Testmodus laufende Firmware auch über die Firmware-Verwaltung im Kontext-Menü von LANconfig freizuschalten. Dazu wurde in LANconfig 8.84 der Firmware-Auswahl-Dialog überarbeitet.

3.1.3 Schlüssel-Fingerprints bei der Inbetriebnahme von CC-Geräten exportieren

Ab LANconfig 8.84 haben Sie die Möglichkeit, bei der Inbetriebnahme von CC-Geräten die eingespielten SSH-Key Fingerprints komfortabel mit LANconfig zu exportieren. LANconfig legt dazu beim Durchlaufen des CC-Inbetriebnahme-Assistenten die Datei **CCWizSummary.csv** an, welche die IP-Adresse des Gerätes, den Gerätenamen und dessen (SSH) Schlüssel-Fingerprint enthält. Über die so erzeugte Liste kann sich dann z. B. ein Systemadministrator bei der Fernwartung bzw. nach einem Rollout vor dem Login vergewissern, dass er mit dem korrekten Gerät verbunden ist.

Standardmäßig speichert LANconfig die CSV-Datei unter `C:\Program Files (x86)\LANCOM\LANconfig\Logging\`. Sie haben aber auch die Möglichkeit, diesen Pfad im Eingabefeld unter **Extras** > **CC-Inbetriebnahme-Assistent starten** > **Einstellungen** > **Pfad** zu verändern.

3.1.4 TLS/STARTTLS-Unterstützung und zusätzliche Authentifizierungsmethoden mit SMTP-Servern

Ab LCOS 8.84 nutzt das Gerät standardmäßig den Port 587 für die Verbindung zu SMTP-Servern. Außerdem erfolgt der Verbindungsaufbau bevorzugt über STARTTLS. Als Authentifizierungsmethode steht neben PLAIN nun auch eine sichere Authentifizierung zur Verfügung, wobei sich das Gerät nach den Vorgaben des SMTP-Servers richten kann.

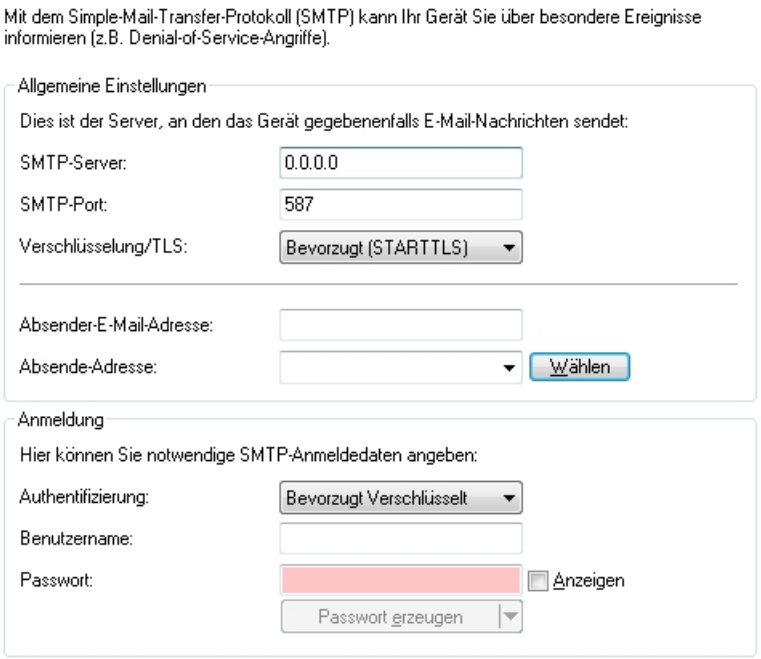
Einrichtung einer E-Mail-Adresse für den Nachrichtenversand

Bei bestimmten Ereignissen können Sie im LANCOM festlegen, dass es eine Nachricht an eine definierte E-Mail-Adresse versendet. Diese Ereignisse können z. B. sein:

- Informationen über Verbindungsabbrüche auf einer WAN-Schnittstelle
- Meldungen der Firewall oder des Content-Filters
- Versand von VPN-Profilen

Die E-Mail-Adresse richten sie wie folgt ein:

Im Konfigurationsdialog von LANconfig können Sie die E-Mail-Adresse unter **Meldungen** > **SMTP-Konto** konfigurieren.



SMTP-Server: Geben Sie in diesem Feld die IP-Adresse des SMTP-Servers an.

SMTP-Port: Standardmäßig ist hier der Port 587 für unverschlüsselt übertragene E-Mails voreingestellt.

Verschlüsselung/TLS: Bestimmen Sie hier, ob und wie das Gerät die Verbindung verschlüsseln soll. Die möglichen Werte haben folgende Bedeutung:

- **Keine**: Keine Verschlüsselung. Das Gerät beachtet eine ggf. vom Server gesendete STARTTLS-Antwort nicht.
- **Verschlüsselt (SMTPS)**: Das Gerät verwendet SMTPS, verschlüsselt also ab Verbindungsaufbau.
- **Bevorzugt (STARTTLS)**: Der Verbindungsaufbau erfolgt unverschlüsselt. Bietet der SMTP-Server STARTTLS an, verschlüsselt das Gerät. Diese Einstellung ist der Defaultwert.
- **Erforderlich (STARTTLS)**: Der Verbindungsaufbau erfolgt unverschlüsselt. Bietet der SMTP-Server kein STARTTLS an, überträgt das Gerät keine Daten.

Absender-E-Mail-Adresse: Geben Sie hier eine gültige E-Mail-Adresse ein, die das LANCOM als Absender-Adresse verwendet. An diese Adresse versendet der angegebene SMTP-Server z. B. Nachrichten bei Zustellproblemen. Ist diese Adresse nicht angegeben oder ungültig, kann ein entsprechend konfigurierter SMTP-Server die Zustellung von Nachrichten verweigern.

Absende-Adresse: Optional können Sie hier eine alternative Absende-Adresse bestimmen, die das LANCOM verwenden soll. Falls Sie z. B. Loopback-Adressen konfiguriert haben, können Sie diese hier als Absender-Adressen angeben. Das Feld akzeptiert verschiedene Eingabeformate:

- Name des IP-Netzwerkes (ARF-Netz), dessen Adresse das Gerät einsetzen soll.
- "INT" für die Adresse des ersten Intranets.

- "DMZ" für die Adresse der ersten DMZ. Falls es eine Schnittstelle mit Namen "DMZ" gibt, nutzt das Gerät deren Adresse.
- "LB0"..."LBF" für eine der 16 Loopback-Adressen oder deren Name.
- Eine beliebige IP-Adresse in der Form `x.x.x.x`.

Authentifizierung: Bestimmen Sie hier, ob und wie sich das Gerät beim SMTP-Server authentifizieren soll. Die möglichen Werte haben folgende Bedeutung:

- **Keine**: Grundsätzlich keine Authentifizierung.
- **Bevorzugt Klartext**: Die Authentifizierung erfolg im Klartext (PLAIN, LOGIN), wenn der Server eine Authentifizierung verlangt. Ist keine Klartext-Authentifizierung vorgesehen, verwendet das Gerät eine sichere Authentifizierung.
- **Bevorzugt Verschlüsselt**: Eine sichere Authentifizierung findet statt, wenn sie möglich ist. Ansonsten verwendet das Gerät je nach Server-Einstellung eine Klartext- oder gar keine Authentifizierung.
- **Verschlüsselt**: Die Authentifizierung erfolgt mit verschlüsselter Übertragung des Passwortes (z. B. CRAM-MD5), wenn der Server eine Authentifizierung verlangt. Eine Klartext-Authentifizierung findet nicht statt.

Benutzername: Geben Sie hier den Benutzernamen ein, mit dem sich das LANCOM am SMTP-Server anmelden soll.

Passwort: Geben Sie hier das Passwort ein, mit dem sich das LANCOM am SMTP-Server anmelden soll.

Ergänzungen im Setup-Menü

Serverport

Geben sie hier die Nummer des SMTP-Ports des o. a. Servers für unverschlüsselt übertragene E-Mails an. Standardmäßig hat dieser die Nummer 587.

SNMP-ID:

2.27.2

Pfad Telnet:

Setup > **Mail**

Mögliche Werte:

max. 10 Zeichen

Default:

587

SMTP-benutze-TLS

Bestimmen Sie hier, ob und wie das Gerät die Verbindung verschlüsseln soll. Die möglichen Werte haben folgende Bedeutung:

- **Nein**: Keine Verschlüsselung. Das Gerät beachtet eine ggf. vom Server gesendete STARTTLS-Antwort nicht.
- **Ja**: Das Gerät verwendet SMTPS, verschlüsselt also ab Verbindungsaufbau.
- **Bevorzugt**: Der Verbindungsaufbau erfolgt unverschlüsselt. Bietet der SMTP-Server STARTTLS an, verschlüsselt das Gerät. Diese Einstellung ist der Defaultwert.
- **Erforderlich**: Der Verbindungsaufbau erfolgt unverschlüsselt. Bietet der SMTP-Server kein STARTTLS an, überträgt das Gerät keine Daten.

SNMP-ID:

2.27.12

Pfad Telnet:

Setup > **Mail**

Mögliche Werte:

Nein

Ja

Bevorzugt

Erforderlich

Default:

Bevorzugt

SMTP-Authentifizierung

Bestimmen Sie hier, ob und wie sich das Gerät beim SMTP-Server authentifiziert. Das Verhalten das Gerätes ist abhängig von der Server-Einstellung: Wenn der Server keine Authentifizierung erfordert, erfolgt in jedem Fall eine Anmeldung. Andernfalls verhält sich das Gerät den nachfolgend beschriebenen Einstellungen entsprechend.

SNMP-ID:

2.27.13

Pfad Telnet:

Setup > **Mail**

Mögliche Werte:

Keine

Grundsätzlich keine Authentifizierung.

Klartext-bevorzugt

Die Authentifizierung erfolgt bevorzugt im Klartext (PLAIN, LOGIN), wenn der Server eine Authentifizierung verlangt. Akzeptiert dieser keine Klartext-Authentifizierung, verwendet das Gerät die sichere Authentifizierung.

Verschluesselt

Die Authentifizierung erfolgt ohne Übertragung des Passwortes im Klartext (z. B. CRAM-MD5), wenn der Server eine Authentifizierung verlangt. Eine Klartext-Authentifizierung findet nicht statt.

Bevorzugt-Verschluesselt

Die Authentifizierung erfolgt bevorzugt verschlüsselt (z. B. CRAM-MD5), wenn der Server eine Authentifizierung verlangt. Akzeptiert dieser keine sichere Authentifizierung, verwendet das Gerät die Klartext-Authentifizierung.

Default-Wert:

Bevorzugt-Verschluesselt

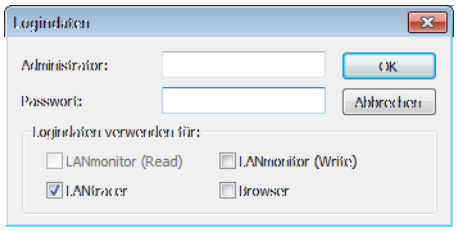
3.1.5 SNMP-Community an externe Programme übermitteln

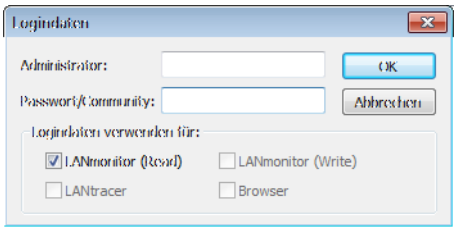
Ab LANconfig 8.84 haben Sie die Möglichkeit, die Zugangsdaten für den Aufruf externer Programme auch in Form einer SNMP-Community zu hinterlegen (**Gerät** > **Eigenschaften** > **Protokolle & Logins**). LANconfig übermittelt die Angaben dann automatisch beim Aufruf des betreffenden Programms.

Logindaten

Hinterlegen Sie in diesem Bereich die Zugangsdaten für die externen Programme. Klicken Sie **Neu**, um ein oder mehrere Programm(e) auszuwählen und die dafür geltenden Zugangsdaten einzugeben.

Je nach Auswahl fragt das Dialogfenster unterschiedliche Zugangsdaten ab. In jedem Fall haben Sie die Möglichkeit, sich mit dem Benutzernamen und Passwort Ihres Administrator-Zugangs beim betreffenden Programm zu authentisieren. Im Falle von LANmonitor besteht alternativ die Möglichkeit, auch eine (individuelle) SNMP-Community für den Lesezugriff anzugeben. Weitere Informationen zum schreibgeschützten SNMP-Zugriff finden Sie im Referenzhandbuch.

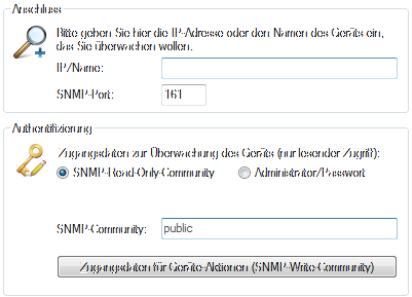




3.2 Ergänzungen im LANmonitor

3.2.1 Gerätezugriff über SNMP-Communities

Ab LANmonitor 8.84 haben Sie die Möglichkeit, die Zugangsdaten für den SNMP-Zugriff auch in Form einer SNMP-Community zu hinterlegen (Dialog **Gerät** > **Hinzufügen** > **Allgemein** sowie **Gerät** > **Eigenschaften** > **Allgemein**).



Authentifizierung

Wählen Sie in diesem Abschnitt aus, wie und mit welchen Zugangsdaten Sie sich am Gerät authentisieren. Die zu wählende Einstellung hängt davon ab, ob Sie den SNMP-Lesezugriff auf dem Gerät eingeschränkt und eine eigene Community definiert haben. Mehr dazu erfahren Sie im Referenzhandbuch.

- **SNMP-Read-Only-Community**: Wählen Sie diese Einstellung, wenn die Authentisierung am Gerät über
  - die öffentliche Community `public`; oder
  - eine eigene Community in Form eines Master-Passworts oder Benutzername:Passwort-Paares

  erfolgt. Diese geben Sie anschließend im Eingabefeld **Community** an.
- **Administrator/Passwort**: Wählen Sie diese Einstellung, wenn die Authentisierung am Gerät über
  - eine eigene Community in Form eines Benutzername:Passwort-Paares; oder
  - die Zugangsdaten eines Administratorkontos

  erfolgt. Den Benutzernamen geben Sie anschließend im Eingabefeld **Administrator**, das Passwort im Eingabefeld **Passwort** an.

Achten Sie dabei auf die korrekte Schreibweise, da bei Eingabe falscher Daten der SNMP-Zugang zum Gerät gesperrt wird.

Darüber hinaus haben Sie optional die Möglichkeit, die **Zugangsdaten für Geräte-Aktionen (SNMP-Write-Community)** wahlweise für die aktuelle Sitzung oder dauerhaft in LANmonitor zu speichern. Diese Daten sind für alle Geräte-Aktionen (z. B. das Löschen oder Zurücksetzen von Status-Werten) erforderlich. Wenn Sie keine Daten hinterlegen, fragt das Programm sie bei der nächsten Aktion ab.

Für den reinen Lesezugriff ist die Angabe einer Read-Only-Community anstelle eines Administratorkontos die bevorzugte Wahl, da SNMP-Pakete bei SNMPv2 im Klartext übertragen werden.

4 Diagnose

4.1 Dokumentation von Ereignissen auf den xDSL-Schnittstellen

Ab LCOS 8.84 protokolliert das Gerät auch Zustandsänderung auf den xDSL-Schnittstellen.

Das Gerät erzeugt bei den folgenden xDSL-Schnittstellen-Ereignissen je einen SYSLOG-Eintrag:

Status	Bedeutung	SYSLOG-Severity
xDSL: Booting modem: ...	Das Modem startet neu.	NOTICE
xDSL: Set up line to <Leitungsmodus>/<Leitungstyp>	Das xDSL-Modul baut die Verbindung mit dem angegebenen Modus und Typ auf. Folgende Werte sind möglich: ■ Leitungsmodus: Disabled, Auto sowie alle unter **Setup** > **Schnittstellen** > **ADSL-Interface bzw. VDSL-Interface** konfigurierbaren Modi. ■ Leitungstyp: POTS, ISDN	INFORM
xDSL: Line is up. DS-Rate: ..., US-Rate: ..., DS-Margin: ..., US-Margin: ..., DS-Attn: ..., US-Attn: ..., Mode: ..., Profile:	Das Modem hat die Verbindung erfolgreich mit angegebenen Werten aufgebaut.	NOTICE
xDSL: Line data update. DS-Rate: ..., US-Rate: ..., DS-Margin: ..., US-Margin: ..., DS-Attn: ..., US-Attn: ..., Mode: ..., Profile: ...	Nach einer Synchronisation nehmen Modem und DSLAM eine Optimierung der xDSL-Verbindung vor. Dadurch können sich ggf. die Leitungswerte ändern. Nach einer Minute gibt das Modem die aktuellen Leitungswerte aus.	NOTICE
xDSL: Line data update.	Nach einer Synchronisation nehmen Modem und DSLAM eine Optimierung der xDSL-Verbindung vor. Nach einer Minute gibt das Modem diese Meldung aus, wenn sich die Leitungswerte nach der Synchronisation nicht geändert haben.	NOTICE
xDSL: Line disconnected due to	Die Verbindung ist aus dem angegebenem Grund abgebrochen. Folgende Werte sind möglich: ■ modem reboot ■ retrain ■ silence ■ high line error rate ■ protocol setting ■ line type setting ■ automode line type switch ■ modem timeout ■ VC parameter change	NOTICE

Status	Bedeutung	SYSLOG-Severity
xDSL: SNR margin (dB, Down/Up): .../...	Der Wert zwischen notwendigem und gemessenem Signal-Rausch-Abstand (SNR) hat sich um mehr als 1dB geändert.	INFORM

4.2 SYSLOG: Erweiterte Statusanzeige des Einbuchvorgangs ins Mobilfunknetz

Ab LCOS-Version 8.84 zeigt das SYSLOG noch mehr Informationen über den Status des Einbuchvorgangs in ein Mobilfunknetz (UMTS, GPRS, LTE) an.

4.2.1 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:

Status	Bedeutung	SYSLOG-Severity
WWAN: Currently not searching for network	Das Modem ist nicht eingebucht und sucht derzeit nicht nach einem Funknetz.	INFORM
WWAN: Searching for network	Das Modem ist nicht eingebucht und sucht nach einem Funknetz.	INFORM
WWAN: Registered to home network	Das Modem hat sich erfolgreich ins Funknetz seines Mobilfunkproviders eingebucht.	INFORM
WWAN: Registered to foreign network	Das Modem hat sich erfolgreich ins Funknetz eines Roaming-Partners seines Mobilfunkproviders eingebucht.	INFORM
WWAN: Unknown registration	Initialwert. Das Modem hat noch keine Rückmeldung vom Funkmodul über den Einbuchungsstatus erhalten.	INFORM
WWAN: Network registration denied	Der Mobilfunkprovider hat die Einbuchung ins Funknetz abgelehnt.	ERROR
WWAN: Lost network registration	Das Modem hat die Verbindung zum eingebuchten Funknetz verloren.	NOTICE
WWAN: Failed to set network	Das Modem hat den Befehl zum Setzen des Netzwerks mit einer Fehlermeldung beantwortet. Dieser Fehler tritt z. B. auf, wenn das Netzwerk unerreichbar ist oder nicht existiert, oder ein Fehler im Gerät vorliegt.	ERROR
WWAN: Failed to set network mode	Das Modem hat den Befehl zum Setzen des Netzwerkmodus mit einer Fehlermeldung beantwortet. Dieser Fehler tritt z. B. auf, wenn das Netzwerk unerreichbar ist oder nicht existiert, oder ein Fehler im Gerät vorliegt.	ERROR
WWAN: Using modem '...'.	Zeigt das verwendete Modem an.	INFORM
WWAN: Modem is gone.	Modem ist nicht mehr verfügbar.	INFORM

Status	Bedeutung	SYSLOG-Severity
WWAN: Resetting modem.	Re-Init durch Modem-Reset	WARNING
WWAN: Local disconnect.	D-Kanal-Disconnect	INFORM
WWAN: Local disconnect (Release).	D-Kanal-Release	INFORM
WWAN: Force 2G mode at ... dB.	Modem startet den 2G-Fallback	NOTICE
WWAN: Ending forced 2G mode.	Modem beendet den 2G-Fallback	INFO
WWAN: Forced 2G mode disabled.	Der 2G-Fallback-Modus ist deaktiviert.	INFO
WWAN: PIN missing in profile.	PIN fehlt im Profil.	ERROR
WWAN: PUK required.	Modem fordert PUK.	ERROR
WWAN: Invalid PIN.	Falsche PIN	ERROR
WWAN: Failed to set APN	Fehler beim Setzen des APN. Das Modem hat den Befehl zum Setzen eines APNs mit einer Fehlermeldung beantwortet. Dieser Fehler tritt z. B. auf, wenn das Netzwerk unerreichbar ist bzw. nicht existiert oder ein Fehler im Gerät vorliegt.	ERROR
WWAN: Using profile '...'.	Name des verwendeten Profils.	NOTICE
WWAN: Can not find profile '...'.	Profil nicht vorhanden.	ERROR
WWAN: Disonnected.	Physikalische Verbindung beendet.	INFORM
WWAN: Connected: '...'.	Das Modem hat eine Datenverbindung zum Netzwerk hergestellt und kann ab jetzt Daten über das Mobilfunk-Netzwerk übertragen.	INFORM
WWAN: Cell-ID is ..., Local Area Code is	Funkzellen-ID und Ländercode.	INFORM
WWAN: Current Network is '...'.	Netzwerk (Text)	INFORM
WWAN: Current Network is	Netzwerk (Nummer)	INFORM
WWAN: Mode ..., Band '...'.	Anzeige von Netzwerk-Modus und Band	INFORM
WWAN: Mode ..., Band '...', Bandwith in MHz: ..., Channel (Rx/Tx): .../....	Anzeige von Netzwerk-Modus, Band, Bandbreite sowie Kanal (Empfangs- und Senderichtung).	INFORM
WWAN: Mode ..., Band '...', Channel (Rx/Tx): .../....	Anzeige von Netzwerk-Modus, Band sowie Kanal (Empfangs- und Senderichtung).	INFORM
WWAN: Max. Datarate (Ds/Us): .../....	Aktuelle QoS-Datenrate (Down- und Upstream)	INFORM
WWAN: Network mode is '...'.	Aktueller Modus. Mögliche Werte sind: ■ GPRS ■ EDGE ■ UMTS ■ HSPA ■ LTE	INFORM
WWAN: Signal strength is ... dBm.	Aktuelle Signalstärke	INFORM
WWAN: Using stored APN. APN: '...', PDP type:	Aktuell verwendeter Zugangspunkt im Netzwerk.	INFORM
WWAN: Setting new APN. APN: '...', PDP type:	Wechsel des Netzwerk-Zugangspunktes	INFORM
WWAN: Temperature is ...°C.	Aktuelle Modultemperatur	INFORM

Status	Bedeutung	SYSLOG-Severity
WWAN: Temperature status: '...'.	Aktueller Temperaturstatus des Moduls. Mögliche Werte sind: ■ Normal ■ High Warning ■ High Critical ■ Low Critical	INFORM (Normal), WARNING (High Warning), CRITICAL (High Critical, Low Critical)
WWAN: Closing device: '...'.	Das Gerät, über das die Verbindung ins WAN läuft, fährt herunter.	INFORM
WWAN: Hangup: '...'.	Das Modem beendet die Netzwerk-Verbindung.	INFORM
WWAN: Error in modem init: '___'.	Bei der Initialisierung des Modems ist ein Fehler aufgetreten.	ERROR

5 Routing und WAN-Verbindungen

5.1 Volumen-Budget

Ab LCOS 8.84 erfasst das Gerät das gesamte Datenvolumen aller WAN-Schnittstellen in Sende- und Empfangsrichtung, um z. B. bei einer Drosselung der Datenrate entsprechend reagieren zu können.

5.1.1 Datenvolumen auf der WAN-Schnittstelle

Mobilfunk- oder Festnetzanbieter können je nach Vertrag auch bei Flatrates ab einem bestimmten Datenvolumen eine Drosselung der Übertragungsrate aktivieren. Das Gerät erfasst das verbrauchte Datenvolumen je WAN-Schnittstelle, archiviert die Werte für bis zu 12 Monate und kann bei Erreichen eines festgelegten Grenzwertes Aktionen ausführen. Die Budgets gelten auch für VPN-, PPTP- oder alle weiteren Arten von Gegenstellen.

Beim Monatswechsel speichert das Gerät die Daten des abgelaufenen Monats in einer Archiv-Tabelle und setzt den Zähler des laufenden Monats auf Null zurück. Das aktuelle Datenvolumen sowie die im Archiv gespeicherten Daten können Sie über LANmonitor oder im Status-Menü von WEBconfig einsehen. Das Archiv beinhaltet immer Daten der letzten 12 Monate. Im 13. Monat überschreibt das Gerät automatisch die Archiv-Daten des 1. Monats.

Dieses Feature ist derzeit ausschließlich für die folgenden Geräteypen und -serien verfügbar:

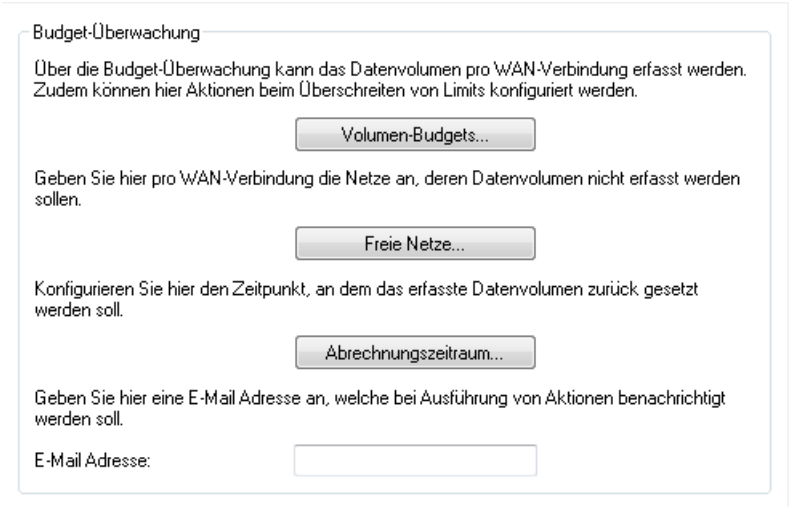
- LANCOM L-45x Serie
- LANCOM 1781 Serie
- LANCOM 1780EW-3G, 1780EW-4G
- LANCOM WLC-4006+, WLC-4025+, WLC-4100
- LANCOM 7100 VPN, 7100+ VPN, 9100 VPN, 9100+ VPN
- LANCOM IAP-321, IAP-321-3G, IAP-3G
- LANCOM OAP-322, OAP-321, OAP-321-3G, OAP-3G

Konfiguration von Datenvolumen-Budgets

Der folgende Abschnitt beschreibt, wie Sie mit LANconfig die Datenvolumen für Gegenstellen verwalten können.

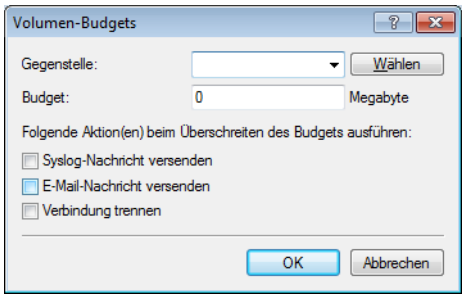
1. Starten Sie LANconfig über **Start** > **Programme** > **LANCOM** > **LANconfig** und öffnen Sie die Konfiguration des Gerätes, für das Sie die Erfassung des Datenvolumens einrichten möchten.
   Hinweise zur Geräte-Konfiguration über LANconfig finden Sie im Abschnitt LCMS-Abschnitt des Referenzhandbuchs.

2. Wechseln Sie im Konfigurationsdialog in die Ansicht **Management** > **Budget**.



Wenn das Gerät bei Überschreiten des festgelegten Datenvolumens eine Email versenden soll, geben Sie bereits in diesem Dialog im Feld **E-Mail Adresse** die entsprechende Adresse ein.

3. Klicken Sie auf die Schaltfläche **Volumen-Budgets** und anschließend auf **Hinzufügen**.



Im Feld **Gegenstelle** können Sie die Gegenstelle auswählen, für die Sie das Volumen-Budget angeben wollen. Mit **Wählen** können Sie aus den verfügbaren Gegenstellen auswählen bzw. neue Gegenstellen verwalten.

Geben Sie im Feld **Budget** das Datenvolumen an. Dieser Wert richtet sich meistens nach dem im Provider-Vertrag verhandelten Datenvolumen bis zur Drosselung der Übertragungsrate.

Sie können zusätzlich Aktionen definieren, die das Gerät bei Erreichen des Budgets ausführen soll:

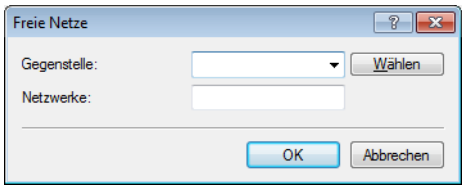
- **Syslog-Nachricht versenden**: Das Gerät erzeugt eine Syslog-Nachricht (mit dem Flag "Critical"), die Sie im Syslog-Speicher des Gerätes, über LANmonitor oder einen speziellen Syslog-Client auswerten können.
- **E-Mail-Nachricht versenden**: Das Gerät verschickt eine Benachrichtigung an die Email-Adresse, die Sie im Dialog weiter oben angegeben haben.
- **Verbindung trennen**: Das Gerät trennt die Verbindung zur Gegenstelle.

> Die Aktion **Verbindung trennen** aktiviert die Gebührensperre. Das Gerät kann bis zum Ablauf des Monats keine Verbindung mehr zu dieser Gegenstelle aufbauen, wenn Sie nicht zuvor das Volumen-Budget für diese Gegenstelle erhöhen.

Sie können auch festlegen, dass das Gerät mehrere Aktionen ausführen soll. Ist die Aktion **Verbindung trennen** darunter, führt das Gerät diese Aktion als letzte aus.

4. Klicken Sie auf **OK**, um diesen Eintrag in die Tabelle aufzunehmen, und anschließend erneut auf **OK**, um alle Einträge in die Konfiguration des Gerätes zu übernehmen.

5. Wenn die Datenübertragung bestimmter Netze das Volumen-Budget zu einer Gegenstelle nicht belastet, können Sie diese Netze aus der Erfassung herausnehmen. Klicken Sie dazu auf die Schaltfläche **Freie Netze** und anschließend auf **Hinzufügen**.

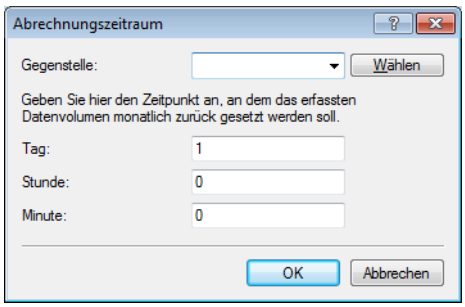


Im Feld **Gegenstelle** können Sie die Gegenstelle auswählen, für die Sie die Ausnahme angeben wollen. Mit **Wählen** können Sie aus den verfügbaren Gegenstellen auswählen bzw. neue Gegenstellen verwalten.

Sie können pro Gegenstelle auch mehrere Einträge vornehmen, indem Sie den Gegenstellennamen um das #-Zeichen und eine Ziffer erweitern (z. B. "INTERNET", "INTERNET#1", "INTERNET#2", ...). Das ist dann sinnvoll, wenn Sie explizit eine Ausnahme definieren möchten, die nur temporär aktiv ist. Sobald diese Ausnahme nicht mehr gültig ist, löschen Sie nur den Eintrag mit der entsprechend nummerierten Gegenstelle.

Im Feld **Netzwerke** können Sie IPv4- und IPv6-Adressen sowie ganze Netze in Prefix-Schreibweise (z. B. "192.168.1.0/24") angeben. Trennen Sie die einzelnen Einträge durch Komma. Auch hier können Sie die Gegenstellennamen um das #-Zeichen und eine Ziffer erweitern.

6. Klicken Sie auf **OK**, um diesen Eintrag in die Tabelle aufzunehmen, und anschließend erneut auf **OK**, um alle Einträge in die Konfiguration des Gerätes zu übernehmen.
7. Um festzulegen, wann das Gerät die monatliche Aufzeichnung von vorne beginnt, klicken Sie auf **Abrechnungszeitraum**.
8. Wenn Sie die Vorgabe ändern möchten, markieren Sie die Zeile mit der Gegenstellen-Bezeichnung "*" und klicken Sie auf die Schaltfläche **Bearbeiten**, ansonsten klicken Sie auf **Hinzufügen**.



Im Feld **Gegenstelle** können Sie die Gegenstelle auswählen, für die Sie den Intervall-Beginn festlegen wollen. Mit **Wählen** können Sie aus den verfügbaren Gegenstellen auswählen bzw. neue Gegenstellen verwalten.

Für den Gegenstellennamen können Sie auch Wildcards verwenden. Die Wildcard "*" gilt in diesem Fall für alle Gegenstellen.

In den Feldern **Tag**, **Stunde** und **Minute** bestimmen Sie, an welchem Tag im Monat und zu welcher Uhrzeit das Gerät das Budget für die angegebene Gegenstelle wieder zurücksetzt.

Standardmäßig setzt das Gerät am Monatsersten um 00:00 Uhr das Budget für alle Gegenstellen zurück.

Wenn Sie im Feld **Tag** den Wert "31" eingeben, setzt das Gerät das Budget in Monaten mit weniger Tagen (z. B. Februar oder November) nicht zurück.

9. Klicken Sie auf **OK**, um diesen Eintrag in die Tabelle aufzunehmen, und anschließend erneut auf **OK**, um alle Einträge in die Konfiguration des Gerätes zu übernehmen.
10. Klicken Sie abschließend auf **OK**, um die Konfiguration ins Gerät zu laden.

5.1.2 Ergänzungen im Setup-Menü

Budgets-Zuruecksetzen

Sie können manuell Einheiten-, Zeit- und Volumen-Budgets zurücksetzen.

Geben Sie als Parameter den Namen der WAN-Verbindung an. Mit '*' als Parameter setzen Sie alle Volumen-Budgets zurück. Wenn Sie keinen Parameter angeben, setzen Sie nur die Einheiten- bzw. Zeit-Zähler zurück.

Indem Sie das aktuelle Budget zurücksetzen, heben Sie auch eine bestehende Gebührensperre auf.

SNMP-ID:

2.3.12

Pfad Telnet:

Setup > **Gebuehren**

Aktivieren-Reserve

Einige Provider bieten die Möglichkeit, bei Erreichen des Daten- oder Zeitvolumen-Limits ein zusätzliches Budget freizuschalten. Mit dieser Aktion können Sie das Budget um ein entsprechendes Daten- bzw. Zeit-Volumen erhöhen.

Geben Sie als zusätzliche Parameter den Namen der WAN-Verbindung sowie die Höhe des Budgets in MB an. Wenn Sie kein Budget angeben, schalten Sie das für diese WAN-Verbindung angegebene Budget erneut frei.

Mit der Aktivierung eines zusätzlichen Budgets heben Sie auch eine bestehende Gebührensperre wieder auf.

SNMP-ID:

2.3.16

Pfad Telnet:

Setup > **Gebuehren**

Volumen-Budgets

Mobilfunk- oder Festnetzanbieter können je nach Vertrag auch bei Flatrates ab einem bestimmten Datenvolumen eine Drosselung der Übertragungsrate aktivieren. In diesem Verzeichnis können Sie für jede Gegenstelle ein Datenvolumen festlegen und eine Aktion definieren, die das Gerät bei Überschreiten dieses Limits ausführen soll.

SNMP-ID:

2.3.17

Pfad Telnet:

Setup > **Gebuehren**

Gegenstelle

Name der Gegenstelle, für die dieses Datenvolumen gelten soll.

SNMP-ID:

2.3.17.1

Pfad Telnet:

Setup > **Gebuehren** > **Volumen-Budgets**

Mögliche Werte:

Auswahl aus der Liste der definierten Gegenstellen

Max. 16 Zeichen

Default:

Leer

Limit-MB

Datenvolumen in Megabyte, das für die angegebene Gegenstelle gültig sein soll.

SNMP-ID:

2.3.17.2

Pfad Telnet:

Setup > **Gebuehren** > **Volumen-Budgets**

Mögliche Werte:

0 - 4.294.967.295 MByte

Max. 10 Zeichen

Besondere Werte:

0: Keine Überwachung des Datenvolumens

Default:

0

Aktion

Aktion, die das Gerät bei Überschreiten des Budgets ausführen soll. Mögliche Aktionen sind:

- **syslog**: Das Gerät erzeugt eine Syslog-Nachricht (mit dem Flag "Critical"), die Sie im Syslog-Speicher des Gerätes, über LANmonitor oder einen speziellen Syslog-Client auswerten können.
- **mail**: Das Gerät verschickt eine Benachrichtigung an die Email-Adresse, die Sie unter **Setup** > **Gebuehren** > **Gebuehren-Email** angegeben haben.
- **trennen**: Das Gerät trennt die Verbindung zur Gegenstelle.

Die Aktion **Verbindung trennen** aktiviert die Gebührensperre. Das Gerät kann bis zum Ablauf des Monats keine Verbindung mehr zu dieser Gegenstelle aufbauen, wenn Sie nicht zuvor das Volumen-Budget für diese Gegenstelle erhöhen.

Sie können auch festlegen, dass das Gerät mehrere Aktionen ausführen soll. Ist die Aktion **trennen** darunter, führt das Gerät diese Aktion als letzte aus.

SNMP-ID:

2.3.17.3

Pfad Telnet:

Setup > **Gebühren** > **Volumen-Budgets**

Mögliche Werte:

syslog

mail

trennen

Default:

leer

Freie-Netze

Wenn die Datenübertragung bestimmter Netze das Volumen-Budget zu einer Gegenstelle nicht belastet, können Sie diese Netze aus der Erfassung herausnehmen.

SNMP-ID:

2.3.18

Pfad Telnet:

Setup > **Gebuehren**

Gegenstelle

Name der Gegenstelle, für die die Ausnahme gelten soll.

Sie können pro Gegenstelle auch mehrere Einträge vornehmen, indem Sie den Gegenstellennamen um das #-Zeichen und eine Ziffer erweitern (z. B. "INTERNET", "INTERNET#1", "INTERNET#2", ...). Das ist dann sinnvoll, wenn Sie explizit eine Ausnahme definieren möchten, die nur temporär aktiv ist. Sobald diese Ausnahme nicht mehr gültig ist, löschen Sie nur den Eintrag mit der entsprechend nummerierten Gegenstelle.

SNMP-ID:

2.3.18.1

Pfad Telnet:

Setup > **Gebuehren** > **Freie-Netze**

Mögliche Werte:

Auswahl aus der Liste der definierten Gegenstellen

Max. 20 Zeichen

Default:

Leer

Freie-Netze

Über diesen Parameter definieren Sie einzelne IPv4- und IPv6-Adressen sowie ganze Netze (in Prefix-Schreibweise, z. B. "192.168.1.0/24"), die von der Budget-Erfassung befreit sind.

SNMP-ID:

2.3.18.2

Pfad Telnet:

Setup > **Gebuehren** > **Freie-Netze**

Mögliche Werte:

Gültige IPv4- und IPv6-Adresse(n), max. 100 Zeichen. Mehrere Werte trennen Sie durch eine kommaseparierte Liste.

Default:

Leer

Budget-Kontrolle

In diesem Verzeichnis legen Sie fest, wann das Gerät die monatliche Aufzeichnung von vorne beginnt.

SNMP-ID:

2.3.19

Pfad Telnet:

Setup > **Gebuehren**

Gegenstelle

Name der Gegenstelle, für die der festgelegte Zeitpunkt gelten soll.

Für den Gegenstellennamen können Sie auch Wildcards verwenden. Die Wildcard "*" gilt in diesem Fall für alle Gegenstellen.

SNMP-ID:

2.3.19.1

Pfad Telnet:

Setup > **Gebuehren** > **Budget-Kontrolle**

Mögliche Werte:

Auswahl aus der Liste der definierten Gegenstellen

Max. 16 Zeichen

Default:

Leer

Tag

Tag des Monats, an dem das Gerät das Budget zur Kontrolle des Datenvolumens wieder zurücksetzt.

SNMP-ID:

2.3.19.2

Pfad Telnet:

Setup > **Gebuehren** > **Budget-Kontrolle**

Mögliche Werte:

1 - 31

Default:

1

Stunde

Stunde, zu der das Gerät das Budget zur Kontrolle des Datenvolumens wieder zurücksetzt.

SNMP-ID:

2.3.19.3

Pfad Telnet:

Setup > **Gebuehren** > **Budget-Kontrolle**

Mögliche Werte:

0 - 23

Default:

0

Minute

Minute, zu der das Gerät das Budget zur Kontrolle des Datenvolumens wieder zurücksetzt.

SNMP-ID:

2.3.19.4

Pfad Telnet:

Setup > **Gebuehren** > **Budget-Kontrolle**

Mögliche Werte:

0 - 59

Default:

0

Gebuehren-Email

Wenn das Gerät bei Überschreiten des Datenvolumens eine Email versenden soll, geben Sie die Email-Adresse hier an.

SNMP-ID:

2.3.20

Pfad Telnet:

Setup > **Gebuehren**

Mögliche Werte:

gültige Email-Adresse mit bis zu 255 Zeichen

Default:

Leer

5.1.3 Ergänzungen im Status-Menü

Werte-loeschen

Diese Aktion löscht alle Werte der Gebühren-Statistik.

Indem Sie das aktuelle Budget zurücksetzen, heben Sie auch eine bestehende Gebührensperre auf.

Die Archiv-Tabelle für die Erfassung der Datenvolumen bleibt hiervon unberührt. Diese Tabelle löschen Sie mit der separaten Aktion **Archiv-loeschen**.

SNMP-ID:

1.24.3

Pfad Telnet:

Status > **Gebuehren**

Volumen-Budgets

In dieser Tabelle speichert das Gerät die im aktuellen Zeitintervall verbrauchten Datenmengen je Gegenstelle.

SNMP-ID:

1.24.12

Pfad Telnet:

Status > **Gebuehren**

Gegenstelle

Name der Gegenstelle

Daten-MB

Aktuell mit der Gegenstelle ausgetauschtes Datenvolumen in MByte.

Daten-KB

Aktuell mit der Gegenstelle ausgetauschtes Datenvolumen in kByte.

Limit-MB

Datenbudget für den Datenaustausch mit der Gegenstelle im aktuellen Zeitintervall.

Prozent

Prozentualer Verbrauch des Budgets zum aktuellen Zeitpunk.

Flags

Hinweis bei Überschreitung des festgelegten Limits. Folgende Werte sind möglich:

- Alarm nicht bestätigt: Dieser Hinweis zeigt an, dass der LANmonitor den Alarm noch nicht bestätigt hat.
- Limit überschritten: Das Datenbudget für diese Verbindung ist überschritten. Die Verbindung bleibt jedoch weiterhin bestehen.
- Gebührensperre: Das Datenbudget für diese Verbindung ist überschritten und die Verbindung ist bis zu Beginn des nächsten Abrechnungszeitraumes unterbrochen.

Monat

Monat des aktuellen Erfassungsintervalls.

Jahr

Jahr des aktuellen Erfassungsintervalls.

Archiv

In dieser Tabelle speichert das Gerät die in den letzten 12 Monaten gespeicherten Budgetdaten. Im 13. Monat überschreibt das Gerät automatisch die Archiv-Daten des 1. Monats.

SNMP-ID:

1.24.13

Pfad Telnet:

Status > **Gebuehren**

Gegenstelle

Name der Gegenstelle

akt-Monat

Zeigt das im aktuellen Monat übertragene Datenvolumen an.

akt-Jahr

Zeigt das im aktuellen Jahr übertragene Datenvolumen an.

akt-Limit

Zeigt das Daten-Budget des aktuellen Zeitintervalls an.

akt-Flags

Zeigt einen Hinweis an, wenn im aktuellen Erfassungszeitraum das Datenvolumen mit der Gegenstelle überschritten ist.

MB-<Monat>

Zeigt das im entsprechenden Monat erfasste Datenvolumen in MByte an.

KB-<Monat>

Zeigt das im entsprechenden Monat erfasste Datenvolumen in kByte an.

Archiv-loeschen

Diese Aktion löscht alle Einträge des Archivs.

SNMP-ID:

1.24.14

Pfad Telnet:

Status > **Gebuehren**

Aktivieren-Reserve

Einige Provider bieten die Möglichkeit, bei Erreichen des Datenvolumen-Limits ein zusätzliches Budget freizuschalten. Mit dieser Aktion können Sie das Budget um einen entsprechenden Betrag erhöhen.

Geben Sie als zusätzliche Parameter den Namen der WAN-Verbindung sowie die Höhe des Budgets in MB an. Wenn Sie kein Budget angeben, schalten Sie das für diese WAN-Verbindung angegebene Budget erneut frei.

Mit der Aktivierung eines zusätzlichen Budgets heben Sie auch eine bestehende Gebührensperre wieder auf.

SNMP-ID:

1.24.14

Pfad Telnet:

Status > **Gebuehren**

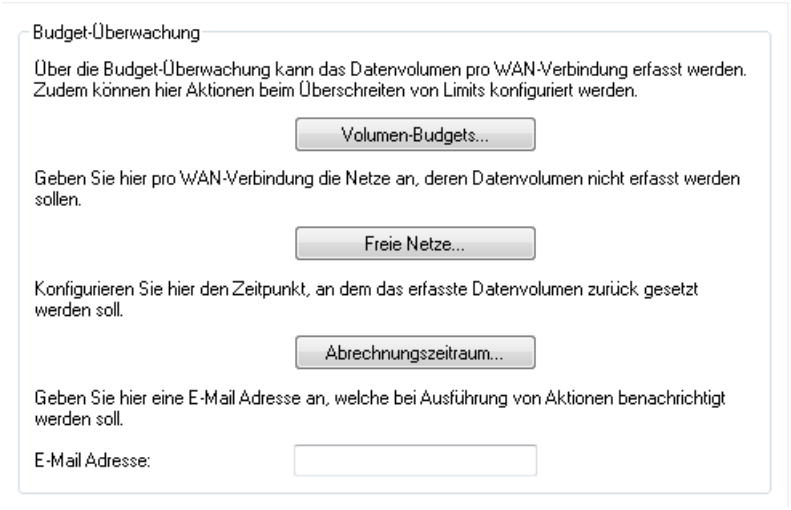
5.1.4 Ergänzungen in LANconfig

Budget-Überwachung

Mobilfunk- oder Festnetzanbieter können je nach Vertrag auch bei Flatrates ab einem bestimmten Datenvolumen eine Drosselung der Übertragungsrate aktivieren. Das Gerät erfasst das verbrauchte Datenvolumen je WAN-Schnittstelle, archiviert die Werte für bis zu 12 Monate und kann bei Erreichen eines festgelegten Grenzwertes Aktionen ausführen. Die Budgets gelten auch für VPN-, PPTP- oder alle weiteren Arten von Gegenstellen.

Beim Monatswechsel speichert das Gerät die Daten des abgelaufenen Monats in einer Archiv-Tabelle und setzt den Zähler des laufenden Monats auf Null zurück. Das aktuelle Datenvolumen sowie die im Archiv gespeicherten Daten können Sie über LANmonitor oder im Status-Menü von WEBconfig einsehen. Das Archiv beinhaltet immer Daten der letzten 12 Monate. Im 13. Monat überschreibt das Gerät automatisch die Archiv-Daten des 1. Monats.

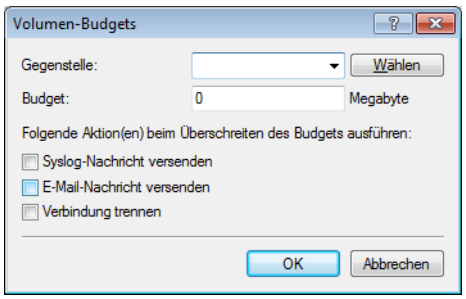
Die Budget-Überwachung können Sie unter **Managment** > **Budget** konfigurieren.



Wenn das Gerät bei Überschreiten des festgelegten Datenvolumens eine Email versenden soll, geben Sie bereits in diesem Dialog im Feld **E-Mail Adresse** die entsprechende Adresse ein.

Volumen-Budgets

Um ein Datenvolumen für die Kommunikation mit einer Gegenstelle festzulegen, klicken Sie auf die Schaltfläche **Volumen-Budgets** und anschließend auf **Hinzufügen**.



Im Feld **Gegenstelle** können Sie die Gegenstelle auswählen, für die Sie das Volumen-Budget angeben wollen. Mit **Wählen** können Sie aus den verfügbaren Gegenstellen auswählen bzw. neue Gegenstellen verwalten.

Geben Sie im Feld **Budget** das Datenvolumen an. Dieser Wert richtet sich meistens nach dem im Provider-Vertrag verhandelten Datenvolumen bis zur Drosselung der Übertragungsrate.

Sie können zusätzlich Aktionen definieren, die das Gerät bei Erreichen des Budgets ausführen soll:

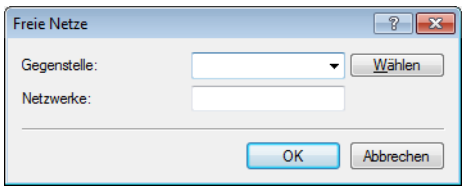
- **Syslog-Nachricht versenden**: Das Gerät erzeugt eine Syslog-Nachricht (mit dem Flag "Critical"), die Sie im Syslog-Speicher des Gerätes, über LANmonitor oder einen speziellen Syslog-Client auswerten können.
- **E-Mail-Nachricht versenden**: Das Gerät verschickt eine Benachrichtigung an die Email-Adresse, die Sie im Dialog weiter oben angegeben haben.
- **Verbindung trennen**: Das Gerät trennt die Verbindung zur Gegenstelle.

> Die Aktion **Verbindung trennen** aktiviert die Gebührensperre. Das Gerät kann bis zum Ablauf des Monats keine Verbindung mehr zu dieser Gegenstelle aufbauen, wenn Sie nicht zuvor das Volumen-Budget für diese Gegenstelle erhöhen.

Sie können auch festlegen, dass das Gerät mehrere Aktionen ausführen soll. Ist die Aktion **Verbindung trennen** darunter, führt das Gerät diese Aktion als letzte aus.

Freie Netze

Wenn die Datenübertragung bestimmter Netze das Volumen-Budget zu einer Gegenstelle nicht belastet, können Sie diese Netze aus der Erfassung herausnehmen. Klicken Sie dazu auf die Schaltfläche **Freie Netze** und anschließend auf **Hinzufügen**.



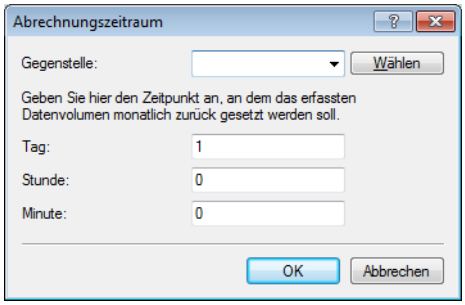
Im Feld **Gegenstelle** können Sie die Gegenstelle auswählen, für die Sie die Ausnahme angeben wollen. Mit **Wählen** können Sie aus den verfügbaren Gegenstellen auswählen bzw. neue Gegenstellen verwalten.

> Sie können pro Gegenstelle auch mehrere Einträge vornehmen, indem Sie den Gegenstellennamen um das #-Zeichen und eine Ziffer erweitern (z. B. "INTERNET", "INTERNET#1", "INTERNET#2", ...). Das ist dann sinnvoll, wenn Sie explizit eine Ausnahme definieren möchten, die nur temporär aktiv ist. Sobald diese Ausnahme nicht mehr gültig ist, löschen Sie nur den Eintrag mit der entsprechend nummerierten Gegenstelle.

Im Feld **Netzwerke** können Sie IPv4- und IPv6-Adressen sowie ganze Netze in Prefix-Schreibweise (z. B. "192.168.1.0/24") angeben. Trennen Sie die einzelnen Einträge durch Komma. Auch hier können Sie die Gegenstellennamen um das #-Zeichen und eine Ziffer erweitern.

Abrechnungszeitraum

Um festzulegen, wann das Gerät die monatliche Aufzeichnung von vorne beginnt, klicken Sie auf **Abrechnungszeitraum**.



Im Feld **Gegenstelle** geben Sie die Gegenstelle an, für die Sie den Intervall-Beginn festlegen wollen. Über die Schaltfläche **Wählen** lassen sich die verfügbaren Gegenstellen auswählen bzw. neue Gegenstellen verwalten.

Für den Gegenstellennamen lassen sich auch Wildcards verwenden. Die Wildcard "*" gilt in diesem Fall für alle Gegenstellen.

In den Feldern **Tag**, **Stunde** und **Minute** bestimmen Sie, an welchem Tag im Monat und zu welcher Uhrzeit das Gerät das Budget für die angegebene Gegenstelle wieder zurücksetzt.

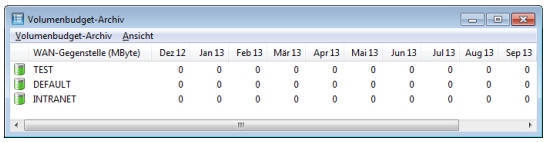
Standardmäßig setzt das Gerät am Monatsersten um 00:00 Uhr das Budget für alle Gegenstellen zurück.

Wenn Sie im Feld **Tag** den Wert "31" eingeben, setzt das Gerät das Budget in Monaten mit weniger Tagen (z. B. Februar oder November) nicht zurück.

5.1.5 Ergänzungen im LANmonitor

Volumen-Budget-Archiv anzeigen

Zeigt das Volumen-Budget-Archiv aller WAN-Schnittstellen an.

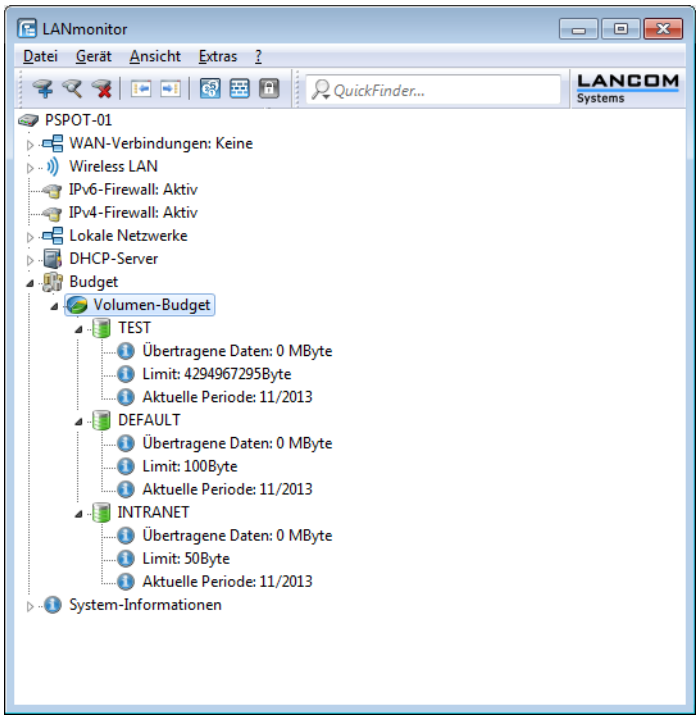


Budget-Auswertung

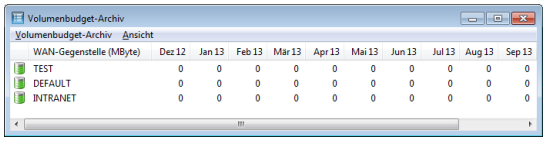
Mobilfunk- oder Festnetzanbieter können je nach Vertrag auch bei Flatrates ab einem bestimmten Datenvolumen eine Drosselung der Übertragungsrate aktivieren. Das Gerät erfasst das verbrauchte Datenvolumen je WAN-Schnittstelle, archiviert die Werte für bis zu 12 Monate und kann bei Erreichen eines festgelegten Grenzwertes Aktionen ausführen. Die Budgets gelten auch für VPN-, PPTP- oder alle weitere Arten von Gegenstellen.

Beim Monatswechsel speichert das Gerät die Daten des abgelaufenen Monats in einer Archiv-Tabelle und setzt den Zähler des laufenden Monats auf Null zurück. Das aktuelle Datenvolumen sowie die im Archiv gespeicherten Daten

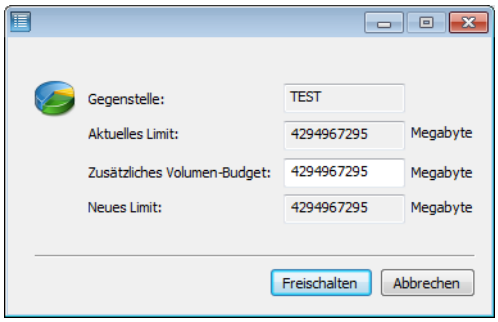
können Sie über LANmonitor oder im Status-Menü von WEBconfig einsehen. Das Archiv beinhaltet immer Daten der letzten 12 Monate. Im 13. Monat überschreibt das Gerät automatisch die Archiv-Daten des 1. Monats.



Mit einem Rechts-Klick auf **Volumen-Budget** können Sie alle angezeigten Volumen-Budgets zurücksetzen oder sich das Volumen-Budget-Archiv anzeigen lassen.



Mit einem Rechtsklick auf eine WAN-Schnittstelle können Sie das Budget für die entsprechende Schnittstelle zurücksetzen oder ein zusätzliches Volumen-Budget freischalten.



5.2 Skriptvariable für dynamische IPv6-Adressen

Ab LCOS-Version 8.84 steht Ihnen zusätzlich zur Variable %a für dynamische IPv4-Adressen die neue Variable %z für dynamische IPv6-Adressen in DynDNS- bzw. Aktions-Tabellen-Skripten zur Verfügung.

Der Gebrauch der Variablen %z erfordert die Angabe der IPv6-Adresse. Wenn Sie keine Adresse bereitstellen, führt das Gerät das Skript nicht aus.

Neu in der Aktions-Tabelle ist die Aktions-Präfix `dnscheck6:` hinzugekommen, mit der Sie eine IPv6-DNS-Namensauflösung einleiten. Sie können z. B. mit der Aktion `dnscheck6:myserver.dyndns.org` die IPv6-Adresse des angegebenen Servers ermitteln.

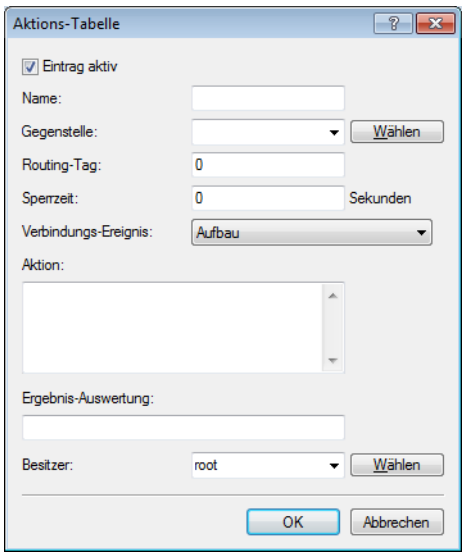
5.3 Aktionen aus der Aktionstabelle einer WAN-Verbindung zuordnen

Ab LCOS 8.84 können Sie vom LANCOM Aktionen in der Aktionstabelle über bestimmte WAN-Verbindungen ausführen lassen. Damit ist es z. B. möglich, je WAN-Verbindung einen eigenen DynDNS-Anbieter zu verwenden.

5.3.1 Konfiguration

In der Aktions-Tabelle können Sie Aktionen definieren, die das LANCOM ausführen soll, wenn sich der Zustand einer WAN-Verbindung ändert.

Im LANconfig finden Sie die Aktions-Tabelle unter **Kommunikation** > **Allgemein** > **Aktions-Tabelle**



- **Eintrag aktiv**: Aktiviert oder deaktiviert diesen Eintrag.
- **Name**: Name der Aktion. Diesen Namen können Sie mit dem Platzhalter %h (Hostname) in den Feldern **Aktion** und **Ergebnis-Auswertung** referenzieren.
- **Gegenstelle**: Name der Gegenstelle, deren Zustandswechsel die in diesem Eintrag definierte Aktion auslösen soll.
- **Routing-Tag**: Über das Routing-Tag bestimmen Sie, über welche Gegenstelle das LANCOM die Aktion ausführt. Diese Gegenstelle muss natürlich mit dem entsprechenden Routing-Tag versehen sein.
- **Sperrzeit**: Unterbricht die wiederholte Ausführung der in diesem Eintrag definierten Aktion für die eingestellte Zeit in Sekunden (max. 10 Zeichen).
- **Verbindungs-Ereignis**: Die Aktion erfolgt, wenn der hier eingestellte Zustandswechsel der WAN-Verbindung eintritt. Mögliche Werte sind:
  - Aufbau – die Aktion erfolgt, wenn das Gerät die Verbindung erfolgreich aufgebaut hat.
  - Abbau ohne Fehler – die Aktion erfolgt, wenn das Gerät die Verbindung selbst beendet (z. B. durch eine manuelle Trennung oder den Ablauf einer Haltezeit).
  - Ende (Abbau oder Abbruch) – die Aktion erfolgt, sobald die Verbindung beendet ist (unabhängig vom Grund für den Verbindungsabbau).

- Abbruch mit Fehler – die Aktion erfolgt, wenn die Verbindung beendet ist, das Gerät selbst aber diesen Abbau nicht ausgelöst oder erwartet hat.
- Aufbaufehler – die Aktion erfolgt, wenn ein Verbindungsaufbau nicht erfolgreich war.
- Volumen erreicht – die Aktion erfolgt, wenn das festgelegte Volumen erreicht ist.
- Volumen zurückgesetzt – die Aktion erfolgt, wenn ein Zustandswechsel von 'Volumen überschritten' zu 'Volumen nicht mehr überschritten' stattfindet; also z. B. Sie ein überschrittenes Volumen zurücksetzen oder das Gerät nach dem Überschreiten eine neue Abrechnungsperiode beginnt. Ist zum Zeitpunkt der Rücksetzung das Volumen noch nicht überschritten, erfolgt keine Aktion.

- **Aktion**: Hier beschreiben Sie die Aktion, die das Gerät beim Zustandswechsel der WAN-Verbindung ausführen soll. Pro Eintrag dürfen Sie nur eine Aktion angeben (max. 250 Zeichen). Für jeden der folgenden Werte ist der Doppelpunkt (:) Teil des Aktions-Wertes. Mögliche Werte sind:
  - `exec:` – Mit diesem Präfix leiten Sie alle Befehle ein, wie Sie sie auch an der Telnet-Konsole eingegeben würden. Sie können z. B. mit der Aktion `exec:do /o/m/d` alle bestehenden Verbindungen beenden.
  - `dnscheck:` – Mit diesem Präfix leiten Sie eine IPv4-DNS-Namensauflösung ein. Sie können z. B. mit der Aktion `dnscheck:myserver.dyndns.org` die IPv4-Adresse des angegebenen Servers ermitteln.
  - `dnscheck6:` – Mit diesem Präfix leiten Sie eine IPv6-DNS-Namensauflösung ein. Sie können z. B. mit der Aktion `dnscheck6:myserver.dyndns.org` die IPv6-Adresse des angegebenen Servers ermitteln.
  - `http:` – Mit diesem Präfix lösen Sie eine HTTP-Get-Anfrage aus. Sie können z. B. mit der folgenden Aktion eine DynDNS-Aktualisierung bei dyndns.org durchführen:

    ```
    http://username:password@members.dyndns.org/nic/update?
    system=dyndns&hostname=%h&myip=%a
    ```

    Die Bedeutung der Platzhalter `%h` und `%a` erfahren Sie in den folgenden Absätzen.
  - `https:` – Wie `http:`, nur über eine verschlüsselte Verbindung.
  - `gnudip:` – Mit diesem Präfix lösen Sie eine Anfrage über das GnuDIP-Protokoll an einen entsprechenden DynDNS-Server aus. Sie können z. B. mit der folgenden Aktion eine DynDNS-Aktualisierung bei einem DynDNS-Anbieter über das GnuDIP-Protokoll durchführen:
    `gnudip://gnudipsrv?method=tcp&user=myserver&domn=mydomain.org&pass=password&reqc=0&addr=%a`
    Die Bedeutung des Platzhalters `%a` erfahren Sie in den folgenden Absätzen.
  - `repeat:` – Mit diesem Präfix und der Angabe einer Zeit in Sekunden erfolgen alle Aktionen mit der Bedingung "Aufbau" wiederholt, sobald die Verbindung aufgebaut ist. Mit der Aktion `repeat:300` erfolgen z. B. alle Aufbau-Aktionen wiederholt im fünf Minuten-Rythmus.
  - `mailto:` – Mit diesem Präfix lösen Sie den Versand einer E-Mail aus. Sie können z. B. mit der folgenden Aktion eine E-Mail an den Systemadministrator versenden, sobald eine Verbindung beendet ist:
    `mailto:admin@mycompany.de?subject=VPN-Verbindung abgebrochen um %t?body=VPN-Verbindung zu Filiale 1 wurde unterbrochen`.

    Mögliche Variablen zur Erweiterung der Aktionen sind:
    - `%a` – WAN-IPv4-Adresse der WAN-Verbindung, in deren Kontext diese Aktion erfolgt.

      Der Gebrauch der Variablen `%z` erfordert die Angabe der IPv6-Adresse. Wenn Sie keine Adresse bereitstellen, führt das Gerät das Skript nicht aus.
    - `%z` – WAN-IPv6-Adresse der WAN-Verbindung, in deren Kontext diese Aktion erfolgt.
    - `%H` – Hostname der WAN-Verbindung, in deren Kontext diese Aktion erfolgt.
    - `%h` – wie %H, nur Hostname in Kleinbuchstaben.
    - `%c` – Verbindungsname der WAN-Verbindung, in deren Kontext diese Aktion erfolgt.
    - `%n` – Gerätename
    - `%s` – Seriennummer des Gerätes
    - `%m` – MAC-Adresse des Gerätes (wie im Sysinfo)
    - `%t` – Uhrzeit und Datum, im Format `YYYY-MM-DD hh:mm:ss`
    - `%e` – Bezeichnung des Fehlers, der bei einem nicht erfolgreichen Verbindungsaufbau gemeldet wurde.

    Das Ergebnis der Aktionen können Sie im Feld **Ergebnis-Auswertung** auswerten.

- **Ergebnis-Auswertung**: Das Ergebnis der Aktion können Sie hier auswerten, um je nach Ergebnis eine bestimmte Anzahl von Einträge beim Abarbeiten der Aktions-Tabelle zu überspringen. Mögliche Werte für die Aktionen sind (maximal 50 Zeichen):
  - `contains=` – Dieses Präfix prüft, ob das Ergebnis der Aktion die definierte Zeichenkette enthält.
  - `isequal=` – Dieses Präfix prüft, ob das Ergebnis der Aktion der definierten Zeichenkette genau entspricht.
  - `?skipiftrue=` – Dieses Suffix überspringt die definierte Anzahl von Zeilen in der Liste der Aktionen, wenn das Ergebnis der Abfrage mit "contains" oder "isequal" das Ergebnis WAHR liefert.
  - `?skipiffalse=` – Dieses Suffix überspringt die definierte Anzahl von Zeilen in der Liste der Aktionen, wenn das Ergebnis der Abfrage mit "contains" oder "isequal" das Ergebnis FALSCH liefert.

  Optionale Variablen für die Aktionen sind dieselben wie für die Aktion oben.

  Beispiel: Mit einem DNS-Check fragt das Gerät die IP-Adresse einer Adresse der Form "myserver.dyndns.org" ab. Mit der Prüfung `contains=%a?skipiftrue=2` können Sie die beiden folgenden Einträge der Aktions-Tabelle überspringen, wenn die mit dem DNS-Check ermittelte IP-Adresse mit der aktuellen IP-Adresse des Gerätes (%a) übereinstimmt.
- **Besitzer**: Besitzer der Aktion. Mit den Rechten dieses Besitzers werden die exec-Aktionen ausgeführt. Verfügt der Besitzer nicht über die notwendigen Rechte (z. B. Administratoren mit Leserechten), so kann das Gerät die Aktion nicht ausführen.

5.3.2 Ergänzungen im Setup-Menü

Routing-Tag

Um Aktionen in der Aktionstabelle einer bestimmten WAN-Verbindung zuzuordnen, benötigen Sie das entsprechende Routing-Tag. Das LANCOM führt die Aktion über die mit diesem Routing-Tag gekennzeichnete Verbindung aus.

SNMP-ID:

2.2.25.10

Pfad Telnet:

Setup > **WAN** > **Aktions-Tabelle**

Mögliche Werte:

Max. 5 Zeichen aus 0123456789

Default:

0

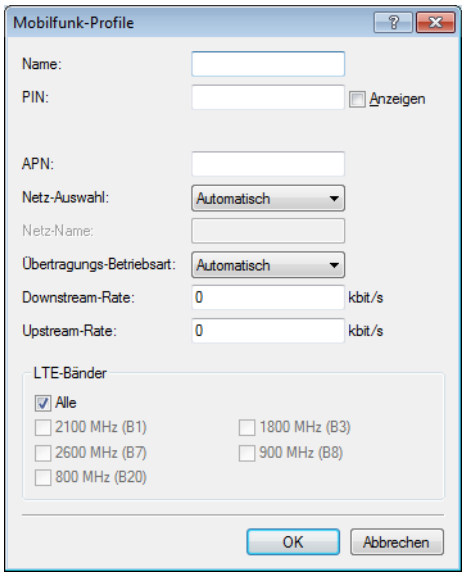
5.4 Auswahl der Frequenzbänder im LTE-Mobilfunknetz

Ab LCOS 8.84 können Sie bei einem LANCOM 4G-Router fest vorgeben, dass er bestimmte Frequenzbänder zur Datenübertragung im LTE-Mobilfunknetz nutzen soll.

5.4.1 Ergänzungen in LANconfig

Auswahl der Frequenzbänder im LTE-Mobilfunknetz

Unter **Schnittstellen** > **WAN** > **Mobilfunk-Einstellungen** können Sie in den jeweiligen Mobilfunk-Profilen festlegen, welche Frequenzbänder das LTE-Modem verwenden soll.



Wenn aufgrund ungünstiger Umgebungsbedingungen der Router ständig zwischen zwei Frequenzbändern wechselt, kann das zu Instabilitäten bei der Übertragung führen.

Mit der Auswahl im Abschnitt **LTE-Bänder** geben Sie dem Mobilfunk-Router vor, welche Frequenzbänder er verwenden darf bzw. soll. Zur Auswahl stehen die folgenden Frequenzbänder:

- **2100 MHz (B1)**: 2,1GHz-Band ist aktiviert.
- **1800 MHz (B3)**: 1,8GHz-Band ist aktiviert.
- **2600 MHz (B7)**: 2,6GHz-Band ist aktiviert.
- **900 MHz (B8)**: 900MHz-Band ist aktiviert.
- **800 MHz (B20)**: 800MHz-Band ist aktiviert.
- **Alle**: Alle Frequenzbänder sind aktiviert.

Diese Auswahl schränkt nur die Frequenzbänder bei der Übertragung im LTE-Standard ein. Für UMTS und GPRS bleiben grundsätzlich alle Bänder erlaubt.

5.4.2 Ergänzungen im Setup-Menü

LTE-Baender

Wenn aufgrund ungünstiger Umgebungsbedingungen der Router ständig zwischen zwei Frequenzbändern wechselt, kann das zu Instabilitäten bei der Übertragung führen. Mit dieser Auswahl geben Sie dem Mobilfunk-Router vor, welche Frequenzbänder er verwenden darf bzw. soll. Zur Auswahl stehen die folgenden Frequenzbänder:

- **B1_2100**: 2,1GHz-Band ist aktiviert.
- **B3_1800**: 1,8GHz-Band ist aktiviert.
- **B7_2600**: 2,6GHz-Band ist aktiviert.
- **B8_900**: 900MHz-Band ist aktiviert.
- **B20_800**: 800MHz-Band ist aktiviert.
- **Alle**: Alle Frequenzbänder sind aktiviert.

Diese Auswahl schränkt nur die Frequenzbänder bei der Übertragung im LTE-Standard ein. Für UMTS und GPRS bleiben grundsätzlich alle Bänder erlaubt.

SNMP-ID:

2.23.41.1.10

Pfad Telnet:

Setup > **Schnittstellen** > **Mobilfunk** > **Profile**

Mögliche Werte:

Alle

B1_2100

B3_1800

B7_2600

B8_900

B20_800

Default:

Alle

5.5 Datenpakete aus dem LAN via X.25 weiterleiten (ISDN)

Die im LCOS integrierte TCP-X.25-Bridge erlaubt Ihnen, Daten aus einem TCP/IP-Netzwerk via ISDN in ein X.25-Netz (und zurück) weiterzuleiten. Auf diese Weise haben Sie die Möglichkeit, eine Backup-Verbindung in ein X.25-Netz einrichten, falls über die WAN-Verbindung Störungen auftreten.

Die nachfolgenden Schritte zeigen Ihnen, wie sie die TCP-X.25-Bridge in Ihrem Gerät für ein solches Szenario konfigurieren. Dem Beispiel liegen moderne Debit-/Kreditkarten-Terminals zu Grunde, die heute in vielen Fällen ausschließlich via TCP/IP mit einem zentralen Rechner oder Netzwerk kommunizieren und in denen mindestens zwei verschiedene IP-Adressen konfigurierbar sind. Als primäre(n) IP-Adresse und Port tragen Sie in Ihrem Terminal wie gewohnt das Zielnetz oder den Zielrechner ein. Als sekundäre(n) IP-Adresse und Port hinterlegen Sie Ihr LANCOM, an welches das Terminal seine Datenpakete sendet, falls das primäre Ziel nicht erreichbar ist.

Das LANCOM seinerseits prüft anhand der im LCOS hinterlegten Einstellungen, ob die betreffenden Daten weiterzuleiten sind. Ist dies der Fall, baut das Gerät über die ISDN-Schnittstelle eine Verbindung zur konfigurierten Zieladresse auf und leitet die TCP/IP-Datenpakete über X.25 transparent weiter. Die betreffende Gegenstelle muss dazu ebenfalls über ISDN erreichbar sein und X.25 unterstützen.

Die Zahl der logischen Verbindungen über die TCP-X.25-Bridge ist gegenwärtig auf eine begrenzt. Erreicht das Gerät bei bereits bestehender Verbindung eine weitere Verbindungsanfrage an, wird diese ignoriert. Das betreffende Terminal muss in diesem Fall seine TCP-Verbindungsanfragen solange wiederholen, bis die andere X.25-Verbindung abgebaut ist.

1. Wecheln Sie auf der Konsole oder in WEBconfig in das Setup-Menü und rufen Sie die Tabelle **WAN** > **X.25-Bridge** > **Abgehende-Rufe** auf.
2. Fügen Sie anschließend einen neuen Datensatz hinzu, und ergänzen Sie die Default-Einstellungen um die nachfolgenden Basis-Angaben. Weitere Informationen zu den Parametern entnehmen Sie bitte der CLI- bzw. Menüreferenz.
   - **Name**
   - **Terminal-Port**

- **Lokaler-Port**
- **ISDN-Remote**
- **ISDN-Lokal**
- **X.25-Remote**
- **X.25-Lokal**

Die Angabe einer **Terminal-IP** und **Loopback-Adresse** ist optional, bei Konfigurationen mit mehreren lokalen Netzen aber dringend empfehlenswert.

Für Verbindungen zu einigen Anbietern (z. B. **TeleCash**) ist darüber hinaus die Angabe der **Protokoll-ID** und die **Userdata** erforderlich.

Fertig! Damit ist die Basiskonfiguration der TCP-X.25-Bridge abgeschlossen.

5.5.1 Ergänzungen im Status-Menü

X.25-Bridge

Dieser Menüpunkt enhält die Status-Werte für die TCP-X.25-Bridge.

SNMP-ID:

1.4.45

Pfad Telnet:

Status > **WAN**

Verbindungen

Diese Tabelle zeigt die Liste aller aktiven Verbindungen über die TCP-X.25-Bridge. Aufgelistet sind die aktuellen Zustände der zu einer Verbindung gehörenden TCP-, ISDN- und X.25-Bestandteile sowie deren Verbindungsparameter.

SNMP-ID:

1.4.45.2

Pfad Telnet:

Status > **WAN** > **X.25-Bridge**

Index

Nummer des Tabelleneintrags

SNMP-ID:

1.4.45.2.1

Pfad Telnet:

Status > **WAN** > **X.25-Bridge** > **Verbindungen**

Richtung

Zeigt die Richtung an, aus der die Verbindung über die TCP-X.25-Bridge aufgebaut ist.

SNMP-ID:

1.4.45.2.2

Pfad Telnet:

Status > **WAN** > **X.25-Bridge** > **Verbindungen**

Mögliche Werte:

Ausgehend
Abgehende Verbindung

TCP-Zustand

Zeigt den Zustand der TCP-Verbindung von Ihrem Gerät zu einer LAN-Gegenstelle (z. B. einem Terminal) an.

SNMP-ID:

1.4.45.2.3

Pfad Telnet:

Status > **WAN** > **X.25-Bridge** > **Verbindungen**

Mögliche Werte:

Aufbauen
Verbunden
Abbauen
Nicht-Verbunden

ISDN-Zustand

Zeigt den Zustand der ISDN-Verbindung von Ihrem Gerät zur X.25-Gegenstelle (bzw. deren ISDN-Dienst) an.

SNMP-ID:

1.4.45.2.4

Pfad Telnet:

Status > **WAN** > **X.25-Bridge** > **Verbindungen**

Mögliche Werte:

Aufbauen
Verbunden
Abbauen
Nicht-Verbunden

X.25-Zustand

Zeigt den Zustand der X.25-Verbindung von Ihrem Gerät zur X.25-Gegenstelle an.

SNMP-ID:

1.4.45.2.5

Pfad Telnet:

Status > **WAN** > **X.25-Bridge** > **Verbindungen**

Mögliche Werte:

Aufbauen
Verbunden
Abbauen
Nicht-Verbunden

Terminal-IP

Zeigt die IP-Adresse der LAN-Gegenstelle (z. B. eines Terminals) an.

SNMP-ID:

1.4.45.2.6

Pfad Telnet:

Status > **WAN** > **X.25-Bridge** > **Verbindungen**

Terminal-Port

Zeigt den Port der LAN-Gegenstelle (z. B. eines Terminals) an, über den die TCP-Verbindung besteht.

SNMP-ID:

1.4.45.2.7

Pfad Telnet:

Status > **WAN** > **X.25-Bridge** > **Verbindungen**

Lokale-IP

Zeigt die IP-Adresse Ihres Gerätes im LAN, unter der Ihr Gerät Datenpakete über die TCP-X.25-Bridge annimmt und verschickt.

SNMP-ID:

1.4.45.2.8

Pfad Telnet:

Status > **WAN** > **X.25-Bridge** > **Verbindungen**

Lokaler-Port

Zeigt den Port Ihres Gerätes an, über den die TCP-Verbindung zur LAN-Gegenstelle besteht.

SNMP-ID:

1.4.45.2.9

Pfad Telnet:

Status > **WAN** > **X.25-Bridge** > **Verbindungen**

Routing-Tag

Zeigt das Quell-Tag (erwartetes Schnittstellen- bzw. Routing-Tag) des ARF-Kontextes der betreffenden Verbindung..

SNMP-ID:

1.4.45.2.10

Pfad Telnet:

Status > **WAN** > **X.25-Bridge** > **Verbindungen**

ISDN-Remote

Zeigt die ISDN-Rufnummer der X.25-Gegenstelle (bzw. deren ISDN-Dienst) an.

SNMP-ID:

1.4.45.2.11

Pfad Telnet:

Status > **WAN** > **X.25-Bridge** > **Verbindungen**

ISDN-Lokal

Zeigt die ISDN-Rufnummer Ihres Gerätes an.

SNMP-ID:

1.4.45.2.12

Pfad Telnet:

Status > **WAN** > **X.25-Bridge** > **Verbindungen**

X.25-Remote

Zeigt die X.25-Adresse der X.25-Gegenstelle an.

SNMP-ID:

1.4.45.2.13

Pfad Telnet:

Status > **WAN** > **X.25-Bridge** > **Verbindungen**

X.25-Lokal

Zeigt die X.25-Adresse Ihres Gerätes an.

SNMP-ID:

1.4.45.2.14

Pfad Telnet:

Status > **WAN** > **X.25-Bridge** > **Verbindungen**

Protokoll-ID

Zeigt die für diese Verbindung konfigurierte X.25-Protokollnummer an. Bei abgehenden Verbindungen entspricht dies der im LCOS hinterlegten Protokollnummer.

SNMP-ID:

1.4.45.2.15

Pfad Telnet:

Status > **WAN** > **X.25-Bridge** > **Verbindungen**

Userdata

Zeigt die für diese Verbindung übermittelten X.25-Userdaten an. Bei abgehenden Verbindungen entspricht dies den im LCOS hinterlegten Userdaten.

SNMP-ID:

1.4.45.2.16

Pfad Telnet:

Status > **WAN** > **X.25-Bridge** > **Verbindungen**

Payload-Groesse

Zeigt die für diese Verbindung ausgehandelte Größe des X.25-Payloads an.

Das Gerät übermittelt beim Verbindungsaufbau zunächst die im LCOS konfigurierte Größe. Die Gegenstelle kann den Wert ändern. Nimmt Sie eine Änderung vor, zeigt der Status-Wert den geänderten Payload an, andernfalls den im LCOS konfigurierten.

Der X.25-Standard erlaubt die Festlegung unterschiedlicher Größen für gesendete und empfangene Pakete. Der Status-Wert zeigt ausschließlich die Größe der vom Gerät verschickten Pakete.

SNMP-ID:

1.4.45.2.17

Pfad Telnet:

Status > **WAN** > **X.25-Bridge** > **Verbindungen**

TCP-Ports

Diese Tabelle zeigt die Liste sämtlicher lokalen Ports, die Ihr Gerät auf eingehende TCP-Verbindungen für die TCP-X.25-Bridge prüft (TCP-Listener). Existiert für einen Port ein gültige Konfigurationszeile in der Tabelle *2.2.45.2 Abgehende-Rufe* auf Seite 47, akzeptiert das Gerät die TCP-Verbindung; andernfalls lehnt es die Verbindungsanfrage über die TCP-X.25-Bridge ab.

SNMP-ID:

1.4.45.3

Pfad Telnet:

Status > **WAN** > **X.25-Bridge**

Lokaler-Port

Nummers des Ports, den Ihr Gerät auf eingehende TCP-Verbindungen für die TCP-X.25-Bridge prüft (TCP-Listener).

SNMP-ID:

1.4.45.3.1

Pfad Telnet:

Status > **WAN** > **X.25-Bridge** > **TCP-Ports**

Verbindungen-trennen

Mit dieser Aktion veranlassen Sie den sofortigen Abbau der X.25-Verbindung und die Schließung des dafür verwendeten ISDN-Kanals.

SNMP-ID:

1.4.45.4

Pfad Telnet:

Status > **WAN** > **X.25-Bridge**

Mögliche Argumente:

keine

5.5.2 Ergänzungen im Setup-Menü

X.25-Bridge

Dieser Menüpunkt enhält die Einstellungen für die TCP-X.25-Bridge.

SNMP-ID:

2.2.45

Pfad Telnet:

Setup > **WAN**

Abgehende-Rufe

Diese Tabelle einhält die Einstellungen für die eingehenden TCP-Verbindungen (der LAN-Gegenstelle) und abgehenden X.25-Verbindungen (zur X.25-Gegenstelle).

SNMP-ID:

2.2.45.2

Pfad Telnet:

Setup > **WAN** > **X.25-Bridge**

Name

Geben Sie einen Namen für den Tabelleneintrag bzw. die zu konfigurierende X.25-Verbindung an.

SNMP-ID:

2.2.45.2.1

Pfad Telnet:

Setup > **WAN** > **X.25-Bridge** > **Abgehende-Rufe**

Mögliche Werte:

max. 16 Zeichen aus `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default-Wert:

DEFAULT

Prio

Geben Sie die Priorität der gewählten X.25-Verbindung an. Je kleiner der Wert, desto höher die Priorität..

LCOS sortiert die angezeigten Tabelleneinträge gemäß der gesetzten Prioritäten in absteigender Reihenfolge.

SNMP-ID:

2.2.45.2.2

Pfad Telnet:

Setup > **WAN** > **X.25-Bridge** > **Abgehende-Rufe**

Mögliche Werte:

0 … 65535

Default-Wert:

0

Terminal-IP

Geben Sie die IPv4-Adresse der Gegenstelle in Ihrem LAN an, welche Datenpakete über die gewählte X.25-Verbindung senden darf.

SNMP-ID:

2.2.45.2.3

Pfad Telnet:

Setup > **WAN** > **X.25-Bridge** > **Abgehende-Rufe**

Mögliche Werte:

max. 39 Zeichen aus `[0-9][A-F][a-f]:.`

Besondere Werte:

0.0.0.0

Die TCP-X.25-Bridge ist für sämtliche Gegenstellen in Ihrem LAN benutzbar und auch für Gegenstellen aus dem WAN offen.

Default-Wert:

0.0.0.0

Terminal-Port

Geben Sie den Port der Gegenstelle in Ihrem LAN an, über den die Gegenstelle die Datenpakete senden darf.

SNMP-ID:

2.2.45.2.4

Pfad Telnet:

Setup > **WAN** > **X.25-Bridge** > **Abgehende-Rufe**

Mögliche Werte:

0 … 65535

Besondere Werte:

0

Die TCP-X.25-Bridge erlaubt Verbindungen über einen beliebigen Port.

Default-Wert:

0

Loopback-Adresse

Geben Sie die IPv4-Adresse an, in deren ARF-Kontext Ihr Gerät vom Terminal kommende Verbindungen annimmt. Die Loopback-Adresse ersetzt hierbei die beiden Angaben IP-Adresse/Routing-Tag. Das Gerät wählt das Routing-Tag und seine lokale Adresse anhand der Loopback-Adresse. Ist die Loopback-Adresse leer, nimmt das Gerät Verbindungen auf jeder Adresse (auch dem WAN!) an.

SNMP-ID:

2.2.45.2.5

Pfad Telnet:

Setup > **WAN** > **X.25-Bridge** > **Abgehende-Rufe**

Mögliche Werte:

max. 16 Zeichen aus `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default-Wert:

leer

Lokaler-Port

Geben Sie den TCP-Port an, über den Ihr Gerät eine Verbindung zur X.25-Gegenstelle aufbaut.

SNMP-ID:

2.2.45.2.6

Pfad Telnet:

Setup > **WAN** > **X.25-Bridge** > **Abgehende-Rufe**

Mögliche Werte:

1 … 65535

Default-Wert:

1998

ISDN-Remote

Geben Sie die ISDN-Rufnummer der X.25-Gegenstelle ein.

SNMP-ID:

2.2.45.2.7

Pfad Telnet:

Setup > **WAN** > **X.25-Bridge** > **Abgehende-Rufe**

Mögliche Werte:

max. 21 Zeichen `[0-9]`

Default-Wert:

0

ISDN-Lokal

Geben Sie die ISDN-Rufnummer an, die Ihr Gerät als abgehende Nummer einsetzt.

SNMP-ID:

2.2.45.2.8

Pfad Telnet:

Setup > **WAN** > **X.25-Bridge** > **Abgehende-Rufe**

Mögliche Werte:

max. 21 Zeichen `[0-9]`

Default-Wert:

leer

X.25-Remote

Geben Sie die X.25-Adresse der X.25-Gegenstelle an.

SNMP-ID:

2.2.45.2.9

Pfad Telnet:

Setup > **WAN** > **X.25-Bridge** > **Abgehende-Rufe**

Mögliche Werte:

max. 14 Zeichen `[0-9]`

Default-Wert:

leer

X.25-Lokal

Geben Sie die X.25-Adresse Ihres Gerätes an.

SNMP-ID:

2.2.45.2.10

Pfad Telnet:

Setup > **WAN** > **X.25-Bridge** > **Abgehende-Rufe**

Mögliche Werte:

max. 14 Zeichen `[0-9]`

Default-Wert:

leer

Protokoll-ID

Geben Sie die X.25-Protokollnummer ein. Ihr Gerät setzt diese ID als Bytes 0 bis 3 in die X.25-*Userdata* ein.

SNMP-ID:

2.2.45.2.11

Pfad Telnet:

Setup > **WAN** > **X.25-Bridge** > **Abgehende-Rufe**

Mögliche Werte:

max. 8 Zeichen `[0-9][a-f]`

Default-Wert:

00000000

Userdata

Hinterlegen Sie in den X.25-Paketdaten weitere Zusatzinformationen, die Ihr Gerät an die X.25-Gegenstelle übermittelt.

SNMP-ID:

2.2.45.2.12

Pfad Telnet:

Setup > **WAN** > **X.25-Bridge** > **Abgehende-Rufe**

Mögliche Werte:

max. 8 Zeichen `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`#`

Default-Wert:

leer

Payload-Groesse

Geben Sie die Größe des X.25-Payloads an. Zulässige Werte sind reine Zweierpotenzen von 16 bis 1024.

Der X.25-Standard erlaubt die Festlegung unterschiedlicher Größen für gesendete und empfangene Pakete. Die Konfiguration bezieht sich auf beide Richtungen.

SNMP-ID:

2.2.45.2.13

Pfad Telnet:

Setup > **WAN** > **X.25-Bridge** > **Abgehende-Rufe**

Mögliche Werte:

16 … 1024 Byte

Default-Wert:

128

Daten-Trace

Über diesen Parameter aktivieren bzw. deaktivieren Sie den Trace der Datenpakete, welche die X.25-Bridge passieren. Die Ausgabe des Traces erfolgt auf der Konsole, auf der Sie den Trace aktiviert haben.

SNMP-ID:

2.2.45.5

Pfad Telnet:

Setup > **WAN** > **X.25-Bridge**

Mögliche Werte:

Aus

Das Gerät gibt keine Trace-Daten aus.

Ein

Das Gerät gibt Trace-Daten mit der Richtung der Übertragung und der Anzahl der Datenbytes aus. Beispiel für einen Daten-Trace:

```
[X.25-Bridge] 2014/01/15 13:55:39,331
Receiving 256 bytes of data from X.25.
```

Erweitert

Identisch mit **Ein**; das Gerät gibt die Daten jedoch zusätzlich als Dump aus. Beispiel für einen Daten-Trace mit zusätzlichem Dump (verkürzt):

```
[X.25-Bridge] 2014/01/15 13:55:39,331
Receiving 256 bytes of data from X.25.

Adr:= 04394380
Len:= 00000100
00000000:  C2 79 .. 46 60  50 8C .. E3 B7 | .6y..GF` P.......
00000010:  2D AE .. 24 5D  E9 B6 .. 40 59 | -.0..U$] ..l..g@Y
00000030:  A5 36 .. 3C 6B  01 21 .. 9D 14 | .6.M..<k .!H..u..
00000040:  94 38 .. 89 AA  54 22 .. 81 F7 | .8..2m.. T".=....
00000050:  E0 7C .. F3 28  B6 E8 .. 74 2F | .|.....( ..a]b.t/
[...]
```

Default-Wert:

Aus

Disconnect-Verzoegerung

Über diesen Parameter definieren Sie die Zeit, die das Gerät nach Abbau einer X.25-Verbindung wartet, bevor es die ISDN-Verbindung abbaut. Innerhalb dieser Zeit sind weitere X.25-Verbindungen ohne den kompletten Neuaufbau der ISDN-Verbindung herstellbar.

SNMP-ID:

2.2.45.4

Pfad Telnet:

Setup > **WAN** > **X.25-Bridge**

Mögliche Werte:

0 … 99 Sekunden

Besondere Werte:

0

Dieser Wert deaktiviert die Wartezeit. Das Gerät baut ISDN-Verbindungen zusammen mit der X.25-Verbindung ab.

Default-Wert:

5

5.6 HNAT-Tracing

Ab LCOS 8.84 steht Ihnen ein neuer trace-Befehle zur Fehlersuche auf Geräten mit Hardware-NAT (HNAT) zur Verfügung:

Tabelle 1: Übersicht aller durchführbaren Traces

Dieser Parameter ...	... ruft beim Trace die folgende Anzeige hervor:
hnat	Informationen zum Hardware-NAT

Die aktuellen Statusinformationen zum HNAT lassen sich mit dem Befehl `show eth hnat` anzeigen.

6 IPv6

6.1 IPv6-Präfix-Delegation vom WWAN ins LAN

Ab LCOS 8.84 kann der WWAN-Router ein IPv6-/64-Präfix per DHCPv6 oder Router-Advertising im LAN ankündigen.

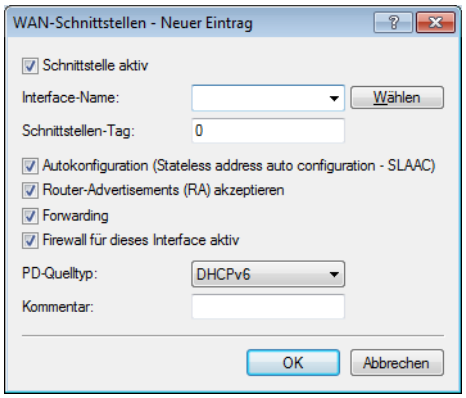
6.1.1 Ergänzungen in LANconfig

IPv6-Präfix-Delegation vom WWAN ins LAN

In Mobilfunknetzwerken mit IPv6-Unterstützung ist erst ab 3GPP-Release 10 eine Unterstützung von DHCPv6-Präfix-Delegation vorgesehen. Damit ist es in Mobilfunknetzen vor Release 10 nur möglich, einem Endgerät genau ein /64-Präfix z. B. durch Router-Advertisements zuzuweisen. Bei Smartphones oder Laptops lässt sich mit dieser Methode einfach eine IPv6-Unterstützung realisieren. Router benötigen bei IPv6 aber mindestens ein weiteres Präfix, das sie an Clients ins LAN propagieren können.

Die IPv6-Präfix-Delegation vom WWAN ins LAN macht es möglich, dass Clients das auf der WAN-Mobilfunkseite zugewiesene /64-Präfix im LAN verwenden können. Damit ist ein Betrieb eines Routers in IPv6-Mobilfunknetzwerk ohne DHCPv6-Präfix-Delegation und Neighbor Discovery Proxy (ND-Proxy) möglich. Der Router kündigt das bezogene /64-Präfix per Router-Advertisement im LAN an, statt es auf dem WAN-Interface hinzuzufügen. Clients können dann aus diesem Präfix eine Adresse generieren und diese für die IPv6-Kommunikation benutzen.

Sie konfigurieren dazu den IPv6-Internetzugang genau wie einen normaler Internetzugang. Sie müssen dazu lediglich unter **IPv6** > **Allgemein** > **IPv6-Schnittstellen** > **WAN-Schnittstelle** den Parameter **PD-Quelltyp** des entsprechenden WAN-Interfaces von 'DHCPv6" auf "Router-Advertisement" setzen.



Es gelten folgende Einschränkungen:

- Sie können das Feature nur auf Punkt-zu-Punkt-Verbindungen (z. B. PPP) nutzen, wobei die Gegenstelle automatisch allen Datenverkehr an den Router sendet, da kein ND-Proxy vorhanden ist.
- Sie können nur genau ein IPv6-Netz im LAN anlegen, da nur ein /64-Präfix zur Verfügung steht.
- Das Feature ist nicht geeignet für Szenarien, in denen ein vorgeschalteter Router keine Präfix-Delegierung beherrscht oder durchführt, ausgenommen Punkt-zu-Punkt-Verbindungen.
- Die automatisch erzeugte IPv6-Adresse auf dem WAN-Interface ist von Clients aus dem LAN nicht zu erreichen, da kein ND-Proxy vorhanden ist.

6.1.2 Ergänzungen im Setup-Menü

PD-Modus

In Mobilfunknetzwerken mit IPv6-Unterstützung ist erst ab 3GPP-Release 10 eine Unterstützung von DHCPv6-Präfix-Delegation vorgesehen. Damit ist es in Mobilfunknetzen vor Release 10 nur möglich, einem Endgerät genau ein /64-Präfix z. B. durch Router-Advertisements zuzuweisen. Bei Smartphones oder Laptops lässt sich mit dieser Methode einfach eine IPv6-Unterstützung realisieren. Router benötigen bei IPv6 aber mindestens ein weiteres Präfix, das sie an Clients ins LAN propagieren können.

Die IPv6-Präfix-Delegation vom WWAN ins LAN macht es möglich, dass Clients das auf der WAN-Mobilfunkseite zugewiesene /64-Präfix im LAN verwenden können. Damit ist ein Betrieb eines Routers in IPv6-Mobilfunknetzwerk ohne DHCPv6-Präfix-Delegation und Neighbor Discovery Proxy (ND-Proxy) möglich. Der Router kündigt das bezogene /64-Präfix per Router-Advertisement im LAN an, statt es auf dem WAN-Interface hinzuzufügen. Clients können dann aus diesem Präfix eine Adresse generieren und diese für die IPv6-Kommunikation benutzen.

Mit dieser Option legen Sie fest, wie der Router die Präfix-Delegation durchführt:

- DHCPv6: Die Präfix-Delegation erfolgt über DHCPv6
- Router-Advertisement: Die Präfix-Delegation erfolgt über Router-Advertisement, der DHCPv6-Client startet dabei nicht.

Pfad Telnet:

Setup > **IPv6** > **WAN-Interfaces**

Mögliche Werte:

DHCPv6

Router-Advertisement

Default:

DHCPv6

7 Zertifikatsverwaltung

7.1 Verwendung interner LCOS-Variablen im SCEP-Client

Ab LCOS Version 8.84 ist beim SCEP-Client auch die Verwendung der folgenden internen LCOS-Variablen möglich:

- %% fügt ein Prozentzeichen ein.
- %f fügt die Version und das Datum der aktuellen im Gerät aktiven Firmware ein.
- %r fügt die Hardware-Release des Gerätes ein.
- %v fügt die Version des aktuellen im Gerät aktiven Loaders ein.
- %m fügt die MAC-Adresse des Gerätes ein.
- %s fügt die Seriennummer des Gerätes ein.
- %n fügt den Namen des Gerätes ein.
- %l fügt den Standort des Gerätes ein.
- %d fügt den Typ des Gerätes ein.

8 WLAN

8.1 LANCOM Active Radio Control (ARC)

Mit dem intelligenten WLAN-Optimierungskonzept **LANCOM Active Radio Control (ARC)** optimieren Sie nachhaltig Ihr Funkfeld und vermeiden proaktiv Störquellen im WLAN. Active Radio Control besteht aus mehreren, sich ideal ergänzenden Funktionen im LANCOM Betriebssystem LCOS, mithilfe dessen Sie die Leistungsfähigkeit Ihres WLANs deutlich verbessern. Alle Funktionen von Active Radio Control sind kostenlos enthalten im LANCOM Betriebssystem LCOS und lassen sich einfach über die entsprechenden Management-Tools bedienen.

RF Optimization (Funkfeldoptimierung)

Automatische Auswahl optimaler WLAN-Kanäle: WLAN-Clients profitieren von einem verbesserten Durchsatz dank reduzierter Kanalüberlappungen. In Controller basierten WLAN-Installationen erfolgt eine automatische Auswahl optimaler Kanäle für verwaltete Access Points.

Mehr Informationen zu RF Optimization finden Sie im entsprechenden Abschnitt des Referenzhandbuchs.

Band Steering

Nutzen Sie die Bandbreite Ihres WLANs optimal aus: Der automatische, vom Access Point gesteuerte Wechsel von Clients in das 5-GHz-Frequenzband verdoppelt die WLAN-Performance, weil meist nur dort genügend Kanäle für eine Kanalbündelung zur Verfügung stehen.

Mehr Informationen zum Band Steering finden Sie im entsprechenden Abschnitt des Referenzhandbuchs.

Adaptive Noise Immunity

Besserer WLAN-Durchsatz durch Immunität vor Störsignalen: WLAN-Clients profitieren von deutlich mehr Datendurchsatz dank einer ungestörten Funkabdeckung. Durch aktivierte Adaptive Noise Immunity blendet ein Access Point Störquellen im Funkfeld aus und fokussiert sich ausschließlich auf WLAN-Clients mit ausreichender Signalstärke.

Mehr Informationen zur Adaptive Noise Immunity finden Sie *im entsprechenden Abschnitt* des Referenzhandbuchs.

Spectral Scan

Überprüfen Sie Ihr WLAN-Funkspektrum auf Störquellen: Mit LANCOM Spectral Scan haben Sie ein professionelles Werkzeug für ein effizientes WLAN-Troubleshooting. Ein Scan des gesamten Funkspektrums identifiziert Störquellen außerhalb des WLANs und ermöglicht eine grafische Darstellung.

Mehr Informationen zum Spectral Scan finden Sie im entsprechenden Abschnitt des Referenzhandbuchs.

8.2 Maximaler EIRP-Wert abhängig vom Übertragungsstandard

Um die Sendeleistungsdichte im 802.11b-Übertragungsstandard nicht zu überschreiten, ist ein EIRP-Wert von maximal 18dBm möglich. Im Übertragungsstandard 802.11gn kann der EIRP-Wert maximal 20dBm betragen. Ab LCOS 8.84 richtet sich der maximale EIRP-Wert eines WLAN-fähigen LANCOM-Gerätes automatisch nach dem verwendeten Übertragungsstandard.

8.3 Maximale Übertragungsrate für Multi- und Broadcasts anpassen

Ab LCOS 8.84 kann das LANCOM die Übertragungsrate für Broad- und Multicast-Sendungen automatisch am Access Point mit der geringsten Übertragungsrate ausrichten.

8.3.1 Automatische Anpassung der Übertragungsrate für Multicast- und Broadcast-Sendungen

Während bei Unicast-Sendungen Access Point und Client die optimale Übertragungsgeschwindigkeit miteinander aushandeln können, findet systembedingt bei Multicast- und Broadcast-Sendungen die Kommunikation nur in eine Richtung statt: Vom Access Point zum Client. Die Clients können dem Access Point nicht zurückmelden, mit welcher maximalen Übertragungsgeschwindigkeit sie tatsächlich kommunizieren können.

Der Access Point hat zwei Möglichkeiten, die Übertragungsgeschwindigkeit für Multicast- und Broadcast-Sendungen festzulegen:

- **Feste Bitrate**: Die Übertragungsrate ist so bemessen, dass der langsamste Client im WLAN auch unter ungünstigen Bedingungen die Sendungen fehlerfrei und verständlich erhalten kann. Das kann dazu führen, dass das LANCOM selbst dann mit einer geringeren Übertragungsrate sendet, wenn Umgebungsbedingungen und Clients eigentlich eine höhere Rate erlauben würden. Doch damit würde der Access Point das WLAN unnötig ausbremsen.
- **Automatische Bitrate**: Bei automatischer Festlegung der Übertragungsrate sammelt der Access Point die Informationen über die Übertragungsraten der einzelnen WLAN-Clients. Die Rate teilen die Clients dem Access Point automatisch bei jeder Unicast-Kommunikation mit. Aus der Liste der angemeldeten Clients wählt der Access Point nun ständig die jeweils niedrigste Übertragungsrate aus und überträgt damit die Multicast- und Broadcast-Sendungen.

8.3.2 Ergänzungen im Setup-Menü

Basis-Rate

Die Basis-Rate ist die Übertragungsrate, mit der das LANCOM alle Multicast- und Broadcast-Pakete versendet.

Die hier eingestellte Geschwindigkeit sollte es auch unter ungünstigen Bedingungen erlauben, die langsamsten Clients im WLAN zu erreichen. Stellen Sie hier nur dann eine höhere Geschwindigkeit ein, wenn alle Clients in diesem logischen WLAN auch mit dieser Geschwindigkeit zu erreichen sind.

Wenn Sie hier "Auto" auswählen, richtet sich das Gerät automatisch nach der Übertragungsrate des langsamsten WLAN-Clients im Netzwerk.

SNMP-ID:

2.23.20.2.4

Pfad Telnet:

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

Mögliche Werte:

Auto

Auswahl aus den angebotenen Geschwindigkeiten von 1Mbit/s - 54Mbit/s

Default:

2Mbit/s

8.3.3 Ergänzungen im Status-Menü

Netzwerke

Zeigt Informationen zu den WLAN-Schnittstellen des Gerätes.

SNMP-ID:

1.3.56

Pfad Telnet:

Status > **WLAN**

Ifc

Name des Interfaces

Aktiv

Zeigt an, ob das Interface aktiviert ist.

Netzwerkname

Zeigt den Namen des Netzwerks an (SSID)

BSSID

MAC-Adresse des Access Points für dieses WLAN

Radio-Modus

Zeigt an, welche Übertragungsstandards der Access Point benutzt.

VLAN-Id

Zeigt die VLAN-ID des Interfaces an.

Anzahl Stationen

Gibt an, wieviele Stationen aktuell am Access Point angemeldet sind.

MCast-Pwr-Save

Zeigt an, ob der Power-Save-Modus aktiviert ist.

APSD

Zeigt an, ob APSD im jeweiligen WLAN (SSID) aktiv ist. APSD wird hier nur als aktiv angezeigt, wenn sowohl APSD in den Einstellungen des logischen WLANs als auch das globale QoS-Modul aktiviert sind.

Alarm-Status

Zeigt den Alarm-Status der Schnittstelle an.

Basis-Rate

Gibt die Übertragungsrate für Multicast- und Broadcast-Sendungen an.

MAC-Filter

Gibt an, ob der MAC-Filter aktiviert ist.

Zugriffsmodus

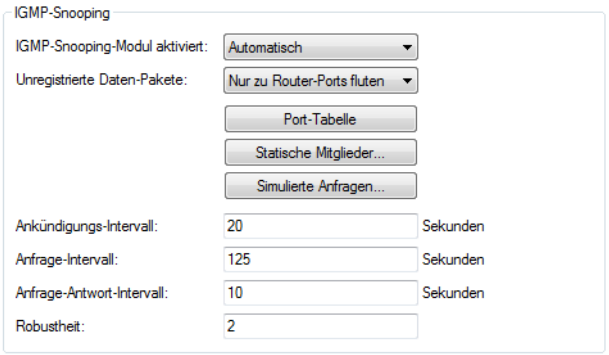
Gibt an, ob der Access Point die in der Zugriffsliste aufgeführten Stationen gesperrt oder freigeschaltet sind.

8.4 IGMP-Snooping mit Auto-Modus

Ab LCOS-Version 8.84 kann die Bridge automatisch erkennen, ob sich mindestens ein Querier im Netzwerk befindet. Nur dann lernt sie die Mitgliedschaften für Multicast-Gruppen und leitet die entsprechenden Multicasts weiter.

8.4.1 Allgemeine Einstellungen

Die Konfiguration des IGMP-Snooping finden Sie im LANconfig unter **Schnittstellen** > **IGMP-Snooping**



IGMP-Snooping-Modul aktiviert

Aktiviert oder deaktiviert IGMP Snooping für das Gerät und alle definierten Querier-Instanzen. Ohne IGMP-Snooping verhält sich die Bridge wie ein einfacher Switch und sendet alle Multicasts auf alle Ports weiter.

Mögliche Werte:

- Ja
- Nein
- Automatisch

Default:

- Automatisch

In der Einstellung **Automatisch** aktiviert die Bridge das IGMP-Snooping nur, wenn auch Querier im Netz vorhanden sind.

Wenn diese Funktion deaktiviert ist, sendet die Bridge alle IP-Multicast-Pakete über alle Ports. Bei einer Änderung des Betriebszustandes setzt die Bridge die IGMP-Snooping-Funktion vollständig zurück, d. h. sie löscht alle dynamisch gelernten Werte (Mitgliedschaften, Router-Port-Eigenschaften).

Unregistrierte Datenpakete

Diese Option definiert die Verarbeitung von Multicast-Paketen mit Ziel-Adressen außerhalb des reservierten Adress-Bereiches `224.0.0.x`, für die weder dynamisch gelernte noch statisch konfigurierte Mitgliedschaften vorhanden sind.

Mögliche Werte:

- Nur zu Router-Ports fluten: Sendet diese Pakete an alle Router-Ports.
- Zu allen Ports fluten: Sendet diese Pakete an alle Ports.
- Verwerfen: Verwirft diese Pakete.

Default:

- Nur-Router-Ports

Ankündigungs-Intervall

Das Intervall in Sekunden, in dem die Geräte Pakete aussenden, mit denen sie sich als Multicast-fähige Router bekanntmachen. Aufgrund dieser Information können andere IGMP-Snooping-fähige Geräte schneller lernen, welche ihrer Ports Sie als Router-Ports verwenden sollen. Beim Aktivieren von Ports kann ein Switch z. B. eine entsprechende Anfrage nach Multicast-Routern versenden, die der Router mit einer solchen Bekanntmachung beantworten kann. Diese Methode ist je nach Situation ggf. deutlich schneller als die alternative Lernmöglichkeit über die IGMP-Anfragen.

Mögliche Werte:

- 4 bis 180 Sekunden

Default:

- 20

Anfrage-Intervall

Intervall in Sekunden, in dem ein Multicast-fähiger Router (oder ein simulierter Querier) IGMP-Anfragen an die Multicast-Adresse `224.0.0.1` schickt und damit Rückmeldungen der Stationen über die Mitgliedschaft in Multicast-Gruppen auslöst. Diese regelmäßigen Abfragen beeinflussen den Zeitpunkt, nach dem die Bridge die Mitgliedschaft in bestimmten Multicast-Gruppen "altern" lässt und löscht.

- Ein Querier sendet nach der Anfangsphase IGMP-Anfragen in diesem Intervall.
- Ein Querier kehrt zurück in den Querier-Status nach einer Zeit von "Robustheit*Anfrage-Intervall+(Anfrage-Antwort-Intervall/2)".
- Ein Router-Port verliert seine Eigenschaften nach einer Alterungszeit von "Robustheit*Anfrage-Intervall+(Anfrage-Antwort-Intervall/2)".

Mögliche Werte:

- Zahl aus 10 Ziffern größer als 0.

Default:

- 125

Das Anfrage-Intervall muss größer als das Anfrage-Antwort-Intervall sein.

Anfrage-Antwort-Intervall

Intervall in Sekunden, beeinflusst das Timing zwischen den IGMP-Anfragen und dem Altern der Router-Ports bzw. Mitgliedschaften.

Intervall in Sekunden, in dem ein Multicast-fähiger Router (oder ein simulierter Querier) Antworten auf seine IGMP-Anfragen erwartet. Diese regelmäßigen Abfragen beeinflussen den Zeitpunkt, nach dem die Mitgliedschaft in bestimmten Multicast-Gruppen "altern" und gelöscht werden.

Mögliche Werte:

- Zahl aus 10 Ziffern größer als 0.

Default:

- 10

Das Anfrage-Antwort-Intervall muss kleiner als das Anfrage-Intervall sein.

Robustheit

Dieser Wert bestimmt die Robustheit des IGMP-Protokolls. Diese Option toleriert den Paketverlust von IGMP-Anfragen gegenüber den Join-Nachrichten.

Mögliche Werte:

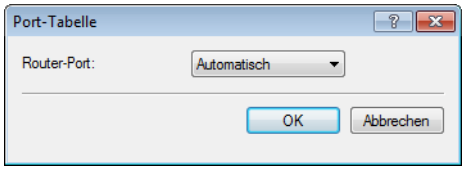
- Zahl aus 10 Ziffern größer als 0.

Default:

- 2

8.4.2 Port-Einstellungen

In dieser Tabelle können Sie die Port-bezogenen Einstellungen für IGMP Snooping vornehmen.



Port

Auf diesen Port geziehen sich die Einstellungen.

Mögliche Werte:

- Auswahl aus der Liste der im Gerät verfügbaren Ports.

Default:

- N/A

Router-Port

Diese Option definiert das Verhalten des Ports.

Mögliche Werte:

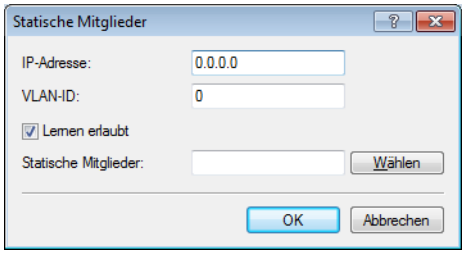
- Ja: Dieser Port verhält sich immer wie ein Router-Port, unabhängig von den IGMP-Anfragen oder Router-Meldungen, die die Bridge auf diesem Port evtl. empfängt.
- Nein: Dieser Port verhält sich nie wie ein Router-Port, unabhängig von den IGMP-Anfragen oder Router-Meldungen, die die Bridge auf diesem Port evtl. empfängt.
- Automatisch: Dieser Port verhält sich wie ein Router-Port, wenn eine IGMP-Anfragen oder Router-Meldung empfangen wurde. Der Port verliert diese Eigenschaft wieder, wenn die Bridge auf diesem Port für die Dauer von "Robustheit*Anfrage-Intervall+(Anfrage-Antwort-Intervall/2)" keine entsprechenden Pakete empfängt.

Default:

- Automatisch

8.4.3 Statische-Mitglieder

Diese Tabelle erlaubt die manuelle Definition von Mitgliedschaften, die z. B. nicht automatisch gelernt werden können oder sollen.



IP-Adresse

Die IP-Adresse der manuell definierten Multicast-Gruppe.

Mögliche Werte:

- Gültige IP-Multicast-Adresse.

Default:

- 0.0.0.0

VLAN-ID

Die VLAN-ID, auf welche die Bridge diese statische Mitgliedschaft anwenden soll. Für eine IP-Multicast-Adresse können Sie durchaus mehrere Einträge mit unterschiedlichen VLAN-IDs eintragen.

Mögliche Werte:

- 0 bis 4096.

Default:

- 0

Besondere Werte:

- Wenn "0" als VLAN gewählt wird, werden die IGMP-Anfragen ohne VLAN-Tag ausgegeben. Dieser Wert ist daher nur sinnvoll, wenn die Verwendung von VLAN generell deaktiviert ist.

Lernen erlaubt

Mit dieser Option aktivieren Sie das automatische Lernen von Mitgliedschaften für diese Multicast-Gruppe. Wenn das automatische Lernen deaktiviert ist, verschickt die Bridge die Pakete nur über die für die Multicast-Gruppe manuell definierten Ports.

Mögliche Werte:

- aktiviert
- deaktiviert

Default:

- Aktiviert

Statische Mitglieder

An diese Ports stellt die Bridge die Pakete mit der entsprechenden IP-Multicast-Adresse immer zu, unabhängig von empfangenen Join-Nachrichten.

Mögliche Werte:

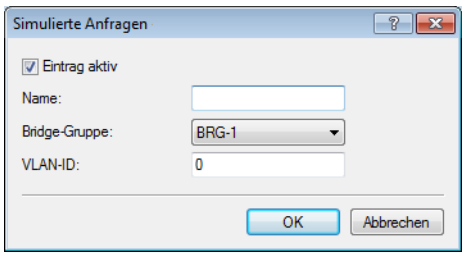
- Kommaseparierte Liste der gewünschten Ports, maximal 215 alphanumerische Zeichen.

Default:

- Leer

8.4.4 Simulierte-Anfrager

Diese Tabelle enthält alle im Gerät definierten simulierten Querier. Diese Einheiten werden eingesetzt, wenn kein Multicast-Router im Netzwerk vorhanden ist, aber dennoch die Funktionen des IGMP-Snooping benötigt werden. Um die Querier auf bestimmte Bridge-Gruppen oder VLANs einzuschränken, können Sie mehrere unabhängige Querier definieren, welche dann die entsprechenden VLAN-IDs nutzen.



Eintrag aktiv

Aktiviert oder deaktiviert die Querier-Instanz.

Mögliche Werte:

- Aktiviert
- Deaktiviert

Default:

- Aktiviert

Name

Name der Querier-Instanz.

Mögliche Werte:

- 8 alphanumerische Zeichen.

Default:

- Leer

Bridge-Gruppe

Schränkt die Querier-Instanz auf eine bestimmte Bridge-Gruppe ein.

Mögliche Werte:

- Auswahl aus der Liste der verfügbaren Bridge-Gruppen
- keine

Default:

- BRG-1

Besondere Werte:

- Ist "keine" Bridge-Gruppe gewählt, gibt die Bridge die IGMP-Anfragen auf allen Brigde-Gruppen aus.

VLAN-ID

Schränkt die Querier-Instanz auf ein bestimmtes VLAN ein.

Mögliche Werte:

- 0 bis 4096

Default:

- 0

Besondere Werte:

- Ist "0" als VLAN-ID gewählt, gibt die Bridge die IGMP-Anfragen ohne VLAN-Tag aus. Dieser Wert ist daher nur sinnvoll, wenn die Verwendung von VLAN generell deaktiviert ist.

8.4.5 Ergänzungen im Setup-Menü

In-Betrieb

Aktiviert oder deaktiviert IGMP-Snooping für das Gerät und alle definierten Querier-Instanzen. Ohne IGMP-Snooping verhält sich die Bridge wie ein einfacher Switch und sendet alle Multicasts auf alle Ports weiter.

Wenn diese Funktion deaktiviert ist, sendet die Bridge alle IP-Multicast-Pakete auf alle Ports. Bei einer Änderung des Betriebszustandes setzt das Gerät die IGMP-Snooping-Funktion vollständig zurück, d. h. es löscht alle dynamisch gelernten Werte (Mitgliedschaften, Router-Port-Eigenschaften).

SNMP-ID:

2.20.30.1

Pfad Telnet:

Setup > **LAN-Bridge** > **IGMP-Snooping**

Mögliche Werte:

nein

ja

Auto

Default:

nein

8.5 DHCP-Antworten von Broadcast in Unicast umwandeln

Um die Zuverlässigkeit der Zustellung von DHCP-Antworten im WLAN zu steigern, haben Sie ab LCOS 8.84 die Möglichkeit, als Broadcast gesendete Datenpakete (welche keinen speziellen Adressaten, keine optimierten Sendetechniken wie ARP-Spoofing oder IGMP/MLD-Snooping und eine niedrige Datenrate aufweisen) vom Gerät in Unicast-Datenpakete umwandeln lassen.

In LANconfig erreichen Sie dies über die Einstellung **Broadcast-DHCP-Antworten in Unicast konvertieren** im Dialog **Wireless-LAN** > **Allgemein** > **Logische WLAN-Einstellungen** > **WLAN-Netzwerk […]** > **Übertragung**.

Diese Funktion ist bereits integraler Bestandteil der Einstellung **Nur Unicasts übertragen, Broad und Multicasts unterdrücken** und muss dafür nicht explizit aktiviert werden.

8.5.1 Ergänzungen im Setup-Menü

in-Unicast-wandeln

Über diesen Parameter legen Sie fest, welche Art von als Broadcast gesendeten Datenpaketen das Gerät innerhalb eines WLAN-Netzwerks automatisch in Unicast umwandelt.

SNMP-ID:

2.23.20.2.25

Pfad Telnet:

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

Mögliche Werte:

- Keine Auswahl
- **DHCP**: Wandelt Antwort-Nachrichten des DHCP-Servers in Unicasts um, sofern der Server sie als Broadcast versendet hat. Dies steigert die Zuverlässigkeit der Zustellung, da als Broadcast gesendete Datenpakete keinen speziellen Adressaten, keine optimierten Sendetechniken wie ARP-Spoofing oder IGMP/MLD-Snooping und eine niedrige Datenrate aufweisen.

Default:

DHCP

8.6 Adaptive Noise Immunity zur Abschwächung von Interferenzen im WLAN

Ab LCOS-Version 8.84 beherrschen LANCOM Access Points die sogenannte adaptive Rausch-Immunität (Adaptive Noise Immunity, ANI), um unterschiedliche Störungen durch Interferenzen im WLAN zu kompensieren.

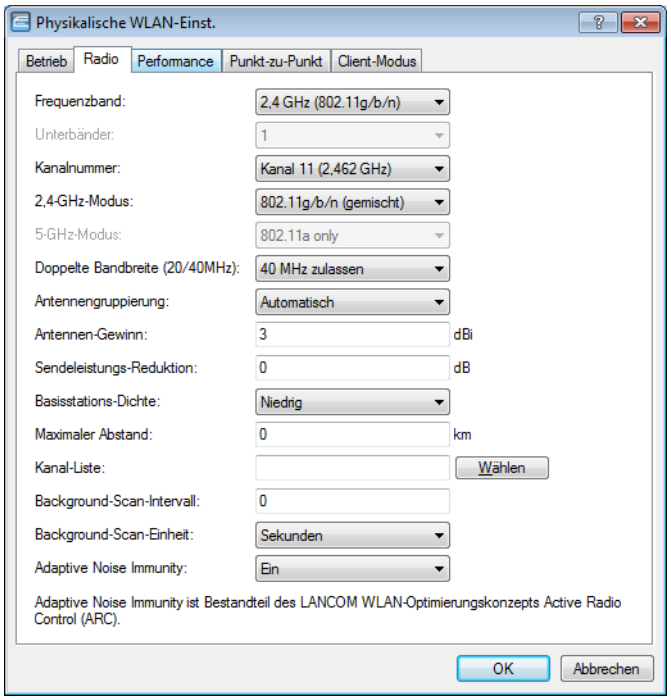
8.6.1 Ergänzungen in LANconfig

Adaptive Noise Immunity zur Abschwächung von Interferenzen im WLAN

Innerhalb eines WLANs kann es aus unterschiedlichen Gründen zu Störungen durch Interferenzen kommen. Einerseits stören Geräte wie Mikrowellenherde oder Funktelefone die Datenübertragung, andererseits können die Netzgeräte selber durch Aussendung von Störfrequenzen die Kommunikation behindern. Die Art dieser Störungen ist jeweils charakteristisch. Bei der adaptiven Rausch-Immunität (Adaptive Noise Immunity, ANI) ermittelt der Access Point anhand verschiedener Fehlerzustände die für die aktuelle Situation beste Kompensation der Störungen. Durch die automatische Erhöhung der Rausch-Immunität wird die Funkzelle gezielt verkleinert, sodass sich die Auswirkungen der Interferenzen auf die Datenübertragung verringern.

Die aktuellen Werte sowie die Aufzeichnung der vergangenen Aktionen finden Sie im WEBconfig unter **Status** > **WLAN** > **Rausch-Immunität**.

Die adaptive Rausch-Immunität aktivieren Sie in LANconfig unter **Wireless-LAN** > **Allgemein** > **Interfaces** > **Physikalische WLAN-Einstellungen** > **Radio**.



Aktivieren Sie die Adaptive Noise Immunity, indem Sie im Auswahlfeld **Adaptive-Noise-Immunity** den Wert "Ein" auswählen.

Adaptive Noise Immunity ist Bestandteil von *LANCOM Active Radio Control (ARC)*

8.6.2 Ergänzungen im Setup-Menü

Adaptive-Rausch-Immunitaet

Innerhalb eines WLANs kann es aus unterschiedlichen Gründen zu Störungen durch Interferenzen kommen. Einerseits stören Geräte wie Mikrowellenherde oder Funktelefone die Datenübertragung, andererseits können die Netzgeräte selber durch Aussendung von Störfrequenzen die Kommunikation behindern. Die Art dieser Störungen ist jeweils charakteristisch. Bei der adaptiven Rausch-Immunität (Adaptive Noise Immunity, ANI) ermittelt der Access Point anhand verschiedener Fehlerzustände die für die aktuelle Situation beste Kompensation der Störungen. Durch die automatische Erhöhung der Rausch-Immunität wird die Funkzelle gezielt verkleinert, sodass sich die Auswirkungen der Interferenzen auf die Datenübertragung verringern.

Die aktuellen Werte sowie die Aufzeichnung der vergangenen Aktionen finden Sie unter **Status** > **WLAN** > **Rausch-Immunität**.

SNMP-ID:

2.23.20.8.23

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **Radio-Einstellungen**

Mögliche Werte:

nein

ja

Default:

ja

8.6.3 Ergänzungen im Status-Menü

Rausch-Immunität

In diesem Verzeichnis finden Sie die aktuell ermittelten Werte des WLANs sowie die Aufzeichnungen über vergangene Ereignisse.

SNMP-ID:

1.3.63

Pfad Telnet:

Status > **WLAN**

Momentane-Parameter

Diese Tabelle zeigt die aktuellen ANI-Parameter aller Bänder und Funk-Kanäle.

Wenn Adaptive Noise Immunity deaktiviert ist, beinhaltet die Tabelle entweder die Defaultwerte nach der Initialisierung der WLAN-Schnittstelle bzw. die manuell vorgegebenen Werte.

SNMP-ID:

1.3.63.1

Pfad Telnet:

Status > **WLAN** > **Rausch-Immunität**

Band

Zeigt das Band an, auf dem der Access Point die aktuellen Parameter misst. Mögliche Anzeigen sind:

- 2,4 GHz
- 5 GHz

Funk-Kanal

Zeigt die verfügbaren Funk-Kanäle in entsprechenden Band an.

Interface

Zeigt das WLAN-Interface an, an dem der Access Point die aktuellen Parameter misst.

Alter

Zeigt das Alter der Messung an.

Rausch-Immunitaet

Gibt das Maß der Rausch-Immunität an. Je höher der Wert, desto "immuner" ist der Access Point gegenüber Interferenzen. Der Wertebereich ist abhängig vom genutzten Funkmodul.

Spurious-Immunitaet

Parameter zur internen Verwendung des WLAN-Moduls.

Fir-Step

Parameter zur internen Verwendung des WLAN-Moduls.

OFDM-Schwache-Signale-Erkennung

Parameter zur internen Verwendung des WLAN-Moduls.

CCK-Schwaches-Signal-Erkennungs-Schwellwert

Parameter zur internen Verwendung des WLAN-Moduls.

MRC-CCK

Parameter zur internen Verwendung des WLAN-Moduls.

Die Wertebereiche für die einzelnen Messwerte sind abhängig vom verwendeten Funkmodul. Welches Funkmodul in Ihrem Gerät verbaut ist, entnehmen Sie der Spalte **WLAN** > **Interfaces** > **Karten-ID** im Status-Menü.

Funkmodul-Chipsatz	Rausch-Immunitaet	OFDM-Schwache-Signale-Erkennung	CCK-Schwaches-Signal-Erkennungs-Schwellwert	Fir-Step	Spurious-Immunitaet	MRC-CCK
AR5212/5213/2414/5414	0 bis 4	0, 1	0, 1	0 bis 3	0 bis 7	leer
AR9160/9280	0 bis 4	0, 1	0, 1	0 bis 3	0 bis 7	leer
AR9380/9382/9390	leer	0, 1	0, 1	0 bis 8	0 bis 7	0, 1

Log-Tabelle

Diese Tabelle zeigt die aufgezeichneten ANI-Ereignisse je Band, Kanal und WLAN-Schnittstelle an.

Bei Extrembedingungen (sehr starke oder sehr schwache Interferenzen) können die Parameter ihren Maximalwert erreichen. Sollten sich die Interferenzen innerhalb dieser Extremwerte ändern, schreibt der Access Point diesen Maximalwert trotzdem nur einmal in die Tabelle.

SNMP-ID:

1.3.63.2

Pfad Telnet:

Status > **WLAN** > **Rausch-Immunität**

Index

Enthält die laufende Nummer des Eintrags

Zeit

Zeigt den Zeitpunkt des Ereignisses an.

Interface

Zeigt das WLAN-Interface an, an dem das Ereignis bzw. die Aktion des Access Points erfolgte.

Band

Zeigt das Band an, für das das Ereignis galt.

Funk-Kanal

Zeigt den Funk-Kanal an, für den das Ereignis galt.

Ereignis

Zeigt die Änderungen der ANI-Parameter an. Mögliche Werte sind:

- min.-Immunität:
- Wertaenderung:

Parameter

Parameter zur internen Verwendung des WLAN-Moduls.

Wert

Parameter zur internen Verwendung des WLAN-Moduls.

8.7 Opportunistic Key Caching

Um das WLAN-Roaming bei Verschlüsselung über WPA2-Enterprise zu beschleunigen, steht ab LCOS-Version 8.84 das Opportunistic Key Caching zur Verfügung.

8.7.1 Opportunistic Key Caching (OKC)

Authentifizierung von WLAN-Clients über EAP und 802.11X ist mittlerweile Standard in Unternehmens-Netzwerken, und auch beim öffentlichen Internet-Zugang findet es im Rahmen der Hotspot 2.0-Spezifikation immer mehr Verbreitung. Der Nachteil der Authentifizierung über 802.11X ist, dass die Zeit von Anmeldung bis zur Verbindung durch den Austausch von bis zu zwölf Datenpaketen zwischen WLAN-Client und Access Point sich merklich verlängert. Für die meisten Anwendungen, bei denen es nur um den Austausch von Daten geht, mag das nicht ins Gewicht fallen. Zeitkritische Anwendungen wie z. B. Voice-over-IP sind jedoch davon abhängig, dass die Neuanmeldung in einer benachbarten WLAN-Funkzelle die Kommunikation nicht beeinträchtigt.

Um dem entgegenzuwirken, haben sich bestimmte Authentifizierungsstrategien wie PMK-Caching und Pre-Authentifizierung etabliert, wobei auch durch Pre-Authentifizierung nicht alle Probleme behoben sind. Einerseits ist nicht sichergestellt, wie der WLAN-Client erkennt, ob der Access Point Pre-Authentifizierung beherrscht. Andererseits führt Pre-Authentifizierung zu einer erheblichen Belastung des RADIUS-Servers, der die Authentifizierungen von allen Clients und allen Access Points im WLAN-Netzwerk verarbeiten muss.

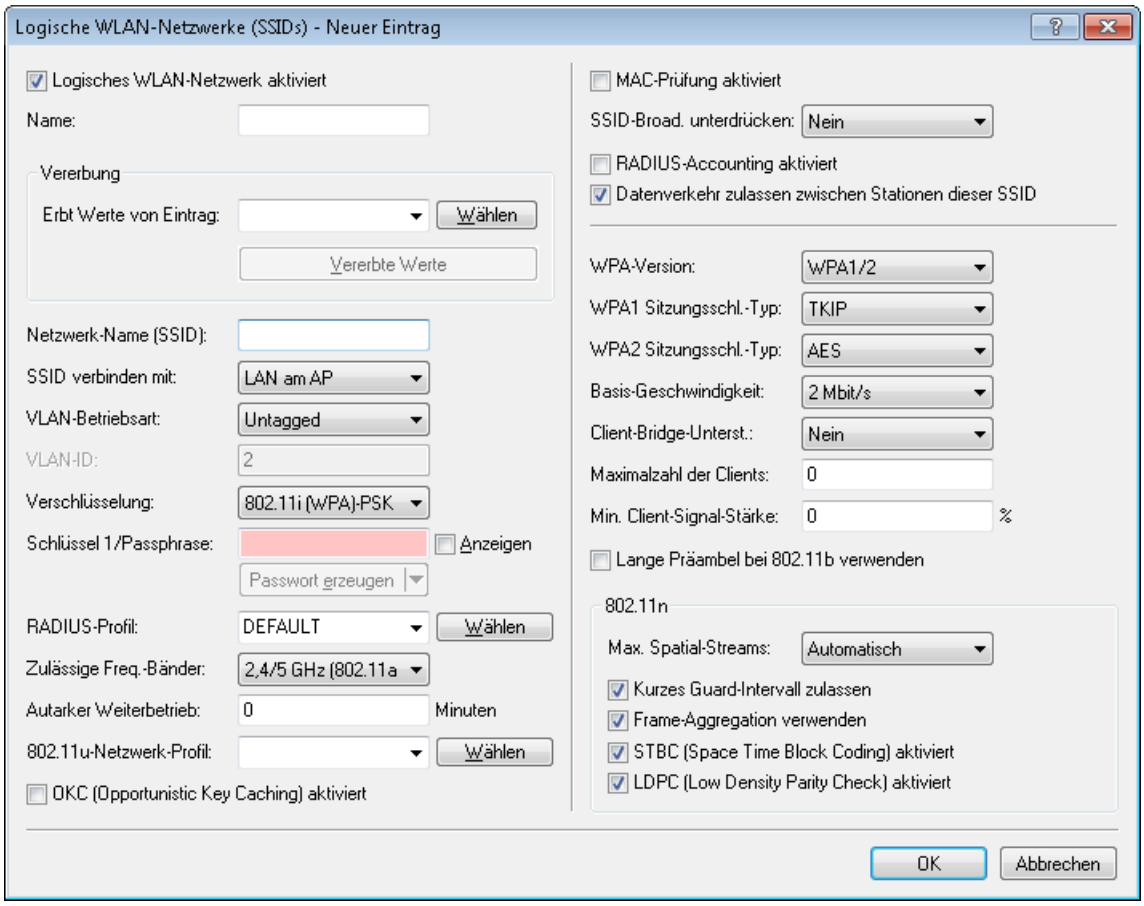
Das opportunistische Schlüssel-Caching verlagert die Schlüsselverwaltung auf einen WLAN-Controller oder zentralen Switch, der alle Access Points im Netzwerk verwaltet. Meldet sich ein Client bei einem Access Point an, übernimmt der nachgeschaltete WLAN-Controller als Authenticator die Schlüsselverwaltung und sendet dem Access Point den PMK, den schließlich der Client erhält. Wechselt der Client die Funkzelle, errechnet er aus diesem PMK und der MAC-Adresse des neuen Access Points eine PMKID und sendet die an den neuen Access Point in der Erwartung, dass der OKC aktiviert hat (deshalb "opportunistisch"). Kann der Access Point mit der PMKID nichts anfangen, handelt er mit dem Client eine normale 802.11X-Authentifizierung aus.

Ein LANCOM-Access Point kann auch OKC durchführen, falls der WLAN-Controller vorübergehend nicht erreichbar ist. In diesem Fall speichert er den PMK und sendet ihn an den WLAN-Controller, sobald er wieder verfügbar ist. Der schickt den PMK anschließend an alle Access Points im Netzwerk, so dass der Client sich beim Wechsel der Funkzelle dort über OKC anmelden kann.

8.7.2 Ergänzungen in LANconfig

Logische WLAN-Netzwerke

Unter **WLAN-Controller** > **Profile** > **Logische WLAN-Netzwerke** können Sie die Parameter für die logischen WLAN-Netzwerke einstellen, die der WLAN-Controller den Access Points zuweisen soll. Für jedes logische WLAN-Netzwerk können Sie die folgenden Parameter definieren:



Logisches WLAN-Netzwerk aktiviert

Aktivieren Sie das logische WLAN-Netzwerk, indem Sie diese Option anklicken.

Name

Geben Sie hier einen Namen an, der das logische WLAN-Netzwerk eindeutig kennzeichnet.

Vererbung

Möchten Sie Einträge erzeugen, die sich nur in wenigen Werten von vorhandenen Einträgen unterscheiden, können Sie einen "Eltern"-Eintrag sowie die zu übernehmenden Einträge hier gezielt auswählen.

Auch ein "Eltern"-Eintrag kann selber geerbte Einträge enthalten. Achten Sie darauf, dass die Konstruktionen für geerbte Einträge nicht zu komplex und damit schwer nachvollziehbar und konfigurierbar sind.

Netzwerk-Name (SSID)

Geben Sie hier die SSID des WLAN-Netzwerkes an. Alle Stationen, die zu diesem WLAN-Netz gehören, müssen dieselbe SSID verwenden.

SSID verbinden mit

Wählen Sie hier aus, mit welcher logischen Schnittstelle des Access Points die SSID verknüpft sein soll bzw. wohin der Access Point Datenpakete dieser SSID leiten soll.

- "LAN": Der Access Point lädt die Datenpakete standardmäßig lokal ins LAN weiter (LAN-1). Dazu muss er entsprechend konfiguriert sein.
- "WLC-Tunnel-x": Die SSID ist mit einem WLC-Bridge-Layer-3-Tunnel verbunden. Der Access Point liefert alle Datenpakete in diesen Tunnel und damit zum WLC. Dieser Tunnel muss auf dem WLC konfiguriert sein.

Beachten Sie, dass Sie bei Weiterleitung aller Datenpakete zum WLC zwar zentrale Routen und Filter definieren können, dieses jedoch eine hohe Last auf dem WLA-Controller erzeugt. Dafür müssen dort entsprechend hohe Bandbreiten zur Verfügung stehen, um den gesamten Datenverkehr dieser und ggf. weiterer über WLC-Tunnel mit diesem WLAN-Controller verbundenen SSIDs übertragen zu können.

VLAN-Betriebsart

Stellen Sie hier die VLAN-Betriebsart des Access Points für Pakete dieses WLAN-Netzwerkes (SSID) ein. Die Verwendung von VLAN-IDs ist abhängig davon, ob das VLAN-Modul in den physikalischen WLAN-Parametern des Access Points aktiviert ist. Ansonsten ignoriert der Access Point alle VLAN-Einstellungen in den logischen Netzwerken. Es ist möglich, das Netzwerk trotz aktiviertem VLAN auch ungetagged zu betreiben:

- "Untagged": Der Access Point markiert Datenpakete dieser SSID nicht mit einer VLAN-ID.

  Es ist möglich ein WLAN-Netzwerk trotz aktiviertem VLAN auch ungetagged zu betreiben. Intern ist dafür die VLAN-ID "1" reserviert.
- "Tagged": Der Access Point markiert die Datenpakete mit der nachfolgend bestimmten VLAN-ID.

VLAN-ID

VLAN-ID für dieses logische WLAN-Netzwerk.

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

Verschlüsselung

Bestimmen Sie hier das Verschlüsselungsverfahren bzw. bei WEP die Schlüssellänge für die Verschlüsselung von Datenpaketen in diesem WLAN.

Schlüssel 1/Passphrase

Sie können die Schlüssel oder Passphrasen als ASCII-Zeichenkette eingeben. Bei WEP ist alternativ die Eingabe einer Hexadezimalzahl durch ein vorangestelltes "0x" möglich. Folgende Zeichenkettenlängen ergeben sich für die verwendeten Formate:

- WPA-PSK: 8 bis 63 ASCII-Zeichen
- WEP128 (104 Bit): 13 ASCII- oder 26 Hexadezimal-Zeichen
- WEP64 (40 Bit): 5 ASCII- oder 10 Hexadezimal-Zeichen

RADIUS-Profil

Geben Sie an, welches RADIUS-Profil der Access Point für dieses Netzwerk erhalten soll, damit dieser bei Bedarf eine direkte Verbindung zum RADIUS-Server aufbauen kann. Lassen Sie dieses Feld leer, wenn der WLAN-Controller RADIUS-Anfragen abwickeln soll.

Die RADIUS-Profile müssen Sie in der entsprechenden Tabelle konfigurieren.

Zulässige Freq.-Bänder

Bestimmen Sie das Frequenzband, das die Netzwerkteilnehmer zur Übertragung von Daten im WLAN verwenden sollen. Sie können sowohl das 2,4 GHz-Band, das 5 GHz-Band als auch beide Bänder auswählen.

Autarker Weiterbetrieb

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

Der WLAN-Controller weist den Access Point die Konfiguration zu, der sie optional im Flash gespeichert (in einem Bereich, der nicht mit LANconfig oder anderen Tools auszulesen ist). Falls die Verbindung zum WLAN-Controller abbricht, 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, bevor die Verbindung zum WLAN-Controller wiederhergestellt ist, löscht der Access Point die Konfiguration im Flash – der Access Point stellt seinen Betrieb ein. Sobald der WLAN-Controller wieder erreichbar ist, überträgt der WLAN-Controller die Konfiguration erneut zum Access Point.

Diese Maßnahme stellt einen wirksamen Schutz gegen Diebstahl dar, da der Access Point die sicherheitsrelevanten Parameter der Konfiguration nach Ablauf der eingestellten Zeit automatisch löscht.

Stellt der Access Point im Backupfall eine Verbindung zu einem sekundären WLAN-Controller her, so unterbricht der Access Point den Count-Down für den autarken Weiterbetrieb. 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 der Access Point die Konfigurationsdaten im Flash erst nach Ablauf der eingestellten Zeit für den autarken Weiterbetrieb löscht, nicht jedoch durch die Trennung vom Stromnetz!

802.11u-Netzwerk-Profil

Wählen Sie aus der Liste ein Hotspot-2.0-Profil aus.

OKC aktiviert

Mit dieser Option aktivieren Sie das opportunistische Schlüssel-Caching (Opportunistic Key Caching). Das OKC ermöglicht es WLAN-Clients, schnell und komfortabel in WLAN-Umgebungen mit WPA2-Enterprise-Verschlüsselung zwischen WLAN-Zellen zu wechseln (Roaming).

MAC-Prüfung aktiviert

In der MAC-Filterliste (**Wireless-LAN** > **Stationen** > **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.

SSID-Broad. unterdrücken

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

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

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

- **Nein**: Der 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.

RADIUS-Accounting aktiviert

Aktivieren Sie diese Option, wenn Sie das RADIUS-Accounting in diesem logischen WLAN-Netzwerkm aktivieren wollen.

Datenverkehr zulassen zwischen Stationen dieser SSID

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

WPA-Version

Wählen Sie hier die WPA-Version aus, die der Access Point den WLAN-Clients zur Verschlüsselung anbieten soll.

- WPA1: Nur WPA1
- WPA2: Nur WPA2
- WPA1/2: Sowohl WPA1 als auch WPA2 in einer SSID (Funkzelle)

WPA1 Sitzungsschl.-Typ

Wenn Sie als Verschlüsselungsmethode "802.11i (WPA)-PSK" nutzen, können Sie hier das Verfahren zur Generierung des Sitzungs- bzw. Gruppenschlüssels für WPA1 auswählen:

- AES: Der Access Point verwendet das AES-Verfahren.
- TKIP: Der Access Point verwendet das TKIP-Verfahren.
- AES/TKIP: Der Access Point verwendet das AES-Verfahren. Falls die Client-Hardware das AES-Verfahren nicht unterstützt, wechselt der Access Point zum TKIP-Verfahren.

WPA2 Sitzungsschl.-Typ

Wählen Sie hier das Verfahren zur Generierung des Sitzungs- bzw. Gruppenschlüssels für WPA2 aus.

Basis-Geschwindigkeit

Die eingestellte Basis-Geschwindigkeit sollte es auch unter ungünstigen Bedingungen erlauben, die langsamsten Clients im WLAN zu erreichen. Stellen Sie hier nur dann eine höhere Geschwindigkeit ein, wenn alle Clients in diesem logischen WLAN auch "schneller" zu erreichen sind. Bei automatischer Festlegung der Übertragungsrate sammelt der Access Point die Informationen über die Übertragungsraten der einzelnen WLAN-Clients. Die Rate teilen die Clients dem Access Point automatisch bei jeder Unicast-Kommunikation mit. Aus der Liste der angemeldeten Clients wählt der Access Point nun ständig die jeweils niedrigste Übertragungsrate aus und überträgt damit die Multicast- und Broadcast-Sendungen.

Client-Bridge-Unterst.

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.

Maximalzahl der Clients

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.

Min. Client-Signal-Stärke

Mit diesem Eintrag bestimmen Sie den Schwellwert in Prozent für die minimale Signalstärke für Clients beim Einbuchen. Unterschreitet ein Client diesen Wert, sendet der 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.

Lange Präambel bei 802.11b verwenden

Normalerweise handeln die Clients im 802.11b-Modus die Länge der zu verwendenden Präambel mit dem Access Point selbst aus. Stellen Sie hier die "lange Präambel" nur dann fest ein, wenn die Clients diese feste Einstellung verlangen.

Max. Spatial-Streams

Mit der Funktion des Spatial-Multiplexing kann der Access Point mehrere separate Datenströme über separate Antennen übertragen, um so den Datendurchsatz zu verbessern. Der Einsatz dieser Funktion ist nur dann zu empfehlen, wenn die Gegenstelle die Datenströme mit entsprechenden Antennen verarbeiten kann.

In der Einstellung 'Automatisch' nutzt der Access Point alle Spatial-Streams, die das jeweilige WLAN-Modul unterstützt.

Kurzes Guard-Intervall zulassen

Dieser Option reduziert die Sendepause zwischen zwei Signalen von 0,8 µs (Standard) auf 0,4 µs (Short Guard Interval). Dadurch steigt die effektiv für die Datenübertragung genutzte Zeit und damit der Datendurchsatz. Auf der anderen Seite ist das WLAN-System damit anfälliger für Störungen, welche durch die Interferenzen zwischen zwei aufeinanderfolgenden Signalen auftreten können.

Im Automatik-Modus wird das kurze Guard-Intervall aktiviert, sofern die jeweilige Gegenstelle diese Betriebsart unterstützt. Alternativ kann die Nutzung des kurzen Guard-Intervalls auch ausgeschaltet werden.

Frame-Aggregation verwenden

Bei der Frame-Aggregation werden mehrere Datenpakete (Frames) zu einem größeren Paket zusammengefasst und gemeinsam versendet. Dieses Verfahren reduziert den Overhead der Pakete, der Datendurchsatz steigt.

Die Frame-Aggregation eignet sich weniger gut bei schnell bewegten Empfängern oder für zeitkritische Datenübertragungen wie Voice over IP.

STBC (Space Time Block Coding) aktiviert

Aktivieren Sie hier das Space Time Block Coding.

Die Funktion 'STBC' variiert den Versand von Datenpaketen zusätzlich über die Zeit, um auch zeitliche Einflüsse auf die Daten zu minimieren. Durch den zeitlichen Versatz der Sendungen besteht für den Empfänger eine noch bessere Chance, fehlerfreie Datenpakete zu erhalten, unabhängig von der Anzahl der Antennen.

LDPC (Low Density Parity Check) aktiviert

Aktivieren Sie hier den Low Density Parity Check.

Bevor der Sender die Datenpakete abschickt, erweitert er den Datenstrom abhängig von der Modulationsrate um Checksummen-Bits, um dem Empfänger damit die Korrektur von Übertragungsfehlern zu ermöglichen. Standardmäßig nutzt der Übertragungsstandard IEEE 802.11n das bereits aus den Standards 802.11a und 802.11g bekannte 'Convolution Coding' (CC) zur Fehlerkorrektur, ermöglicht jedoch auch eine Fehlerkorrektur nach der LDPC-Methode (Low Density Parity Check).

Im Unterschied zur CC-Kodierung nutzt die LDPC-Kodierung größere Datenpakete zur Checksummenberechnung und kann zusätzlich mehr Bit-Fehler erkennen. Die LDPC-Kodierung ermöglicht also bereits durch ein besseres Verhältnis von Nutz- zu Checksummen-Daten eine höhere Datenübertragungsrate.

8.7.3 Ergänzungen im Setup-Menü

OKC

Das opportunistische Schlüssel-Caching verlagert die Schlüsselverwaltung der WLAN-Clients auf einen WLAN-Controller oder zentralen Switch, der alle Access Points im Netzwerk verwaltet. Meldet sich ein Client bei einem Access Point an, übernimmt der nachgeschaltete WLAN-Controller als Authenticator die Schlüsselverwaltung und sendet dem Access Point den PMK, den schließlich der Client erhält. Wechselt der Client die Funkzelle, errechnet er aus diesem PMK und der MAC-Adresse des neuen Access Points eine PMKID und sendet die an den neuen Access Point in der Erwartung, dass der OKC aktiviert hat (deshalb "opportunistisch"). Kann der Access Point mit der PMKID nichts anfangen, handelt er mit dem Client eine normale 802.11X-Authentifizierung aus.

Ein LANCOM Access Point kann auch OKC durchführen, falls der WLAN-Controller vorübergehend nicht erreichbar ist. In diesem Fall speichert er den PMK und sendet ihn an den WLAN-Controller, sobald er wieder verfügbar ist. Der schickt den PMK anschließend an alle Access Points im Netzwerk, so dass der Client sich beim Wechsel der Funkzelle dort über OKC anmelden kann.

Mit dieser Einstellung aktivieren Sie OKC auf dem vom WLAN-Controller zu verwaltenden Access Point.

SNMP-ID:

2.37.1.1.40

Pfad Telnet:

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

Mögliche Werte:

Ja

Nein

Default:

ja

8.7.4 Ergänzungen im Status-Menü

Inhalt

Dieses Tabelle enthält alle Einträge des PMK-Caches.

SNMP-ID:

1.3.60.2

Pfad Telnet:

Status > **WLAN** > **PMK-Caching** > **Inhalt**

Authenticator

Dieser Eintrag enthält die MAC-Adresse des authentifizierenden Access Points.

Supplicant

Dieser Eintrag enthält die MAC-Adresse des sich authentifizierenden WLAN-Clients.

Quelle

Dieser Eintrag zeigt an, auf welchem Weg der WLAN-Client den PMK bezogen hat:

- **Unbekannt**: Die Quelle ist unbekannt. Dieser Eintrag sollte im normalen Betrieb nicht vorkommen.
- **Authentifizierung**: Der PMK ist das Ergebnis einer normalen 802.1x-Authentifizierung zwischen WLAN-Client und Access Point.

- **Prä-Authentifizierung**: Der PMK ist das Ergebnis einer 802.1x-Prä-Authentifizierung zwischen WLAN-Client und einem weiteren Access Point.

OKC: Der PMK ist das Ergebnis eines Opportunistic Key Caching.

Benutzername

Dieser Eintrag enthält den Benutzernamen, den der RADIUS-Server bei Zugangsgenehmigung an den Access Point sendet.

Übermittelt der RADIUS-Server keinen Benutzernamen, bleibt dieses Feld leer.

VLAN-Id

Dieser Eintrag enthält die VLAN-Id, die der RADIUS-Server bei Zugangsgenehmigung an den Access Point sendet.

Übermittelt der RADIUS-Server keinen VLAN-Id, bleibt dieses Feld leer.

Lebenszeit

Dieser Eintrag enthält die Lebenszeit des PMKs in Sekunden. Sie berechnet sich aus der Gültigkeit der Sitzung, die der RADIUS-Server in der Zugangsgenehmigung übermittelt.

Die Wert beträgt 0 Sekunden, wenn der RADIUS keine Dauer überträgt bzw. der PMK keinen Gültigkeitszeitraum besitzt.

Abgelaufen

Dieser Eintrag zeigt, ob ein PMK abgelaufen ist. Ist das der Fall, akzeptiert der Access Point keine PMK-Caching- oder Authentifizierungs-Versuche mit diesem PMK mehr. Stattdessen startet er eine neue 802.1x-Authentifizierung.

Verschlüsselung

Diese Tabellen enthalten Informationen über die Verschlüsselung je Schnittstelle.

SNMP-ID:

1.3.64

Pfad Telnet:

Status > **WLAN**

Interface

Bezeichnung der Schnittstelle

Verschlüsselung

Zeigt an, ob für das entsprechende Interface die Verschlüsselung eingeschaltet ist.

Methode

Zeigt die Verschlüsselungsmethode an. Falls die Verschlüsselung deaktiviert ist, enthält diese Spalte den Wert "Kein"

WPA-Version

Zeigt die WPA-Version der Verschlüsselung an.

WPA1-Sitzungsschluessel

Zeigt das Protokoll für den WPA1-Sitzungsschlüssel an.

WPA2-Sitzungsschluessel

Zeigt das Protokoll für den WPA2-Sitzungsschlüssel an.

PMK-Caching

Zeigt an, ob das PMK-Caching (Speichern des Pairwise Master Key) auf der Schnittstelle aktiviert ist.

Prae-Authentisierung

Zeigt an, ob die Prä-Authentifizierung an dieser Schnittstelle aktiviert ist.

OKC

Zeigt an, ob das Opportunistic Key Caching auf der Schnittstelle aktiviert ist.

8.8 Feature-Erweiterung der WLC-Tunnel-Schnittstelle

WLC-Tunnel-Schnittstellen stellen "virtuelle Ethernet-Schnittstellen" dar, die bisher jedoch im Vergleich zu physikalischen Ethernet-Schnittstellen noch einige Einschränkungen besaßen. Ab LCOS-Version 8.84 unterstützen WLC-Tunnel-Schnittstellen zusätzlich die folgenden Features:

- Sie können je Benutzer eine Bandbreitenlimitierung einstellen.
- VRRP funktioniert (Eintragen von zusätzlichen MAC-Adressen)
- Sie können je Benutzer eine VLAN-ID vergeben.

8.9 Unterstützung von 802.11u/Hotspot 2.0 auf WLAN-Controllern

Mit LCOS 8.84 erhalten Sie die Möglichkeit, die für Access Points unter LCOS 8.82 eingeführten IEEE-802.11u-/Hotspot-2.0-Funktionalitäten auch mit dem WLAN-Controller zu konfigurieren und über Profile den angeschlossenen Access Points zuzuweisen. Die Einstellungsmöglichkeiten entsprechen dabei denen der Access Points.

8.9.1 Ergänzungen im Status-Menü

IEEE802.11u

Dieses Menü zeigt die Einstellungen für IEEE802.11u bzw. Hotspot 2.0, die das Gerät vom WLC insgesamt zugewiesen bekommen hat.

SNMP-ID:

1.59.108

Pfad Telnet:

Setup > **WLAN-Management**

Netzwerk-Profile

Diese Tabelle zeigt das Netzwerk- bzw. 802.11u-Profil, welches das Gerät vom WLC zugewiesen bekommen hat.

SNMP-ID:

1.59.108.1

Pfad Telnet:

Setup > **WLAN-Management** > **IEEE802.11u**

Name

Name des Netzwerk- bzw. 802.11u-Profils

Operating

Zeigt an, ob unter dem betreffenden Profil die Unterstützung für Verbindungen nach IEEE 802.11u aktiviert ist

Hotspot2.0

Zeigt an, ob unter dem betreffenden Profil die Unterstützung für Hotspot 2.0 aktiviert ist

Internet

Zeigt an, ob unter dem betreffenden Profil das Internet-Bit gesetzt ist

Network-Type

Typ, der das logische WLAN-Netzwerk am ehesten charakterisiert (z. B. privat, öffentlich, Zugang mit oder ohne Authorisierung, usw.)

Asra

Zeigt an, ob unter dem betreffenden Profil das Asra-Bit gesetzt ist

HESSID-Type

Zeigt an, woher die MAC-Adresse für die HESSID stammt. Mögliche Werte sind:

- `auto`: Automatische Berechnung der HESSID durch den WLC
- `user`: Manuelle Vergabe der HESSID durch den Netzwerkadministrator
- `none`: Keine HESSID vorhanden

HESSID-MAC

MAC-Adresse der HESSID

ANQP-Profil

ANQP-Profil, das auf dem WLC für das 802.11u-Profil verwendet wird

HS20-Profil

Hotspot-2.0- bzw. HS20-Profil, das auf dem WLC für das 802.11u-Profil verwendet wird

ANQP-Profile

Diese Tabelle zeigt das ANQP-Profil, welches das Gerät vom WLC zugewiesen bekommen hat.

SNMP-ID:

1.59.108.2

Pfad Telnet:

Setup > **WLAN-Management** > **IEEE802.11u**

Name

Name des ANQP-Profils

Include-in-Beacon-OUI

Organizationally Unique Identifier (abgekürzt OUI, vereinfacht OI), die ein Access Point in seinen Beacons ausstrahlt

Additional-OUI

OI(s), die ein Access Point nach dem GAS-Request einer Station zusätzlich aussendet

Domain-List

Liste der Domains, denen ein Hotspot angehört

NAI-Realm-List

Zugewiesenes NAI-Realm-Profil

Cellular-List

Zugewiesenes Mobilfunknetzwerk-Profil

Network-Auth-Type-List

Zugewiesene Authentifizierungs-Parameter

Hotspot2.0-Profile

Diese Tabelle zeigt das Hotspot2.0-Profil, welches das Gerät vom WLC zugewiesen bekommen hat.

SNMP-ID:

1.59.108.3

Pfad Telnet:

Setup > **WLAN-Management** > **IEEE802.11u**

Name

Name der Hotspot2.0-Profils

Operator-Name

Zugewiesene Profilliste für den Hotspot-Betreiber

Connection-Capabilities

Zugewiesene Verbindungs-Fähigkeiten

Operating-Class

Code für die globale Betriebsklasse der verwalteten Access Points

Network-Authentication-Type

Diese Tabelle zeigt das Network-Authentication-Type-Profil, welches das Gerät vom WLC für das ANQP-Profil zugewiesen bekommen hat.

SNMP-ID:

1.59.108.4

Pfad Telnet:

Setup > **WLAN-Management** > **IEEE802.11u**

Name

Name des Network-Authentication-Type-Profils

Network-Auth-Type

Kontext, vor dem die Weiterleitung gilt

Redirect-URL

Adresse, 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

Cellular-Network-Information-List

Diese Tabelle zeigt das Mobilfunknetz-Profil, welches das Gerät vom WLC für das ANQP-Profil zugewiesen bekommen hat.

SNMP-ID:

1.59.108.5

Pfad Telnet:

Setup > **WLAN-Management** > **IEEE802.11u**

Name

Name des Mobilfunknetz-Profils

Country-Code

Zugewiesener Mobile Country Code (MCC) des Hotspot-Betreibers oder seiner Roaming-Partner

Network-Code

Zugewiesener Mobile Network Code (MNC) des Hotspot-Betreibers oder seiner Roaming-Partner

Venue-Name

Diese Tabelle zeigt das Venue-Name-Profil (Profil für zur Verwaltung der Standort-Informationen eines Access Points), welches das Gerät vom WLC zugewiesen bekommen hat.

SNMP-ID:

1.59.108.6

Pfad Telnet:

Setup > **WLAN-Management** > **IEEE802.11u**

Name

Name des Venue-Name-Profils

Language

Sprache, in der die Informationen zum Standort hinterlegt sind

Venue-Name

Beschreibung zum Standort des Gerätes ein

NAI-Realms

Diese Tabelle zeigt das NAI-Realm-Profil, welches das Gerät vom WLC für das ANQP-Profil zugewiesen bekommen hat.

SNMP-ID:

1.59.108.7

Pfad Telnet:

Setup > **WLAN-Management** > **IEEE802.11u**

Name

Name des NAI-Realm-Profils

NAI-Realm

Zugewiesener Realm für das Wi-Fi-Netzwerk

EAP-Method

Zugewiesene Authentifizierungsmethode für den NAI-Realm

Auth-Parameter-List

Zugewiesene Authentifizierungs-Parameter für die EAP-Methode

Operator-List

Diese Tabelle zeigt das Betreiber-Profil, welches das Gerät vom WLC für das Hotspot2.0-Profil zugewiesen bekommen hat.

SNMP-ID:

1.59.108.8

Pfad Telnet:

Setup > **WLAN-Management** > **IEEE802.11u**

Name

Name des Betreiber-Profils

Language

Zugewiesene Sprache für den Hotspot-Betreiber

Operator-Name

Zugewiesener Klartext-Name des Hotspot-Betreibers

General

Diese Tabelle zeigt das Standortprofil-Profil, welches das Gerät vom WLC zugewiesen bekommen hat.

SNMP-ID:

1.59.108.9

Pfad Telnet:

Setup > **WLAN-Management** > **IEEE802.11u**

Name

Name des Standortprofils

Link-Status

Konnektivitäts-Status der verwalteten Access Points mit dem Internet

Downlink-Speed

Nominalwert der Empfangs-Bandbreite (Downlink)

Uplink-Speed

Nominalwert der Sende-Bandbreite (Uplink)

IPv4-Addr-Type

Mitteilung an eine IEEE-802.11u-fähige Station über die Verfügbarkeit von IPv4-Adressräumen

IPv6-Addr-Type

Mitteilung an eine IEEE-802.11u-fähige Station über die Verfügbarkeit von IPv6-Adressräumen

Venue-Group

Zugewiesene Standort-Gruppe

Venue-Type

Zugewiesener Standort-Typ-Code

Venue-Name

Zugewiesenes Venue-Name-Profil (Profil für zur Verwaltung der Standort-Informationen eines Access Points)

IEEE802.11u

Dieses Menü zeigt die Einstellungen für IEEE802.11u bzw. Hotspot 2.0, die das Gerät den verwalteten Access Points derzeit zugewiesen hat.

SNMP-ID:

1.73.2.17

Pfad Telnet:

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

Netzwerk-Profile

Diese Tabelle zeigt die einzelnen Netzwerk-Profile, die das Gerät derzeit den verwalteten Access Points über das 802.11u-Profil in den logischen WLAN-Netzwerken zugewiesen hat.

SNMP-ID:

1.73.2.17.1

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u**

Name

Name des Netzwerk- bzw. 802.11u-Profils

Operating

Zeigt an, ob unter dem betreffenden Profil die Unterstützung für Verbindungen nach IEEE 802.11u aktiviert ist

Hotspot2.0

Zeigt an, ob unter dem betreffenden Profil die Unterstützung für Unterstützung für Hotspot 2.0 aktiviert ist

Internet

Zeigt an, ob unter dem betreffenden Profil das Internet-Bit gesetzt ist

Network-Type

Typ, der das logische WLAN-Netzwerk am ehesten charakterisiert (z. B. privat, öffentlich, Zugang mit oder ohne Authorisierung, usw.)

Asra

Zeigt an, ob unter dem betreffenden Profil das Asra-Bit gesetzt ist

HESSID-Type

Zeigt an, woher die MAC-Adresse für die HESSID stammt. Mögliche Werte sind:

- `auto`: Automatische Berechnung der HESSID durch den WLC
- `user`: Manuelle Vergabe der HESSID durch den Netzwerkadministrator
- `none`: Keine HESSID vorhanden

HESSID-MAC

MAC-Adresse der HESSID

ANQP-Profil

ANQP-Profil, das für das 802.11u-Profil verwendet wird

HS20-Profil

Hotspot-2.0- bzw. HS20-Profil, das für das 802.11u-Profil verwendet wird

ANQP-Profile

Diese Tabelle zeigt die einzelnen ANQP-Profile, die das Gerät derzeit den verwalteten Access Points über das Netzwerk- bzw. 802.11u-Profil in den logischen WLAN-Netzwerken zugewiesen hat.

SNMP-ID:

1.73.2.17.2

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u**

Name

Name des ANQP-Profils

Include-in-Beacon-OUI

Organizationally Unique Identifier (abgekürzt OUI, vereinfacht OI), die ein Access Point in seinen Beacons ausstrahlt

Additional-OUI

OI(s), die ein Access Point nach dem GAS-Request einer Station zusätzlich aussendet

Domain-List

Liste der Domains, denen ein Hotspot angehört

NAI-Realm-List

Zugewiesenes NAI-Realm-Profil

Cellular-List

Zugewiesenes Mobilfunknetzwerk-Profil

Network-Auth-Type-List

Zugewiesene Authentifizierungs-Parameter

Hotspot2.0-Profile

Diese Tabelle zeigt die einzelnen Hotspot2.0-Profile, die das Gerät derzeit den verwalteten Access Points über das Netzwerk- bzw. 802.11u-Profil in den logischen WLAN-Netzwerken zugewiesen hat.

SNMP-ID:

1.73.2.17.3

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u**

Name

Name der Hotspot2.0-Profils

Operator-Name

Zugewiesene Profilliste für den Hotspot-Betreiber

Connection-Capabilities

Zugewiesene Verbindungs-Fähigkeiten

Operating-Class

Code für die globale Betriebsklasse der verwalteten Access Points

Network-Authentication-Type

Diese Tabelle zeigt die einzelnen Network-Authentication-Type-Profile, die das Gerät derzeit für ein oder mehrere ANQP-Profile verwendet.

SNMP-ID:

1.73.2.17.4

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u**

Name

Name des Network-Authentication-Type-Profils

Network-Auth-Type

Kontext, vor dem die Weiterleitung gilt

Redirect-URL

Adresse, 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

Cellular-Network-Information-List

Diese Tabelle zeigt die einzelnen Mobilfunknetz-Profile, die das Gerät derzeit für ein oder mehrere ANQP-Profile verwendet.

SNMP-ID:

1.73.2.17.5

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u**

Name

Name des Mobilfunknetz-Profils

Country-Code

Zugewiesener Mobile Country Code (MCC) des Hotspot-Betreibers oder seiner Roaming-Partner

Network-Code

Zugewiesener Mobile Network Code (MNC) des Hotspot-Betreibers oder seiner Roaming-Partner

Venue-Name

Diese Tabelle zeigt die einzelnen Venue-Name-Profile (Profile für zur Verwaltung der Standort-Informationen eines Access Points), die das Gerät für ein oder mehrere Standortprofile verwendet.

SNMP-ID:

1.73.2.17.6

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u**

Name

Name des Venue-Name-Profils

Language

Sprache, in der die Informationen zum Standort hinterlegt sind

Venue-Name

Beschreibung zum Standort des Gerätes ein

NAI-Realms

Diese Tabelle zeigt die einzelnen NAI-Realm-Profile, die das Gerät derzeit für ein oder mehrere ANQP-Profile verwendet.

SNMP-ID:

1.73.2.17.7

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u**

Name

Name des NAI-Realm-Profils

NAI-Realm

Zugewiesener Realm für das Wi-Fi-Netzwerk

EAP-Method

Zugewiesene Authentifizierungsmethode für den NAI-Realm

Auth-Parameter-List

Zugewiesene Authentifizierungs-Parameter für die EAP-Methode

Operator-List

Diese Tabelle zeigt die einzelnen Betreiber-Profile, die das Gerät derzeit für ein oder mehrere Hotspot2.0-Profile verwendet.

SNMP-ID:

1.73.2.17.8

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u**

Name

Name des Betreiber-Profils

Language

Zugewiesene Sprache für den Hotspot-Betreiber

Operator-Name

Zugewiesener Klartext-Name des Hotspot-Betreibers

General

Diese Tabelle zeigt die einzelnen Standortprofil-Profile, die das Gerät derzeit für ein oder mehrere WLAN-Profile verwendet.

SNMP-ID:

1.73.2.17.9

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u**

Name

Name des Standortprofils

Link-Status

Konnektivitäts-Status der verwalteten Access Points mit dem Internet

Downlink-Speed

Nominalwert der Empfangs-Bandbreite (Downlink)

Uplink-Speed

Nominalwert der Sende-Bandbreite (Uplink)

IPv4-Addr-Type

Mitteilung an eine IEEE-802.11u-fähige Station über die Verfügbarkeit von IPv4-Adressräumen

IPv6-Addr-Type

Mitteilung an eine IEEE-802.11u-fähige Station über die Verfügbarkeit von IPv6-Adressräumen

Venue-Group

Zugewiesene Standort-Gruppe

Venue-Type

Zugewiesener Standort-Typ-Code

Venue-Name

Zugewiesenes Venue-Name-Profil (Profil für zur Verwaltung der Standort-Informationen eines Access Points)

8.9.2 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. Über Profile lassen sich diese Einstellungen schließlich den an den WLAN-Controller angeschlossenen Access Points zuweisen.

SNMP-ID:

2.37.1.17

Pfad Telnet:

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

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 **Netzwerk-Profile** 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:

2.37.1.17.2

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u**

Name

Vergeben Sie hierüber einen Namen für das ANQP-Profil. Diesen Namen geben Sie später in der Tabelle **Netzwerk-Profile** unter **ANQP-Profil** an.

SNMP-ID:

2.37.1.17.2.1

Pfad Telnet:

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

2.37.1.17.2.2

Pfad Telnet:

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

2.37.1.17.2.3

Pfad Telnet:

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

2.37.1.17.2.4

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **ANQP-Profile**

Mögliche Werte:

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

Default:

NAI-Realm-List

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

SNMP-ID:

2.37.1.17.2.5

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **ANQP-Profile**

Mögliche Werte:

Name aus Tabelle **Setup** > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **NAI-Realms**, max. 65 Zeichen. Mehrere Namen trennen Sie durch eine kommaseparierte Liste.

Default:

Cellular-List

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

SNMP-ID:

2.37.1.17.2.6

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **ANQP-Profile**

Mögliche Werte:

Name aus Tabelle **Setup** > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **Cellular-Network-Information-List**, max. 65 Zeichen. Mehrere Namen trennen Sie durch eine kommaseparierte Liste.

Default:

Network-Auth-Type-List

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

SNMP-ID:

2.37.1.17.2.7

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **ANQP-Profile**

Mögliche Werte:

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

Default:

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** als kommaseparierte Liste referenzieren.

Tabelle 2: Übersicht der möglichen Authentifizierungs-Parameter

Parameter	Sub-Parameter	Erläuterung
NonEAPAuth.		Bezeichnet das Protokoll, welches der Realm für die Phase-2-Authentifizierung erfordert:

Parameter	Sub-Parameter	Erläuterung
	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
	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.

SNMP-ID:

2.37.1.17.10

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u**

Name

Dieser Eintrag zeigt den Namen des Authentifizierungsparameters, auf den Sie in der Tabelle **NAI-Realms** im Eingabefeld **Auth-Parameter** als kommaseparierte Liste referenzieren.

SNMP-ID:

2.37.1.17.10.1

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **Auth-Parameter**

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 **ANQP-Profile** einem ANQP-Profil zu.

SNMP-ID:

2.37.1.17.5

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **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 **ANQP-Profile** unter **Cellular-List** an.

SNMP-ID:

2.37.1.17.5.1

Pfad Telnet:

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

2.37.1.17.5.2

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **Cellular-Network-Information-List**

Mögliche Werte:

Gültigen MCC, 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:

2.37.1.17.5.3

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **Cellular-Network-Information-List**

Mögliche Werte:

Gültigen MNC, max. 32 Zeichen

Default:

Connection-Capability

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

SNMP-ID:

2.37.1.17.11

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u**

Name

Dieser Eintrag zeigt den Namen der Verbindungsfähigkeit, auf die Sie in der Tabelle **Hotspot2.0-Profile** im Eingabefeld **Connection-Capabilities** als kommaseparierte Liste referenzieren.

SNMP-ID:

2.37.1.17.11.1

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **Connection-Capability**

General

Über diese Tabelle verwalten Sie die allgemeinen Einstellungen für IEEE 802.11u/Hotspot 2.0.

Auf einem Standalone Access Point liegen diese Einstellungen in Form separater Parameter vor. Auf einem WLAN Controller sind diese Parameter in Tabellen zusammengefasst, die Sie den verwalteten Access Points anschließend über das WLAN-Profil (Tabelle **Gesamtprofile**) zuweisen.

SNMP-ID:

2.37.1.17.9

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u**

Name

Vergeben Sie hierüber einen Namen für das Profil der allgemeinen Einstellungen. Diesen Namen geben Sie später in der Tabelle **Setup** > **WLAN-Management** > **AP-Konfiguration** > **Gesamtprofile** unter **Hotspot2.0-General** an.

SNMP-ID:

2.37.1.17.9.1

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **General**

Mögliche Werte:

String, max. 32 Zeichen

Default:

Link-Status

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

SNMP-ID:

2.37.1.17.9.2

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **General**

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:

2.37.1.17.9.3

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **General**

Mögliche Werte:

0 bis 4294967295, in KBit/s

Default:

0

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:

2.37.1.17.9.4

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **General**

Mögliche Werte:

0 bis 4294967295, in KBit/s

Default:

0

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:

2.37.1.17.9.5

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **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:

2.37.1.17.9.6

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **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:

2.37.1.17.9.7

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **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:

2.37.1.17.9.8

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **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

Standort-Gruppe	Code = Standort-Typ-Code
	■ 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

Default:

0

Venue-Name

Geben Sie in diesem Feld einen oder mehrere gültige Listeneinträge aus der Tabelle **Venue-Name** an, welche den Standort des Gerätes spezifizieren. Dabei erfasst der Parameter alle Listeneinträge, die dem hier angegebenem Vanue-Namen entsprechen.

SNMP-ID:

2.37.1.17.9.9

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **General**

Mögliche Werte:

Name aus Tabelle **Setup** > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **Venue-Name**, max. 32 Zeichen. Mehrere Namen trennen Sie durch eine mit rautenseparierte ('#') Liste.

Default:

Hotspot2.0-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 **Netzwerk-Profile**

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:

2.37.1.17.3

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u**

Name

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

SNMP-ID:

2.37.1.17.3.1

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **Hotspot2.0-Profile**

Mögliche Werte:

String, max. 32 Zeichen

Default:

Operator-Name

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

SNMP-ID:

2.37.1.17.3.2

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **Hotspot2.0-Profile**

Mögliche Werte:

Name aus Tabelle **Setup** > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **Operator-List**, max. 65 Zeichen

Default:

Connection-Capabilities

Geben Sie in diesem Feld einen oder mehrere gültige Einträge aus 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:

2.37.1.17.3.3

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **Hotspot2.0-Profile**

Mögliche Werte:

Name aus Tabelle **Setup** > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **Connection-Capability**, max. 250 Zeichen. Mehrere Namen trennen Sie durch eine kommaseparierte Liste.

Default:

Operating-Class

Geben Sie hier den Code für die globale Betriebsklasse der verwalteten Access Points an. Über die Betriebsklasse teilen Sie einer Station mit, auf welchen Frequenzbändern und Kanälen ein 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 einen Access Point 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:

2.37.1.17.3.4

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **Hotspot2.0-Profile**

Mögliche Werte:

Betriebsklassen-Code, max. 32 Zeichen

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 **ANQP-Profile** einem ANQP-Profil zu.

SNMP-ID:

2.37.1.17.7

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **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** > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **ANQP-Profile** unter **NAI-Realm-List** an.

SNMP-ID:

2.37.1.17.7.1

Pfad Telnet:

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

2.37.1.17.7.2

Pfad Telnet:

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

2.37.1.17.7.3

Pfad Telnet:

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

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:

2.37.1.17.7.4

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **NAI-Realms**

Mögliche Werte:

Name aus Tabelle **Setup** > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **Auth-Parameter**, max. 65 Zeichen. Mehrere Namen trennen Sie durch eine kommaseparierte Liste.

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.

Den Namen des Network-Authentication-Type-Profils geben Sie später in der Tabelle **ANQP-Profile** unter **Network-Auth-Type-List** an.

SNMP-ID:

2.37.1.17.4

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u**

Name

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

SNMP-ID:

2.37.1.17.4.1

Pfad Telnet:

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

2.37.1.17.4.2

Pfad Telnet:

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

2.37.1.17.4.3

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **Network-Authentication-Type**

Mögliche Werte:

URL, max. 65 Zeichen

Default:

Netzwerk-Profile

Die Tabelle **Netzwerk-Profile** ist die höchste Verwaltungsebene für 802.11u und Hotspot 2.0. Hier haben Sie die Möglichkeit, die Funktionen für jedes angelegte Profil ein- oder auszuschalten, Ihnen nachgelagerte Profillisten (wie z. B. für ANQP oder HS20) zuzuweisen oder allgemeine Einstellungen vorzunehmen.

SNMP-ID:

2.37.1.17.1

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u**

Name

Über diesen Parameter vergeben Sie einen Namen für das 802.11u-Profil. Dieses Profil weisen Sie anschließend in der Tabelle **Setup** > **WLAN-Management** > **AP-Konfiguration** > **Netzwerkprofile** unter **802.11u-Profil** einem logischen WLAN-Netzwerk zu.

SNMP-ID:

2.37.1.17.1.1

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **Netzwerk-Profile**

Mögliche Werte:

String, max. 32 Zeichen

Default:

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 802.11u-fähige Geräte als erste Filterkriterien bei der Netzsuche.

SNMP-ID:

2.37.1.17.1.2

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **Netzwerk-Profile**

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:

2.37.1.17.1.3

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **Netzwerk-Profile**

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:

2.37.1.17.1.4

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **Netzwerk-Profile**

Mögliche Werte:

ja

nein

Default:

nein

Network-Type

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

SNMP-ID:

2.37.1.17.1.5

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **Netzwerk-Profile**

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:

2.37.1.17.1.6

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **Netzwerk-Profile**

Mögliche Werte:

ja

nein

Default:

nein

HESSID-Type

Geben Sie an, welche HESSID das Gerät für das homogene ESS an die Access Points übermittelt.

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) oder die MAC-Adresse des WLCs. 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:

2.37.1.17.1.7

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **Netzwerk-Profile**

Mögliche Werte:

- **auto**: Das Gerät generiert für alle Access Points des betreffenden Netzwerkprofils eine gemeinsame HESSID, basierend auf seiner eigenen MAC-Adresse.
- **user**: Vergeben Sie manuell eine HESSID für alle Access Points des betreffenden Netzwerkprofils.
- **none**: Die angeschlossenen Access Points bekommen keine HESSID zugewiesen.

Default:

auto

HESSID-MAC

Sofern Sie als **HESSID-Type** 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 Points in Ihrem homogenen ESS oder die MAC-Adresse des WLCs in Großbuchstaben und ohne Trennzeichen, z. B. `008041AEFD7E` für die MAC-Adresse 00:80:41:ae:fd:7e.

Sofern ein Access Point nicht in mehreren homogenen ESS vertreten ist, ist die HESSID für alle seine Schnittstellen identisch!

SNMP-ID:

2.37.1.17.1.8

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **Netzwerk-Profile**

Mögliche Werte:

MAC-Adresse, in Großbuchstaben und ohne Trennzeichen

Default:

000000000000

ANQP-Profil

Über diesen Parameter spezifizieren Sie ein gültiges ANQP-Profil, das Sie für das 802.11u-Profil verwenden wollen.

SNMP-ID:

2.37.1.17.1.10

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **Netzwerk-Profile**

Mögliche Werte:

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

Default:

HS20-Profil

Über diesen Parameter spezifizieren Sie ein gültiges Hotspot-2.0- bzw. HS20-Profil, das Sie für das 802.11u-Profil verwenden wollen.

SNMP-ID:

2.37.1.17.1.10

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **Netzwerk-Profile**

Mögliche Werte:

Name aus Tabelle **Setup** > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **Hotspot2.0-Profile**, 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:

2.37.1.17.8

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u**

Name

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

SNMP-ID:

2.37.1.17.8.1

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **Operator-List**

Mögliche Werte:

String, max. 32 Zeichen

Default:

Language

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

SNMP-ID:

2.37.1.17.8.1

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **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:

2.37.1.17.8.3

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **Operator-List**

Mögliche Werte:

String, max. 65 Zeichen

Default:

Venue-Name

In diese Tabelle geben Sie allgemeine Informationen zum Standort eines 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:

2.37.1.17.6

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u**

Name

Tragen Sie einen Namen für den Listeneintrag in der Tabelle ein, über den Sie auf die angelegten Standortinformationen aus anderen Tabellen referenzieren.

SNMP-ID:

2.37.1.17.6.1

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **Venue-Name**

Mögliche Werte:

String, max. 65 Zeichen

Default:

Language

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

SNMP-ID:

2.37.1.17.6.2

Pfad Telnet:

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

2.37.1.17.6.3

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **Venue-Name**

Mögliche Werte:

String, max. 65 Zeichen

Default:

IEEE802.11u-Netzwerk-Profil

Über diesen Parameter spezifizieren Sie den Namen eines 802.11u-Netzwerk-Pofils, welches Sie dem logischen WLAN-Netzwerk zuweisen möchten.

SNMP-ID:

2.37.1.1.39

Pfad Telnet:

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

Mögliche Werte:

Name aus Tabelle **Setup** > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **Netzwerk-Profile**, max. 32 Zeichen

Default:

IEEE802.11u-General

Über diesen Parameter spezifizieren Sie den Namen des Standortprofils, das für das WLAN-Profil (also das hiesige Gesamtprofil) gelten sollen.

SNMP-ID:

2.37.1.3.6

Pfad Telnet:

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

Mögliche Werte:

Name aus Tabelle **Setup** > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **General**, max. 32 Zeichen

Default:

9 Public Spot

9.1 Beliebiges Rufnummernformat bei Smart Ticket

Ab LCOS 8.84 haben Nutzer von Smart Ticket die Möglichkeit, beim Anfordern der Anmeldedaten über SMS Ihre Rufnummer in einem beliebigen Format anzugeben (0049…/+49…/etc.). Das Gerät entfernt dabei führende Nullen oder ein führendes '+'-Zeichen automatisch und speichert die Rufnummer in einem standardisierten Format (49…) in der RADIUS-Benutzertabelle.

9.2 Versand der Anmeldedaten über ein GSM-fähiges Gerät (Smart-Ticket)

Ab LCOS 8.84 haben Sie die Möglichkeit, den Versand der Anmeldedaten im Anmeldungsmodus **Anmeldedaten werden über SMS versendet**

- direkt über ein geräteeigenes 3G/4G WWAN-Modul;
- das 3G/4G WWAN-Modul eines anderen Gerätes

anstelle eines externen E-Mail2SMS-Gateways abzuwickeln.

9.2.1 SMS-Anmeldung konfigurieren

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

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

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

Für den erfolgreichen Versand der Anmeldedaten als Kurznachricht durch ein 3G/4G WWAN-fähiges Gerät muss unter **Meldungen** > **SMS-Nachrichten** dessen internes SMS-Modul eingerichtet sein (siehe *Basiskonfiguration des SMS-Moduls* auf Seite 149).

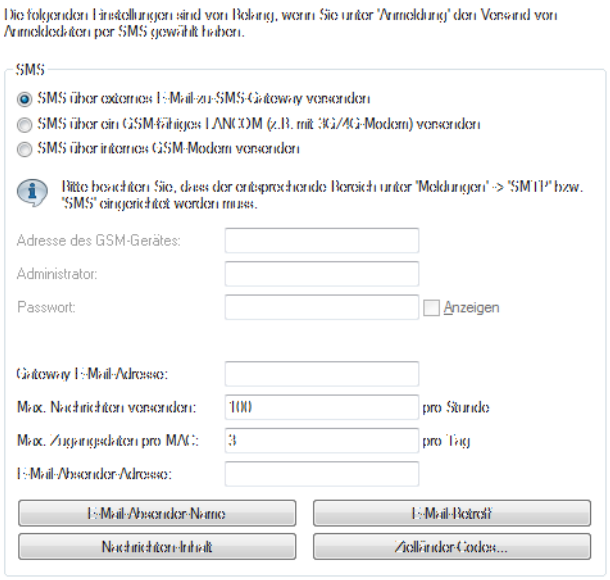
Der SMS-Versand eignet sich für Installationen mit einem maximalen Durchsatz von 10 SMS pro Minute.

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

Darüber hinaus haben Sie in dem Dialog auch die Möglichkeit, individuelle Texte festzulegen, die das Gerät für den Versand der Anmeldedaten nutzt; siehe *Nachrichtentexte anpassen* auf Seite 121. Standardmäßig setzt das Gerät vordefinierte Textbausteine ein; eine Übersicht dieser Standardtexte finden Sie unter *Standardtexte für E-Mail-Absender, -Betreff und -Inhalt* auf Seite 122.

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

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



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

   - Für den Versand der Anmeldedaten als SMS über das geräteeigene 3G/4G WWAN-Modul, wählen Sie die Einstellung **SMS über internes GSM-Modem versenden** und fahren anschließend mit dem nächsten Konfigurations-Hauptschritt fort.
   - Für den Versand der Anmeldedaten als SMS über das 3G/4G WWAN-Modul eines anderen Gerätes, führen Sie zunächst die Schritte im Abschnitt *Geräte mit 3G/4G WWAN-Modul als SMS-Gateway einsetzen* auf Seite 114 aus und fahren anschließend mit dem nächsten Konfigurations-Hauptschritt fort.
   - Für Versand der Anmeldedaten als E-Mail an ein externes E-Mail2SMS-Gateway, wählen Sie die Einstellung **SMS über externes E-Mail-zu-SMS-Gateway versenden** und fahren im Anschluss an die nachstehenden Unterschritte mit dem nächsten Konfigurations-Hauptschritt fort.

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

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

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

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

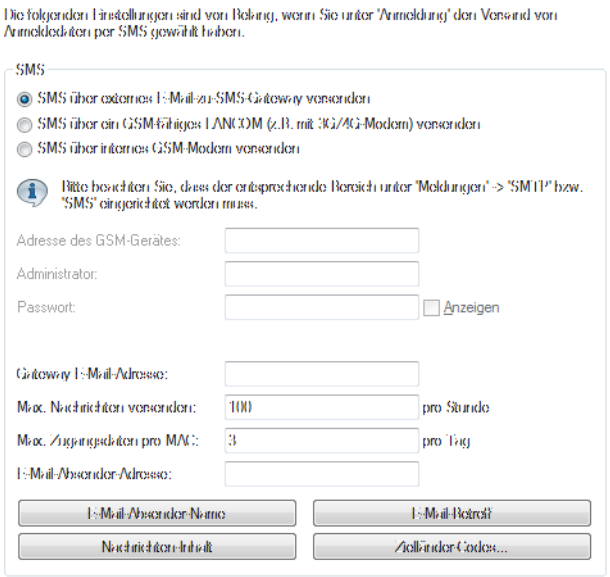
9. Schreiben Sie die Konfiguration zurück auf das Gerät.

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

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

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

1. Starten Sie LANconfig und richten Sie auf dem 3G/4G-Gerät, das als SMS-Gateway fungieren soll, dass SMS-Modul ein (siehe *Basiskonfiguration des SMS-Moduls* auf Seite 149). Darüber hinaus empfiehlt es sich, für den Zugang einen separaten Administrator ohne Zugriffsrechte (Auswahl **Keine**) mit dem alleinigen Funktionsrecht **Senden von SMS** anzulegen.
2. Öffnen Sie den Konfigurationsdialog für das Gerät, das den Public Spot bereitstellt.
3. Wechseln Sie in die Ansicht **Public-Spot** > **SMS**.



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

9.2.2 Ergänzungen im Setup-Menü

SMS-Senden

Über diesen Parameter legen Sie fest, auf welche Art und Weise der SMS-Versand erfolgt. Dabei können Sie – je nach Gerätetyp – zwischen mehreren Varianten wählen.

Für den erfolgreichen Versand der Anmeldedaten als Kurznachricht durch ein 3G/4G WWAN-fähiges Gerät muss unter **Setup** > **SMS** dessen internes SMS-Modul eingerichtet sein.

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

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

SNMP-ID:

2.24.41.2.15

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **E-Mail2Sms-Authentifizierung**

Mögliche Werte:

Direkt-Senden

Versand der Anmeldedaten als SMS über das geräteeigene 3G/4G WWAN-Modul.

HTTP2SMS

Versand der Anmeldedaten als SMS über das 3G/4G WWAN-Modul eines anderen Gerätes

Sie haben bei der Public Spot-Anmeldung via SMS die Möglichkeit, den Versand der Zugangsdaten über ein anderes LANCOM-Gerät mit 3G/4G WWAN-Modul abzuwickeln. Dazu hinterlegen Sie im Gerät, das den Public Spot bereitstellt, die Adresse und die Zugangsdaten des anderen Gerätes. Für den Versand der SMS meldet sich das Public Spot-Modul am anderen Gerät an und initiiert über die aufgerufene URL den Versand der Kurznachricht durch das fremde 3G/4G WWAN-Modul.

Stellen Sie sicher, dass das SMS-Modul auf dem anderen Gerät korrekt konfiguriert ist. Darüber hinaus empfiehlt es sich, für den Zugang einen separaten Administrator ohne Zugriffsrechte (Auswahl **Keine**) mit dem alleinigen Funktionsrecht **Senden von SMS** anzulegen.

SMS-Gateway

Versand der Anmeldedaten als E-Mail an ein externes E-Mail2SMS-Gateway, welches die Umwandlung der E-Mail in eine SMS übernimmt.

Default-Wert:

SMS-Gateway

HTTP-Benutzername

Über diesen Parameter geben Sie den Benutzernamen an, mit dem sich Ihr Gerät an einem anderen LANCOM-Gerät anmeldet.

SNMP-ID:

2.24.41.2.16

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **E-Mail2Sms-Authentifizierung**

Mögliche Werte:

max. 16 Zeichen aus `[0-9][A-Z][a-z] @{|}~!$%&'()+-,/:;<=>?[\]^_.#*``

Default-Wert:

leer

HTTP-Passwort

Über diesen Parameter geben Sie das Passwort für den Benutzernamen an, mit dem sich Ihr Gerät an einem anderen LANCOM-Gerät anmeldet.

SNMP-ID:

2.24.41.2.17

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **E-Mail2Sms-Authentifizierung**

Mögliche Werte:

max. 16 Zeichen aus `[0-9][A-Z][a-z] @{|}~!$%&'()+-,/:;<=>?[\]^_.#*``

Default-Wert:

leer

HTTP-Gateway-Adresse

Über diesen Parameter geben Sie die IP-Adresse des anderen LANCOM-Gerätes an, welches Sie für den SMS-Versand verwenden wollen.

SNMP-ID:

2.24.41.2.18

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **E-Mail2Sms-Authentifizierung**

Mögliche Werte:

Gültige IPv4-/IPv6-Adresse, max. 15 Zeichen aus `[0-9][A-F][a-f]:./`

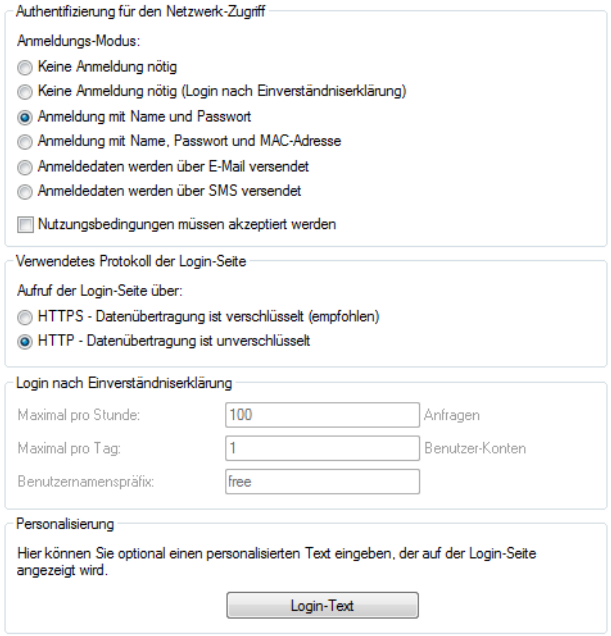
Default-Wert:

leer

9.3 Nutzungsbedingungen bei Anmeldung mit Name, Password (und MAC-Adresse)

Mit LCOS 8.84 steht Ihnen auch für die Anmeldungsmodi **Anmeldung mit Name und Passwort** und **Anmeldung mit Name, Passwort und MAC-Addresse** die bereits von der Smart Ticket-Anmeldung bekannte Bestätigung von Nutzungsbedingungen zur Verfügung. Auf diese Weise haben Sie z. B. die Möglichkeit, auch die Anmeldung über Voucher an die Bestätigung von Nutzungsbedingungen zu koppeln, bevor ein Nutzer den Netzzugriff über den Public Spot erlangt.

In LANconfig schalten Sie die Bestätigung von Nutzungsbedingungen in bestimmten Anmeldungsmodi zukünftig im Dialog **Public-Spot** > **Anmeldung** unter **Nutzungsbedingungen müssen akzeptiert werden** ein oder aus.



9.3.1 Ergänzungen im Setup-Menü

Benutzer-muss-AGBs-akzeptieren

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

Folgende Anmeldungsmodi lassen sich an die Anerkennung von Nutzungsbedingungen koppeln:

- Benutzer+Passwort
- MAC+Benutzer+Passwort
- E-Mail
- E-Mail2SMS

Denken Sie daran, eine individuelle Seitenvorlage in das Gerät zu laden, bevor Sie eine Bestätigung von Nutzungsbedingungen einfordern.

SNMP-ID:

2.24.36

Pfad Telnet:

Setup > **Public-Spot-Modul**

Mögliche Werte:

nein

ja

Default:

nein

9.4 Erweiterte Konfiguration der Benutzer-Templates mit LANconfig

Ab LCOS 8.84 haben Sie künftig die Möglichkeit,

- die Konfiguration der Benutzer-Templates für die selbstständige Benutzeranmeldung via E-Mail/SMS – auch bekannt als Smart Ticket –, sowie
- die Verwaltung der Max-gleichzeitige-Logins-Tabelle für den Benutzer-Erstellungs-Assistenten (Setup-Wizard **Public-Spot-Benutzer einrichten**)

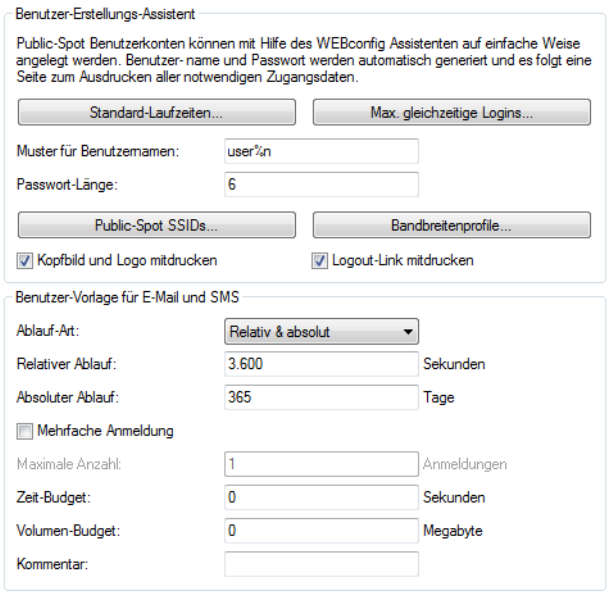
direkt in LANconfig unter **Public-Spot** > **Assistent** vorzunehmen.

9.4.1 Standardwerte für den Public Spot-Assistenten setzen

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

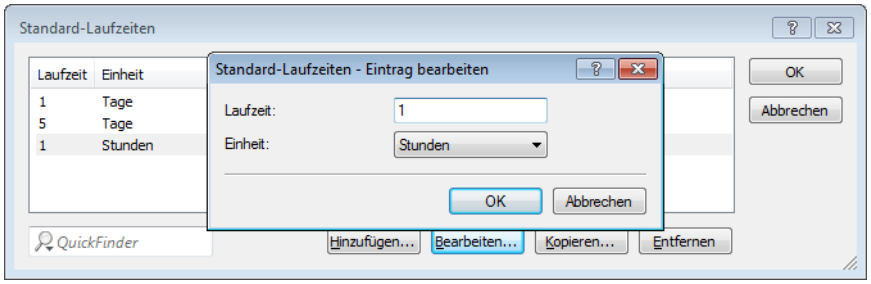
Ausgenommen davon sind die im untenstehenden Dialog abgebildeten Werte für Muster für Benutzernamen und Passwort-Länge, welche ausschließlich dem Gerät als Vorgabewerte dienen.

1. Starten Sie LANconfig und öffnen Sie den Konfigurationsdialog für das Gerät.
2. Wechseln Sie in die Ansicht **Public-Spot** > **Assistent**.

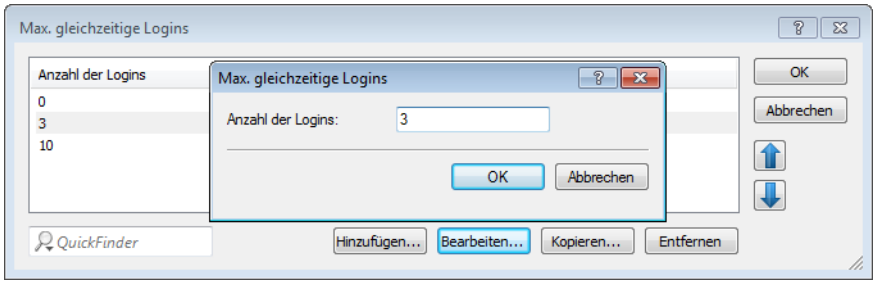


3. Definieren Sie unter **Standard-Laufzeiten**, welche auswählbaren Gültigkeiten von Benutzerkonten und Vouchern der Assistent standardmäßig anbietet.

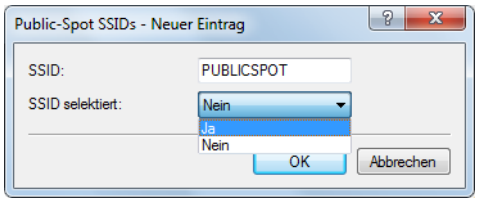
Der Benutzer-Erstellungs-Assistent verwendet die kürzeste Laufzeit als Standardwert.



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



5. Legen Sie unter **Muster für Benutzernamen** fest, nach welchem Muster der Benutzer-Erstellungs-Assistent den Benutzernamen erzeugt.
   Sie können bis zu 19 Zeichen vergeben, wobei der Assistent für die Variable "%n" für jeden Benutzer eine eindeutige Nummer vergibt. Für die Standardbezeichnung `user%n` erscheint auf dem Voucher später z. B. `user12345`.
6. Bestimmen Sie unter **Passwort-Länge** die Länge des Passwortes, das der Benutzer-Erstellungs-Assistent für den Public Spot-Zugang generiert.
   Standardmäßig beträgt die Länge 6 Zeichen. Wenn Sie längere Passwörter vergeben möchten, sollten Sie bedenken, dass dem Gast bei deren Eingabe Fehler passieren können, was zu unnötigen Problemen und Rückfragen führt.
7. Optional: Legen Sie unter **Bandbreitenprofile** Grenzen für den Up- und Downlink eines jeden Public Spot-Benutzers fest.
8. Nur Public Spot über WLAN: Bestimmen Sie unter **Public-Spot SSIDs** die Namen der Public Spot-Netzwerke, für die Sie mit dem Benutzer-Erstellungs-Assistent Benutzerkonten standardmäßig anlegen.



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

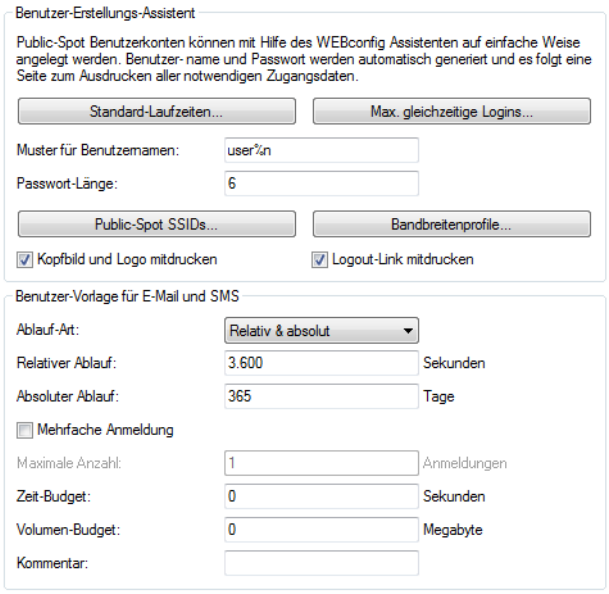
Über die Pfeil-Schaltflächen ändern Sie die Reihenfolge der angezeigten SSIDs. Oft genutzte SSIDs können Sie damit z. B. an die oberen Positionen verschieben.

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

9.4.2 Standardwerte für die Benutzer-Vorlage setzen

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

1. Starten Sie LANconfig und öffnen Sie den Konfigurationsdialog für das Gerät.
2. Wechseln Sie in die Ansicht **Public-Spot** > **Assistent**.



3. Füllen Sie die Eingabefelder im Abschnitt **Benutzer-Vorlage** entsprechend Ihren Vorstellungen aus:
   - **Ablauf-Art**: Über diesen Eintrag definieren Sie, auf welche Art ein automatisch angelegtes Public Spot-Benutzerkonto abläuft. Sie können festlegen, ob die Gültigkeitsdauer eines Benutzer-Accounts absolut (fester Zeitpunkt) und/oder relativ (Zeitspanne ab dem ersten erfolgreichen Login) ist. Wenn Sie beide Werte auswählen, hängt der Ablaufzeitpunkt davon ab, welcher Fall als Erstes eintritt.
   - **Relativer Ablauf**: Über diesen Eintrag definieren Sie die relative Ablaufzeit eines automatisch angelegten Benutzerkontos (in Sekunden). Der von Ihnen gewählte **Ablauf-Typ** muss ein `relativ` beinhalten, damit diese Einstellung greift. Die Gültigkeit des Kontos endet nach der in diesem Feld angegebenen Zeitspanne nach dem ersten erfolgreichen Login des Benutzers.
   - **Absoluter Ablauf**: Über diesen Eintrag definieren Sie die absolute Ablaufzeit eines automatisch angelegten Benutzerkontos (in Tagen). Die von Ihnen gewählte **Ablauf-Art** muss ein `absolut` beinhalten, damit diese Einstellung greift. Die Gültigkeit des Kontos endet zu dem in diesem Feld angegebenen Zeitpunkt, hochgerechnet vom Tag der Kontoerstellung.
   - **Mehrfache Anmeldung**: Über diesen Eintrag erlauben bzw. verbieten Sie ganz allgemein, ob Nutzer eines automatisch erstellten Accounts mehrere Geräte gleichzeitig mit den selben Zugangsdaten am Public Spot anmelden dürfen. Die erlaubte Menge der gleichzeitig angemeldeten Geräte legen Sie über das Eingabefeld **Maximale Anzahl** fest.
   - **Maximale Anzahl**: Über diesen Eintrag legen Sie die maximale Anzahl der Geräte fest, die gleichzeitig unter einem automatisch erstellten Account angemeldet sein dürfen. Der Wert `0` steht dabei für 'unbegrenzt'. Damit diese Einstellung greift, muss gleichzeitig der Parameter **Mehrfache Anmeldung** aktiviert sein.
   - **Zeit-Budget**: Über diesen Eintrag definieren Sie das Zeit-Budget, welches automatisch angelegte Benutzer erhalten. Der Wert `0` deaktiviert die Funktion.

- **Volumen-Budget**: Über diesen Eintrag definieren Sie das Volumen-Budget, welches automatisch angelegte Benutzer erhalten. Der Wert `0` deaktiviert die Funktion.
- **Kommentar**: Über diesen Eintrag vergeben Sie einen Kommentar oder Infotext, mit dem der RADIUS-Server ein automatisch erstelltes Benutzerkonto versieht.

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

9.5 Mehrsprachige(r) Login- und Benachrichtigungstext(e)

Ab LCOS 8.84 haben Sie die Möglichkeit, ausgewählte Texte im LCOS mehrsprachig zu hinterlegen. Folgende Texte werden künftig über Sprachtabellen verwaltet:

- der individuelle Text auf der Anmeldeseite (**Login-Text**; in LANconfig einstellbar unter **Public-Spot** > **Anmeldung**)
- die Standardtexte für E-Mail-Absender, -Betreff und -Inhalt für die Anmeldung über E-Mail/SMS (**E-Mail-Absender-Name**, **E-Mail-Betreff**, **E-Mail-Inhalt**; in LANconfig einstellbar unter **Public-Spot** > **E-Mail/SMS**)

Die Sprachtabellen ergänzen damit die *zusätzlichen Sprachen für Template-Seiten* und funktionieren nach dem selben Prinzip; der vom Gerät gewählte Eintrag in der Sprachtabelle wird durch die Browsersprache bestimmt. Sofern Sie für eine Sprache keinen individuellen Text zu E-Mail-Absender, -Betreff und -Inhalt spezifiziert haben, setzt das Public Spot-Modul die geräteinternen englischen Standardtexte ein (siehe *Standardtexte für E-Mail-Absender, -Betreff und -Inhalt* auf Seite 122). Für den Login-Text sind keine Standardtexte implementiert; hier greift das Gerät direkt auf den individuellen englischen Login-Text zurück (sofern vorhanden).

9.5.1 Nachrichtentexte anpassen

Standardmäßig setzt das Gerät für den Inhalt der versendeten E-Mails oder Kurznachrichten vordefinierte Textbausteine ein; eine Übersicht dieser Standardtexte finden Sie unter *Standardtexte für E-Mail-Absender, -Betreff und -Inhalt* auf Seite 122. Sie haben aber auch die Möglichkeit, eigene Texte zu definieren.

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

1. Starten Sie LANconfig und öffnen Sie den Konfigurationsdialog für das Gerät.
2. Wechseln Sie – je nach gewähltem Anmeldungsmodus – in die Ansicht **Public-Spot** > **E-Mail** bzw. **SMS**.
3. Geben über die Schaltfläche **E-Mail-Absender-Name** zu den verfügbaren Sprachen einen individuellen Absendernamen an, den die vom Public Spot zugestellten E-Mails bzw. Kurznachrichten tragen, z. B. `Provider X`.
4. Geben über die Schaltfläche **E-Mail-Betreff** zu den verfügbaren Sprachen eine individuelle Betreffzeile an, die das Public Spot-Modul für seine E-Mails bzw. Kurznachrichten verwendet. Die dabei zur Verfügungen stehenden Steuerzeichen entnehmen Sie dem Abschnitt *Verfügbare Variablen und Steuerzeichen* auf Seite 122.
5. Geben über die Schaltfläche **E-Mail-Inhalt** bzw. **Nachrichteninhalt** zu den verfügbaren Sprachen einen individuellen Text an, den das Public Spot-Modul für seine E-Mails bzw. Kurznachrichten verwendet. Die dabei zur Verfügungen stehenden Variablen und Steuerzeichen entnehmen Sie dem Abschnitt *Verfügbare Variablen und Steuerzeichen* auf Seite 122.
6. Schreiben Sie die Konfiguration zurück in das Gerät.

Verfügbare Variablen und Steuerzeichen

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

Variablen

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

`$PSpotPasswd`

Platzhalter für das nutzerspezifische Passwort des Public Spot-Zugangs.

`$PSpotLogoutLink`

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

Steuerzeichen

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

`\n`

CRLF (Carriage Return, Line Feed)

`\t`

Tabulator

`\<ASCII>`

ASCII-Code des entsprechenden Zeichens

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

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

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

Tabelle 4: Übersicht der geräteinternen Standardtexte für die Anmeldung über E-Mail/SMS

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

9.5.2 Ergänzungen im Setup-Menü

Name

In dieser Tabelle verwalten Sie die unterschiedlichen Sprachvarianten für den Absender-Namen, welchen das Public Spot-Modul für den Versand der Anmeldedaten via E-Mail verwendet. Sofern Sie für eine Sprache keinen individuellen Text spezifizieren, trägt das Gerät automatisch den geräteinternen Standardtext ein.

SNMP-ID:

2.24.41.1.20

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **E-Mail-Authentifizierung**

Sprache

Dieser Parameter zeigt die Sprachvariante für den individuellen Absender-Namen.

SNMP-ID:

2.24.41.1.20.1

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **E-Mail-Authentifizierung** > **Name**

Inhalt

Über diesen Parameter vergeben Sie den Absender-Namen für die ausgewählte Sprache.

SNMP-ID:

2.24.41.1.20.2

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **E-Mail-Authentifizierung** > **Name**

Mögliche Werte:

Beliebiger String, max. 251 Zeichen aus

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

Default:

Textinhalt

In dieser Tabelle verwalten Sie die unterschiedlichen Sprachvarianten für den Nachrichtentext, welchen das Public Spot-Modul für den Versand der Anmeldedaten via E-Mail verwendet. Sofern Sie für eine Sprache keinen individuellen Text spezifizieren, trägt das Gerät automatisch den geräteinternen Standardtext ein.

SNMP-ID:

2.24.41.1.21

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **E-Mail-Authentifizierung**

Sprache

Dieser Parameter zeigt die Sprachvariante für den individuellen Nachrichtentext.

SNMP-ID:

2.24.41.1.21.1

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **E-Mail-Authentifizierung** > **Textinhalt**

Inhalt

Über diesen Parameter vergeben Sie den Nachrichtentext für die ausgewählte Sprache. Dabei stehen Ihnen verschiedene Variablen und Steuerzeichen zur Verfügung. Die Variablen werden vom Public Spot-Modul beim Versand der E-Mail an den Benutzer automatisch mit Werten gefüllt.

Folgende **Variablen** stehen Ihnen zur Verfügung:

`$PSpotPasswd`

Platzhalter für das nutzerspezifische Passwort des Public Spot-Zugangs.

`$PSpotLogoutLink`

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

Folgende **Steuerzeichen** stehen Ihnen zur Verfügung:

`\n`

CRLF (Carriage Return, Line Feed)

`\t`

Tabulator

`\<ASCII>`

ASCII-Code des entsprechenden Zeichens

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

SNMP-ID:

2.24.41.1.21.2

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **E-Mail-Authentifizierung** > **Textinhalt**

Mögliche Werte:

Beliebiger String, max. 251 Zeichen aus

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

Default:

Betreffzeile

In dieser Tabelle verwalten Sie die unterschiedlichen Sprachvarianten für die Betreffzeile, welche das Public Spot-Modul für den Versand der Anmeldedaten via E-Mail verwendet. Sofern Sie für eine Sprache keinen individuellen Text spezifizieren, trägt das Gerät automatisch den geräteinternen Standardtext ein.

SNMP-ID:

2.24.41.1.22

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **E-Mail-Authentifizierung**

Sprache

Dieser Parameter zeigt die Sprachvariante für den individuellen Betreffzeilen-Text.

SNMP-ID:

2.24.41.1.22.1

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **E-Mail-Authentifizierung** > **Betreffzeile**

Inhalt

Über diesen Parameter vergeben Sie den Betreffzeilen-Text für die ausgewählte Sprache. Dabei stehen Ihnen folgende Steuerzeichen zur Verfügung:

`\n`

CRLF (Carriage Return, Line Feed)

`\t`

Tabulator

`\<ASCII>`

ASCII-Code des entsprechenden Zeichens

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

SNMP-ID:

2.24.41.1.22.2

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **E-Mail-Authentifizierung** > **Betreffzeile**

Mögliche Werte:

Beliebiger String, max. 251 Zeichen aus

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

Default:

Name

In dieser Tabelle verwalten Sie die unterschiedlichen Sprachvarianten für den Absender-Namen, welchen das Public Spot-Modul für den Versand der Anmeldedaten via E-Mail2SMS verwendet. Sofern Sie für eine Sprache keinen individuellen Text spezifizieren, trägt das Gerät automatisch den geräteinternen Standardtext ein.

SNMP-ID:

2.24.41.2.23

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **E-Mail2Sms-Authentifizierung**

Sprache

Dieser Parameter zeigt die Sprachvariante für den individuellen Absender-Namen.

SNMP-ID:

2.24.41.2.23.1

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **E-Mail2Sms-Authentifizierung** > **Name**

Inhalt

Über diesen Parameter vergeben Sie den Absender-Namen für die ausgewählte Sprache.

SNMP-ID:

2.24.41.2.23.2

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **E-Mail2Sms-Authentifizierung** > **Name**

Mögliche Werte:

Beliebiger String, max. 251 Zeichen aus

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

Default:

Textinhalt

In dieser Tabelle verwalten Sie die unterschiedlichen Sprachvarianten für den Nachrichtentext, welchen das Public Spot-Modul für den Versand der Anmeldedaten via E-Mail2SMS verwendet. Sofern Sie für eine Sprache keinen individuellen Text spezifizieren, trägt das Gerät automatisch den geräteinternen Standardtext ein.

SNMP-ID:

2.24.41.2.24

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **E-Mail2Sms-Authentifizierung**

Sprache

Dieser Parameter zeigt die Sprachvariante für den individuellen Nachrichtentext.

SNMP-ID:

2.24.41.2.24.1

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **E-Mail2Sms-Authentifizierung** > **Textinhalt**

Inhalt

Über diesen Parameter vergeben Sie den Nachrichtentext für die ausgewählte Sprache. Dabei stehen Ihnen verschiedene Variablen und Steuerzeichen zur Verfügung. Die Variablen werden vom Public Spot-Modul beim Versand der E-Mail an das SMS-Gateway automatisch mit Werten gefüllt.

Folgende **Variablen** stehen Ihnen zur Verfügung:

`$PSpotPasswd`

Platzhalter für das nutzerspezifische Passwort des Public Spot-Zugangs.

`$PSpotLogoutLink`

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

Folgende **Steuerzeichen** stehen Ihnen zur Verfügung:

`\n`

CRLF (Carriage Return, Line Feed)

`\t`

Tabulator

`\<ASCII>`

ASCII-Code des entsprechenden Zeichens

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

SNMP-ID:

2.24.41.2.24.2

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **E-Mail2Sms-Authentifizierung** > **Textinhalt**

Mögliche Werte:

Beliebiger String, max. 251 Zeichen aus

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

Default:

Betreffzeile

In dieser Tabelle verwalten Sie die unterschiedlichen Sprachvarianten für die Betreffzeile, welche das Public Spot-Modul für den Versand der Anmeldedaten via E-Mail2SMS verwendet. Sofern Sie für eine Sprache keinen individuellen Text spezifizieren, trägt das Gerät automatisch den geräteinternen Standardtext ein.

SNMP-ID:

2.24.41.2.25

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **E-Mail2Sms-Authentifizierung**

Sprache

Dieser Parameter zeigt die Sprachvariante für den individuellen Betreffzeilen-Text.

SNMP-ID:

2.24.41.2.25.1

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **E-Mail2Sms-Authentifizierung** > **Betreffzeile**

Inhalt

Über diesen Parameter vergeben Sie den Betreffzeilen-Text für die ausgewählte Sprache. Dabei stehen Ihnen folgende Steuerzeichen zur Verfügung:

`\n`

CRLF (Carriage Return, Line Feed)

`\t`

Tabulator

`\<ASCII>`

ASCII-Code des entsprechenden Zeichens

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

SNMP-ID:

2.24.41.2.25.2

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **E-Mail2Sms-Authentifizierung** > **Betreffzeile**

Mögliche Werte:

Beliebiger String, max. 251 Zeichen aus

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

Default:

Login-Text

Über diese Tabelle verwalten Sie die Login-Texte.

Sie haben innerhalb des Public Spot-Moduls die Möglichkeit, einen individuellen Text anzugeben, welcher auf der Anmeldeseite innerhalb der Box des Anmeldeformulars eingeblendet wird. Dieser **Login-Text** ist in mehreren Sprachen hinterlegbar; welche Sprache das Gerät letztlich ausgibt, hängt von den Spracheinstellungen des vom Benutzer verwendeten Webbrowsers ab. Wenn Sie für eine Sprache keinen individuellen Login-Text spezifizieren, greift das Gerät auf den englischen Login-Text zurück (sofern vorhanden).

SNMP-ID:

2.24.60

Pfad Telnet:

Setup > **Public-Spot-Modul**

Sprache

Dieser Parameter zeigt die Sprache, für die Sie einen Login-Text vergeben.

SNMP-ID:

2.24.60.1

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Login-Text**

Inhalt

Über diesen Parameter vergeben Sie einen Login-Text für die ausgewählte Sprache. 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:

2.24.60.2

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Login-Text**

Mögliche Werte:

Beliebiger String, max. 254 Zeichen aus

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

Default:

9.6 Neue URL-Platzhalter (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.

Ab LCOS 8.84 stehen Ihnen folgende zusätzliche Variablen zur Auswahl:

%c

Fügt die LAN-MAC-Adresse des LANCOM-Gerätes als 12-stelligen Hexadezimal-String ein. Die Ausgabe erfolgt im Format 'aa:bb:cc:dd:ee:ff'.

%p

Fügt die IP-Adresse des LANCOM-Gerätes in dem ARF-Kontext des jeweiligen Clients ein.

Sofern Ihr Gerät also in verschiedenen IP-Netzwerken aktiv ist, können Sie über diese Variable die IP-Adresse angeben, welche das Gerät in dem Netz benutzt, in dem auch der Client anzutreffen ist.

%r

Fügt die IP-Adresse des Clients ein.

9.7 Benutzerabhängige HTML-Ausgabe im Voucher

Ab LCOS 8.84 haben Sie die Möglichkeit, auf der Voucher-Seite konditionalen HTML-Code einzufügen, den das Gerät nur bei bestimmten Benutzern bzw. Administratoren ausgibt. Dazu verwenden Sie den Tag <pbcond> mit dem Bezeichner USER NAME. USER gilt dabei als Präfix und **muss** dem Benutzernamen (NAME) mit einem Leerzeichen vorangestellt werden. Um also bei Aufruf der Voucher-Seite eine HTML-Ausgabe speziell für den Benutzer 'root' zu erzeugen, verwenden Sie die folgende Syntax:

```
<pbcond USER root>Conditional HTML Code</pbcond>
```

In größeren Public Spot-Szenarien mit zentraler Verwaltung – z. B. auf einem WLAN-Controller – lässt sich diese Abhängigkeit auch zur Standortlokalisierung einsetzen: Dazu erstellen Sie für jeden der betreffenden Access Points einen eigenen Public Spot-Admin und spezifizieren für die einzelnen Administratoren einen konditionalen Voucher-Text.

9.8 LANCOM-Logo und -Kopfbild im Voucher ein-/ausblenden

Ein vom Gerät ausgegebener Voucher enthält standardmäßig das Kopfbild "Hotspot" sowie das Logo "Powered by LANCOM". Sie haben die Möglichkeit, die Einbindung dieser Grafiken über die Option **Kopfbild und Logo mitdrucken** direkt im Gerät zu deaktivieren, ohne dafür ein individuell angepasstes Vouchers-Template einzusetzen, welches diese Grafiken entfernt. In dem Fall wird lediglich ein rein textneutraler Voucher auszugeben.

Ob das Gerät beim Erstellen eines Vouchers ein Kopfbild und Logo einblendet, legen Sie im Dialog **Public-Spot** > **Assistent** über die Einstellung **Kopfbild und Logo mitdrucken** fest.

9.8.1 Ergänzungen im Setup-Menü

Drucke-Logo-Und-Kopfbild

Ein vom Gerät ausgegebener Voucher enthält standardmäßig das Kopfbild "Hotspot" sowie das Logo "Powered by LANCOM". Sie haben die Möglichkeit, die Einbindung dieser Grafiken direkt im Gerät zu deaktivieren, ohne dafür einen individuell angepasstes Vouchers-Template hochladen zu müssen, welches diese Grafiken entfernt. Wenn Sie die Grafikausgabe deaktivieren, wird ein reiner Text-Voucher ausgegeben.

SNMP-ID:

2.24.35

Pfad Telnet:

Setup > **Public-Spot-Modul**

Mögliche Werte:

nein

ja

Default:

ja

9.9 Zusätzliche Sprachen für die Authentifizierungsseiten

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

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

9.10 Besondere Template-Seiten für Smart Ticket

Während das Public Spot-Modul in LCOS-Versionen bis 8.82 noch eine zentrale Login-Seite für sämtliche Anmeldemodi verwendet, haben Sie ab LCOS 8.84 die Möglichkeit, für die Smart-Ticket-Funktion (die selbstständige Benutzeranmeldung via E-Mail/SMS) gesonderte Template-Seiten ins Gerät zu laden. Dazu konfigurieren Sie für die Anmeldung über E-Mail/SMS je zwei Seiten: **Registrierung(…)** und **Anmeldung(…)**.

- Auf der Registrierungsseite geben Benutzer zunächst ihre persönlichen Daten (E-Mail-Adresse oder Mobilfunknummer) ein, um sich beim Public Spot zu registrieren und dessen Zugangsdaten anzufordern.
- Auf der Anmeldungsseite geben Benutzer die ihnen zugesendeten Zugangsdaten ein, um sich schlussendlich am Public Spot zu authentisieren.

Die nachfolgende Tabelle liefert Ihnen eine Übersicht aller damit in Verbindung stehenden Abhängigkeiten, die Sie für das erstellen eigener Seitenvorlagen (Templates) benötigen:

Tabelle 5: Übersicht der Abhängigkeiten der SmartTicket-Anmeldeseiten

Anmeldungsmodus	Seitenbezeichnung	Lokale URL im Gerät	Seitenvorlagen-Bezeichner
Anmeldedaten werden über E-Mail versendet	Registrierung(E-Mail)…	file://pbspot_template_reg_email	<regemailform>
	Anmeldung(E-Mail)…	file://pbspot_template_login_email	<loginemailform>
Anmeldedaten werden über SMS versendet	Registrierung(E-Mail zu SMS)…	file://pbspot_template_reg_sms	<regsmsform>
	Anmeldung(E-Mail zu SMS)…	file://pbspot_template_login_sms	<loginsmsform>

9.10.1 Login-Seiten in Abhängigkeit vom Anmeldungsmodus

Die nachfolgende Tabelle liefert Ihnen darüber hinaus eine Übersicht, welche Login-Seite das Gerät in welchem Anmeldungsmodus ausgibt. Sofern für einen Anmeldungsmodus keine individuelle Seitenvorlage eingerichtet ist; verwendet das Public Spot-Modul dafür die LCOS-interne Standardseite:

Tabelle 6: Übersicht der Login-Seiten der einzelnen Anmeldungsmodi

Anmeldungsmodus	Seitenbezeichnung
Keine Anmeldung nötig	–
Keine Anmeldung nötig (Login nach Einverständniserklärung)	Willkommen…
Anmeldung mit Name und Passwort	Anmeldung…
Anmeldung mit Name, Passwort und MAC-Adresse	Anmeldung…

Anmeldungsmodus	Seitenbezeichnung
Anmeldedaten werden über E-Mail versendet	■ Registrierung(E-Mail)… ■ Anmeldung(E-Mail)…
Anmeldedaten werden über SMS versendet	■ Registrierung(E-Mail zu SMS)… ■ Anmeldung(E-Mail zu SMS)…

9.11 Fehlerseite bei Wegfall der WAN-Verbindung einrichten

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

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

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

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

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

9.11.1 Ergänzungen im Setup-Menü

WAN-Verbindung

Über diesen Parameter benennen Sie die Gegenstelle, deren Verbindungsstatus das Public Spot-Modul überwacht, um bei Wegfall der WAN-Verbindung eine entsprechende Meldung auf der Fehlerseite gegenüber unauthentifizierten Benutzern anzuzeigen. Dadurch werden mögliche Benutzer bereits vorab über die fehlende Verfügbarkeit des Netzwerks informiert.

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

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

SNMP-ID:

2.24.34

Pfad Telnet:

Setup > **Public-Spot-Modul**

Mögliche Werte:

Gültiger Name einer Gegenstelle, max. 16 Zeichen

Default:

9.12 Template Caching

Bei der Konfiguration benutzerdefinierter Template-Seiten haben Sie auf Geräten mit hinreichend großem Arbeitsspeicher (z. B. Public Spot-Gateways) die Möglichkeit, Templates im Gerät zu cachen. Das Caching verbessert die Performance des Public Spot-Moduls insbesondere in größeren Szenarien, indem das Gerät einmal geladene Templates und daraus erzeugte HTML-Seiten intern zwischenspeichert.

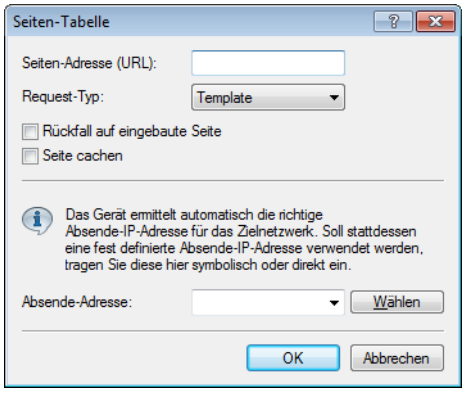
Das Caching ist möglich für:

- Templates abgelegt im lokalen Dateisystem
- Templates abgelegt auf externen HTTP(S)-Servern über statische URLs

Templates auf externen Servern, die mittels Template-Variablen referenziert werden, werden vom Gerät nicht gecached.

Template Caching aktivieren

Um das Caching für eine Seitenvorlage zu aktivieren, setzen Sie in LANconfig unter **Public-Spot** > **Server** > **Seiten-Tabelle** > **<Name der Vorlageseite>** die Einstellung **Seite cachen**.



Im Setup-Menü finden Sie den dazugehörigen Paramter unter **Public-Spot-Modul** > **Seitentabelle** > **Template-Cache** .

Template Cache löschen

Das Gerät löscht bzw. aktualisiert im Cache gespeicherte Templates automatisch, sobald Sie eine neue Template-Datei in das Dateisystem Ihres Gerätes laden (bei lokaler Speicherung) bzw. die Cache-Zeit für ein HTTP(S)-Template abläuft (bei Speicherung auf externem einem Server). Hierzu wertet das Gerät den `Cache-Control`-Header eines HTTP(S)-Templates aus, um die maximale Cache-Zeit zu erfahren.

Sofern kein `Cache-Control`-Header gesetzt ist, wird die Webseite nicht gecached und direkt wieder verworfen. Achten Sie beim Einrichten eines individuellen Templates somit darauf, das entsprechende META-Tag in Verbindung mit einer sinnvollen Cache-Zeit (in Sekunden) zu setzen, z. B. `<meta http-equiv="cache-control" content="max-age=60">`. Die Dauer der Cache-Zeit ist dabei vom Szenario abhängig; es gibt keine konkreten Empfehlungen.

Sie haben aber auch die Möglichkeit, den Template Cache über eine Aktion manuell zu löschen. Starten Sie dazu im Status-Menü unter **Public-Spot** die Aktion **Flush-Template-Cache**.

9.12.1 Ergänzungen im Status-Menü

Flush-Template-Cache

Über diese Aktion veranlassen Sie manuell die Löschung des Template Caches.

Das Gerät löscht bzw. aktualisiert im Cache gespeicherte Templates automatisch, sobald Sie eine neue Template-Datei in das Dateisystem Ihres Gerätes laden (bei lokaler Speicherung) bzw. die Cache-Zeit für ein HTTP(S)-Template abläuft (bei Speicherung auf externem einem Server). Hierzu wertet das Gerät den `Cache-Control`-Header eines HTTP(S)-Templates aus, um die maximale Cache-Zeit zu erfahren.

SNMP-ID:

1.44.9

Pfad Telnet:

Setup > **Public-Spot**

9.12.2 Ergänzungen im Setup-Menü

Template-Cache

Über diesen Parameter aktivieren Sie das Caching von Public Spot-Templates.

Bei der Konfiguration benutzerdefinierter Template-Seiten haben Sie auf Geräten mit hinreichend großem Arbeitsspeicher (z. B. Public Spot-Gateways) die Möglichkeit, Templates im Gerät zu cachen. Das Caching verbessert die Performance des Public Spot-Moduls insbesondere in größeren Szenarien, indem das Gerät einmal geladene Templates und daraus erzeugte HTML-Seiten intern zwischenspeichert.

Das Caching ist möglich für:

- Templates abgelegt im lokalen Dateisystem
- Templates abgelegt auf externen HTTP(S)-Servern über statische URLs

Templates auf externen Servern, die mittels Template-Variablen referenziert werden, werden vom Gerät nicht gecached.

SNMP-ID:

2.24.8.6

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Seitentabelle**

Mögliche Werte:

nein

ja

Default:

nein

9.13 Quick-Link zum Sitzungsinformations-Fenster

Ab LCOS 8.84 haben am Public Spot angemeldete Nutzer die Möglichkeit, durch Eingabe der Kurz-URL `http://logout` in der Adresszeile das Sitzungsinformations-Fenster aufzurufen und sich darüber vom Public Spot abzumelden. Sollte ein Nutzer das Browserfenster z. B. versehentlich oder aus Platzgründen bewusst geschlossen haben, kann er die Seite über die Kurz-URL rasch wiederherstellen.

9.13.1 Ergänzungen im Setup-Menü

Drucke-Logout-Link

Über diesen Parameter legen Sie fest, ob das Gerät beim Erstellen eines Vouchers die URL für die Abmeldung vom Public Spot auf dem Voucher hinterlegt.

Damit die korrekte URL auf dem Voucher erscheint, muss für den Parameter **Geraete-Hostname** (SNMP-ID 2.24.22) der Wert `logout` eingetragen sein.

SNMP-ID:

2.24.37

Pfad Telnet:

Setup > **Public-Spot-Modul**

Mögliche Werte:

nein

ja

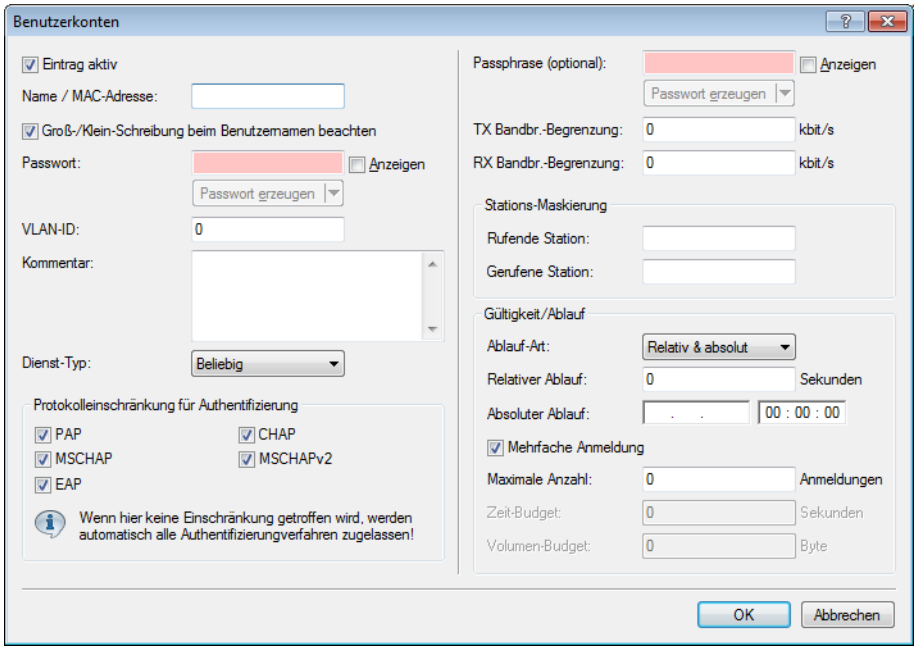
Default:

ja

10 RADIUS

10.1 RADIUS-Benutzerkonten gezielt (de)aktivieren

Ab LCOS 8.84 haben Sie die Möglichkeit, einzelne RADIUS-Benutzerkonten gezielt zu aktivieren bzw. deaktivieren. In LANconfig erfolgt dies unter **RADIUS-Server** > **Allgemein** > **Benutzerkonten** über die Option **Eintrag aktiv**. Auf diese Weise lassen sich z. B. einzelne Benutzerkonten temporär abschalten, ohne dafür das komplette Konto zu löschen.



10.1.1 Ergänzungen im Setup-Menü

aktiv

Über diesen Parameter aktivieren bzw. deaktivieren Sie gezielt einzelne RADIUS-Benutzerkonten. Auf diese Weise lassen sich z. B. einzelne Benutzerkonten temporär abschalten, ohne dafür das komplette Konto zu löschen.

SNMP-ID:

2.25.10.7.20

Pfad Telnet:

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

Mögliche Werte:

Nein

Ja

Default:

Ja

10.2 Über RADIUS in die LCOS-Verwaltungsoberfläche einloggen

Ab LCOS-Version 8.84 besteht zusätzlich zu TACACS+ die Möglichkeit, sich über RADIUS in die Verwaltungsoberfläche des LANCOM einzuloggen.

10.2.1 Über RADIUS in die LCOS-Verwaltungsoberfläche einloggen

Aktuell existieren drei Methoden, sich in die Verwaltungsoberfläche des LANCOM einzuloggen:

- intern: Das LANCOM übernimmt die komplette Benutzerverwaltung mit Anmeldename, Passwort sowie Zugriffs- und Funktionsrechte-Zuordnung.
- TACACS+: Die Benutzerverwaltung erfolgt über einen TACACS+-Server im Netzwerk.
- RADIUS: Die Benutzerverwaltung erfolgt über einen RADIUS-Server im Netzwerk.

Mit RADIUS kann sich der Benutzer über die folgenden Verbindungen einloggen:

- Telnet
- SSH
- WEBconfig
- TFTP
- Outband

Eine RADIUS-Authentifizierung über SNMP ist derzeit nicht unterstützt.

Eine RADIUS-Authentifizierung über LL2M (LANCOM Layer 2 Management Protokoll) ist nicht unterstützt, da LL2M Klartext-Zugriff auf das im LANCOM gespeicherte Passwort benötigt.

Der RADIUS-Server übernimmt die Verwaltung der Benutzer in den Bereichen Authentifizierung, Authorisierung und Accounting (Triple-A-Protokoll), was bei umfangreichen Netzwerk-Installationen mit mehreren Routern die Verwaltung von Admin-Zugängen stark vereinfacht.

Die Anmeldung über einen RADIUS-Server läuft wie folgt ab:

1. Bei der Anmeldung sendet das LANCOM die eingegebenen Anmeldedaten des Benutzers an den RADIUS-Server im Netz. Die Server-Daten sind dazu im LANCOM gespeichert.
2. Der Server prüft die Anmeldedaten auf Gültigkeit.
3. Bei ungültigen Daten sendet er dem LANCOM eine entsprechende Nachricht, und das LANCOM bricht den Anmeldevorgang mit einer Fehlernachricht ab.
4. Bei gültigen Anmeldedaten sendet der Server dem LANCOM mit der Zugangserlaubnis auch die Zugriffs- und Funktionsrechte, so dass der Anwender nur auf die entsprechend freigeschalteten Funktionen und Verzeichnisse zugreifen kann.
5. Falls die Sitzungen des Anwenders durch den RADIUS-Server budgetiert sind (Bereich Accounting), speichert das LANCOM die Sitzungsdaten wie Start, Ende, Benutzername, Authentifizierungsmodus und, wenn vorhanden, den genutzen Port.

10.2.2 Ergänzungen im Setup-Menü

Authentifizierung

Mit Einführung der zusätzlichen Möglichkeit zur Authentifizierung über RADIUS entfällt dieser Menüpunkt.

Die Auswahl der Authentifizierung erfolgt nun unter **Setup** > **Config** > **Authentifizierung** (siehe *Authentifizierung*).

Authentifizierung

Um sich für die Anmeldung an der Verwaltungsoberfläche des LANCOM zu authentifizieren, stehen verschiedene Möglichkeiten zur Verfügung:

- **intern**: Das LANCOM verwaltet die Anwender intern in der Tabelle **Setup** > **Config** > **Admins**.
- **Radius**: Ein RADIUS-Server übernimmt die Verwaltung der Anwender.
- **Tacacs+**: Ein TACACS+-Server übernimmt die Verwaltung der Anwender.

Die notwendigen Daten für den RADIUS-Server verwalten Sie unter **Setup** > **Config** > **Radius** > **Server**. Die notwendigen Daten für den TACACS+-Server verwalten Sie unter **Setup** > **Tacacs+** > **Server**.

Da das RADIUS-Protokoll keine Änderung von Passworten zulässt, kann der per RADIUS eingeloggte Anwender sein Passwort im LANCOM nicht ändern.

SNMP-ID:

2.11.80

Pfad Telnet:

Setup > **Config**

Mögliche Werte:

Intern

Radius

Tacacs+

Default:

Intern

Radius

Wenn sich der Anwender für die Anmeldung an der LANCOM-Verwaltungsoberfläche über einen RADIUS-Server authentifizieren soll, geben Sie hier die notwendigen Server-Daten sowie zusätzliche Verwaltungs-Daten an.

SNMP-ID:

2.11.81

Pfad Telnet:

Setup > **Config**

Server

Diese Tabelle enthält die Einstellungen für den RADIUS-Server

SNMP-ID:

2.11.81.1

Pfad Telnet:

Setup > **Config** > **Radius**

Name

Vergeben Sie hier einen Namen für den RADIUS-Server.

SNMP-ID:

2.11.81.1.1

Pfad Telnet:

Setup > **Config** > **Radius** > **Server**

Mögliche Werte:

max. 16 Zeichen

Default:

Leer

Server

Vergeben Sie hier die IPv4-Adresse des RADIUS-Server.

SNMP-ID:

2.11.81.1.2

Pfad Telnet:

Setup > **Config** > **Radius** > **Server**

Mögliche Werte:

Max. 64 Zeichen

Default:

Leer

Port

Geben Sie hier den Port an, über den der RADIUS-Server mit dem LANCOM kommuniziert.

SNMP-ID:

2.11.81.1.3

Pfad Telnet:

Setup > **Config** > **Radius** > **Server**

Mögliche Werte:

Max. 5 Zeichen

Default:

1812

Protokoll

Geben Sie hier das Protokoll an, mit dem der RADIUS-Server mit dem LANCOM kommuniziert.

SNMP-ID:

2.11.81.1.4

Pfad Telnet:

Setup > **Config** > **Radius** > **Server**

Mögliche Werte:

RADIUS

RADSEC

Default:

RADIUS

Loopback-Adresse

Hier können Sie optional eine Absende-Adresse konfigurieren, die das LANCOM statt der ansonsten automatisch für die Zieladresse gewählten Absende-Adresse verwendet.

SNMP-ID:

2.11.81.1.5

Pfad Telnet:

Setup > **Config** > **Radius** > **Server**

Mögliche Werte:

Name der IP-Netzwerke, deren Adresse das LANCOM einsetzen soll.

"INT" für die Adresse des ersten Intranets.

"DMZ" für die Adresse der ersten DMZ.

Wenn in der Liste der IP-Netzwerke oder in der Liste der Loopback-Adressen ein Eintrag mit dem Namen "DMZ" vorhanden ist, verwendet das LANCOM die zugehörige IP-Adresse.

LB0 bis LBF für eine der 16 Loopback-Adressen.

Eine beliebige gültige IP-Adresse.

Default:

Leer

Secret

Geben Sie hier das Kennwort für den Zugang zum RADIUS-Server an und wiederholen Sie es im zweiten Eingabefeld.

SNMP-ID:

2.11.81.1.6

Pfad Telnet:

Setup > **Config** > **Radius** > **Server**

Mögliche Werte:

Max. 64 Zeichen

Default:

Leer

Backup

Geben Sie den Namen des alternativen RADIUS-Servers an, an den das LANCOM Anfragen weiterleitet, wenn der erste RADIUS-Server nicht erreichbar ist.

Für den Backup-Server müssen Sie einen weiteren Eintrag in der Server-Tabelle vornehmen.

SNMP-ID:

2.11.81.1.7

Pfad Telnet:

Setup > **Config** > **Radius** > **Server**

Mögliche Werte:

Max. 16 Zeichen

Default:

Leer

Kategorie

Bestimmen Sie, für welche Kategorie der RADIUS-Server gelten soll.

Sie können keine, eine oder beide Kategorien auswählen.

SNMP-ID:

2.11.81.1.8

Pfad Telnet:

Setup > **Config** > **Radius** > **Server**

Mögliche Werte:

Authentifizierung

Accounting

Default:

Authentifizierung

Zugriffsrechte-Uebertragung

Im RADIUS-Server ist die Authorisierung der Anwender gespeichert. Bei einer Anfrage sendet der RADIUS-Server die Zugriffs- und Funktionsrechte zusammen mit den Login-Daten an das LANCOM, das daraufhin den Anwender mit entsprechenden Rechten einloggt.

Normalerweise sind Zugriffsrechte im RADIUS Management-Privilege-Level (Attribut 136) definiert, so dass das LANCOM den übertragenen Wert nur auf die internen Zugriffsrechte zu mappen braucht (Option "mapped"). Das Attribut kann die folgenden Werte annehmen, die das LANCOM anschließend mappt:

- 1: User, nur lesen
- 3: User, nur schreiben
- 5: Admin, nur lesen, keine Trace-Rechte
- 7: Admin, schreiben und lesen, keine Trace-Rechte
- 9: Admin, nur lesen
- 11: Admin, schreiben und lesen
- 15: Supervisor
- Alle anderen Werte mappt das LANCOM auf "Kein Zugriff".

Es kann jedoch auch sein, dass der RADIUS-Server zusätzlich Funktionsrechte übertragen soll oder das Attribut 136 bereits anderweitig bzw. andere, hersteller-spezifische Attribute für die Authorisierung verwendet. In diesem Fall müssen

Sie herstellerabhängige Attribute auswählen. Diese Attribute sind wie folgt definiert, basierend auf der LANCOM-Herstellerkennung '2356':

- Zugriffsrechte-ID: 11
- Funktionsrechte-ID: 12

Die übertragenen Werte für die Zugriffsrechte sind identisch zu den oben genannten. Soll der RADIUS-Server auch Funktionsrechte mit übertragen, dann erreichen Sie das wie folgt:

1. Öffnen Sie die Konsole des LANCOMS.
2. Wechseln Sie in das Verzeichnis **Setup** > **Config** > **Admins**.
3. Der Befehl `set ?` zeigt Ihnen das aktuelle Mapping von Funktionsrechten zum entsprechenden Hexadezimalcode (z. B. `Device-Search (0x80)`).
4. Um Funktionsrechte zu kombinieren, addieren Sie deren Hex-Werte.
5. Wandeln Sie den hexadezimalen Wert in eine Dezimalzahl um.
6. Diesen Dezimalwert können Sie in der Funktionsrechte-ID verwenden, um die entsprechenden Funktionsrechte zu übertragen.

SNMP-ID:

2.11.81.2

Pfad Telnet:

Setup > **Config** > **Radius**

Mögliche Werte:

Herstellerabhaengig

Mapped

Default:

Herstellerabhaengig

Accounting

Hier bestimmen Sie, ob das LANCOM die Sitzung des Anwenders aufzeichnen soll. In diesem Fall speichert es die Sitzungsdaten wie Start, Ende, Benutzername, Authentifizierungsmodus und, wenn vorhanden, den genutzen Port.

SNMP-ID:

2.11.81.3

Pfad Telnet:

Setup > **Config** > **Radius**

Mögliche Werte:

Nein

Ja

Default:

Nein

10.2.3 Ergänzungen in LANconfig

Über RADIUS in die LCOS-Verwaltungsoberfläche einloggen

Aktuell können sich Benutzer über RADIUS, TACACS+ oder die interne Benutzerverwaltung des Gerätes in die Verwaltungsoberfläche des LANCOM einloggen.

Mit RADIUS ist das über die folgenden Verbindungen möglich:

- Telnet
- SSH
- WEBconfig
- TFTP
- Outband

Eine RADIUS-Authentifizierung über SNMP ist derzeit nicht unterstützt.

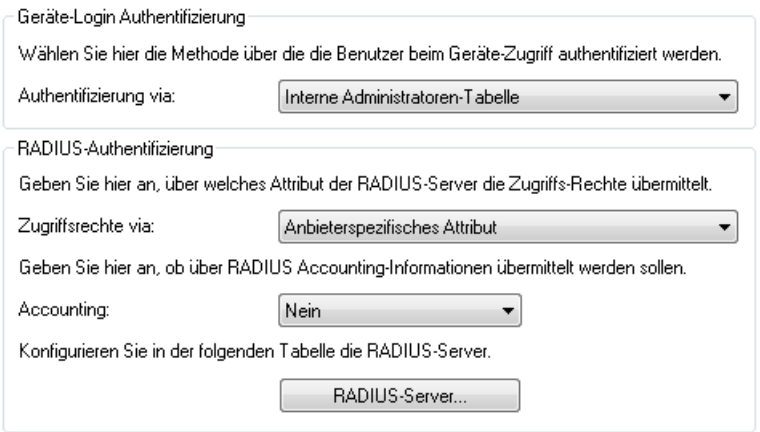
Eine RADIUS-Authentifizierung über LL2M (LANCOM Layer 2 Management Protokoll) ist nicht unterstützt, da LL2M Klartext-Zugriff auf das im LANCOM gespeicherte Passwort benötigt.

Der RADIUS-Server übernimmt die Verwaltung der Benutzer in den Bereichen Authentifizierung, Authorisierung und Accounting (Triple-A-Protokoll), was bei umfangreichen Netzwerk-Installationen mit mehreren Routern die Verwaltung von Admin-Zugängen stark vereinfacht.

Die Anmeldung über einen RADIUS-Server läuft wie folgt ab:

1. Bei der Anmeldung sendet das LANCOM die eingegebenen Anmeldedaten des Benutzers an den RADIUS-Server im Netz. Die Server-Daten sind dazu im LANCOM gespeichert.
2. Der Server prüft die Anmeldedaten auf Gültigkeit.
3. Bei ungültigen Daten sendet er dem LANCOM eine entsprechende Nachricht, und das LANCOM bricht den Anmeldevorgang mit einer Fehlernachricht ab.
4. Bei gültigen Anmeldedaten sendet der Server dem LANCOM mit der Zugangserlaubnis auch die Zugriffs- und Funktionsrechte, so dass der Anwender nur auf die entsprechend freigeschalteten Funktionen und Verzeichnisse zugreifen kann.
5. Falls die Sitzungen des Anwenders durch den RADIUS-Server budgetiert sind (Bereich Accounting), speichert das LANCOM die Sitzungsdaten wie Start, Ende, Benutzername, Authentifizierungsmodus und, wenn vorhanden, den genutzen Port.

Im LANconfig können Sie die Authentifizierungsmethode unter **Management** > **Authentifizierung** festlegen.



Im Abschnitt **Geräte-Login Authentifizierung** wählen Sie die Methode aus, über die sich Benutzer beim Zugriff auf die LANCOM-Verwaltungsoberfläche authentifizieren sollen:

- interne Administratoren-Tabelle: Das LANCOM übernimmt die komplette Benutzerverwaltung mit Anmeldename, Passwort sowie Zugriffs- und Funktionsrechte-Zuordnung.
- RADIUS: Die Benutzerverwaltung erfolgt über einen RADIUS-Server im Netzwerk.
- TACACS+: Die Benutzerverwaltung erfolgt über einen TACACS+-Server im Netzwerk.

Im Abschnitt **RADIUS-Authentifizierung** geben Sie die notwendigen RADIUS-Server-Daten sowie zusätzliche Verwaltungsdaten an.

Zugriffssrechte via

Im RADIUS-Server ist die Authorisierung der Anwender gespeichert. Bei einer Anfrage sendet der RADIUS-Server die Zugriffs- und Funktionsrechte zusammen mit den Login-Daten an das LANCOM, das daraufhin den Anwender mit entsprechenden Rechten einloggt.

Normalerweise sind Zugriffs- und Funktionsrechte im RADIUS Management-Privilege-Level (Attribut 136) definiert, so dass das LANCOM diese Werte nur auf die internen Zugriffs- und Funktionsrechte zu mappen braucht. Es kann jedoch auch sein, dass der RADIUS-Server dieses Attribut bereits anderweitig bzw. andere, hersteller-spezifische Attribute für die Authorisierung verwendet. In diesem Fall kann das LANCOM auch eine herstellerabhängige Authorisierung auswerten. Mögliche Werte sind:

- Anbieterspezifisches Attribut: Das LANCOM wertet das anbieterspezifische Attribut aus (Default).
- Management-Privilege-Level-Attribut: Das LANCOM wertet das Management-Privilege-Level-Attribut des RADIUS-Servers aus.

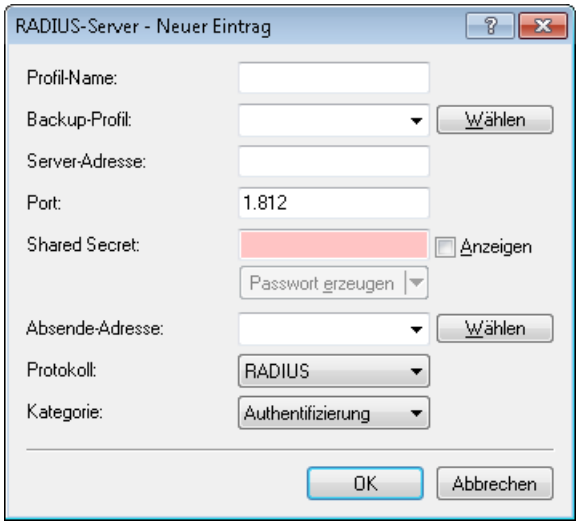
Accounting

Hier bestimmen Sie, ob das LANCOM die Sitzung des Anwenders aufzeichnen soll. Mögliche Werte sind:

- Nein: Das LANCOM zeichnet die Sitzung nicht auf (Default).
- Ja: Das LANCOM zeichnet die Sitzung auf (Start, Ende, Benutzername, Authentifizierungsmodus, Port).

RADIUS-Server

In dieser Tabelle können Sie die Einstellungen für den RADIUS-Server vornehmen



- **Profil-Name**: Vergeben Sie hier einen Namen für den RADIUS-Server.
- **Backup-Profil**: Geben Sie den Namen des alternativen RADIUS-Servers an, an den das LANCOM Anfragen weiterleitet, wenn der erste RADIUS-Server nicht erreichbar ist.

  Für den Backup-Server müssen Sie einen weiteren Eintrag in der Server-Tabelle vornehmen.

- **Server-Adresse**: Vergeben Sie hier die IPv4-Adresse des RADIUS-Server.

- **Port**: Geben Sie hier den Port an, über den der RADIUS-Server mit dem LANCOM kommuniziert (Default: 1812).
- **Shared Secret**: Geben Sie hier das Kennwort für den Zugang zum RADIUS-Server an und wiederholen Sie es im zweiten Eingabefeld.
- **Absende-Adresse**: Hier können Sie optional eine Absende-Adresse konfigurieren, die das LANCOM statt der ansonsten automatisch für die Zieladresse gewählten Absende-Adresse verwendet.
- **Protokoll**: Geben Sie hier das Protokoll an, mit dem der RADIUS-Server mit dem LANCOM kommuniziert. Mögliche Werte sind:
  - RADIUS (Default)
  - RADSEC
- **Kategorie**: Bestimmen Sie, für welche Kategorie der RADIUS-Server gelten soll. Mögliche Werte sind:
  - Deaktiviert
  - Authentifizierung (Default)
  - Accounting
  - Authentifizierung & Accounting

10.3 Getrennte RADIUS-Accounting-Server pro SSID

Ab LCOS 8.84 haben Sie die Möglichkeit, einzelnen logischen WLAN-Interfaces separate RADIUS-Accounting-Server zuzuweisen.

10.3.1 Ergänzungen im Setup-Menü

Server

In dieser Tabelle konfigurieren Sie optional alternative RADIUS-Accounting-Server für logische WLAN-Interfaces. Dadurch erhalten Sie die Möglichkeit, für ausgewählte WLAN-Interfaces spezielle Accounting-Server an Stelle des global konfigurierten einzusetzen.

SNMP-ID:

2.12.45.17

Pfad Telnet:

Setup > **WLAN** > **RADIUS-Accounting**

Name

Name des RADIUS-Servers, welcher das Accounting von WLAN-Clients durchführt. Sie verwenden den hier eingetragenen Namen, um aus anderen Tabellen auf den betreffenden Server zu referenzieren.

SNMP-ID:

2.12.45.17.1

Pfad Telnet:

Setup > **WLAN** > **RADIUS-Accounting** > **Server**

Mögliche Werte:

String, max. 16 Zeichen aus

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

Default:

Server-Adresse

IP-Adresse des RADIUS-Servers, mit dem Sie das Accounting von WLAN-Clients durchführen.

Die allgemeinen Werte für Wiederholung und Timeout müssen im RADIUS-Bereich ebenfalls konfiguriert werden.

SNMP-ID:

2.12.45.17.2

Pfad Telnet:

Setup > **WLAN** > **RADIUS-Accounting** > **Server**

Mögliche Werte:

Gültige IPv4-Adresse

Default:

0.0.0.0

Port

Port zur Kommunikation mit dem RADIUS-Server beim Accounting.

SNMP-ID:

2.12.45.17.3

Pfad Telnet:

Setup > **WLAN** > **RADIUS-Accounting** > **Server**

Mögliche Werte:

0 bis 65535

Default:

0

Schluessel

Geben Sie hier den Schlüssel (Shared Secret) für den Zugang zum Accounting-Server an. Stellen Sie sicher, dass dieser Schlüssel im entsprechenden Accounting-Server übereinstimmend konfiguriert ist.

SNMP-ID:

2.12.45.17.4

Pfad Telnet:

Setup > **WLAN** > **RADIUS-Accounting** > **Server**

Mögliche Werte:

Gültiges Shared-Secret, max. 64 Zeichen

Default:

Loopback-Addr.

Geben Sie hier optional eine andere Adresse (Name oder IP) an, an die der RADIUS Accounting-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:

2.12.45.17.5

Pfad Telnet:

Setup > **WLAN** > **RADIUS-Accounting** > **Server**

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:

Protokoll

Über diesen Eintrag geben Sie das Protokoll an, dass der Accounting-Server verwendet.

SNMP-ID:

2.12.45.17.6

Pfad Telnet:

Setup > **WLAN** > **RADIUS-Accounting** > **Server**

Mögliche Werte:

RADIUS

RADSEC

Default:

RADIUS

Backup

Name des RADIUS-Backup-Servers, welcher das Accounting von WLAN-Clients durchführt, falls der eigentliche Accounting-Server nicht verfügbar ist. Auf diese Weise lassen sich auch Backup-Server miteinander verketten, um mehrere Ausfall-Server zu konfigurieren ("Backup-Chaining").

SNMP-ID:

2.12.45.17.7

Pfad Telnet:

Setup > **WLAN** > **RADIUS-Accounting** > **Server**

Mögliche Werte:

Name aus **Setup** > **WLAN** > **RADIUS-Accounting** > **Server**, max. 16 Zeichen

Default:

Accounting-Server

Alternativer RADIUS-Accounting-Server für das betreffende logische WLAN-Interface. Wenn Sie dieses Feld leer lassen, verwendet das Gerät den global konfigurierten Accounting-Server (sofern RADIUS-Accounting für das Interface aktiviert ist).

SNMP-ID:

2.23.20.1.22

Pfad Telnet:

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

Mögliche Werte:

Name aus **Setup** > **WLAN** > **RADIUS-Accounting** > **Server**, max. 16 Zeichen

Default:

11 SMS-Empfang und -Versand

Sofern Ihr Gerät über ein 3G/4G WWAN-Modul verfügt, ist Ihr Gerät ebenfalls dazu in der Lage, Kurznachrichten über den Short Message Service (SMS) zu empfangen und zu versenden.

Die SMS-Funktion dient dabei vorwiegend als benachrichtigende und funktionserweiternde Schnittstelle für die LCOS-eigenen Module sowie externe Instanzen wie Router, Management-Lösungen, Accounting-Systeme und Ähnliche. Sie haben jedoch auch als Benutzer die Möglichkeit, über die entsprechende *Funktion im LANmonitor* oder mit dem `smssend`-Kommando auf der Konsole Kurznachrichten zu verschicken. Darüber hinaus haben Sie mit LANmonitor auch die Möglichkeit, gesendete oder empfangene Nachrichten *komfortabel zu verwalten*.

Der SMS-Empfang und -Versand muss ebenfalls Vertragsgegenstand der von Ihnen verwendeten SIM-Karte sein.

11.1 Empfang von SMS-Nachrichten

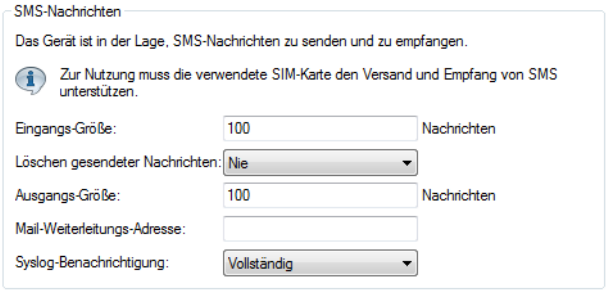
Ihr Gerät ist dazu in der Lage, SMS-Benachrichtungen auf Basis des ETSI-Standards TS 127.005 zu empfangen bzw. abzufragen, zu speichern und auf Wunsch den Erhalt einer SMS im SYSLOG zu protokollieren. Der Eintrag ins SYSLOG erfolgt dabei als "Hinweis", um Sie über ggf. wichtige Meldungen – wie z. B. die Benachrichtigung durch eine externe Instanz – zu informieren. Eine solche Instanz kann beispielsweise das Accounting-System Ihres Providers sein:

Sofern Sie mit dem Gerät eine Verbindung zum Internet über das 3G/4G WWAN-Modul herstellen und der Vertrag mit Ihrem Internet-Provider eine Volumenbegrenzung umfasst, drosselt oder stoppt Ihr Provider die Datenübertragung bei Erreichen dieser Volumengrenze (je nach Vertrag). In Ländern mit entsprechender Gesetzgebung gilt dies z. B. ebenfalls für das Erreichen bestimmter Gebührengrenzen beim Daten-Roaming. Bevor die Datenübertragung jedoch gedrosselt oder gestoppt wird, versenden viele Provider eine SMS, die Sie als Kunde über das Erreichen der Volumengrenze informiert. Mit einer enstprechenden Benachrichtigungseinstellung im Syslog und/oder per E-Mail informiert Sie das Gerät umgehend über den Empfang der SMS, sodass Sie zeitnah darauf reagieren können.

11.2 Basiskonfiguration des SMS-Moduls

Die nachfolgenden Schritte zeigen Ihnen, wie Sie die Basiskonfiguration des SMS-Moduls eines 3G/4G WWAN-fähigen Gerätes vornehmen.

1. Starten Sie LANconfig und öffnen Sie den Konfigurationsdialog für das Gerät.
2. Wechseln Sie in die Ansicht **Meldungen** > **SMS-Nachrichten**.



3. Geben Sie unter **Eingangs-Größe** die maximale Anzahl an Kurznachrichten an, die das Gerät im Nachrichteneingang aufbewahrt.
   Beim Überschreiten der eingestellten Anzahl wird die älteste Nachricht gelöscht. In diesem Fall erfolgt **kein** SYSLOG-Eintrag. Der Wert `0` deaktiviert das Limit, d. h. Nachrichten werden im unbegrenzten Umfang aufbewahrt.
4. Legen Sie unter **Löschen gesendeter Nachrichten** fest, wie das Gerät mit versendeten Kurznachrichten umgeht.
   - **Sofort**: Versendete Kurznachrichten werden nicht gespeichert.
   - **Nie**: Versendete Kurznachrichten werden dauerhaft gespeichert.
5. Geben Sie unter **Ausgangs-Größe** die maximale Anzahl an Kurznachrichten an, die das Gerät im Nachrichtenausgang aufbewahrt.
   Beim Überschreiten der eingestellten Anzahl wird die älteste Nachricht gelöscht. In diesem Fall erfolgt **kein** SYSLOG-Eintrag. Der Wert `0` deaktiviert das Limit, d. h. Nachrichten werden im unbegrenzten Umfang aufbewahrt.
6. Legen Sie unter **Syslog-Benachrichtigung** fest, ob und wie das Gerät eingehende Kurznachrichten im SYSLOG protokolliert.
   - **Nein**: Im SYSLOG erfolgt für eingehende Kurznachrichten kein Eintrag.
   - **Nur Absender/kein Inhalt**: Der Eingang einer Kurznachricht wird zusammen mit der Absender-Rufnummer im SYSLOG erfasst.
   - **Vollständig**: Der Eingang einer Kurznachricht wird zusammen mit der Absender-Rufnummer und dem vollständigen Nachrichtentext im SYSLOG erfasst.
7. Optional: Geben Sie unter **Mail-Weiterleitungs-Adresse** die E-Mail-Adresse an, an die das Gerät eingehende Kurznachrichten weiterleiten soll.

   Damit die E-Mail-Weiterleitung funktioniert, muss ein gültiges SMTP-Konto im Gerät konfiguriert sein.
8. Übertragen Sie die Konfiguration zurück an das Gerät.

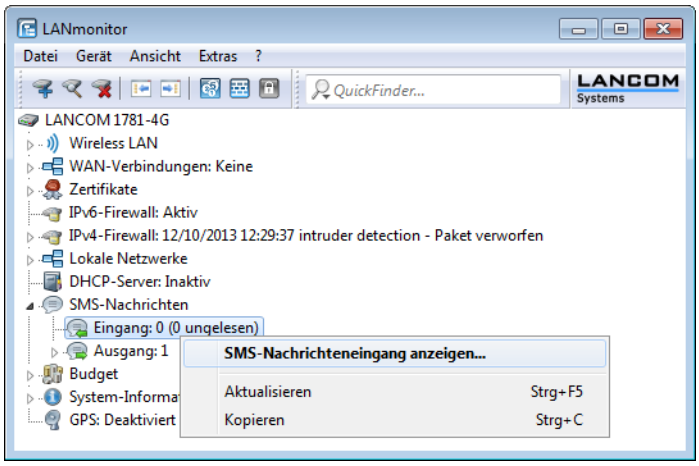
Fertig! Damit ist die Basiskonfiguration des SMS-Moduls abgeschlossen.

11.3 SMS-Nachrichten mit LANmonitor verwalten

Der nachfolgende Abschnitt zeigt, wie Sie auf einem 3G/4G WWAN-fähigen Gerät mit LANmonitor eingegangene oder versendete Kurznachrichten einsehen und bei Bedarf löschen.

1. Starten Sie LANmonitor und navigieren Sie im Menübaum des betreffenden Gerätes zu **SMS-Nachrichten** > **Eingang** bzw. **Ausgang**.
   Sofern im Gerät bereits Kurznachrichten vorliegen, zeigt LANmonitor direkt unter **Eingang** die letzten fünf empfangenen und unter **Ausgang** die letzten fünf gesendeten SMS an.

2. Öffnen Sie das Kontextmenü auf dem entsprechenden Eintrag und wählen Sie **SMS-Nachrichteneingang anzeigen** bzw. **SMS-Nachrichtenausgang anzeigen**.



Es öffnet sich ein neues Fenster, in dem LANmonitor alle eingegangenen bzw. versendeten Kurznachrichten und deren Status auflistet. Im **SMS-Nachrichteneingang** haben Sie die Möglichkeit, einzelne oder mehrere ausgewählte Nachrichten wahlweise zu löschen oder als gelesen/ungelesen zu markieren; der Status ist der Lesestatus (entsprechend **Neu** oder **Gelesen**). Im **SMS-Nachrichtenausgang** lassen sich die Nachrichten nur löschen; der Status ist der Sendestatus (**Ungesendet** oder **Gesendet**).

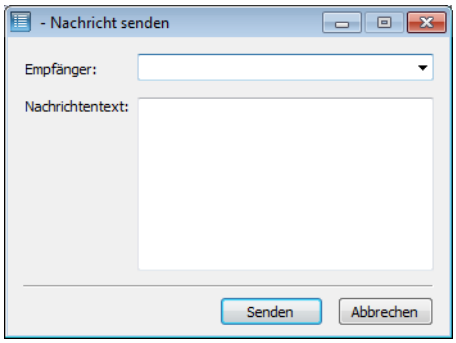
Die angezeigten Nachrichten verwalten Sie über das Kontextmenü. Um den kompletten Nachrichteneingang bzw. -ausgang zu löschen, wählen Sie in der Menüleiste unter **Nachrichten** die betreffende Aktion.

Um zwischen Nachrichteneingang und -ausgang bequem hin- und herzuwechseln, wählen Sie in der Menüleiste unter **Ansicht** die entsprechende Nachrichtenbox aus.

11.4 SMS-Nachrichten mit LANmonitor versenden

Der folgende Abschnitt zeigt, wie Sie mit LANmonitor Kurznachrichten über ein 3G/4G WWAN-fähiges Gerät versenden.

1. Starten Sie LANmonitor und navigieren Sie im Menübaum des betreffenden Gerätes zu **SMS-Nachrichten**.
2. Öffnen Sie das Kontextmenü auf dem Eintrag und wählen Sie **Nachricht senden**.
3. Geben Sie in dem sich öffnenden Editorfenster die Rufnummer des Empfängers und den zu versendenden Nachrichtentext ein.
   Die Anzahl der Zeichen ist dabei auf eine Kurznachricht (max. 160 Zeichen) beschränkt. Eine Übersicht der verfügbaren Zeichen finden Sie im Abschnitt *Zeichensatz für den SMS-Versand* auf Seite 152.



4. Klicken Sie **Senden**, um die Nachricht über das geräteinterne SMS-Modul zu verschicken.

11.5 URL-Platzhalter für den SMS-Versand

Sie haben die Möglichkeit, das SMS-Modul in seiner Rolle als Schnittstelle auch über eine URL anzusprechen. Dazu integrieren Sie vorgegebene Platzhalter (Parameter) in die URL, was den SMS-Versand über das Gerät per HTTP(S)-Aufruf erlaubt. Somit eignen sich LANCOM Mobilfunk-Router insbesondere auch für den Einsatz als SMS-Gateway.

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

Die Authentifizierung am Gerät erfolgt mit Ihren Zugangsdaten; deren Einbindung in die URL gibt die Credential-Schreibweise Ihres Browsers vor. Typischerweise lautet diese Schreibweise `Benutzername:Passwort@Host`.

Je nach Einsatzszenario (z. B. SMS-Gateway) empfiehlt es sich, für den Zugang einen Administrator ohne Zugriffsrechte (**Keine**) mit dem alleinigen Funktionsrecht **Senden von SMS** anzulegen.

Nicht alle Webbrowser unterstützen die Übermittlung von Zugangsdaten über die URL. Hierzu gehört u. a. der Microsoft Internet Explorer in seinen aktuellen Versionen. Weichen Sie in diesem Fall auf einen anderen Browser aus, um den SMS-Versand über die URL zu nutzen.

Der URL-Aufruf erfolgt über die Syntax:

```
(http|https)://<User>:<Password>@<Host>/sms/?<Param1>=<Value1>&…&oldauth
```

Der Parameter `oldauth` ist dabei **zwingend** erforderlich; andernfalls sendet keiner der von Ihnen verwendeten Browser die Zugangsdaten an das Gerät. Darüber hinaus sind folgende Platzhalter definiert:

`DestinationAddress`

Rufnummer, an die das Gerät die SMS schicken soll. Es gelten die gleichen Konventionen wie für normale Telefonanrufe. Geben Sie den Parameter wie folgt an:

```
&DestinationAddress=01511234567
&DestinationAddress=00491511234567
```

`Content`

Inhalt der Kurznachricht. Die Anzahl der Zeichen ist dabei auf eine Kurznachricht (max. 160 Zeichen) beschränkt. Eine Übersicht der verfügbaren Zeichen finden Sie im Abschnitt *Zeichensatz für den SMS-Versand* auf Seite 152.

Um Leerzeichen und andere Sonderzeichen in die SMS einzubauen, müssen Sie diese in URL-kodierter Form an das Gerät übermitteln. Leerzeichen beispielsweise kodieren Sie mittels `%20` und Punkte mit `%2E`. Geben Sie den Parameter wie folgt an:

```
&Content=Dies%20ist%20eine%20Nachricht%2E
```

Mehr zu dem Thema erfahren Sie im Internet unter dem Stichwort "URL Encoding" sowie unter *www.w3schools.com*.

Manche Browser führen die URL-Kodierung automatisch durch. Generell ist jedoch zu empfehlen, Inhalte eigenständig zu kodieren, um die korrekte Umwandlung aller Zeichen sicherzustellen.

11.6 Zeichensatz für den SMS-Versand

Der Umfang der in einer SMS verfügbaren Zeichen (max. 160 Zeichen zu je 7 Bit = 1.120 Bit) ergibt sich aus dem GSM-Basiszeichensatz (ingesamt 128 Zeichen) sowie ausgewählten Zeichen aus dem erweiterten GSM-Zeichensatz. Mit

dem erweiterten Zeichensatz lassen sich zusätzliche Zeichen darstellen; diese belegen jedoch den doppelten Speicherplatz und reduzieren die maximale Zeichenanzahl entsprechend. Zeichen, die nicht im SMS-Modul implementiert sind, ignoriert das Gerät beim Versand.

Folgende Zeichen sind im **GSM-Basiszeichensatz** definiert:

@	Δ	SP	0	¡	P	¿	p
£	_	!	1	A	Q	a	q
$	Φ	"	2	B	R	b	r
¥	Γ	#	3	C	S	c	s
è	Λ	¤	4	D	T	d	t
é	Ω	%	5	E	U	e	u
ù	Π	&	6	F	V	f	v
ì	Ψ	'	7	G	W	g	w
ò	Σ	(	8	H	X	h	x
Ç	Θ	)	9	I	Y	i	y
LF	Ξ	*	:	J	Z	j	z
Ø	ESC	+	;	K	Ä	k	ä
ø	Æ	,	<	L	Ö	l	ö
CR	æ	-	=	M	Ñ	m	ñ
Å	ß	.	>	N	Ü	n	ü
å	É	/	?	O	§	o	à

Folgende Zeichen sind aus dem **erweiterten GSM-Zeichensatz** implementiert:

{|}[]~^\€

11.7 Ergänzungen im Status-Menü

11.7.1 SMS

Dieses Menü enthält die Statuswerte für das SMS-Modul, welches den Versand und Empfang von Kurznachrichten (SMS) übernimmt.

SNMP-ID:

1.83

Pfad Telnet:

Status

Eingang

In dieser Tabelle speichert das Gerät alle empfangenen Kurznachrichten (SMS) ab.

SNMP-ID:

1.83.1

Pfad Telnet:

Status > **SMS**

Idx

Dieser Statuswert gibt den Indexeintrag der Kurznachricht wieder.

MsgRef

Dieser Statuswert gruppiert mehrere Nachrichtenteile zu einer mehrteiligen Nachricht.

Teil

Dieser Statuswert gibt bei mehrteiligen Nachrichten die Reihenfolge an.

Sender

Dieser Statuswert zeigt die Rufnummer an, von der das Gerät die Kurznachricht empfangen hat.

Status

Dieser Statuswert zeigt den Lesestatus für die Kurznachricht an, also ob die Nachricht von einem Administrator bereits gelesen wurde oder nicht.

Mögliche Werte:

- **neu**
- **gelesen**

Zeitstempel

Dieser Statuswert gibt den Empfangszeitpunkt der Kurznachricht an.

Inhalt

Dieser Statuswert zeigt den Inhalt der empfangenen Kurznachricht an.

Ausgang

In dieser Tabelle speichert das Gerät alle gesendeten Kurznachrichten (SMS).

SNMP-ID:

1.83.2

Pfad Telnet:

Status > **SMS**

Idx

Dieser Statuswert gibt den Indexeintrag der Kurznachricht wieder.

MsgRef

Dieser Statuswert gruppiert mehrere Nachrichtenteile zu einer mehrteiligen Nachricht.

Teil

Dieser Statuswert gibt bei mehrteiligen Nachrichten die Reihenfolge an.

Empfaenger

Dieser Statuswert zeigt die Rufnummer an, an die das Gerät die Kurznachricht gesendet hat.

Status

Dieser Statuswert zeigt den Übermittlungsstatus der Kurznachricht an.

Mögliche Werte:

- **unsent**: Die Nachricht wurde noch nicht an das Funk-Modul übergeben.
- **sent**: Die Nachricht wurde an das Service Center zur Zustellung an den Empfänger übergeben.

Zeitstempel

Dieser Statuswert gibt den Versandzeitpunkt der Kurznachricht an.

Inhalt

Dieser Statuswert zeigt den Inhalt der gesendeten Kurznachricht an.

Eingangs-Nachrichten

Dieser Statuswert zeigt die Gesamtzahl der Nachrichten an, die sich im Nachrichteneingang befinden.

SNMP-ID:

1.83.3

Pfad Telnet:

Status > **SMS**

Ungelesene-Nachrichten

Dieser Statuswert zeigt die Anzahl der ungelesenen Nachrichten an, die sich im Nachrichteneingang befinden.

SNMP-ID:

1.83.4

Pfad Telnet:

Status > **SMS**

Ausgangs-Nachrichten

Dieser Statuswert zeigt die Gesamtzahl der Nachrichten an, die sich im Nachrichtenausgang befinden.

SNMP-ID:

1.83.5

Pfad Telnet:

Status > **SMS**

SMSC-Adresse

Dieser Statuswert zeigt die Rufnummer des Service Centers an, die in der USIM-Karte des Gerätes hinterlegt ist. Das Service Center ist in diesem Fall eine Einheit im Netz Ihres Providers, welche die Nachrichten zwischen dem Funknetz und dem Gerät weiterleitet und ggf. zwischenspeichert. Das Gerät verwendet diese Rufnummer, sofern Sie unter *SNMP-ID 2.83.1* keine abweichende Nummer eingetragen haben.

SNMP-ID:

1.83.6

Pfad Telnet:

Status > **SMS**

Eingang-Leeren

Mit dieser Aktion leeren Sie die Tabelle *1.83.1*.

SNMP-ID:

1.83.7

Pfad Telnet:

Status > **SMS**

Mögliche Parameter:

Keine Parameter vorhanden

Ausgang-Leeren

Mit dieser Aktion leeren Sie die Tabelle *1.83.2*.

SNMP-ID:

1.83.8

Pfad Telnet:

Status > **SMS**

Mögliche Parameter:

Keine Parameter vorhanden

Eingang-Gelesen

Mit dieser Aktion markieren Sie die in der Tabelle *1.83.1* gespeicherten Nachrichten als gelesen.

SNMP-ID:

1.83.9

Pfad Telnet:

Status > **SMS**

Mögliche Parameter:

Keine Parameter vorhanden

11.8 Ergänzungen im Setup-Menü

11.8.1 SMS

Dieses Menü enthält die Einstellungsmöglichkeiten für das SMS-Modul, welches den Versand und Empfang von Kurznachrichten (SMS) übernimmt.

SNMP-ID:

2.83

Pfad Telnet:

Setup

SMSC-Adresse

Über diesen Parameter konfigurieren Sie eine abweichende Rufnummer für das "Short Message Service Center" (SMSC).

Standardmäßig verwendet das Gerät die in Ihrer USIM-Karte hinterlegte Rufnummer, welche Sie über den Statuswert **SMSC-Nummer** (*SNMP-ID 1.83.5*) abrufen. Durch Angabe einer abweichenden Rufnummer lässt sich die SMS jedoch gezielt an ein bestimmtes SMSC senden.

SNMP-ID:

2.83.1

Pfad Telnet:

Setup > **SMS**

Mögliche Werte:

Gültige SMSC-Rufnummer, max. 31 Zeichen

Default:

Eingangs-Groesse

Über diesen Parameter setzen Sie die maximale Anzahl an Kurznachrichten, die das Gerät im Nachrichteneingang aufbewahrt. Beim Überschreiten der eingestellten Anzahl wird die älteste Nachricht gelöscht. In diesem Fall erfolgt **kein** SYSLOG-Eintrag.

SNMP-ID:

2.83.2

Pfad Telnet:

Setup > **SMS**

Mögliche Werte:

0 bis 999999

Besondere Werte:

0: Dieser Wert deaktiviert das Limit, d. h. Nachrichten werden im unbegrenzten Umfang aufbewahrt.

Default:

100

Ausgangs-Groesse

Über diesen Parameter setzen Sie die maximale Anzahl an Kurznachrichten, die das Gerät im Nachrichtenausgang aufbewahrt. Beim Überschreiten der eingestellten Anzahl wird die älteste Nachricht gelöscht. In diesem Fall erfolgt **kein** SYSLOG-Eintrag.

SNMP-ID:

2.83.3

Pfad Telnet:

Setup > **SMS**

Mögliche Werte:

0 bis 999999

Besondere Werte:

0: Dieser Wert deaktiviert das Limit, d. h. Nachrichten werden im unbegrenzten Umfang aufbewahrt.

Default:

100

Ausgangs-Aufbewahrung

Über diesen Parameter konfigurieren Sie, wie das Gerät mit versendeten Kurznachrichten umgeht.

SNMP-ID:

2.83.4

Pfad Telnet:

Setup > **SMS**

Mögliche Werte:

- **Keine**: Versendete Kurznachrichten werden nicht gespeichert.
- **Alle**: Versendete Kurznachrichten werden dauerhaft gespeichert.

Default:

Alle

Mail-Weiterleitungs-Addr.

Über diesen Parameter richten Sie eine optionale E-Mail-Adresse ein, an die das Gerät eingehende Kurznachrichten weiterleitet.

Damit die E-Mail-Weiterleitung funktioniert, muss ein gültiges SMTP-Konto im Gerät konfiguriert sein.

SNMP-ID:

2.83.5

Pfad Telnet:

Setup > **SMS**

Mögliche Werte:

Gültige E-Mail-Adresse, max. 31 Zeichen

Default:

Syslog

Über diesen Parameter legen Sie fest, ob und wie das Gerät eingehende Kurznachrichten im SYSLOG protokolliert.

SNMP-ID:

2.83.8

Pfad Telnet:

Setup > **SMS**

Mögliche Werte:

- **Nein**: Im SYSLOG erfolgt für eingehende Kurznachrichten kein Eintrag.
- **Absender**: Der Eingang einer Kurznachricht wird zusammen mit der Absender-Rufnummer im SYSLOG erfasst.
- **Vollstaendig**: Der Eingang einer Kurznachricht wird zusammen mit der Absender-Rufnummer und dem vollständigen Nachrichtentext im SYSLOG erfasst.

Default:

Nein

11.9 Ergänzungen der Kommandozeilenbefehle

11.9.1 SMS-Senden-Kommando

Ab LCOS 8.84 steht Ihnen auf der Kommandozeile der Befehl `smssend` zum manuellen Versenden von Kurznachrichten via SMS zur Verfügung, sofern Ihr Gerät über ein 3G/4G WWAN-Modul verfügt.

Tabelle 7: Übersicht aller auf der Kommandozeile eingebbaren Befehle

Befehl	Beschreibung
smssend [-s <SMSC-Number>] (-d <Destination>) (-t <Text>)	Nur auf Geräten mit 3G/4G WWAN-Modul verfügbar: Versendet eine Kurznachricht an die angegebene Ziel-Rufnummer. ■ `-s <SMSC-Number>`: Alternative SMSC-Rufnummer (optional). Wenn Sie diesen Befehlsbestandteil weglassen, verwendet das Gerät die in der USIM-Karte hinterlegte oder die unter SNMP-ID 2.83.1 konfigurierte Rufnummer. ■ `-d <Destination>`: Ziel-Rufnummer ■ `-t <Text>`: Inhalt der Kurznachricht mit <=160 Zeichen. Eine Übersicht der verfügbaren Zeichen finden Sie im Abschnitt *Zeichensatz für den SMS-Versand* auf Seite 152. Sonderzeichen sind nur in UTF8-kodierter Form möglich.

Legende

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

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