LCOS 10.94

Addendum

11/2025

LANCOM SYSTEMS

Inhalt

Copyright

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

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

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

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

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

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

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

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

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

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

LANCOM Systems GmbH

A Rohde & Schwarz Company

Adenauerstr. 20/B2

52146 Würselen

Deutschland

www.lancom-systems.de

1 Addendum zur LCOS-Version 10.94

Dieses Dokument beschreibt die Änderungen und Ergänzungen in der LCOS-Version 10.94 gegenüber der vorherigen Version.

2 Konfiguration

2.1 Unterstützung für Alias auf der CLI

Ab LCOS 10.94 können auf der CLI Kommando-Aliase konfiguriert werden. Mit diesen Kommando-Aliasen können CLI-Befele auf der Konsole verkürzt bzw. definiert werden.

2.1.1 Ergänzungen im Setup-Menü

2.1.1.1 Kommando-Aliasse

Hier können Sie auf der CLI Kommando-Aliase konfigurieren. Mit diesen Kommando-Aliasen können CLI-Befele auf der Konsole verkürzt bzw. definiert werden. Zum Beispiel das Setzen von Parametern oder die Anzeige einer (Status-)Tabelle.

Definieren Sie dazu Paare einens neuen Alias und des dazu auszuführenden Kommandos. Beispiele:

› Im folgenden Beispiel soll das benutzerdefinierte Alias „show wwan“ den Status des Mobilfunkmodems aus dem Statusbaum mit dem Befehl „ls /status/modem-mobile“ anzeigen.

```
root@:/Setup/Config/Command-Aliases
> add "show wwan" "ls /status/modem-mobile"
set ok:
Command                          Definition
=================================-======================================
show wwan                        ls /status/modem-mobile
```

› Es wird ein Alias angelegt, mit dem das Kommando Ping zwei Pakete an die IP-Adresse 8.8.8.8 senden soll:

```
root@:/Setup/Config/Command-Aliases
> add "pingtest" "ping 8.8.8.8 -c2"
set ok:
Command                          Definition
=================================-======================================
pingtest                         ping 8.8.8.8 -c2

root@:/Setup/Config/Command-Aliases
> pingtest

    56 Byte Packet from 8.8.8.8 seq.no=0 time=6.687 ms
    56 Byte Packet from 8.8.8.8 seq.no=1 time=6.425 ms

 ---8.8.8.8 ping statistic---
 56 Bytes Data, 2 Packets transmitted, 2 Packets received, 0% loss
```

SNMP-ID:

2.11.98

Pfad Konsole:

Setup > **Config**

2.1.1.1.1 Kommando

Definieren Sie hier den neuen Alias als Kommando dieses Alias-Eintrags.

SNMP-ID:

2.11.98.1

Pfad Konsole:

Setup > **Config** > **Kommando-Aliasse**

Mögliche Werte:

max. 32 Zeichen aus `[a-z][0-9]`

2.1.1.1.2 Definition

Definieren Sie hier das für dieses Alias auszuführende Kommando dieses Alias-Eintrags.

SNMP-ID:

2.11.98.2

Pfad Konsole:

Setup > **Config** > **Kommando-Aliasse**

Mögliche Werte:

max. 128 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!"$%&'()*+-,/:;<=>?[\]^_. ``

2.2 Historie in der Konsole unterstützen

Ab LCOS 10.94 werden eingegebene CLI-Befehle standardmäßig persistent gespeichert und sind somit nach einem Reboot verfügbar. Die eingegebenen Befehle lassen sich mit dem Kommando „history" anzeigen sowie mit den „Pfeil-nach-oben" und „Pfeil-nach-unten" auf der Tastatur aufrufen. Das persistente Speichern lässt sich per Konfiguration deaktivieren.

Befehl	Beschreibung
`history [options][<count>]`	Zeigt eine Liste der letzen ausgeführten Befehle. Mit dem Befehl `!#` können die Befehle der Liste unter Ihrer Nummer (#) direkt aufgerufen werden: Mit `!3` wird z. B. der dritte Befehl der Liste ausgeführt. Die Historie wird Boot-Persistent gesichert. Siehe auch *2.11.99 Persistente-Historie*. › `-c`: Löscht die gespeicherte Historie. › `-w`: Schreibt die aktuelle Historie in eine Datei. › `-a`: Fügt die Kommandos der Historie aus dieser Sessian am Ende einer Datei hinzu. › `<count>`: Gibt nur die in <count> angegebene Anzahl an Kommandos auf der Kommandozeile aus.

2.2.1 Ergänzungen im Setup-Menü

2.2.1.1 Persistente-Historie

Bei aktiver persistenter CLI-Historie werden eingegebene CLI-Befehle standardmäßig persistent gespeichert und sind somit nach einem Reboot verfügbar. Die eingegebenen Befehle lassen sich mit dem Kommando „history" anzeigen sowie mit den „Pfeil-nach-oben" und „Pfeil-nach-unten" auf der Tastatur aufrufen. Das persistente Speichern lässt sich hier deaktivieren.

Die Anzahl der Einträge in der History-Liste definieren Sie in *2.11.100 Historie-Dateigroessen-Limit*.

SNMP-ID:

2.11.99

Pfad Konsole:

Setup > **Config**

Mögliche Werte:

Nein

Persistente CLI-Historie ist deaktiviert.

Ja

Persistente CLI-Historie ist aktiviert.

Default-Wert:

Ja

2.2.1.2 Historie-Dateigroessen-Limit

Definiert die Anzahl der Einträge in der History-Liste

Siehe auch *2.11.99 Persistente-Historie*.

SNMP-ID:

2.11.100

Pfad Konsole:

Setup > **Config**

Mögliche Werte:

max. 4 Zeichen aus `[0-9]`

Default-Wert:

100

2.3 Show-Kommando für Detailinformationen zu PPPoE-Benutzern

Ab LCOS 10.94 können Sie über den Befehl `show pppoe-user-detail <user-name>` Status-Informationen über den jeweiligen aktiven Benutzer bzw. der Gegenstelle im PPPoE-Server anzeigen.

3 Sicherheit

3.1 Zwei-Faktor-Authentifizierung (2FA) für den Gerätezugriff

Der Zugriff auf die Management-Protokolle (z. B. WEBconfig, SSH, Telnet) kann per Zwei-Faktor-Authentifizierung (2FA), zusätzlich zum normalen Passwort, abgesichert werden. Dabei kann die Funktion für weitere Administratoren oder für den standardmäßigen Root-Benutzer getrennt konfiguriert werden.

In bestimmten Fällen ist es erforderlich, dass Management-Protokolle über unsichere Kanäle, z. B. das Internet, erlaubt werden müssen. Um diese Wege zusätzlich abzusichern und das Gerät vor Brute-Force-Angriffen zu schützen, kann die Zwei-Faktor-Authentifizierung für verschiedene Wege granular aktiviert werden.

Dabei werden die bekannten Authenticator-Apps für mobile Geräte wie Smartphones unterstützt.

Es ist zu beachten, dass im Fall eines Verlusts des Authenticators im schlimmsten Fall nur ein vollständiger Geräte-Reset möglich ist. Daher wird empfohlen nicht für alle Konfigurationswege 2FA anzufordern, z. B. nicht für den Zugriff per serieller Schnittstelle oder den Zugriff aus dem LAN heraus, so dass bei Verlust oder Fehlkonfiguration der Zugriff auf normalem Wege auch ohne 2FA weiterhin möglich ist.

Insbesondere wird der 2FA-Schutz für den Zugriff über die WAN-Schnittstelle inkl. der Nutzung von nur verschlüsselten Protokollen wie HTTPS oder SSH empfohlen.

Die Nutzung der 2FA setzt eine korrekte Uhrzeit des Geräts voraus. Daher sollte in jedem Fall der Zeitbezug per NTP-Client auf dem Router konfiguriert werden in LANconfig unter **Datum/Zeit** > **Synchronisierung**.

Der Ablauf der grundlegenden Konfiguration der Zwei-Faktor-Authentifizierung ist wie folgt:

1. Erzeugung eines Eintrags in der Tabelle „Admin-OTPs“ (LANconfig: **Management** > **Admin** > **Geräte-Konfiguration** > **Admin-OTPs**) unter Angabe des Administrator-Account-Namens für den dieser Eintrag gelten soll
2. Aufruf der WEBconfig unter**Extras** > **Admin-OTPs**. Von dort kann der erzeugte QR-Code für den Benutzer anzeigt, gespeichert oder von der externen Authenticator-App eingescannt werden
3. Beim Aufruf der Managementverbindung des Admin-Benutzers wird dieser nach dem Passwort zur Eingabe des Einmalpassworts (OTP) aufgefordert

Erzeugung von QR-Codes für Verbindung mit dem Authenticator

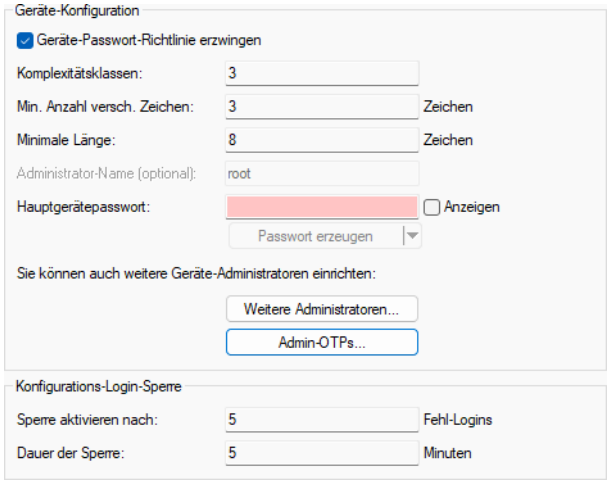
Die Erzeugung der QR-Codes für die Verbindung des Authenticators mit dem Gerät erfolgt über die WEBconfig unter **Extras** > **Admin-OTPs** oder alternativ über die CLI via „show Admin-OTP-QR“.

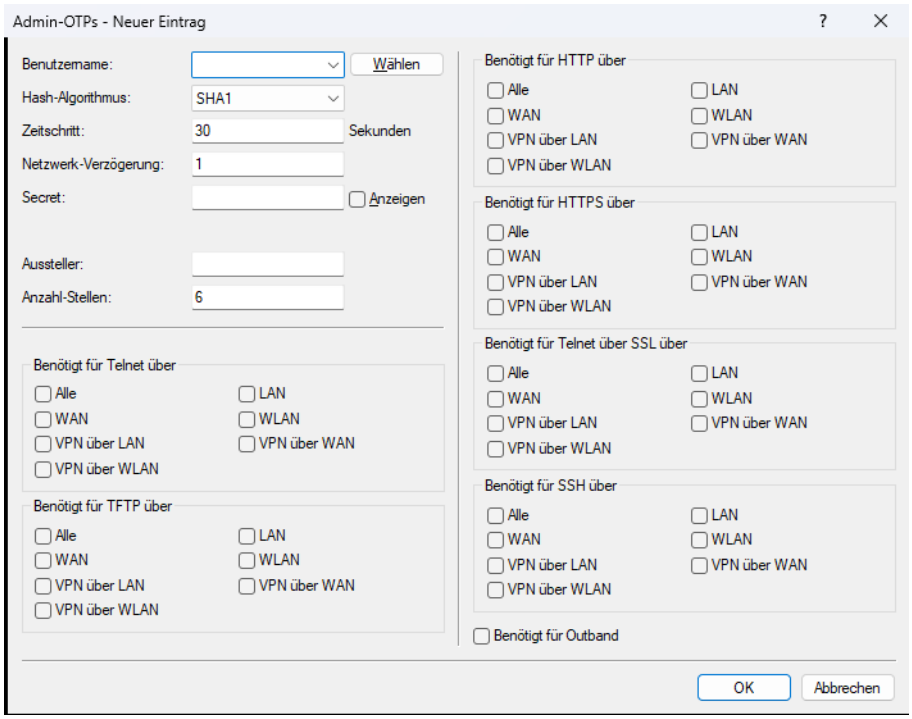
Show-Kommandos

- Admin-OTP – Zeigt die Administrator-OTP-Profile
- Admin-OTP-CODES – Zeigt die Administrator-OTP-Profile (codes only)
- Admin-OTP-QR – Zeigt die Administrator-OTP-Profile (QR code only)
- Admin-OTP-URI – Zeigt die Administrator-OTP-Profile (URI only)

3.1.1 Admin-OTPs

Die Einstellungen zu OTPs für die Administratoren-Accounts finden Sie in LANconfig unter **Management** > **Admin** > **Geräte-Konfiguration** > **Admin-OTPs**.





Benutzername

Benutzername des Administrators, für den die Zwei-Faktor-Authentifizierung aktiviert werden soll, z. B. „root“.

Hash-Algorithmus

Definiert den verwendeten Hash-Algorithmus.

Beachten Sie, dass die Authenticator-App den maximal möglichen Hash-Algorithmus unterstützt.

Zeitschritt

Definiert das Intervall in Sekunden, nach dem ein neues OTP berechnet wird.

Netzwerk-Verzögerung

Definiert, um wie viele Zeitschritte die Uhr des Clients maximal abweichen darf. Das Gerät prüft das um diesen Wert ältere bzw. neuere OTP.

Secret

Definiert das eigentliche Shared Secret, das mit der Authenticator-App geteilt werden muss. Das Secret muss für jeden Benutzer unterschiedlich sein. Es gibt aktuell in der Tabelle drei Eingabemöglichkeiten:

Base32 (Default)

Präfix „base32:" und danach das Base32-kodierte Secret. Der Präfix darf auch weggelassen werden.

Hexadezimal

Präfix „hex:" und danach eine gerade Anzahl von Hex-Digits.

Plain text passphrase

Präfix „ascii:" und danach die Zeichen.

Für den Google Authenticator muss das Secret 16 Zeichen (80 Bit, Base32 codiert) lang sein, z. B. E3U5IDWEE3KFCJ7G

Aussteller

Frei definierbarer Text, der im Authenticator dazu dient, mehrere Schlüssel auseinanderzuhalten bzw. der allgemeinen Anzeige dient, wenn der gleiche Benutzername verwendet wird. Der Wert darf keinen Doppelpunkt enthalten.

Anzahl-Stellen

Länge der OTPs.

Für den Google Authenticator sollte der Wert 6 verwendet werden.

Benötigt für *Protokoll* über

Definiert, ob die Zwei-Faktor-Authentifizierung für diesen Benutzer bei Anmeldung über dieses *Protokoll* erforderlich ist bzw. durch das Gerät abgefragt werden soll. Es ist granular konfigurierbar, über welche Zugriffswege die Zwei-Faktor-Authentifizierung erforderlich ist, z. B. nur über eine WAN-Verbindung.

Alle

Zwei-Faktor-Authentifizierung wird für alle Zugangsprotokolle verwendet.

WAN

Zwei-Faktor-Authentifizierung wird für den Zugang über „WAN" verwendet.

VPN über LAN

Zwei-Faktor-Authentifizierung wird für den Zugang über „VPN über LAN" verwendet.

VPN über WLAN

Zwei-Faktor-Authentifizierung wird für den Zugang über „VPN über WLAN" verwendet.

LAN

Zwei-Faktor-Authentifizierung wird für den Zugang über „LAN" verwendet.

WLAN

Zwei-Faktor-Authentifizierung wird für den Zugang über „WLAN" verwendet.

VPN über WAN

Zwei-Faktor-Authentifizierung wird für den Zugang über „VPN über WAN" verwendet.

Benötigt für Outbamd

Definiert, ob die Zwei-Faktor-Authentifizierung für diesen Benutzer bei Anmeldung über die serielle Schnittstelle erforderlich ist bzw. durch das Gerät abgefragt werden soll.

3.1.2 Ergänzungen im Setup-Menü

3.1.2.1 Admin-OTPs

Der Zugriff auf die Management-Protokolle (z. B. WEBconfig, SSH, Telnet) kann per Zwei-Faktor-Authentifizierung (2FA), zusätzlich zum normalen Passwort, abgesichert werden. Dabei kann die Funktion für weitere Administratoren oder für den standardmäßigen Root-Benutzer getrennt konfiguriert werden.

In bestimmten Fällen ist es erforderlich, dass Management-Protokolle über unsichere Kanäle, z. B. das Internet, erlaubt werden müssen. Um diese Wege zusätzlich abzusichern und das Gerät vor Brute-Force-Angriffen zu schützen, kann die Zwei-Faktor-Authentifizierung für verschiedene Wege granular aktiviert werden.

Dabei werden die bekannten Authenticator-Apps für mobile Geräte wie Smartphones unterstützt.

Es ist zu beachten, dass im Fall eines Verlusts des Authenticators im schlimmsten Fall nur ein vollständiger Geräte-Reset möglich ist. Daher wird empfohlen nicht für alle Konfigurationswege 2FA anzufordern, z. B. nicht für den Zugriff per serieller Schnittstelle oder den Zugriff aus dem LAN heraus, so dass bei Verlust oder Fehlkonfiguration der Zugriff auf normalem Wege auch ohne 2FA weiterhin möglich ist.

Insbesondere wird der 2FA-Schutz für den Zugriff über die WAN-Schnittstelle inkl. der Nutzung von nur verschlüsselten Protokollen wie HTTPS oder SSH empfohlen.

Die Nutzung der 2FA setzt eine korrekte Uhrzeit des Geräts voraus. Daher sollte in jedem Fall der Zeitbezug per NTP-Client auf dem Router konfiguriert werden in LANconfig unter **Datum/Zeit** > **Synchronisierung**.

Der Ablauf der grundlegenden Konfiguration der Zwei-Faktor-Authentifizierung ist wie folgt:

1. Erzeugung eines Eintrags in der Tabelle „Admin-OTPs" (LANconfig: **Management** > **Admin** > **Geräte-Konfiguration** > **Admin-OTPs**) unter Angabe des Administrator-Account-Namens für den dieser Eintrag gelten soll
2. Aufruf der WEBconfig unter**Extras** > **Admin-OTPs**. Von dort kann der erzeugte QR-Code für den Benutzer anzeigt, gespeichert oder von der externen Authenticator-App eingescannt werden
3. Beim Aufruf der Managementverbindung des Admin-Benutzers wird dieser nach dem Passwort zur Eingabe des Einmalpassworts (OTP) aufgefordert

In dieser Tabelle werden die OTP-Administratoren definiert.

SNMP-ID:

2.11.101

Pfad Konsole:

Setup > **Config**

3.1.2.1.1 Administrator

Benutzername des Administrators, für den die Zwei-Faktor-Authentifizierung aktiviert werden soll, z. B. „root".

SNMP-ID:

2.11.101.1

Pfad Konsole:

Setup > **Config** > **Admin-OTPs**

Mögliche Werte:

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

3.1.2.1.2 Hash-Algorithmus

Definiert den verwendeten Hash-Algorithmus.

Beachten Sie, dass die Authenticator-App den maximal möglichen Hash-Algorithmus unterstützt.

SNMP-ID:

2.11.101.2

Pfad Konsole:

Setup > **Config** > **Admin-OTPs**

Mögliche Werte:

SHA1
SHA256
SHA512

3.1.2.1.3 Zeitschritt

Definiert das Intervall in Sekunden, nach dem ein neues OTP berechnet wird.

SNMP-ID:

2.11.101.3

Pfad Konsole:

Setup > **Config** > **Admin-OTPs**

Mögliche Werte:

max. 10 Zeichen aus `[0-9]`

3.1.2.1.4 Netzwerk-Verzoegerung

Definiert, um wie viele Zeitschritte die Uhr des Clients maximal abweichen darf. Das Gerät prüft das um diesen Wert ältere bzw. neuere OTP.

SNMP-ID:

2.11.101.4

Pfad Konsole:

Setup > **Config** > **Admin-OTPs**

Mögliche Werte:

max. 3 Zeichen aus `[0-9]`

3.1.2.1.5 Secret

Definiert das eigentliche Shared Secret, das mit der Authenticator-App geteilt werden muss. Das Secret muss für jeden Benutzer unterschiedlich sein. Es gibt aktuell in der Tabelle drei Eingabemöglichkeiten:

Base32 (Default)

Präfix „base32:" und danach das Base32-kodierte Secret. Der Präfix darf auch weggelassen werden.

Hexadezimal

Präfix „hex:" und danach eine gerade Anzahl von Hex-Digits.

Plain text passphrase

Präfix „ascii:" und danach die Zeichen.

Für den Google Authenticator muss das Secret 16 Zeichen (80 Bit, Base32 codiert) lang sein, z. B. E3U5IDWEE3KFCJ7G

SNMP-ID:

2.11.101.5

Pfad Konsole:

Setup > **Config** > **Admin-OTPs**

Mögliche Werte:

max. 32 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

3.1.2.1.6 Aussteller

Frei definierbarer Text, der im Authenticator dazu dient, mehrere Schlüssel auseinanderzuhalten bzw. der allgemeinen Anzeige dient, wenn der gleiche Benutzername verwendet wird. Der Wert darf keinen Doppelpunkt enthalten.

SNMP-ID:

2.11.101.6

Pfad Konsole:

Setup > **Config** > **Admin-OTPs**

Mögliche Werte:

max. 32 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

3.1.2.1.7 Anzahl-Stellen

Länge der OTPs.

Für den Google Authenticator sollte der Wert 6 verwendet werden.

SNMP-ID:

2.11.101.7

Pfad Konsole:

Setup > **Config** > **Admin-OTPs**

Mögliche Werte:

max. 3 Zeichen aus `[0-9]`

3.1.2.1.8 Auf-Outband-Verlangen

Definiert, ob die Zwei-Faktor-Authentifizierung für diesen Benutzer bei Anmeldung über die serielle Schnittstelle erforderlich ist bzw. durch das Gerät abgefragt werden soll.

SNMP-ID:

2.11.101.11

Pfad Konsole:

Setup > **Config** > **Admin-OTPs**

Mögliche Werte:

Nein
Ja

3.1.2.1.9 Auf-Telnet-Verlangen

Definiert, ob die Zwei-Faktor-Authentifizierung für diesen Benutzer bei Anmeldung über Telnet erforderlich ist bzw. durch das Gerät abgefragt werden soll. Es ist granular konfigurierbar, über welche Zugriffswege die Zwei-Faktor-Authentifizierung erforderlich ist, z. B. nur über eine WAN-Verbindung.

SNMP-ID:

2.11.101.12

Pfad Konsole:

Setup > **Config** > **Admin-OTPs**

Mögliche Werte:

niemals
LAN
WAN
WLAN
VPN-ueber-LAN
VPN-ueber-WAN
VPN-ueber-WLAN
immer

3.1.2.1.10 Auf-TFTP-Verlangen

Definiert, ob die Zwei-Faktor-Authentifizierung für diesen Benutzer bei Anmeldung über TFTP erforderlich ist bzw. durch das Gerät abgefragt werden soll. Es ist granular konfigurierbar, über welche Zugriffswege die Zwei-Faktor-Authentifizierung erforderlich ist, z. B. nur über eine WAN-Verbindung.

SNMP-ID:

2.11.101.13

Pfad Konsole:

Setup > **Config** > **Admin-OTPs**

Mögliche Werte:

niemals
LAN
WAN
WLAN
VPN-ueber-LAN
VPN-ueber-WAN
VPN-ueber-WLAN
immer

3.1.2.1.11 Auf-HTTP-Verlangen

Definiert, ob die Zwei-Faktor-Authentifizierung für diesen Benutzer bei Anmeldung über HTTP erforderlich ist bzw. durch das Gerät abgefragt werden soll. Es ist granular konfigurierbar, über welche Zugriffswege die Zwei-Faktor-Authentifizierung erforderlich ist, z. B. nur über eine WAN-Verbindung.

SNMP-ID:

2.11.101.14

Pfad Konsole:

Setup > **Config** > **Admin-OTPs**

Mögliche Werte:

niemals
LAN
WAN
WLAN
VPN-ueber-LAN
VPN-ueber-WAN
VPN-ueber-WLAN
immer

3.1.2.1.12 Auf-HTTPS-Verlangen

Definiert, ob die Zwei-Faktor-Authentifizierung für diesen Benutzer bei Anmeldung über HTTPS erforderlich ist bzw. durch das Gerät abgefragt werden soll. Es ist granular konfigurierbar, über welche Zugriffswege die Zwei-Faktor-Authentifizierung erforderlich ist, z. B. nur über eine WAN-Verbindung.

SNMP-ID:

2.11.101.16

Pfad Konsole:

Setup > **Config** > **Admin-OTPs**

Mögliche Werte:

niemals
LAN
WAN
WLAN
VPN-ueber-LAN
VPN-ueber-WAN
VPN-ueber-WLAN
immer

3.1.2.1.13 Auf-Telnet-SSL-Verlangen

Definiert, ob die Zwei-Faktor-Authentifizierung für diesen Benutzer bei Anmeldung über Telnet-SSL erforderlich ist bzw. durch das Gerät abgefragt werden soll. Es ist granular konfigurierbar, über welche Zugriffswege die Zwei-Faktor-Authentifizierung erforderlich ist, z. B. nur über eine WAN-Verbindung.

SNMP-ID:

2.11.101.17

Pfad Konsole:

Setup > **Config** > **Admin-OTPs**

Mögliche Werte:

niemals
LAN
WAN
WLAN
VPN-ueber-LAN
VPN-ueber-WAN
VPN-ueber-WLAN
immer

3.1.2.1.14 Auf-SSH-Verlangen

Definiert, ob die Zwei-Faktor-Authentifizierung für diesen Benutzer bei Anmeldung über SSH erforderlich ist bzw. durch das Gerät abgefragt werden soll. Es ist granular konfigurierbar, über welche Zugriffswege die Zwei-Faktor-Authentifizierung erforderlich ist, z. B. nur über eine WAN-Verbindung.

SNMP-ID:

2.11.101.18

Pfad Konsole:

Setup > **Config** > **Admin-OTPs**

Mögliche Werte:

niemals
LAN
WAN
WLAN
VPN-ueber-LAN
VPN-ueber-WAN
VPN-ueber-WLAN
immer

4 Routing und WAN-Verbindungen

4.1 eSIM

Um Zugang zu Mobilfunknetzen zu erhalten, vergeben Mobilfunkprovider sogenannte SIM-Karten (Subscriber Identity Module Card) an ihre Kunden. Dabei vergibt jeder Provider eigene und individuelle SIM-Karten pro Kunde. Die SIM-Karten bestehen aus einem Träger aus Plastik und einem Sicherheitschip mit entsprechenden Sicherheitsschlüsseln, die Zugang zum Mobilfunknetz gewähren. Möchte ein Kunde den Provider wechseln, musste der Kunde die alte SIM-Karte gegen eine SIM-Karte des neuen Providers im Gerät austauschen. Die SIM-Karten werden vom Provider in der Regel auf dem Postweg versendet, die der Kunden nach einigen Tagen nach Abschluss des Vertrags erhält.

Eine eSIM ist vereinfacht gesprochen die digitale Version der klassischen SIM-Karte. Diese besteht aus einem Chip (z. B. im M2FF-Formatfaktor), der fest im Mobiltelefon oder Router verbaut ist und einer Lösung zur Verwaltung von Mobilfunkprofilen bzw. der Technologie, auch als eUICC (embedded Universal Integrated Circuit Card), bezeichnet. eUICC-Funktionaliät kann auf unterschiedlichen Formfaktoren bereitgestellt werden. Im Folgenden werden die Begriffe eSIM und eUICC zur Vereinfachung synonym verwendet.

Grundsätzlich existieren drei verschieden Typen bzw. Lösungsarchitekturen von eSIMs:

1. M2M-eSIM: Machine-to-Machine (M2M) eSIMs sind für Maschinen und Gerätetypen entworfen ohne Benutzeroberfläche oder die Interkation eines Benutzers am Gerät. Dabei werden die M2M eSIMs zentral von einem Verwaltungsportal bzw. Provisierungssystem gesteuert und können Over-the-Air (OTA) per SMS an das Endgerät übertragen werden. In der Regel handelt es sich hierbei geschlossene Systeme von Lösungsanbietern für Kunden mit vielen Endgeräten. M2M-eSIMs sind nach dem Standard SGP.02 spezifiziert.
2. Consumer-eSIMs: Consumer eSIMs werden von Mobilfunkprovidern herausgegeben und werden in Mobiltelefonen, Smartwatches oder Routern verwendet. In der Regel stellt der Provider einen QR-Code oder Aktivierungscode zur Verfügung mit denen der Kunde die eSIM bzw. das Profil auf dem Endgerät installieren kann. Weiterhin existieren geschlossene bzw. proprietäre Provisierungssysteme von bestimmten Smartphone-Herstellern, mit denen der Mobilfunkprovider den Kunden benachrichtigen kann, dass die eSIM zur Abholung bereit ist. Im Unterschied zur M2M-eSIM muss der Endkunde das Installieren der eSIM starten. Endgeräte besitzen eine Software, den sog. Local Profile Assistant (LPA), der die verschlüsselte Kommunikation zwischen dem verbauten eSIM-Chip/Mobilfunkchip und dem System des Mobilfunkproviders herstellt. Der Download des eSIM-Profils muss dabei immer über eine vorhandene Internetverbindung, z.B. über das integrierte WLAN im Mobiltelefon, hergestellt werden. Consumer-eSIMs sind nach dem SGP.22 Standard definiert.
3. IoT-eSIM: IoT-SIMs sind für eine große Menge an IoT-Geräten entworfen worden und kombinieren die Teilfunktion eines LPAs auf dem Endgerät mit einem Server zur Verwaltung der eSIMs. IoT-eSIMs sind im Standard SGP.32 definiert und zeitlich gesehen die neuste der Lösungsarchitekturen.

In LANCOM Routern ist eine eSIM-Chip im M2FF-Formfaktor mit eUICC-Funktionalität verbaut. Dabei handelt es sich um eine Consumer-eSIM nach dem SGP.22 Standard. Diese Lösung ist kompatibel mit gängigen eSIMs wie sie von Mobilfunkprovidern für Mobiltelefone vergeben werden. Die eSIM ist nutzbar mit allen Mobilfunkprofilen für Consumer eSIMs nach dem SGP.22 Standard und wird nicht technisch eingeschränkt. Grundsätzlich müssen eSIMs vom Mobilfunkprovider unterstützt werden und dürfen nicht auf bestimmte Endgeräte bzw. Gerätetypen vom Provider begrenzt sein.

Ab LCOS 10.94 unterstützen LANCOM Router neben klassischen Plastik-SIM-Karten auch eine eSIM-Lösung in Mobilfunkroutern. Dazu sind mehrere Voraussetzungen notwendig:

1. Mindestens LCOS 10.94 Firmware
2. Mobilfunkrouter mit verbauten eSIM-Chip on Board
3. Ggf. Update der WWAN-Firmware auf die Mindestversion zur Unterstützung der eSIM-Funktionalität

Der grobe Ablauf einer eSIM-Installation auf einem LANCOM Router ist wie folgt:

1. Abschluss eines Mobilfunkvertrags bei einem Provider.
2. Der Provider stellt einen QR-Code bzw. Aktivierungscode (beide Elemente enthalten die identischen Informationen nur in einem anderen Darstellungsformat) der eSIM zur Verfügung.
3. Der Aktivierungscode wird über die WEBconfig oder Kommandozeile des Routers eingefügt. Der Router lädt im nächsten Schritt das entsprechende Profil vom Server des Providers über eine vorhandene Internetverbindung (z. B. DSL oder Glasfaser) auf den integrierten Chip herunter. Das Profil wird fest im Chip gespeichert. Im Aktivierungscode ist neben der Server URL auch ein Code zum Abruf der eSIM enthalten.
4. Die erfolgreich heruntergeladene eSIM wird in der WWAN-Profiltabelle des Routers zur Verwendung konfiguriert.

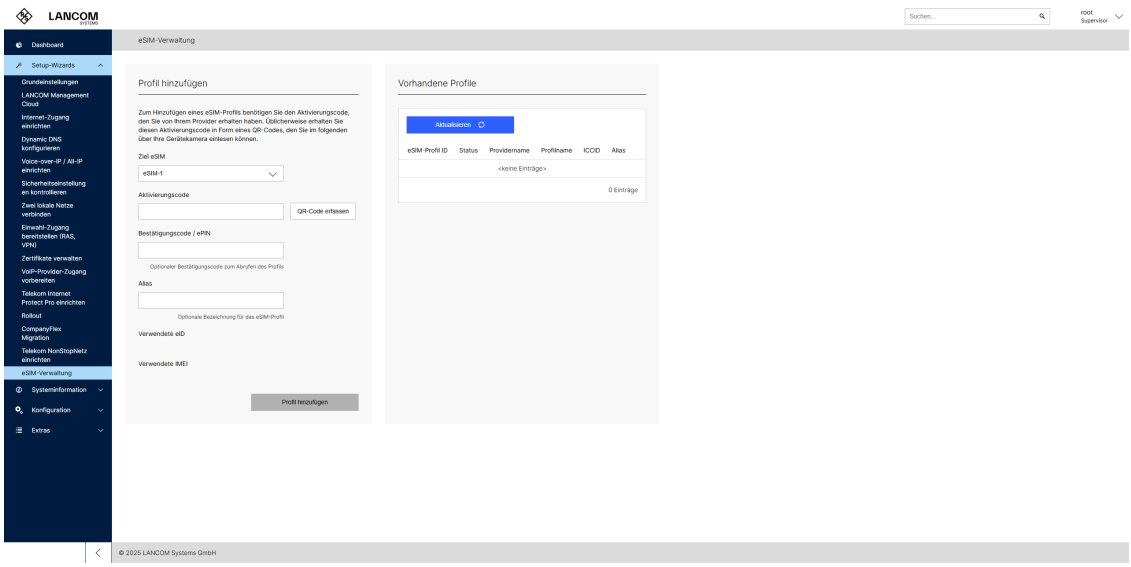
Zum Download der eSIM benötigt der Router eine vorhandene Internetverbindung, z. B. über DSL oder Glasfaser, ähnlich wie es bei einem Mobiltelefon erforderlich ist, so dass das Gerät eine WLAN-Verbindung hat. Es ist technisch nicht möglich die eSIM über das WWAN-Modem im selben Gerät herunterzuladen, da der Prozess der eSIM-Installation eine exklusive, zusammenhängende Operation im Mobilfunkchip ist und der Router dabei den Zugriff von der physischen SIM-Karte auf die eSIM umschalten muss.

Weitere Hinweise zum Einsatz:

- Es können bis zu acht eSIM-Profile auf der integrierten eSIM gespeichert werden
- eSIMs können über die WEBconfig oder per CLI-Kommandos installiert und verwaltet werden
- Ein ggf. optional vorhandenes GSMA-Testprofil auf der eSIM kann gefahrlos gelöscht werden und dient zur Vereinfachung von Tests für Mobilfunkprovider oder Anwendungsentwicklern sowie für Zulassungs- bzw. Testverfahren
- Die eSIM ist als „virtueller SIM-Slot" realisiert, der bis zu acht Profile enthalten kann
- Immer das aktive eSIM-Profil wird verwendet, wenn die eSIM per „eSIM-1" in der SIM-Slot-Konfiguration referenziert wird
- Wenn das interne Mobilfunkmodem nicht verfügbar ist, ist kein Zugriff auf die eSIM-Verwaltung möglich
- Ein Gerätereset ist keine sichere Methode, um die eSIM-Profile zu löschen, da nicht sichergestellt ist, dass das Mobilfunkmodem im Zustand ist, so dass Modem in diesem Moment Zugriff auf die eSIM hat
- Sollen die eSIMs sicher gelöscht werden, so müssen die Profile manuell über die eSIM-Verwaltung gelöscht werden. Ist dies nicht möglich, so kann das entsprechende eSIM-Profil notfalls vom Provider gesperrt werden, so wie dies auch bisher bei physischem SIM-Karten möglich ist
- eSIMs können in der Regel nur einmal heruntergeladen werden bzw. nicht erneut heruntergeladen werden. eSIMs müssen vom Provider grundsätzlich erneut zum Herunterladen freigegeben werden.
- Heruntergeladene eSIMs sind fest mit dem verbauten Chip verbunden und können nicht zwischen verschiedenen Geräten übertragen werden.

4.1.1 Konfiguration

Öffnen Sie in der WEBconfig des Geräts den Abschnitt **Profil hinzufügen** unter **Setup-Wizards** > **eSIM-Verwaltung**.



Ziel eSIM

Wählen Sie die gewünschte Ziel eSIM aus, z. B. eSIM-1.

Aktivierungscode

Fügen Sie hier den eSIM-Aktivierungscode ein, den Sie vom Mobilfunkprovider erhalten haben, z. B. `LPA:1$prov.exmaple.com$ABCDEFGH12345`.

Hierbei handelt es sich um den sog. LPA-String („Local Profile Assistant"-String). Dieser ist eine Zeichenkette, die die Adresse des SM-DP+ Servers (Server für das Profil-Management) und einen Aktivierungscode enthält, um ein eSIM-Profil manuell auf einem Gerät zu installieren, der identisch zum Inhalt des QR-Codes ist. Die Zeichenkette hat das Format LPA:1$SM-DP+Adresse$Aktivierungscode und wird vom LPA im Gerät verwendet, um das eSIM-Profil vom SM-DP+ Server über eine bestehende Internetverbindung herunterzuladen und zu installieren.

Der Aktivierungscode kann entweder als Text eingefügt werden oder per QR-Code eingelesen werden, falls das Gerät über eine Kamera verfügt.

Bestätigungscode / ePIN

Optionaler Bestätigungscode, der zusammen mit dem Aktivierungscode eingegeben wird. Manche Provider bezeichnen diesen auch als ePIN. Den Code erhalten Sie von ihrem Mobilfunkprovider zusammen mit dem QR-Code/Aktivierungscode.

Alias

Das Alias ist eine optionale Bezeichnung für das eSIM-Profil. Darüber kann das Profil in der Profiltabelle leichter identifiziert werden.

Verwendete eID

Anzeige der eID (Embedded Identity Document). Die eID ist die weltweit eindeutige Identifizierung der verbauten eSIM in dem Gerät. Die Angabe dient der Information.

Verwendete IMEI

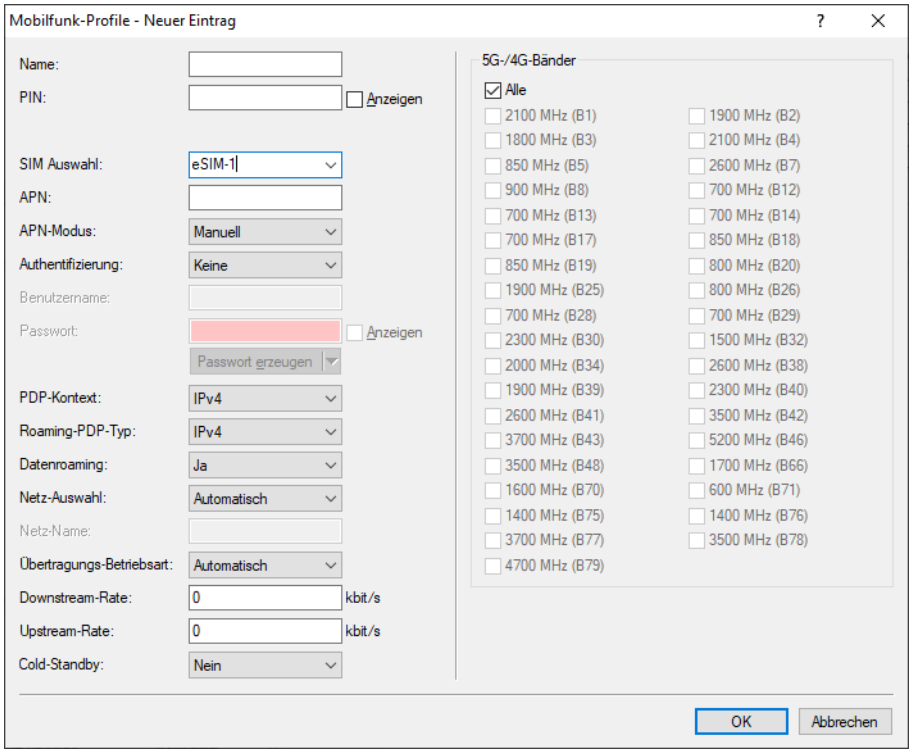
Anzeige der IMEI (International Mobile Equipment Identity). Die IMEI ist eine 15-stellige Nummer, die Ihrem LANCOM Mobilfunkrouter zugeordnet ist und diesen weltweit eindeutig identifiziert. Die Angabe dient der Information.

Abschnitt „Vorhandene Profile“

Dieser Bereich zeigt die gespeicherten eSIM-Profil auf dem lokalen Gerät an. Es kann grundsätzlich immer nur ein eSIM-Profil gleichzeitig aktiv sein. Das aktive Profil kann in der Konfiguration der WWAN-Profile in der SIM-Auswahl als „eSIM-1“ verwendet werden.

WWAN-Profil in LANconfig zuweisen

Öffnen Sie in LANconfig unter **Schnittstellen** > **WAN** > **Mobilfunk-Einstellungen** > **Mobilfunk-Profile**.



SIM-Auswahl

Definiert den verwendeten SIM-Slot oder eSIM des Geräts. Möglich Werte (abhängig vom Gerät):

- SIM-1 (Default): erster SIM-Slot im Gerät
- SIM-2: zweiter SIM-Slot im Gerät
- eSIM-1: fest verbaute eSIM im Gerät. Es wird das aktuell in der WEBconfig konfigurierte aktive Profil verwendet.
- Iccid:<iccid der SIM-Karte oder des eSIM-Profils>: Mit diesem Wert kann die SIM-Karte oder das eSIM-Profil explizit durch die eindeutige ICCID (Integrated Circuit Card Identification) ausgewählt werden. Die ICCID der installierten eSIM-Profile finden Sie in der eSIM-Verwaltung der WEBconfig.

4.1.2 CLI-Konfiguration

eSIMs können neben der Verwaltung über die WEBconfig auch über die Kommandozeile verwaltet werden. Darüber können eSIM-Profile heruntergeladen oder gelöscht werden.

Unter **Status** > **Modem-Mobile** > **eSIM** finden Sie die Status-Tabelle **eSIM-Profiles**, welche die aktuell installierten eSIMs anzeigt.

Außerdem finden Sie hier die Aktionen Change-Alias, Delete-Profile und Download-Profile.

Change-Alias

Mit diesem Kommando kann das Alias bzw. der frei definierbare Bezeichner der eSIM verändert werden.

Usage: do Change-Alias "<eSIM Profile ID>" "<New alias>"

Delete-Profile

Mit diesem Kommando kann ein eSIM-Profil gelöscht werden.

Usage: do Delete-Profile <eSIM Profile ID>

Download-Profile

Mit diesem Kommando kann der Download eines eSIM-Profils durchgeführt werden.

Usage: do Download-Profile [Option]... "<eSIM activation code>"

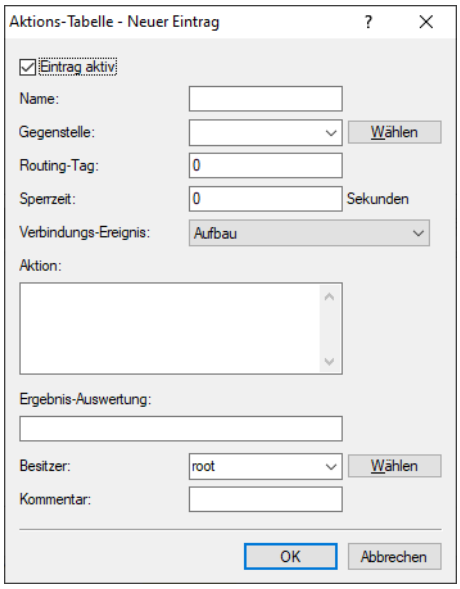
Optionen:

- -a "<Alias>" – Alias für das Profil nach dem Download setzen
- -c "<Confirmation code>" – Bestätigungscode angeben
- -s "<Target SIM>" – Ziel-SIM festlegen (Standard: eSIM-1)

4.2 Weitere IPv6-Variable für die Aktionstabelle

Ab LCOS 10.94 kann in der Aktionstabelle eine weitere Variable für IPv6 verwendet werden.

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



Unter **Aktion** können Sie diese Variable zur Erweiterung der Aktionen verwenden:

%w

Variable für IPv6. Mit der Variable %w kann zusammen mit dem Netzwerknamen, z. B. %{wINTRANET}, eine statische Adresse mit festem Host-Identifier für eine beliebige Station im lokalen Netzwerk übertragen werden.

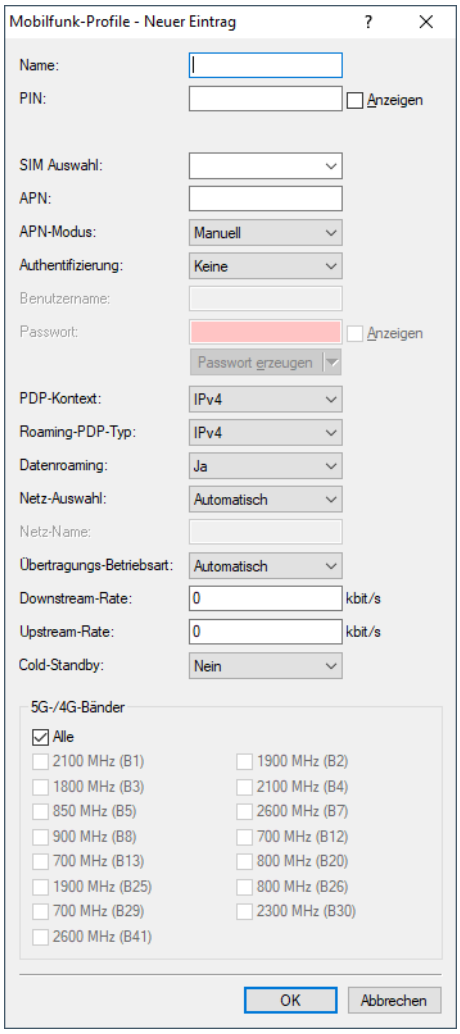
Beispiel: `%{wINTRANET}dd06:57b3:f1ee:201e` ergibt zusammen mit dem Präfix `2003:c9:1703:5b51::/64` auf dem Netzwerk INTRANET:

```
2003:c9:1703:5b51:dd06:57b3:f1ee:20ff
```

Dabei wird das Präfix so formatiert, dass nur noch der 64-Bit-Host-Anteil angehängt werden muss, um eine vollständige 128 Bit-Adresse zu ergeben. Die Präfixlänge „::64/" wird dabei abgeschnitten.

4.3 APN-Zugangsdaten in WWAN-Profiltabelle konfigurierbar machen

Ab LCOS 10.94 können Sie in der WWAN-Profiltabelle unter **Schnittstellen** > **WAN** > **Mobilfunk-Profile** definieren, ob für die Anmeldung am APN eine Authentifizierung erforderlich ist.



Authentifizierung

Geben Sie hier an, ob ob für die Anmeldung am APN eine Authentifizierung erforderlich ist. Mögliche Werte: Keine, PAP, CHAP

Benutzername

Falls für die Anmeldung am APN eine Authentifizierung erforderlich ist, dann geben Sie hier den Butzernamen an.

Passwort

Falls für die Anmeldung am APN eine Authentifizierung erforderlich ist, dann geben Sie hier das Passwort an.

4.3.1 Ergänzungen im Setup-Menü

4.3.1.1 Authentifizierung

Geben Sie hier an, ob ob für die Anmeldung am APN eine Authentifizierung erforderlich ist.

SNMP-ID:

2.23.41.1.19

Pfad Konsole:

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

Mögliche Werte:

Kein(e)
PAP
CHAP

Default-Wert:

Kein(e)

4.3.1.2 Benutzer

Falls für die Anmeldung am APN eine Authentifizierung erforderlich ist, dann geben Sie hier den Butzernamen an.

SNMP-ID:

2.23.41.1.20

Pfad Konsole:

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

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default-Wert:

leer

4.3.1.3 Passwort

Falls für die Anmeldung am APN eine Authentifizierung erforderlich ist, dann geben Sie hier das Passwort an.

SNMP-ID:

2.23.41.1.21

Pfad Konsole:

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

Mögliche Werte:

max. 32 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default-Wert:

leer

4.4 WWAN-Bridge-Mode

Das im Router integrierte Mobilfunkmodem kann in zwei Betriebsarten verwendet werden: Router-Modus sowie Bridge-Modus. Im Router-Modus baut der Router die Mobilfunkverbindung selbst auf und erhält auf seiner WWAN-Verbindung eine IP-Adresse (z. B. IPv4-Adresse und / oder IPv6-Adresse / Präfix) mit der ein dahinterliegendes Netzwerk mittels Network Address Translation (NAT) Zugriff zum Internet erhält. Die vom Provider vergebene IP-Adresse wird in diesem Fall mit mehreren Clients im LAN geteilt.

Im Bridge-Modus agiert der Router als einfache Netzwerk-Bridge und leitet alle IP-Pakete vom Mobilfunknetz an genau ein nachgeschaltetes Gerät weiter. Dieses Gerät erhält somit direkt die vom Provider vergebene IP-Adresse und muss die WAN-Verbindung (über DHCP) zum Provider aufbauen und sich um das NAT und Routing für das interne Netz kümmern.

Der Bridge-Mode ist dann sinnvoll, wenn das Gerät als reines Modem arbeiten soll, um z. B. in einer Router-Kaskade doppeltes NAT zu vermeiden. Der WWAN-Bridge-Mode ist vom Prinzip vergleichbar mit dem Bridge-Mode für DSL-Modems.

Das Gerät, welches den Bridge-Mode bereitstellt, hat selbst auf dem WWAN-Interface keine IP-Adresse und kann somit selbst keine direkte Verbindung ins Mobilfunknetz herstellen, da die Datenpakete transparent weitergeleitet werden. Soll das Gerät beispielsweise über die LMC verwaltet werden, so muss der Zugang zum Internet über einen anderen Weg erfolgen.

Es erhält genau der erste Client, der sich mit dem Gerät im Bridge-Modus verbunden hat, die vom Mobilfunknetz vergebene IP-Adresse. Die Pakete vom Mobilfunk-Modem werden ohne VLAN-Tag übergeben.

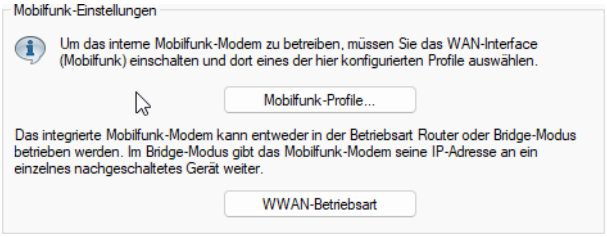
Es wird empfohlen auf dem nachgeschalteten Gerät ein ICMP-Polling auf der WAN-Verbindung einzurichten, da es konzeptbedingt nicht möglich ist, dass das Modem das nachgeschaltete Gerät über einen Verbindungsabbruch mit Adresswechsel zu informieren. Durch das ICMP-Polling kann das nachgeschaltete Gerät einen Abbruch der Mobilfunkverbindung erkennen.

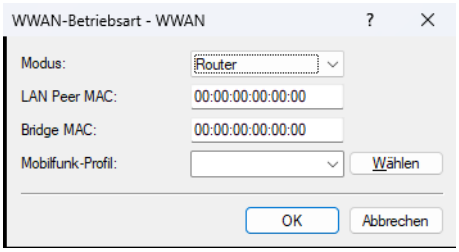
Die Konfiguration des WWAN-Bridge-Modus erfolgt grob in den folgenden Schritten:

1. Die Betriebsart des WWAN-Modems wird auf „Bridge“ konfiguriert, wobei auch ein entsprechendes WWAN-Profil für die Mobilfunkparameter angegeben werden muss
2. Das Interface „WWAN“ wird zusammen mit einem LAN-Interface (z. B. LAN-2) in eine gemeinsame Bridge-Gruppe konfiguriert. Das entsprechende LAN-Interface wird einem ETH-Port zugeordnet.

4.4.1 Konfiguration

Die Konfiguration des WWAN-Bridge-Modus finden Sie in LANconfig unter **Schnittstellen** > **WAN** > **Mobilfunk-Einstellungen** > **WWAN-Betriebsart**.





Modus

Definiert die Betriebsart der internen Mobilfunkschnittstelle im Gerät. Mögliche Werte:

Router

Im Router-Modus baut der Router die Mobilfunkverbindung selbst auf und erhält auf seiner WWAN-Verbindung eine IP-Adresse mit der ein dahinterliegendes Netzwerk mittels Network Address Translation (NAT) Zugriff zum Internet erhält.

Bridge

Im Bridge-Modus agiert der Router als einfache Netzwerk-Bridge und leitet alle IP-Pakete vom Mobilfunknetz an genau ein nachgeschaltetes Gerät weiter. Die genaue Bridge-Konfiguration erfolgt in der LAN-Bridge.

LAN Peer MAC

MAC-Adresse des Geräts bzw. Clients im LAN, dass die IP-Adresse direkt vom Mobilfunknetz erhalten soll. Ist die MAC-Adresse 0, dann wird die aus empfangenen Paketen gelernte MAC-Adresse automatisch verwendet.

Bridge MAC

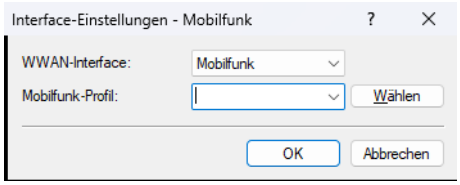
MAC-Adresse, die als Absenderadresse verwendet wird. Ist die MAC-Adresse 0, dann wird eine aus der MAC-Adresse des Geräts automatisch abgeleitete „locally administered" Adresse verwendet.

Mobilfunk-Profil

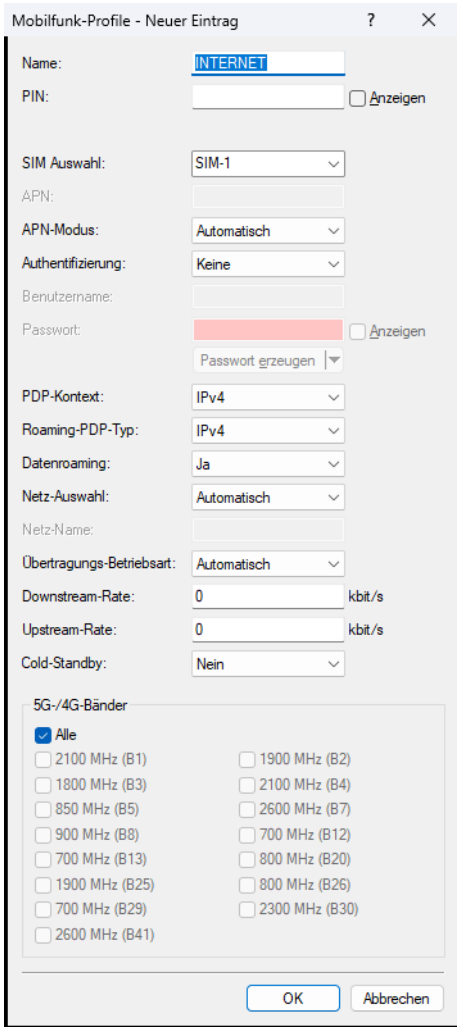
Definiert das zu verwendende WWAN-Profil.

4.4.2 WWAN-Bridge-Mode-Tutorial

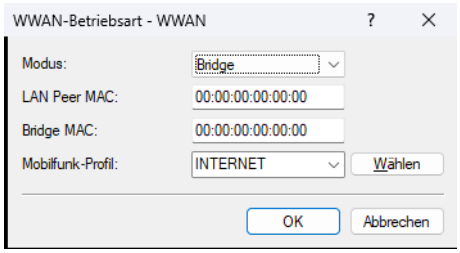
1. Öffnen Sie die Konfiguration mit LANconfig unter **Schnittstellen** > **WAN** > **Schnittstellen-Einstellungen** > **Interface-Einstellungen** > **Mobilfunk**. Setzen Sie **Mobilfunk-Profil** auf „leer".



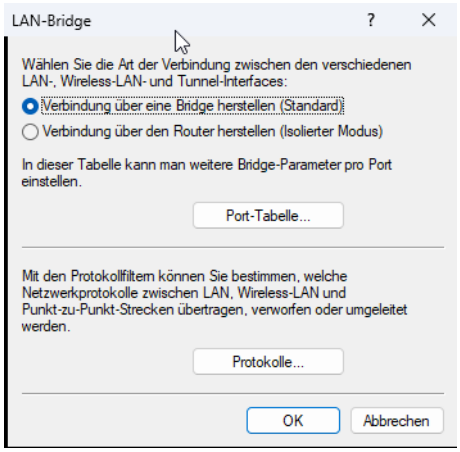
2. Öffnen Sie die Konfiguration unter **Schnittstellen** > **WAN** > **Mobilfunk-Einstellungen** > **Mobilfunk-Profile**. Setzen Sie hier die notwendigen Einstellungen für Ihren Mobilfunk-Provider.



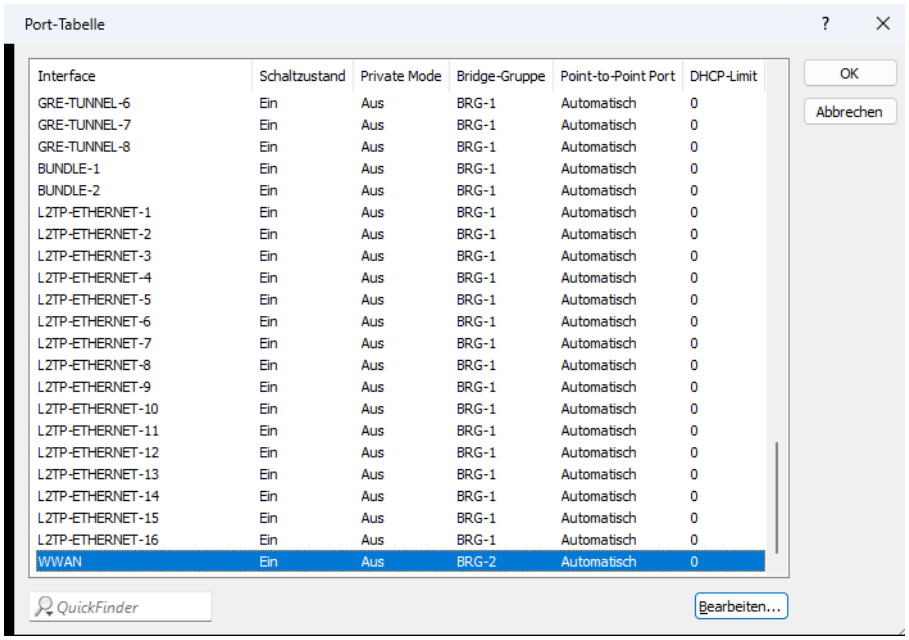
3. Öffnen Sie die Konfiguration unter **Schnittstellen** > **WAN** > **Mobilfunk-Einstellungen** > **WWAN-Betriebsart**. Setzen Sie den **Modus** auf „Bridge“, **LAN Peer MAC** und **Bridge MAC** auf „00:00:00:00:00:00“ und wählen Sie als **Mobilfunk-Profil** den Namen des WWAN-Profiles aus Schritt 2.



4. Aktivieren Sie die LAN-Bridge unter **Schnittstellen** > **LAN** > **LAN-Bridge-Einstellungen** > **LAN-Bridge**.



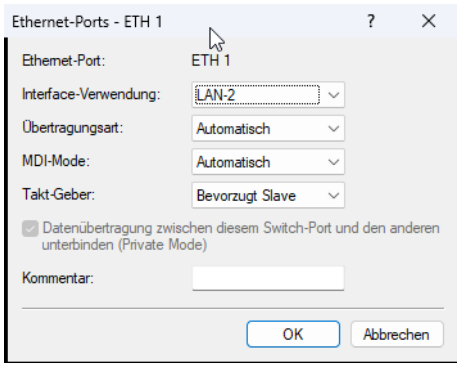
5. Öffnen Sie die **Port-Tabelle**. Um die Daten vom Mobilfunkmodem an einen Ethernet-Port weiterzugeben, müssen das WWAN-Interface und ein entsprechendes LAN-Interface in eine gemeinsame Bridge-Gruppe konfiguriert werden. In diesem Beispiel werden LAN-2 und WWAN in die Bridge-Gruppe BRG-2 konfiguriert. Verwenden Sie ggf. eine andere Bridge-Gruppe, falls BRG-2 schon für WLAN oder andere Funktionen verwendet wird.



Interface	Schaltzustand	Private Mode	Bridge-Gruppe	Point-to-Point Port	DHCP-Limit
GRE-TUNNEL-6	Ein	Aus	BRG-1	Automatisch	0
GRE-TUNNEL-7	Ein	Aus	BRG-1	Automatisch	0
GRE-TUNNEL-8	Ein	Aus	BRG-1	Automatisch	0
BUNDLE-1	Ein	Aus	BRG-1	Automatisch	0
BUNDLE-2	Ein	Aus	BRG-1	Automatisch	0
L2TP-ETHERNET-1	Ein	Aus	BRG-1	Automatisch	0
L2TP-ETHERNET-2	Ein	Aus	BRG-1	Automatisch	0
L2TP-ETHERNET-3	Ein	Aus	BRG-1	Automatisch	0
L2TP-ETHERNET-4	Ein	Aus	BRG-1	Automatisch	0
L2TP-ETHERNET-5	Ein	Aus	BRG-1	Automatisch	0
L2TP-ETHERNET-6	Ein	Aus	BRG-1	Automatisch	0
L2TP-ETHERNET-7	Ein	Aus	BRG-1	Automatisch	0
L2TP-ETHERNET-8	Ein	Aus	BRG-1	Automatisch	0
L2TP-ETHERNET-9	Ein	Aus	BRG-1	Automatisch	0
L2TP-ETHERNET-10	Ein	Aus	BRG-1	Automatisch	0
L2TP-ETHERNET-11	Ein	Aus	BRG-1	Automatisch	0
L2TP-ETHERNET-12	Ein	Aus	BRG-1	Automatisch	0
L2TP-ETHERNET-13	Ein	Aus	BRG-1	Automatisch	0
L2TP-ETHERNET-14	Ein	Aus	BRG-1	Automatisch	0
L2TP-ETHERNET-15	Ein	Aus	BRG-1	Automatisch	0
L2TP-ETHERNET-16	Ein	Aus	BRG-1	Automatisch	0
WWAN	Ein	Aus	BRG-2	Automatisch	0

6. Öffnen Sie **Schnittstellen** > **LAN** > **Ethernet-Switch-Einstellungen** > **Ethernet-Ports**.und konfigurieren Sie einen Ethernet-Port so, dass das LAN-Interface aus der gemeinsamen Bridge-Gruppe mit dem WWAN-Interface verwendet

wird. In diesem Beispiel wird LAN-2 an Ethernet-Port ETH-1 gebunden, die zusammen mit WWAN in der Bridge-Gruppe BRG-2 sind.



Bitte beachten Sie folgende Punkte:

- Eine Route oder WWAN-Gegenstellenkonfiguration ist für ein WWAN-Gerät im Bridge-Modus nicht erforderlich, da das Gerät nicht als Router arbeitet und nur eine Bridge-Konfiguration erforderlich ist. Es wird empfohlen ggf. vorhanden WWAN-Gegenstellenkonfigurationen (inkl. der Default WWAN-Zero-Touch-Gegenstelle) zu löschen, um Konfigurationsfehler sowie unnötige Fehlermeldungen zu fehlgeschlagenen Gegenstellen-Aufbauversuchen zu vermeiden.
- Der Router kann im Bridge-Betrieb nicht selbst über das Mobilfunkmodem mehr das Internet erreichen.
- Achten Sie darauf, dass am Ethernet-Port des Bridge-Modes nur ein Endgerät verbunden ist, da nur ein Endgerät eine IP-Adresse vom Mobilfunknetz erhalten kann, mit der Konfiguration der LAN-Peer-MAC-Adresse kann sichergestellt werden, dass nur eine feste MAC-Adresse die IP-Adresse erhält.
- In der WWAN-Bridge-Gruppe darf kein interner oder externe DHCP-Server aktiv sein.

4.4.3 Ergänzungen im Setup-Menü

4.4.3.1 WWAN

Einstellungen zu WWAN.

SNMP-ID:

2.46

Pfad Konsole:

Setup

4.4.3.1.1 WAN-Bridge

Das im Router integrierte Mobilfunkmodem kann in zwei Betriebsarten verwendet werden: Router-Modus sowie Bridge-Modus. Im Router-Modus baut der Router die Mobilfunkverbindung selbst auf und erhält auf seiner WWAN-Verbindung eine IP-Adresse (z. B. IPv4-Adresse und / oder IPv6-Adresse / Präfix) mit der ein dahinterliegendes Netzwerk mittels Network Address Translation (NAT) Zugriff zum Internet erhält. Die vom Provider vergebene IP-Adresse wird in diesem Fall mit mehreren Clients im LAN geteilt.

Im Bridge-Modus agiert der Router als einfache Netzwerk-Bridge und leitet alle IP-Pakete vom Mobilfunknetz an genau ein nachgeschaltetes Gerät weiter. Dieses Gerät erhält somit direkt die vom Provider vergebene IP-Adresse und muss

die WAN-Verbindung (über DHCP) zum Provider aufbauen und sich um das NAT und Routing für das interne Netz kümmern.

Der Bridge-Mode ist dann sinnvoll, wenn das Gerät als reines Modem arbeiten soll, um z. B. in einer Router-Kaskade doppeltes NAT zu vermeiden. Der WWAN-Bridge-Mode ist vom Prinzip vergleichbar mit dem Bridge-Mode für DSL-Modems.

Das Gerät, welches den Bridge-Mode bereitstellt, hat selbst auf dem WWAN-Interface keine IP-Adresse und kann somit selbst keine direkte Verbindung ins Mobilfunknetz herstellen, da die Datenpakete transparent weitergeleitet werden. Soll das Gerät beispielsweise über die LMC verwaltet werden, so muss der Zugang zum Internet über einen anderen Weg erfolgen.

Es erhält genau der erste Client, der sich mit dem Gerät im Bridge-Modus verbunden hat, die vom Mobilfunknetz vergebene IP-Adresse. Die Pakete vom Mobilfunk-Modem werden ohne VLAN-Tag übergeben.

Es wird empfohlen auf dem nachgeschalteten Gerät ein ICMP-Polling auf der WAN-Verbindung einzurichten, da es konzeptbedingt nicht möglich ist, dass das Modem das nachgeschaltete Gerät über einen Verbindungsabbruch mit Adresswechsel zu informieren. Durch das ICMP-Polling kann das nachgeschaltete Gerät einen Abbruch der Mobilfunkverbindung erkennen.

Die Konfiguration des WWAN-Bridge-Modus erfolgt grob in den folgenden Schritten:

1. Die Betriebsart des WWAN-Modems wird auf „Bridge“ konfiguriert, wobei auch ein entsprechendes WWAN-Profil für die Mobilfunkparameter angegeben werden muss
2. Das Interface „WWAN“ wird zusammen mit einem LAN-Interface (z. B. LAN-2) in eine gemeinsame Bridge-Gruppe konfiguriert. Das entsprechende LAN-Interface wird einem ETH-Port zugeordnet.

SNMP-ID:

2.46.2

Pfad Konsole:

Setup > **WWAN**

Interface

Bestimmt den Namen des internen Mobilfunkmodems, z. B. WWAN, welches verwendet werden soll.

SNMP-ID:

2.46.2.1

Pfad Konsole:

Setup > **WWAN** > **WAN-Bridge**

Mode

Definiert die Betriebsart der internen Mobilfunkschnittstelle im Gerät.

SNMP-ID:

2.46.2.2

Pfad Konsole:

Setup > **WWAN** > **WAN-Bridge**

Mögliche Werte:

Router

Im Router-Modus baut der Router die Mobilfunkverbindung selbst auf und erhält auf seiner WWAN-Verbindung eine IP-Adresse mit der ein dahinterliegendes Netzwerk mittels Network Address Translation (NAT) Zugriff zum Internet erhält.

Bridge

Im Bridge-Modus agiert der Router als einfache Netzwerk-Bridge und leitet alle IP-Pakete vom Mobilfunknetz an genau ein nachgeschaltetes Gerät weiter. Die genaue Bridge-Konfiguration erfolgt in der LAN-Bridge.

Default-Wert:

Router

LAN-Peer-MAC

MAC-Adresse des Geräts bzw. Clients im LAN, dass die IP-Adresse direkt vom Mobilfunknetz erhalten soll. Ist die MAC-Adresse 0, dann wird die aus empfangenen Paketen gelernte MAC-Adresse automatisch verwendet.

SNMP-ID:

2.46.2.3

Pfad Konsole:

Setup > **WWAN** > **WAN-Bridge**

Mögliche Werte:

max. 12 Zeichen aus `[a-f][0-9]`

Default-Wert:

000000000000

Bridge-MAC

MAC-Adresse, die als Absenderadresse verwendet wird. Ist die MAC-Adresse 0, dann wird eine aus der MAC-Adresse des Geräts automatisch abgeleitete „locally administered" Adresse verwendet.

SNMP-ID:

2.46.2.4

Pfad Konsole:

Setup > **WWAN** > **WAN-Bridge**

Mögliche Werte:

max. 12 Zeichen aus `[a-f][0-9]`

Default-Wert:

000000000000

Profil

Definiert das zu verwendende WWAN-Profil.

SNMP-ID:

2.46.2.5

Pfad Konsole:

Setup > **WWAN** > **WAN-Bridge**

Mögliche Werte:

max. 12 Zeichen aus `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

5 Virtual Private Networks – VPN

5.1 WireGuard

WireGuard ist ein einfaches und schlankes VPN-Protokoll. Im Gegensatz zu IKEv2 / IPSec ist der Fokus bei WireGuard auf Einfachheit, Schnelligkeit und gute Bedienbarkeit. Ebenso ist WireGuard ein Protokoll mit sehr kompakter Code-Basis und Funktionsumfang und ist somit ideal für den Einsatz auf IoT-Geräten und Embedded-Geräten geeignet.

IKEv2 ist ein von der IETF standardisiertes Protokoll mit vielen Erweiterungen und hoher Flexibilität, gelichzeitig, aber auch hoher Komplexität. Während IKEv2 beispielswiese Kryptoagilität besitzt, d. h. die Verschlüsselungsverfahren austauschbar sind bzw. zwischen den Endpunkten verhandelt werden können, ist bei WireGuard der Schlüsseltausch mit Curve25519 sowie das Verschlüsselungsprotokoll (ChaCha20 / Poly1305) fest definiert. Bei WireGuard ist nur eine Authentifizierung per Public- / Private-Key möglich, während die Authentifizierung bei IKEv2 flexibel ist, z. B. über PSK, Zertifikate oder EAP. Ebenso werden bei IKEv2 viele Erweiterungen unterstützt wie RADIUS oder Zwei-Faktor-Authentifizierung, was bei WireGuard nicht möglich ist. WireGuard unterstützt darüber hinaus nur die Übertragung über UDP. WireGuard besitzt dafür ein integriertes Roaming analog zum MOBIKE bei IKEv2.

IKEv2 / IPSec wird weiterhin als Standard-Protokoll für die Filialvernetzung bzw. SD-WAN aufgrund der großen Anzahl von Konfigurations- und Einsatzszenarien im LCOS empfohlen. WireGuard besitzt auf LANCOM Router-Plattformen keine Hardware-Beschleunigung für ChaChaPoly1305, so dass die Verschlüsselung in Software durchgeführt werden muss. Für Szenarien mit hoher VPN-Durchsatzleistung wird daher weiterhin IKEv2 / IPSec empfohlen.

IKEv2 / IPSec basiert im LCOS auf langjähriger Praxis in der VPN-Standortvernetzung und vielen Protokoll- und Feature-Erweiterungen für mittlere, große und komplexe VPN- bzw. SD-WAN-Szenarien. Im LCOS ist WireGuard daher eine ideale Ergänzung für einfache Szenarien, wo in der Regel nur grundlegende verschlüsselte Verbindungen benötigt werden. Ein anderes Einsatzszenario für WireGuard ist, bei dem das VPN-Protokoll z. B. durch einen Dienstleister oder VPN-Provider vorgegeben wird.

WireGuard ist vom Konzept ein „stilles" Protokoll, d.h. es werden erst Kontroll- oder Verhandlungspakte ausgetauscht, sobald Nutzdaten übertragen werden sollen. Bei IKE wird der Tunnelaufbau sofort gestartet, sobald dies in der Konfiguration so definiert ist. Aus diesem Grund gibt es bei WireGuard im LCOS keine Haltezeit bzw. eine Konfiguration dazu. WireGuard unterstützt IPv4 und IPv6, sowohl als Transportprotokoll als auch bei der Datenübertragung innerhalb des Tunnels.

Bei IPv6 müssen in der IPv6-Firewall in der Inbound-Tabelle die eingehenden UDP-Ports für den Tunnel manuell konfiguriert werden, da die Ports bei WireGuard frei konfigurierbar sind.

WireGuard-Tunnel im LCOS können sowohl „Unnumbered", d. h. ohne konfigurierte IP-Adresse, als auch mit konfigurierten IP-Adressen über **Kommunikation** > **Protokolle** > **IP-Parameter** definiert werden.

WireGuard gilt im LCOS als Interface-Typ „VPN". Die ist relevant im Zusammenhang beispielsweise mit der Zugriffs-Liste auf die Management-Protokolle auf das Gerät selbst unter **Management** > **Admin** > **Zugriffseinstellungen**.

Soll WireGuard zu einem VPN-Provider genutzt werden, der z. B. öffentliche IP-Adressen oder Subnetze zum Router über WireGuard routet, so greift hier die Einstufung als sicherer Interfacetyp „VPN".

In diesem Fall sind die Ports der Management-Protokolle oder der Voice Call Manager (VCM), die den Zugriff „nur über VPN" erlauben auf der öffentlichen IP-Adresse des WireGuard-Tunnels offen bzw. erreichbar. Falls dies nicht gewünscht sein sollte, müssen weitere Regeln für Zugriffstationen (für Management-Protokolle) oder die Einstellung auf „auf WAN nicht erlaubt" konfiguriert werden.

Dieses Verhalten gilt ebenso für den Fall das ein IPSec / IKE / IKEv2-Interface eine öffentliche IP-Adresse besitzt.

5.1.1 Lizenzierung

WireGuard zählt im LCOS als VPN-Tunnel und geht in die Lizenzzählung des Geräts mit ein und teilt sich den Lizenzpool mit anderen VPN-Tunnel wie IKE/IPSec oder PPTP-MPPE. Eine WireGuard-Lizenz geht in die Lizenzzählung ein, sobald Daten über den WireGuard-Tunnel übertragen werden. Es können beliebig viele WireGuard-Tunnel konfiguriert werden.

Weitere WireGuard-Lizenzen können über die VPN-Option aufgerüstet werden.

Beispiel:

Hat ein Gerät eine Lizenz für 5 VPN-Tunnel und es sind bereits 3 IPSec-Tunnel aufgebaut, so können noch zwei WireGuard-Tunnel verwendet werden.

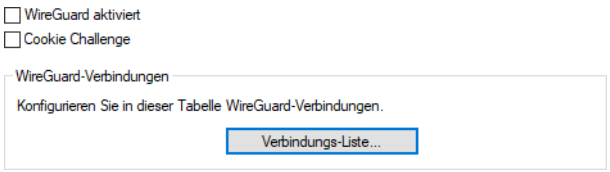
5.1.2 Konfiguration

Eine WireGuard-Konfiguration im LCOS besteht aus mindestens zwei Konfigurationselementen sowie weiteren optionalen Elementen:

1. Eintrag in der Tabelle der WireGuard-Tunnel-Konfiguration.
2. Eintrag in der IPv4- und/oder in der IPv6-Routing-Tabelle. Der Eintrag entspricht dem Konzept der „Allowed-IP-Adresses“ bei WireGuard auf anderen Plattformen.
3. (Optional) Lokale IP-Adressen für die WireGuard-Gegenstelle konfigurieren über die IP-Parameter-Tabelle in LANconfig unter **Kommunikation** > **Protokolle** > **IP-Parameter**.
4. (Optional) Firewallkonfiguration zur granularen Steuerung der Zugriffsrechte im Netzwerk.

5.1.3 Konfiguration mit LANconfig

WireGuard wird in LANconfig unter **VPN** > **WireGuard** konfiguriert.



WireGuard aktiviert

Aktiviert oder Deaktiviert die WireGuard-Funktion im Gerät.

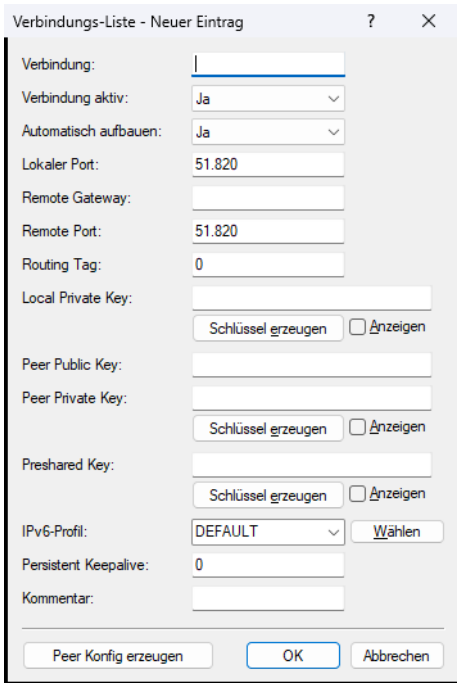
Cookie Challenge

Die Cookie Challenge ist eine Schutzmechanismus vor CPU-Erschöpfungsangriffen während des Handshakes. Grundsätzlich ist die Berechnung der Diffie-Hellman (DH)-Funktion während des WireGuard-Handshakes sehr CPU-intensiv. Ein Angreifer könnte versuchen, den Router mit einer großen Anzahl von Handshake-Anfragen zu überlasten, um ihn zum Absturz zu bringen oder seine Leistung stark zu beeinträchtigen (CPU-Erschöpfungsangriff). Dieser Mechanismus zwingt den Angreifer, für jede Handshake-Anfrage einen zusätzlichen Netzwerk-Roundtrip durchzuführen und das Cookie zu beantworten. Dies erhöht die Kosten für den Angriff erheblich und macht ihn weniger effektiv. Es ermöglicht dem Server, die Anzahl der tatsächlich durchgeführten DH-Berechnungen zu begrenzen und seine Ressourcen zu schützen.

Wenn die Cookie-Challenge aktiviert ist, sendet das Gerät beim Handshake immer eine Cookie-Reply-Nachricht.

Verbindungsliste

In dieser werden die WireGuard-Verbindungen definiert.



Verbindung

Name der WireGuard-Verbindung bzw. der WireGuard-Gegenstelle.

Verbindung aktiv

Aktiviert bzw. Deaktiviert diese Verbindung.

Automatisch aufbauen

Definiert, ob der WireGuard-Tunnel automatisch – z. B. nach dem Gerätestart oder nach dem Aufbau der WAN-Verbindung – aufgebaut werden soll, oder nur dann, wenn tatsächlich Nutzdaten übertragen werden. Dieser Schalter muss zusammen mit dem Schalter „Persistent-Keepalive“ konfiguriert werden, damit sich die WireGuard-Gegenstelle wie andere Gegenstellen verhält, die dauerhaft aktiv gehalten werden sollen.

Bei „Ja“ wird die WireGuard-Verbindung unabhängig vom Nutzdatenverkehr permanent aufgebaut. Bei „Nein“ wird die Verbindung nur bei vorhandenem Nutzdatenverkehr aufgebaut.

Lokaler Port

Definiert den lokalen (UDP-)Port auf dem diese Verbindung vom Gerät angenommen werden soll. Pro Port muss der konfigurierte lokale Private-Key identisch sein. Mehrere konfigurierte Verbindungen auf dem gleichen lokalen Port und unterschiedlichen Private-Keys werden nicht unterstützt und führen dazu, dass Verbindungen nicht aufgebaut werden können bzw. die interne Konfiguration nicht erzeugt werden kann.

Bei einem WireGuard-Tunnel mit IPv6 als Transportprotokoll müssen in der IPv6-Firewall in der Inbound-Tabelle die eingehenden UDP-Ports für den Tunnel manuell konfiguriert bzw. erlaubt werden.

Remote Gateway

IPv4-, IPv6- oder DNS-Adresse des entfernten Gateways oder Clients. Ist die IP-Adresse der remote Seite unbekannt oder dynamisch, so kann der Eintrag leer gelassen werden. In diesem Fall muss die Verbindung von der entfernten Seite aufgebaut werden. Wird eine explizite IP-Adresse konfiguriert, so muss diese beim Verbindungsaufbau exakt übereinstimmen.

Erlaubte Werte: IPv4-Adresse, IPv6-Adresse, 0.0.0.0, :: oder leerer Eintrag. Die Werte 0.0.0.0 bzw. :: für IPv6 haben die gleiche Funktion wie ein leerer Eintrag.

Remote Port

Port der Seite des entfernten Gateways. Ist der entfernte Port von eingehenden Verbindungen dynamisch oder unbekannt, so kann der Eintrag leer gelassen werden oder mit 0 konfiguriert werden. Wird ein expliziter Port konfiguriert, so muss dieser beim Verbindungsaufbau exakt übereinstimmen und wird im Fehlerfall verworfen bzw. abgelehnt.

Erlaubte Werte: Port, 0, leerer Eintrag

Routing Tag

Routing Tag, über das die WireGuard-Verbindung aufgebaut werden soll.

Local Private Key

Lokaler Private-Key der WireGuard-Verbindung im Base64-Format. Einträge im Hex-Key-Format werden nicht unterstützt. Aus dem lokalen Private-Key berechnet das Gerät automatisch seinen Public-Key.

Pro lokalen Port muss der konfigurierte lokale Private-Key identisch sein. Mehrere konfigurierte Verbindungen auf dem gleichen lokalen Port und unterschiedlichen Private-Keys werden nicht unterstützt und führen dazu, dass Verbindungen nicht aufgebaut werden können bzw. die interne Konfiguration nicht erzeugt werden kann.

Der lokale Private Key ist geheim und wird in der Regel nicht mit der entfernen Seite geteilt. Es sei denn, ein Administrator erstellt Schlüsselpaare für seine verwalteten Geräte. In diesem Fall kennt der Administrator alle Schlüsselpaare seiner Geräte.

Peer Public Key

Public Key des entfernten bzw. Remote-Gateways im Base64-Format. Einträge im Hex-Key-Format werden nicht unterstützt.

Jeder Kommunikationspartner der WireGuard-Verbindung muss ein individuelles Schlüsselpaar aus Public-/Private-Key erzeugen und der entfernen Seite seinen Public-Key mitteilen.

Peer Private Key

Der Peer Private Key ist optional und wird nur dann konfiguriert, wenn LANconfig für die Gegenseite eine Konfiguration bzw. QR-Code erzeugen soll. Er ist für die Funktion im LCOS nicht erforderlich und wird nur in der Konfiguration gespeichert, damit die Konfiguration für die Gegenseite ggf. zu einem späteren Zeitpunkt erneut angezeigt bzw. generiert werden kann.

Preshared Key

Optionaler zusätzlicher Schlüssel, der bei der Verbindung neben dem Public-/Private-Schlüsselpaar verwendet werden soll. Der Schlüssel muss auf beiden Kommunikationspartnern identisch konfiguriert werden.

IPv6-Profil

Dieser Eintrag definiert das IPv6-WAN-Profil. Ein leerer Eintrag schaltet IPv6 für dieses Interface ab.

Die IPv6-WAN-Profile konfigurieren Sie unter **IPv6** > **Allgemein** > **IPv6-Schnittstellen** > **WAN-Profile**.

Persistent Keepalive

Definiert die Zeit in Sekunden, in der das entfernte Gerät (Peer) WireGuard Keepalive-Pakete senden soll. Der Wert 0 deaktiviert das Senden von Keepalive-Paketen.

Das „Persistent Keepalive" in WireGuard sorgt dafür, dass die Verbindung auch dann aktiv gehalten wird, wenn gerade kein Datenverkehr stattfindet. Durch das regelmäßige Senden von Keepalive-Paketen wird die Verbindung, z. B. in NAT-Gateways auf der Strecke, aktiv gehalten und verhindert so ungewollte Verbindungsabbrüche.

Kommentar

Geben Sie einen Kommentar zu diesem Eintrag an.

5.1.3.1 Konfigurationsprofile für Clients

LANconfig kann innerhalb der WireGuard-Konfigurationseite minimale Konfigurationsprofile im WireGuard-Konfingurationsformat als Text oder QR-Code für entfernte WireGuard-Clients erzeugen. Diese Konfiguration kann entweder als Text-Konfiguration in kompatible WireGuard-Clients per Copy&Paste importiert werden oder direkt per QR-Code von einer mobilen App eingescannt werden.

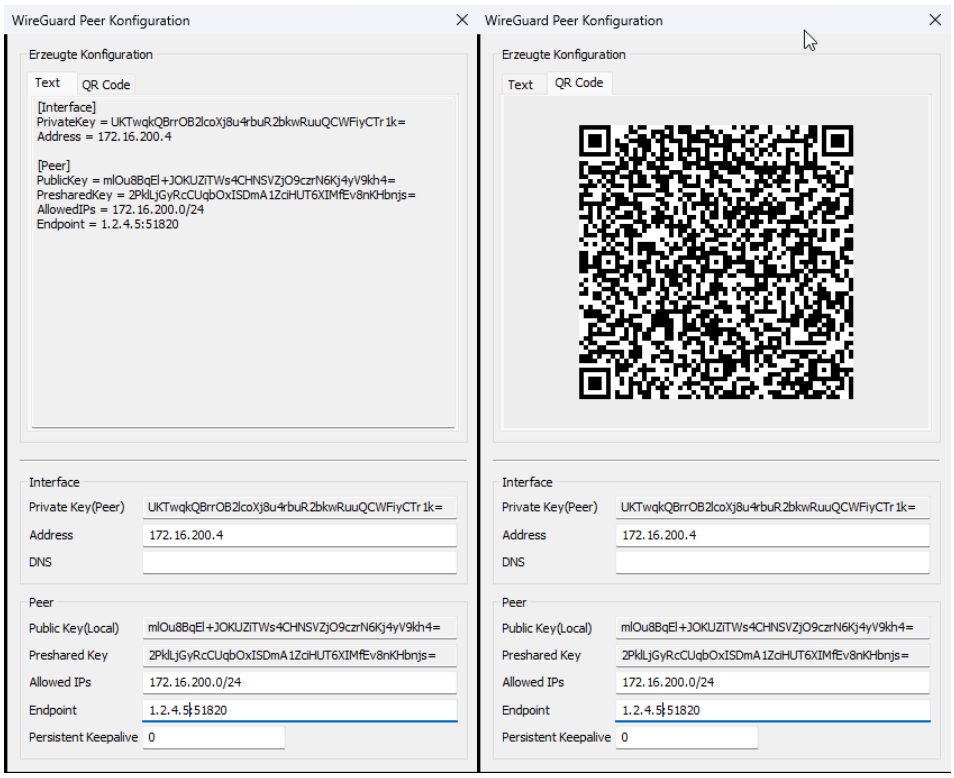
Diese Funktion entspricht der Funktion eines Wizards, allerdings mit dem Vorteil, dass diese Konfiguration jederzeit erneut aufgerufen und angezeigt werden kann.

Dazu muss allerdings der Router bzw. LANconfig den Private Key der Gegenseite speichern, was bei einem WireGuard-Partner aus unterschiedlichen administrativen Hoheiten normalerweise nicht gewünscht ist. In der Regel erzeugt jeder Kommunikationspartner ein Private-/Public-Schlüsselpaar und teilt der Gegenseite nur den Public Key mit. Der Private Key bleibt geheim und nur dem jeweiligen Kommunikationspartner bekannt. Diese Funktion ist ideal geeignet für Administratoren die Konfigurationen für Geräte unter eigener Kontrolle erzeugen möchten.

Die Parameter DNS sowie Pre-Shared-Key sind optional. Alle anderen Parameter müssen eingetragen werden, damit eine minimale Konfiguration erzeugt werden kann.

Die Parameter **Adresse**, **Erlaubte IPs** sowie **Endpunkt** werden nicht durch LANconfig gespeichert und müssen beim erneuten Aufruf der Konfiguration wieder eingetragen werden.

Rufen Sie die Funktion LANconfig für die jweilige WireGuard-Verbinung unter **VPN** > **WireGuard** > **Verbindungsliste** > **Peer Konfig erzeugen** auf.



Unterstützte Konfigurationsparameter für die Gegenseite:

Interface

Private Key

Definiert den privaten Schlüssel des Clients.

Adresse

Lokale IP-Adresse der WireGuard-Schnittstelle auf der Client-Seite

DNS

DNS-Server, den der Client für die DNS-Namensauflösung verwenden soll (optional).

Peer

Aus der Sicht des entfernten Clients ist hier das LCOS der Peer

Public Key

Öffentlicher Schlüssel des LCOS.

Pre-Shared-Key

Optionaler, zusätzlicher Schlüssel, der bei der Verbindung neben dem Public-/Private-Schlüsselpaar verwendet werden soll. Der Schlüssel muss auf beiden Kommunikationspartnern identisch konfiguriert werden

Erlaubte IPs

IP-Adressen, die der Client in den WireGuard-Tunnel routen bzw. dort erlauben soll. Hier müssen die lokalen Netze des Routers eingetragen werden, die der Client erreichen soll.

Endpunkt

Öffentliche IP-Adresse inkl. Port im Format <IP-Adresse>:<Port> des LCOS zu dem der Client die Verbindung aufbauen soll.

Persistent Keepalive

Definiert die Zeit in Sekunden, in der das entfernte Gerät (Peer) WireGuard Keepalive-Pakete senden soll. Der Wert 0 deaktiviert das Senden von Keepalive-Paketen.

Das „Persistent Keepalive" in WireGuard sorgt dafür, dass die Verbindung auch dann aktiv gehalten wird, wenn gerade kein Datenverkehr stattfindet. Durch das regelmäßige Senden von Keepalive-Paketen wird die Verbindung, z. B. in NAT-Gateways auf der Strecke, aktiv gehalten und verhindert so ungewollte Verbindungsabbrüche.

QR-Code

Über den angezeigten QR-Code können Sie die Konfiguration in eine WireGuard-App übernehmen. Öffnen Sie die Wirguard-App und fügen Sie einen neuen Peer per QR-Code hinzu. Anschließend können dort ggf. weitere Parameter geändert oder hinzugefügt werden.

5.1.4 Trace-Befehle

Dieser Parameter ...	... ruft beim Trace die folgende Anzeige hervor:
`WireGuard`	Aktiviert die grundlegenden WireGuard-Traces der Verhandlungspakete und Status- sowie Debug-Informationen.
`WG-Packet`	Zeigt die WireGuard-Nutzdaten-Pakete an.

5.1.5 Show-Kommandos

- `wg-connection` – Zeigt Informationen über WireGuard-Verbindungen an
- `wg-detail` – Zeigt Detail-Informationen über WireGuard-Verbindungen an

› `wg-peer` – Zeigt Informationen über konfigurierte WireGuard-Peers an

5.1.6 Ergänzungen im Setup-Menü

5.1.6.1 WireGuard

WireGuard ist ein einfaches und schlankes VPN-Protokoll. Im Gegensatz zu IKEv2 / IPSec ist der Fokus bei WireGuard auf Einfachheit, Schnelligkeit und gute Bedienbarkeit. Ebenso ist WireGuard ein Protokoll mit sehr kompakter Code-Basis und Funktionsumfang und ist somit ideal für den Einsatz auf IoT-Geräten und Embedded-Geräten geeignet.

Eine WireGuard-Konfiguration im LCOS besteht aus mindestens zwei Konfigurationselementen sowie weiteren optionalen Elementen:

1. Eintrag in der Tabelle der WireGuard-Tunnel-Konfiguration.
2. Eintrag in der IPv4- und/oder in der IPv6-Routing-Tabelle. Der Eintrag entspricht dem Konzept der „Allowed-IP-Adresses" bei WireGuard auf anderen Plattformen.
3. (Optional) Lokale IP-Adressen für die WireGuard-Gegenstelle konfigurieren über die IP-Parameter-Tabelle in LANconfig unter **Kommunikation** > **Protokolle** > **IP-Parameter**.
4. (Optional) Firewallkonfiguration zur granularen Steuerung der Zugriffsrechte im Netzwerk.

SNMP-ID:

2.19.70

Pfad Konsole:

Setup > **VPN**

5.1.6.1.1 Aktiv

Aktiviert oder Deaktiviert die WireGuard-Funktion im Gerät.

SNMP-ID:

2.19.70.1

Pfad Konsole:

Setup > **VPN** > **WireGuard**

Mögliche Werte:

nein
ja

Default-Wert:

nein

5.1.6.1.2 Cookie-Challenge

Die Cookie Challenge ist eine Schutzmechanismus vor CPU-Erschöpfungsangriffen während des Handshakes. Grundsätzlich ist die Berechnung der Diffie-Hellman (DH)-Funktion während des WireGuard-Handshakes sehr CPU-intensiv. Ein Angreifer könnte versuchen, den Router mit einer großen Anzahl von Handshake-Anfragen zu überlasten, um ihn zum Absturz zu

bringen oder seine Leistung stark zu beeinträchtigen (CPU-Erschöpfungsangriff). Dieser Mechanismus zwingt den Angreifer, für jede Handshake-Anfrage einen zusätzlichen Netzwerk-Roundtrip durchzuführen und das Cookie zu beantworten. Dies erhöht die Kosten für den Angriff erheblich und macht ihn weniger effektiv. Es ermöglicht dem Server, die Anzahl der tatsächlich durchgeführten DH-Berechnungen zu begrenzen und seine Ressourcen zu schützen.

Wenn die Cookie-Challenge aktiviert ist, sendet das Gerät beim Handshake immer eine Cookie-Reply-Nachricht.

SNMP-ID:

2.19.70.2

Pfad Konsole:

Setup > **VPN** > **WireGuard**

Mögliche Werte:

nein
ja

Default-Wert:

nein

5.1.6.1.3 Peers

In dieser Tabelle werden die WireGuard-Verbindungen definiert.

SNMP-ID:

2.19.70.3

Pfad Konsole:

Setup > **VPN** > **WireGuard**

Gegenstelle

Name der WireGuard-Verbindung bzw. der WireGuard-Gegenstelle.

SNMP-ID:

2.19.70.3.1

Pfad Konsole:

Setup > **VPN** > **WireGuard** > **Peers**

Mögliche Werte:

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

Default-Wert:

leer

Aktiv

Aktiviert bzw. Deaktiviert diese Verbindung.

SNMP-ID:

2.19.70.3.2

Pfad Konsole:

Setup > **VPN** > **WireGuard** > **Peers**

Mögliche Werte:

nein
ja

Default-Wert:

ja

Lokaler-Port

Definiert den lokalen (UDP-)Port auf dem diese Verbindung vom Gerät angenommen werden soll. Pro Port muss der konfigurierte lokale Private-Key identisch sein. Mehrere konfigurierte Verbindungen auf dem gleichen lokalen Port und unterschiedlichen Private-Keys werden nicht unterstützt und führen dazu, dass Verbindungen nicht aufgebaut werden können bzw. die interne Konfiguration nicht erzeugt werden kann.

Bei einem WireGuard-Tunnel mit IPv6 als Transportprotokoll müssen in der IPv6-Firewall in der Inbound-Tabelle die eingehenden UDP-Ports für den Tunnel manuell konfiguriert bzw. erlaubt werden.

SNMP-ID:

2.19.70.3.3

Pfad Konsole:

Setup > **VPN** > **WireGuard** > **Peers**

Mögliche Werte:

max. 5 Zeichen aus `[0–9]`

Default-Wert:

51820

Entferntes-Gateway

IPv4-, IPv6- oder DNS-Adresse des entfernten Gateways oder Clients. Ist die IP-Adresse der remote Seite unbekannt oder dynamisch, so kann der Eintrag leer gelassen werden. In diesem Fall muss die Verbindung von der entfernten Seite aufgebaut werden. Wird eine explizite IP-Adresse konfiguriert, so muss diese beim Verbindungsaufbau exakt übereinstimmen.

Erlaubte Werte: IPv4-Adresse, IPv6-Adresse, 0.0.0.0, :: oder leerer Eintrag. Die Werte 0.0.0.0 bzw. :: für IPv6 haben die gleiche Funktion wie ein leerer Eintrag.

SNMP-ID:

2.19.70.3.4

Pfad Konsole:

Setup > **VPN** > **WireGuard** > **Peers**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9].-:%?`

Default-Wert:

leer

Entfernter-Port

Port der Seite des entfernten Gateways. Ist der entfernte Port von eingehenden Verbindungen dynamisch oder unbekannt, so kann der Eintrag leer gelassen werden oder mit 0 konfiguriert werden. Wird ein expliziter Port konfiguriert, so muss dieser beim Verbindungsaufbau exakt übereinstimmen und wird im Fehlerfall verworfen bzw. abgelehnt.

Erlaubte Werte: Port, 0, leerer Eintrag

SNMP-ID:

2.19.70.3.5

Pfad Konsole:

Setup > **VPN** > **WireGuard** > **Peers**

Mögliche Werte:

max. 5 Zeichen aus `[0-9]`

Default-Wert:

51820

Rtg-Tag

Routing Tag, über das die WireGuard-Verbindung aufgebaut werden soll.

SNMP-ID:

2.19.70.3.6

Pfad Konsole:

Setup > **VPN** > **WireGuard** > **Peers**

Mögliche Werte:

0 … 65535

Default-Wert:

0

Lokaler-Privater-Schluessel

Lokaler Private-Key der WireGuard-Verbindung im Base64-Format. Einträge im Hex-Key-Format werden nicht unterstützt. Aus dem lokalen Private-Key berechnet das Gerät automatisch seinen Public-Key.

Pro lokalen Port muss der konfigurierte lokale Private-Key identisch sein. Mehrere konfigurierte Verbindungen auf dem gleichen lokalen Port und unterschiedlichen Private-Keys werden nicht unterstützt und führen dazu, dass Verbindungen nicht aufgebaut werden können bzw. die interne Konfiguration nicht erzeugt werden kann.

Der lokale Private Key ist geheim und wird in der Regel nicht mit der entfernen Seite geteilt. Es sei denn, ein Administrator erstellt Schlüsselpaare für seine verwalteten Geräte. In diesem Fall kennt der Administrator alle Schlüsselpaare seiner Geräte.

SNMP-ID:

2.19.70.3.7

Pfad Konsole:

Setup > **VPN** > **WireGuard** > **Peers**

Mögliche Werte:

max. 44 Zeichen aus `[A-Z][a-z][0-9]+/=`

Default-Wert:

leer

Privater-Peer-Schluessel

Der Peer Private Key ist optional und wird nur dann konfiguriert, wenn LANconfig für die Gegenseite eine Konfiguration bzw. QR-Code erzeugen soll. Er ist für die Funktion im LCOS nicht erforderlich und wird nur in der Konfiguration gespeichert, damit die Konfiguration für die Gegenseite ggf. zu einem späteren Zeitpunkt erneut angezeigt bzw. generiert werden kann.

SNMP-ID:

2.19.70.3.9

Pfad Konsole:

Setup > **VPN** > **WireGuard** > **Peers**

Mögliche Werte:

max. 44 Zeichen aus `[A-Z][a-z][0-9]+/=`

Default-Wert:

leer

Oeffentlicher-Peer-Schluessel

Public Key des entfernten bzw. Remote-Gateways im Base64-Format. Einträge im Hex-Key-Format werden nicht unterstützt.

Jeder Kommunikationspartner der WireGuard-Verbindung muss ein individuelles Schlüsselpaar aus Public-/Private-Key erzeugen und der entfernen Seite seinen Public-Key mitteilen.

SNMP-ID:

2.19.70.3.10

Pfad Konsole:

Setup > **VPN** > **WireGuard** > **Peers**

Mögliche Werte:

max. 44 Zeichen aus `[A-Z][a-z][0-9]+/=`

Default-Wert:

leer

Geteilter-Schluessel

Optionaler zusätzlicher Schlüssel, der bei der Verbindung neben dem Public-/Private-Schlüsselpaar verwendet werden soll. Der Schlüssel muss auf beiden Kommunikationspartnern identisch konfiguriert werden.

SNMP-ID:

2.19.70.3.11

Pfad Konsole:

Setup > **VPN** > **WireGuard** > **Peers**

Mögliche Werte:

max. 44 Zeichen aus `[A-Z][a-z][0-9]+/=`

Default-Wert:

leer

IPv6

Dieser Eintrag definiert das IPv6-WAN-Profil. Ein leerer Eintrag schaltet IPv6 für dieses Interface ab.

SNMP-ID:

2.19.70.3.13

Pfad Konsole:

Setup > **VPN** > **WireGuard** > **Peers**

Mögliche Werte:

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

Default-Wert:

leer

Kommentar

Geben Sie einen Kommentar zu diesem Eintrag an.

SNMP-ID:

2.19.70.3.14

Pfad Konsole:

Setup > **VPN** > **WireGuard** > **Peers**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default-Wert:

leer

Persistent-Keepalive

Definiert die Zeit in Sekunden, in der das entfernte Gerät (Peer) WireGuard Keepalive-Pakete senden soll. Der Wert 0 deaktiviert das Senden von Keepalive-Paketen.

Das „Persistent Keepalive" in WireGuard sorgt dafür, dass die Verbindung auch dann aktiv gehalten wird, wenn gerade kein Datenverkehr stattfindet. Durch das regelmäßige Senden von Keepalive-Paketen wird die Verbindung, z. B. in NAT-Gateways auf der Strecke, aktiv gehalten und verhindert so ungewollte Verbindungsabbrüche.

SNMP-ID:

2.19.70.3.15

Pfad Konsole:

Setup > **VPN** > **WireGuard** > **Peers**

Mögliche Werte:

max. 3 Zeichen aus `[0-9]`

Default-Wert:

0

Immer-Aktiv

Definiert, ob der WireGuard-Tunnel automatisch – z. B. nach dem Gerätestart oder nach dem Aufbau der WAN-Verbindung – aufgebaut werden soll, oder nur dann, wenn tatsächlich Nutzdaten übertragen werden. Dieser Schalter muss zusammen mit dem Schalter „Persistent-Keepalive" konfiguriert werden, damit sich die WireGuard-Gegenstelle wie andere Gegenstellen verhält, die dauerhaft aktiv gehalten werden sollen.

SNMP-ID:

2.19.70.3.16

Pfad Konsole:

Setup > **VPN** > **WireGuard** > **Peers**

Mögliche Werte:

nein

Die WireGuard-Verbindung wird ausschließlich bei vorhandenem Nutzdatenverkehr aufgebaut.

ja

Die WireGuard-Verbindung wird dauerhaft aufgebaut – unabhängig davon, ob Nutzdaten übertragen werden.

Default-Wert:

ja

6 Voice over IP – VoIP

6.1 Konfiguration der Leitungen: SIP-Leitungen

Ab LCOS 10.94 kann in der SIP-Leitungstabelle (**Voice-Call-Manager** > **Leitungen** > **SIP-Leitungen**) im Feld **Account-Number** eine Rufnummer eingetragen werden, die zu diesem SIP-Anschluss gehört.

6.1.1 Ergänzungen im Setup-Menü

6.1.1.1 Account-Number

Tragen Sie hier eine Rufnummer ein, die zu diesem SIP-Anschluss gehört.

Bei SIP-Leitungen des Typs „Flex" wird diese Quellrufnummer dann, zur Account-Verifizierung, im PPI übertragen.

Wird die FROM Rufnummer durch das Callrouting verändert oder sendet das SIP-Telefon eine Rufnummer, die nicht zum Anschluss passt, führt dies dann nicht zur Ablehnung des Rufes durch den Provider.

So können CLIP no screening Anrufe über den VCM direkt durchgeführt werden, sofern das Leistungsmerkmal beim SIP-Provider verfügbar ist.

SNMP-ID:

2.33.4.1.1.43

Pfad Konsole:

Setup > **Voice-Call-Manager** > **Line** > **SIP-Provider** > **Line**

Mögliche Werte:

max. 32 Zeichen aus `[A-Z][a-z][0-9]#@\{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default-Wert:

leer

6.2 Priorisierte Rufnummern

Ab LCOS 10.94 können Notfallrufnummern hinterlegt werden.

6.2.1 Ergänzungen im Setup-Menü

6.2.1.1 Preferred-Numbers

Tragen Sie in dieser Tabelle Notfallrufnummern ein. Kann ein Ruf zu einer Notfallrufnummer aufgrund einer Fehlermeldung vom SIP-Provider nicht aufgebaut werden, wird ein bereits aufgebauter Ruf, der über diese Leitung (Leitungstyp Trunk/Flex) bzw. dem Leitungsverbund (Leitungstyp Einzel-Account/Provider) geführt wird, abgebaut. So wird sichergestellt, dass ein Sprachkanal für diese Notruf zur Verfügung steht.

Ein Leitungsverbund wird hierbei über die Tabelle „Dynamische SIP-Leitungen" definiert. Dabei gehören SIP-Leitungen mit demselben „Dynamic-Line-Name" zu einem Verbund. Hierbei handelt es sich meist um mehrere Einzelrufnummern, über die insgesamt eine bestimmte Anzahl an Sprachkanälen zur Verfügung stehen.

SNMP-ID:

2.33.12.1

Pfad Konsole:

Setup > **Voice-Call-Manager** > **Call-Handling**

6.2.1.1.1 Called-Number

Tragen Sie hier Ihre Rufnummer ein.

SNMP-ID:

2.33.12.1.1

Pfad Konsole:

Setup > **Voice-Call-Manager** > **Call-Handling** > **Preferred-Numbers**

Mögliche Werte:

max. 19 Zeichen aus `[A-Z][0-9]#@{|}~!$%&'()+-,/:;<=>?[]^_.`

Default-Wert:

leer

6.2.1.1.2 Type

Tragen Sie hier den Rufnummerntyp ein.

SNMP-ID:

2.33.12.1.2

Pfad Konsole:

Setup > **Voice-Call-Manager** > **Call-Handling** > **Preferred-Numbers**

Mögliche Werte:

Emergency

Dies ist eine Notfallrufnummer.

Private

Diese Rufnummern unterbinden die Overlap-Dialing-Wartezeit für dieses Ziel.

6.2.1.1.3 Kommentar

Hier tragen Sie einen Kommentar zu der ausgewählten Rufnummer ein.

SNMP-ID:

2.33.12.1.4

Pfad Konsole:

Setup > **Voice-Call-Manager** > **Call-Handling** > **Preferred-Numbers**

Mögliche Werte:

max. 63 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[]^_. `

Default-Wert:

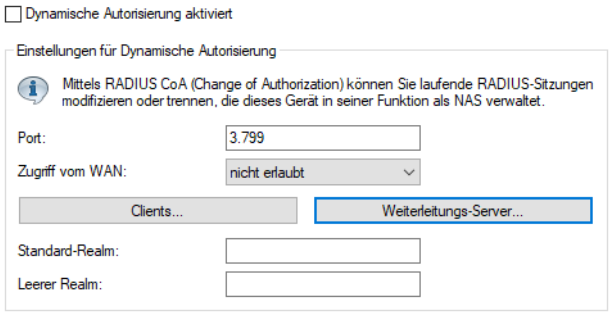
leer

7 RADIUS

7.1 RADIUS CoA für 802.1X Authenticator Ethernet Ports

Der 802.1X Authenticator für Ethernet Ports unterstützt RADIUS Change of Authorizaion (CoA) und Disconnect Messages (DM) für 802.1X sowie bei der Authentifizierung basierend auf MAC-Adressen.

Es wird die gemeinsame Konfiguration der Dynamischen Autorisierung verwendet. Im LANconfig unter **RADIUS** > **Dyn. Autorisierung** und auf der CLI unter **Setup** > **RADIUS** > **Dyn-Auth.** Diese Konfiguration wird auch von Public Spot oder IKEv2 verwendet.



Die folgenden CoA-Funktionen werden unterstützt:

- Trennen der Sitzung eines aktuellen Benutzers (Disconnect Message)
- Veränderung der aktuellen Sitzung des Benutzers durch Änderung des VLANs per CoA-Nachricht

Beispiele:

1. Die aktuell aktiven Sitzungen können über das Status-Menü angezeigt werden:

```
root@test-8021x-dm:/
> ls /Status/LAN/IEEE802.1x/Authenticator-Ifc-Status/
Ifc   Operating Mode        State         MAC-Auth.-Bypass MAC-Address  VLAN-ID Auth-Count Conflicting-MAC
===============-----------------------------------------------------------------------------------------
ETH-2 Yes       Single-Host authenticated No               e89c255b7b86 0       1          000000000000


Conflict-Age
-----------------
0
```

2. Der Status für CoA kann über das Show-Kommando „show ethernet-dynauth“ angezeigt werden:

```
> show ethernet-dynauth
MAC address e8:9c:25:5b:7b:86 on ETH-2: NAS-Identifier 'test-8021x-dm', User-Name 'test'
```

3. Ein Trennen der Sitzung eines 802.1X-Benutzers kann mit dem CLI-Befehl „Radclient“ unter **Setup** > **RADIUS** > **Dyn-Auth.** im LCOS durchgeführt werden, z. B.:

```
do Radclient 192.168.1.112 disconnect 12345678 "NAS-Identifier=test-8021x-dm;User-Name=test;"
```

   Dabei ist:

   - „192.168.1.112“ die IP-Adresse des NAS, d. h. des Routers
   - „disconnect“ die Disconnect-Nachricht, die versendet werden soll
   - „12345678“ das konfigurierte Dyn-Auth/CoA-Passwort
   - „NAS-Identifier“ der Name des Routers bzw. die eindeutige Identifizierung des NAS
   - „User-Name“ der 802.1X Benutzername der in der Authentifizierung vom Client verwendet wurde

Die Verwendung aller dieser Parameter ist erforderlich.

4. Die Änderung des VLANs einer aktuellen Sitzung für einen MAC-authentifizierten Benutzer kann wie folgt durchgeführt werden:

```
do Radclient 192.168.1.112 coa 12345678 "NAS-Identifier=test-8021x-dm;User-Name=e89c255b7b86;
   Tunnel-Type:0=VLAN;Tunnel-Medium-Type:0=IEEE-802;Tunnel-Private-Group-Id:0=200;
```

Dabei ist:

- „192.168.1.112“ die IP-Adresse des NAS, d. h. des Routers
- „coa“ die CoA-Nacricht, die versendet werden soll
- „12345678“ das konfigurierte Dyn-Auth/CoA-Passwort
- „NAS-Identifier“ der Name des Routers bzw. die eindeutige Identifizierung des NAS
- „Tunnel-Type:0=VLAN;Tunnel-Medium-Type:0=IEEE-802;Tunnel-Private-Group-Id:0=200“ sind die erforderlichen RADIUS-Attribute um den Client hier in das VLAN 200 zu verschieben

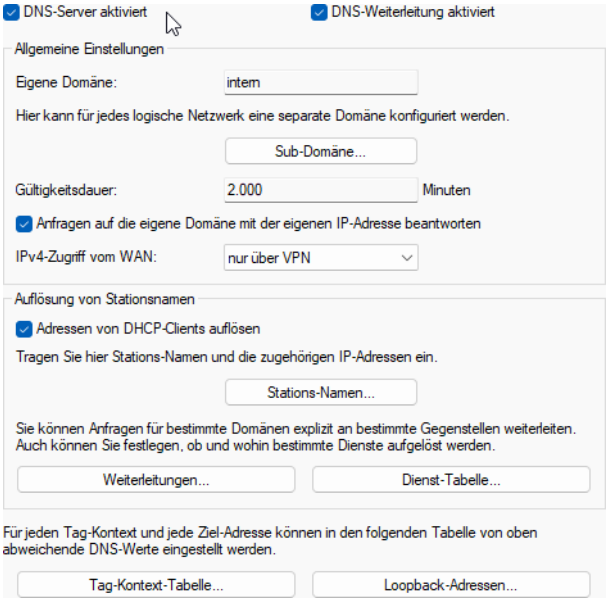
Die Verwendung aller dieser Parameter ist erforderlich.

Zur Analyse der CoA-Funktionalität stehen die Traces „DYN-AUTH-Client“ sowie „DYN-AUTH-Server“ zur Verfügung.

8 Weitere Dienste

8.1 IPv4-WAN-Zugriff im DNS

Ab LCOS 10.94 können Sie den IPv4-WAN-Zugriff im DNS unter **DNS** > **Allgemein** konfigurieren.



IPv4-Zugriff vom WAN

Definiert, ob der Zugriff von WAN-Schnittstellen auf den DNS-Server oder DNS-Forwarder über IPv4 grundsätzlich erlaubt ist. Der Zugriff auf diese Dienste über IPv6 wird ausschließlich über die IPv6-Inbound-Firewall gesteuert.

Der Zugriff kann über diesen Schalter global für die entsprechenden Schnittstellentypen gesteuert werden. Soll der Zugriff granularer als auf dieser Ebene erfolgen, so können entsprechende IPv4-Firewall-Regeln konfiguriert werden.

Der Zugriff auf den DNS-Dienst muss über VPN erlaubt werden, wenn VPN-Clients den Router als DNS-Server oder DNS-Forwarder nutzen sollen, z. B. zur Auflösung von lokal konfigurierten Stationsnamen.

Der Zugriff auf den DNS-Dienst über WAN muss erlaubt werden, wenn Clients sich auf den Router per PPPoE, L2TP oder PPTP einwählen sollen. Eine granulare Steuerung auf den lokalen DNS-Dienst per Firewall-Regeln wird in diesem Fall empfohlen.

Als VPN-Schnittstellen gelten IPSec-VPN (IKEv1/IKEv2) sowie WireGuard. Als WAN-Schnittstellen gelten alle WAN-Gegenstellen wie Internetverbindungen sowie RAS-Einwahlen auf den LANCOM Router in der Rolle als PPPoE-, PPTP oder L2TP-Server.

8.1.1 Ergänzungen im Setup-Menü

8.1.1.1 IPv4-WAN-Zugriff

Definiert, ob der Zugriff von WAN-Schnittstellen auf den DNS-Server oder DNS-Forwarder über IPv4 grundsätzlich erlaubt ist. Der Zugriff auf diese Dienste über IPv6 wird ausschließlich über die IPv6-Inbound-Firewall gesteuert.

Der Zugriff kann über diesen Schalter global für die entsprechenden Schnittstellentypen gesteuert werden. Soll der Zugriff granularer als auf dieser Ebene erfolgen, so können entsprechende IPv4-Firewall-Regeln konfiguriert werden.

Der Zugriff auf den DNS-Dienst muss über VPN erlaubt werden, wenn VPN-Clients den Router als DNS-Server oder DNS-Forwarder nutzen sollen, z. B. zur Auflösung von lokal konfigurierten Stationsnamen.

Der Zugriff auf den DNS-Dienst über WAN muss erlaubt werden, wenn Clients sich auf den Router per PPPoE, L2TP oder PPTP einwählen sollen. Eine granulare Steuerung auf den lokalen DNS-Dienst per Firewall-Regeln wird in diesem Fall empfohlen.

Als VPN-Schnittstellen gelten IPSec-VPN (IKEv1/IKEv2) sowie WireGuard. Als WAN-Schnittstellen gelten alle WAN-Gegenstellen wie Internetverbindungen sowie RAS-Einwahlen auf den LANCOM Router in der Rolle als PPPoE-, PPTP oder L2TP-Server.

SNMP-ID:

2.17.18

Pfad Konsole:

Setup > **DNS**

Mögliche Werte:

Nein

Der Zugriff auf den DNS-Server und DNS-Forwarder über IPv4 von WAN- sowie VPN-Schnittstellen ist nicht erlaubt.

Ja

Der Zugriff auf den DNS-Server und DNS-Forwarder ist von allen Schnittstellen wie LAN, WAN und VPN über IPv4 grundsätzlich erlaubt.

VPN

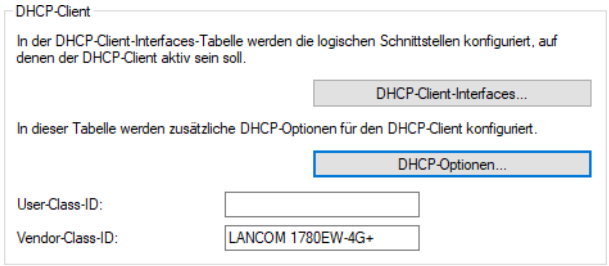
Der Zugriff auf den DNS-Server und DNS-Forwarder ist von LAN-Schnittstellen sowie über VPN (IPSec-VPN sowie WireGuard) über IPv4 erlaubt. Nicht erlaubt ist der Zugriff von WAN-Schnittstellen wie Internetverbindungen sowie RAS-Einwahlen auf den LANCOM Router in der Rolle als PPPoE-, PPTP oder L2TP-Server.

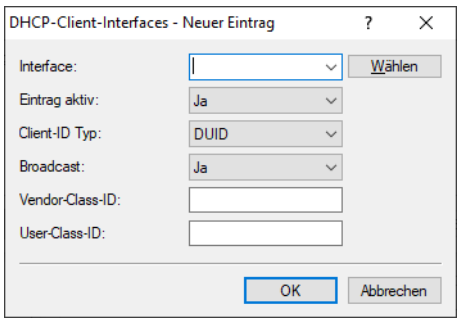
Default-Wert:

VPN

8.2 Neue DHCPv4-Client-Konfiguration

Ab LCOS 10.94 können Sie Client-Interfaces des DHCP-Clients für IPv4 unter **IPv4** > **DHCPv4** > **DHCP-Client** > **DHCP-Client-Interfaces** konfigurieren.





Interface

Name des Interfaces, auf dem der Client aktiv ist (LAN-, physikalisches WAN-, oder WWAN-Interface). Es existieren je nach Gerät nach einem System-Reset Default-Einträge für Zero-Config: „INTERNET-DHCPDEF", „INTERNET-DEFAULT" oder „WWAN-DEFAULT".

Eintrag aktiv

Schalter, ob dieser Eintrag aktiv ist.

Client-ID Typ

Schalter, der den Typ der Client-ID angibt.

Broadcast

Schalter, der den Typ der Client-ID angibt.

Vendor-Class-ID

String, der den Vendor-Class-Identifier enthält, der auf dme Interface gemeldet werden soll. Wenn dieser Wert leer ist, dann wird der (globale) Wert unter **IPv4** > **DHCPv4** > **DHCP-Client** > **Vendor-Class-ID** verwendet.

User-Class-ID

String, der den User-Class-Identifier enthält, der auf dme Interface gemeldet werden soll. Wenn dieser Wert leer ist, dann wird der (globale) Wert unter **IPv4** > **DHCPv4** > **DHCP-Client** > **User-Class-ID** verwendet.

Weitere Änderungen

- Unter **setup** > **dhcp** > **client** (SNMP-ID 2.10.40) sind die Menüpunkte **LAN-Client-ID-Type** (SNMP-ID 31) und **WAN-Client-ID-Type** (SNMP-ID 32) entfallen, da die Werte nun pro Client eingestellt werden können
- Unter **setup** > **dhcp** > **network-list** (SNMP-ID 2.10.20) wurde für den **Aktiv** Schalter die Option „Client" entfernt

- Unter **setup** > **wan** > **layer** (SNMP-ID 2.2.4) wurde für die Spalte **Layer-3** (SNMP-ID 3) die Werte „DHCP“ und „B-DHCP“ entfernt.
- Es gibt einen Konfig-Konverter, der folgendes macht:
  - für alle WAN-Verbindungen, die einen Layer mit DHCP oder B-DHCP verwenden, wird ein Eintrag in der Tabelle **setup** > **dhcp** > **client** > **Interfaces** angelegt. Das gilt für DSL, xDSL und WWAN-Verbindungen.
  - für alle LAN-Interfaces, auf denen der Operating-Schalter auf „Client“ steht, wird ein Eintrag in der Tabelle **setup** > **dhcp** > **client** > **Interfaces** angelegt. Zudem wird der Eintrag aus **setup** > **dhcp** > **network-list** entfernt.

8.2.1 Ergänzungen im Setup-Menü

8.2.1.1 Interfaces

Konfigurieren Sie in dieser Tabelle Client-Interfaces des DHCP-Clients für IPv4.

SNMP-ID:

2.10.40.1

Pfad Konsole:

Setup > **DHCP** > **Client**

8.2.1.1.1 Interface

Name des Interfaces, auf dem der Client aktiv ist (LAN-, physikalisches WAN-, oder WWAN-Interface). Es existieren je nach Gerät nach einem System-Reset Default-Einträge für Zero-Config: „INTERNET-DHCPDEF“, „INTERNET-DEFAULT“ oder „WWAN-DEFAULT”.

SNMP-ID:

2.10.40.1.1

Pfad Konsole:

Setup > **DHCP** > **Client** > **Interfaces**

Mögliche Werte:

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

Default-Wert:

leer

8.2.1.1.2 Aktiv

Schalter, ob dieser Eintrag aktiv ist.

SNMP-ID:

2.10.40.1.2

Pfad Konsole:

Setup > **DHCP** > **Client** > **Interfaces**

Mögliche Werte:

Nein
Ja

Default-Wert:

Ja

8.2.1.1.3 Client-ID-Typ

Schalter, der den Typ der Client-ID angibt.

SNMP-ID:

2.10.40.1.3

Pfad Konsole:

Setup > **DHCP** > **Client** > **Interfaces**

Mögliche Werte:

MAC
DUID

Default-Wert:

DUID

8.2.1.1.4 Broadcast

Schalter, der angibt, ob der Client das „Broadcast"-Flag setzt. Auf einem LAN-Interface wird dieser Wert immer auf „Ja" gestellt.

SNMP-ID:

2.10.40.1.4

Pfad Konsole:

Setup > **DHCP** > **Client** > **Interfaces**

Mögliche Werte:

Nein
Ja

Default-Wert:

Ja

8.2.1.1.5 Vendor-Class-Identifer

String, der den Vendor-Class-Identifier enthält, der auf dme Interface gemeldet werden soll. Wenn dieser Wert leer ist, dann wird der (globale) Wert unter *2.10.40.3 Vendor-Class-Identifier* verwendet.

SNMP-ID:

2.10.40.1.5

Pfad Konsole:

Setup > **DHCP** > **Client** > **Interfaces**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default-Wert:

leer

8.2.1.1.6 User-Class-Identifer

String, der den User-Class-Identifier enthält, der auf dme Interface gemeldet werden soll. Wenn dieser Wert leer ist, dann wird der (globale) Wert unter *2.10.40.2 User-Class-Identifier* verwendet.

SNMP-ID:

2.10.40.1.6

Pfad Konsole:

Setup > **DHCP** > **Client** > **Interfaces**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default-Wert:

leer

9 Ergänzungen im Menüsystem

9.1 Ergänzungen im Setup-Menü

9.1.1 Parameter-Format

Ab LCOS-Version 10.94 wird der neue Parameter lineid unterstützt.

Format des in der PAP-ACK-Nachricht enthaltenen Parameter-Strings für diesen Provider. Mögliche Platzhalter sind:

- {txrate} – Upstream-Rate
- {rxrate} – Downstream-Rate
- {lineid} – Line-ID der Verbindung. Diese wird nur zur Information bzw. zur Identifizierung des Anschlusses angezeigt

Beispiel: Der Provider schickt in seiner PAP-ACK-Nachricht den String „SRU=39983#SRD=249973#". Der zugehörige Parameter-String ist dann „SRU={txrate}#SRD={rxrate}#".

SNMP-ID:

2.2.62.2

Pfad Konsole:

Setup > **WAN** > **Provider-Spezifika**

Mögliche Werte:

max. 250 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default-Wert:

leer

9.1.2 Schluesselaustausch-Algorithmen

Ab LCOS-Version 10.94 wird mlkem768x25519-sha256 bei SSH unterstützt.

Die MAC-Schluesselaustausch-Algorithmen dienen der Aushandlung des Schlüssel-Algorithmus. Wählen Sie aus den verfügbaren Algorithmen einen oder mehrere aus.

SNMP-ID:

2.11.28.3

Pfad Konsole:

Setup > **Config** > **SSH**

Mögliche Werte:

diffie-hellman-group1-sha1
diffie-hellman-group14-sha1
diffie-hellman-group-exchange-sha1
diffie-hellman-group-exchange-sha256
ecdh-sha2
curve25519-sha256
curve448-sha512
sntrup761x25519-sha512
diffie-hellman-group14-sha256
diffie-hellman-group15-sha512
diffie-hellman-group16-sha512
diffie-hellman-group17-sha512
diffie-hellman-group18-sha512
sntrup4591761x25519-sha512
mlkem768x25519-sha256

Hybrid-Post-Quantum-Algorithmus mlkem768x25519. Hierbei wird der Post-Quantum-Algorithmus ML-KEM (Module-Lattice-Based Key-Encapsulation Mechanism) mit dem bekannten klassischen Verfahren Curve25519 kombiniert.

Default-Wert:

diffie-hellman-group-exchange-sha256

ecdh-sha2

curve25519-sha256

curve448-sha512

sntrup761x25519-sha512

diffie-hellman-group14-sha256

diffie-hellman-group15-sha512

diffie-hellman-group16-sha512

mlkem768x25519-sha256

9.1.3 Elliptische-Kurven

Ab LCOS-Version 10.94 wird bei TLS der Hybrid-Post-Quantum-Algorithmus X25519MLKEM768 unterstützt.

Legen Sie fest, welche elliptischen Kurven zur Verschlüsselung verwendet werden sollen.

SNMP-ID:

2.21.40.9

Pfad Konsole:

Setup > **HTTP** > **SSL**

Mögliche Werte:

secp256r1

secp256r1 wird zur Verschlüsselung verwendet.

secp384r1

secp384r1 wird zur Verschlüsselung verwendet.

secp521r1

secp521r1 wird zur Verschlüsselung verwendet.

x25519

x25519 wird zur Verschlüsselung verwendet.

x448

x448 wird zur Verschlüsselung verwendet.

X25519MLKEM768

X25519MLKEM768 wird zur Verschlüsselung verwendet. Der Algorithmus X25519MLKEM768 kombiniert den Post-Quantum-Algorithmus ML-KEM (Module-Lattice-Based Key-Encapsulation Mechanism) mit dem bekannten klassischen Verfahren Curve25519. Post-Quantum-Algorithmus-Keyagreement wird grundsätzlich nur für TLS 1.3 unterstützt. Für TLS 1.2 kann dieses neue Verfahren nicht genutzt werden, da dies dort im Standard durch die IETF nicht definiert ist.

Default-Wert:

secp256r1

secp384r1

secp521r1

x25519

x448

X25519MLKEM768

9.1.4 Passwort

Ab LCOS 10.94 wurde die zulässige Eingabelänge für das BGP-Passwort auf 254 Zeichen erweitert.

Gerät und BGP-Nachbar übertragen dieses Passwort als MD5-Signatur in den TCP-Paketen, um sich zu authentifizieren.

Ohne die Angabe eines Passwortes ist die Authentifizierung deaktiviert.

SNMP-ID:

2.93.1.2.8

Pfad Konsole:

Setup > **Routing-Protokolle** > **BGP** > **Nachbarn**

Mögliche Werte:

max. 254 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default-Wert:

leer

10 Entfallene Features

Ab LCOS 10.94 sind die folgenden Features entfallen:

- AutoWDS (2.37.1.15, 2.37.1.16, 2.59.4)
- LANCOM Battery Pack (2.97)
- Der Wert „Exclusive“ wurde bei **Setup** > **WAN** > **RADIUS** > **Aktiv** entfernt. Bestehende Konfigurationen wurden auf „ja“ geändert, RADIUS bleibt somit aktiv.