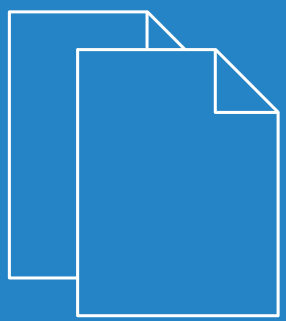
SICHER. **VERNETZT.**

LCOS 10.20

Addendum



01/2019

LANCOM Systems

Inhalt

1 Addendum zur LCOS-Version 10.20

Dieses Dokument beschreibt die Änderungen und Ergänzungen in der LCOS-Version 10.20 gegenüber der vorherigen Version.

2 Konfiguration

2.1 Software zur Konfiguration

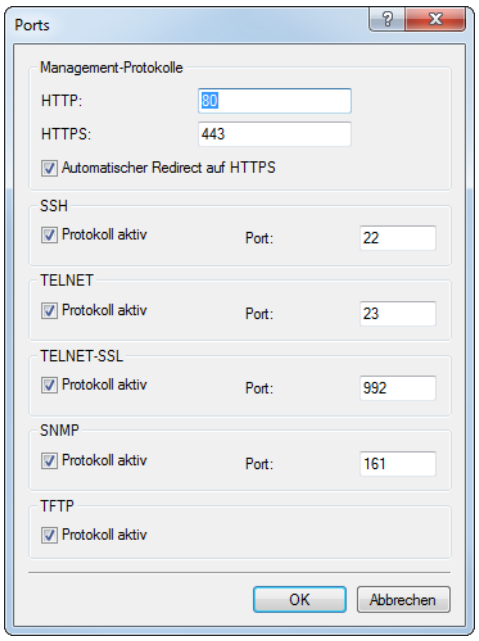
2.1.1 Automatische Umleitung des WEBconfig-Zugriffs auf HTTPS

Ab LCOS-Version 10.20 wechselt WEBconfig bei einer unverschlüsselten Verbindungsanfrage automatisch auf eine verschlüsselte HTTPS-Verbindung.

Dadurch wird die Sicherheit in den Fällen erhöht, bei denen man ein LANCOM Gerät über WEBconfig konfigurieren will, aber in die Adressleiste des Browsers nur die IP-Adresse oder den Namen eingibt. Der Browser würde daraufhin eine unverschlüsselte HTTP-Verbindung aufbauen.

Damit eine verschlüsselte HTTPS-Verbindung aufgebaut würde, musste man bei der Eingabe im Browser normalerweise immer explizit `https://` als Präfix angeben. Durch diese Änderung wird die Eingabe vereinfacht und gleichzeitig werden sensible Daten wie z. B. das Passwort beim Login oder die Konfiguration durch die verschlüsselte Verbindung geschützt.

Für Neukonfigurationen wird dieses Feature immer eingeschaltet. Bereits bestehende Konfigurationen werden nicht automatisch geändert. Bei diesen können Sie die Funktion unter **Management** > **Admin** > **Management-Protokolle** > **Ports** > **Automatischer Redirect auf HTTPS** einschalten.



Ergänzungen im Setup-Menü

Automatic-Redirect-to-HTTPS

Dieser Schalter legt fest, ob der WEBconfig-Login-Dialog bei einer unverschlüsselten Verbindungsanfrage automatisch auf eine verschlüsselte HTTPS-Verbindung umschaltet. Für Neukonfigurationen wird dies immer eingeschaltet. Bereits bestehende Konfigurationen werden nicht geändert.

SNMP-ID:

2.21.24

Pfad Telnet:

Setup > HTTP

Mögliche Werte:

Nein

WEBconfig schaltet bei einer unverschlüsselten Verbindungsanfrage nicht automatisch auf eine verschlüsselte Verbindung um.

Ja

WEBconfig schaltet bei einer unverschlüsselten Verbindungsanfrage automatisch auf eine verschlüsselte Verbindung um.

Default-Wert:

Ja

2.1.2 Befehle für die Konsole

Ab LCOS-Version 10.20 unterstützt Ihr Gerät die folgenden neuen Befehle bzw. Optionen.

Tabelle 1: Übersicht aller neu auf der Kommandozeile eingebbaren Befehle

Befehl	Beschreibung
`find <Begriff>`	Sucht nach dem <Begriff> und gibt alle Menüeinträge aus, die den Suchbegriff enthalten.
`lig [[-i <instance>] | [-m <server>]] [-id <num>] destination-eid [-retries <num>] [-rtg-tag <num>] [-source-eid <num>]`	LIG (Locator/ID Separation Protocol Internet Groper) ist ein in RFC 6835 spezifiziertes Kommandozeilentool um LISP Mappings bei einem Map-Resolver abzufragen. Mögliche Optionsschalter sind: › `-i <instance>`: Name der LISP-Instanz, die für die Zielabfrage verwendet wird › `-m <server>`: LISP Map-Server, der für die Zielabfrage verwendet wird › `-id <num>`: LISP-Instanz-ID [0-16777215], die für die Zielabfrage verwendet wird › `destination-eid`: Abgefragte Ziel-EID › `-retries <num>`: LISP-Wiederholungen zum Map-Server [0-10] › `-rtg-tag <num>`: Verwendetes Routing-Tag › `-source-eid <num>`: Verwendete Source-EID Bespiel: `lig -i LISP-INST 172.16.200.1`
`readscript [-n] [-d] [-i] [-c] [-m] [-h] [-s <password>] [-o]`	Erzeugt eine Textausgabe aller Befehle und Parameter, die für die Konfiguration des Gerätes im aktuellen Zustand benötigt werden. Neu ist der folgende Optionsschalter: › `-o`: Ersetzt die Passwörter durch ein "*", sodass diese nicht in der Textausgabe sichtbar sind. **Zugriffsrecht**: Supervisor-Read
`show admin-distance`	Zeigt die administrative (Routing-)Distanz aller internen Anwendungen bzw. Routing-Protokolle. **Zugriffsrecht**: Supervisor-Read, Local-Admin-Read

Befehl	Beschreibung
`show ip-addresses`	Zeigt alle IPv4- und IPv6-Adressen des Gerätes für LAN- und WAN-Schnittstellen mit erweiterten Status-Informationen an. **Zugriffsrecht**: Supervisor-Read, Local-Admin-Read
`show ipv4-addresses`	Zeigt alle IPv4-Adressen des Gerätes für LAN- und WAN-Schnittstellen mit erweiterten Status-Informationen an. **Zugriffsrecht**: Supervisor-Read, Local-Admin-Read
`show lisp instance`	Zeigt Statusinformationen über alle konfigurierten LISP-Instanzen an. **Zugriffsrecht**: Supervisor-Read, Local-Admin-Read
`show lisp instance [instance]`	Zeigt Statusinformationen über die LISP-Instanz mit dem Namen [instance] an. **Zugriffsrecht**: Supervisor-Read, Local-Admin-Read
`show lisp map-cache`	Zeigt Statusinformationen über die vorhandenen Map-Cache-Einträge aller Instanzen an. **Zugriffsrecht**: Supervisor-Read, Local-Admin-Read
`show lisp map-cache [instance]`	Zeigt Statusinformationen über die vorhandenen Map-Cache-Einträge der Instanz mit dem Namen [instance] an. **Zugriffsrecht**: Supervisor-Read, Local-Admin-Read
`show lisp registrations`	Zeigt Statusinformationen über die beim Map-Server registrierten EIDs / RLOCs aller Instanzen an. **Zugriffsrecht**: Supervisor-Read, Local-Admin-Read
`show lisp registrations [instance]`	Zeigt Statusinformationen über die beim Map-Server registrierten EIDs / RLOCs der Instanz mit dem Namen [instance] an. **Zugriffsrecht**: Supervisor-Read, Local-Admin-Read
`show VLAN`	Das VLAN-Modul kann von anderen LCOS-Modulen zur Laufzeit instruiert werden, weitere VLANs und VLAN-Mitgliedschaften zur statischen Konfiguration hinzuzufügen. Das wird z. B. vom CAPWAP oder vom WLAN/802.1X genutzt. Über die neue Option `VLAN` zeigt der Befehl `show` diese nun an. **Zugriffsrecht**: Supervisor-Read, Local-Admin-Read
`ssldefaults [-j]`	Dieses Kommando setzt nach einer Sicherheitsabfrage die SSL- / TLS-Einstellungen in allen Untermenüs der aktuellen Konfiguration auf die Standardwerte zurück. Im LCOS bringt jedes Modul sein eigenes Untermenü für SSL- / TLS-Einstellungen mit. Hiermit gibt es eine Methode, alle Einstellungen in diesen verteilten Untermenüs auf die aktuellen sicheren Voreinstellungen zurückzusetzen. Mit dem Parameter `-j` wird die Sicherheitsabfrage automatisch beantwortet, sodass das Kommando aus Skripten heraus non-interaktiv aufgerufen werden kann.

2.2 LANCOM Auto Updater

Der LANCOM Auto Updater ermöglicht die automatische Aktualisierung von im Feld befindlichen LANCOM Geräten ohne weiteren Benutzereingriff. LANCOM Geräte können auf Wunsch ohne Nutzerinteraktion nach neuen Software-Updates suchen, diese herunterladen und einspielen. Sie wählen, ob Sie Security Updates, Release Updates oder alle Updates automatisch installieren möchten. Sollen keine automatischen Updates durchgeführt werden, so kann das Feature auch zur Prüfung auf neue Updates verwendet werden.

Der LANCOM Auto Updater kontaktiert zur Update-Prüfung und zum Firmware-Download den LANCOM Update-Server. Die Kontaktaufnahme erfolgt via HTTPS. Bei der Kontaktaufnahme wird der Server mittels der im LANCOM Gerät bereits

hinterlegten TLS-Zertifikate validiert. Zusätzlich sind Firmware-Dateien für aktuelle LANCOM Geräte signiert. Der LANCOM Auto Updater validiert vor dem Einspielen einer Firmware diese Signatur.

2.2.1 Konfiguration des Auto Updaters

Die Konfiguration des LANCOM Auto Updaters finden Sie in LANconfig unter **Management** > **Software-Update**.

Update-Modus

Stellen Sie hier den Betriebsmodus ein. Die folgenden Modi werden unterstützt:

Prüfen & Aktualisieren

- Der Auto Updater prüft regelmäßig beim Update-Server auf neue Updates.
- Der Update-Server ermittelt anhand der **Update-Strategie** das passende Update, bestimmt den Zeitpunkt für Download und Installation des Update innerhalb des vom Benutzer konfigurierten Zeitfensters und übermittelt dies an den Auto Updater.
- Die Installation der Firmware erfolgt im Testmodus. Nach der Installation führt der Auto Updater eine Verbindungsprüfung durch. Hierbei wird geprüft, ob weiterhin eine Verbindung zum Update-Server aufgebaut werden kann, der Internetzugang also weiterhin gewährleistet ist. Dies wird mehrere Minuten lang versucht, um eine eventuelle VDSL-Synchronisation oder einen WWAN-Verbindungsaufbau abzuwarten. Konnte der Update-Server erfolgreich kontaktiert werden, wird der Testmodus beendet, die Firmware ist nun regulär aktiv. Konnte der Updateserver nicht kontaktiert werden, muss davon ausgegangen werden, dass der Internetzugang nicht mehr möglich ist und es wird wieder die zweite (und damit die vorher aktive) Firmware gestartet.

nur Prüfen

- Der Auto Updater prüft regelmäßig beim Update-Server auf neue Updates.
- Die Verfügbarkeit eines neuen Updates wird dem Benutzer im LCOS-Menübaum und via Syslog signalisiert.
- Der Benutzer hat die Gelegenheit, manuell – aber über den Auto Updater gesteuert – auf das neueste verfügbare Update zu aktualisieren.

Ein manuelles Update wird über den folgenden Befehl auf der Kommandozeile gestartet:

```
do /setup/Automatisches-Firmware-Update/Aktualisiere-Firmware-jetzt
```

Manuell

- Der Auto Updater prüft nur nach Aufforderung durch den Benutzer auf neue Updates.
- Der Benutzer hat die Gelegenheit, manuell – aber über den Auto Updater gesteuert – auf das neueste verfügbare Update zu aktualisieren.

Ein manuelles Update wird über den folgenden Befehl auf der Kommandozeile gestartet:

```
do /setup/Automatisches-Firmware-Update/Aktualisiere-Firmware-jetzt
```

Prüf-Intervall

Stellen Sie ein, ob die Überprüfung auf ein verfügbares Update täglich oder wöchentlich stattfinden soll.

Update-Strategie

neueste Version

Releaseübergreifend immer die neueste Version. Beispiel: 10.20 Rel ist installiert; es wird auf 10.20 RU1 aktualisiert, aber auch auf 10.30 Rel. Es wird also immer auf die neueste Version aktualisiert, aber nicht wieder auf ein vorheriges Release zurückgewechselt.

aktuelle Version

Innerhalb eines Releases die neueste RU/SU/PR. Beispiel: 10.20 Rel ist installiert; es wird auf 10.20 RU1 aktualisiert, aber nicht auf 10.30 Rel.

nur Sicherheitsupdates

Innerhalb eines Releases das neueste SU. Beispiel: 10.20 Rel ist installiert; es wird auf 10.20 SU1 aktualisiert, aber nicht auf 10.20 RU2.

neueste Version ohne Rel.

Releaseübergreifend das neueste RU/SU/PR. Es wird erst bei Verfügbarkeit eines RU aktualisiert. Beispiel: Eine beliebige 10.20 ist installiert; es wird auf 10.30 RU1 aktualisiert, aber nicht auf 10.30 Rel.

Zeitfenster für Prüfung

Stellen Sie hier das Zeitfenster für die Prüfung und den Download neuer Aktualisierungen ein. Die tägliche Start- und Endzeit für dieses Zeitfenster kann stundengenau eingestellt werden. Die Standardeinstellung für beide Werte ist 0, es kann also rund um die Uhr auf Updates geprüft und ein Download gestartet werden. Innerhalb des konfigurierten Zeitfensters wird vom Auto Updater ein zufälliger Zeitpunkt für die Update-Prüfung und den Download geplant.

Zeitfenster für Installation

Stellen Sie hier das Zeitfenster für die Update-Installation ein. Die tägliche Start- und Endzeit für dieses Zeitfenster kann stundengenau eingestellt werden. Die Standardeinstellung definiert ein Zeitfenster zwischen 2:00 Uhr und 4:00 Uhr. Wenn ein Update gefunden wurde, dann wird dieses also in diesem Zeitraum installiert und das Gerät neu gestartet, um das Update zu aktivieren. Innerhalb des konfigurierten Zeitfensters wird vom Auto Updater ein zufälliger Zeitpunkt für die Installation geplant.

E-Mail-Benachrichtigungen senden

Stellen Sie hier ein, ob der LANCOM Auto Updater E-Mail-Benachrichtigungen an die angegebene E-Mail-Adresse versendet. Mittels der E-Mail-Benachrichtigungen kann sich der Administrator zu Ereignissen rund um das automatische Firmware-Update mit dem Auto-Updater informieren lassen. Eine E-Mail wird zu folgenden Ereignissen gesendet:

- ein Update wurde gefunden (bei Update-Modus "nur Prüfen")
- ein Update wurde gefunden und ein Zeitpunkt zur automatischen Installation wurde geplant (bei Update-Modus „Prüfen & Aktualisieren“)
- ein Update wurde erfolgreich installiert (inklusive erfolgreicher Erreichbarkeitsprüfung)

- ein Update konnte nicht erfolgreich installiert werden und es wurde ein Rückfall auf die zuvor installierte Firmware durchgeführt
- Fehlermeldungen des Auto-Updaters (z. B. Update-Server konnte nicht erreicht werden)

Eine Benachrichtigung erfolgt nur bei automatisch ausgeführten Aktionen. Werden Aktionen von Hand gestartet, z. B. eine Update-Prüfung via LANmonitor oder WEBconfig, dann erfolgt keine E-Mail-Benachrichtigung.

E-Mail-Adresse

Stellen Sie hier die E-Mail-Adresse ein, die verwendet werden soll, wenn die E-Mail-Benachrichtigungen aktiviert werden.

Basis-URL

Gibt die URL des Servers an, der die aktuellen Firmware-Versionen zur Verfügung stellt.

Absende-Adresse

Über die Angabe einer Loopback-Adresse kann das Routing Tag automatisch bestimmt werden.

2.2.2 Ergänzungen im Setup-Menü

Automatisches-Firmware-Update

Der LANCOM Auto Updater ermöglicht die automatische Aktualisierung von im Feld befindlichen LANCOM Geräten ohne weiteren Benutzereingriff (unattended). LANCOM Geräte können auf Wunsch ohne Nutzerinteraktion nach neuen Software-Updates suchen, diese herunterladen und einspielen. Sie wählen, ob Sie Security Updates, Release Updates oder alle Updates automatisch installieren möchten. Sollen keine automatischen Updates durchgeführt werden, so kann das Feature auch zur Prüfung auf neue Updates verwendet werden.

Der LANCOM Auto Updater kontaktiert zur Update-Prüfung und zum Firmware-Download den LANCOM Update-Server. Die Kontaktaufnahme erfolgt via HTTPS. Bei der Kontaktaufnahme wird der Server mittels der im LANCOM Gerät bereits hinterlegten TLS-Zertifikate validiert. Zusätzlich sind Firmware-Dateien für aktuelle LANCOM Geräte signiert. Der LANCOM Auto Updater validiert vor dem Einspielen einer Firmware diese Signatur.

SNMP-ID:

2.107

Pfad Telnet:

Setup

Modus

Stellen Sie hier den Betriebsmodus des LANCOM Auto Updaters ein.

SNMP-ID:

2.107.1

Pfad Telnet:

Setup > **Automatisches-Firmware-Update**

Mögliche Werte:

manuell

Der Auto Updater prüft nur nach Aufforderung durch den Benutzer auf neue Updates.

Der Benutzer hat die Gelegenheit, manuell – aber über den Auto Updater gesteuert – auf das neueste verfügbare Update zu aktualisieren.

pruefen

Der Auto Updater prüft regelmäßig beim LANCOM Update-Server auf neue Updates. Die Verfügbarkeit eines neuen Updates wird dem Benutzer im LCOS-Menübaum und via Syslog signalisiert. Der Benutzer hat die Gelegenheit, manuell – aber über den Auto Updater gesteuert – auf das neueste verfügbare Update zu aktualisieren.

pruefen-und-updaten

Der Auto Updater prüft regelmäßig beim LANCOM Update-Server auf neue Updates. Der Update-Server ermittelt anhand der Versions-Policy das passende Update, bestimmt den Zeitpunkt für Download und Installation des Update innerhalb des vom Benutzer konfigurierten Zeitfensters und übermittelt dies an den Auto Updater. Die Installation der Firmware erfolgt im Testmodus. Nach der Installation führt der Auto Updater eine Verbindungsprüfung durch. Hierbei wird geprüft, ob weiterhin eine Verbindung zum Update-Server aufgebaut werden kann, der Internetzugang also weiterhin gewährleistet ist. Dies wird mehrere Minuten lang versucht, um eine eventuelle VDSL-Synchronisation oder einen WWAN-Verbindungsaufbau abzuwarten. Konnte der Update-Server erfolgreich kontaktiert werden, wird der Testmodus beendet, die Firmware ist nun regulär aktiv. Konnte der Updateserver nicht kontaktiert werden, muss davon ausgegangen werden, dass der Internetzugang nicht mehr möglich ist und es wird wieder die zweite (und damit die vorher aktive) Firmware gestartet.

Default-Wert:

pruefen-und-updaten

Pruefe-Firmware-jetzt

Dieser Befehl veranlasst das Gerät, zu prüfen, ob auf dem LANCOM Update-Server eine neuere Firmware vorhanden ist.

SNMP-ID:

2.107.2

Pfad Telnet:

Setup > **Automatisches-Firmware-Update**

Aktualisiere-Firmware-jetzt

Dieser Befehl veranlasst das Gerät, die neueste Firmware vom LANCOM Update-Server herunterzuladen und zu installieren.

SNMP-ID:

2.107.3

Pfad Telnet:

Setup > **Automatisches-Firmware-Update**

Aktuelle-Aktion-abbrechen

Dieser Befehl veranlasst das Gerät, die aktuelle laufende Aktion des Auto Updaters abzubrechen. Dies bezieht sich sowohl auf manuell gestartete als auch auf geplant ausgeführte Aktionen.

SNMP-ID:

2.107.4

Pfad Telnet:

Setup > **Automatisches-Firmware-Update**

Updater-Konfiguration-Zuruecksetzen

Dieser Befehl setzt die auf den Auto Updater bezogenen bootpersistenten Konfigurationsdateien zurück. Dies schließt die lokale Blacklist ein, die Firmware-Versionen enthält, mit denen ein automatisches Update fehlgeschlagen ist.

SNMP-ID:

2.107.5

Pfad Telnet:

Setup > **Automatisches-Firmware-Update**

Basis-URL

Gibt die URL des Servers an, der die aktuellen Firmware-Versionen zur Verfügung stellt.

SNMP-ID:

2.107.6

Pfad Telnet:

Setup > **Automatisches-Firmware-Update**

Mögliche Werte:

max. 252 Zeichen aus `[A-Z][a-z][0-9]/?.-;:@&=$_+!*'(),%`

Default-Wert:

https://update.lancom-systems.de

Pruefintervall

Der Auto Updater bestimmmt beim ersten Start einen zufälligen Zeitraum innerhalb eines Tages oder einer Woche, an dem die Prüfung durchgeführt wird. Das eigentliche Update soll dann im nächsten Zeitraum zwischen 2-4 Uhr (Voreinstellung) durchgeführt werden.

SNMP-ID:

2.107.7

Pfad Telnet:

Setup > **Automatisches-Firmware-Update**

Mögliche Werte:

taeglich
woechentlich

Default-Wert:

taeglich

Versionsrichtlinie

Stellen Sie hier die Versionsrichtlinie des LANCOM Auto Updaters ein. Diese steuert, welche Firmware-Versionen einem Gerät zum Update angeboten werden.

SNMP-ID:

2.107.8

Pfad Telnet:

Setup > **Automatisches-Firmware-Update**

Mögliche Werte:

neueste
Releaseübergreifend immer die neueste Version. Beispiel: 10.20 Rel ist installiert; es wird auf 10.20 RU1 aktualisiert, aber auch auf 10.30 Rel. Es wird also immer auf die neueste Version aktualisiert, aber nicht wieder auf ein vorheriges Release zurückgewechselt.

aktuelle
Innerhalb eines Releases die neueste RU/SU/PR. Beispiel: 10.20 Rel ist installiert; es wird auf 10.20 RU1 aktualisiert, aber nicht auf 10.30 Rel.

nur-Sicherheitsupdates
Innerhalb eines Releases das neueste SU. Beispiel: 10.20 Rel ist installiert; es wird auf 10.20 SU1 aktualisiert, aber nicht auf 10.20 RU2.

neueste-ohne-REL
Releaseübergreifend das neueste RU/SU/PR. Es wird erst bei Verfügbarkeit eines RU aktualisiert. Beispiel: Eine beliebige 10.20 ist installiert; es wird auf 10.30 RU1 aktualisiert, aber nicht auf 10.30 Rel.

Default-Wert:

nur-Sicherheitsupdates

Loopback-Addr.

Über die Angabe einer Loopback-Adresse kann das Routing Tag automatisch bestimmt werden.

SNMP-ID:

2.107.9

Pfad Telnet:

Setup > **Automatisches-Firmware-Update**

Mögliche Werte:

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

Default-Wert:

leer

Pruefungszeit-Anfang

Anfang des Zeitintervalls als Stundenangabe, in dem die Überprüfung stattfindet, ob ein Firmware-Update vorhanden ist und dieses ggfs. heruntergeladen wird. Die Voreinstellung für Anfang und Ende ist jeweils 0, es kann also rund um die Uhr auf Updates geprüft und ein Download gestartet werden. Innerhalb des konfigurierten Zeitfensters wird vom Auto Updater ein zufälliger Zeitpunkt für die Update-Prüfung und den Download geplant.

SNMP-ID:

2.107.10

Pfad Telnet:

Setup > **Automatisches-Firmware-Update**

Mögliche Werte:

max. 2 Zeichen aus `[0-9]`

Default-Wert:

0

Pruefzeit-Ende

Ende des Zeitintervalls als Stundenangabe, in dem die Überprüfung stattfindet, ob ein Firmware-Update vorhanden ist und dieses ggfs. heruntergeladen wird. Die Voreinstellung für Anfang und Ende ist jeweils 0, es kann also rund um die Uhr auf Updates geprüft und ein Download gestartet werden. Innerhalb des konfigurierten Zeitfensters wird vom Auto Updater ein zufälliger Zeitpunkt für die Update-Prüfung und den Download geplant.

SNMP-ID:

2.107.11

Pfad Telnet:

Setup > **Automatisches-Firmware-Update**

Mögliche Werte:

max. 2 Zeichen aus `[0-9]`

Default-Wert:

0

Installationszeit-Anfang

Anfang des Zeitintervalls als Stundenangabe, in dem die Installation eines Firmware-Updates durchgeführt wird. Die Voreinstellung ist zwischen 2 und 4 Uhr morgens. Nach der Installation findet ein Neustart des Gerätes statt.

SNMP-ID:

2.107.12

Pfad Telnet:

Setup > **Automatisches-Firmware-Update**

Mögliche Werte:

max. 2 Zeichen aus `[0-9]`

Default-Wert:

2

Installationszeit-Ende

Ende des Zeitintervalls als Stundenangabe, in dem die Installation eines Firmware-Updates durchgeführt wird. Die Voreinstellung ist zwischen 2 und 4 Uhr morgens. Nach der Installation findet ein Neustart des Gerätes statt.

SNMP-ID:

2.107.13

Pfad Telnet:

Setup > **Automatisches-Firmware-Update**

Mögliche Werte:

max. 2 Zeichen aus `[0-9]`

Default-Wert:

4

E-Mail-Benachrichtigung

Stellen Sie hier ein, ob der LANCOM Auto Updater E-Mail-Benachrichtigungen an die in 2.107.15 angegebene E-Mail-Adresse versendet. Mittels der E-Mail-Benachrichtigungen kann sich der Administrator zu Ereignissen rund um das automatische Firmware-Update mit dem Auto-Updater informieren lassen. Eine E-Mail wird zu folgenden Ereignissen gesendet:

- ein Update wurde gefunden (bei Update-Modus "nur Prüfen")
- ein Update wurde gefunden und ein Zeitpunkt zur automatischen Installation wurde geplant (bei Update-Modus „Prüfen & Aktualisieren")
- ein Update wurde erfolgreich installiert (inklusive erfolgreicher Erreichbarkeitsprüfung)
- ein Update konnte nicht erfolgreich installiert werden und es wurde ein Rückfall auf die zuvor installierte Firmware durchgeführt
- Fehlermeldungen des Auto-Updaters (z. B. Update-Server konnte nicht erreicht werden)

Eine Benachrichtigung erfolgt nur bei automatisch ausgeführten Aktionen. Werden Aktionen von Hand gestartet, z. B. eine Update-Prüfung via LANmonitor oder WEBconfig, dann erfolgt keine E-Mail-Benachrichtigung.

SNMP-ID:

2.107.14

Pfad Telnet:

Setup > **Automatisches-Firmware-Update**

Mögliche Werte:

nein

Der Auto Updater versendet keine Benachrichtigungen.

ja

Der Auto Updater versendet Benachrichtigungen.

Default-Wert:

nein

E-Mail-Adresse

Stellen Sie hier die E-Mail-Adresse ein, die vom LANCOM Auto Updater verwendet werden soll, wenn die E-Mail-Benachrichtigungen unter 2.107.14 aktiviert werden.

SNMP-ID:

2.107.15

Pfad Telnet:

Setup > **Automatisches-Firmware-Update**

Mögliche Werte:

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

Default-Wert:

leer

2.3 Rechteverwaltung für verschiedene Administratoren

2.3.1 Verbesserter Schutz der Gerätekonfiguration gegen unerwünschte Änderungen

Ab LCOS-Version 10.20 ist der Zugriff auf die Tabelle **Konfiguration** > **Management** > **Admin** > **Weitere Administratoren** ausschließlich für den Root-Administrator möglich. Für in dieser Tabelle konfigurierte weitere Administratoren ist dies nicht mehr möglich, selbst wenn für diese unter 'Zugriffs-Rechte' „Alle“ konfiguriert ist.

Auf der CLI ist die Tabelle für weitere Administratoren mit dieser Änderung nicht mehr sichtbar. Auch das Auslesen mittels „readscript“ ist nicht mehr möglich. Wird durch einen weiteren Administrator in einem Skript versucht, auf die Tabelle zuzugreifen, werden die entsprechenden Skript-Zeilen nicht ausgeführt und mit einem „Script Error“ quittiert.

Die Cron-Tabelle verwendet den konfigurierten Benutzer, daher können die Befehle „loadconfig / loadscript“, sofern sie über die Cron-Tabelle ausgeführt werden, die Konfiguration nur komplett lesen, wenn dies mit dem Root-Administrator erfolgt.

In LANconfig wird die Tabelle weiterhin angezeigt, bei Zugriff durch einen weiteren Administator ist diese aber immer leer. Änderungen werden nicht zurückgeschrieben.

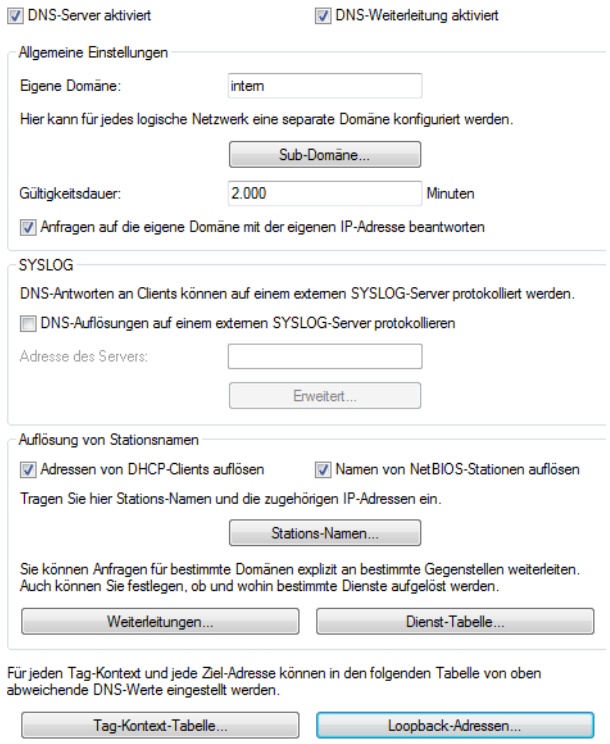
Der Zugriff via SNMP (lesen/schreiben) auf diese Tabelle ist im Rahmen dieses Features entfallen.

3 Routing und WAN-Verbindungen

3.1 Advanced Routing and Forwarding (ARF)

3.1.1 Routing-Tags für DNS-Weiterleitung

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

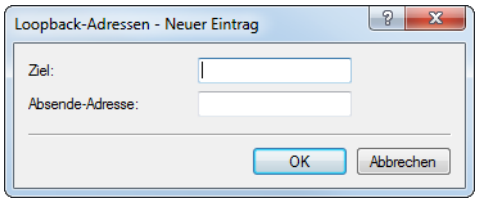


Ab LCOS-Version 10.20 ist die Möglichkeit hinzugekommen, für DNS-Weiterleitungen für jedes Ziel eine eigene Loopback-Adresse anzugeben.

Loopback-Adressen

Im LANconfig lassen sich unter **IPv4** > **DNS** > **Loopback-Adressen** Loopback-Adressen für jede Gegenstelle hinterlegen. Somit gibt es dann eine einstellbare Absende-Adresse für DNS-Weiterleitungen. Jede Loopback-Adresse besteht aus genau einer Gegenstelle und Loopback-Adresse. Da pro Loopback-Adresse nur genau eine Gegenstelle eingetragen

werden kann, müssen hier zwei Einträge erfolgen, falls in den DNS-Weiterleitungen für eine Domain zwei Gegenstellen konfiguriert wurden.



Folgende Optionen sind je Loopback-Adresse möglich:

Ziel

Die Gegenstelle für eine Loopback-Adresse. Dies ist entweder ein Interface-Name, eine IPv4- oder IPv6-Adresse. Nach einem „@" kann ein Routing-Tag hinzugefügt werden. Die Gegenstelle muss genauso auch in der Tabelle DNS-Weiterleitungen vorkommen.

Absende-Adresse

Die Loopback-Adresse für eine bestimmte Gegenstelle. Dies ist entweder ein Interface-Name, eine IPv4- oder IPv6-Adresse oder eine benannte Loopback-Adresse.

Ergänzungen im Setup-Menü

Loopback-Adressen

Diese Tabelle bietet Ihnen die Möglichkeit, Loopback-Adressen für jede Gegenstelle zu hinterlegen. Somit gibt es dann eine einstellbare Absende-Adresse für DNS-Weiterleitungen. Jede Loopback-Adresse besteht aus genau einer Gegenstelle und Loopback-Adresse. Die Gegenstelle muss genauso auch in der Tabelle DNS-Weiterleitungen vorkommen. Da pro Loopback-Adresse nur genau eine Gegenstelle eingetragen werden kann, müssen hier zwei Einträge erfolgen, falls in den DNS-Weiterleitungen für eine Domain zwei Gegenstellen konfiguriert wurden.

SNMP-ID:

2.17.17

Pfad Telnet:

Setup > **DNS**

Gegenstelle

Die Gegenstelle als Teil einer Loopback-Adresse. Dies ist entweder ein Interface-Name, eine IPv4- oder IPv6-Adresse. Nach einem „@" kann ein Routing-Tag hinzugefügt werden. Die Gegenstelle muss genauso auch in der Tabelle DNS-Weiterleitungen vorkommen.

SNMP-ID:

2.17.17.1

Pfad Telnet:

Setup > **DNS** > **Loopback-Adressen**

Mögliche Werte:

max. 39 Zeichen aus `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default-Wert:

leer

Loopback-Adresse

Die Loopback-Adresse für eine bestimmte Gegenstelle. Dies ist entweder ein Interface-Name, eine IPv4 oder IPv6-Adresse oder eine benannte Loopback-Adresse.

SNMP-ID:

2.17.17.2

Pfad Telnet:

Setup > **DNS** > **Loopback-Adressen**

Mögliche Werte:

max. 39 Zeichen aus `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default-Wert:

leer

3.2 Locator / ID Separation Protocol (LISP)

Ab LCOS-Version 10.20 steht Ihnen LISP zur Auswahl.

Das Locator / ID Separation Protocol (LISP) nach RFC 6830 ist eine neue Routing-Architektur, das eine IP-Adresse in zwei Entitäten aufspaltet: Routing Locator (RLOC) und Endpoint Identifier (EID). Das Ziel ist eine hochskalierbare Routing-Architektur mit integriertem Routing- und Tunnel- bzw. Overlay-Protokoll zu erreichen.

Klassische Routing-Protokolle wie RIP, OSPF oder BGP arbeiten nach dem „Push-Prinzip" und verteilen proaktiv ihre besten Routen an ihre Nachbarn. Die Skalierbarkeit dieser Architektur ist nur begrenzt, insbesondere stellen sehr große BGP-Tabellen bzw. Routing-Tabellen zunehmend eine Herausforderung dar.

LISP arbeitet nach dem „Pull-Prinzip" und funktioniert ähnlich wie das Domain Name System (DNS). LISP-Router registrieren ihre Netze, genannt Endpoint Identifiers (EID), bei einer zentralen Instanz, genannt Map-Server bzw. Map-Resolver. Neben dem EID registrieren sie ebenso ihre globale (WAN-) Adresse, genannt Routing Locator (RLOC). Dadurch wird eine Trennung in Ortsinformation (Locator) und Identität (ID) erreicht.

Möchte ein anderer Router Daten zu einem entfernten LISP-Netz übertragen, so wird zunächst der LISP Map-Resolver nach den Zuordnungen zwischen dem angefragten EID-Präfix und dem Routing Locator befragt. Im nächsten Schritt wird zwischen beiden LISP-Routern ein Datentunnel etabliert.

LISP bringt aktuell keine Verschlüsselung des Datentunnels mit und wird in der Regel beim Einsatz in unsicheren Netzen wie dem Internet mit VPN kombiniert. Anwendungsszenarien für LISP sind Multi-VPNs.

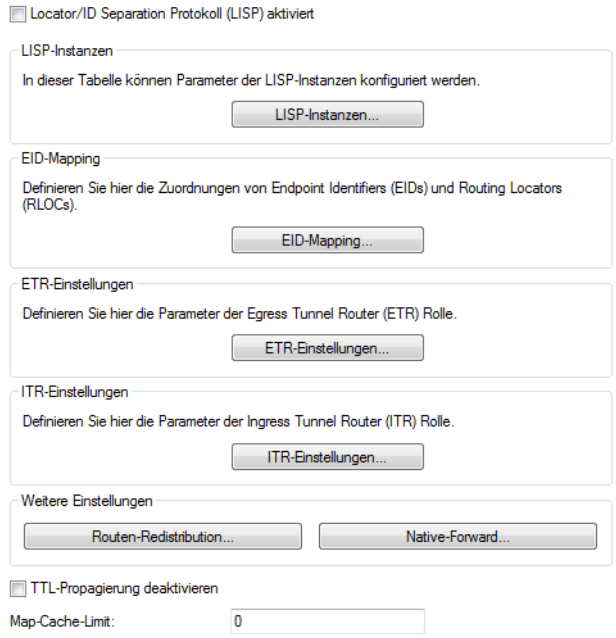
LCOS unterstützt ab Version 10.20 die folgenden Rollen:

- Ingress Tunnel Router (ITR)
- Egress Tunnel Router (ETR)

Nicht unterstützt wird aktuell die Rolle des Map-Servers bzw. des Map-Resolvers.

3.2.1 Konfiguration

Die Konfiguration des LISP-Routings finden Sie in LANconfig unter **Routing Protokolle** > **LISP**. Über den Schalter **Locator / ID Separation Protocol (LISP) aktiviert** wird dieses Routing-Protokoll ein- bzw. ausgeschaltet.



TTL-Propagierung deaktivieren

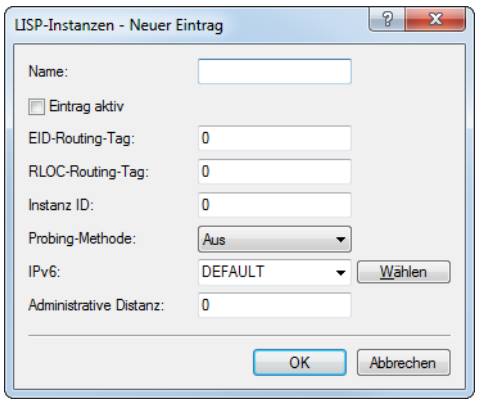
Bei Aktivierung wird vom ITR die Time-To-Live (TTL) nicht vom äußeren in den inneren Header kopiert. Dadurch erscheint für einen Client bei der Ausführung von Traceroute der LISP-Tunnel als ein Hop. Falls deaktiviert, dann werden alle Hops zwischen ITR und ETR durch Traceroute angezeigt.

Map-Cache-Limit

Definiert die maximale Anzahl von Einträgen im Map-Cache über alle LISP-Instanzen. Nach dem Erreichen des Limits werden neue Einträge abgelehnt. Erst nachdem ältere Einträge im Map-Cache ungültig geworden sind werden neue Einträge akzeptiert. Eine 0 bedeutet keine Beschränkung.

LISP-Instanzen

Diese Tabelle enthält die globale Konfiguration der LISP-Instanzen auf dem Gerät.



Name

Definiert einen eindeutigen Namen für eine LISP-Instanz. Dieser Name wird in weiteren LISP-Tabellen referenziert.

Eintrag aktiv

Aktiviert oder deaktiviert diese LISP-Instanz.

EID-Routing-Tag

Routing-Tag des Endpoint Identifiers (EID) dieser Instanz.

RLOC-Routing-Tag

Routing-Tag des Routing Locators (RLOC) dieser Instanz.

Instanz-ID

LISP Instance ID als numerischer Tag aus RFC 8060 (LISP Canonical Address Format (LCAF)) zur Segmentierung der Netze im Zusammenhang mit ARF.

Probing-Methode

Definiert die Methode mit der die Erreichbarkeit der RLOCs der Map-Cache-Einträge periodisch geprüft wird. Möglich Methoden:

- Aus: Die Erreichbarkeit der RLOCs wird nicht periodisch geprüft.
- RLOC-Probing: Die Erreichbarkeit der RLOCs wird durch LISP RLOC-Nachrichten periodisch geprüft.

IPv6

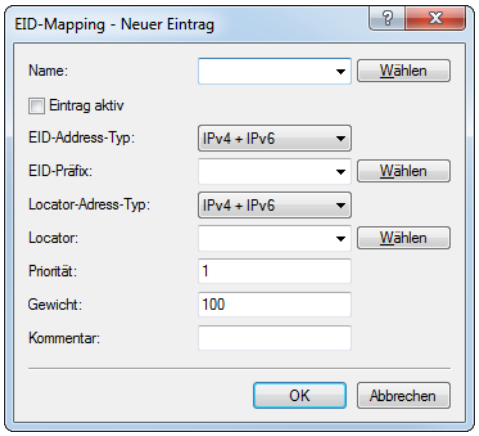
Name des IPv6-WAN-Profils aus der IPv6-WAN-Interface-Tabelle. Ein Eintrag wird zwingend benötigt, falls IPv6-EIDs verwendet werden.

Administrative Distanz

Die administrative Distanz dieser LISP-Instanz.

EID-Mapping

Diese Tabelle definiert die Abbildung von EIDs auf RLOCs, die beim Map-Server registriert werden sollen.



Name

Referenziert den Namen der LISP-Instanz.

Eintrag aktiv

Aktiviert oder deaktiviert dieses EID-Mapping.

EID-Adress-Typ

Protokollversion des EID-Präfix bei Referenzierung des EID-Präfix über einen Interface- bzw. Netzwerknamen. Mögliche Werte:

- **IPv4**: Es wird nur das IPv4-Präfix des referenzierten Interfaces verwendet.
- **IPv6**: Es wird nur das IPv6-Präfix des referenzierten Interfaces verwendet.
- **IPv4+IPv6**: Es wird sowohl das IPv4-Präfix als auch das IPv6-Präfix des referenzierten Interfaces verwendet.

EID-Präfix

EID-Präfix des EID-Mappings. Mögliche Werte sind ein IPv4-Netzwerkname oder ein IPv6-Interface, z. B. INTRANET, oder eine benannte Loopbackadresse.

Locator-Adress-Typ

Protokollversion des RLOCs bei Referenzierung des EID-Präfix über einen Interface-Namen. Mögliche Werte:

- **IPv4**: Es wird nur die IPv4-Adresse als RLOC des referenzierten Interfaces verwendet.
- **IPv6**: Es wird nur die IPv6-Adresse als RLOC des referenzierten Interfaces verwendet.
- **IPv4+IPv6**: Es wird sowohl die IPv4-Adresse als auch die IPv6-Adresse als RLOC des referenzierten Interfaces verwendet.

Locator

RLOC des EID-Mappings. Mögliche Werte sind benannte Gegenstellen, IPv6-WAN-Interfaces, oder Loopback-Interfaces.

Priorität

Die Priorität des EID-Mappings. Default: 1.

Gewicht

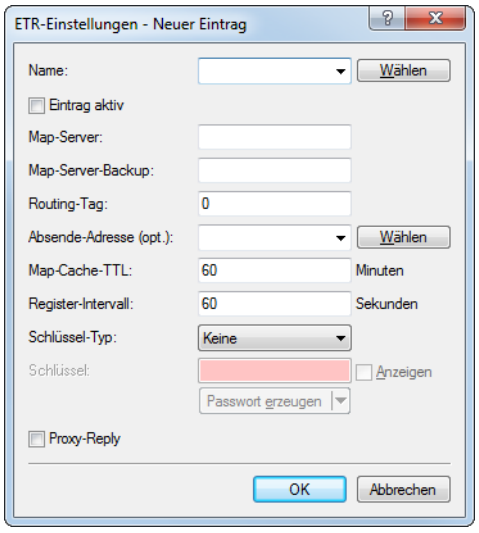
Das Gewicht des EID-Mappings. Default: 100.

Kommentar

Geben Sie eine aussagekräftige Beschreibung für diesen Eintrag an.

ETR-Einstellungen

Diese Tabelle definiert die Parameter für die Rolle als Egress Tunnel Router (ETR).



Name

Referenziert den Namen der LISP-Instanz.

Eintrag aktiv

Aktiviert oder deaktiviert diese ETR-Einstellungen.

Map-Server

IPv4- oder IPv6-Adresse des LISP Map-Servers

Map-Server-Backup

IPv4- oder IPv6-Adresse des LISP Backup-Map-Servers. Die LISP-Registrierung wird parallel sowohl an den primären Map-Server als auch an den Backup-Map-Server gesendet.

Routing-Tag

Routing-Tag, das zum Erreichen des Map-Servers verwendet werden soll.

Absende-Adresse (opt)

Enthält die Absender-Adresse als benanntes Interface, die bei LISP-Kommunikation mit dem Map-Server verwendet wird.

Map-Cache-TTL

Time-To-Live der EID-Mappings in Minuten, die beim Map-Server registriert werden.

Register-Intervall

Registrierungsintervall in Sekunden, in dem Map-Registrierungen an den Map-Server gesendet werden.

Schlüssel-Typ

Verwendeter Algorithmus für die Authentifizierung am Map-Server. Mögliche Werte:

- Keine
- HMAC-SHA-1-96
- HMAC-SHA-256-128

Schlüssel

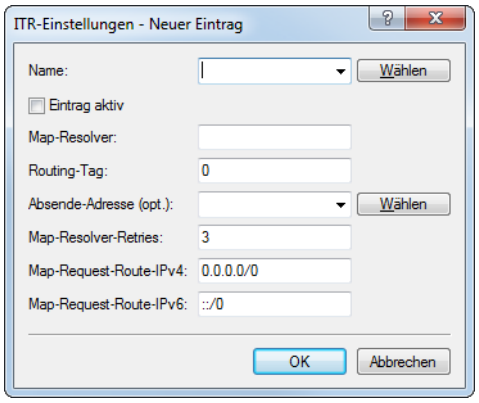
Schlüssel bzw. Passwort, mit dem die Registrierung des EID-Mappings am Map-Server erfolgt.

Proxy-Reply

Definiert, ob das Proxy-Reply-Bit in Map-Registrierungen gesetzt wird. In diesem Fall agiert der Map-Server als Proxy und antwortet stellvertretend für den ETR bei Map-Requests.

ITR-Einstellungen

Diese Tabelle definiert die Parameter für die Rolle als Ingress Tunnel Router (ITR).



Name

Referenziert den Namen der LISP-Instanz.

Eintrag aktiv

Aktiviert oder deaktiviert diese ITR-Einstellungen.

Map-Resolver

IPv4- oder IPv6-Adresse des LISP Map-Resolvers.

Routing-Tag

Routing-Tag, das zum Erreichen des Map-Resolvers verwendet wird.

Absende-Adresse (opt)

Enthält die Absender-Adresse als benanntes Interfaces, die bei LISP-Kommunikation mit dem Map-Resolver verwendet wird.

Map-Resolver-Retries

Anzahl der Wiederholungen bei Map-Anfragen an den Map-Resolver. Default: 3

Map-Request-Route-IPv4

Definiert die IPv4-Route bzw. das Präfix für die LISP-Map-Requests durchgeführt werden sollen.

Map-Request-Route-IPv6

Definiert die IPv6-Route bzw. das Präfix für die LISP-Map-Requests durchgeführt werden sollen.

Routen-Redistribution

Durch Routen-Redistribution können Routen aus der Routing-Tabelle in den LISP-Map-Cache importiert werden. Für diese Routen werden entsprechende Map-Requests durchgeführt.

Ebenso können durch Routen-Redistribution Routen aus der Routing-Tabelle importiert werden und dynamisch als EID-Präfix beim Map-Server registriert werden.

Name

Referenziert den Namen der LISP-Instanz.

Routen weiter verteilen

Definiert die Routenquellen der importierten Routen.

- **Statisch**: Das Gerät importiert statische Routen aus der Routing-Tabelle in den LISP-Map-Cache oder in die EID-Tabelle als EID-Präfix.
- **Verbunden**: Das Gerät importiert von direkt angeschlossenen Netzwerken aus der Routing-Tabelle in den LISP-Map-Cache oder in die EID-Tabelle als EID-Präfix.
- **OSPF**: Das Gerät importiert OSPF-Routen aus der Routing-Tabelle in den LISP-Map-Cache oder in die EID-Tabelle als EID-Präfix.

- **BGP**: Das Gerät importiert BGP-Routen aus der Routing-Tabelle in den LISP-Map-Cache oder in die EID-Tabelle als EID-Präfix.

Ziel

Definiert das Ziel der nach LISP importierten Routen. Mögliche Werte:

- **Map-Cache**: Importiert die Routen in den Map-Cache. Für diese Routen führt LISP Map-Requests aus.
- **EID-Tabelle**: Import die Routen in die LISP-EID-Tabelle. Diese Routen werden beim Map-Server als EID-Präfix mit dem konfigurierten RLOC registriert.

Locator-Adress-Typ

Protokollversion des RLOCs bei Referenzierung des EID-Präfix über einen Interface-Namen. Mögliche Werte:

- **IPv4**: Es wird nur die IPv4-Adresse als RLOC des referenzierten Interfaces verwendet.
- **IPv6**: Es wird nur die IPv6-Adresse als RLOC des referenzierten Interfaces verwendet.
- **IPv4+IPv6**: Es wird sowohl die IPv4-Adresse als auch die IPv6-Adresse als RLOC des referenzierten Interfaces verwendet.

Locator

Definiert den RLOC mit dem die importierten EID-Präfixe beim Map-Server registriert werden. Mögliche Werte sind benannte Gegenstellen, IPv6-WAN-Interfaces, oder Loopback-Interfaces.

Priorität

Die Priorität. Default: 1

Gewicht

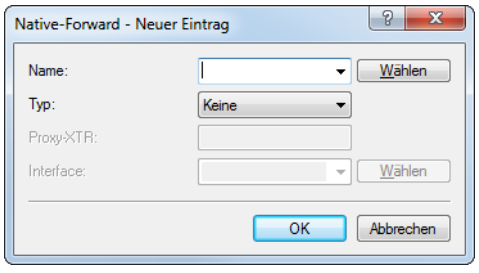
Das Gewicht. Default: 100

Native-Forward

Sollen LISP-Netzwerke mit Nicht-LISP-Netzwerken kommunizieren, dann können Proxy-Router verwendet werden. Diese Rollen werden als Proxy Ingress Tunnel Router (Proxy-ITR) und Proxy Egress Tunnel Router (Proxy-ETR) bezeichnet.

Erhält ein LISP-Router vom Map-Resolver eine negative Antwort, d. h. es liegt keine Abbildung zwischen angefragten EID zu einem RLOC vor, so kann der LISP-Router die zugehörigen Pakete entweder an einen Proxy xTR senden (Paket mit LISP-Header) oder über ein anderes lokales Interface versenden (Paket ohne LISP-Header).

LCOS unterstützt nur Szenarien bei denen PITR- und PETR-Funktionen auf dem gleichen Router betrieben werden.



Name

Referenziert den Namen der LISP-Instanz.

Typ

Definiert, auf welchem Weg Pakete zu Nicht-LISP-Netzwerken gesendet werden sollen.

- **Keine**: Pakete zu Nicht-LISP-Netzwerken werden nicht weitergeleitet und verworfen
- **ProxXTR**: Pakete zu Nicht-LISP-Netzwerken werden an einen ProxyXTR gesendet
- **Interface**: Pakete zu Nicht-LISP-Netzwerken werden über ein lokales Interface gesendet

Proxy-XTR

IPv4- oder IPv6-Adresse des Proxy-XTRs über den Pakete zu Nicht-LISP-Netzwerken gesendet werden.

Interface

Name des Interfaces über das Pakete zu Nicht-LISP-Netzwerken gesendet werden.

3.2.2 LISP-Tutorial

In diesem Tutorial soll das ARF-Netzwerk mit Namen INTRANET und Tag 1 als LISP-Netzwerk konfiguriert werden. Dazu wird das Netzwerk mit seinem Präfix als EID-Präfix beim MAP-Server 1.1.1.1 registriert. Die Registrierung erfolgt über die WAN-Gegenstelle INTERNET (Default-Route) mit Tag 0. Die IP-Adresse auf der Gegenstelle INTERNET kann dabei dynamisch oder statisch sein. Diese Adresse wird als RLOC-Adresse beim MAP-Server registriert.

Daten aus dem INTRANET sollen in den LISP-Tunnel geschickt werden. Dazu stellt der Router für alle unbekannten Ziele einen Map-Request an den MAP-Resolver 1.1.1.1.

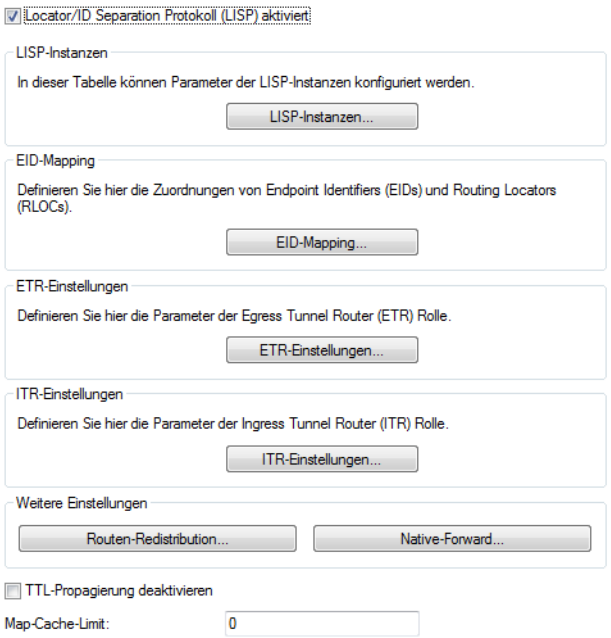
Liefert der Map-Resolver ein positives Mapping, so baut LISP automatisch einen dynamischen Tunnel zum entfernten LISP-Router auf und trägt entsprechende Routen in die Routing-Tabelle ein.

Liefert der Map-Resolver ein negatives Mapping, d. h. das Ziel-Präfix ist unbekannt bzw. auf dem Map-Server / Resolver nicht registriert, so kann das Paket optional ohne Tunnel direkt über die Gegenstelle INTERNET versendet werden (Native Forward).

Eine manuelle Konfiguration von LISP-Routen ist nicht erforderlich. Diese werden von LISP automatisch angelegt und wieder entfernt.

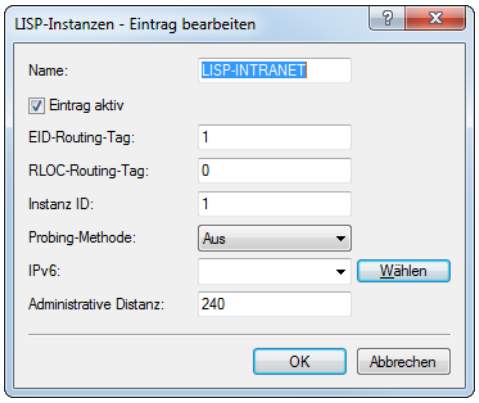
Es müssen grundsätzlich immer manuell Einträge für die jeweiligen Routing-Tags in der WAN-Tag-Tabelle angelegt werden.

1. Aktivieren Sie als erstes das LISP-Protokoll unter **Routing Protokolle** > **LISP** > **Locator/ID Separation-Protokoll (LISP) aktiviert**.

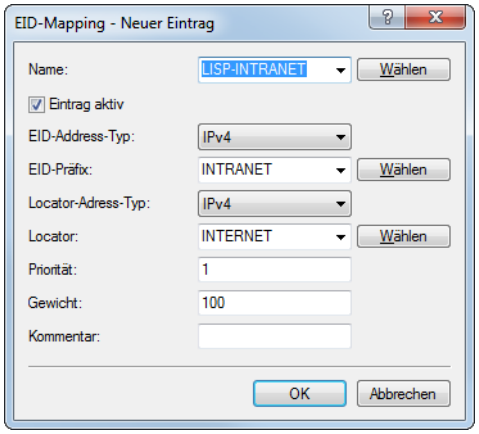


2. Legen Sie einen neuen Eintrag in der Tabelle der LISP-Instanzen an. Gehen Sie dazu nach **Routing Protokolle** > **LISP** > **LISP-Instanzen** und klicken auf **Hinzufügen**.
   a) Geben Sie dieser LISP-Instanz einen **Namen**, z. B. LISP-INTRANET.

b) Setzen Sie den **Eintrag aktiv**.
c) Setzen Sie das **EID-Routing-Tag** auf 1.
d) Setzen Sie das **RLOC-Routing-Tag** auf den Wert des Tags der WAN-Gegenstelle INTERNET, hier also 0.
e) Setzen Sie die **Instanz ID** auf den im LISP-Map-Server angelegten Wert, hier also 1 wie das Tag des INTRANET.
f) Nehmen Sie bei **IPv6** den Eintrag **DEFAULT** weg, da wir hier nur IPv4 betrachten.

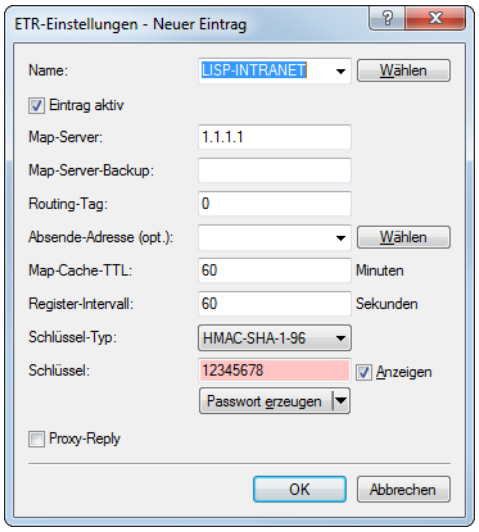


3. Legen Sie einen neuen Eintrag in der Tabelle EID-Mapping an, über den die Vreknüpfung des EID-Präfixes und des Locators erfolgen. Gehen Sie dazu nach **Routing Protokolle** > **LISP** > **EID-Mapping** und klicken auf **Hinzufügen**.
a) Wählen Sie als **Name** den der zuvor angelegten LISP-Instanz, hier LISP-INTRANET.
b) Setzen Sie den **Eintrag aktiv**.
c) Setzen Sie sowohl den **EID-Adress-Typ** als auch den **Locator-Adress-Typ** auf IPv4.
d) Wählen Sie als **EID-Präfix** INTRANET.
e) Wählen Sie als **Locator** INTERNET.

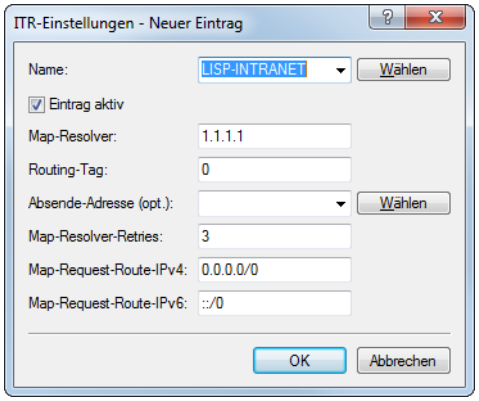


4. Legen Sie einen neuen Eintrag mit den Parametern zur Kommunikation mit dem Map-Server in der Tabelle ETR-Einstellungen an. Gehen Sie dazu nach **Routing Protokolle** > **LISP** > **ETR-Einstellungen** und klicken auf **Hinzufügen**.
a) Wählen Sie als **Name** den der zuvor angelegten LISP-Instanz, hier LISP-INTRANET.
b) Setzen Sie den **Eintrag aktiv**.
c) Setzen Sie den **Map-Server** auf 1.1.1.1.
d) Setzen Sie das **Routing-Tag** auf 0.

e) Setzen Sie den **Schlüssel-Typ** und **Schlüssel** für die Verbindung mit dem Map-Server. Diese müssen mit dem auf Map-Server konfigurierten Typ und Passwort übereinstimmen. In diesem Beispiel nehmen wir HMAC-SHA-1-96 und 12345678.

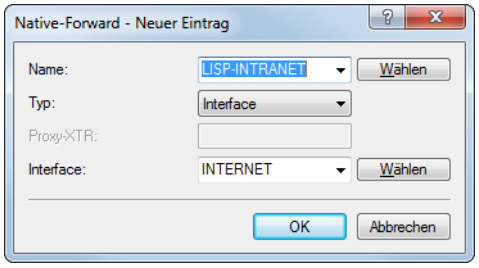


5. Legen Sie einen neuen Eintrag mit den Parametern zur Kommunikation mit dem Map-Resolver in der Tabelle ITR-Einstellungen an. Gehen Sie dazu nach **Routing Protokolle** > **LISP** > **ITR-Einstellungen** und klicken auf **Hinzufügen**.
   a) Wählen Sie als **Name** den der zuvor angelegten LISP-Instanz, hier LISP-INTRANET.
   b) Setzen Sie den **Eintrag aktiv**.
   c) Setzen Sie den **Map-Resolver** auf 1.1.1.1.
   d) Setzen Sie das **Routing-Tag** auf 0.



6. Optional: Pakete an Zieladressen, die keine LISP-Netze sind, können direkt über ein lokales Interfrace, also ohne Verwendung des LISP-Tunnels, versendet werden. In unserem Beispiel wird hierzu das Interface INTERNET verwendet. Legen Sie einen neuen Eintrag in der Tabelle Native-Forward an. Gehen Sie dazu nach **Routing Protokolle** > **LISP** > **Native-Forward** und klicken auf **Hinzufügen**.
   a) Wählen Sie als **Name** den der zuvor angelegten LISP-Instanz, hier LISP-INTRANET.
   b) Setzen Sie den **Typ** auf **Interface**.

c) Wählen Sie als **Interface** INTERNET.



7. Legen Sie unter **Kommunikation** > **Gegenstellen** > **WAN-Tag-Tabelle** mit einem Klick auf **Hinzufügen** einen Eintrag für die gerade erstellte LISP-Instanz mit der Instanz-ID 1 an.

   Für jede LISP-Instanz muss in der WAN-Tag-Tabelle ein Eintrag mit dem zugehörigen Schnittstellen-Tag für EID / ARF-Netz angelegt werden.

   Dazu muss ein Eintrag angelegt werden, wobei der Gegenstellenname LISP-<LISP-Instanz-ID>* lautet. Der Gegenstellename wird gebildet aus dem Schlüsselwort LISP, ergänzt um die entsprechende LISP-Instanz-ID (in Hexadezimal-Form) sowie um die Wildcard *. Dies dient der eindeutigen Zuordnung des ankommenden Datenverkehrs der LISP-Tunnel zu EID / ARF-Netzwerk.

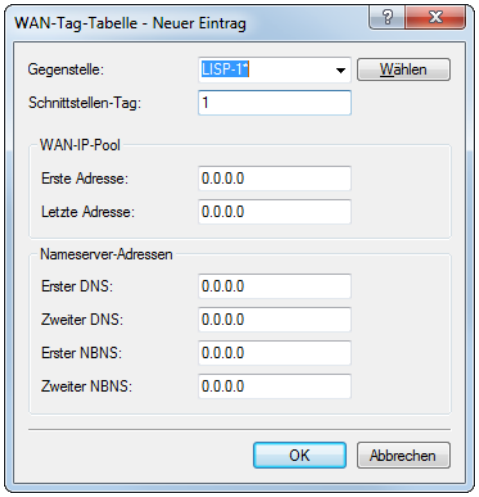
   Die Instanz-ID muss Hexadezimal ohne führendes 0x angegeben werden.

   Darstellung: LISP-<LISP-Instanz-ID>*

   Beispiele:

   - für die LISP-Instanz 1: LISP-1*
   - für die LISP-Instanz 15: LISP-F*

   a) Geben Sie in das Feld **Gegenstelle** nach dem gerade beschriebenen Muster für die LISP-Instanz mit der Instanz-ID 1 den Wert „LISP-1*“ ein.
   b) Als **Schnittstellen-Tag** geben Sie die 1 ein.



Fertig!

3.2.3 Ergänzungen im Setup-Menü

LISP

Einstellungen für Locator / ID Separation Protocol (LISP).

SNMP-ID:

2.93.4

Pfad Telnet:

Setup > **Routing-Protokolle**

Instances

Diese Tabelle enthält die globale Konfiguration der LISP-Instanzen auf dem Gerät.

SNMP-ID:

2.93.4.1

Pfad Telnet:

Setup > **Routing-Protokolle** > **LISP**

Name

Definiert einen eindeutigen Namen für eine LISP-Instanz. Dieser Name wird in weiteren LISP-Tabellen referenziert.

SNMP-ID:

2.93.4.1.1

Pfad Telnet:

Setup > **Routing-Protokolle** > **LISP** > **Instances**

Mögliche Werte:

max. 24 Zeichen aus `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Aktiv

Aktiviert oder deaktiviert diese LISP-Instanz.

SNMP-ID:

2.93.4.1.2

Pfad Telnet:

Setup > **Routing-Protokolle** > **LISP** > **Instances**

Mögliche Werte:

Nein
Ja

EID-Rtg-Tag

Routing-Tag des Endpoint Identifiers (EID) dieser Instanz.

SNMP-ID:

2.93.4.1.3

Pfad Telnet:

Setup > **Routing-Protokolle** > **LISP** > **Instances**

Mögliche Werte:

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

RLOC-Rtg-Tag

Routing-Tag des Routing Locators (RLOC) dieser Instanz.

SNMP-ID:

2.93.4.1.4

Pfad Telnet:

Setup > **Routing-Protokolle** > **LISP** > **Instances**

Mögliche Werte:

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

Instance-ID

LISP Instance ID als numerischer Tag aus RFC 8060 (LISP Canonical Address Format (LCAF)) zur Segmentierung der Netze im Zusammenhang mit ARF.

SNMP-ID:

2.93.4.1.5

Pfad Telnet:

Setup > **Routing-Protokolle** > **LISP** > **Instances**

Mögliche Werte:

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

Probing-Method

Definiert die Methode mit der die Erreichbarkeit der RLOCs der Map-Cache-Einträge periodisch geprüft wird.

SNMP-ID:

2.93.4.1.6

Pfad Telnet:

Setup > **Routing-Protokolle** > **LISP** > **Instances**

Mögliche Werte:

Off

Die Erreichbarkeit der RLOCs wird nicht periodisch geprüft.

RLOC-Probing

Die Erreichbarkeit der RLOCs wird durch LISP RLOC-Nachrichten periodisch geprüft.

IPv6

Name des IPv6-WAN-Profils aus der IPv6-WAN-Interface-Tabelle. Ein Eintrag wird zwingend benötigt, falls IPv6-EIDs verwendet werden.

SNMP-ID:

2.93.4.1.8

Pfad Telnet:

Setup > **Routing-Protokolle** > **LISP** > **Instances**

Mögliche Werte:

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

Default-Wert:

600

Admin-Distance

Administrative Routing-Distanz.

SNMP-ID:

2.93.4.1.9

Pfad Telnet:

Setup > **Routing-Protokolle** > **LISP** > **Instances**

Mögliche Werte:

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

Default-Wert:

240

EID-Mapping

Diese Tabelle definiert die Abbildung von EIDs auf RLOCs, die beim Map-Server registriert werden sollen.

SNMP-ID:

2.93.4.2

Pfad Telnet:

Setup > **Routing-Protokolle** > **LISP**

Name

Referenziert den Namen der LISP-Instanz.

SNMP-ID:

2.93.4.2.1

Pfad Telnet:

Setup > **Routing-Protokolle** > **LISP** > **EID-Mapping**

Mögliche Werte:

max. 24 Zeichen aus `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

EID-Address-Type

Diese Bitmaske definiert die Protokollversion des EID-Präfix bei Referenzierung des EID-Präfix über einen Interface- bzw. Netzwerknamen.

SNMP-ID:

2.93.4.2.2

Pfad Telnet:

Setup > **Routing-Protokolle** > **LISP** > **EID-Mapping**

Mögliche Werte:

IPv4
IPv6

EID-Prefix

EID-Präfix des EID-Mappings. Mögliche Werte sind ein IPv4-Netzwerkname oder ein IPv6-Interface, z. B. INTRANET, oder eine benannte Loopbackadresse.

SNMP-ID:

2.93.4.2.3

Pfad Telnet:

Setup > **Routing-Protokolle** > **LISP** > **EID-Mapping**

Mögliche Werte:

max. 43 Zeichen aus `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Locator-Address-Type

Diese Bitmaske definiert die Protokollversion des RLOCs bei Referenzierung des EID-Präfix über einen Interface-Namen.

SNMP-ID:

2.93.4.2.4

Pfad Telnet:

Setup > **Routing-Protokolle** > **LISP** > **EID-Mapping**

Mögliche Werte:

IPv4
IPv6

Locator

RLOC des EID-Mappings. Mögliche Werte sind benannte Gegenstellen, IPv6-WAN-Interfaces, oder Loopback-Interfaces.

SNMP-ID:

2.93.4.2.5

Pfad Telnet:

Setup > **Routing-Protokolle** > **LISP** > **EID-Mapping**

Mögliche Werte:

max. 39 Zeichen aus `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Aktiv

SNMP-ID:

2.93.4.2.6

Pfad Telnet:

Setup > **Routing-Protokolle** > **LISP** > **EID-Mapping**

Mögliche Werte:

Nein
Ja

Priority

Die Priorität des EID-Mappings.

SNMP-ID:

2.93.4.2.7

Pfad Telnet:

Setup > **Routing-Protokolle** > **LISP** > **EID-Mapping**

Mögliche Werte:

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

Default-Wert:

1

Weight

Das Gewicht des EID-Mappings.

SNMP-ID:

2.93.4.2.8

Pfad Telnet:

Setup > **Routing-Protokolle** > **LISP** > **EID-Mapping**

Mögliche Werte:

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

Default-Wert:

100

Kommentar

Geben Sie eine aussagekräftige Beschreibung für diesen Eintrag an.

SNMP-ID:

2.93.4.2.9

Pfad Telnet:

Setup > **Routing-Protokolle** > **LISP** > **EID-Mapping**

Mögliche Werte:

max. 25 Zeichen aus `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

ITR-Settings

Diese Tabelle definiert die Parameter für die Rolle als Ingress Tunnel Router (ITR).

SNMP-ID:

2.93.4.3

Pfad Telnet:

Setup > **Routing-Protokolle** > **LISP**

Name

Referenziert den Namen der LISP-Instanz.

SNMP-ID:

2.93.4.3.1

Pfad Telnet:

Setup > **Routing-Protokolle** > **LISP** > **ITR-Settings**

Mögliche Werte:

max. 24 Zeichen aus `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Map-Resolver

IPv4- oder IPv6-Adresse des LISP Map-Resolvers.

SNMP-ID:

2.93.4.3.2

Pfad Telnet:

Setup > **Routing-Protokolle** > **LISP** > **ITR-Settings**

Mögliche Werte:

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

Aktiv

Aktiviert oder deaktiviert diese ITR-Einstellungen.

SNMP-ID:

2.93.4.3.3

Pfad Telnet:

Setup > **Routing-Protokolle** > **LISP** > **ITR-Settings**

Mögliche Werte:

Nein
Ja

Loopback-Address

Enthält die Absender-Adresse als benanntes Interfaces, die bei LISP-Kommunikation mit dem Map-Resolver verwendet wird.

SNMP-ID:

2.93.4.3.4

Pfad Telnet:

Setup > **Routing-Protokolle** > **LISP** > **ITR-Settings**

Mögliche Werte:

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

Rtg-Tag

Routing-Tag, das zum Erreichen des Map-Resolvers verwendet wird.

SNMP-ID:

2.93.4.3.5

Pfad Telnet:

Setup > **Routing-Protokolle** > **LISP** > **ITR-Settings**

Mögliche Werte:

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

Map-Resolver-Retries

Anzahl der Wiederholungen bei Map-Anfragen an den Map-Resolver.

SNMP-ID:

2.93.4.3.6

Pfad Telnet:

Setup > **Routing-Protokolle** > **LISP** > **ITR-Settings**

Mögliche Werte:

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

Default-Wert:

3

Map-Request-Route-IPv4

Definiert die IPv4-Route bzw. das Präfix für die LISP-Map-Requests durchgeführt werden sollen.

SNMP-ID:

2.93.4.3.7

Pfad Telnet:

Setup > **Routing-Protokolle** > **LISP** > **ITR-Settings**

Mögliche Werte:

max. 18 Zeichen aus `[A-F][a-f][0-9]:.`

Map-Request-Route-IPv6

Definiert die IPv6-Route bzw. das Präfix für die LISP-Map-Requests durchgeführt werden sollen.

SNMP-ID:

2.93.4.3.8

Pfad Telnet:

Setup > **Routing-Protokolle** > **LISP** > **ITR-Settings**

Mögliche Werte:

max. 43 Zeichen aus `[A-F][a-f][0-9]:.`

ETR-Settings

Diese Tabelle definiert die Parameter für die Rolle als Egress Tunnel Router (ETR).

SNMP-ID:

2.93.4.4

Pfad Telnet:

Setup > **Routing-Protokolle** > **LISP**

Name

Referenziert den Namen der LISP-Instanz.

SNMP-ID:

2.93.4.4.1

Pfad Telnet:

Setup > **Routing-Protokolle** > **LISP** > **ETR-Settings**

Mögliche Werte:

max. 24 Zeichen aus `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Map-Server

IPv4- oder IPv6-Adresse des LISP Map-Servers

SNMP-ID:

2.93.4.4.2

Pfad Telnet:

Setup > **Routing-Protokolle** > **LISP** > **ETR-Settings**

Mögliche Werte:

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

Aktiv

Aktiviert oder deaktiviert diese ETR-Einstellungen.

SNMP-ID:

2.93.4.4.3

Pfad Telnet:

Setup > **Routing-Protokolle** > **LISP** > **ETR-Settings**

Mögliche Werte:

Nein
Ja

Loopback-Address

Enthält die Absender-Adresse als benanntes Interface, die bei LISP-Kommunikation mit dem Map-Server verwendet wird.

SNMP-ID:

2.93.4.4.4

Pfad Telnet:

Setup > **Routing-Protokolle** > **LISP** > **ETR-Settings**

Mögliche Werte:

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

Rtg-Tag

Routing-Tag, das zum Erreichen des Map-Servers verwendet werden soll.

SNMP-ID:

2.93.4.4.5

Pfad Telnet:

Setup > **Routing-Protokolle** > **LISP** > **ETR-Settings**

Mögliche Werte:

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

Map-Cache-TTL-Minutes

Time-To-Live der EID-Mappings in Minuten, die beim Map-Server registriert werden.

SNMP-ID:

2.93.4.4.6

Pfad Telnet:

Setup > **Routing-Protokolle** > **LISP** > **ETR-Settings**

Mögliche Werte:

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

Map-Register-Interval-Seconds

Registrierungsintervall in Sekunden, in dem Map-Registrierungen an den Map-Server gesendet werden.

SNMP-ID:

2.93.4.4.7

Pfad Telnet:

Setup > **Routing-Protokolle** > **LISP** > **ETR-Settings**

Mögliche Werte:

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

Key-Type

Verwendeter Algorithmus für die Authentifizierung am Map-Server.

SNMP-ID:

2.93.4.4.8

Pfad Telnet:

Setup > **Routing-Protokolle** > **LISP** > **ETR-Settings**

Mögliche Werte:

Kein(e)
HMAC-SHA-1-96
HMAC-SHA-256-128

Key

Schlüssel bzw. Passwort, mit dem die Registrierung des EID-Mappings am Map-Server erfolgt.

SNMP-ID:

2.93.4.4.9

Pfad Telnet:

Setup > **Routing-Protokolle** > **LISP** > **ETR-Settings**

Mögliche Werte:

max. 24 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.` `

Proxy-Reply

Definiert, ob das Proxy-Reply-Bit in Map-Registrierungen gesetzt wird. In diesem Fall agiert der Map-Server als Proxy und antwortet stellvertretend für den ETR bei Map-Requests.

SNMP-ID:

2.93.4.4.10

Pfad Telnet:

Setup > **Routing-Protokolle** > **LISP** > **ETR-Settings**

Mögliche Werte:

Nein
Ja

Map-Server-Backup

IPv4- oder IPv6-Adresse des LISP Backup-Map-Servers. Die LISP-Registrierung wird parallel sowohl an den primären Map-Server als auch an den Backup-Map-Server gesendet.

SNMP-ID:

2.93.4.4.11

Pfad Telnet:

Setup > **Routing-Protokolle** > **LISP** > **ETR-Settings**

Mögliche Werte:

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

Aktiv

Über diesen Schalter wird das Routing-Protokoll Locator / ID Separation Protocol (LISP) ein- bzw. ausgeschaltet.

SNMP-ID:

2.93.4.5

Pfad Telnet:

Setup > **Routing-Protokolle** > **LISP**

Mögliche Werte:

Nein
Ja

Default-Wert:

Nein

Disable-TTL-Propagation

Falls Sie diesen Schalter aktivieren, dann wird vom ITR die Time-To-Live (TTL) nicht vom äußeren in den inneren Header kopiert. Dadurch erscheint für einen Client bei der Ausführung von Traceroute der LISP-Tunnel als ein Hop. Falls deaktiviert, dann werden alle Hops zwischen ITR und ETR durch Traceroute angezeigt.

SNMP-ID:

2.93.4.7

Pfad Telnet:

Setup > **Routing-Protokolle** > **LISP**

Mögliche Werte:

Nein
Ja

Default-Wert:

Nein

Map-Cache-Limit

Definiert die maximale Anzahl von Einträgen im Map-Cache über alle LISP-Instanzen. Nach dem Erreichen des Limits werden neue Einträge angelehnt. Erst nachdem ältere Einträge im Map-Cache ungültig geworden sind werden neue Einträge akzeptiert. Eine 0 bedeutet keine Beschränkung.

SNMP-ID:

2.93.4.8

Pfad Telnet:

Setup > **Routing-Protokolle** > **LISP**

Mögliche Werte:

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

Default-Wert:

0

Native-Forward

SNMP-ID:

2.93.4.9

Pfad Telnet:

Setup > **Routing-Protokolle** > **LISP**

Name

Referenziert den Namen der LISP-Instanz.

SNMP-ID:

2.93.4.9.1

Pfad Telnet:

Setup > **Routing-Protokolle** > **LISP** > **Native-Forward**

Mögliche Werte:

max. 24 Zeichen aus `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Type

SNMP-ID:

2.93.4.9.3

Pfad Telnet:

Setup > **Routing-Protokolle** > **LISP** > **Native-Forward**

Mögliche Werte:

Kein(e)
ProxyXTR
Interface

Proxy-XTR

SNMP-ID:

2.93.4.9.4

Pfad Telnet:

Setup > **Routing-Protokolle** > **LISP** > **Native-Forward**

Mögliche Werte:

max. 43 Zeichen aus `[A-F][a-f][0-9]:.`

Interface

SNMP-ID:

2.93.4.9.5

Pfad Telnet:

Setup > **Routing-Protokolle** > **LISP** > **Native-Forward**

Mögliche Werte:

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

Redistribution

Durch Routen-Redistribution können Routen aus der Routing-Tabelle in den LISP-Map-Cache importiert werden. Für diese Routen werden entsprechende Map-Requests durchgeführt.

Ebenso können durch Routen-Redistribution Routen aus der Routing-Tabelle importiert werden und dynamisch als EID-Präfix beim Map-Server registriert werden.

SNMP-ID:

2.93.4.10

Pfad Telnet:

Setup > **Routing-Protokolle** > **LISP**

Name

Referenziert den Namen der LISP-Instanz.

SNMP-ID:

2.93.4.10.1

Pfad Telnet:

Setup > **Routing-Protokolle** > **LISP** > **Redistribution**

Mögliche Werte:

max. 24 Zeichen aus `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Source

Diese Bitmaske definiert die Routenquellen der importierten Routen.

SNMP-ID:

2.93.4.10.2

Pfad Telnet:

Setup > **Routing-Protokolle** > **LISP** > **Redistribution**

Mögliche Werte:

Connected

Das Gerät importiert von direkt angeschlossenen Netzwerken aus der Routing-Tabelle in den LISP-Map-Cache oder in die EID-Tabelle als EID-Präfix.

Static

Das Gerät importiert statische Routen aus der Routing-Tabelle in den LISP-Map-Cache oder in die EID-Tabelle als EID-Präfix.

OSPF

Das Gerät importiert OSPF-Routen aus der Routing-Tabelle in den LISP-Map-Cache oder in die EID-Tabelle als EID-Präfix.

BGP

Das Gerät importiert BGP-Routen aus der Routing-Tabelle in den LISP-Map-Cache oder in die EID-Tabelle als EID-Präfix.

Destination

Definiert das Ziel der nach LISP importierten Routen.

SNMP-ID:

2.93.4.10.3

Pfad Telnet:

Setup > **Routing-Protokolle** > **LISP** > **Redistribution**

Mögliche Werte:

Map-Cache

Importiert die Routen in den Map-Cache. Für diese Routen führt LISP Map-Requests aus.

Eid-Table

Import die Routen in die LISP-EID-Tabelle. Diese Routen werden beim Map-Server als EID-Präfix mit dem konfigurierten RLOC registriert.

Locator

Definiert den RLOC mit dem die importierten EID-Präfixe beim Map-Server registriert werden. Mögliche Werte sind benannte Gegenstellen, IPv6-WAN-Interfaces, oder Loopback-Interfaces.

SNMP-ID:

2.93.4.10.4

Pfad Telnet:

Setup > **Routing-Protokolle** > **LISP** > **Redistribution**

Mögliche Werte:

max. 39 Zeichen aus `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Priority

Die Priorität.

SNMP-ID:

2.93.4.10.6

Pfad Telnet:

Setup > **Routing-Protokolle** > **LISP** > **Redistribution**

Mögliche Werte:

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

Default-Wert:

1

Weight

Das Gewicht des EID-Mappings.

SNMP-ID:

2.93.4.2.8

Pfad Telnet:

Setup > **Routing-Protokolle** > **LISP** > **EID-Mapping**

Mögliche Werte:

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

Default-Wert:

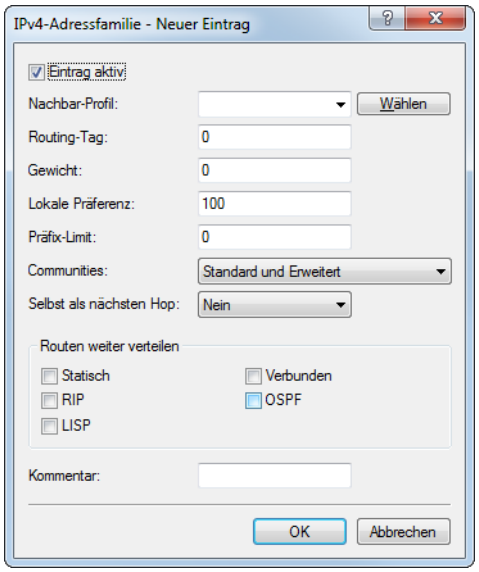
100

3.3 Routen-Redistribution von LISP- und RIP-Routen im BGP

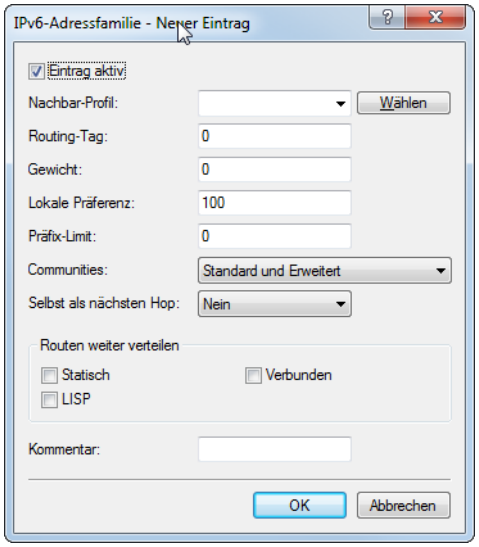
Durch Routen-Redistribution können LISP- und RIP-Routen ab LCOS-Version 10.20 nach BGP weiterverteilt werden. Hierzu werden die Routen mit entsprechendem Typ aus der Routing-Tabelle ausgelesen und durch BGP weiterverteilt.

Die Weiterverteilung von RIP-Routen wird nur für IPv4-Routen unterstützt.

Es gibt für diese Features zwei neue Schalter. Diese sind zu finden in LANconfig unter **Routing Protokolle** > **BGP** > **IPv4-Adressfamilie**



bzw. **Routing Protokolle** > **BGP** > **IPv6-Adressfamilie**.



Bei Auswahl der Option LISP verteilt das Gerät LISP-Routen aus der Routing-Tabelle an die BGP-Nachbarn. Bei Auswahl der Option RIP verteilt das Gerät RIP-Routen aus der Routing-Tabelle an die BGP-Nachbarn.

3.3.1 Ergänzungen im Setup-Menü

Route-Weiterverteilen

Bestimmt, ob das Gerät bestimmte Routen an BGP-Nachbarn dieses Profils weiterleiten soll.

Wenn keine Option ausgewählt ist, verteilt das Gerät keine Routen an die BGP-Nachbarn dieses Nachbar-Profils (Default-Einstellung).

SNMP-ID:

2.93.1.4.1.9

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Adressfamilie** > **IPv4**

Mögliche Werte:

Statisch

Das Gerät verteilt statische Routen aus der Routing-Tabelle an die BGP-Nachbarn.

Verbunden

Das Gerät verteilt Routen von direkt angeschlossenen Netzwerken an die BGP-Nachbarn.

RIP

Das Gerät verteilt RIP-Routen aus der Routing-Tabelle an die BGP-Nachbarn.

OSPF

Das Gerät verteilt OSPF-Routen aus der Routing-Tabelle an die BGP-Nachbarn.

LISP

Das Gerät verteilt LISP-Routen aus der Routing-Tabelle an die BGP-Nachbarn.

Route-Weiterverteilen

Bestimmt, ob das Gerät bestimmte Routen an BGP-Nachbarn dieses Profils weiterleiten soll.

Wenn keine Option ausgewählt ist, verteilt das Gerät keine Routen an die BGP-Nachbarn dieses Nachbar-Profils (Default-Einstellung).

SNMP-ID:

2.93.1.4.2.9

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Adressfamilie** > **IPv6**

Mögliche Werte:

Statisch

Das Gerät verteilt statische Routen aus der Routing-Tabelle an die BGP-Nachbarn.

Verbunden

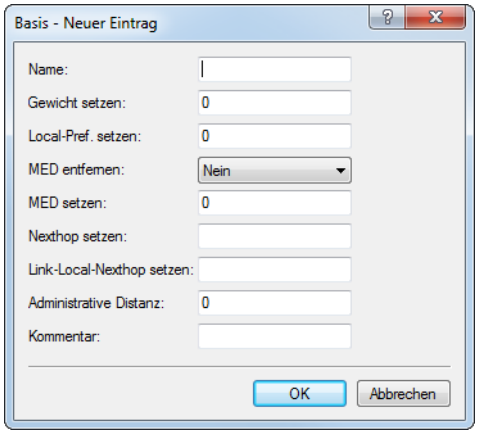
Das Gerät verteilt Routen von direkt angeschlossenen Netzwerken an die BGP-Nachbarn.

LISP

Das Gerät verteilt LISP-Routen aus der Routing-Tabelle an die BGP-Nachbarn.

3.4 BGP: Setzen der administrativen Distanz per Policy

Der Parameter **Administrative Distanz** unter **Routing-Protokolle** > **BGP** > **BGP-Regelwerk** > **Basis** definiert, mit welcher „Administrativen Distanz" empfangene Präfixe im BGP in die Routing-Tabelle eingetragen werden sollen.



Die Liste der fest definierten „Administrativen Distanzen" der verschiedenen Systemdienste bzw. Routing-Protokolle können auf der Kommandozeile per `show admin-distance` angezeigt werden.

3.4.1 Ergänzungen im Setup-Menü

Admin-Distanz-Setzen

Dieser Parameter definiert, mit welcher „Administrativen Distanz" empfangene Präfixe im BGP in die Routing-Tabelle eingetragen werden sollen. Die Liste der fest definierten „Administrativen Distanzen" der verschiedenen Systemdienste bzw. Routing-Protokolle können auf der CLI per show admin-distance angezeigt werden.

SNMP-ID:

2.93.1.5.2.1.9

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Regelwerk** > **Anpassungen** > **Basis**

Mögliche Werte:

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

3.5 DSLoL für WLAN-Router

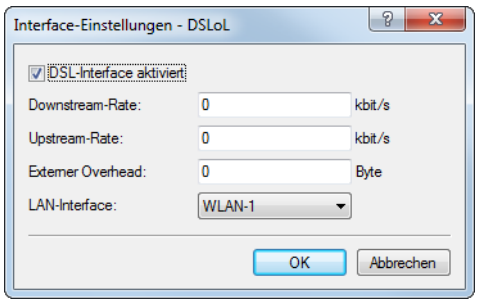
Eine IPv4-Maskierung („NAT") ist nur über eine WAN-Verbindung möglich. Wenn man in Richtung eines LAN- oder WLAN-Interface maskieren will, dann muss das entsprechende LAN- oder WLAN-Interface als DSL-Port deklariert werden, so dass dieser für den Aufbau einer WAN-Verbindung (typischerweise IPoE oder DHCPoE) verwendet werden kann.

Dies war bis LCOS 10.12 nur für Access Points möglich. Ab LCOS 10.20 ist DSLoL auch für WLAN-Router verfügbar.

Ein exemplarisches Szenario für DSLoL:

Ein WLAN-Router soll verwendet werden, um eine Internetverbindung primär über WLAN herzustellen. Dazu wird der WLAN-Clientmodus verwendet. Ist das WLAN nicht verfügbar, soll stattdessen als Backup die Internetverbindung über

LTE hergestellt werden. Hierzu wird ganz regulär eine LTE-Verbindung konfiguriert; sowie unter Zuhilfenahme von DSLoL über das WLAN-Interface eine weitere Internetverbindung über WLAN. Dazu in LANconfig unter **Schnittstellen** > **WAN** > **Interface-Einstellungen** > **DSLoL** die Option **DSL-Interface aktiviert** auswählen und diesem Interface das vorher als WLAN-Client eingerichtete WLAN als **LAN-Interface** zuweisen.



Nun kann die LTE-Verbindung als Backup für die WLAN / DSLoL-Internetverbindung konfiguriert werden.

4 IPv6

4.1 IPv6-WAN-Interface

Die Konfigurationslogik der IPv6-WAN-Interfaces wurde geändert. Es gibt jetzt unter **IPv6** > **Allgemein** > **WAN-Schnittstellen** einen DEFAULT-Eintrag. Dieser wird automatisch bei jeder Gegenstelle ausgewählt, wenn man keinen anderen Eintrag anlegt und bei der Gegenstelle auswählt. Dazu gibt es in der Konfiguration bei allen Gegenstellen einen neuen Parameter **IPv6**, mit dem die IPv6-WAN-Schnittstelle ausgewählt werden kann. Ein leerer Eintrag schaltet IPv6 für dieses Interface ab.

Ein Eintrag in der Tabelle WAN-Schnittstellen kann von Gegenstellen mehrfach referenziert werden.

4.1.1 Ergänzungen im Setup-Menü

IPv6

Dieser Eintrag gibt den Namen der IPv6-WAN-Schnittstelle an. Ein leerer Eintrag schaltet IPv6 für dieses Interface ab.

SNMP-ID:

2.2.2.8

Pfad Telnet:

Setup > **WAN** > **Einwahl-Gegenstellen**

Mögliche Werte:

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

Default-Wert:

DEFAULT

IPv6

Dieser Eintrag gibt den Namen der IPv6-WAN-Schnittstelle an. Ein leerer Eintrag schaltet IPv6 für dieses Interface ab.

SNMP-ID:

2.2.19.19

Pfad Telnet:

Setup > **WAN** > **DSL-Breitband-Gegenstellen**

Mögliche Werte:

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

Default-Wert:

DEFAULT

IPv6

Dieser Eintrag gibt den Namen der IPv6-WAN-Schnittstelle an. Ein leerer Eintrag schaltet IPv6 für dieses Interface ab.

SNMP-ID:

2.2.21.9

Pfad Telnet:

Setup > **WAN** > **PPTP-Gegenstellen**

Mögliche Werte:

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

Default-Wert:

DEFAULT

IPv6

Dieser Eintrag gibt den Namen der IPv6-WAN-Schnittstelle an. Ein leerer Eintrag schaltet IPv6 für dieses Interface ab.

SNMP-ID:

2.2.37.5

Pfad Telnet:

Setup > **WAN** > **L2TP-Gegenstellen**

Mögliche Werte:

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

Default-Wert:

DEFAULT

IPv6

Dieser Eintrag gibt den Namen der IPv6-WAN-Schnittstelle an. Ein leerer Eintrag schaltet IPv6 für dieses Interface ab.

SNMP-ID:

2.2.51.11

Pfad Telnet:

Setup > **WAN** > **GRE-Tunnel**

Mögliche Werte:

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

Default-Wert:

DEFAULT

IPv6

Dieser Eintrag gibt den Namen der IPv6-WAN-Schnittstelle an. Ein leerer Eintrag schaltet IPv6 für dieses Interface ab.

SNMP-ID:

2.19.9.20

Pfad Telnet:

Setup > **VPN** > **VPN-Gegenstellen**

Mögliche Werte:

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

Default-Wert:

DEFAULT

IPv6

Dieser Eintrag gibt den Namen der IPv6-WAN-Schnittstelle an. Ein leerer Eintrag schaltet IPv6 für dieses Interface ab.

SNMP-ID:

2.19.36.1.21

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **Gegenstellen**

Mögliche Werte:

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

Default-Wert:

DEFAULT

Interface-Name

Vergeben Sie hier einen Namen für das IPv6-WAN-Interface. Dieser Name wird bei der Gegenstelle angegeben. Voreingestellt ist ein Default-Eintrag. Dieser wird automatisch ausgewählt, wenn bei der Gegenstelle keine explizite Angabe erfolgt. Ein leerer Eintrag schaltet IPv6 für dieses Interface ab.

Ein Eintrag in der Tabelle WAN-Schnittstellen kann von Gegenstellen mehrfach referenziert werden.

SNMP-ID:

2.70.7.1

Pfad Telnet:

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

Mögliche Werte:

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

Default-Wert:

DEFAULT

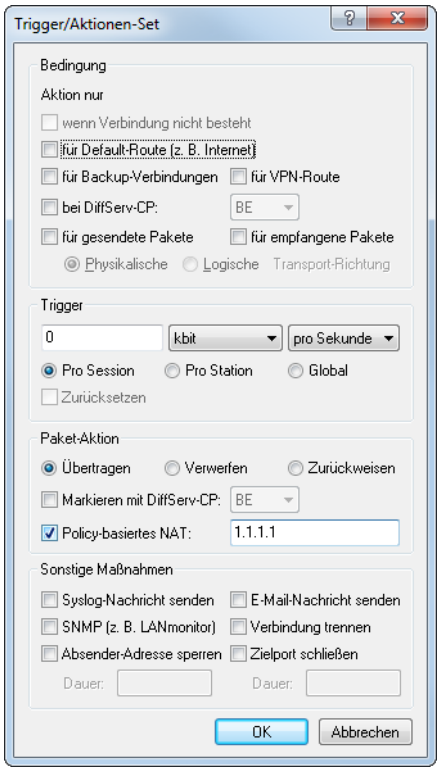
5 Firewall

5.1 WAN Policy-Based NAT

Ab LCOS-Version 10.20 ist es möglich WAN Policy-Based NAT zu verwenden.

WAN Policy-Based NAT ermöglicht die Adressumsetzung (Maskierung) von Verbindungen basierend auf Firewall-Regeln. Es kann konfiguriert werden, hinter welcher vom Provider zugewiesenen WAN-IPv4-Adresse interne Adressen umgesetzt (maskiert) werden sollen. Ideal für Szenarien, in denen der Provider mehrere statische IPv4-Adressen zugewiesen hat, z. B. für den Betrieb von Mailservern und Webservern mit verschiedenen WAN-Adressen.

In der Firewall gibt es dazu die neue Paket-Option **Policy-basiertes NAT** unter **Firewall/QoS** > **IPv4-Regeln** > **Aktions-Objekte**. Diese Aktion ist zusammen mit der Option **Übertragen** verwendbar und ermöglicht das maskieren bzw. NAT hinter eine definierten IPv4-Adresse.



Der Parameter muss als feste IP-Adresse eingetragen werden. Dynamische IP-Adressen werden nicht unterstützt.

NAT ist nur möglich, falls eine WAN-Schnittstelle beteiligt ist. NAT zwischen zwei LAN-Schnittstellen wird nicht unterstützt.

Auf der Konsole (`/Setup/IP-Router/Firewall/Aktions-Tabelle`) kann dazu die Variable `%Y` als Aktion verwendet werden.

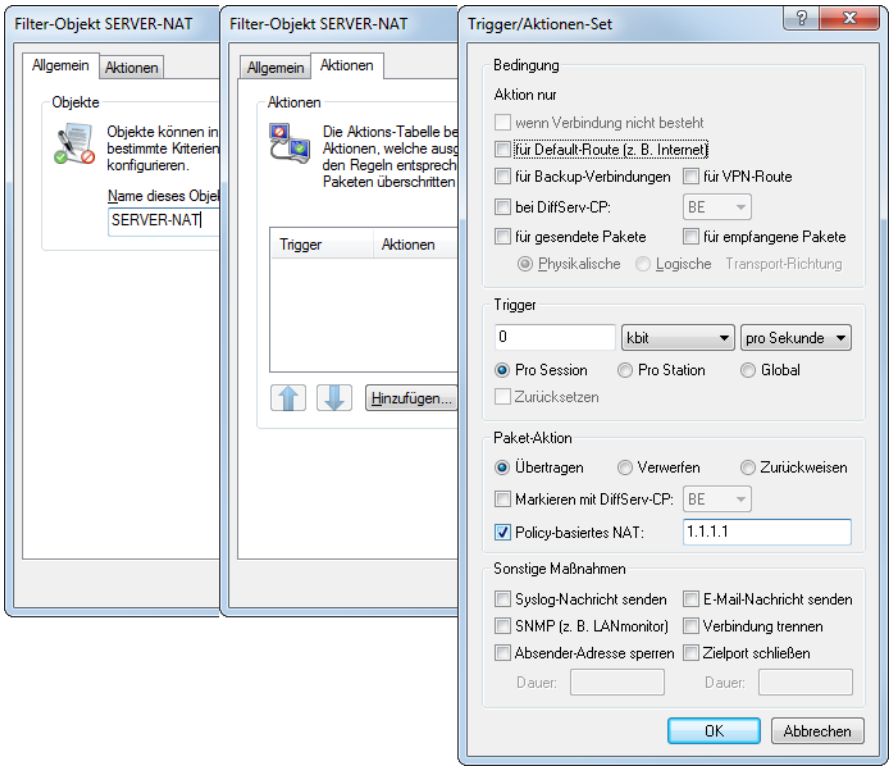
5.1.1 Konfiguration eines Policy-basierten NATs mit Firewall-Regeln

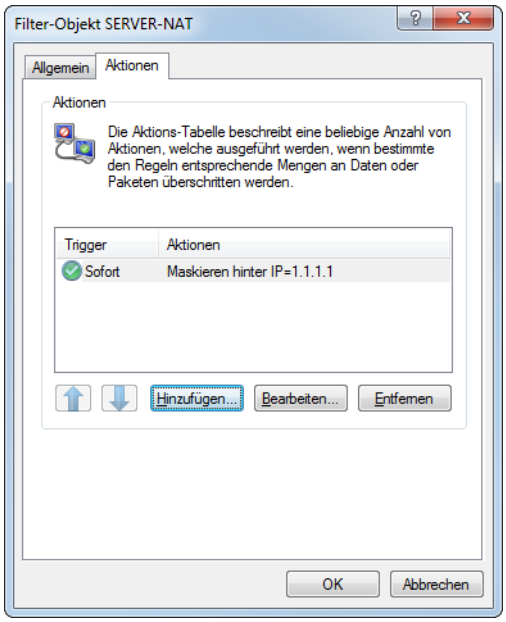
In dem folgenden Beispiel ist ein IPv4-Netzwerk (Intranet) mit Subnetz 192.168.80.0/24 konfiguriert. Der Internetprovider hat mehrere öffentliche IP-Adressen zugewiesen. Der Internetzugang ist mit dem Setup-Assistenten eingerichtet worden. Die Clients aus dem Intranet werden automatisch hinter der öffentlichen IP-Adresse, die mit dem Assistenten angelegt wurde, maskiert.

Aus diesem Netzwerk soll nun ein Server mit der internen IP-Adresse 192.168.80.21 hinter der öffentlichen IP-Adresse 1.1.1.1 maskiert werden.

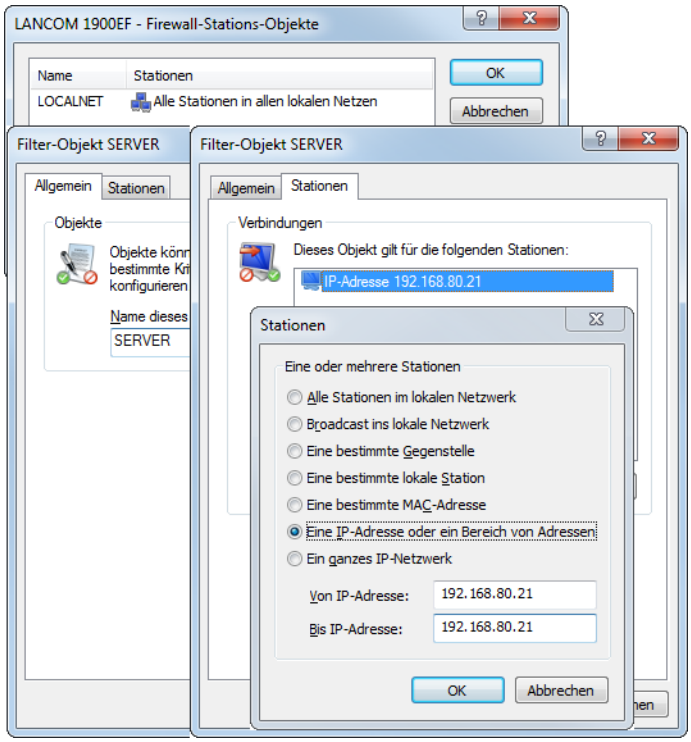
Die „Rückwärtsrichtung" der Maskierung bzw. Erreichbarkeit des Servers von außen, wird über einen Portforwarding-Eintrag realisiert, der nicht Teil dieses Beispiels ist.

1. Legen Sie unter **Firewall/QoS** > **IPv4-Regeln** > **Aktions-Objekte** ein neues Firewall-Aktionsobjekt an. Setzen Sie unter Aktion die Paket-Aktion auf **Übertragen** und dann **Policy-basiertes NAT** auf 1.1.1.1.

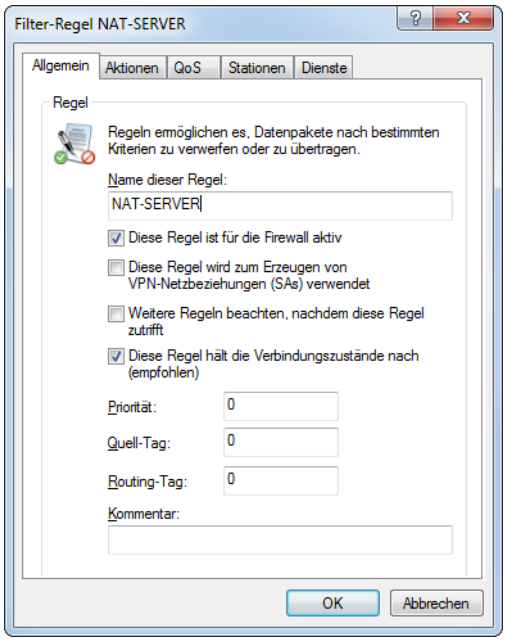




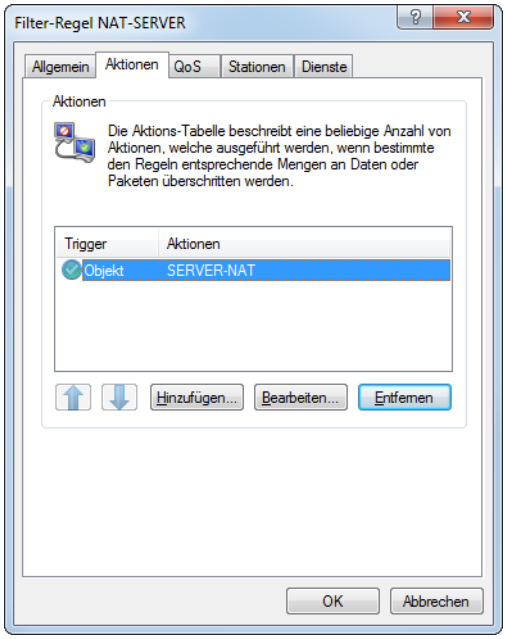
2. Legen Sie unter **Firewall/QoS** > **IPv4-Regeln** > **Stations-Objekte** ein neues Stationsobjekt an, das für die IP-Adresse 192.168.80.21 definiert wird.



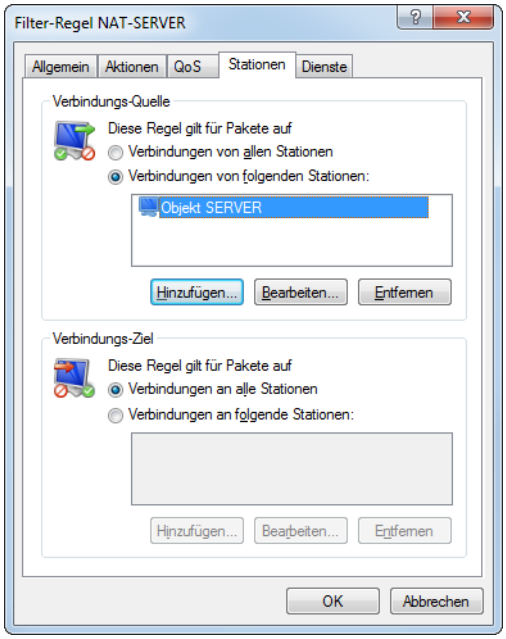
3. Als nächstes legen Sie unter **Firewall/QoS** > **IPv4-Regeln** > **Firewall-Regeln** eine Filter-Regel an.

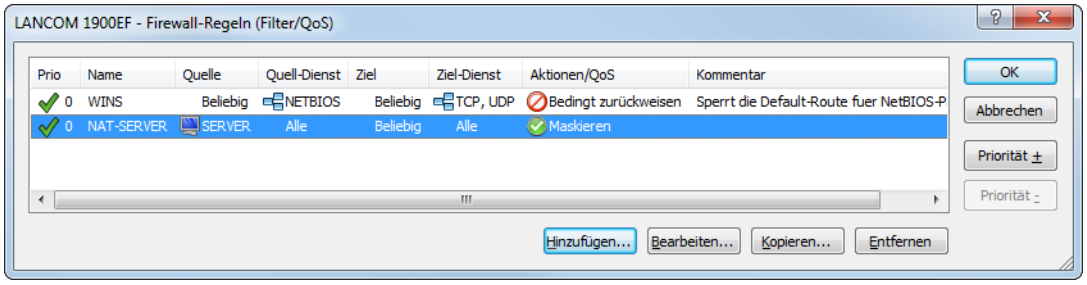


4. In dieser Filter-Regel geben Sie unter **Aktionen** die weiter oben neu definierte Aktion „SERVER-NAT" an.



5. Danach noch in dieser Filter-Regel unter **Stationen** das neu angelegte Stationsobjekt verwenden. Ggfs. können Sie bei Bedarf als **Verbindungsziel** noch die Internetleitung angeben.



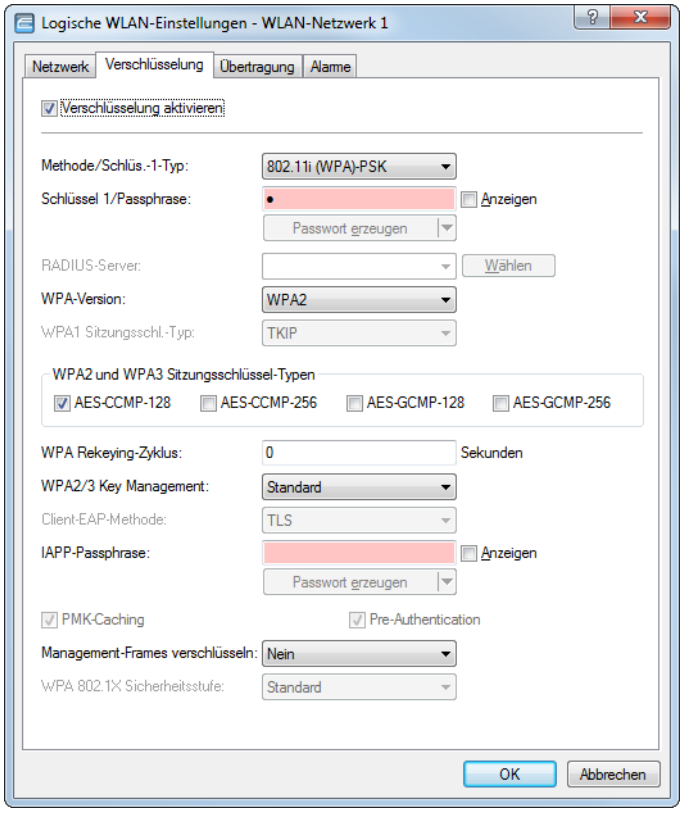


6 Wireless LAN – WLAN

6.1 Verschiebung der WLAN-Verschlüsselungseinstellungen in die logischen WLAN-Einstellungen

Zur Vereinfachung der Konfiguration befinden sich die WLAN-Verschlüsselungseinstellungen nun als zusätzlicher Reiter im Dialog zur Konfiguration der logischen WLAN-Einstellungen. Bei der Konfiguration einer SSID entfällt somit nun das aufwändige Wechseln zwischen dem Dialog der logischen WLAN-Einstellungen und dem Dialog der WLAN-Verschlüsselungseinstellungen.

Die logischen WLAN-Einstellungen finden Sie unter **Wireless-LAN** > **Allgemein** > **Interfaces** > **Logische WLAN-Einstellungen**.

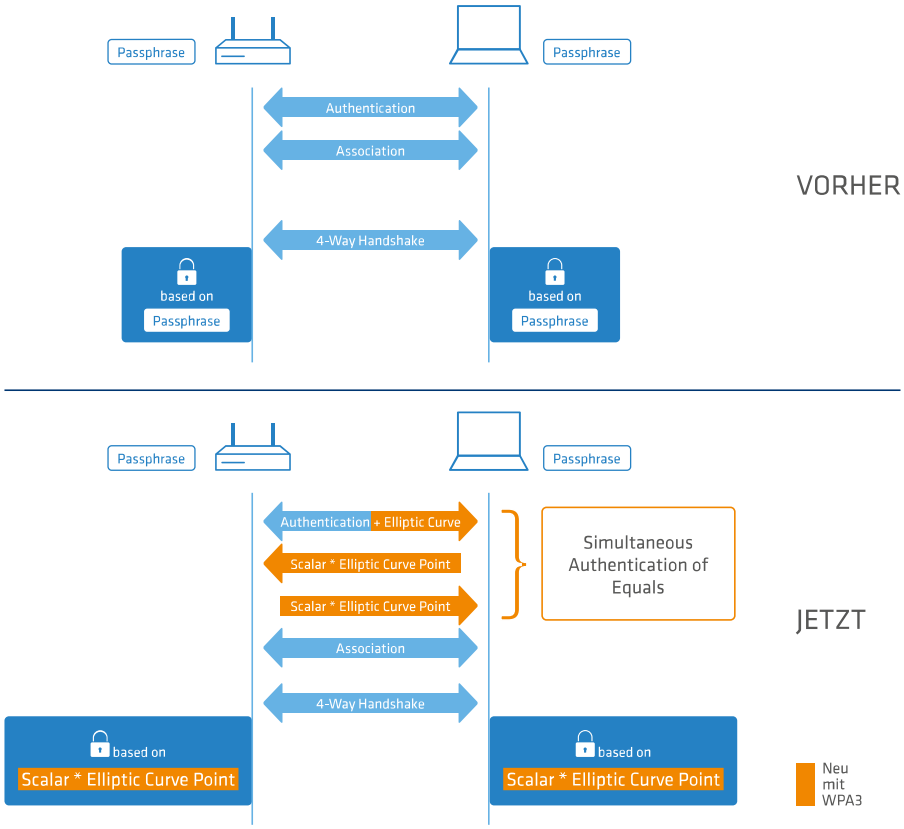


6.2 WPA3 (Wi-Fi Protected Access 3)

Der 2018 eingeführte WPA3-Standard der Wi-Fi-Alliance bietet gegenüber dem bereits 2004 eingeführten Vorgängerstandard WPA2 eine verbesserte Sicherheit durch eine Kombination verschiedener aktueller Sicherheitsverfahren. Wie WPA2 existiert auch WPA3 in den Ausprägungen WPA3-Personal und WPA3-Enterprise.

WPA3-Personal bietet durch die Verwendung des Authentisierungsverfahrens Simultaneous Authentication of Equals (SAE) eine Methode, die lediglich ein Passwort für die Authentifizierung voraussetzt und dennoch Brute-Force- und

Wörterbuch-Attacken ins Leere laufen lässt. Zudem bietet dieses Verfahren erstmalig Forward Secrecy – dies bedeutet, dass in der Vergangenheit mitgeschnittener, WPA3-gesicherter Datenverkehr auch später nicht mehr entschlüsselt werden kann, wenn der Angreifer Kenntnis des Pre-Shared Keys erlangt.



Zusätzlich kann bei WPA3-Enterprise die Unterstützung für CNSA Suite B-Kryptographie eingeschaltet werden, welche ein optionaler Teil von WPA3-Enterprise für Hochsicherheitsumgebungen ist. Suite B stellt sicher, dass alle Glieder in der Verschlüsselungskette aufeinander abgestimmt sind. Suite B bildet Klassen von Bitlängen für Hash-, symmetrische und asymmetrische Verschlüsselungsverfahren, die passende Schutzniveaus bieten. So passt zum Beispiel zu AES mit 128 Bit ein SHA-2-Hash mit 256 Bit. Wenn Suite B zum Einsatz kommt, ist die Unterstützung aller anderen Kombinationen ausdrücklich ausgeschlossen. In der Verschlüsselungskette gibt es folglich nur noch gleich starke Glieder.

In beiden Varianten ist nun die Verwendung von Protected Management Frames (PMF) nach IEEE 802.11w verpflichtend. PMF verhindern, dass Angreifer durch Deassoziieren mittels gefälschter Management Frames und Belauschen der Wiederanmeldung Material bekommen, um das WLAN-Passwort zu errechnen.

6.2.1 WPA3-Personal

In den WLAN-Verschlüsselungseinstellungen unter **Wireless-LAN** > **Allgemein** > **Interfaces** > **Logische WLAN-Einstellungen**. können nun die neuen WPA-Versionen **WPA3** und **WPA2/3** ausgewählt werden.

Bei Auswahl von **WPA3** können sich nur noch WLAN-Clients anmelden, die WPA3-Personal unterstützen; die Authentisierung wird mit dieser Konfiguration nur noch über Simultaneous Authentication of Equals (SAE) zugelassen. Ebenfalls wird für diese SSID nun die Verwendung von PMF (Protected Management Frames nach 802.11w; verpflichtender Bestandteil von WPA3) erzwungen.

Bei Auswahl von **WPA2/3** werden diese beiden WPA-Versionen parallel angeboten. Diese Auswahl ermöglicht den Mischbetrieb von WLAN-Clients, die nur WPA2 unterstützen mit WLAN-Clients, die bereits WPA3 unterstützen. Für WPA3-kompatible WLAN-Clients wird in dieser Konfiguration die Verwendung von PMF erzwungen; für WPA2-kompatible WLAN-Clients wird PMF aus Gründen der Abwärtskompatibilität optional angeboten.

6.2.2 WPA3-Enterprise

WPA3-Enterprise ändert oder ersetzt die in WPA2-Enterprise definierten Protokolle nicht grundlegend. Stattdessen definiert es Richtlinien, um eine größere Konsistenz bei der Anwendung dieser Protokolle zu gewährleisten und die gewünschte Sicherheit zu gewährleisten.

In den WLAN-Verschlüsselungseinstellungen unter **Wireless-LAN** > **Allgemein** > **Interfaces** > **Logische WLAN-Einstellungen**. können nun die neuen WPA-Versionen **WPA3** und **WPA2/3** ausgewählt werden.

Bei Auswahl von **WPA3** können sich nur noch WLAN-Clients anmelden, die WPA3-Enterprise unterstützen. Für diese SSID wird die Verwendung von PMF (Protected Management Frames nach 802.11w; verpflichtender Bestandteil von WPA3) erzwungen.

Bei Auswahl von **WPA2/3** werden diese beiden WPA-Versionen parallel angeboten. Diese Auswahl ermöglicht den Mischbetrieb von WLAN-Clients, die nur WPA2 unterstützen mit WLAN-Clients, die bereits WPA3 unterstützen. Für WPA3-kompatible WLAN-Clients wird in dieser Konfiguration die Verwendung von PMF erzwungen; für WPA2-kompatible WLAN-Clients wird PMF aus Gründen der Abwärtskompatibilität optional angeboten.

Suite B-Kryptographie

Zusätzlich kann die Unterstützung für CNSA Suite B-Kryptographie eingeschaltet werden, welche ein optionaler Teil von WPA3-Enterprise für Hochsicherheitsumgebungen ist. Suite B stellt sicher, dass alle Glieder in der Verschlüsselungskette aufeinander abgestimmt sind. Suite B bildet Klassen von Bitlängen für Hash-, symmetrische und asymmetrische Verschlüsselungsverfahren, die passende Schutzniveaus bieten. So passt zum Beispiel zu AES mit 128 Bit ein SHA-2-Hash mit 256 Bit. Wenn Suite B zum Einsatz kommt, ist die Unterstützung aller anderen Kombinationen ausdrücklich ausgeschlossen. In der Verschlüsselungskette gibt es folglich nur noch gleich starke Glieder.

Weitere Informationen zu CNSA Suite B finden Sie unter folgendem Link: *CNSA Algorithm Suite Factsheet*

Mit dem Schalter **WPA 802.1X Sicherheitsstufe** unter **Wireless-LAN** > **Allgemein** > **Interfaces** > **Logische WLAN-Einstellungen** kann die Suite B-Kryptographie optional eingeschaltet werden. Wird die Unterstützung für „Suite B 192 Bits“ eingeschaltet, werden die folgenden EAP Cipher-Suiten erzwungen:

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

Andere Cipher-Suiten können nicht verwendet werden. Ebenfalls wird eine Mindest-Schlüssellänge von 3072 Bit für die RSA- und Diffie-Hellman-Schlüsselaustauschverfahren, sowie 384 Bit für die ECDSA- und ECDHE-Schlüsselaustauschverfahren erzwungen. Zusätzlich wird der Sitzungschlüssel-Typ AES-GCMP-256 erzwungen.

Werden diese Cipher-Suiten von den verwendeten WLAN-Clients oder der restlichen Infrastruktur (z. B. RADIUS-Server) nicht unterstützt, dann ist keine Verbindung möglich!

Wird die Unterstützung für „Suite B 128 Bits“ eingeschaltet, werden die folgenden EAP Cipher-Suiten erzwungen:

- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

Andere Cipher-Suiten können nicht verwendet werden. Ebenfalls wird eine Mindest-Schlüssellänge von 3072 Bit für die RSA- und Diffie-Hellman-Schlüsselaustauschverfahren, sowie 384 Bit für die ECDSA- und ECDHE-Schlüsselaustauschverfahren erzwungen. Zusätzlich wird der Sitzungschlüssel-Typ AES-GCMP-128 erzwungen.

Da die Sitzunggschlüssel-Typen AES-GCMP-128 und AES-GCMP-256 nicht von allen WLAN-Modulen unterstützt werden, kann die Verwendung der Suite B-Kryptographie je nach Gerätetyp eingeschränkt oder nicht möglich sein.

Werden diese Cipher-Suiten von den verwendeten WLAN-Clients oder der restlichen Infrastruktur (z. B. RADIUS-Server) nicht unterstützt, dann ist keine Verbindung möglich!

6.2.3 WPA3-Gerätesupport

In der folgenden Tabelle sehen Sie, welche Access Points und WLAN-Router WPA3-Personal, WPA3-Enterprise und WPA3-Enterprise inkl. Suite B / 192-bit-Encryption unterstützen. Wenn ein zweites WLAN-Modul vorhanden ist, dann wird dies für beide Module separat angegeben.

AP-Modell	WLAN-1	WLAN-2
LN-170x	> WPA3-Personal > WPA3-Enterprise inkl. Suite B	> WPA3-Personal > WPA3-Enterprise inkl. Suite B
LN-86x	> WPA3-Personal > WPA3-Enterprise inkl. Suite B	> WPA3-Personal > WPA3-Enterprise inkl. Suite B
LN-830(E) / L-822	> WPA3-Personal > WPA3-Enterprise inkl. Suite B	> WPA3-Personal > WPA3-Enterprise
LN-630	> WPA3-Personal > WPA3-Enterprise inkl. Suite B	> WPA3-Personal > WPA3-Enterprise
L-330 / L-322 / L-321 / L-151	> WPA3-Personal > WPA3-Enterprise inkl. Suite B	> WPA3-Personal > WPA3-Enterprise inkl. Suite B
OAP-821 / IAP-821	> WPA3-Personal > WPA3-Enterprise	> WPA3-Personal > WPA3-Enterprise
OAP-822 / OAP-830 / IAP-822	> WPA3-Personal > WPA3-Enterprise	> WPA3-Personal > WPA3-Enterprise
1780EW-4G+	> WPA3-Personal > WPA3-Enterprise	keine zweite WLAN-Schnittstelle verbaut
Alle anderen WLAN-Router	> WPA3-Personal > WPA3-Enterprise inkl. Suite B	keine zweite WLAN-Schnittstelle verbaut

6.2.4 Ergänzungen im Setup-Menü

WPA-Version

Mit dieser WPA-Version werden die Daten in diesem logischen WLAN verschlüsselt.

SNMP-ID:

2.23.20.3.9

Pfad Telnet:

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

Mögliche Werte:

WPA1
WPA2
WPA1/2
WPA2/3
WPA3
WPA1/2/3

Default-Wert:

WPA2

SAE-Gruppen

Das Authentisierungsverfahrens SAE (Simultaneous Authentication of Equals) verwendet elliptische Kurven. Mehr Informationen hierzu bekommt man bei der *Standards for Efficient Cryptography Group*.

SNMP-ID:

2.23.20.3.26

Pfad Telnet:

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

Mögliche Werte:

secp256r1
secp384r1
secp521r1
secp192r1
secp224r1

Default-Wert:

secp256r1

secp384r1

secp521r1

WPA2-3-Sitzungsschluessel

Ab LCOS 10.20 löst diese Einstellung den Wert 2.23.20.3.13 **WPA2-Sitzungsschluessel** ab.

Wählen Sie hier die Verfahren aus, welche zur Generierung der WPA-Sitzungs- bzw. -Gruppen-Schlüssel angeboten werden sollen. Es können die folgenden Verfahren des Advanced Encryption Standard (AES) angeboten werden.

SNMP-ID:

2.23.20.3.27

Pfad Telnet:

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

Mögliche Werte:

AES-CCMP-128
AES-CCMP-256
AES-GCMP-128
AES-GCMP-256

Default-Wert:

AES-CCMP-128

WPA-802.1X-Security-Level

Einstellung der 802.1X-Sicherheitsstufe. Bei Verwendung von WPA3-Enterprise kann die Unterstützung für CNSA Suite B-Kryptographie eingeschaltet werden, welche ein optionaler Teil von WPA3-Enterprise für Hochsicherheitsumgebungen ist.

Bei Verwendung von CNSA Suite B-Kryptographie können nur die angegebenen Cipher-Suiten verwendet werden. Ebenfalls wird eine Mindest-Schlüssellänge von 3072 Bit für die RSA- und Diffie-Hellman-Schlüsselaustauschverfahren, sowie 384 Bit für die ECDSA- und ECDHE-Schlüsselaustauschverfahren erzwungen. Zusätzlich wird der Sitzungschlüssel-Typ AES-GCMP-128 bei „Suite B 128 Bits“ erzwungen.

Werden diese Cipher-Suiten von den verwendeten WLAN-Clients oder der restlichen Infrastruktur (z. B. RADIUS-Server) nicht unterstützt, dann ist keine Verbindung möglich!

SNMP-ID:

2.23.20.3.28

Pfad Telnet:

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

Mögliche Werte:

Standard
Suite-B-128-Bit

Aktiviert „Suite B 128 Bits“. Die folgenden EAP Cipher-Suiten werden erzwungen:

- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

Suite-B-192-Bit

Aktiviert „Suite B 192 Bits“. Die folgenden EAP Cipher-Suiten werden erzwungen:

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

Default-Wert:

Standard

6.3 Enhanced Open

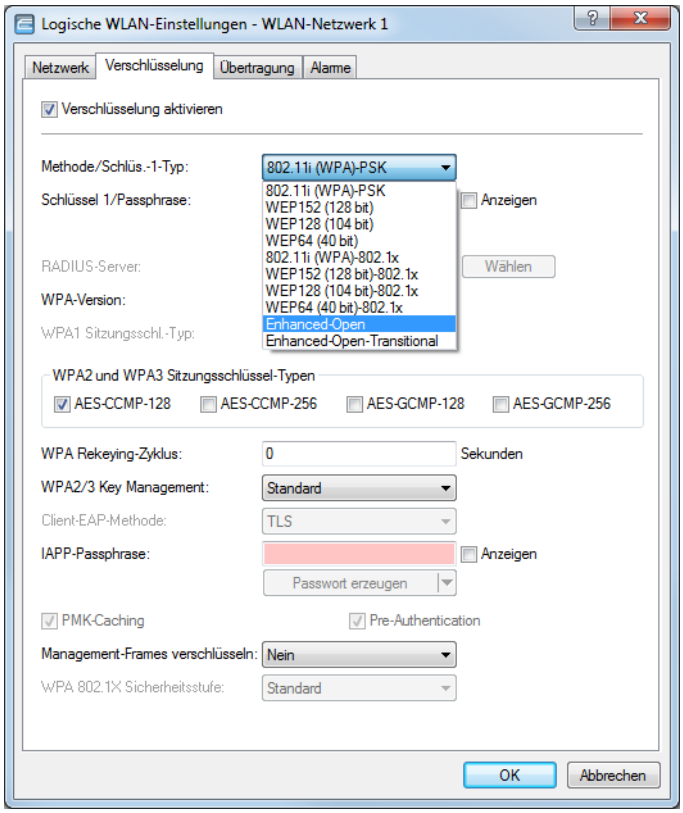
Hotspots werden bisher hauptsächlich unverschlüsselt betrieben, wodurch auf der Funkschnittstelle keinerlei Vertraulichkeit der übertragenen Daten gegeben ist. Auch die verbreitete Praxis, einen Hotspot mit WPA2-PSK abzusichern und den gemeinsamen Schlüssel etwa durch einen Aushang bekannt zu machen, bietet nur eingeschränkte Sicherheit – Da WPA2-PSK keine Perfect Forward Secrecy bietet, kann ein Angreifer, dem dieser Schlüssel bekannt ist, nachträglich damit abgesicherten Datenverkehr entschlüsseln. Das Enhanced Open-Verfahren kann verwendet werden, um diese Risiken zu minimieren. Es bietet verschlüsselte Kommunikation für alle Clients, die dieses Verfahren unterstützen, so dass nicht jeder in der gleichen Funkzelle alles einfach mitlesen kann. Es bleibt das Risiko einer Man-in-the-Middle-Attacke, aber im Vergleich zu einem unverschlüsselten offenen Hotspot ist es ein deutlich geringeres Risiko.

Public Spot mit Enhanced Open

Zur Verwendung von Enhanced Open bei Public Spot siehe auch *Einrichtung eines sicheren Hotspots mit Enhanced Open*.

Konfiguration

Enhanced Open kann in den WLAN-Verschlüsselungseinstellungen unter **Wireless-LAN** > **Allgemein** > **Interfaces** > **Logische WLAN-Einstellungen** als Verschlüsselungsmethode eingestellt werden. Mehr ist nicht notwendig, um die Kommunikation mit Clients, dieses Verfahren unterstützen, zu verschlüsseln.



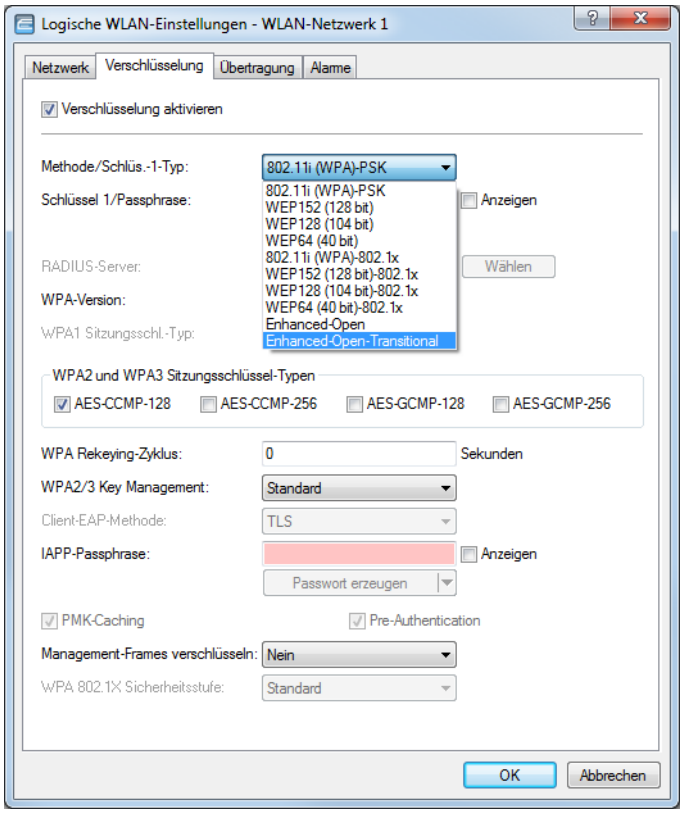
6.3.1 Enhanced Open Transitional Mode

Der Enhanced Open Transitional Mode kann verwendet werden, um gleichzeitig Clients anzubinden, die bereits Enhanced Open unterstützen, sowie solche, die noch nicht Enhanced Open unterstützen. Wird der Transitional Mode konfiguriert, wird zusätzlich zu der regulären Enhanced Open-SSID automatisch parallel eine unverschlüsselte / offene SSID mit gleichem Namen und identischen sonstigen Einstellungen aktiviert.

Hierfür ist es erforderlich, dass auf dem gewählten Radio-Modul noch mindestens eine weitere SSID zu diesem Zeitpunkt unbelegt / nicht in Nutzung ist. Je nach Gerät stehen je Radio-Modul insgesamt 15 oder 16 SSIDs zur Verfügung. Steht keine SSID zur Verfügung, wird sowohl die offene Transitional-SSID, als auch die eigentliche Enhanced Open-SSID nicht aktiviert.

Konfiguration

Der Enhanced Open Transitional Mode kann in den WLAN-Verschlüsselungseinstellungen unter **Wireless-LAN** > **Allgemein** > **Interfaces** > **Logische WLAN-Einstellungen** als Verschlüsselungsmethode eingestellt werden.



6.3.2 Ergänzungen im Setup-Menü

Methode

Wählt das Verschlüsselungs-Verfahren bzw. bei WEP die Schlüssellänge aus, die bei der Verschlüsselung von Datenpaketen auf dem Wireless LAN verwendet wird.

Beachten Sie, dass nicht jedes Verschlüsselungs-Verfahren von jeder Wireless-Karte unterstützt wird.

SNMP-ID:

2.23.20.3.4

Pfad Telnet:

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

Mögliche Werte:

802.11i-WPA-PSK
WEP-128-Bits
WEP-104-Bits
WEP-40-Bits
802.11i-WPA-802.1X
WEP-128-Bits-802.1X
WEP-104-Bits-802.1X
WEP-40-Bits-802.1X
Enhanced-Open
Enhanced-Open-Transitional

Default-Wert:

802.11i-WPA-PSK

Enhanced-Open-Gruppen

Das Authentisierungsverfahrens Enhanced Open verwendet elliptische Kurven.

SNMP-ID:

2.23.20.3.22

Pfad Telnet:

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

Mögliche Werte:

secp256r1
secp384r1
secp521r1

Default-Wert:

secp256r1

secp384r1

secp521r1

6.4 LANCOM Enhanced Passphrase Security (LEPS)

Mit dem Verschlüsselungsverfahren WPA2 wird der Datenverkehr im WLAN gegen unerwünschte „Lauschangriffe" geschützt. Die Verwendung einer Passphrase als zentraler Schlüssel ist dabei sehr einfach zu handhaben, ein RADIUS-Server wie in 802.1X-Installationen wird nicht benötigt.

Dennoch birgt die Verwendung des abhörsicheren Verfahrens WPA2 einige Schwachstellen:

- Eine Passphrase gilt **global** für **alle** WLAN-Clients

- Die Passphrase kann durch Unachtsamkeit ggf. an Unbefugte weitergegeben werden
- Mit der „durchgesickerten" Passphrase kann jeder Angreifer in das Funknetzwerk eindringen

In der Praxis bedeutet das: Falls die Passphrase „verloren geht" oder ein Mitarbeiter mit Kenntnis der Passphrase das Unternehmen verlässt, müsste aus Sicherheitsaspekten die Passphrase im Access Point geändert werden – und damit auch in allen WLAN-Clients. Da das nicht immer sichergestellt werden kann, würde sich also ein Verfahren anbieten, bei dem nicht eine globale Passphrase für alle WLAN-Clients gemeinsam gilt, sondern für jeden Benutzer im WLAN eine eigene Passphrase konfiguriert werden kann. In diesem Fall muss z. B. beim Ausscheiden eines Mitarbeiters aus dem Unternehmen nur seine „persönliche" Passphrase gelöscht werden, alle anderen behalten ihre Gültigkeit und Vertraulichkeit.

Mit LEPS hat LANCOM Systems GmbH zwei effiziente Verfahren entwickelt, welche die einfache Konfigurierbarkeit von IEEE 802.11i mit Passphrase nutzen und dabei die möglichen Unsicherheiten bei der Nutzung einer globalen Passphrase vermeiden.

Mit LEPS-U (LANCOM Enhanced Passphrase Security User) vergeben Sie einzelnen Clients oder ganzen Gruppen ein individuelles WLAN-Passwort für eine SSID. Über LEPS-MAC (LANCOM Enhanced Passphrase Security MAC) authentifizieren Sie die Clients noch zusätzlich anhand ihrer MAC-Adresse – ideal für sichere Unternehmensnetzwerke!

6.4.1 LANCOM Enhanced Passphrase Security User (LEPS-U)

Mit LANCOM Enhanced Passphrase Security User (LEPS-U) kann eine Menge von Passphrasen konfiguriert werden, die dann den einzelnen Benutzern oder Gruppen zugeordnet werden können. Somit gibt es nicht eine globale Passphrase für eine SSID, sondern mehrere, die dann individuell verteilt werden können.

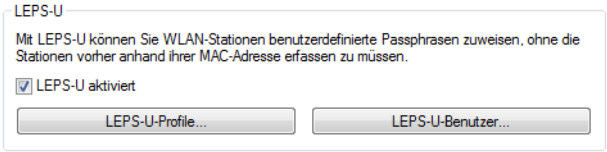
Dies kann für das Onboarding von Geräten in das Netzwerk genutzt werden. Wenn ein Netzwerk-Betreiber z. B. mehrere WLAN-Geräte in verschiedene Bereiche seines Netzwerks „onboarden" will, aber die Geräte nicht selber konfigurieren will, da dies die Benutzer der Geräte selber erledigen sollen. In diesem Fall erhalten die Benutzer lediglich einen Preshared Key für das Firmen-WLAN ausgehändigt, welchen die Benutzer selber für ihre Geräte verwenden können. Je nach Preshared Key werden die Benutzer automatisch durch Zuordnung zu einem VLAN einem bestimmten Netzwerk zugewiesen. Da LEPS-U ausschließlich auf der Infrastrukturseite konfiguriert wird, ist jederzeit die volle Kompatibilität zu Fremdprodukten gegeben.

Die Unsicherheit von globalen Passphrasen wird durch LEPS-U grundsätzlich behoben. Jedem Benutzer wird hierbei seine eigene individuelle Passphrase zugewiesen. Falls eine einem Benutzer zugeordnete Passphrase „verloren geht" oder ein Mitarbeiter mit Kenntnis seiner Passphrase das Unternehmen verlässt, dann muss nur die Passphrase dieses Benutzers geändert bzw. gelöscht werden. Alle anderen Passphrasen behalten ihre Gültigkeit und Vertraulichkeit.

Aus technischen Gründen ist LEPS-U nur mit der WPA-Version WPA2 kompatibel.

Konfiguration

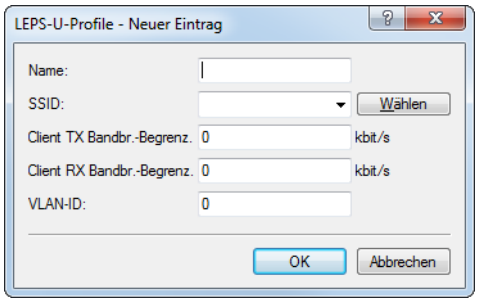
Die Konfiguration der **LEPS-U-Profile** und **LEPS-U-Benutzer** finden Sie in LANconfig unter **Wireless-LAN** > **Stationen/LEPS** > **LEPS-U**. Über den Schalter **LEPS-U aktiviert** wird LEPS-U eingeschaltet.



Bei der Konfiguration von LEPS-U wird jedem Benutzer, der sich mit Clients im WLAN anmelden können soll, eine individuelle Passphrase zugeordnet. Dazu werden LEPS-U-Profile angelegt, damit einige Einstellungen nicht bei jedem Benutzer erneut vorgenommen werden müssen. Anschließend legen Sie die LEPS-U-Benutzer mit der zugehörigen individuellen Passphrase an und verknüpfen diesen mit einem der vorher angelegten LEPS-U-Profile.

LEPS-U-Profile

Konfigurieren Sie hier LEPS-U-Profile und verbinden Sie sie mit einer SSID. Anschließend können die LEPS-U-Profile den LEPS-U-Benutzern zugeordnet werden.



Name

Vergeben Sie hier einen eindeutigen Namen für das LEPS-U-Profil.

SSID

Wählen Sie hier die SSID bzw. beim WLC das logische WLAN-Netzwerk aus, für die das LEPS-U-Profil gültig sein soll. Es können sich nur LEPS-U-Benutzer an der SSID bzw. beim WLC an dem logischen WLAN-Netzwerk anmelden, mit der sie über das LEPS-U-Profil verbunden sind.

Client TX Bandbr.-Begrenz.

Hier können Sie eine Sende-Bandbreiten-Begrenzung in kbit/s für die sich einbuchenden WLAN-Clients einstellen.

Client RX Bandbr.-Begrenz.

Hier können Sie eine Empfangs-Bandbreiten-Begrenzung in kbit/s für die sich einbuchenden WLAN-Clients einstellen.

VLAN-ID

Hier können Sie festlegen, welcher VLAN-ID ein LEPS-U-Benutzer, der mit diesem Profil verbunden ist, zugewiesen wird.

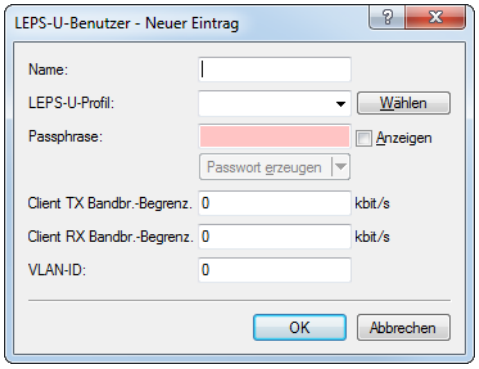
LEPS-U-Benutzer

Legen Sie hier einzelne LEPS-U-Benutzer an. Jeder LEPS-U-Benutzer muss mit einem zuvor angelegten Profil verbunden werden und eine individuelle WPA-Passphrase zugewiesen bekommen. Mit dieser Passphrase kann sich dann ein beliebiger Client an der SSID anmelden, für die der Benutzereintrag durch die Verknüpfung des Profils gültig ist. Der Benutzer wird anhand der verwendeten Passphrase identifiziert und dem in dieser Tabelle konfigurierten VLAN zugewiesen. Wird hier kein VLAN zugewiesen, wird er dem am Profil konfigurierten VLAN zugewiesen. Einstellungen am einzelnen Benutzer haben somit Priorität gegenüber Einstellungen am Profil.

Es gibt plattformspezifische Beschränkungen bei der Anzahl der gleichzeitig angelegten LEPS-U-Benutzer.

Gerät	Benutzer
L-15x, L-3xx, OAP-32x, OAP-8xx, IAP-32x, IAP-82x, LN-630acn	› pro SSID bis zu 300 Benutzer › Access Point gesamt: 2.000 Benutzer
L-45x, L(N)-8xx, L-13xx, LN-17xx	› pro SSID bis zu 1.000 Benutzer

Gerät	Benutzer
	> Access Point gesamt: 6.000 Benutzer



Name

Vergeben Sie hier einen eindeutigen Namen für den LEPS-U-Benutzer.

LEPS-U-Profil

Wählen Sie hier das Profil aus, für das der LEPS-U-Benutzer gültig sein soll. Es können sich nur LEPS-U-Benutzer an der SSID anmelden, mit der sie über das LEPS-U-Profil verbunden sind.

Passphrase

Vergeben Sie hier die Passphrase, mit der der LEPS-U-Benutzer sich am WLAN anmelden soll.

Als Passphrase können Zeichenketten mit 8 bis 64 Zeichen verwendet werden. Wir empfehlen als Passphrasen zufällige Zeichenketten von mindestens 32 Zeichen Länge.

Client TX Bandbr.-Begrenz.

Hier können Sie eine Sende-Bandbreiten-Begrenzung in kbit/s für die sich einbuchenden WLAN-Clients einstellen. Wird hier keine Begrenzung konfiguriert, gilt eine eventuelle, im LEPS-U-Profil konfigurierte Begrenzung. Wird sowohl im LEPS-U-Profil als auch am LEPS-U-Benutzer eine Begrenzung konfiguriert, gilt die am LEPS-U-Benutzer konfigurierte Begrenzung.

Client RX Bandbr.-Begrenz.

Hier können Sie eine Empfangs-Bandbreiten-Begrenzung in kbit/s für die sich einbuchenden WLAN-Clients einstellen. Wird hier keine Begrenzung konfiguriert, gilt eine eventuelle, im LEPS-U-Profil konfigurierte Begrenzung. Wird sowohl im LEPS-U-Profil als auch am LEPS-U-Benutzer eine Begrenzung konfiguriert, gilt die am LEPS-U-Benutzer konfigurierte Begrenzung.

VLAN-ID

Hier können Sie festlegen, welcher VLAN-ID der LEPS-U-Benutzer zugewiesen wird. Wird hier keine VLAN-ID konfiguriert, gilt eine eventuelle, im LEPS-U-Profil konfigurierte VLAN-ID. Wird sowohl im LEPS-U-Profil als auch am LEPS-U-Benutzer eine VLAN-ID konfiguriert, gilt die am LEPS-U-Benutzer konfigurierte VLAN-ID.

6.4.2 LANCOM Enhanced Passphrase Security MAC (LEPS-MAC)

Bei LEPS-MAC wird jeder MAC-Adresse in einer zusätzlichen Spalte der ACL (Access Control List) eine **individuelle** Passphrase zugeordnet – eine beliebige Folge aus 8 bis 63 ASCII-Zeichen. Nur die Verbindung von Passphrase und MAC-Adresse erlaubt die Anmeldung am Access Point.

Da Passphrase und MAC-Adresse verknüpft sind, ist auch das Spoofing der MAC-Adressen wirkungslos – LEPS-MAC schließt damit auch einen möglichen Angriffspunkt gegen die ACL aus. Wenn als Verschlüsselungsart WPA2 verwendet wird, kann zwar die MAC-Adresse abgehört werden – die Passphrase wird bei diesem Verfahren jedoch nie über die

WLAN-Strecke übertragen. Angriffe auf das WLAN werden so deutlich erschwert, da durch die Verknüpfung von MAC-Adresse und Passphrase immer beide Teile bekannt sein müssen, um eine Verschlüsselung zu verhandeln.

LEPS-MAC kann sowohl lokal im Gerät genutzt werden als auch mit Hilfe eines RADIUS-Servers zentral verwaltet werden. LEPS-MAC funktioniert mit sämtlichen am Markt befindlichen WLAN-Client-Adaptern, ohne dass dort eine Änderung stattfinden muss. Da LEPS-MAC ausschließlich im Access Point konfiguriert wird, ist jederzeit die volle Kompatibilität zu Fremdprodukten gegeben.

Im Vergleich zu LEPS-U ist der Verwaltungsaufwand etwas höher, da für jedes Gerät die MAC-Adresse eingetragen werden muss.

Konfiguration

Bei der Konfiguration von LEPS-MAC wird jeder MAC-Adresse eines im WLAN zugelassenen Clients eine eigene Passphrase zugeordnet. Dies kann entweder als Eintrag in der Liste unter **Wireless-LAN** > **Stationen/LEPS** > **LEPS-MAC** > **Stationsregeln** oder im RADIUS-Server geschehen. Pro MAC-Adresse wird ein Eintrag erzeugt – im Sinne des RADIUS-Servers ist die jeweilige MAC-Adresse also ein Benutzer. Zusätzlich muss unter **Wireless-LAN** > **Allgemein** > **Interfaces** > **Logische WLAN-Einstellungen** der MAC-Filter aktiviert sein, d. h., die Daten von den hier eingetragenen WLAN-Clients werden übertragen.

Als Passphrase können Zeichenketten mit 8 bis 64 Zeichen verwendet werden. Wir empfehlen als Passphrasen zufällige Zeichenketten von mindestens 32 Zeichen Länge.

Bei Speicherung der client-spezifischen Passphrasen in der Benutzertabelle eines RADIUS-Servers kann auch ein LAN-gebundenes Gerät als zentraler RADIUS-Server dienen und die Vorteile von LEPS-MAC nutzen.

6.4.3 Ergänzungen im Setup-Menü

LEPS-U

Mit LANCOM Enhanced Passphrase Security User (LEPS-U) können Sie WLAN-Stationen benutzerdefinierte Passphrasen zuweisen, ohne die Stationen vorher anhand ihrer MAC-Adresse erfassen zu müssen.

SNMP-ID:

2.12.133

Pfad Telnet:

Setup > **WLAN**

Aktiv

Schaltet LEPS-U ein oder aus. Im ausgeschalteten Zustand werden die angelegten LEPS-U-Benutzer bei der Anmeldung von WLAN-Clients nicht beachtet.

SNMP-ID:

2.12.133.1

Pfad Telnet:

Setup > **WLAN** > **LEPS-U**

Mögliche Werte:

Nein
Ja

Default-Wert:

Nein

Profile

Konfigurieren Sie hier LEPS-U-Profile und verbinden Sie sie mit einer SSID. Anschließend können die LEPS-U-Profile den LEPS-U-Benutzern zugeordnet werden. Dabei können Sie für einen Benutzer die Profilwerte durch individuelle Werte überschreiben.

SNMP-ID:

2.12.133.2

Pfad Telnet:

Setup > **WLAN** > **LEPS-U**

Name

Vergeben Sie hier einen eindeutigen Namen für das LEPS-U-Profil.

SNMP-ID:

2.12.133.2.1

Pfad Telnet:

Setup > **WLAN** > **LEPS-U** > **Profile**

Mögliche Werte:

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

Netzwerkname

Wählen Sie hier die SSID bzw. beim WLC das logische WLAN-Netzwerk aus, für die das LEPS-U-Profil gültig sein soll. Es können sich nur LEPS-U-Benutzer an der SSID bzw. beim WLC an dem logischen WLAN-Netzwerk anmelden, mit der sie über das LEPS-U-Profil verbunden sind.

SNMP-ID:

2.12.133.2.2

Pfad Telnet:

Setup > **WLAN** > **LEPS-U** > **Profile**

Mögliche Werte:

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

Pro-Client-Tx-Limit

Hier können Sie eine Sende-Bandbreiten-Begrenzung in kbit/s für die sich einbuchenden WLAN-Clients einstellen.

SNMP-ID:

2.12.133.2.3

Pfad Telnet:

Setup > **WLAN** > **LEPS-U** > **Profile**

Mögliche Werte:

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

Besondere Werte:

0

Keine Begrenzung.

Pro-Client-Rx-Limit

Hier können Sie eine Empfangs-Bandbreiten-Begrenzung in kbit/s für die sich einbuchenden WLAN-Clients einstellen.

SNMP-ID:

2.12.133.2.4

Pfad Telnet:

Setup > **WLAN** > **LEPS-U** > **Profile**

Mögliche Werte:

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

Besondere Werte:

0

Keine Begrenzung.

VLAN-Id

Hier können Sie festlegen, welcher VLAN-ID ein LEPS-U-Benutzer, der mit diesem Profil verbunden ist, zugewiesen wird.

SNMP-ID:

2.12.133.2.5

Pfad Telnet:

Setup > **WLAN** > **LEPS-U** > **Profile**

Mögliche Werte:

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

Benutzer

Legen Sie hier einzelne LEPS-U-Benutzer an. Jeder LEPS-U-Benutzer muss mit einem zuvor angelegten Profil verbunden werden.

SNMP-ID:

2.12.133.3

Pfad Telnet:

Setup > **WLAN** > **LEPS-U**

Name

Vergeben Sie hier einen eindeutigen Namen für den LEPS-U-Benutzer.

SNMP-ID:

2.12.133.3.1

Pfad Telnet:

Setup > **WLAN** > **LEPS-U** > **Benutzer**

Mögliche Werte:

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

Profil

Wählen Sie hier das Profil aus, für das der LEPS-U-Benutzer gültig sein soll. Es können sich nur LEPS-U-Benutzer an der SSID anmelden, mit der sie über das LEPS-U-Profil verbunden sind.

SNMP-ID:

2.12.133.3.2

Pfad Telnet:

Setup > **WLAN** > **LEPS-U** > **Benutzer**

Mögliche Werte:

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

WPA-Passphrase

Vergeben Sie hier die Passphrase, mit der der LEPS-U-Benutzer sich am WLAN anmelden soll.

SNMP-ID:

2.12.133.3.3

Pfad Telnet:

Setup > **WLAN** > **LEPS-U** > **Benutzer**

Mögliche Werte:

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

Pro-Client-Tx-Limit

Hier können Sie eine Sende-Bandbreiten-Begrenzung in kbit/s für die sich einbuchenden WLAN-Clients einstellen. Wird hier keine Begrenzung konfiguriert, gilt eine eventuelle, im LEPS-U-Profil konfigurierte Begrenzung. Wird sowohl im LEPS-U-Profil als auch am LEPS-U-Benutzer eine Begrenzung konfiguriert, gilt die am LEPS-U-Benutzer konfigurierte Begrenzung.

SNMP-ID:

2.12.133.3.4

Pfad Telnet:

Setup > **WLAN** > **LEPS-U** > **Benutzer**

Mögliche Werte:

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

Besondere Werte:

0

Keine Begrenzung.

Pro-Client-Rx-Limit

Hier können Sie eine Empfangs-Bandbreiten-Begrenzung in kbit/s für die sich einbuchenden WLAN-Clients einstellen. Wird hier keine Begrenzung konfiguriert, gilt eine eventuelle, im LEPS-U-Profil konfigurierte Begrenzung. Wird sowohl im LEPS-U-Profil als auch am LEPS-U-Benutzer eine Begrenzung konfiguriert, gilt die am LEPS-U-Benutzer konfigurierte Begrenzung.

SNMP-ID:

2.12.133.3.5

Pfad Telnet:

Setup > **WLAN** > **LEPS-U** > **Benutzer**

Mögliche Werte:

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

Besondere Werte:

0

Keine Begrenzung.

VLAN-Id

Hier können Sie festlegen, welcher VLAN-ID der LEPS-U-Benutzer zugewiesen wird. Wird hier keine VLAN-ID konfiguriert, gilt eine eventuelle, im LEPS-U-Profil konfigurierte VLAN-ID. Wird sowohl im LEPS-U-Profil als auch am LEPS-U-Benutzer eine VLAN-ID konfiguriert, gilt die am LEPS-U-Benutzer konfigurierte VLAN-ID.

SNMP-ID:

2.12.133.3.6

Pfad Telnet:

Setup > **WLAN** > **LEPS-U** > **Benutzer**

Mögliche Werte:

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

LEPS-U

Mit LANCOM Enhanced Passphrase Security User (LEPS-U) können Sie WLAN-Stationen benutzerdefinierte Passphrasen zuweisen, ohne die Stationen vorher anhand ihrer MAC-Adresse erfassen zu müssen.

SNMP-ID:

2.37.1.25

Pfad Telnet:

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

Profile

Konfigurieren Sie hier LEPS-U-Profile und verbinden Sie sie mit einer SSID. Anschließend können die LEPS-U-Profile den LEPS-U-Benutzern zugeordnet werden. Dabei können Sie für einen Benutzer die Profilwerte durch individuelle Werte überschreiben.

SNMP-ID:

2.37.1.25.1

Pfad Telnet:

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

Name

Vergeben Sie hier einen eindeutigen Namen für das LEPS-U-Profil.

SNMP-ID:

2.37.1.25.1.1

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **LEPS-U** > **Profile**

Mögliche Werte:

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

Netzwerkprofil

Wählen Sie hier die SSID bzw. beim WLC das logische WLAN-Netzwerk aus, für die das LEPS-U-Profil gültig sein soll. Es können sich nur LEPS-U-Benutzer an der SSID bzw. beim WLC an dem logischen WLAN-Netzwerk anmelden, mit der sie über das LEPS-U-Profil verbunden sind.

SNMP-ID:

2.37.1.25.1.2

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **LEPS-U** > **Profile**

Mögliche Werte:

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

Pro-Client-Tx-Limit

Hier können Sie eine Sende-Bandbreiten-Begrenzung in kbit/s für die sich einbuchenden WLAN-Clients einstellen.

SNMP-ID:

2.37.1.25.1.3

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **LEPS-U** > **Profile**

Mögliche Werte:

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

Besondere Werte:

0

Keine Begrenzung.

Pro-Client-Rx-Limit

Hier können Sie eine Empfangs-Bandbreiten-Begrenzung in kbit/s für die sich einbuchenden WLAN-Clients einstellen.

SNMP-ID:

2.37.1.25.1.4

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **LEPS-U** > **Profile**

Mögliche Werte:

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

Besondere Werte:

0

Keine Begrenzung.

VLAN-Id

Hier können Sie festlegen, welcher VLAN-ID ein LEPS-U-Benutzer, der mit diesem Profil verbunden ist, zugewiesen wird.

SNMP-ID:

2.37.1.25.1.5

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **LEPS-U** > **Profile**

Mögliche Werte:

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

Benutzer

Legen Sie hier einzelne LEPS-U-Benutzer an. Jeder LEPS-U-Benutzer muss mit einem zuvor angelegten Profil verbunden werden.

SNMP-ID:

2.37.1.25.2

Pfad Telnet:

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

Name

Vergeben Sie hier einen eindeutigen Namen für den LEPS-U-Benutzer.

SNMP-ID:

2.37.1.25.2.1

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **LEPS-U** > **Benutzer**

Mögliche Werte:

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

Profil

Wählen Sie hier das Profil aus, für das der LEPS-U-Benutzer gültig sein soll. Es können sich nur LEPS-U-Benutzer an der SSID anmelden, mit der sie über das LEPS-U-Profil verbunden sind.

SNMP-ID:

2.37.1.25.2.2

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **LEPS-U** > **Benutzer**

Mögliche Werte:

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

WPA-Passphrase

Vergeben Sie hier die Passphrase, mit der der LEPS-U-Benutzer sich am WLAN anmelden soll.

SNMP-ID:

2.37.1.25.2.3

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **LEPS-U** > **Benutzer**

Mögliche Werte:

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

Pro-Client-Tx-Limit

Hier können Sie eine Sende-Bandbreiten-Begrenzung in kbit/s für die sich einbuchenden WLAN-Clients einstellen. Wird hier keine Begrenzung konfiguriert, gilt eine eventuelle, im LEPS-U-Profil konfigurierte Begrenzung. Wird sowohl im LEPS-U-Profil als auch am LEPS-U-Benutzer eine Begrenzung konfiguriert, gilt die am LEPS-U-Benutzer konfigurierte Begrenzung.

SNMP-ID:

2.37.1.25.2.4

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **LEPS-U** > **Benutzer**

Mögliche Werte:

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

Besondere Werte:

0

Keine Begrenzung.

Pro-Client-Rx-Limit

Hier können Sie eine Empfangs-Bandbreiten-Begrenzung in kbit/s für die sich einbuchenden WLAN-Clients einstellen. Wird hier keine Begrenzung konfiguriert, gilt eine eventuelle, im LEPS-U-Profil konfigurierte Begrenzung. Wird sowohl im LEPS-U-Profil als auch am LEPS-U-Benutzer eine Begrenzung konfiguriert, gilt die am LEPS-U-Benutzer konfigurierte Begrenzung.

SNMP-ID:

2.37.1.25.2.5

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **LEPS-U** > **Benutzer**

Mögliche Werte:

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

Besondere Werte:

0

Keine Begrenzung.

VLAN-Id

Hier können Sie festlegen, welcher VLAN-ID der LEPS-U-Benutzer zugewiesen wird. Wird hier keine VLAN-ID konfiguriert, gilt eine eventuelle, im LEPS-U-Profil konfigurierte VLAN-ID. Wird sowohl im LEPS-U-Profil als auch am LEPS-U-Benutzer eine VLAN-ID konfiguriert, gilt die am LEPS-U-Benutzer konfigurierte VLAN-ID.

SNMP-ID:

2.37.1.25.2.6

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **LEPS-U** > **Benutzer**

Mögliche Werte:

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

6.5 Client Management

Mit Client Management werden WLAN-Clients stets auf den für sie idealen Access Point sowie das beste Frequenzband gesteuert. Dieses Feature steigert somit die Qualität drahtloser Netzwerke jeder Größenordnung - egal ob im stand-alone-Betrieb oder orchestriert über die LANCOM Management Cloud. Die beliebten, aber bislang getrennten Funktionen Band Steering und Client Steering werden hiermit kombiniert und auch ohne den Betrieb mit einem WLAN-Controller bereitgestellt.

Im Vergleich zum bisherigen WLC-gestützten Client Steering funktioniert Client Management autark und ohne WLC. die Access Points kommunizieren dazu untereinander mittels des Protokolls IAPP.

Damit die Kommunikation der Access Points untereinander funktioniert, ist es erforderlich, dass alle Access Points IAPP-Nachrichten austauschen können. IAPP-Nachrichten werden als Multicast übertragen. Gegebenenfalls sind

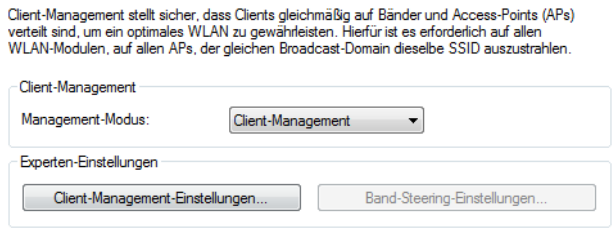
auf Infrastrukturseite, insbesondere auf Switches, passende Ausnahmeregelungen im IGMP-Snooping oder anderen Filtermechanismen zu schaffen. IAPP verwendet die Multicast-Gruppe 224.0.1.76.

LANCOM Switches in der Defaulteinstellung sind bereits korrekt für das Client Management eingestellt.

Client Management stellt somit sicher, dass Clients gleichmäßig auf Frequenzbänder und Access Points verteilt sind, um ein optimales WLAN zu gewährleisten. Hierfür ist es erforderlich, dass sowohl auf allen WLAN-Modulen als auch auf allen Access Points der gleichen Broadcast-Domäne dieselbe SSID ausgestrahlt wird.

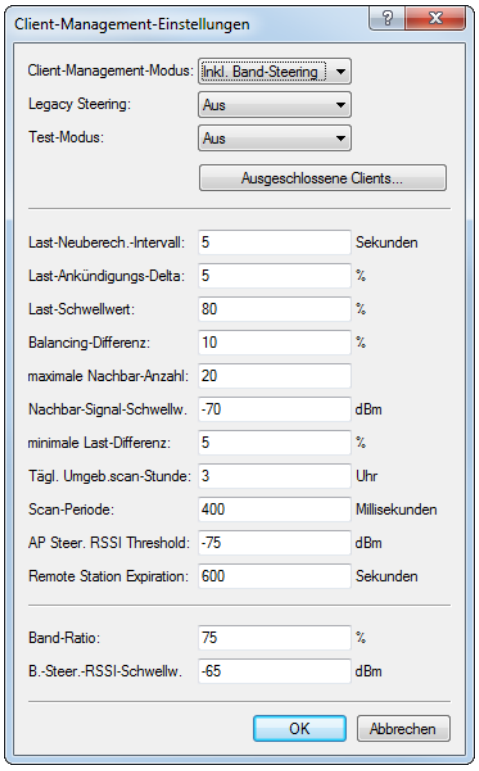
6.5.1 Konfiguration des Client Managements

Das Client Management können Sie unter **Wireless-LAN** > **Client-Management** > **Client-Management** > **Management-Modus** ein- bzw. ausschalten. Auf Neuinstallationen ist es per Voreinstellung eingeschaltet und benötigt normalerweise keine besonderen Einstellungen. Bei einem Access Point mit mehreren WLAN-Modulen kann alternativ auch das **AP-basierte Band-Steering** aktiviert werden.



Experten-Einstellungen

Konfigurieren Sie unter **Wireless-LAN** > **Client-Management** > **Experten-Einstellungen** > **Client-Management** die Einstellungen des Client Managements. Mit den Voreinstellungen funktioniert das Client Management optimal in Büro- und Schulumgebungen.



Client-Management-Modus

Bei Access Point mit mehreren WLAN-Modulen kann das Client Management mit und ohne Band Steering durchgeführt werden.

Standardeinstellung: inkl. Band Steering

Legacy-Steering

Konfiguriert, ob auch Clients, die 802.11v nicht oder nicht korrekt unterstützen, vom Client Management auf andere Access Points geleitet werden sollen. Auch bei aktivem Legacy-Steering wird das Client Management weiterhin erst 802.11v-fähige Clients auf andere Access Points leiten; erst anschließend werden Clients, die 802.11v nicht unterstützen, geleitet. Legacy-Steering erzwingt das Umleiten dieser Clients durch eine erzwungene Trennung des Clients vom WLAN. Anschließend wird das erneute Einbuchen des Clients am aktuellen AP für eine gewisse Zeit blockiert, damit der Client seibsttätig einen anderen Access Point wählt. Dies kann im Gegensatz zum Leiten der Clients mittels 802.11v zu einer verschlechterten Benutzererfahrung führen. Dies ist vorrangig vom Verhalten der Legacy-Clients abhängig.

Standardeinstellung: Aus

Test-Modus

Betreibt Client-Management im Test-Modus: Umgebungs-Scans werden durchgeführt, Steering-Entscheidungen werden vom System getroffen und im Syslog verzeichnet, aber es findet kein tatsächliches Steering der Clients statt. Verwenden Sie den Test-Modus, um das Verhalten des Client Managements zu prüfen ohne tatsächliche Änderungen an Ihrem Netzwerk durchzuführen.

Standardeinstellung: Aus

Ausgeschlossene Clients

In vielen Umgebungen gibt es spezielle Clients, von denen bekannt ist, dass sie sich nicht gut verhalten. Stellen Sie sich ein Krankenhaus mit kundenspezifischen VoIP-Telefonen vor, die nicht in der Lage sind, Verbindungsabbrüche ordnungsgemäß zu behandeln, und die dazu neigen, sich an einen bestimmten Access Point zu halten. Um nun nicht das Client Management komplett abschalten zu müssen, kann man diese Clients von der Steuerung ausnehmen.

Konfigurieren Sie in der Tabelle die MAC-Adressen der Clients, die von einer Steuerung ausgenommen werden sollen. Als Wildcard-Zeichen kann der `*` verwendet werden, der für beliebige Zeichen steht. Dieses darf aber nicht als einziges Zeichen einer MAC-Adresse verwendet werden. Möglich sind also z. B. `01:23:45:12:34:56`, `01:*:56` oder `01:23:*`.

Last-Neuberechnungs-Intervall

Konfiguriert das Intervall, in dem die Last auf dem AP berechnet wird und Entscheidungen zum Steering der Clients getroffen werden. Erhöhen Sie den Wert, um die Last im Netzwerk zu reduzieren. Verringern Sie den Wert, um schneller eine Neuverteilung der Clients zu erreichen. Werte < 2 Sekunden werden aufgrund von negativen Effekten in der Netzwerk-Laufzeit nicht empfohlen. Werten von > 10 Sekunden werden nicht empfohlen, da das Steering der Clients sonst nicht rechtzeitig erfolgt. Es wird empfohlen, den standardmäßig eingestellten Wert nicht zu ändern.

Standardwert: 5 Sekunden

Last-Ankündigungs-Delta

Konfiguriert, bei welcher prozentualen Änderung der aktuellen Last ein Access Point diese auch außerhalb des regulären Ankündigungs-Intervalls an andere Access Points kommuniziert. Erhöhen Sie den Wert in Installationen mit vielen mobilen Clients. Verringern Sie den Wert in Installationen mit wenig beweglichen Clients. Die Standardeinstellung wurde in Hinblick auf Büro- und Schulumgebungen gewählt. Beachten Sie, dass dieser Wert unterhalb des für die Balancing-Differenz konfigurierten Wertes liegen sollte, um Fehlberechnungen zu vermeiden.

Standardwert: 5 %

Last-Schwellenwert

Konfiguriert den Last-Schwellenwert, ab dem der Access Point unabhängig vom Last-Schwellenwert der Nachbar-Access-Points mit dem Steering beginnt. Erhöhen Sie den Wert in low-quality/high-density-Szenarien wie Stadien. Verringern Sie den Wert in high-quality/high-throughput-Szenarien wie Büro/Schule.

Standardwert: 80 %

Balancing-Differenz

Konfiguriert die Last-Differenz zwischen Access Points, ab der Clients zum weniger belasteten Access Point geleitet werden. Hohe Werte führen zu weniger ausgeglichenen Installationen, niedrige Werte zu mehr Steering der Clients. Erhöhen Sie den Wert, wenn zu viel Client Steering betrieben wird. Verringern Sie den Wert, wenn eine maximal ausgeglichene Installation erforderlich ist. Die Standardeinstellung wurde in Hinblick auf Büro- und Schulumgebungen gewählt.

Standardwert: 10 %

maximale Nachbar-Anzahl

Konfiguriert die Anzahl an Nachbar-Access Points, die vom Client Management auf dem aktuellen Access Point berücksichtigt werden. In High-Density-Szenarien kann eine niedrige Anzahl Vorteile bringen, da Clients so vorrangig auf in der Nähe befindliche Access Points geleitet werden und weniger Management-Kommunikation zwischen den einzelnen Access Points notwendig ist. Werte < 4 werden nicht empfohlen, da so keine ausreichende Anzahl an Access Points für eine sinnvolle Steering-Entscheidung zur Verfügung steht. Werte > 72 werden aufgrund von Limitierungen des 802.11-Protokolls nicht unterstützt.

Standardwert: 20 APs

Nachbar-Signal-Schwellenwert

Konfiguriert die Signalstärke, mit der ein AP gesehen werden muss, um als Nachbar-Access Point eingestuft zu werden. Erhöhen Sie den Wert für High-Density-Szenarien (z. B: -60, -50). Verringern Sie den Wert für Szenarien, in der eine große Abdeckung gefordert ist (z. B. -80,-90).

Standardwert: -70 dBm

minimale Last-Differenz

Konfiguriert die minimale Last-Differenz zwischen benachbarten Access Points, ab der zwischen diesen Access Points ein Steering durchgeführt wird. Das Steering wird nur durchgeführt, wenn der konfigurierte Last-Schwellenwert überschritten wurde. Zur Vermeidung von Fehlberechnung sollte die minimale Last-Differenz die konfigurierte Balancing-Differenz nicht überschreiten. Erhöhen Sie den Wert, um weniger Steering in der Installation zu betreiben. Verringern Sie den Wert, um mehr Steering in der Installation zu betreiben.

Standardwert: 5 %

Täglicher Umgebungsscan zu Stunde

Konfiguriert die Uhrzeit (00-23), zu der täglich der Umgebungs-Scan ausgeführt wird, welcher für das Client Management benötigt wird. Der genaue Zeitpunkt des Scans wird über ein Zeitfenster von 30 Minuten verteilt, um Konflikte zwischen gleichzeitig laufenden Umgebungs-Scans zu minimieren. Der Umgebungs-Scan dauert ca. 15 Sekunden an. Währenddessen können keine WLAN-Daten über das scannende WLAN-Modul übertragen werden.

Standardwert: 3 Uhr

Scan-Periode

Konfiguriert die Laufzeit des Umgebungs-Scans, der zur Identifikation von Nachbar-Access Points dient. Die Scan-Periode sollte das 2- bis 2,5-fache des konfigurierten Beacon-Intervalls betragen; der Standardwert wurde bereits für das Standard-Beacon-Intervall passend gewählt. Dieser Wert ist von 200 ms bis 1000 ms konfigurierbar.

Standardwert: 400 ms

AP Steer. RSSI Threshold

Die Signalstärke, die ein Client auf einem entferntem Access Point haben muss, damit er zu diesem gesteuert wird.

Eine höhere Signalschwelle bewirkt einen niedrigeren Wert potentiell steuerbarer Clients und limitiert somit die Möglichkeiten des Client Managements. Gleichzeitig wäre sie in Umgebungen mit hohen Qualtitätsanforderungen sinnvoll, z. B. bei starker Verwendung von VoIP. Dafür wird eine sehr gute Ausleuchtung und höhere Dichte der Access Points benötigt.

Eine niedrigere Signalschwelle bewirkt einen höheren Wert potentiell steuerbarer Clients, allerdings kann der Algorithmus hierbei auch Clients Access Points mit schlechter Signalqualität zuweisen. Es kann sogar passieren, dass sich Clients weigern, zu einem Access Point mit schlechterer Signalqualität gesteuert zu werden. Es würde in Umgebungen helfen, in denen ein großes Areal abgedeckt werden soll. Werte unterhalb von -80 dBm führen zu einem sehr schlechten Ergebnis, da die Wahrscheinlichkeit steigt, dass Clients sich nicht mit dem Access Point verbinden können, zu dem sie gesteuert werden sollen.

Der Standardwert passt für Büroumgebungen.

Standardwert: -75 dBm

Remote Station Expiration

Zeit, in der ein Access Point sich die Informationen über die Clients eines benachbarten Access Points merkt. Diese Informationen werden zur Beschleunigung der Lenkentscheidungen verwendet. Der Standardwert passt für Büroumgebungen mit einem relativ statischen Aufbau und wenigen sich bewegenden Clients. In Umgebungen mit vielen sich bewegenden oder nur kurzzeitig verbundenen Clients sollte man niedrigere Werte setzen. Zu hohe Werte führen zu Fehlsteuerungen, wenn die Informationen des Caches nicht mehr gültig sind.

Standardwert: 600 Sekunden

Band-Ratio

Konfiguriert die gewünschte Verteilung der Clients zwischen den Radio-Bändern. Das konfigurierte Verhältnis spezifiziert, welcher Anteil an Clients auf das 5 GHz-Band geleitet werden soll.

Standardwert: 75 %

Band-Steering-RSSI-Schwellenwert

Konfiguriert die Signalstärke (RSSI), mit der ein Client auf dem jeweils anderen Radio-Band „gesehen" werden muss, damit er auf dieses Band geleitet wird. Die Standardeinstellung wurde in Hinblick auf Büro-Umgebungen gewählt.

Standardwert: -65 dBm

6.5.2 Ergänzungen im Setup-Menü

Client-Steering

Hier bestimmen Sie die Einstellungen für das Client Management bzw. das WLAN Band Steering der am Access Point angemeldeten WLAN-Clients.

SNMP-ID:

2.12.87

Pfad Telnet:

Setup > **WLAN**

In-Betrieb

Mit dieser Option aktivieren Sie WLAN Band Steering bzw. das Client Management im Access Point. Sollte ein WLC aktiv sein, dann ist diese Funktionalität hier nicht gegeben, da sie vom WLC übernommen wird.

SNMP-ID:

2.12.87.1

Pfad Telnet:

Setup > **WLAN** > **Client-Steering**

Mögliche Werte:

Client-Management

Aktiviert das Client Management im Access Point. Im Folgenden angegebene Prozenteinstellungen beziehen sich auf die maximale Last eines Access Points. Diese ist auf 80 Clients eingestellt und nicht änderbar.

Radioband

Aktiviert das WLAN Band Steering im Access Point.

Nein

Schaltet dieses Feature aus.

Default-Wert:

Nein

Probelauf

Das Client Management führt einen Probelauf durch. Die Scans werden durchgeführt, Entscheidungen werden berechnet und protokolliert, aber nicht ausgeführt.

SNMP-ID:

2.12.87.6

Pfad Telnet:

Setup > **WLAN** > **Client-Steering**

Mögliche Werte:

Nein
Ja

Default-Wert:

Nein

Last-Aktualisierungs-Intervall

Intervall in Sekunden, nach dem die Last des Access Points beim Client Management berechnet wird. Daraus ergibt sich die Entscheidung, ob Clients gesteuert werden sollen. Falls ja, dann findet die Steuerung ebenfalls im Rahmen dieses Intervalls statt.

Ein höherer Wert verringert die Netzwerklast und hat einen beschränkt positiven Effekt in sehr großen Netzen. Ein niedrigerer Wert führt zu einer schnelleren Verteilung der Clients. Allerdings sollte man nicht unter 2 und nicht über 10 Sekunden gehen.

SNMP-ID:

2.12.87.7

Pfad Telnet:

Setup > **WLAN** > **Client-Steering**

Mögliche Werte:

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

Besondere Werte:

0

Dieser Wert deaktiviert die Verzögerung.

Default-Wert:

5

Last-Ankuendigungs-Delta

Falls beim Client Management eine Lastveränderung oberhalb des angegebenen Prozentwerts geschieht, dann wird außerhalb des regulären Intervalls die aktuelle Last an die per Scan bekannten benachbarten Access Points gemeldet. Der Wert sollte erhöht werden, wenn man sich in Umgebungen mit vielen sich bewegenden Geräten befindet. Die Vorgabe von 5 % (4 Clients) ist sinnvoll in Umgebungen mit wenigen sich bewegenden Geräten wie z. B. Büro oder Klassenräume.

SNMP-ID:

2.12.87.8

Pfad Telnet:

Setup > **WLAN** > **Client-Steering**

Mögliche Werte:

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

Default-Wert:

5

Last-Schwellwert

Prozentuale Lastschwelle, ab der beim Client Management ein Access Point versucht, die bei ihm angemeldeten Geräte unabhängig von der Last der benachbarten Access Points zu steuern. In schwierigen Umgebungen mit schlechter Übertragungsqualität bzw. hoher Dichte der angemeldeten Geräte sollten sie den Wert erhöhen. In optimalen Umgebungen

mit hoher Übertragungsqualität und hohem Durchsatz wie Büro- oder Klassenräumen kann die Lastschwelle verringert werden. Der Standardwert liegt mit 80 % (64 Clients) zwischen diesen Extremen.

SNMP-ID:

2.12.87.9

Pfad Telnet:

Setup > **WLAN** > **Client-Steering**

Mögliche Werte:

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

Default-Wert:

80

Ausgleichs-Unterschied

Der prozentuale Lastunterschied beim Client Management zwischen zwei benachbarten Access Points, ab dem der höher belastete Access Point versucht, Clients zum weniger belasteten Access Point zu steuern. Ein hoher Wert führt zu einem unausgeglichenen Szenario während ein niedriger Wert mehr Steuerungsversuche nach sich zieht. Falls zu viele Steuerungsversuche beobachtet werden, dann sollte dieser Wert erhöht werden. Falls man ein möglichst ausgeglichenes Szenario wünscht, dann muss man den Wert verringern. Die Voreinstellung von 10 % (8 Clients) Unterschied sollte für eine Büro- oder Klassenraumumgebung passen.

SNMP-ID:

2.12.87.10

Pfad Telnet:

Setup > **WLAN** > **Client-Steering**

Mögliche Werte:

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

Default-Wert:

10

Maximale-Anzahl-an-Nachbarn

Anzahl der benachbarten Access Points beim Client Management, die bei der Steuerung der Clients sowie beim Informationsaustausch zwischen den Access Points berücksichtigt werden. In High-Density-Umgebungen ist ein niedriger Wert empfehlenswert, so dass Clients an nahgelegene Access Poins gesteuert werden bei reduziertem Kommunikationsaufwand zwischen den Access Points. Als Minimum sollte man 4 Access Points berücksichtigen. Das Maximum sind 72 Access Points, wobei dieser Wert eine Beschränkung des 802.11-Protokolls ist. Eine Erhöhung über den voreingestellten Wert von 20 liefert im Normalfall keine Verbesserung mehr.

SNMP-ID:

2.12.87.11

Pfad Telnet:

Setup > **WLAN** > **Client-Steering**

Mögliche Werte:

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

Default-Wert:

20

Nachbar-Signalstaerke-Schwelle

Signalstärke in dBm, ab der ein Access Point beim Client Management als benachbart angesehen wird. Niedrigere Werte (-80, -90) sind sinnvoll bei Netzwerken, die einen weiten Bereich überdecken. Höhere Werte (-60, -50) sind in High-Density-Umgebungen sinnvoll.

SNMP-ID:

2.12.87.12

Pfad Telnet:

Setup > **WLAN** > **Client-Steering**

Mögliche Werte:

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

Default-Wert:

-70

Alte-Steuerung

Normalerweise wird beim Client Management nur versucht, Clients zu einem anderen Access Point zu steuern, wenn diese das Protokoll 802.11v korrekt unterstützen. Falls man diesen Parameter auf „Ja" einstellt, dann wird eine Steuerung mit jedem Client versucht. Dadurch wird dem Client bei einem Steuerungsversuch der Zugang zum Access Point für einige Zeit verweigert. Dadurch soll er dazu gebracht werden, von sich aus zu einem anderen Access Point zu wechseln. Aus Benutzersicht ist das WLAN einfach einige Zeit weg.

SNMP-ID:

2.12.87.13

Pfad Telnet:

Setup > **WLAN** > **Client-Steering**

Mögliche Werte:

Nein
Ja

Default-Wert:

Nein

Minimal-Last-Unterschied

Minimaler prozentualer Lastunterschied zwischen Access Points beim Client Management, ab dem eine Steuerung von Clients erfolgt. Wird nur betrachtet, falls die Lastschwelle überschritten wurde. Sollte nicht größer eingestellt werden als der Wert „Ausgleichs-Unterschied", da dann die Berechnungen falsch sein können. Außerdem nicht niedriger als 2 %, da sonst die Gefahr besteht, das ein Client zwischen zwei Access Points hin und her verschoben wird.

Ein niedriger Wert führt zu mehr Steuerungsereignissen in Umgebungen mit hoher Last. Dies kann sinnvoll sein, wenn in einer solchen Umgebung die Clients verhältnismäßig stationär sind. Ein hoher Wert führt zu weniger Steuerungsereignissen – sinnvoll in Umgebungen mit hoher Last und vielen sich bewegenden Clients.

SNMP-ID:

2.12.87.14

Pfad Telnet:

Setup > **WLAN** > **Client-Steering**

Mögliche Werte:

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

Default-Wert:

5

Taegliche-Umgebungsscan-Stunde

Uhrzeit, ab der ein Umgebungsscan beim Client Management stattfindet. Der Scan wird zufällig innerhalb eines Zeitfensters von 30 Minuten ausgeführt, damit die Wahrscheinlichkeit von Konflikten zwischen Access Points während des Scans minimiert wird. Ein Scan benötigt etwa 15 Sekunden mit der Standardeinstellung des Werts „Scan-Periode". Während dieser Zeit kann der Access Point keinen Client bedienen, daher sollten zur gewählten Stunde möglichst wenige Clients aktiv sein. Die Voreinstellung ist 3 Uhr Morgens.

SNMP-ID:

2.12.87.15

Pfad Telnet:

Setup > **WLAN** > **Client-Steering**

Mögliche Werte:

0 … 23

Default-Wert:

3

Scan-Periode

Zeit in Millisekunden, die der Umgebungs-Scan beim Client Management nach anderen Access Points auf einem Kanal sucht. Dies sollte das 2 bis 2,5-fache des eigenen Beacon-Intervalls sein. Der Standardwert funktioniert mit dem gängigen Beacon-Intervall. Höhere Werte werden nur mit höheren Beacon-Intervallen benötigt, erhöhen dabei aber das Risiko von Scan-Konflikten während der Startphase des Access Points oder während der nächtlichen Scans.

SNMP-ID:

2.12.87.16

Pfad Telnet:

Setup > **WLAN** > **Client-Steering**

Mögliche Werte:

200 … 1000

Default-Wert:

400

AP-Steering-RSSI-Schwelle

Die Signalstärke in dBm, die ein Client beim Client Management auf einem entferntem Access Point haben muss, damit er zu diesem gelenkt wird.

Eine höhere Signalschwelle bewirkt einen niedrigeren Wert potentiell lenkbarer Clients und limitiert somit die Möglichkeiten des Client Managements. Gleichzeitig wäre sie in Umgebungen mit hohen Qualtitätsanforderungen sinnvoll, z. B. bei starker Verwendung von VoIP. Dafür wird eine sehr gute Ausleuchtung und höhere Dichte der Access Points benötigt.

Eine niedrigere Signalschwelle bewirkt einen höheren Wert potentiell lenkbarer Clients, allerdings kann der Algorithmus hierbei auch Clients Access Points mit schlechter Signalqualität zuweisen. Es kann sogar passieren, dass sich Clients weigern, zu einem Access Point mit schlechterer Signalqualität gelenkt zu werden. Es würde in Umgebungen helfen, in denen ein großes Areal abgedeckt werden soll. Werte unterhalb von -80 dBm führen zu einem sehr schlechten Ergebnis, da die Wahrscheinlichkeit steigt, dass Clients sich nicht mit dem Access Point verbinden können, zu dem sie gelenkt werden sollen.

Der Standardwert passt für Büroumgebungen.

SNMP-ID:

2.12.87.17

Pfad Telnet:

Setup > **WLAN** > **Client-Steering**

Mögliche Werte:

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

Default-Wert:

-75

Entfernte-Stationen-Ablaufzeit

Zeit in Sekunden, in der ein Access Point sich die Informationen über die Clients eines benachbarten Access Points merkt. Diese Informationen werden zur Beschleunigung der Lenkentscheidungen des Client Managements verwendet. Der Standardwert passt für Büroumgebungen mit einem relativ statischen Aufbau und wenigen sich bewegenden Clients. In Umgebungen mit vielen sich bewegenden oder nur kurzzeitig verbundenen Clients sollte man niedrigere Werte setzen. Zu hohe Werte führen zu Fehlsteuerungen, wenn die Informationen des Caches nicht mehr gültig sind.

SNMP-ID:

2.12.87.18

Pfad Telnet:

Setup > **WLAN** > **Client-Steering**

Mögliche Werte:

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

Default-Wert:

600

Blacklist-Clients

In vielen Umgebungen gibt es spezielle Clients, von denen bekannt ist, dass sie sich nicht gut verhalten. Stellen Sie sich ein Krankenhaus mit kundenspezifischen VoIP-Telefonen vor, die nicht in der Lage sind, Verbindungsabbrüche ordnungsgemäß zu behandeln, und die dazu neigen, sich an einen bestimmten Access Point zu halten. Um nun nicht das Client Management komplett abschalten zu müssen, kann man diese Clients von der Steuerung ausnehmen. Entweder explizit oder über Wildcards. Dadurch können Sie die beste Benutzererfahrung für kompatible Clients erzielen, ohne dass dies Auswirkungen auf nicht kompatible Clients hat.

SNMP-ID:

2.12.87.19

Pfad Telnet:

Setup > **WLAN** > **Client-Steering**

MAC-Adresse

Die MAC-Adressen der Clients, die von einer Steuerung ausgenommen werden sollen. Als Wildcard-Zeichen kann der `*` verwendet werden, der für beliebige Zeichen steht. Dieses darf aber nicht als einziges Zeichen einer MAC-Adresse verwendet werden. Möglich sind also z. B. `01:23:45:12:34:56`, `01:*:56` oder `01:23:*`.

SNMP-ID:

2.12.87.19.1

Pfad Telnet:

Setup > **WLAN** > **Client-Steering** > **Blacklist-Clients**

Mögliche Werte:

max. 20 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default-Wert:

leer

Umgebungs-Scan-Starten

Hierüber lässt sich der Umgebungs-Scan des Client Managements als Aktion manuell starten. Dies kann verwendet werden, wenn neue Access Points hinzugekommen sind und diese noch nicht in der Tabelle der benachbarten Access Points sichtbar sind. Starten Sie die Aktion mittels `do Umgebungs-Scan-Starten`.

SNMP-ID:

2.12.87.20

Pfad Telnet:

Setup > **WLAN** > **Client-Steering**

Client-Management-Modus

Betriebsmodus des Client Managements. Zur Auswahl stehen die ausschließliche Steuerung der Clients zwischen Access Points als auch zusätzlich mit Band Steering zur Optimierung der vorhandenen Frequenzbänder eines Access Points.

SNMP-ID:

2.12.87.21

Pfad Telnet:

Setup > **WLAN** > **Client-Steering**

Mögliche Werte:

AP-Steering
AP+Band-Steering

Default-Wert:

AP+Band-Steering

Band-Verhaeltnis

Verhältnis der Verteilung auf die Bänder in Prozent. Dies wird für die Band-Steering-Funktionalität des Client Managements verwendet.

Das Verhältnis gibt an, wie viele Clients mit 5 GHz auf diesem Access Point verbunden werden sollen. Wenn mehr Clients mit 5 GHz verbunden sind, werden einige Clients auf 2,4 GHz gesteuert. Wenn mehr Clients mit 2,4 GHz verbunden sind, werden einige Clients auf 5 GHz gesteuert.

Verringern Sie den Prozentsatz, wenn Sie mit einer Kanalbreite von 20 MHz in 5 GHz arbeiten und Ihr 2,4 GHz-Spektrum frei ist, es also wenige in Konflikt stehende SSIDs und wenige andere Benutzer wie Bluetooth gibt. Wählen Sie ein höheres Verhältnis, wenn Ihr 2,4 GHz-Band voll ist.

SNMP-ID:

2.12.87.22

Pfad Telnet:

Setup > **WLAN** > **Client-Steering**

Mögliche Werte:

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

Default-Wert:

75

Band-Steering-RSSI-Schwelle

Signalstärke in dBm, die ein Client auf dem anderen Band haben muss, damit er gesteuert wird. Dies wird für die Band-Steering-Funktionalität des Client Managements verwendet.

Eine höhere Signalschwelle bewirkt einen niedrigeren Wert potentiell lenkbarer Clients und limitiert somit die Möglichkeiten des Client Managements. Gleichzeitig wäre sie in Umgebungen mit hohen Qualtitätsanforderungen sinnvoll, z. B. bei starker Verwendung von VoIP. Dafür wird eine sehr gute Ausleuchtung und höhere Dichte der Access Points benötigt.

Eine niedrigere Signalschwelle bewirkt einen höheren Wert potentiell lenkbarer Clients, allerdings kann der Algorithmus hierbei auch Clients ein Band mit schlechter Signalqualität zuweisen. Es kann sogar passieren, dass sich Clients weigern, zu einem Band mit schlechterer Signalqualität gelenkt zu werden. Es würde in Umgebungen helfen, in denen ein großes Areal abgedeckt werden soll. Werte unterhalb von -80 dBm führen zu einem sehr schlechten Ergebnis, da die Wahrscheinlichkeit steigt, dass Clients sich nicht mit verbinden können

Der Standardwert passt für Büroumgebungen.

SNMP-ID:

2.12.87.23

Pfad Telnet:

Setup > **WLAN** > **Client-Steering**

Mögliche Werte:

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

Default-Wert:

-65

Roaming-Ziele

Wenn Client Management aktiviert ist, dann wird die Tabelle in `/Status/WLAN/Roaming-Ziele` automatisch befüllt. Zusätzlich werden die manuell in dieser Tabelle hinzugefügten Ziele ebenfalls in die Liste der Nachbarn in einer 802.11k-Ankündigung aufgenommen, selbst wenn diese nicht in Reichweite sind. Die Anzahl der automatisch hinzugefügten Roaming-Ziele wird durch *2.12.87.11 Maximale-Anzahl-an-Nachbarn* auf Seite 91 beschränkt.

SNMP-ID:

2.12.132

Pfad Telnet:

Setup > **WLAN**

Name

Im Rahmen des Client Management werden hier die Namen der Roaming-Ziele dieses Access Points nach einem Umgebungsscan eingetragen. Dies ist ein Bestandteil des Standards IEEE 802.11k. In diesem Standard wird ein Weg beschrieben, WLAN-Clients über potentielle Roaming-Ziele, also weitere Access Points der selben SSID in Reichweite, zu informieren. Diese Information an den WLAN-Client erfolgt über den im Standard definierten „Neighbour Report".

SNMP-ID:

2.12.132.1

Pfad Telnet:

Setup > **WLAN** > **Roaming-Ziele**

Mögliche Werte:

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

7 Quality-of-Service

7.1 Konfigurierbare DSCP-Markierungen für interne LANCOM Dienste

Ab LCOS 10.20 können interne LCOS-Anwendungen mit konfigurierbaren DiffServ-CodePoints (DSCP) markiert werden. Dies ermöglicht es nachgeschalteter Hardware, diese Pakete zu erkennen und zu priorisieren. Weitere Informationen zu den DiffServ-CodePoints finden Sie im Referenzhandbuch im Kapitel Quality of Service.

7.1.1 Ergänzungen im Setup-Menü

DSCP-Markierung

Interne LCOS-Anwendungen können mit konfigurierbaren DiffServ-CodePoints (DSCP) markiert werden. Dies ermöglicht es nachgeschalteter Hardware, diese Pakete zu erkennen und zu priorisieren. Weitere Informationen zu den DiffServ-CodePoints finden Sie im Referenzhandbuch im Kapitel Quality of Service.

Durch diese Konfiguration werden nur die Kontrollnachrichten der jeweiligen Protokolle markiert.

SNMP-ID:

2.11.94

Pfad Telnet:

Setup > **Config**

Anwendung

Spalte mit den internen Anwendungen.

SNMP-ID:

2.11.94.1

Pfad Telnet:

Setup > **Config** > **DSCP-Markierung**

DSCP

Spalte mit den DiffServ-Codepoints. Es wird für die möglichen internen Anwendungen der jeweilige Default-Wert aufgeführt.

SNMP-ID:

2.11.94.2

Pfad Telnet:

Setup > **Config** > **DSCP-Markierung**

Mögliche Werte:

BGP

CS6

OSPF

CS6

RIP

CS6

IKE

CS6

Inkl. Dynamic-VPN-UDP-Pakete, nicht jedoch unterstützt bei SSL-Encapsulation.

TACACS

BE/CS0

SNMP

BE/CS0

L2TP

CS6

PPTP

CS6

LISP

CS6

TFTP

BE/CS0

ICMP

BE/CS0

8 Virtual Private Networks – VPN

8.1 OCSP-Server

Ab LCOS-Version 10.20 unterstützten LANCOM Geräte einen Server bzw. Responder für das Online Certificate Status Protocol (OCSP).

Online Certificate Status Protocol (OCSP) ist ein in RFC 6960 definiertes Verfahren zur Prüfung der Gültigkeit eines Zertifikats bei einer zentralen Instanz. Im Gegensatz zu Zertifikatssperrlisten (CRLs) muss bei der Verwendung nicht regelmäßig die komplette CRL heruntergeladen werden; stattdessen wird on-demand beim Verbindungsaufbau eine OCSP-Anfrage an den OCSP-Server gestellt, sodass die Information über die Gültigkeit des Zertifikats immer aktuell ist. Da hierbei nur die Gültigkeitsinformation für ein Zertifikat übertragen wird, müssen weniger Daten übertragen werden. Somit sind die Gültigkeitsinformationen im Vergleich zum CRL-basierten Verfahren stets aktuell und die Überprüfung passiert schneller.

Der OCSP-Server kann nur in Zusammenhang mit einer Zertifizierungsstelle (CA) auf dem selben Gerät eingesetzt werden (LANCOM Smart Certificate). Es ist nicht möglich, Gültigkeitsinformationen für Zertifikate anderer CAs über den OCSP-Server bereitzustellen.

Damit der OCSP-Server bei der Erzeugung von Zertifikaten per LANCOM Smart Certificate verwendet wird, muss diesem ein Zertifikat zugewiesen werden und das Profil zur Erstellung von Zertifikaten um einen Eintrag erweitert werden, damit diese den OCSP-Server kennen.

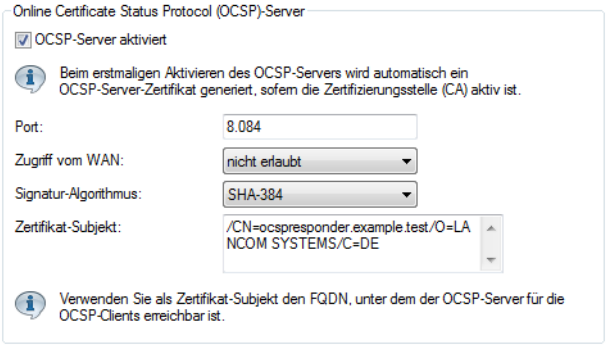
8.1.1 OCSP-Server konfigurieren

Um den OCSP-Server zu konfigurieren, sind folgende Schritte erforderlich:

1. Aktivieren Sie den OCSP-Server unter **Zertifikate** > **OCSP** > **Online Certificate Status Protocol (OCSP)-Server** > **OCSP-Server aktiviert**.
2. Weisen Sie dem OCSP-Server ein Zertifikat zu.

   Für den Betrieb des OCSP-Server ist es erforderlich, dass dieser ein Zertifikat von der CA erhält, über deren Zertifikate er Auskunft geben soll. Mit diesem Zertifikat werden die OCSP-Antworten signiert.

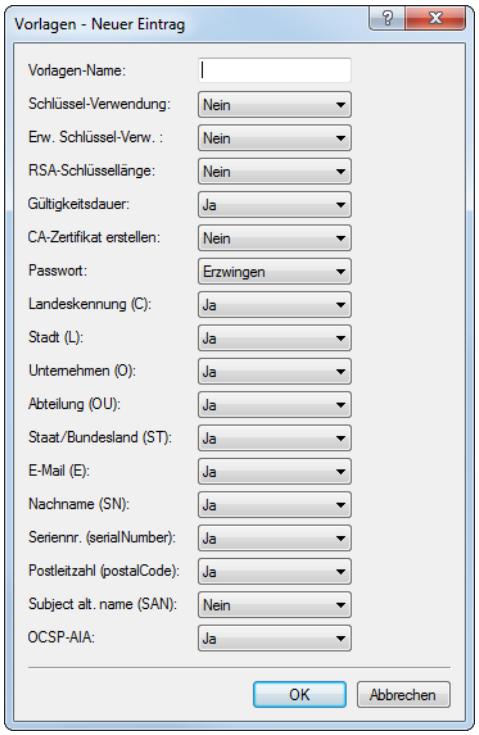
   Hierzu ist unter **Zertifikate** > **OCSP** > **Online Certificate Status Protocol (OCSP)-Server** das **Zertifikat-Subject** für den OCSP-Server zu konfigurieren. Aus dieser Information wird dann beim erstmaligen Aktivieren das Zertifikat für den OCSP-Server automatisch erzeugt.



Geben Sie im Zertifikat-Subject als CN den FQDN an, unter dem der OCSP-Server für die OCSP-Clients erreichbar ist.

3. Erweitern Sie die Smart Certificate-Vorkonfiguration um Informationen zum OCSP-Server

   a) Unter **Zertifikate** > **Zertifikatsbehandlung** > **Web-Interface der CA** > **Vorlagen** konfigurieren Sie, dass bei der Erzeugung eines Zertifikats mittels Smart Certificate CA das Feld "OCSP-AIA" (Authority Information Access) konfiguriert werden kann. Verwenden Sie die "Default"-Vorlage, ist dies bereits automatisch der Fall. Verwenden Sie eine benutzerdefinierte Vorlage, dann schalten Sie das Feld „OCSP-AIA“ aktiv.

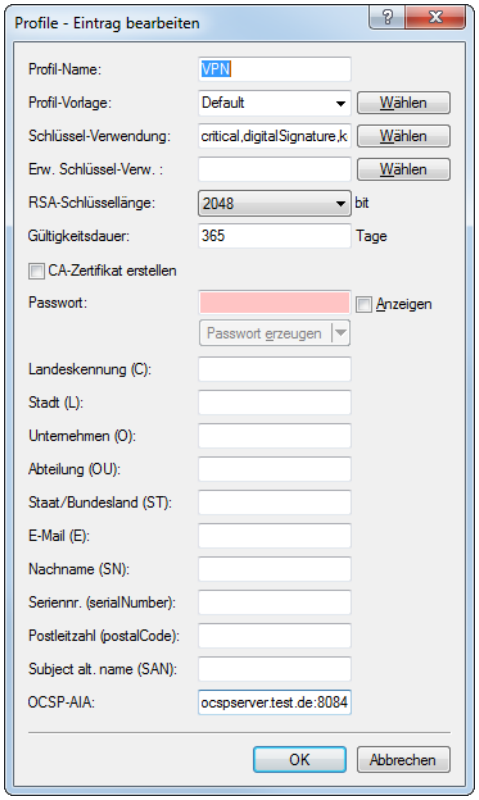


   b) Unter **Zertifikate** > **Zertifikatsbehandlung** > **Web-Interface der CA** > **Profile** legen Sie als nächstes einen Default-Wert für das Feld OCSP-AIA im gewünschten Smart-Certificate-Profil fest.

   Dieser Schritt ist optional. Wenn Sie hier keinen Default-Wert festlegen, dann müssen Sie manuell einen Wert bei der Erzeugung eines Zertifikats angeben.

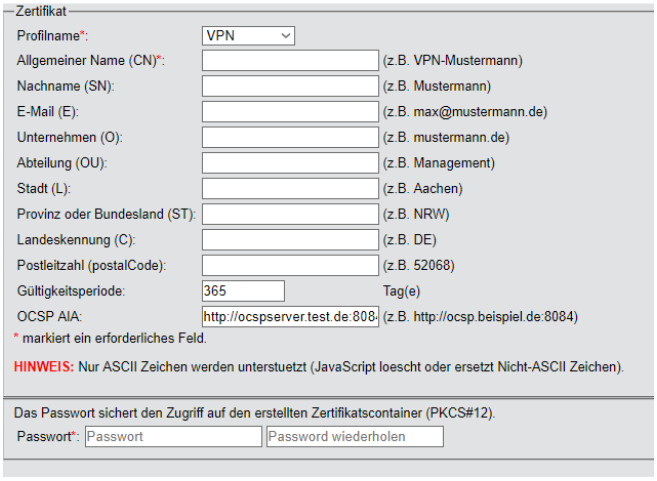
   Konfigurieren Sie hier den Namen oder die IP-Adresse, unter dem der OCSP-Server für die OCSP-Clients erreichbar ist. Dieser wurde bereits oben bei der Erzeugung des OCSP-Server-Zertifikats verwendet. Fügen Sie auch die Portnummer an, unter der der OCSP-Server erreichbar ist. Standardmäßig ist der Port 8084.

Im Beispiel wird der Default-Wert für das Profil „VPN“ auf „ocspserver.test.de:8084“ angepasst:



Die Konfiguration des OCSP-Servers ist damit abgeschlossen.

Wird nun über WEBconfig ein Zertifikat mittels Smart Certificate erzeugt, dann wird diesem automatisch die OCSP-AIA angefügt, sodass der Client beim Verbindungsaufbau zur Gültigkeitsprüfung den OCSP-Server kontaktiert.



Zur Prüfung der Gültigkeit zieht der OCSP-Server wiederum die geräteinterne Zertifikatsliste heran, so dass Zertifikate über die Smart Certificate-Weboberfläche bequem zurückgezogen oder wieder für gültig erklärt werden können.

8.1.2 Ergänzungen im Setup-Menü

OCSP-AIA

Geben Sie hier den Namen oder die IP-Adresse an, unter dem der OCSP-Server für OCSP-Clients erreichbar ist.

SNMP-ID:

2.39.2.14.1.19

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA** > **Web-Schnittstelle** > **Profile**

Mögliche Werte:

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

Default-Wert:

leer

OCSP-AIA

Bei der Erzeugung eines Zertifikats mittels Smart Certificate kann das Feld „OCSP AIA" (OCSP Authority Information Access) eingeblendet werden.

SNMP-ID:

2.39.2.14.2.18

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA** > **Web-Schnittstelle** > **Vorlage**

Mögliche Werte:

ja

Das Feld ist sichtbar und durch den Anwender änderbar.

nein

Das Feld ist unsichtbar, der eingetragene Wert gilt als Defaultwert.

erforderlich

Das Feld ist sichtbar, der Anwender muss einen Wert eintragen.

fest

Das Feld ist sichtbar, aber nicht durch den Anwender änderbar.

Default-Wert:

ja

OCSP-Server

Diese Tabelle enthält die Einstellungen für den OCSP-Server.

SNMP-ID:

2.39.7

Pfad Telnet:

Setup > **Zertifikate**

Aktiv

Schalten Sie den OCSP-Server hier ein oder aus.

SNMP-ID:

2.39.7.1

Pfad Telnet:

Setup > **Zertifikate** > **OCSP-Server**

Mögliche Werte:

Ja
Nein

Default-Wert:

Nein

Port

Der vom OCSP-Server verwendete Port.

SNMP-ID:

2.39.7.2

Pfad Telnet:

Setup > **Zertifikate** > **OCSP-Server**

Mögliche Werte:

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

Default-Wert:

8084

Zertifikat-Subjekt

Für den Betrieb des OCSP-Servers ist es erforderlich, dass dieser ein Zertifikat von der Zertifizierungsstelle (CA) erhält, über deren Zertifikate er Auskunft geben soll. Mit diesem Zertifikat werden die OCSP-Antworten signiert. Hier tragen Sie den Namen oder die IP-Adresse ein, unter dem die OCSP-Clients den OCSP-Server kontaktieren werden, z. B. `/CN=ocspresponder.example.test/O=LANCOM SYSTEMS/C=DE`

Geben Sie im Zertifikat-Subject als CN den FQDN an, unter dem der OCSP-Server für die OCSP-Clients erreichbar ist.

SNMP-ID:

2.39.7.3

Pfad Telnet:

Setup > **Zertifikate** > **OCSP-Server**

Mögliche Werte:

max. 251 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default-Wert:

/CN=ocspresponder.example.test/O=LANCOM SYSTEMS/C=DE

WAN-Zugang

Diese Einstellung bestimmt, ob und wie der OCSP-Server aus dem WAN ansprechbar ist.

SNMP-ID:

2.39.7.4

Pfad Telnet:

Setup > **Zertifikate** > **OCSP-Server**

Mögliche Werte:

Ja
Nein
Ueber-VPN

Default-Wert:

Nein

Signature-Algo

Der Algorithmus, mit dem das vom OCSP-Server verwendete Zertifikat erzeugt wurde.

SNMP-ID:

2.39.7.5

Pfad Telnet:

Setup > **Zertifikate** > **OCSP-Server**

Mögliche Werte:

SHA1
SHA-256
SHA-384
SHA-512

Default-Wert:

SHA-256

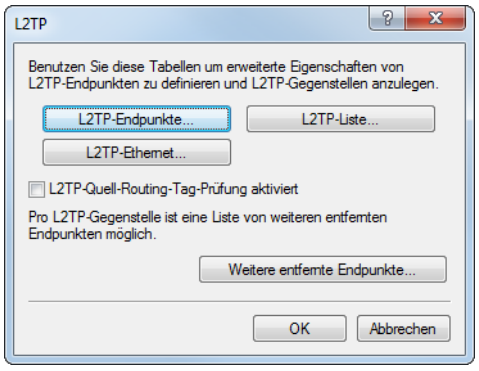
8.2 Layer-3-Ethernet-Tunnel mit Layer 2 Tunneling Protocol Version 3 (L2TPv3)

Bei L2TPv3 wird Ethernet-Traffic (Layer 2) getunnelt über UDP übertragen. Hiermit können also LANs über Netzwerk- und Standortgrenzen hinweg verbunden werden.

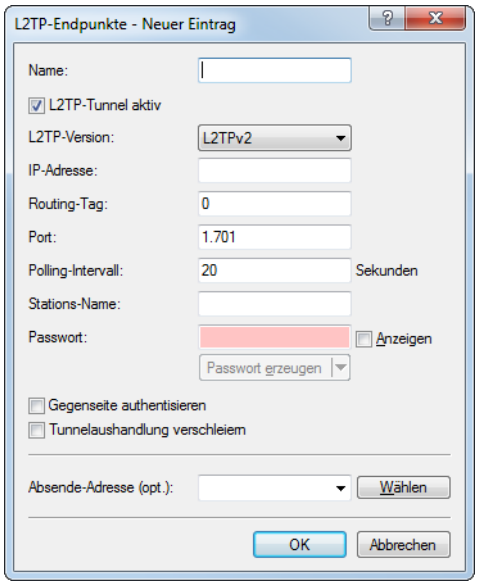
Insbesondere bietet es sich an, WLAN-Traffic auf Seiten der Access Points in einen L2TPv3 Ethernet-Tunnel einzukoppeln und an einem zentralen Konzentrator wieder auszukoppeln. Dies erforderte ohne L2TPv3 immer einen WLAN-Controller, der dieses mittels CAPWAP Layer-3-Tunnel realisiert hat. Nun ist dies mit L2TPv3 losgelöst von WLAN-Controllern möglich, so dass der WLAN-Traffic getunnelt übertragen und zentral ausgekoppelt werden kann.

Ab LCOS 10.20 sind Layer-3-Ethernet-Tunnel mit L2TPv3 konfigurierbar. Die Konfiguration erfolgt in der bereits mit Version 2 des Protokolls vorhandenen L2TP-Endpunkte-Tabelle und in der neuen L2TP-Ethernet-Tabelle. Für ein entsprechendes Szenario siehe *Konfiguration eines WLAN-Szenarios mit zentraler Auskopplung der Nutzdaten* auf Seite 109.

Mit LANconfig konfigurieren Sie L2TP unter **Kommunikation** > **Gegenstellen** > **L2TP**.



Für Version 3 wurde die Konfiguration der L2TP-Endpunkte-Tabelle unter **L2TP-Endpunkte** um die folgenden Parameter erweitert:



L2TP-Tunnel aktiv

Aktiviert den konfigurierten L2TP-Tunnel.

L2TP-Version

Die verwendete L2TP-Protokollversion, entweder Version 2 oder 3.

Ethernet-Tunnel sind nur mit Version 3 möglich. Achten Sie darauf, für diesen Fall hier das Protokoll „L2TPv3" auszuwählen.

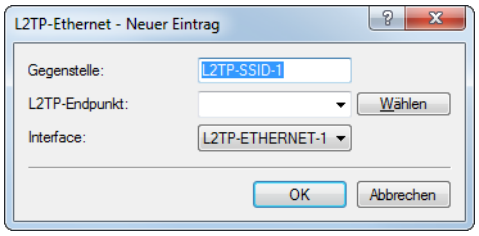
L2TPv3 wird im LCOS immer in UDP gekapselt. Dadurch ist eine problemlose Übertragung durch NAT-Gateways hindurch möglich.

Falls Sie eine IP-Adresse oder einen Hostnamen angeben, dann wird versucht, eine Verbindung aufzubauen. Wird das entsprechende Feld leer gelassen, wird keine Verbindung aufgebaut, es können aber Verbindungen angenommen werden. Konfigurierte Eigenschaften wie Stations-Name oder Passwort werden beim Verbindungsaufbau durch die Gegenseite geprüft; beim Annehmen von Verbindungen werden diese entsprechend geprüft.

Da die verschiedenen impliziten Abhängigkeiten bei der Verbindungsannahme und der Authentisierung nicht direkt offensichtlich sind, hier einige Erläuterungen dazu:

- Es wird geprüft, ob der von der Gegenseite übermittelte Hostname einem konfigurierten L2TP-Endpunkt entspricht. Der Hostname kann in der L2TP-Endpunktetabelle der Gegenseite unter **Stations-Name** konfiguriert werden. Wird dieses Feld leer gelassen, wird der Gerätename zur Authentifizierung verwendet.
- Ist dies der Fall, wird für den Verbindungsaufbau mit der Konfiguration für eben diesen L2TP-Endpunkt fortgefahren.
- Ist dies nicht der Fall, wird geschaut ob ein „Wildcard"-Eintrag in der L2TP-Endpunkte-Tabelle existiert. Dies ist ein Eintrag ohne konfigurierten Hostnamen / Stations-Namen und ohne Routing-Tag. Es wird für den Verbindungsaufbau dann mit der Konfiguration dieses „Wildcard"-Eintrages fortgefahren.
- Ist für den passenden Eintrag der L2TP-Endpunkte-Tabelle die Authentisierung eingeschaltet, wird die Authentisierung anhand des konfigurierten Passworts gemacht.
- Ist das Passwort leer und die Authentisierung eingeschaltet, wird eine RADIUS-Authentisierung durchgeführt.
- Ist die Authentisierung ausgeschaltet wird mit einem „Wildcard"-Eintrag dementsprechend jeder eingehende Tunnel akzeptiert.

Unter **L2TP-Ethernet** verknüpfen Sie L2TPv3-Sessions mit einer der 16 virtuellen L2TP-Ethernet-Schnittstellen. Die virtuellen L2TP-Ethernet-Schnittstellen können anschließend an anderer Stelle in der Konfiguration verwendet werden, z. B. in der LAN-Bridge zur Verknüpfung mit WLAN- oder LAN-Schnittstellen.



Gegenstelle

Konfigurieren Sie hier den Namen, anhand dessen der Ethernet-Tunnel auf der Gegenseite zugeordnet werden soll. Je Ethernet-Tunnel muss dieser Name also auf aufbauender und annehmender Seite gleich lauten.

L2TP-Endpunkt

Konfigurieren Sie hier den Namen des in der L2TP-Endpunkte-Tabelle konfigurierten L2TP-Endpunkts. Somit wird eine Ethernet-Tunnel-Session über diesen Endpunkt aufgebaut. Wenn nur Verbindungen angenommen, aber nicht selber aufgebaut werden sollen, kann durch leer lassen des Feldes erwirkt werden, dass beliebige Sessions angenommen werden. Natürlich müssen diese trotzdem über einen akzeptierten / aufgebauten Endpunkt aus der L2TP-Endpunkte-Tabelle „laufen". Dies kann in Szenarien, in denen nicht jeder Endpunkt auf der annehmenden Seite separat konfiguriert werden soll, sinnvoll sein.

Interface

Die für die L2TPv3-Session zu verwendende virtuelle L2TP-Ethernet-Schnittstelle.

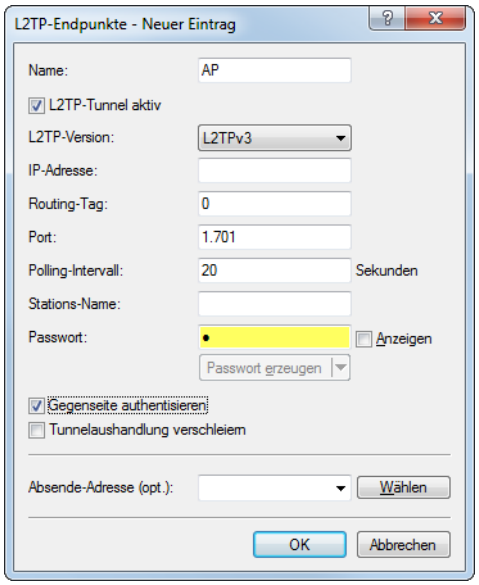
8.2.1 Konfiguration eines WLAN-Szenarios mit zentraler Auskopplung der Nutzdaten

Hier wird exemplarisch beschrieben, wie mittels L2TPv3 ein Szenario umgesetzt werden kann, in dem mehrere Access Points ihre Nutzdaten zu einem zentralen Router (hier „Konzentrator" genannt) übertragen, wo diese über einen separaten Ethernet-Port ausgekoppelt werden.

Vor LCOS 10.20 wurde für dieses Szenario ein WLAN-Controller benötigt.

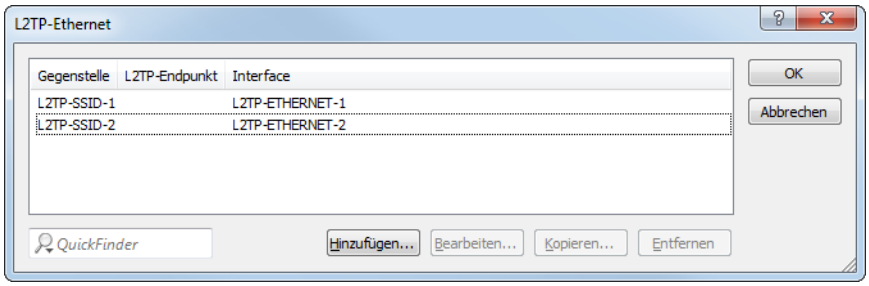
1. Bereiten Sie die WLAN-Konfiguration auf den Access Points vor. Um Roaming zu ermöglichen, sollten SSID-Namen und Verschlüsselungseinstellungen identisch konfiguriert sein.
2. Konfigurieren Sie nun den Konzentrator, der die L2TPv3-Ethernet-Sessions der einzelnen Access Points annehmen soll.
   a) Erstellen Sie unter **Kommunikation** > **Gegenstellen** > **L2TP** in der Tabelle L2TP-Endpunkte einen neuen Eintrag. Vergeben Sie einen aussagekräftigen Namen für den neuen Eintrag. Setzen Sie die **L2TP-Version** auf „L2TPv3". Geben Sie keine **IP-Adresse** an. Setzen Sie ein Passwort, um die Sicherheit zu erhöhen und wählen Sie „Gegenseite

authentisieren", damit das Passwort beim Verbindungsaufbau zur Authentisierung verwendet wird. Belassen Sie die restlichen Einstellungen auf ihren Standardwerten.



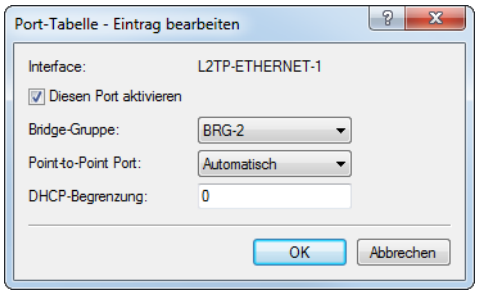
Die **IP-Adresse** ist leer. Es handelt sich daher um einen „Wildcard"-Eintrag, der Verbindungen von beliebigen Gegenstellen annehmen kann.

b) Erstellen Sie unter **Kommunikation** > **Gegenstellen** > **L2TP** in der Tabelle L2TP-Ethernet einen neuen Eintrag. Vergeben Sie unter **Gegenstelle** einen Namen, der den Ethernet-Tunnel identifiziert, z. B. den Namen der SSID, mit der der Tunnel auf den Access Points verknüpft werden soll. Lassen Sie das Feld **L2TP-Endpunkt** leer, um beliebige (authentisierte) Sessions anzunehmen. Auf diese Weise müssen Sie nicht noch für jeden Access Point einen Eintrag in der L2TP-Endpunkte-Tabelle anlegen – stattdessen genügt der im vorherigen Schritt erzeugte Wildcard-Eintrag. Konfigurieren Sie nun noch unter **Interface**, mit welchem virtuellen Interface der L2TP-Ethernet-Tunnel verbunden werden soll. Falls Sie auf den Access Points mehr als eine SSID verwenden, die zentral ausgekoppelt werden sollen, können Sie in dieser Tabelle je SSID einen weiteren Eintrag anlegen, der unter **Gegenstelle** einen eindeutigen Namen aufweist.



In unserem Szenario werden die Nutzdaten aller verbundener Access Points in das hier konfigurierte virtuelle Interface geleitet. Auch werden die Nutzdaten aller mit diesem virtuellen Interface verbundener Access Points untereinander gebridged – ähnlich dem Verfahren mit WLAN-Controller-gestütztem Layer-3-Tunnel.

c) Verknüpfen Sie unter **Schnittstellen** > **LAN** > **LAN-Bridge-Einstellungen** > **Port-Tabelle** das oben gewählte virtuelle L2TP-Interface mit einem LAN-Interface, in dem Sie die selbe Bridge-Gruppe setzen. Wiederholen Sie dies für eventuelle weitere virtuelle L2TP-Interfaces für weitere SSIDs.

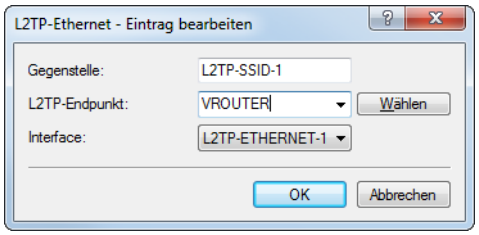


d) Die Konfiguration des Konzentrators ist damit abgeschlossen.

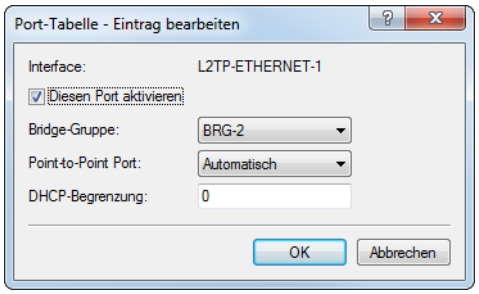
3. Konfigurieren Sie nun exemplarisch einen Access Point, der Nutzdaten an den Konzentrator leiten soll.

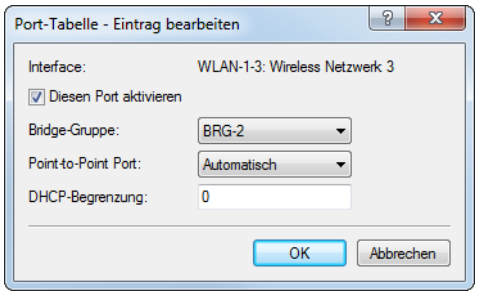
a) Erstellen Sie unter **Kommunikation** > **Gegenstellen** > **L2TP** in der Tabelle L2TP-Endpunkte einen neuen Eintrag. Vergeben Sie einen aussagekräftigen Namen für den neuen Eintrag. Setzen Sie die **L2TP-Version** auf „L2TPv3". Geben Sie die IP-Adresse oder den Hostnamen an, unter dem der Access Point den Konzentrator kontaktieren soll. Setzen Sie das bei der Konfiguration des Konzentrators vergebene Passwort und wählen Sie „Gegenseite authentisieren", damit das Passwort zur Authentisierung verwendet wird. Belassen Sie die restlichen Einstellungen auf ihren Standardwerten.

b) Erstellen Sie unter **Kommunikation** > **Gegenstellen** > **L2TP** in der Tabelle L2TP-Ethernet einen neuen Eintrag. Vergeben Sie unter **Gegenstelle** einen Namen, der den Ethernet-Tunnel identifiziert. Dieser muss gleich dem Namen lauten, der für diesen Ethernet-Tunnel auf dem Konzentrator vergeben wurde. Tragen Sie im Feld **L2TP-Endpunkt** den im vorherigen Schritt erzeugten Eintrag der L2TP-Endpunkte-Tabelle ein – über diesen Endpunkt wird der Ethernet-Tunnel dann aufgebaut. Konfigurieren Sie nun noch unter **Interface**, mit welchem virtuellen Interface der L2TP-Ethernet-Tunnel verbunden werden soll.



c) Verknüpfen Sie unter **Schnittstellen** > **LAN** > **LAN-Bridge-Einstellungen** > **Port-Tabelle** das oben gewählte virtuelle L2TP-Interface mit einem WLAN-Interface, in dem Sie die selbe Bridge-Gruppe setzen. Wiederholen Sie dies für eventuelle weitere virtuelle L2TP-Interfaces für weitere SSIDs.





d) Führen Sie die Konfiguration wie hier beschrieben für weitere Access Points durch. Wenn Sie die Konfiguration auf diese Weise durchgeführt haben, dann kann auf allen Access Points die identische Konfiguration verwendet werden und es sind keine Access-Point-spezifischen Anpassungen notwendig.

8.2.2 Ergänzungen im Setup-Menü

Version

Die verwendete L2TP-Protokollversion dieses L2TP-Endpunkts, entweder Version 2 oder 3.

Ethernet-Tunnel sind nur mit Version 3 möglich. Achten Sie darauf, für diesen Fall hier das Protokoll „L2TPv3" auszuwählen.

SNMP-ID:

2.2.35.11

Pfad Telnet:

Setup > **WAN** > **L2TP-Endpunkte**

Mögliche Werte:

L2TPv2

Layer 2 Tunneling Protocol Version 2

L2TPv3

Layer 2 Tunneling Protocol Version 3

Aktiv

Dieser L2TP-Endpunkt ist aktiv oder inaktiv.

SNMP-ID:

2.2.35.12

Pfad Telnet:

Setup > **WAN** > **L2TP-Endpunkte**

Mögliche Werte:

Nein

L2TP-Endpunkt ist inaktiv.

Ja

L2TP-Endpunkt ist aktiv.

L2TP-Ethernet

In dieser Tabelle verknüpfen Sie L2TPv3-Sessions mit einer der 16 virtuellen L2TP-Ethernet-Schnittstellen. Die virtuellen L2TP-Ethernet-Schnittstellen können anschließend an anderer Stelle in der Konfiguration verwendet werden, z. B. in der LAN-Bridge zur Verknüpfung mit WLAN- oder LAN-Schnittstellen.

SNMP-ID:

2.2.39

Pfad Telnet:

Setup > **WAN**

Remote-End

Konfigurieren Sie hier den Namen, anhand dessen der Ethernet-Tunnel auf der Gegenseite zugeordnet werden soll. Je Ethernet-Tunnel muss dieser Name also auf aufbauender und annehmender Seite gleich lauten.

SNMP-ID:

2.2.39.1

Pfad Telnet:

Setup > **WAN** > **L2TP-Ethernet**

Mögliche Werte:

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

L2TP-Endpunkt

Konfigurieren Sie hier den Namen des in der L2TP-Endpunkte-Tabelle konfigurierten L2TP-Endpunkts. Somit wird eine Ethernet-Tunnel-Session über diesen Endpunkt aufgebaut. Wenn nur Verbindungen angenommen, aber nicht selber aufgebaut werden sollen, kann durch leer lassen des Feldes erwirkt werden, dass beliebige Sessions angenommen werden. Natürlich müssen diese trotzdem über einen akzeptierten / aufgebauten Endpunkt aus der L2TP-Endpunkte-Tabelle „laufen". Dies kann in Szenarien, in denen nicht jeder Endpunkt auf der annehmenden Seite separat konfiguriert werden soll, sinnvoll sein.

SNMP-ID:

2.2.39.2

Pfad Telnet:

Setup > **WAN** > **L2TP-Ethernet**

Mögliche Werte:

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

Interface

Die für die L2TPv3-Session zu verwendende virtuelle L2TP-Ethernet-Schnittstelle.

SNMP-ID:

2.2.39.3

Pfad Telnet:

Setup > **WAN** > **L2TP-Ethernet**

Mögliche Werte:

L2TP-ETHERNET-1 … L2TP-ETHERNET-16

16 virtuelle L2TP-Ethernet-Schnittstellen

8.3 IKEv2

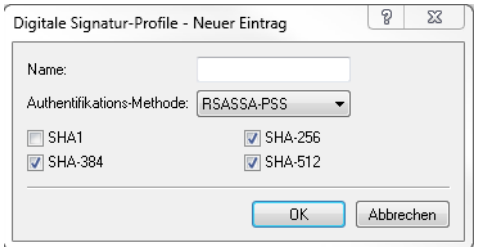
8.3.1 IKEv2 mit LANconfig konfigurieren

IKEv2 konfigurieren Sie unter **VPN** > **IKEv2/IPSec**.

Digitale Signatur-Profile

Ab LCOS-Version 10.20 unterstützt Ihr Gerät bei Auswahl des älteren RSASSA-PKCS1-v1_5 in der Aushandlung des Verfahrens mit der Gegenstelle auch das neuere RSASSA-PSS.

In dieser Tabelle konfigurieren Sie die Parameter für die IKEv2-Authentifizierung.



Name

Enthält den eindeutigen Namen dieses Eintrages. Diesen Namen können Sie an drei Stellen zuweisen. Im Bereich **Authentifizierung** in den Feldern **Lokales Dig.Signature-Prof.** und **Entf. Dig. Signature-Profil** sowie unter **Erweiterte Einstellungen** > **Authentifizierung** > **Identitäten** > **Entf. Dig. Signature-Profil**.

Authentifizierungs-Methode

Legt die Authentifizierungsmethode für die digitale Signatur fest. Mögliche Werte sind:

- RSASSA-PSS: RSA mit verbessertem probabilistischem Signatur-Schema nach Version 2.1 von PKCS #1 (probabilistic signature scheme with appendix)
- RSASSA-PKCS1-v1_5: RSA nach der älteren Version des Signature-Schemas nach Version 1.5 von PKCS #1 (signature scheme with appendix)

Bei Auswahl von RSASSA-PKCS1-v1_5 wird geprüft, ob die Gegenstelle auch das bessere Verfahren RSASSA-PSS unterstützt und ggfs. auf dieses gewechselt. Falls RSASSA-PSS ausgewählt ist, dann ist ein Rückfall auf das ältere RSASSA-PKCS1-v1_5 nicht vorgesehen.

Legen Sie zudem die zu verwendenden Secure Hash Algorithmen (SHA) fest.

Ergänzungen im Setup-Menü

Auth-Methode

Legt die Authentifizierungsmethode für die Digitale Signatur fest.

Bei Auswahl von RSASSA-PKCS1-v1_5 wird geprüft, ob die Gegenstelle auch das bessere Verfahren RSASSA-PSS unterstützt und ggfs. auf dieses gewechselt. Falls RSASSA-PSS ausgewählt ist, dann ist ein Rückfall auf das ältere RSASSA-PKCS1-v1_5 nicht vorgesehen.

SNMP-ID:

2.19.36.3.4.2

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **Digital-Signatur-Profile**

Mögliche Werte:

RSASSA-PSS
RSASSA-PKCS1-v1_5

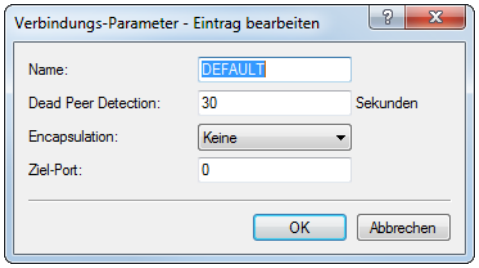
Default-Wert:

RSASSA-PSS

Verbindungs-Parameter

Ab LCOS 10.20 gibt es die neuen Parameter **Encapsulation** und **Ziel-Port** in der Tabelle **VPN** > **IKEv2/IPSec** > **VPN-Verbindungen** > **Verbindungs-Parameter**.

In dieser Tabelle definieren Sie die Parameter von IKEv2-VPN-Verbindungen, die nicht Bestandteil der SA-Verhandlung sind. Es existiert ein Standardeintrag „DEFAULT" mit gängigen Einstellungen.



Encapsulation

In manchen Szenarien kann der normale VPN-Port 500 nicht sinnvoll verwendet werden, z. B., wenn Firewalls im Weg sind. Hier können sie SSL bzw. UDP einstellen. In Verbindung mit **Ziel-Port** kann ein beliebiger Ziel-Port konfiguriert werden. Der Aufbau des IKEv2-Tunnels wird bei UDP mit Port 4500 bzw. mit dem in **Ziel-Port** eingestellten Port durchgeführt. Sollte dort 500 eingestellt sein, dann wird dies ignoriert und stattdessen der Port 4500 verwendet. Bei SSL wir der Aufbau des Tunnels mit Port 443 durchgeführt bzw. mit dem in Destination-Port eingestellten Port. Sollte dort 500 oder 4500 eingestellt sein, dann wird dies ignoriert und stattdessen der Port 443 verwendet. In der Einstellung „Keine" wird der Port 500 genommen und die Einstellung in **Ziel-Port** ignoriert.

Den konfigurierbaren Port kann man für Szenarien verwenden, wo ein LANCOM Router selbst schon auf den Standard-Ports VPN-Tunnel annimmt. Durch eine Portforwarding-Regel könnten somit diese Ports auf beliebige Ziele weitergeleitet werden.

Ziel-Port

Hier können Sie den Ziel-Port definieren, der abhängig von der Einstellung in **Encapsulation** genommen wird. Bei einer von 500 abweichenden Einstellung wird automatisch eine UDP-Encapsulation durchgeführt.

Ergänzungen im Setup-Menü

Encapsulation

In manchen Szenarien kann der normale VPN-Port 500 nicht sinnvoll verwendet werden, z.B., wenn Firewalls im Weg sind. Hier können Sie die Ports 443 bzw. 4500 einstellen. In Verbindung mit **Destination-Port** kann ein beliebiger Ziel-Port konfiguriert werden. Bei einer von 500 abweichenden Einstellung wird automatisch eine UDP-Encapsulation durchgeführt. Den konfigurierbaren Port kann man für Szenarien verwenden, wo ein LANCOM Router selbst schon auf den Standard-Ports VPN-Tunnel annimmt. Durch eine Portforwarding-Regel könnten somit diese Ports auf beliebige Ziele weitergeleitet werden.

Ankommende VPN-Tunnel werden weiterhin auf den Standard-Ports 443, 500 sowie 4500 angenommen. Diese können nicht frei konfiguriert werden.

SNMP-ID:

2.19.36.4.7

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **Allgemeines**

Mögliche Werte:

UDP

Der Aufbau des IKEv2-Tunnels wird mit Port 4500 durchgeführt bzw. mit dem in Destination-Port eingestellten Port. Sollte dort 500 eingestellt sein, dann wird dies ignoriert und stattdessen der Port 4500 verwendet.

SSL

Der Aufbau des IKEv2-Tunnels wird mit Port 443 durchgeführt bzw. mit dem in Destination-Port eingestellten Port. Sollte dort 500 oder 4500 eingestellt sein, dann wird dies ignoriert und stattdessen der Port 443 verwendet.

None

Der Aufbau des IKEv2-Tunnels wird mit Port 500 durchgeführt. Die Einstellung in Destination-Port wird ignoriert.

Default-Wert:

None

Destination-Port

Hier können Sie den Zielport der IKEv2-Verbindung definieren, der abhängig von der Einstellung in **Encapsulation** genommen wird. Bei einer von 500 abweichenden Einstellung wird automatisch eine UDP-Encapsulation durchgeführt.

SNMP-ID:

2.19.36.4.8

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **Allgemeines**

Mögliche Werte:

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

Default-Wert:

0

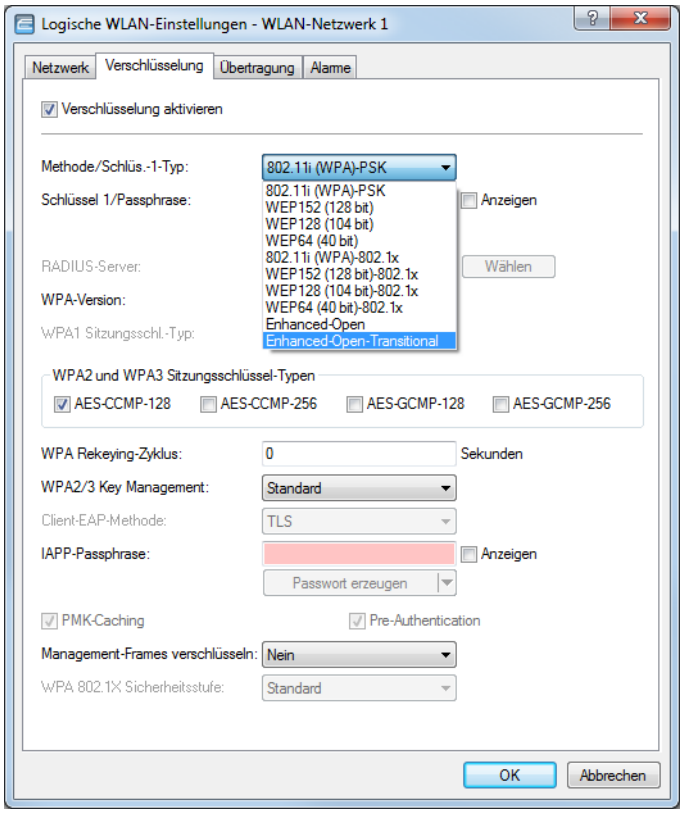
9 Public Spot

9.1 Einrichtung eines sicheren Hotspots mit Enhanced Open

Mit Enhanced Open bietet sich erstmals die Möglichkeit, einen sicheren und trotzdem einfach bedienbaren Hotspot anzubieten.

Hierzu wird Enhanced Open mit der LANCOM Public Spot Option kombiniert.

Richten Sie hierzu das für den Hotspot zu nutzende WLAN wie gewohnt ein – wählen Sie allerdings als Verschlüsselungsmethode **Enhanced Open-Transitional**:



Die Eingabe eines Schlüssels ist nicht erforderlich und auch nicht möglich: Ein Enhanced Open-fähiger Client baut ohne Angabe eines Schlüssels eine verschlüsselte Verbindung zum Access Point auf. Die Benutzererfahrung ist damit identisch zu der bei Verwendung eines unverschlüsselten WLANs: Das Eingeben eines vorher erhaltenen Schlüssels wie bei WPA2-PSK entfällt.

Die Nutzung des Transitional-Modus bewirkt, dass die selbe SSID gleichzeitig von Clients verwendet werden kann, die Enhanced Open unterstützen, sowie von Clients, die noch kein Enhanced Open unterstützen. Im letztgenannten Fall kommt allerdings keine Verschlüsselung zum Einsatz, so dass die SSID wie eine ohne Verschlüsselung betriebene SSID funktioniert. Sobald Enhanced Open in der Zukunft eine hohe Marktdurchdringung erreicht hat, kann vom Transitional-Modus in den regulären Enhanced Open-Modus gewechselt werden.

Anschließend kann wie gewohnt mit der Konfiguration des Public Spot-Moduls fortgefahren werden. Da das Public Spot-Modul unabhängig von den Verschlüsselungseinstellungen der WLAN-Schnittstellen ist, können alle Funktionen des Public Spot-Moduls in Zusammenhang mit Enhanced Open ohne Einschränkung verwendet werden.

Zusammenfassend eignet sich Enhanced Open ideal für den Betrieb von Hotspots, da es ein höheres Sicherheitsniveau als die bisher verwendeten, unverschlüsselten Hotspots bietet. Durch den optionalen Transitional-Modus ist sichergestellt, dass auch Clients, welche Enhanced Open noch nicht unterstützen, transparent angebunden werden können.

9.2 Benutzerliste entfernt

Die alte Benutzerliste des Public Spot (LANconfig: **Konfiguration** > **Public-Spot** > **Benutzer** > **Benutzer-Liste**) ist entfallen. Seit LCOS 7.70 ist der bevorzugte Weg zur Konfiguration von Public Spot-Benutzern der interne RADIUS-Server, daher wird diese alte Tabelle nicht mehr benötigt. Sollten sich zum Zeitpunkt des Upgrades noch Einträge in der Benutzerliste befinden, werden diese automatisch zu RADIUS-Benutzern konvertiert. Diese konvertierten Benutzer sind durch einen Eintrag im Kommentarfeld als solche erkennbar (z. B. "moved by root").

Sollte zu diesem Zeitpunkt in der RADIUS-Benutzertabelle ein gleichnamiger Eintrag bereits bestehen, wird dieser überschrieben.

10 RADIUS

10.1 Im- / Export von RADIUS-Benutzerdaten per CSV-Datei

Der interne RADIUS-Server ist im Prinzip eine Benutzerdatenbank. Daher soll hier eine einfache Möglichkeit gezeigt werden, mit der Sie Benutzereinträge im- und exportieren können. Insbesondere ist dies für Public-Spot-Benutzer relevant, die z. B. in größerer Zahl von einem externen System erzeugt werden. Aber auch für LEPS-MAC können Sie hier die Daten vereinfacht importieren. Als Format für den Datenaustausch wird csv (comma separated values) genommen, wobei als Default-Separator der einzelnen Datenfelder ein Semikolon dient.

10.1.1 Export von RADIUS-Benutzerdaten per CSV-Datei

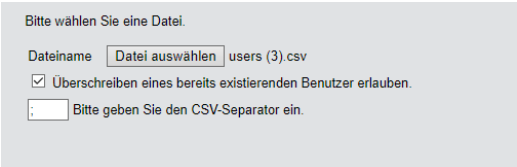
Um die Benutzerdaten des RADIUS-Servers über WEBconfig zu exportieren, gehen Sie folgendermaßen vor.

Klicken Sie auf **Extras** > **RADIUS-Benutzer exportieren**.
Die Benutzerdaten werden als Datei `users.csv` heruntergeladen. Als Trennzeichen dient das Semikolon; in der ersten Zeile sind die Bezeichner der Datenbankfelder.

10.1.2 Import von RADIUS-Benutzerdaten per CSV-Datei

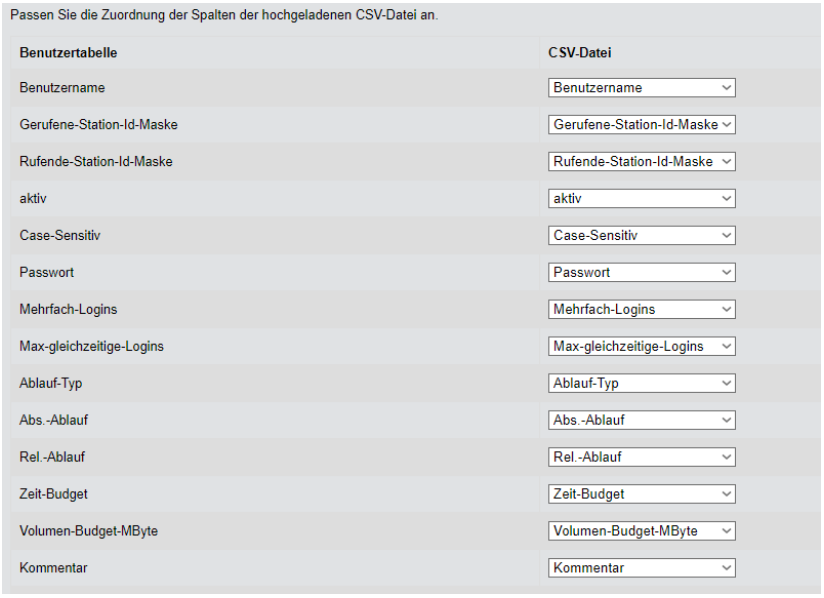
Um die Benutzerdaten des RADIUS-Servers über WEBconfig zu importieren, gehen Sie folgendermaßen vor.

1. Führen Sie wie in *Export von RADIUS-Benutzerdaten per CSV-Datei* auf Seite 120 beschrieben einen Export der Benutzerdaten durch, um die korrekte Kopfzeile mit den Bezeichnern der Datenbankfelder zu erhalten.
2. Erstellen Sie eine CSV-Importdatei mit einer Kopfzeile, welche die im vorigen Schritt ermittelten korrekten Bezeichner der Datenbankfelder beinhaltet. Die Importdatei muss nicht alle Spalten enthalten.
3. Wechseln Sie zum Menüpunkt **Extras** > **RADIUS-Benutzer importieren**.
4. Wählen Sie mit **Datei auswählen** die zu importierende CSV-Datei aus.
5. Geben Sie den CSV-Separator ein. Standardmäßig ist bereits „;“ voreingestellt.



6. Starten Sie den Upload.

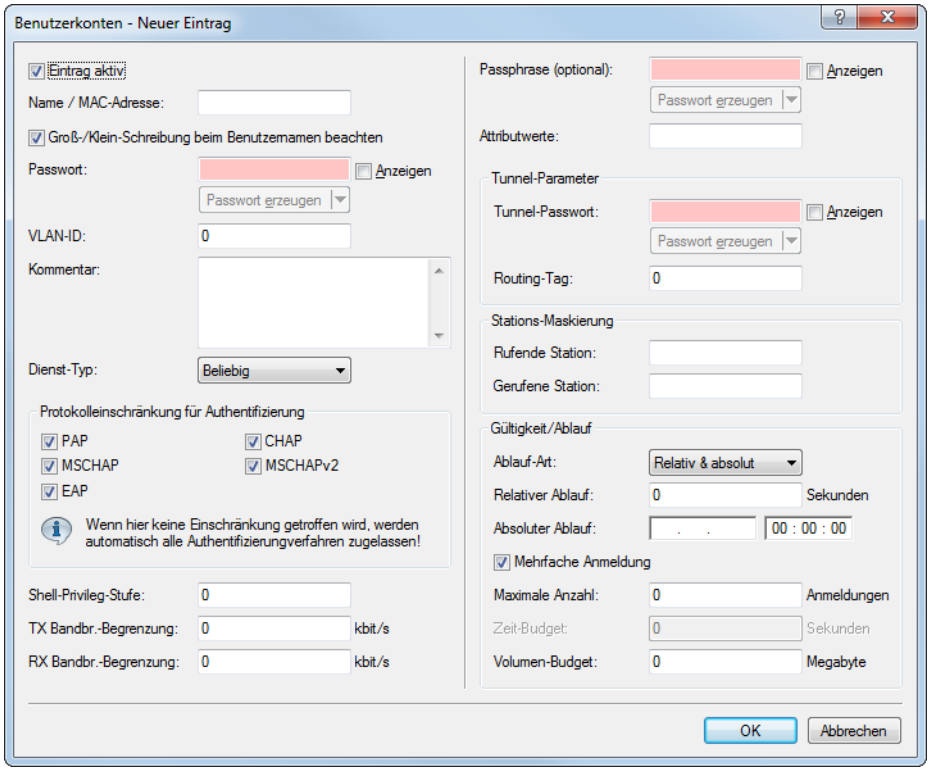
7. Kontrollieren Sie nun die Zuordnung der unterstützten Spalten zu den in der CSV-Datei erkannten Spalten. Die Zuordnung kann in diesem Dialog angepasst werden. Wenn Sie die Spaltennamen aus der zuvor exportierten CSV-Datei übernommen haben, ist keine Anpassung notwendig.



8. Wählen Sie **Import starten**, um den Vorgang abzuschließen und die Benutzerdaten zu übernehmen.

10.2 Benutzerdefinierte Attribute für RADIUS-Benutzer im RADIUS-Server.

In der RADIUS-Benutzer-Datenbank unter **RADIUS** > **Server** > **Benutzerkonten** ist der Parameter **Attributwerte** hinzugekommen, über den herstellerspezifische Attribute frei hinzugefügt werden können.



Attributwerte

Neben den vom LANCOM RADIUS-Server unterstützen Attributen, mit denen man Benutzer versehen kann, gibt es noch eine unüberschaubare Menge von herstellerspezifischen Attributen (VSAs, vendor specific attributes). Hier können diese Attribute für RADIUS-Benutzer als kommaseparierte Liste von Attributen und Werten der Form <Attribut_1>=<Wert_1>,<Attribut_2>=<Wert_2>,… frei konfiguriert werden.

10.2.1 Ergänzungen im Setup-Menü

Attribut-Werte

Benutzerdefinierte Attribute für RADIUS-Benutzer im RADIUS-Server.

Neben den vom LANCOM RADIUS-Server unterstützen Attributen, mit denen man Benutzer versehen kann, gibt es noch eine unüberschaubare Menge von herstellerspezifischen Attributen (VSAs, vendor specific attributes). Hier können diese Attribute für RADIUS-Benutzer frei konfiguriert werden.

SNMP-ID:

2.25.10.7.25

Pfad Telnet:

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

Mögliche Werte:

Kommaseparierte Liste von Attributen und Werten der Form
<Attribut_1>=<Wert_1>,<Attribut_2>=<Wert_2>,…

max. 251 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!"$%&'()*+-,/:;<=>?[\]^_.`

Default-Wert:

leer

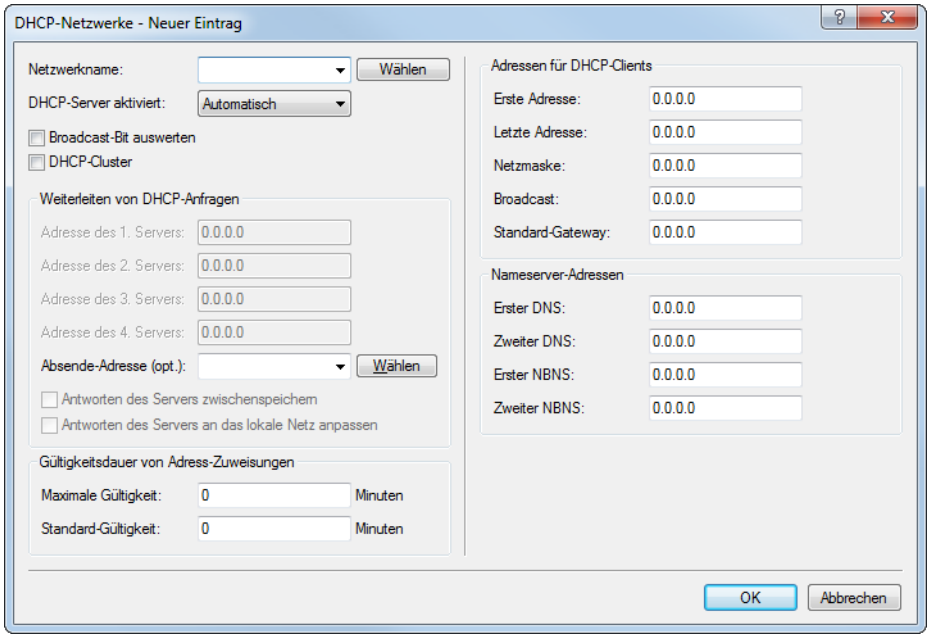
11 Weitere Dienste

11.1 Automatische IP-Adressverwaltung mit DHCP

11.1.1 Konfiguration der DHCPv4-Parameter mit LANconfig

Absendeadresse für DHCP-Relay-Agent

In der DHCP-Netzwerk-Tabelle (LANconfig: **IPv4** > **DHCPv4** > **DHCP-Netzwerke**) gibt es eine neue Option, um einem Relay-Agent eine optionale Absende-Adresse zuzuweisen.



Absende-Adresse (opt.)

Weisen Sie hier einem Relay-Agent eine optionale Absende-Adresse (Name eines ARF-Netzes, benannte Loopbackadresse) zu, die für die Weiterleitung von Client-Nachrichten verwendet wird.

Ergänzungen im Setup-Menü

Loopback-Adresse

Weisen Sie hier einem Relay-Agent eine Loopback-Adresse (Name eines ARF-Netzes, benannte Loopbackadresse) zu, die für die Weiterleitung von Client-Nachrichten verwendet wird.

SNMP-ID:

2.10.20.22

Pfad Telnet:

Setup > **DHCP**

Mögliche Werte:

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

Default-Wert:

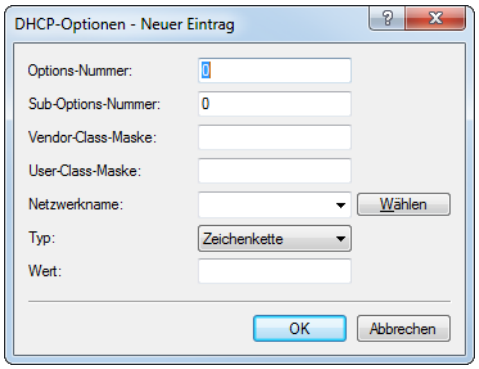
leer

DHCP-Optionen

Ab LCOS-Version 10.20 unterstützen LANCOM Geräte Sub-Optionen für die DHCP-Optionen.

Mit den DHCP-Optionen überträgt der DHCP-Server zusätzliche Konfigurationsparameter an die DHCP-Clients. Der Vendor-Class-Identifier (DHCP-Option 60) zeigt z. B. den Gerätetyp an. Die DHCP-Option 43 wird von verschiedenen Geräteherstellern verwendet, um während der Erstinbetriebnahme via DHCP weitere Informationen an Netzwerkgeräte zu verteilen. Die entsprechenden Parameter sind herstellerspezifisch.

Die Konfiguration der DHCP-Optionen in LANconfig befindet sich unter **IPv4** > **DHCPv4** > **DHCP-Optionen**. Klicken Sie auf **Hinzufügen**, um einen neuen Eintrag anzulegen.



Options-Nummer

Nummer der Option, die an die DHCP-Clients übermittelt werden soll. Die Options-Nummer beschreibt die übermittelte Information, z. B. „17" (Root Path) für den Pfad zu einem Boot-Image für einen PC ohne eigene Festplatte, der über BOOTP sein Betriebssystem bezieht.

Eine Liste aller DHCP-Optionen finden Sie im „RFC 2132 – DHCP Options and BOOTP Vendor Extensions" der Internet Engineering Task Force (IETF).

Sub-Options-Nummer

Nummer der Sub-Option, die an die DHCP-Clients übermittelt werden soll. Eine DHCP-Option kann über Sub-Optionen weiter aufgeteilt werden. Z. B. wird Netzwerkgeräten wie SIP-Telefonen über die DHCP-Option 43 häufig mitgeteilt, wo ihre Firmware und Konfiguration heruntergeladen werden kann. Die dafür einzustellenden Sub-Optionen werden dann durch den jeweiligen Hersteller definiert.

Vendor-Class-Maske

Einige DHCP-Clients übermitteln bei Anfragen an DHCP-Server eine Vendor-Class-Id und / oder eine User-Class-ID. Diese erlauben es normalerweise, den Client eindeutig einem Hersteller oder sogar einer bestimmten Geräteklasse zuzuordnen – so enthalten die DHCP-Anfragen von LANCOM Geräten immer den String „LANCOM" in der Vendor-Class-ID, ggf. ergänzt um den genauen Gerätetyp. Der DHCP-Server kann diese Information nutzen, um jedem Gerätetyp nur die jeweils passenden DHCP-Optionen zu übermitteln. Dies ist insbesondere bei der DHCP-Option 43 relevant, da deren Inhalt nicht standardisiert ist, sondern Vendor-spezifisch – je nach Hersteller oder Geräte-Art müssen unterschiedliche Informationen vom DHCP-Server übermittelt werden. Dazu können die beiden Felder „Vendor-Class-Maske" und „User-Class-Maske" als Filter

verwendet werden. Hier können Strings eingetragen werden, auf deren Vorhandensein der DHCP-Server eingehende Anfragen prüft. Nur wenn der konfigurierte Filter zur DHCP-Anfrage passt, wird anschließend die DHCP-Option ausgeliefert. Es darf mit den Wildcards „*" (beliebig viele Zeichen) und „?" (genau ein beliebiges Zeichen) gearbeitet werden. Bleiben die Felder leer, werden sie nicht beachtet und die Option wird immer ausgeliefert.

Für LANCOM Geräte würde hier also z. B. „*LANCOM*" eingetragen.

User-Class-Maske

Filterkriterium, das von einigen Herstellern bei Anfragen an den DHCP-Server verwendet wird. Siehe auch Vendor-Class-Maske. Hier können Strings eingetragen werden, auf deren Vorhandensein der DHCP-Server eingehende Anfragen prüft. Nur wenn der konfigurierte Filter zur DHCP-Anfrage passt, wird anschließend die DHCP-Option ausgeliefert. Es darf mit den Wildcards „*" (beliebig viele Zeichen) und „?" (genau ein beliebiges Zeichen) gearbeitet werden. Bleiben die Felder leer, werden sie nicht beachtet und die Option wird immer ausgeliefert.

Netzwerkname

Name des IP-Netzwerks, in dem diese DHCP-Option verwendet werden soll.

Typ

Typ des Eintrags. Dieser Wert ist abhängig von der jeweiligen Option. RFC 2132 definiert z. B. die Option „35" (ARP Cache Timeout) wie folgt:

```
ARP Cache Timeout Option
This option specifies the timeout in seconds for ARP cache entries.
The time is specified as a 32-bit unsigned integer.
The code for this option is 35, and its length is 4.
Code Len Time
+-----+-----+-----+-----+-----+-----+
| 35  | 4   | t1  | t2  | t3  | t4  |
+-----+-----+-----+-----+-----+-----+
```

Aus dieser Beschreibung können Sie ablesen, dass für diese Option der Typ „32-Bit-Integer" verwendet wird.

Den Typ der Option entnehmen Sie bitte dem entsprechenden RFC bzw. bei herstellerspezifischen DCHP-Optionen der jeweiligen Herstellerdokumentation.

Wert

In diesem Feld definieren Sie den Inhalt der DHCP-Option.

IP-Adressen werden in der üblichen Schreibweise von IPv4-Adressen angegeben, also z. B. als „123.123.123.100", Integer-Typen werden als normale Dezimalzahlen eingetragen, Strings als einfacher Text.

Mehrere Werte in einem Feld werden mit Kommas separiert, also z. B. „123.123.123.100, 123.123.123.200".

Die mögliche Länge des Optionswertes entnehmen Sie bitte dem entsprechenden RFC bzw. bei herstellerspezifischen DCHP-Optionen der jeweiligen Herstellerdokumentation.

Ergänzungen im Setup-Menü

Sub-Options-Nummer

Nummer der Sub-Option, die an die DHCP-Clients übermittelt werden soll. Eine DHCP-Option kann über Sub-Optionen weiter aufgeteilt werden. Z. B. wird Netzwerkgeräten wie SIP-Telefonen über die DHCP-Option 43 häufig mitgeteilt, wo ihre Firmware und Konfiguration heruntergeladen werden kann. Die dafür einzustellenden Sub-Optionen werden dann durch den jeweiligen Hersteller definiert.

SNMP-ID:

2.10.26.5

Pfad Telnet:

Setup > **DHCP** > **Zusaetzliche-Optionen**

Mögliche Werte:

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

Default-Wert:

leer

Vendor-Class-Maske

Einige DHCP-Clients übermitteln bei Anfragen an DHCP-Server eine Vendor-Class-Id und / oder eine User-Class-Id. Diese erlauben es normalerweise, den Client eindeutig einem Hersteller oder sogar einer bestimmten Geräteklasse zuzuordnen – so enthalten die DHCP-Anfragen von LANCOM Geräten immer den String „LANCOM" in der Vendor-Class-Id, ggf. ergänzt um den genauen Gerätetyp. Der DHCP-Server kann diese Information nutzen, um jedem Gerätetyp nur die jeweils passenden DHCP-Optionen zu übermitteln. Dies ist insbesondere bei der DHCP-Option 43 relevant, da deren Inhalt nicht standardisiert ist, sondern Vendor-spezifisch – je nach Hersteller oder Geräte-Art müssen unterschiedliche Informationen vom DHCP-Server übermittelt werden. Dazu können die beiden Felder „Vendor-Class-Maske" und „User-Class-Maske" als Filter verwendet werden. Hier können Strings eingetragen werden, auf deren Vorhandensein der DHCP-Server eingehende Anfragen prüft. Nur wenn der konfigurierte Filter zur DHCP-Anfrage passt, wird anschließend die DHCP-Option ausgeliefert. Es darf mit den Wildcards „*" (beliebig viele Zeichen) und „?" (genau ein beliebiges Zeichen) gearbeitet werden. Bleiben die Felder leer, werden sie nicht beachtet und die Option wird immer ausgeliefert.

SNMP-ID:

2.10.26.6

Pfad Telnet:

Setup > **DHCP** > **Zusaetzliche-Optionen**

Mögliche Werte:

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

Default-Wert:

leer

User-Class-Maske

Einige DHCP-Clients übermitteln bei Anfragen an DHCP-Server eine Vendor-Class-Id und / oder eine User-Class-Id. Diese erlauben es normalerweise, den Client eindeutig einem Hersteller oder sogar einer bestimmten Geräteklasse zuzuordnen. Der DHCP-Server kann diese Information nutzen, um jedem Gerätetyp nur die jeweils passenden DHCP-Optionen zu übermitteln. Dies ist insbesondere bei der DHCP-Option 43 relevant, da deren Inhalt nicht standardisiert ist, sondern Vendor-spezifisch – je nach Hersteller oder Geräte-Art müssen unterschiedliche Informationen vom DHCP-Server übermittelt werden. Dazu können die beiden Felder „Vendor-Class-Maske" und „User-Class-Maske" als Filter verwendet werden. Hier können Strings eingetragen werden, auf deren Vorhandensein der DHCP-Server eingehende Anfragen prüft. Nur wenn der konfigurierte Filter zur DHCP-Anfrage passt, wird anschließend die DHCP-Option ausgeliefert. Es darf mit den Wildcards „*" (beliebig viele Zeichen) und „?" (genau ein beliebiges Zeichen) gearbeitet werden. Bleiben die Felder leer, werden sie nicht beachtet und die Option wird immer ausgeliefert.

SNMP-ID:

2.10.26.7

Pfad Telnet:

Setup > **DHCP** > **Zusaetzliche-Optionen**

Mögliche Werte:

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

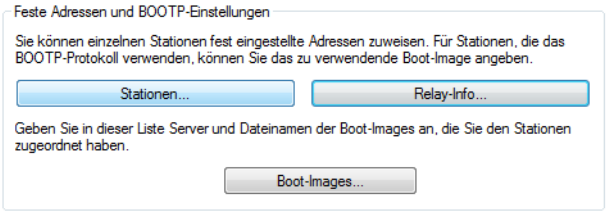
Default-Wert:

leer

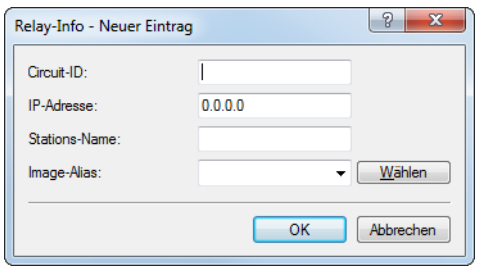
Zuweisung von IP-Adressen basierend auf DHCP-Option 82

IP-Adressen können mittels DHCP unter Nutzung der Option 82 in Abhängigkeit des Switchports zugewiesen werden, an den das Endgerät angeschlossen ist. Der jeweilige Switch fügt an die DHCP-Anfrage per DHCP-Option 82 die Circuit-ID hinzu, die den Port bezeichnet, an dem dieses Gerät angeschlossen ist. Diese Information kann dann von DHCP-Server verwendet werden, um eine bestimmte IP-Adresse zuzuweisen. Dadurch wird ein Bezug zwischen einer IP-Adresse und einem Ort hergestellt. Dadurch wird die Netzüberwachung vereinfacht.

Im LANconfig können Sie die Zuweisung der IP-Adressen basierend auf dem Switchport unter **IPv4** > **BOOTP** mit einem Klick auf **Relay-Info** für jeden Port separat festlegen.



Nach Auswahl des per DHCP-Option 82 automatisch hinzugefügten Switchports können Sie die folgenden Einstellungen festlegen:



Circuit-ID

Hier wird die vom Relay-Agent oder Switch per DHCP-Option 82 eingefügte „Circuit-ID" abgelegt, die zur Auswahl der Adresszuweisung dienen soll. Der enthaltene String wird case-sensitive ausgewertet. Abhängig von dem jeweiligen Switch wird die „Circuit-ID" vom Relay-Agent in verschiedenen Formaten geliefert und dementsprechend abgelegt. Dies kann ein kompletter Hexadezimaler-String mit führendem 0x sein. Alternativ kann die Syntax genutzt werden, die es auch beim User-Class-Identifier oder Vendor-Class-Identifier erlaubt, Binärwerte einzugeben:

Dabei werden Binärwerte in der Form `{Wert/Bitlänge}` angegeben. Der Wert kann dabei dezimal, hexadezimal (führendes 0x) oder oktal (führende 0) angegeben werden, während für die Bitlänge die Stufen 8, 16, 24, 32, 48 und 64 zur Verfügung stehen. Der Wert wird dabei in Big-Endian-Darstellung abgelegt. Soll der Wert in Little-Endian-Darstellung abgelegt werden, so sind „negative" Bitlängen anzugeben: -8, -16, -24, -32, -48 oder -64

Eine Circuit-ID (00 02 00 1e 4d 45 53 2d 33 37 32 38) kann somit in einer der folgenden Darstellungen abgelegt werden:

- 0x0002001e4d45532d33373238
- {0/8} {2/8} {30/16}
- {0x00/8} {0x02/8} {0x1e/16}
- {00/8} {02/8} {036/16}

IP-Adresse

Geben Sie hier die IP-Adresse ein, die dem Host an diesem Port zugewiesen wird. Diese Spalte darf nicht unspezifiert (0.0.0.0) sein. Das führt letztendlich dazu, daß sich pro Circuit-ID immer nur ein Host anmelden darf. Solange also hier Eintrag in der DHCP-Tablle existiert, werden alle DHCP-Nachrichten anderer Hosts auf der gleichen Circuit-ID ignoriert. D. h., will man einen anderen Host an dem Port betreiben, so muss sich der bisherige entweder korrekt abmelden (z. B. unter Microsoft Windows: `ipconfig /release`) oder aber der Eintrag muss aus der DHCP-Tabelle gelöscht werden.

Stationsname

Geben Sie hier einen Namen ein, mit dem die Station identifiziert werden soll. Wenn eine Station ihren Namen nicht übermittelt, verwendet das Gerät den hier eingetragenen Namen.

Image-Alias

Wenn die Station das BOOTP-Protokoll verwendet, dann können Sie ein Boot-Image auswählen, über das die Station ihr Betriebssystem laden soll.

Geben Sie den Server, der das Boot-Image zur Verfügung stellt und den Namen der Datei auf dem Server in der Boot-Image-Tabelle ein.

Ergänzungen im Setup-Menü

Relay-Info-Liste

IP-Adressen können mittels DHCP unter Nutzung der Option 82 in Abhängigkeit des Switchports zugewiesen werden, an den das Endgerät angeschlossen ist. Dazu liefern die Switches die „Circuit-ID" der jeweiligen Ports. Anschließend kann dann hier jedem Port genau eine Ip-Adresse, Hostname und ein Boot-Image zugewiesen werden. Letzteres funktioniert analog zur BOOTP-Tabelle.

SNMP-ID:

2.10.27

Pfad Telnet:

Setup > **DHCP**

Circuit-ID

Hier wird die vom Relay-Agent oder Switch per DHCP-Option 82 eingefügte „Circuit-ID" abgelegt, die zur Auswahl der Adresszuweisung dienen soll. Der enthaltene String wird case-sensitive ausgewertet. Abhängig von dem jeweiligen Switch wird die „Circuit-ID" vom Relay-Agent in verschiedenen Formaten geliefert und dementsprechend abgelegt. Dies kann ein kompletter Hexadezimaler-String mit führendem 0x sein. Alternativ kann die Syntax genutzt werden, die es auch beim User-Class-Identifier oder Vendor-Class-Identifier erlaubt, Binärwerte einzugeben:

Dabei werden Binärwerte in der Form `{Wert/Bitlänge}` angegeben. Der Wert kann dabei dezimal, hexadezimal (führendes 0x) oder oktal (führende 0) angegeben werden, während für die Bitlänge die Stufen 8, 16, 24, 32, 48 und

64 zur Verfügung stehen. Der Wert wird dabei in Big-Endian-Darstellung abgelegt. Soll der Wert in Little-Endian-Darstellung abgelegt werden, so sind „negative" Bitlängen anzugeben: -8, -16, -24, -32, -48 oder -64

Eine Circuit-ID (00 02 00 1e 4d 45 53 2d 33 37 32 38) kann somit in einer der folgenden Darstellungen abgelegt werden:

- 0x0002001e4d45532d33373238
- {0/8} {2/8} {30/16}
- {0x00/8} {0x02/8} {0x1e/16}
- {00/8} {02/8} {036/16}

SNMP-ID:

2.10.27.1

Pfad Telnet:

Setup > **DHCP** > **Relay-Info-Liste**

Mögliche Werte:

max. 64 Zeichen aus `[A-F][a-f]x[0-9]{}/`

IP-Adresse

Geben Sie hier die IP-Adresse ein, die dem Host an diesem Port zugewiesen wird. Diese Spalte darf nicht unspezifiert (0.0.0.0) sein. Das führt letztendlich dazu, daß sich pro Circuit-ID immer nur ein Host anmelden darf. Solange also hier Eintrag in der DHCP-Tablle existiert, werden alle DHCP-Nachrichten anderer Hosts auf der gleichen Circuit-ID ignoriert. D. h., will man einen anderen Host an dem Port betreiben, so muss sich der bisherige entweder korrekt abmelden (z. B. unter Microsoft Windows: `ipconfig /release`) oder aber der Eintrag muss aus der DHCP-Tabelle gelöscht werden.

SNMP-ID:

2.10.27.2

Pfad Telnet:

Setup > **DHCP** > **Relay-Info-Liste**

Hostname

Geben Sie hier einen Namen ein, mit dem die Station identifiziert werden soll. Wenn eine Station ihren Namen nicht übermittelt, verwendet das Gerät den hier eingetragenen Namen.

SNMP-ID:

2.10.27.3

Pfad Telnet:

Setup > **DHCP** > **Relay-Info-List**

Mögliche Werte:

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

Default-Wert:

leer

Image-Alias

Wenn die Station das BOOTP-Protokoll verwendet, dann können Sie ein Boot-Image auswählen, über das die Station ihr Betriebssystem laden soll.

Geben Sie den Server, der das Boot-Image zur Verfügung stellt und den Namen der Datei auf dem Server in der Boot-Image-Tabelle ein.

SNMP-ID:

2.10.27.4

Pfad Telnet:

Setup > **DHCP** > **Relay-Info-List**

Mögliche Werte:

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

Default-Wert:

leer

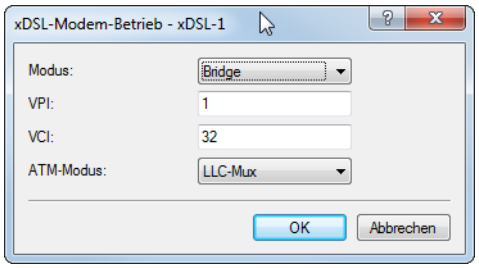
11.2 ADSL- / VDSL-Modem-Betrieb (Brigde-Mode)

Im Zuge der Umstellung von ISDN-Anschlüssen auf All-IP werden vorhandene ISDN-Anschlüsse ggf. in zusätzliche DSL-Anschlüsse gewandelt. Damit diese zusätzlich gewonnene Bandbreite für das gesamte Netzwerk zur Verfügung steht muss der DSL-Anschluss mit dem bereits vorhandenen Router verbunden werden. Ist der DSL-Anschluss des Gateways bereits belegt, kann ein LANCOM VDSL-Router als reines DSL-Modem vorgeschaltet werden. Die Zugangs- und VoIP-Daten werden somit weiter im Hauptgateway hinterlegt. Somit können weitere DSL-Anschlüsse transparent in das vorhandene Szenario eingebunden werden.

Zur Konfiguration gehen Sie folgendermaßen vor:

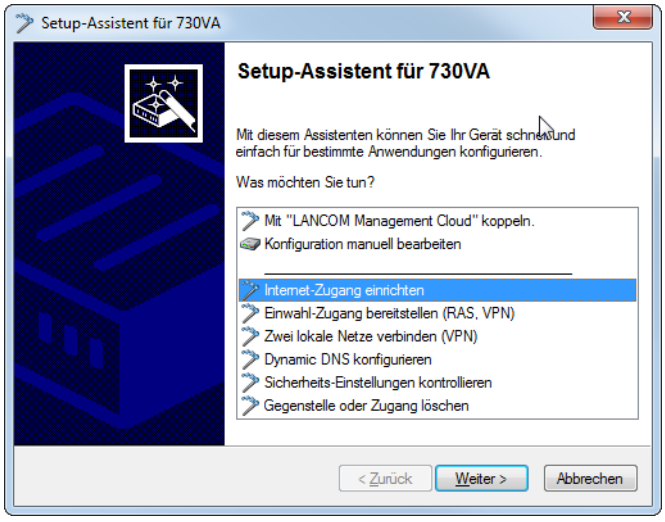
1. Den LANCOM Router, welcher als Modem genutzt werden soll, mit dem VDSL-Anschluss verbinden.
2. Das Hauptgateway über ein Ethernet-Kabel mit dem LANCOM Modem verbinden.
3. Unter **Schnittstellen** > **LAN** > **Port-Tabelle** das verwendete LAN und das xDSL-Interface in eine freie Bridge-Gruppe setzen.

4. In **Schnittstellen** > **WAN** > **Schnittstellen-Einstellungen** > **xDSL-Modem-Betrieb** den VDSL-Port auf Bridge-Modus konfigurieren. Bei Verwendung eines ADSL-Anschlusses müssen Sie ggf. die ATM-Parameter korrigieren (Deutsche Telekom: VPI 1, VCI 32, ATM-Modus LLC-Mux).

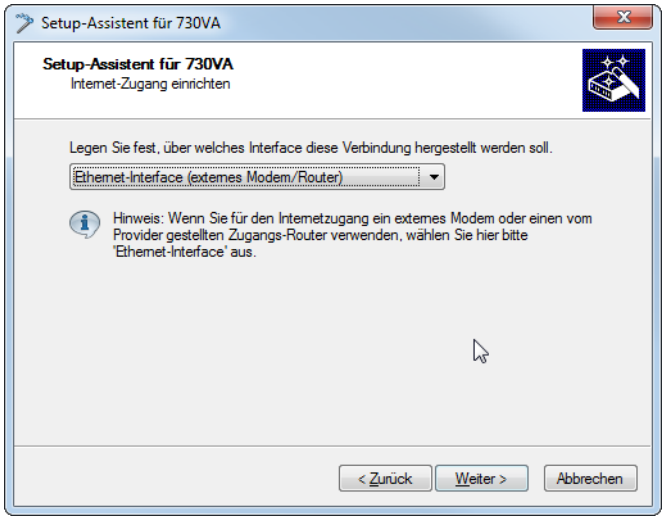


5. Den DHCP-Server unter **IPv4** > **DHCPv4** > **DHCP-Netzwerke** deaktivieren.
6. Dem Router unter **IPv4** > **Allgemein** > **IP-Netzwerke** eine Intranet-IP-Adresse aus einem nicht genutzten Bereich geben (z. B. 192.168.3.254).
7. Richten Sie auf dem Hauptgateway die Internetverbindung mittels Setup-Assistent ein:

   a. Selektieren Sie ihr Gerät in LANconfig und rufen Sie den Setup-Assistenten „Internet-Zugang einrichten“ auf.



   b. Folgen sie den Anweisungen des Setup-Assistenten und wählen jeweils die für Sie passende Option aus. Im Schritt „Interface für diese Verbindung“ wählen Sie die Option **Ethernet-Interface (externes Modem/Router)**.



Wenn der Sync-Status des LANCOM Modems aus dem Netzwerk abrufbar sein soll, dann müssen Sie unter **Kommunikation** > **Gegenstellen** > **Gegenstellen (DSL)** die Gegenstelle „Management" mit Haltezeit „9999" Sekunden, Layername „IPOE" und DSL-Port „1" anlegen.

Legen Sie in der IP-Parameterliste unter **Kommunikation** > **Protokolle** für die Gegenstelle „Management" eine IP-Adresse aus dem ungenutzten Bereich (z. B. 192.168.3.1/24) fest. Anschließend müssen Sie noch unter **IP-Router** > **Routing** > **IPv4-Routing-Tabelle** einen Eintrag für 192.168.3.0/24 auf Gegenstelle „Management" mit deaktivierter IP-Maskierung anlegen. Dann kann das Modem über die IP-Adresse 192.168.3.254 erreicht und ausgelesen werden.

11.2.1 Ergänzungen im Setup-Menü

xDSL

Asymmetrical Digital Subscriber Line (ADSL) bzw. Very High Speed Digital Subscriber Line (VDSL) – Übertragungsverfahren für die Hochgeschwindigkeitsdatenübertragung über normale Telefonverkabelungen.

Mit ADSL bzw. ADSL2+ sind Übertragungen (Downstream) bis zu 24 Mbit/s über normale Telefonkabel realisierbar, für die bidirektionale Übertragung steht ein zweites Frequenzband mit Übertragungsgeschwindigkeiten bis zu 3,5 Mbit/s (Upstream) zur Verfügung – daher auch die Bezeichnung asymmetrisch. Durch das in Deutschland verwendete ADSL-over-ISDN betragen hier die maximalen Geschwindigkeiten 16 Mbit/s (Downstream) und 1125 Kbit/s (Upstream).

VDSL ist eine DSL-Technik, die wesentlich höhere Datenübertragungsraten über gebräuchliche Telefonleitungen liefert als beispielsweise ADSL oder ADSL2+.

SNMP-ID:

2.42

Pfad Telnet:

Setup

WAN-Bridge

Hier konfigurieren Sie den Router für den ADSL- / VDSL-Modem-Betrieb (Brigde-Mode).

SNMP-ID:

2.42.3

Pfad Telnet:

Setup > **xDSL**

Interface

Die xDSL-Schnittstellen des Gerätes.

SNMP-ID:

2.42.3.1

Pfad Telnet:

Setup > **xDSL** > **WAN-Bridge**

Modus

Das Gerät kann im Bridge-Modus arbeiten. Dann verhält es sich wie ein ADSL- / VDSL-Modem.

SNMP-ID:

2.42.3.2

Pfad Telnet:

Setup > **xDSL** > **WAN-Bridge**

Mögliche Werte:

Router

Das Gerät arbeitet als Router.

Bridge

Das Gerät arbeitet im Bridge-Modus.

Default-Wert:

Router

ATM-VPI

Virtual Path Identifier (VPI). Der Wert für VPI wird vom ADSL- / VDSL-Netzbetreiber mitgeteilt. Der Default-Wert passt für die Deutsche Telekom.

SNMP-ID:

2.42.3.3

Pfad Telnet:

Setup > **xDSL** > **WAN-Bridge**

Mögliche Werte:

max. 3 Zeichen aus `[0–9]`

Default-Wert:

1

ATM-VCI

Virtual Channel Identifier (VCI). Der Wert für VCI wird vom ADSL- / VDSL-Netzbetreiber mitgeteilt. Der Default-Wert passt für die Deutsche Telekom.

SNMP-ID:

2.42.3.4

Pfad Telnet:

Setup > **xDSL** > **WAN-Bridge**

Mögliche Werte:

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

Default-Wert:

32

ATM-Muxmode

Diese Einstellung bestimmt die Encapsulation der Datenpakete. Der Default-Wert passt für die Deutsche Telekom.

SNMP-ID:

2.42.3.5

Pfad Telnet:

Setup > **xDSL** > **WAN-Bridge**

Mögliche Werte:

VC-MUX

Multiplexing über ATM durch Aufbau zusätzlicher VCs nach RFC 2684.

LLC-MUX

Multiplexing über ATM mit LLC/SNAP-Kapselung nach RFC 2684. Mehrere Protokolle können im selben VC (Virtual Channel) übertragen werden.

Default-Wert:

LLC-MUX