LCOS 10.70

Addendum

09/2022

LANCOM
SYSTEMS

Inhalt

Copyright

LANCOM Systems GmbH

Adenauerstr. 20/B2

52146 Würselen

Deutschland

www.lancom-systems.de

1 Addendum zur LCOS-Version 10.70

Dieses Dokument beschreibt die Änderungen und Ergänzungen in der LCOS-Version 10.70 gegenüber der vorherigen Version.

2 Konfiguration

2.1 Erweiterung des LoadFirmware-Kommandos

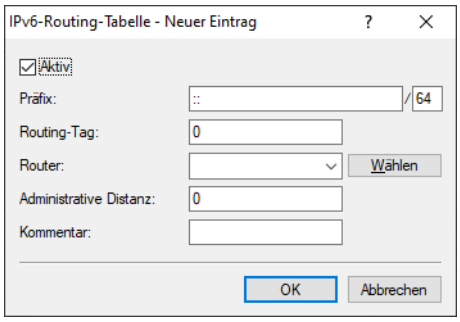
Ab LCOS 10.70 kann bei dem CLI-Kommando `loadfirmware` über den neuen Optionsschalter `-e` veranlasst werden, dass die Firmwaredatei zuerst komplett im lokalen Dateisystem gespeichert wird, bevor das Firmware-Update startet. Für sonstige Dateien oder Konfigurationen / Skripte gilt dies nicht.

3 Routing und WAN-Verbindungen

3.1 Einträge der IPv6-Routing-Tabelle schaltbar

Ab LCOS 10.70 sind Einträge der IPv6-Routing-Tabelle schaltbar.

In LANconfig konfigurieren Sie die Option unter **IP-Router** > **Routing** > **Routing-Tabelle** > **IPv6-Routing-Tabelle**.



Aktiv

Aktiviert bzw. deaktiviert diesen Eintrag in der Routing-Tabelle.

3.1.1 Ergänzungen im Setup-Menü

Aktiv

Aktiviert bzw. deaktiviert diesen Eintrag in der Routing-Tabelle.

SNMP-ID:

2.70.12.1.6

Pfad Konsole:

Setup > **IPv6** > **Router** > **Routing-Tabelle**

Mögliche Werte:

Ja
Nein

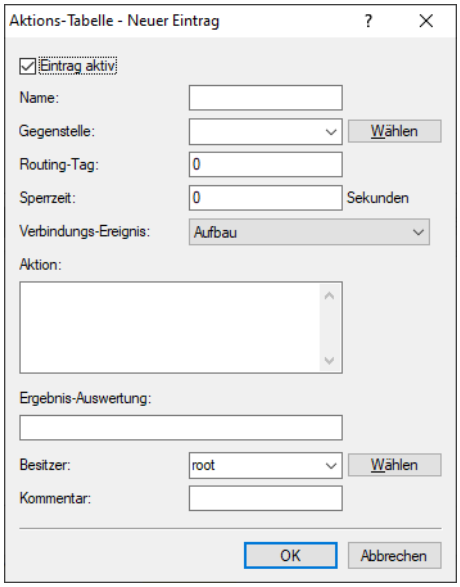
Default-Wert:

Ja

3.2 Kommentarfelder in der Aktions-Tabelle

Ab LCOS 10.70 kann pro Eintrag ein Kommentar in der Aktionstabelle hinzugefügt werden.

In LANconfig konfigurieren Sie die Option unter **Kommunikation** > **Allgemein** > **Aktions-Tabelle**.



Kommentar

Vergeben Sie einen aussagekräftigen Kommentar für diesen Eintrag.

3.2.1 Ergänzungen im Setup-Menü

Kommentar

Vergeben Sie einen aussagekräftigen Kommentar für diesen Eintrag.

SNMP-ID:

2.2.25.10

Pfad Konsole:

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

Mögliche Werte:

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

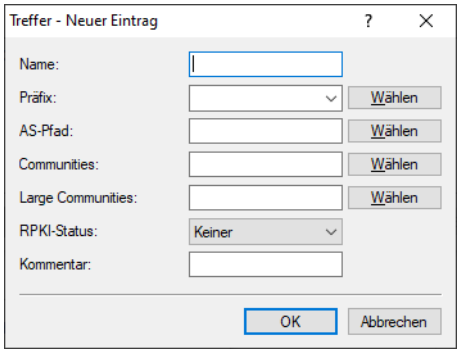
Default-Wert:

leer

3.3 BGP Large Communities

Ab LCOS 10.70 werden BGP Large Communities Attribute nach *RFC 8092* unterstützt. Damit ist es möglich 4-Octet AS-Nummern in Communities zu verwenden. Large Communities werden als separater Konfigurationsparameter im BGP-Regelwerk unterstützt.

3.3.1 Tabelle: Routing-Protokolle > BGP > BGP-Regelwerk > Treffer

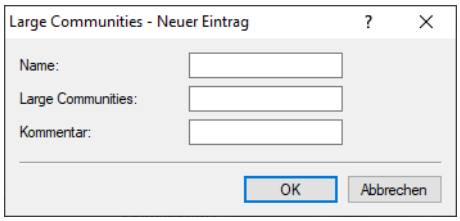


Large Communities

Enthält den entsprechenden Eintrag der Liste unter **Large Communities** im Abschnitt „Präfix- und Attribut-Listen".

Tabelle: Routing-Protokolle > BGP > BGP-Regelwerk > Treffer > Large Communities (Attribut-Liste)

Diese Tabelle enthält Large Community-Listen, um NLRIs anhand ihres Large-Community-Attributes zu erkennen.



Name

Enthält den Namen für diesen Eintrag.

Large Communities

Enthält Large Communities, die dem Large-Community-Attribut der NLRI für eine Übereinstimmung entsprechen müssen.

Die Angabe der Communities erfolgt als kommaseparierte Liste.

Struktur einer Large Community: *<Global Administrator bzw. ASN>*`:`*<Local Data Part 1>*`:`*<Local Data Part 2>*

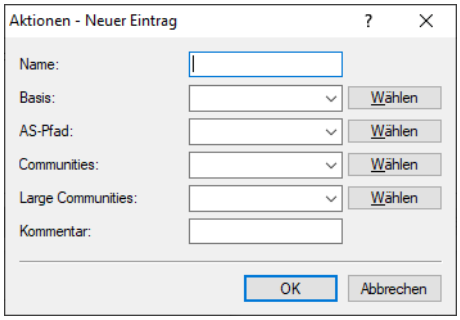
Beispiel einer einzelnen Large Community: `64496:4294967295:2`

Beispiel als kommaseparierte Liste: `64496:4294967295:2, 64496:0:0`

Kommentar

Kommentar zu diesem Eintrag.

3.3.2 Tabelle: Routing-Protokolle > BGP > BGP-Regelwerk > Aktionen



Large Communities

Enthält den Namen für die Manipulation von Large-Community-Einträgen der NLRI.

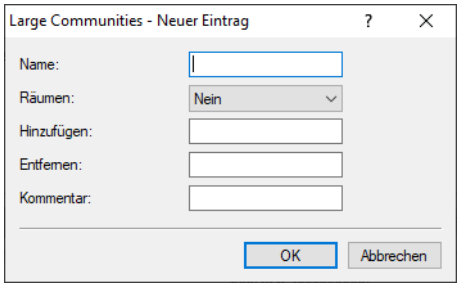
Dieser Eintrag bezieht sich auf die Einträge der Anpassungs-Tabelle unter *Tabelle: Routing-Protokolle BGP BGP-Regelwerk Aktionen Large Communities (Anpassungs-Liste)* auf Seite 10.

Tabelle: Routing-Protokolle > BGP > BGP-Regelwerk > Aktionen > Large Communities (Anpassungs-Liste)

Diese Tabelle enthält Manipulationen der Large-Community-Attribute von NLRI.

Wenn eine Aktion auf einen Eintrag dieser Tabelle zugreift, führt das Gerät alle in der entsprechenden Zeile aufgeführten Änderungen in der folgenden Reihenfolge durch:

1. **Räumen**
2. **Hinzufügen**
3. **Entfernen**



Name

Enthält den Namen für diesen Eintrag.

Räumen

Legt fest, ob das Gerät unbekannte Large Communities aus der NLRI löscht.

Hinzufügen

Legt fest, welche Large Communities das Gerät einer NLRI hinzufügt. Die Angabe der Large Communities erfolgt als kommaseparierte Liste.

Struktur einer Large Community: *<Global Administrator bzw. ASN>*:*<Local Data Part 1>*:*<Local Data Part 2>*

Beispiel einer einzelnen Large Community: `64496:4294967295:2`

Beispiel als kommaseparierte Liste: `64496:4294967295:2, 64496:0:0`

Entfernen

Legt fest, welche Large Communities das Gerät einer NLRI entfernt. Die Angabe der Large Communities erfolgt als kommaseparierte Liste.

Struktur einer Large Community: *<Global Administrator bzw. ASN>*:*<Local Data Part 1>*:*<Local Data Part 2>*

Beispiel einer einzelnen Large Community: `64496:4294967295:2`

Beispiel als kommaseparierte Liste: `64496:4294967295:2, 64496:0:0`

Kommentar

Kommentar zu diesem Eintrag.

3.3.3 Ergänzungen im Setup-Menü

Grosse-Communities

Diese Tabelle enthält Manipulationen der Large-Community-Attribute von NLRI.

Wenn eine Aktion auf einen Eintrag dieser Tabelle zugreift, führt das Gerät alle in der entsprechenden Zeile aufgeführten Änderungen in der folgenden Reihenfolge durch:

1. **Räumen**
2. **Hinzufügen**
3. **Entfernen**

SNMP-ID:

2.93.1.5.2.4

Pfad Konsole:

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

Name

Enthält den Namen für diesen Eintrag.

SNMP-ID:

2.93.1.5.2.4.1

Pfad Konsole:

Setup > **Routing-Protokolle** > **BGP** > **Regelwerk** > **Anpassungen** > **Grosse-Communities**

Mögliche Werte:

max. 16 Zeichen aus `[A-z][a-z][0-9]-_`

Default-Wert:

leer

Raeumen

Legt fest, ob das Gerät unbekannte Large Communities aus der NLRI löscht.

SNMP-ID:

2.93.1.5.2.4.2

Pfad Konsole:

Setup > **Routing-Protokolle** > **BGP** > **Regelwerk** > **Anpassungen** > **Grosse-Communities**

Mögliche Werte:

Ja

Das Gerät löscht unbekannte Large Communities aus der NLRI.

Nein

Das Gerät ändert die Large Communities einer NLRI nicht.

Default-Wert:

Nein

Hinzufuegen

Legt fest, welche Large Communities das Gerät einer NLRI hinzufügt. Die Angabe der Large Communities erfolgt als kommaseparierte Liste.

Struktur einer Large Community: *<Global Administrator bzw. ASN>*:*<Local Data Part 1>*:*<Local Data Part 2>*

Beispiel einer einzelnen Large Community: `64496:4294967295:2`

Beispiel als kommaseparierte Liste: `64496:4294967295:2, 64496:0:0`

SNMP-ID:

2.93.1.5.2.3.3

Pfad Konsole:

Setup > **Routing-Protokolle** > **BGP** > **Regelwerk** > **Anpassungen** > **Grosse-Communities**

Mögliche Werte:

max. 62 Zeichen aus `[0-9],:`

Default-Wert:

leer

Entfernen

Legt fest, welche Large Communities das Gerät einer NLRI entfernt. Die Angabe der Large Communities erfolgt als kommaseparierte Liste.

Struktur einer Large Community: *<Global Administrator bzw. ASN>:<Local Data Part 1>:<Local Data Part 2>*

Beispiel einer einzelnen Large Community: `64496:4294967295:2`

Beispiel als kommaseparierte Liste: `64496:4294967295:2, 64496:0:0`

SNMP-ID:

2.93.1.5.2.4.4

Pfad Konsole:

Setup > **Routing-Protokolle** > **BGP** > **Regelwerk** > **Anpassungen** > **Grosse-Communities**

Mögliche Werte:

max. 62 Zeichen aus `[0-9],:`

Default-Wert:

leer

Kommentar

Kommentar zu diesem Eintrag.

SNMP-ID:

2.93.1.5.2.4.5

Pfad Konsole:

Setup > **Routing-Protokolle** > **BGP** > **Regelwerk** > **Anpassungen** > **Grosse-Communities**

Mögliche Werte:

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

Default-Wert:

leer

Grosse-Communities

Enthält den Namen für die Manipulation von Large-Community-Einträgen der NLRI.

Dieser Eintrag bezieht sich auf die Einträge der Anpassungs-Tabelle unter *2.93.1.5.2.4 Grosse-Communities* auf Seite 11.

SNMP-ID:

2.93.1.5.3.6

Pfad Konsole:

Setup > **Routing-Protokolle** > **BGP** > **Regelwerk** > **Aktionen**

Mögliche Werte:

max. 16 Zeichen aus `[A-z][a-z][0-9]-_`

Default-Wert:

leer

Grosse-Communities

Diese Tabelle enthält Large Community-Listen, um NLRIs anhand ihres Large-Community-Attributes zu erkennen.

SNMP-ID:

2.93.1.5.4.4

Pfad Konsole:

Setup > **Routing-Protokolle** > **BGP** > **Regelwerk** > **Listen**

Name

Enthält den Namen für diesen Eintrag.

SNMP-ID:

2.93.1.5.4.4.1

Pfad Konsole:

Setup > **Routing-Protokolle** > **BGP** > **Regelwerk** > **Listen** > **Grosse-Communities**

Mögliche Werte:

max. 16 Zeichen aus `[A-Z][a-z][0-9]-_`

Default-Wert:

leer

Grosse-Communities

Enthält Large Communities, die dem Large-Community-Attribut der NLRI für eine Übereinstimmung entsprechen müssen.

Die Angabe der Communities erfolgt als kommaseparierte Liste.

Struktur einer Large Community: *<Global Administrator bzw. ASN>:<Local Data Part 1>:<Local Data Part 2>*

Beispiel einer einzelnen Large Community: `64496:4294967295:2`

Beispiel als kommaseparierte Liste: `64496:4294967295:2, 64496:0:0`

SNMP-ID:

2.93.1.5.4.4.2

Pfad Konsole:

Setup > **Routing-Protokolle** > **BGP** > **Regelwerk** > **Listen** > **Grosse-Communities**

Mögliche Werte:

max. 62 Zeichen aus `[0-9],:`

Default-Wert:

leer

Kommentar

Kommentar zu diesem Eintrag.

SNMP-ID:

2.93.1.5.4.4.3

Pfad Konsole:

Setup > **Routing-Protokolle** > **BGP** > **Regelwerk** > **Listen** > **Grosse-Communities**

Mögliche Werte:

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

Default-Wert:

leer

Grosse-Communities

Enthält den entsprechenden Eintrag der Liste unter *2.93.1.5.4.4 Grosse-Communities* auf Seite 14.

SNMP-ID:

2.93.1.5.5.6

Pfad Konsole:

Setup > **Routing-Protokolle** > **BGP** > **Regelwerk** > **Treffer**

Mögliche Werte:

max. 80 Zeichen aus `[A-z][a-z][0-9],-_`

Default-Wert:

leer

3.4 BGP RPKI-RTR

Ab LCOS 10.70 wird Resource Public Key Infrastructure (RPKI) to Router Protokoll (RTR) für BGP unterstützt.

Das Border Gateway Protokoll (BGP) ist grundsätzlich anfällig für sog. Route-Hijacking, d. h. das Routen von nicht-autorisierten Routern angekündigt werden können und somit Datenverkehr vom eigentlichen Ziel auf sich umlenken können. Diese Situation kann sowohl durch Fehlkonfigurationen als auch durch explizite Angriffe versursacht werden.

Resource Public Key Infrastructure (RPKI) ist ein kryptographisches Verfahren, um Routing-Datensätze, die aus Präfix und Autonomen System (AS) bestehen, zu signieren und zu validieren. Dieser Datensatz wird als Route Origin Authorization (ROA) bezeichnet. Weitere Informationen zu RPKI finden sich in *RFC 6480*.

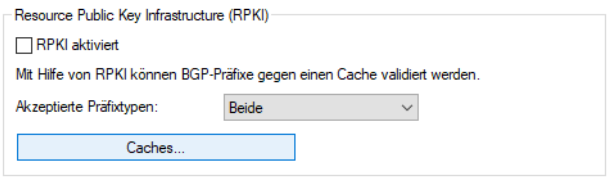
LCOS unterstützt das Resource Public Key Infrastructure to Router Protokoll (RTR) nach *RFC 8210*, mit dem der Router von einem Validator bzw. Cache Informationen über validierte Routen und zugehöriger AS-Nummer erhält. Diese Informationen werden dazu verwendet, um im BGP-Prozess zu prüfen, ob ein Präfix bzw. eine Route von dem korrekten Origin AS versendet wird. Ebenso wird geprüft, ob die Präfixlänge den Informationen aus dem ROA-Datensatz entspricht.

Dieser Cache kann entweder selbst auf einem eigenen Server für eigene Präfixe betrieben werden oder es wird ein öffentlicher Validator verwendet.

Öffentliche RPKI-Caches enthalten eine große Anzahl von ROA-Einträgen. Aufgrund des Speicherverbrauchs wird empfohlen RPKI nur auf Geräten mit genügend Hauptspeicher (mehr als 2 GB) zu verwenden wie z. B. zentralseitige Geräte oder der vRouter mit entsprechend großem Arbeitsspeicher.

3.4.1 RPKI konfigurieren

RPKI finden Sie in LANconfig unter **Routing-Protokolle** > **Allgemein** > **Resource Public Key Infrastructure (RPKI)**. Mit Hilfe von RPKI können BGP-Präfixe gegen einen Cache validiert werden. Dazu wird in der Tabelle **Treffer** des BGP-Regelwerks eine Auswahlmöglichkeit für den RPKI-Status des jeweiligen Präfixes angeboten. Siehe *Konfiguration von RPKI unter BGP* auf Seite 18.



RPKI aktiviert

Aktiviert bzw. Deaktiviert RPKI.

Akzeptierte Präfixtypen

Definiert welche ROA-Präfixtypen (IPv4 bzw. IPv6) gespeichert werden sollen. Um Arbeitsspeicher zu optimieren, wird empfohlen, den Präfixtyp auf die tatsächlich verwendete Adressfamilie (IPv4, IPv6) einzuschränken.

Mögliche Werte:

Beide

Sowohl IPv4- als auch IPv6 RPKI-Datensätze werden im Gerät gespeichert (Default).

IPv4

Nur IPv4-RPKI-Datensätze werden im Gerät gespeichert.

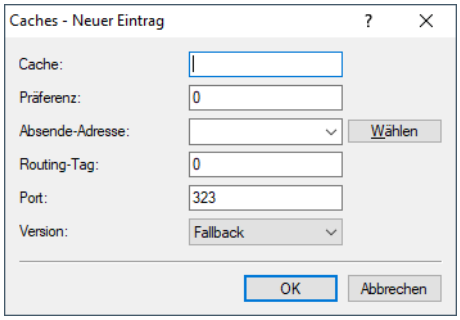
IPv6

Nur IPv6-RPKI-Datensätze werden im Gerät gespeichert

RPKI-Caches

In dieser Tabelle kann der verwendete RPKI-Validator bzw. RPKI-Cache konfiguriert werden. Als Transportprotokoll wird TCP unterstützt.

Die Einstellungen zu den RPKI-Chaches finden Sie in LANconfig unter **Routing-Protokolle** > **Allgemein** > **Resource Public Key Infrastructure (RPKI)** > **Caches**.



Cache

IPv4-, IPv6-Adresse oder Hostname unter der der RPKI-Cache erreicht wird.

Präferenz

Präferenz des Caches, falls mehrere Caches verwendet werden. Geringere Werte resultieren in einer höheren Präferenz. Default: 0

Absende-Adresse

Konfigurieren Sie optional eine Absende-Adresse, die der RPKI-Client statt der ansonsten automatisch für die Zieladresse gewählten Absende-Adresse verwendet. Falls Sie z. B. Loopback-Adressen konfiguriert haben, können Sie diese hier als Absende-Adresse angeben.

Routing-Tag

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen Cache ermittelt wird. Default: 0

Port

Port des RPKI-Caches. Default: 323

Version

Verwendete Protokollversion des PRKI-RTR-Protokolls. Mögliche Werte:

Fallback

Die Kommunikation mit dem Cache wird mit Version 1 gestartet und ggf. auf Version 0 heruntergeschaltet.

Null

Es wird Protokollversion 0 zur Kommunikation mit dem Cache verwendet.

Eins

Es wird Protokollversion 1 zur Kommunikation mit dem Cache verwendet.

3.4.2 Show-Kommandos über CLI

Ihnen stehen folgende Show-Kommandos zur Verfügung:

- **show rpki-v4-cache**

  Zeigt alle aktuell gespeicherten IPv4 ROAs an, die vom Cache empfangen wurden.

- **show rpki-v6-cache**

  Zeigt alle aktuell gespeicherten IPv6 ROAs an, die vom Cache empfangen wurden.

- **show rpki-status**

  Zeigt den aktuellen Status des RPKI-Clients an.

- **show bgp-prefix <Präfix>**

  Das Show-Kommando zeigt neben den BGP-Präfix-Informationen auch den RPKI-Status des jeweiligen Präfixes (`Not found`, `Valid`, `Invalid`, `Not available`). Folgender RPKI-Status für ein BGP-Präfix ist möglich:

  - `Not found`: Der Vaildator hat keine Informationen über dieses Präfix und das zugehörige AS zurückgeliefert. Es kann somit nicht bestimmt werden, ob der Eintrag gültig oder ungültig ist.
  - `Valid`: Der Validator hat Informationen zurückgeliefert die mit dem Präfix und AS im BGP übereinstimmen. Der Eintrag ist somit gültig.
  - `Not valid`: Der Validator hat Informationen zurückgeliefert die mit dem Präfix und AS nicht übereinstimmen. Entweder ist das Origin AS nicht korrekt oder die Präfixlänge stimmt nicht mit den Daten im Validator überein.
  - `Not available`: Es liegen keine Daten zur Prüfung aus dem Vailidator vor. RPKI ist entweder nicht aktiv oder das Gerät hat noch keine Daten vom Validator abgerufen. Das Präfix ist schon im BGP vorhanden bevor Informationen aus dem Validator vorliegen.

- **show bgp-v4-rib**

  Es wurde die Spalte ROA-AS hinzugefügt, die das AS enthält, das zur RPKI-Prüfung verwendet wurde. Ebenso die Spalte ROA-Flag, die das Ergebnis des ROA-Checks enthält.

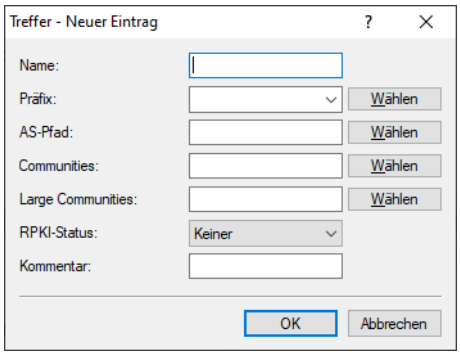
- **show bgp-v6-rib**

  Es wurde die Spalte ROA-AS hinzugefügt, die das AS enthält, das zur RPKI-Prüfung verwendet wurde. Ebenso die Spalte ROA-Flag, die das Ergebnis des ROA-Checks enthält.

3.4.3 Konfiguration von RPKI unter BGP

In der Tabelle **Treffer** des BGP-Regelwerks wird eine neue Auswahlmöglichkeit für den PRKI-Status des jeweiligen Präfixes angeboten.

LANconfig: **Routing-Protokolle** > **BGP** > **>BGP-Regelwerk** > **Treffer**



RPKI-Status

Der Resource Public Key Infrastructure (RPKI)-Status von Präfixen kann in einem BGP-Regelwerk verwendet werden und somit in Regeln auf ein BGP-Präfix angewendet werden. Es wird nicht empfohlen, ungültige Präfixe abzulehnen, sondern diesen eine niedrigere Präferenz zuzuweisen. In diesem Fall wird eine BGP-Regel definiert, die auf Präfixe mit dem RPKI-Status „ungültig" zutrifft. Als Aktion wird die Präferenz dieses Präfixes beispielsweise auf den Wert 10 gesetzt. Ein einmal abgelehntes Präfix wird nicht gespeichert und steht auch später im Prozess nicht mehr zur Verfügung es sei denn das Präfix wird vom BGP-Nachbarn erneut übertragen und neu bewertet.

Keiner

Der RPKI-Status wird nicht ausgewertet.

Nicht gefunden

Der Eintrag trifft zu, falls der PRKI-Status des Präfixes als „nicht gefunden" markiert wird.

Ungültig

Der Eintrag trifft zu, falls der der PRKI-Status des Präfixes als „ungültig" markiert wird.

Gültig

Der Eintrag trifft zu, falls der PRKI-Status des Präfixes als „gültig" markiert wird.

3.4.4 Ergänzungen im Setup-Menü

RPKI-Status

Der Resource Public Key Infrastructure (RPKI)-Status von Präfixen kann in einem BGP-Regelwerk verwendet werden und somit in Regeln auf ein BGP-Präfix angewendet werden. Es wird nicht empfohlen, ungültige Präfixe abzulehnen, sondern diesen eine niedrigere Präferenz zuzuweisen. In diesem Fall wird eine BGP-Regel definiert, die auf Präfixe mit dem RPKI-Status „ungültig" zutrifft. Als Aktion wird die Präferenz dieses Präfixes beispielsweise auf den Wert 10 gesetzt. Ein einmal abgelehntes Präfix wird nicht gespeichert und steht auch später im Prozess nicht mehr zur Verfügung es sei denn das Präfix wird vom BGP-Nachbarn erneut übertragen und neu bewertet.

SNMP-ID:

2.93.1.5.5.7

Pfad Konsole:

Setup > **Routing-Protokolle** > **BGP** > **Regelwerk** > **Treffer**

Mögliche Werte:

Keine

Der RPKI-Status wird nicht ausgewertet.

Nicht-gefunden

Der Eintrag trifft zu, falls der PRKI-Status des Präfixes als „nicht gefunden" markiert wird.

Gueltig

Der Eintrag trifft zu, falls der PRKI-Status des Präfixes als „gültig" markiert wird.

Ungueltig

Der Eintrag trifft zu, falls der der PRKI-Status des Präfixes als „ungültig" markiert wird.

RPKI

Das Border Gateway Protokoll (BGP) ist grundsätzlich anfällig für sog. Route-Hijacking, d. h. das Routen von nicht-autorisierten Routern angekündigt werden können und somit Datenverkehr vom eigentlichen Ziel auf sich umlenken können. Diese Situation kann sowohl durch Fehlkonfigurationen als auch durch explizite Angriffe versursacht werden.

Resource Public Key Infrastructure (RPKI) ist ein kryptographisches Verfahren um Routing-Datensätze, die aus Präfix und Autonomen System (AS) bestehen, zu signieren und zu validieren. Dieser Datensatz wird als Route Origin Authorization (ROA) bezeichnet. Weitere Informationen zu RPKI finden sich in *RFC 6480*.

LCOS unterstützt das Resource Public Key Infrastructure to Router Protokoll (RTR) nach *RFC 8210* mit dem der Router von einem Validator bzw. Cache Informationen über validierte Routen und zugehöriger AS-Nummer erhält. Diese Informationen werden dazu verwendet, um im BGP-Prozess zu prüfen, ob ein Präfix bzw. eine Route von dem korrekten Origin AS versendet wird. Ebenso wird geprüft, ob die Präfixlänge den Informationen aus dem ROA-Datensatz entspricht.

Dieser Cache kann entweder selbst auf einem eigenen Server für eigene Präfixe betrieben werden oder es wird ein öffentlicher Validator verwendet.

Öffentliche RPKI-Caches enthalten eine große Anzahl von ROA-Einträgen. Aufgrund des Speicherverbrauchs wird empfohlen RPKI nur auf Geräten mit genügend Hauptspeicher (mehr als 2 GB) zu verwenden wie z. B. zentralseitige Geräte oder der vRouter mit entsprechend großem Arbeitsspeicher.

In diesem Verzeichnis finden Sie die Konfiguration für RPKI.

SNMP-ID:

2.93.7

Pfad Konsole:

Setup > **Routing-Protokolle**

Caches

In dieser Tabelle kann der verwendete RPKI-Validator bzw. RPKI-Cache konfiguriert werde. Als Transportprotokoll wird TCP unterstützt.

SNMP-ID:

2.93.7.1

Pfad Konsole:

Setup > **Routing-Protokolle** > **RPKI**

Cache

IPv4-, IPv6-Adresse oder Hostname unter der der RPKI-Cache erreicht wird.

SNMP-ID:

2.93.7.1.1

Pfad Konsole:

Setup > **Routing-Protokolle** > **RPKI** > **Caches**

Mögliche Werte:

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

Default-Wert:

leer

Preference

Präferenz des Caches, falls mehrere Caches verwendet werden. Geringere Werte resultieren in einer höheren Präferenz.

SNMP-ID:

2.93.7.1.2

Pfad Konsole:

Setup > **Routing-Protokolle** > **RPKI** > **Caches**

Mögliche Werte:

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

Default-Wert:

0

Loopback

Konfigurieren Sie optional eine Absende-Adresse, die der RPKI-Client statt der ansonsten automatisch für die Zieladresse gewählten Absende-Adresse verwendet. Falls Sie z. B. Loopback-Adressen konfiguriert haben, können Sie diese hier als Absende-Adresse angeben.

SNMP-ID:

2.93.7.1.3

Pfad Konsole:

Setup > **Routing-Protokolle** > **RPKI** > **Caches**

Mögliche Werte:

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

Default-Wert:

0

Rtg-Tag

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen Cache ermittelt wird.

SNMP-ID:

2.93.7.1.4

Pfad Konsole:

Setup > **Routing-Protokolle** > **RPKI** > **Caches**

Mögliche Werte:

0 … 65535

Default-Wert:

0

Port

Port des RPKI-Caches.

SNMP-ID:

2.93.7.1.5

Pfad Konsole:

Setup > **Routing-Protokolle** > **RPKI** > **Caches**

Mögliche Werte:

max. 5 Zeichen aus `[0–9]`

Default-Wert:

323

Version

Verwendete Protokollversion des PRKI-RTR-Protokolls.

SNMP-ID:

2.93.7.1.6

Pfad Konsole:

Setup > **Routing-Protokolle** > **RPKI** > **Caches**

Mögliche Werte:

Null

Es wird Protokollversion 0 zur Kommunikation mit dem Cache verwendet.

Eins

Es wird Protokollversion 1 zur Kommunikation mit dem Cache verwendet.

Rueckfall

Die Kommunikation mit dem Cache wird mit Version 1 gestartet und ggf. auf Version 0 heruntergeschaltet.

Aktiv

Aktiviert bzw. Deaktiviert RPKI.

SNMP-ID:

2.93.7.2

Pfad Konsole:

Setup > **Routing-Protokolle** > **RPKI**

Mögliche Werte:

nein
ja

Default-Wert:

nein

Akzeptierter-Praefix-Typ

Definiert welche ROA-Präfixtypen (IPv4 bzw. IPv6) gespeichert werden sollen. Um Arbeitsspeicher zu optimieren, wird empfohlen, den Präfixtyp auf die tatsächlich verwendete Adressfamilie (IPv4, IPv6) einzuschränken.

SNMP-ID:

2.93.7.3

Pfad Konsole:

Setup > **Routing-Protokolle** > **RPKI**

Mögliche Werte:

Beide
Sowohl IPv4- als auch IPv6 RPKI-Datensätze werden im Gerät gespeichert.

IPv4
Nur IPv4-RPKI-Datensätze werden im Gerät gespeichert.

IPv6
Nur IPv6-RPKI-Datensätze werden im Gerät gespeichert

Default-Wert:

Beide

3.5 BGP: Administrative Shutdown Kommunikation

Ab LCOS 10.70 kann bei dem Kommandozeilenbefehl `do Manueller-Stopp <Name> [<Message>]` der neue optionale Parameter *<Message>* angegeben werden. Über diesen können Sie einen Grund als Nachricht nach *RFC 8203* dem anderen BGP-Router übermitteln.

3.5.1 Ergänzungen im Setup-Menü

Manueller-Stopp

Mit dieser Aktion stoppen Sie einen BGP-Nachbarn manuell.

Geben Sie als Parameter den Namen des Nachbarn an, wie er unter **Setup** > **Routing-Protokolle** > **BGP** > **Nachbarn** im Feld **Name** eingetragen ist (max. 16 Zeichen aus `[A-Z][a-z][0-9]-_`).

Trifft die Angabe des Parameters auf mehrere Nachbarn zu, beendet das Gerät zu allen Nachbarn die Verbindung.

Bestehen mehrere offene Verbindungen zum Nachbarn, beendet das Gerät alle diese Verbindungen.

Optional können Sie einen Grund als Nachricht nach *RFC 8203* dem anderen BGP-Router übermitteln. Geben Sie diesen Grund als weiteren Parameter an.

SNMP-ID:

2.93.1.10

Pfad Konsole:

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

3.6 BGP: Graceful Shutdown Unterstützung

Ab LCOS 10.70 unterstützt BGP die Graceful Shutdown Community nach *RFC 8326*.

Dazu wird bei den Konfigurationsparametern der Communities die bekannte Community `graceful-shutdown` unterstützt.

4 IPv6

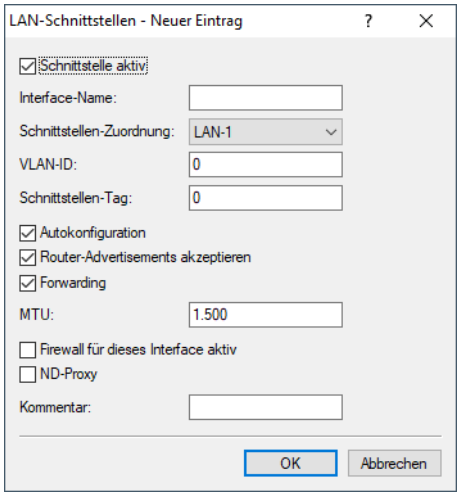
4.1 IPv6 Neighbor Discovery Proxy (NDP)

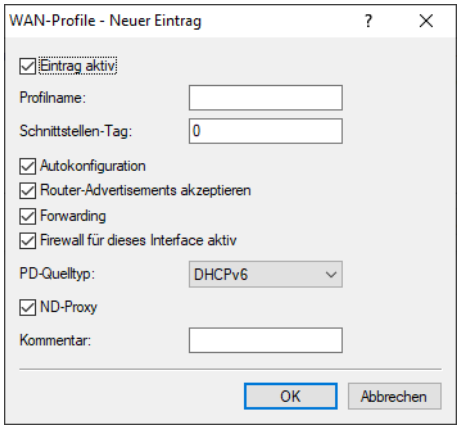
Ab LCOS 10.70 unterstützt das Gerät einen IPv6 Neighbor Discovery Proxy (NDP). Der ND-Proxy entspricht dem IPv4 Pendant ARP-Proxy. Mit dem ND-Proxy binden Sie entfernte IPv6-Stationen in Ihr lokales Netz so ein, als befänden sie sich in Ihrem lokalen Netz. Der Router antwortet dann stellvertretend auf Neighbor-Discovery-Pakete für die entfernte Station.

Szenarien:

- Ein vorgeschalteter Router unterstützt keine DHCPv6-Präfix-Delegierung. Der nachgeschaltete Router aktiviert den ND-Proxy und verwendet auf seiner LAN- und WAN-Schnittstelle das gleiche /64-Präfix. Das LAN-Präfix wird aus dem Router Advertisement des vorgeschalteten Routers der WAN-Schnittstelle erzeugt. Damit ist eine Kommunikation zwischen Stationen im LAN zu Stationen im WAN möglich, die das gleiche /64-Präfix verwenden.
- Ein VPN-Gateway weist Einwahlclients eine IPv6-Adresse aus dem gleichen Präfix zu, das schon auf einer lokalen Schnittstelle konfiguriert ist. Dieser Router muss den ND-Proxy aktivieren, damit eine Kommunikation zwischen Einwahl-Client und Stationen im lokalen LAN mit dem gleichen IPv6-Präfix möglich ist. Das Szenario ist analog zum ARP-Proxy für IPv4.

In LANconfig konfigurieren Sie die Option unter **IPv6** > **Allgemein** > **LAN-Schnittstellen** bzw. **IPv6** > **Allgemein** > **WAN-Profile**.





ND-Proxy

Aktiviert bzw. deaktiviert die IPv6 Neighbor Discovery-Proxyfunktionalität. Der ND-Proxy entspricht dem IPv4-Pendant ARP-Proxy. Mit dem ND-Proxy binden Sie entfernte IPv6-Stationen in Ihr lokales Netz so ein, als befänden sie sich in Ihrem lokalen Netz. Der Router antwortet dann stellvertretend auf Neighbor-Discovery-Pakete für die entfernte Station.

4.1.1 Ergänzungen im Setup-Menü

ND-Proxy

Aktiviert bzw. deaktiviert die IPv6 Neighbor Discovery-Proxyfunktionalität. Der ND-Proxy entspricht dem IPv4-Pendant ARP-Proxy. Mit dem ND-Proxy binden Sie entfernte IPv6-Stationen in Ihr lokales Netz so ein, als befänden sie sich in Ihrem lokalen Netz. Der Router antwortet dann stellvertretend auf Neighbor-Discovery-Pakete für die entfernte Station.

SNMP-ID:

2.70.6.14

Pfad Konsole:

Setup > **IPv6** > **LAN-Interfaces**

Mögliche Werte:

nein
ja

Default-Wert:

nein

ND-Proxy

Aktiviert bzw. Deaktiviert die IPv6 Neighbor Discovery-Proxyfunktionalität. Der ND-Proxy entspricht dem IPv4 Pendant ARP-Proxy. Mit dem ND-Proxy binden Sie entfernte IPv6-Stationen in Ihr lokales Netz so ein, als befänden sie sich in Ihrem lokalen Netz. Der Router antwortet dann stellvertretend auf Neighbor-Discovery-Pakete für die entfernte Station.

SNMP-ID:

2.70.7.12

Pfad Konsole:

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

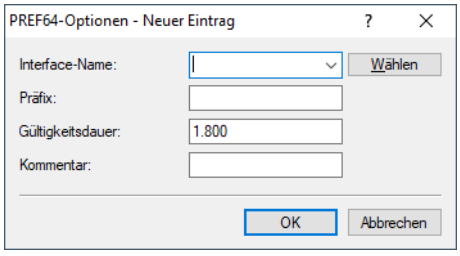
Mögliche Werte:

nein
ja

Default-Wert:

nein

4.2 PREF64-Optionen



Ab LCOS 10.70 unterstützt das Gerät die Präfix-Option in Router Advertisements nach RFC 8781. Konfigurieren Sie diese in LANconfig unter **IPv6** > **Router-Advertisement** > **PREF64-Optionen**.

In dieser Tabelle kann die Präfix-Option in Router Advertisements (PREF64-Option nach *RFC 8781*) für NAT64-Präfixe konfiguriert werden, die an Clients im Router Advertisement angekündigt werden soll. Clients übernehmen dieses Präfix z. B. für 464XLAT.

Interface-Name

Geben Sie den Namen des Interfaces an, auf welchem die PREF64-Option angekündigt werden soll.

Präfix

Definiert das NAT64-Präfix mit Präfixlänge, z. B. 64:ff9b::/96

Gültigkeitsdauer

Gültigkeitsdauer des NAT64-Präfixes in Sekunden. Default: 1800 Sekunden.

Kommentar

Vergeben Sie einen aussagekräftigen Kommentar.

4.2.1 Ergänzungen im Setup-Menü

PREF64-Option

In dieser Tabelle kann die Präfix-Option (PREF64-Option nach *RFC 8781*) für NAT64-Präfixe konfiguriert werden, die an Clients im Router Advertisement angekündigt werden soll. Clients übernehmen dieses Präfix z. B. für 464XLAT.

SNMP-ID:

2.70.2.8

Pfad Konsole:

Setup > **IPv6** > **Router-Advertisements**

Interface-Name

Geben Sie den Namen des Interfaces an, auf welchem die PREF64-Option angekündigt werden soll.

SNMP-ID:

2.70.2.8.1

Pfad Konsole:

Setup > **IPv6** > **Router-Advertisement** > **PREF64-Option**

Mögliche Werte:

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

Default-Wert:

leer

IPv6-Adresse-Praefixlaenge

Definiert das NAT64-Präfix mit Präfixlänge, z. B. 64:ff9b::/96

SNMP-ID:

2.70.2.8.2

Pfad Konsole:

Setup > **IPv6** > **Router-Advertisement** > **PREF64-Option**

Mögliche Werte:

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

Default-Wert:

leer

Scaled-Lifetime

Gültigkeitsdauer des NAT64-Präfixes in Sekunden.

SNMP-ID:

2.70.2.8.3

Pfad Konsole:

Setup > **IPv6** > **Router-Advertisement** > **PREF64-Option**

Mögliche Werte:

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

Default-Wert:

1800

Kommentar

Vergeben Sie einen aussagekräftigen Kommentar.

SNMP-ID:

2.70.2.8.4

Pfad Konsole:

Setup > **IPv6** > **Router-Advertisement** > **PREF64-Option**

Mögliche Werte:

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

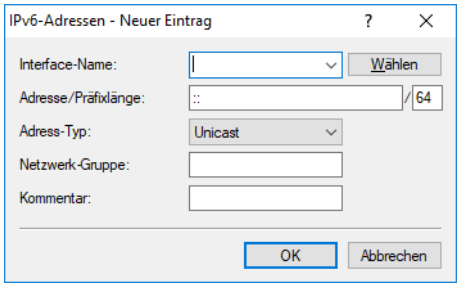
Default-Wert:

leer

4.3 Erweiterung IPv6-Adresstabelle

Ab LCOS 10.70 gibt es die neuen Schalterwerte **Delegiert, Autokonfiguration** und **Delegiert, DHCPv6** in der IPv6-Adressen-Tabelle bei **Adress-Typ**.

In LANconfig konfigurieren Sie die Option unter **IPv6** > **Allgemein** > **IPv6-Adressen**.



Adress-Typ

Bestimmen Sie den Typ der IPv6-Adresse.

Mögliche Optionen:

- Delegiert, Autokonfiguration

  Die IPv6-Adresse wird aus dem empfangenen Router Advertisement Präfix auf dem ausgewählten Interface (Feld **Interface-Name**) und dem Host-Identifier aus dem Feld **Adresse / Präfixlänge** gebildet. Im Feld **Adresse / Präfixlänge** kann z. B. der Wert „::2/64“ eingetragen werden, zusammen mit dem Präfix „2001:db8::/64“ auf dem Interface ergibt sich dann entsprechend die Adresse „2001:db8::2/64“.

- Delegiert, DHCPv6

  Die IPv6-Adresse wird aus dem empfangenen delegierten DHCPv6-Präfix auf dem ausgewählten Interface (Feld **Interface-Name**) und dem Host-Identifier aus dem Feld **Adresse / Präfixlänge** gebildet. Im Feld **Adresse / Präfixlänge** kann z. B. der Wert „::2/64“ eingetragen werden, zusammen mit dem Präfix „2001:db8::/56“ auf dem Interface ergibt sich dann entsprechend die Adresse „2001:db8::2/64“. Ebenso kann eine Adresse aus einem beliebigen Subnetz des delegierte Präfix gebildet werden, z. B. aus „0:0:0:0001::1“ und dem Präfix „2001:db8::/56“ wird die Adresse „2001:db8:0:0001::1/64“.

4.3.1 Ergänzungen im Setup-Menü

Adresstyp

Bestimmen Sie den Typ der IPv6-Adresse.

SNMP-ID:

2.70.4.1.3

Pfad Konsole:

Setup > **IPv6** > **Netzwerk** > **Adressen**

Mögliche Werte:

Unicast

Beim Adresstyp Unicast können sie eine vollständige IPv6-Adresse im Feld *2.70.4.1.2 IPv6-Adresse-Praefixlaenge* inkl. Interface Identifier angeben, z. B. „2001:db8::1234/64“.

Anycast

Beim Adresstyp Anycast können sie ebenfalls eine vollständige IPv6-Adresse im Feld *2.70.4.1.2 IPv6-Adresse-Praefixlaenge* inkl. Interface Identifier angeben, z. B. „2001:db8::1234/64“. Intern behandelt das Gerät diese Adresse als Anycast-Adresse.

EUI-64

Die IPv6-Adresse wird gemäß der IEEE-Norm „EUI-64" gebildet. Die MAC-Adresse der Schnittstelle stellt damit einen eindeutig identifizierbaren Bestandteil der IPv6-Adresse dar. Ein korrektes Eingabeformat für eine IPv6-Adresse inkl. Präfixlänge nach EUI-64 würde lauten: „2001:db8:1::/64".

EUI-64 ignoriert einen eventuell konfigurierten „Interface Identifier" der jeweiligen IPv6-Adresse und ersetzt ihn durch einen „Interface Identifier" nach EUI-64.

Die Präfixlänge bei EUI-64 muss zwingend „/64" sein.

Delegated-Auto-Configuration

Die IPv6-Adresse wird aus dem empfangenen Router Advertisement Präfix auf dem ausgewählten Interface (Feld *2.70.4.1.1 Interface-Name*) und dem Host-Identifier aus dem Feld *2.70.4.1.2 IPv6-Adresse-Praefixlaenge* gebildet. Im Feld *2.70.4.1.2 IPv6-Adresse-Praefixlaenge* kann z. B. der Wert„ ::2/64" eingetragen werden, zusammen mit dem Präfix „2001:db8::/64" auf dem Interface ergibt sich dann entsprechend die Adresse „2001:db8::2/64".

Delegated-DHCPv6

Die IPv6-Adresse wird aus dem empfangenen delegierten DHCPv6-Präfix auf dem ausgewählten Interface (Feld *2.70.4.1.1 Interface-Name*) und dem Host-Identifier aus dem Feld *2.70.4.1.2 IPv6-Adresse-Praefixlaenge* gebildet. Im Feld *2.70.4.1.2 IPv6-Adresse-Praefixlaenge* kann z. B. der Wert „::2/64" eingetragen werden, zusammen mit dem Präfix „2001:db8::/56" auf dem Interface ergibt sich dann entsprechend die Adresse „2001:db8::2/64". Ebenso kann eine Adresse aus einem beliebigen Subnetz des delegierte Präfix gebildet werden, z. B. aus „0:0:0:0001::1" und dem Präfix „2001:db8::/56" wird die Adresse „2001:db8:0:0001::1/64".

Default-Wert:

Unicast

4.4 IPv6 ND-Cache Limit

Ab LCOS 10.70 sind Begrenzungen für den ND-Cache aktiv. Dadurch wird dieser gegen Flooding-Angriffe geschützt. Das globale Cache Limit und das Limit pro Interface können sie über die Kommandozeile ggf. anpassen.

4.4.1 Ergänzungen im Setup-Menü

NDP

In diesem Menü finden Sie Einstellungen zum ND-Cache.

SNMP-ID:

2.70.16

Pfad Konsole:

Setup > **IPv6**

Globales-Cache-Limit

Definiert die maximal erlaubte Anzahl an IPv6-Neighbor-Cache Einträge pro Gerät.

SNMP-ID:

2.70.16.1

Pfad Konsole:

Setup > **IPv6** > **NDP**

Mögliche Werte:

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

Default-Wert:

20000

Cache-Limit-Pro-Interface

Definiert die maximal erlaubte Anzahl an IPv6-Neighbor-Cache Einträge pro Interface.

SNMP-ID:

2.70.16.2

Pfad Konsole:

Setup > **IPv6** > **NDP**

Mögliche Werte:

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

Default-Wert:

10000

5 Virtual Private Networks – VPN

5.1 LANCOM Advanced Mesh VPN (AMVPN)

Klassische VPN-Szenarien in der Standortvernetzung sind in der Regel sternförmig (Hub & Spoke) aufgebaut. Dabei bauen die angebundenen Filialen (Spokes) VPN-Tunnel zu einer oder mehreren Zentralen (Hubs) auf. In solchen traditionellen Szenarien ist ein Hub & Spoke-Netzwerk-Design eine logische Topologieentscheidung, denn es fließen Daten hauptsächlich zwischen Filiale und Zentrale, da dort zentrale Server stehen, z. B. das Warenwirtschaftssystem, Datenbanken oder Webserver.

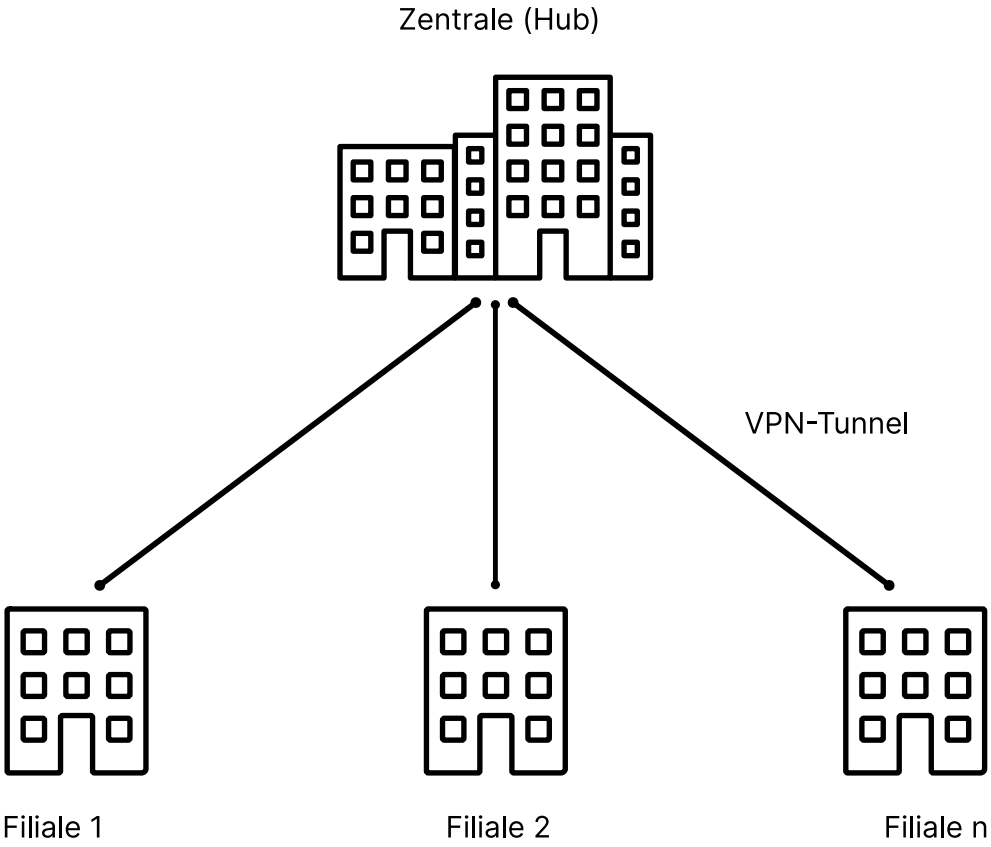


Abbildung 1: Klassische Standortvernetzung (Hub & Spoke)

Die Vorteile dieses sternförmigen Netzwerkdesigns sind der einfache Aufbau und die zentrale Steuerung in der Zentrale. Der Nachteil ist jedoch, dass sämtlicher Datenverkehr - auch der zwischen einzelnen Filialen wie z. B. Telefonie oder Dateiaustausch über einen File-Server - immer über den indirekten Weg über die Zentrale erfolgt. Dadurch wird die

Internetanbindung der Zentrale mit dem Datenverkehr zwischen den Filialen belastet und somit zum Flaschenhals der gesamten Kommunikation.

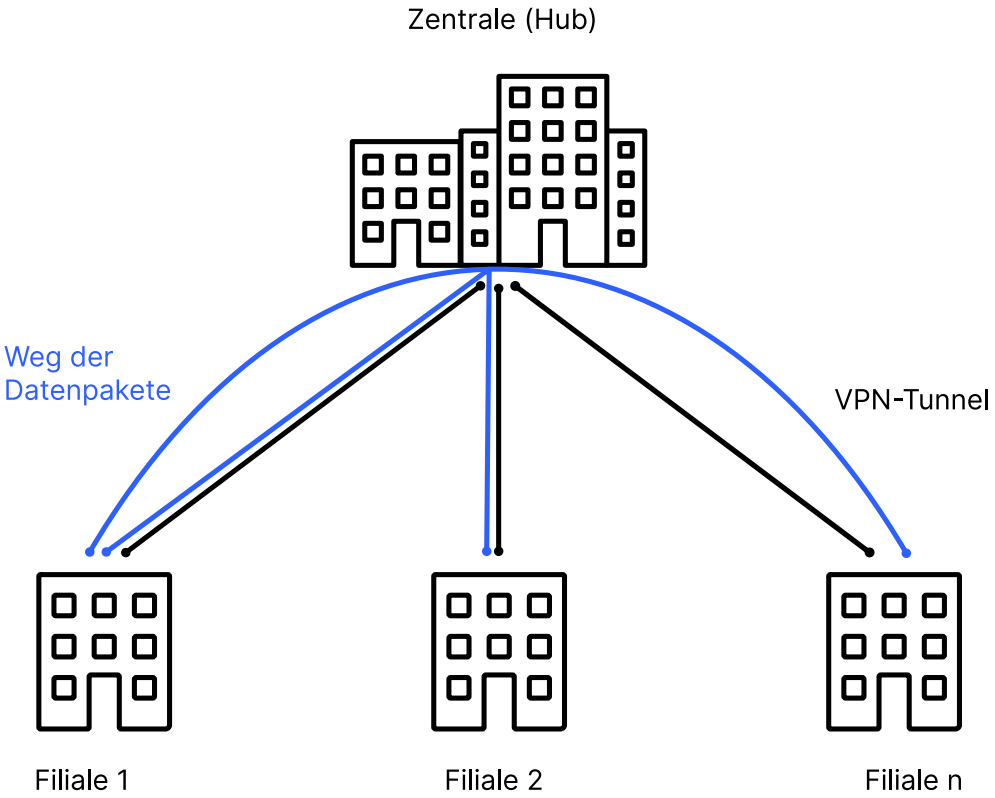


Abbildung 2: Datenaustausch zwischen Filialen bei klassischer Standortvernetzung (Hub & Spoke)

Wenn der Datenverkehr zwischen den Filialen der größte Anteil der Verkehrsbeziehung darstellt, ist es ein praktischer Lösungsansatz, direkte VPN-Tunnel zwischen den Filialen manuell zu konfigurieren. In diesem Fall spricht man von einem VPN-Mesh-Szenario. In einfachen Szenarien funktioniert dieser manuelle Ansatz noch gut. Wenn es allerdings viele Filialen gibt und viele mögliche VPN-Tunnel, so skaliert dieser starre, einzeln und fest konfigurierte Ansatz nicht mehr.

LANCOM bietet für dieses Szenario die Lösung „Advanced Mesh VPN“. Hierbei besteht zunächst eine klassische sternförmige VPN-Struktur, in der alle Filialen zu Beginn einen VPN-Tunnel zur Zentrale aufbauen. Gibt es nun Datenverkehr zwischen den Filialen, so wird dynamisch ein VPN-Tunnel als Abkürzung zwischen den beiden beteiligten Filialen aufgebaut. Die Daten fließen nun direkt in einem VPN-Tunnel zwischen den Filialen, ohne dass die Daten den Weg über die Zentrale gehen.

Dabei fließen nur die ersten Datenpakete immer den langen Weg von der Filiale A über die Zentrale zur zweiten Filiale B. Erst beim Empfang der ersten Datenpakete in der Zielfiliale initiiert die Zielfiliale einen dynamischen VPN-Tunnel zur Filiale mit dem Ursprung des Datenpakets. Fließen nach einiger Zeit keinen Daten mehr, so wird der Tunnel dynamisch wieder abgebaut.

Der Vorteil: Deutlich weniger Traffic in der Zentrale und einhergehend höhere Performance im gesamten Unternehmensnetzwerk.

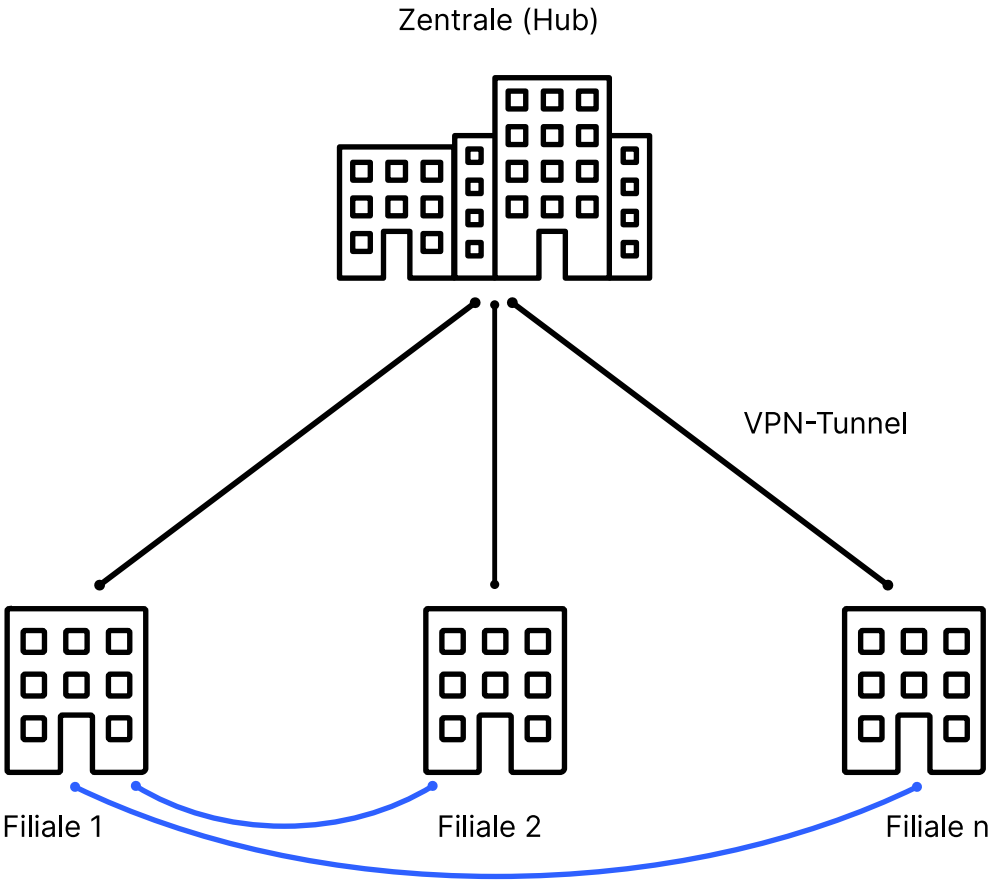


Abbildung 3: Standortvernetzung über Advanced Mesh VPN

Folgende grundsätzlichen Schritte sind zur Konfiguration von Advanced Mesh VPN notwendig:

1. Konfiguration der statischen VPN-Tunnel zwischen Filiale und Zentrale.
2. Anlegen einer Mesh-VPN-Tunnel-Vorlage (Template) in der IKEv2-Gegenstellen-Tabelle, die die gemeinsamen VPN-Eigenschaften wie Verschlüsselung, PSK oder Zertifikat für die dynamischen Mesh-VPN-Tunnel enthält.
3. Aktivierung der Mesh-VPN-Funktionalität und Konfiguration der globalen Mesh-Parameter auf allen beteiligten VPN-Routern.

Wie erfolgt der dynamische Aufbau eines Mesh-VPNs?

1. Filiale A sendet Datenpakete in den VPN-Tunnel über den bestehenden statischen VPN-Tunnel zur Zentrale an Filiale B.
2. Der Router in Filiale B erkennt eine neue Session, da Datenpakete von einem unbekannten Subnetz in dem VPN-Tunnel von der Zentrale ankommen.
3. Filiale B sendet eine verschlüsselte herstellerspezifischen IKEv2-Nachricht an die Zentrale. Die Nachricht enthält die privaten Subnetze bzw. IP-Adressen der gewünschten Kommunikationsbeziehung und die öffentliche IP-Adresse der Filiale B.
4. Die Zentrale empfängt die herstellerspezifische IKEv2-Nachricht im VPN-Tunnel von Filiale B und leitet sie über den VPN-Tunnel, der zur Filiale A führt, an Filiale A.
5. Filiale A empfängt die herstellerspezifische IKEv2-Nachricht der Zentrale.

6. Filiale A erzeugt einen dynamischen Mesh-VPN-Tunnel und baut diesen direkt zur IP-Adresse der Filiale B auf. Die notwendigen Informationen zum Aufbau des Tunnels entnimmt der Router aus der herstellerspezifische IKEv2-Nachricht (Gateway IP-Adresse, Subnetz etc.).
7. Filiale B nimmt den Tunnelaufbau von Filiale A an und aktualisiert ihre lokale Routing-Tabelle auf das Subnetz von Filiale A mit Ziel-Gateway der öffentlichen IP-Adresse von Filiale A. Das private Subnetz der Filiale A wird per IKEv2-Routing als IKEv2-Nachricht während des VPN-Tunnelaufbaus verwendet und ist spezifischer als die Route in die Zentrale.
8. Es fließen nun Daten direkt zwischen Filiale A und B, da die Routen auf beiden Seiten auf den dynamischen VPN-Tunnel zeigen.
9. Werden nach einem Timeout keine Daten mehr übertragen, so wird der Mesh-VPN-Tunnel abgebaut.

- Die ersten Datenpakete fließen immer zuerst über den Tunnel zur Zentrale und lösen dann den Aufbau eines dynamischen Tunnels aus.
- Ein Ping auf die LAN-IP-Adresse des Routers der Gegenseite löst keinen Mesh-VPN-Tunnelaufbau aus. Nur Datenpakete an Endpunkte im LAN lösen einen Tunnelaufbau aus, da nur diese von der Router-Firewall korrekt erkannt werden können. Ein Ping an eine (ggf. nichtexistierende) IP-Adresse im LAN löst aber den Aufbau eines VPN-Mesh-Tunnels aus.
- Bestehende Firewall-Sessions der ersten Datenpakete über die Zentrale werden nach erfolgreichem VPN-Mesh-Tunnelaufbau auf den neu aufgebauten Mesh-Tunnel umgezogen (Session Switchover).
- Die Filiale, die einen dynamischen VPN-Mesh-Tunnel annehmen soll, muss über eine öffentliche IP-Adresse (IPv4 oder IPv6) verfügen und von außen erreichbar sein. Router mit einer Mobilfunkverbindung verfügen in der Regel nicht über eine öffentliche IP-Adresse.
- LANCOM Advanced Mesh VPN ist eine herstellerspezifische Implementierung basierend auf IKEv2 und funktioniert nur zwischen LCOS-basierten LANCOM VPN-Routern. Der LANCOM Advanced VPN Client unterstützt dies nicht.
- Die Sicherheit basiert vollständig auf IKEv2 / IPSec und kann alle Einstellungen wie PSK, Zertifikate, Verschlüsselungsalgorithmen oder LANCOM HSVPN von IKEv2 verwenden.
- Alle beteiligten Router (Filiale, Zentrale) benötigen LCOS 10.70 oder höher.

Für Traces des LANCOM Advanced Mesh VPN wurde der Parameter `VPN-Mesh` hinzugefügt.

5.1.1 Lizenzierung

Mesh-VPN-Tunnel werden separat und zusätzlich zu den normalen VPN-Tunneln gezählt. Sind die Lizenzen für Mesh-VPN-Tunnel erschöpft, so wird kein Mesh-Tunnel aufgebaut und die Daten laufen weiterhin den längeren Weg über die Zentrale. Zentralseitige Geräte sind auf 200 Mesh-Tunnel in allen Ausbaustufen begrenzt.

Die folgenden Mesh-VPN-Lizenzen gelten (in Abhängigkeit der Anzahl der normalen VPN-Tunnel):

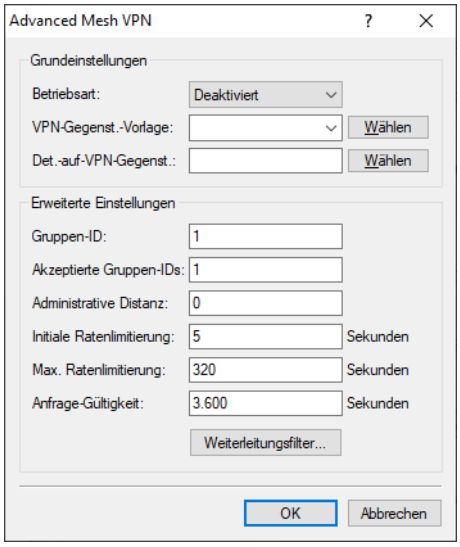
Tabelle 1: Mesh-VPN-Tunnel-Lizenzen

Kategorie	Geräte	Anzahl Lizenzen	
		VPN-Tunnel	Mesh-VPN-Tunnel
CPE	R88x, 88x VoIP, 1640E	3	6
CPE	179x, 18xx	5	10
CPE	179x, 18xx mit VPN 25	25	50
CPE	19xx	25	50
CPE	19xx mit VPN 50	50	100
CPE	19xx mit VPN 100	100	200
Zentrale	ISG-1000	100	200

Kategorie	Geräte	Anzahl Lizenzen	
		VPN-Tunnel	Mesh-VPN-Tunnel
Zentrale	ISG-4000	200	200
Zentrale	ISG-5000	100	200
Zentrale	ISG-8000	250	200

5.1.2 Advanced Mesh VPN konfigurieren

Konfigurieren Sie Advanced Mesh VPN in LANconfig unter **VPN** > **IKEv2 / IPSec** > **Erweiterte Einstellungen** > **Advanced Mesh VPN**.



Betriebsart

Dieser Schalter beeinflusst die Arbeitsweise des Mesh-VPNs und aktiviert das Verhalten als Spoke oder Hub oder beide Rollen gleichzeitig. Mögliche Werte:

Deaktiviert

Die Mesh-VPN-Funktion ist deaktiviert, die Mesh-Nachrichten werden nicht gesendet, weitergeleitet oder verarbeitet. Mesh-VPN-Tunnel können weder aufgebaut noch angenommen werden.

Hub

Das Gerät übernimmt die Rolle des zentralseitigen VPN-Gateways. Die Mesh-Nachrichten werden zwischen den Tunneln weitergeleitet. Das Gerät baut selber keine Mesh-VPN-Tunnel auf oder nimmt sie an.

Spoke

Das Gerät übernimmt die Funktion einer Filiale und baut Mesh-VPN-Tunnel auf und nimmt diese an.

Hub&Spoke

Das Gerät übernimmt die Rolle des zentralseitigen VPN-Gateways und baut außerdem noch Mesh-VPN-Tunnel zu anderen Spokes auf und nimmt Mesh-VPN-Tunnel an.

VPN-Gegenstellen-Vorlage

Dieser Parameter verweist auf einen Eintrag in der IKEv2-Gegenstellen-Tabelle. Dieser Eintrag wird als Konfigurationsvorlage für die Mesh-VPN-Tunnel verwendet.

Detektiere auf VPN-Gegenstelle

Eine kommaseparierte Liste von VPN-Gegenstellen, auf die der (Firewall-)Detektor reagieren soll. Dieser Eintrag wird auf Filialen benötigt, um eingehende Sessions zu detektieren. Kann leer gelassen werden bspw. auf Filialen, die hinter einem NAT (ohne Portforwarding) stehen und daher nicht als Responder eines Mesh-Tunnels fungieren können.

Gruppen-ID

Jedes Gerät kann einer Gruppe zugeordnet werden, mit der die eigenen Requests versendet werden. Damit wird es möglich das Mesh in kleinere Gruppen zu unterteilen, z. B. regionale Mesh-Strukturen.

Akzeptierte Gruppen-IDs

Eine kommaseparierte Liste, die angibt, welche Mesh-Gruppen-IDs akzeptiert werden. Eine Anfrage von einer Gruppen-ID, die nicht unter diesem Punkt aufgeführt ist, wird verworfen.

Administrative Distanz

Die Distanz, mit der die über den Mesh-Tunnel erhaltenen Routen beim IP-Router eingetragen werden. Der Sonderwert „0“ ist gleichbedeutend mit dem internen Default von „15“.

Initiale Ratenlimitierung

Um das Netzwerk zu schonen, werden angeforderte Netze (Adressen) mit einer zeitlichen Sperre versehen. Hier wird die initiale Sperrzeit in Sekunden angegeben.

Max. Ratenlimitierung

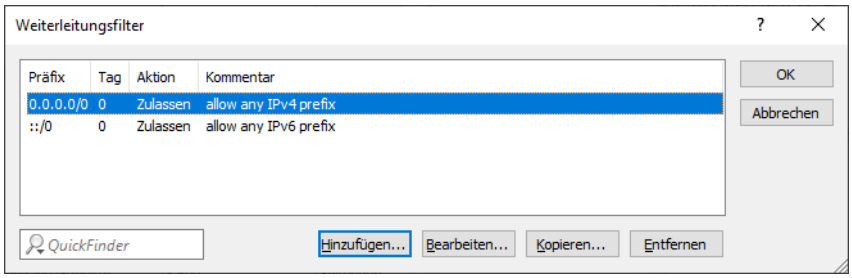
Die Sperrzeit aus der **Initialen Ratenlimitierung** wird jeweils verdoppelt, bis die **Maximale Ratenlimitierung** erreicht wird.

Anfrage Gültigkeit

Nach Ablauf der Sperrzeit werden bereits angefragte Netze (Adressen) weiter vorgehalten. Diese Gültigkeit beginnt immer mit Ablauf der Sperre und bricht ab, wenn das Gerät einen Request für dieses Netzwerk (diese Adresse) sendet oder empfängt.

Weiterleitungsfilter

Mithilfe dieser Filterliste können Anfragen an bestimmte Netzwerke auf dem Hub gefiltert werden. Wenn das angefragte Netzwerk aus einer Mesh-Nachricht mit keiner Tabellenzeile übereinstimmt, wird die Anfrage durchgelassen (Allow-All).



Präfix

Definiert das Präfix, für das eine Regel gelten soll, z. B. 10.0.0.0/24 oder 2001:db8::/32.

Tag

Definiert das zugehörige Routing Tag bzw. den Routing-Kontext zu dem die Filterregel gehört.

Aktion

Definiert die Aktion für diesen Filtereintrag. Mögliche Werte: Zulassen, Ablehnen.

Kommentar

Vergeben Sie diesem Eintrag einen aussagekräftigen Kommentar.

5.1.3 Tutorial: Einrichtung von Advanced Mesh VPN

Ausgangsszenario: Das Szenario besteht aus zwei Filialen (A und B) mit öffentlichen IPv4-Adressen sowie einer Zentrale, ebenfalls mit einer öffentlichen IPv4-Adresse. Die beiden Filialen haben bereits einen statischen IKEv2-VPN-Tunnel zur Zentrale eingerichtet, der aufgebaut ist. Die VPN-Gegenstelle auf den Filialen heißt jeweils „ZENTRALE". Filiale A hat das Subnetz 192.168.1.0/24 und Filiale B das Subnetz 192.168.2.0/24 mit dem Namen „INTRANET".

Konfiguration der Filiale A

1. Legen Sie einen neuen Eintrag, z. B. „MESH-TEMPLATE", in der IKEv2-Verbindungsliste unter **VPN** > **IKEv2 / IPSec** > **Verbindungs-Liste** an.

   Dieser Eintrag dient als Vorlage, aus der die dynamischen Mesh-Tunnel ihre Parameter übernehmen.

2. Als **Haltezeit** wird die Zeit konfiguriert, nach der die Mesh-VPN-Tunnel ohne Datenverkehr getrennt werden sollen, z. B. 300 Sekunden.

   Eine Deaktvierung der Haltezeit über den Wert 0 wird nicht empfohlen, da dynamische Mesh-VPN-Tunnel niemals bei Inaktivität abgebaut werden und Lizenzen verbrauchen.

3. Das **entfernte Gateway** muss leer gelassen werden, da es dynamisch bestimmt wird.
4. Über den Parameter **Routing** wird das lokale Netz an die gegenüberliegende Filiale übertragen, in diesem Fall das Netz „INTRANET".
5. Wählen Sie unter **Authentifizierung** die Option **Quelle verwalten** aus. Erzeugen Sie einen neuen Eintrag, z. B. „MESH". Geben Sie die **lokale Identität** der Filiale an, sowie den **PSK**, der für alle dynamischen Mesh-Tunnel verwendet wird. Der PSK muss auf allen beteiligten Filialen für den Mesh-VPN-Tunnel identisch sein. Lassen Sie das

Feld **entfernte Identität** leer und wählen Sie die Option „Keine Identität" für **entfernter Identitätstyp**, so dass alle ankommenden Identitäten mit dem korrekten PSK als Mesh-Tunnel akzeptiert werden.

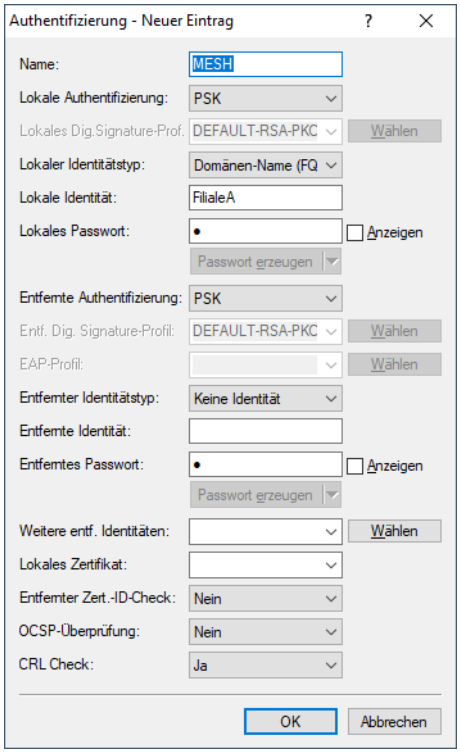


Abbildung 4: Beispiel für die Authentifizierungs-Einstellungen

6. Setzen Sie die **VPN-Regel** auf „ANY". Somit wird 0.0.0.0/0 <=> 0.0.0.0/0 verwendet.
7. Setzen Sie die **Regelerzeugung** auf „Manuell".

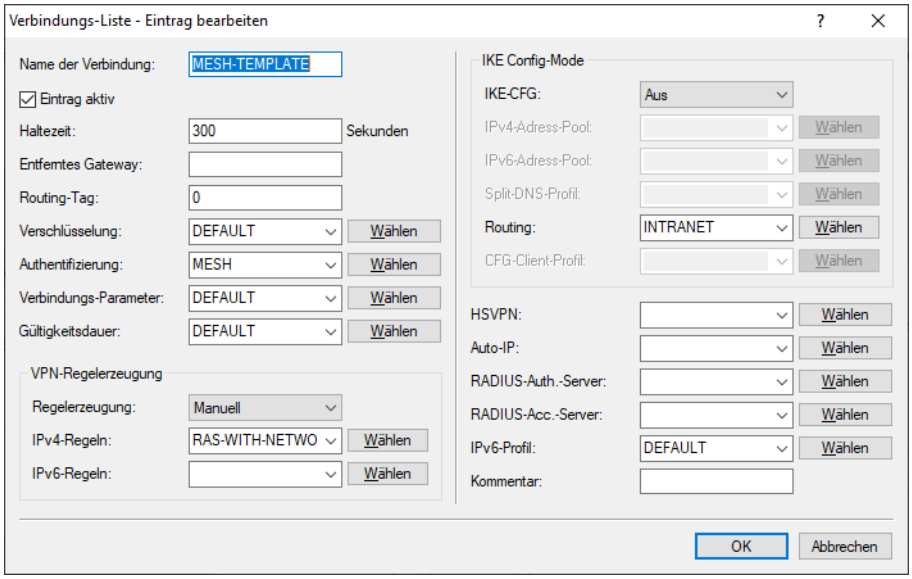


Abbildung 5: Beispiel für das Mesh-VPN-Template in der Verbindungs-Liste

8. Konfigurieren Sie nun die Mesh-VPN-Parameter unter **VPN** > **IKEv2 / IPSec** > **Erweiterte Einstellungen** > **Advanced Mesh VPN**.

9. Setzen Sie die **Betriebsart** auf „Spoke“.
10. Wählen Sie unter **VPN-Gegenstellen-Vorlage** die zuvor angelegte IKEv2-Gegenstelle als Vorlage für die Mesh-VPN-Tunnel aus.
11. Wählen Sie unter **Detektiere auf VPN-Gegenstelle** den Namen der VPN-Gegenstelle aus, der dem Namen des Tunnels zur Zentrale entspricht.

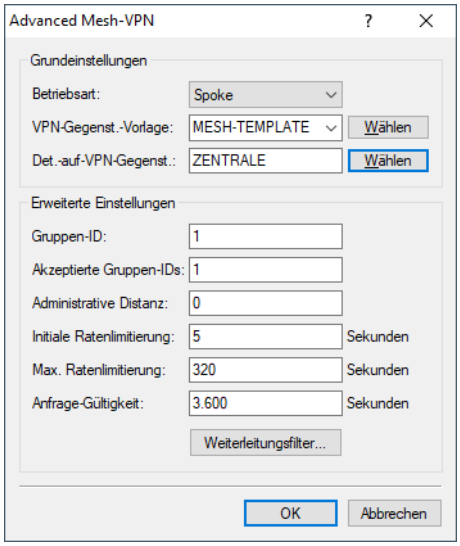


Abbildung 6: Beispiel für die Advanced Mesh VPN-Einstellungen in der Filiale

Konfiguration der Filiale B

12. Die Konfiguration erfolgt analog zur Filiale A. Ändern Sie die **lokale Identität** bei der **Authentifizierung**entsprechend auf den Namen der Filiale B.

Konfiguration der Zentrale

13. Da die Zentrale selbst keine dynamischen Mesh-Tunnel aufbaut, wird auch keine Gegenstellen-Vorlage angelegt. Setzen Sie die **Betriebsart** bei Advanced Mesh VPN auf „Hub“.

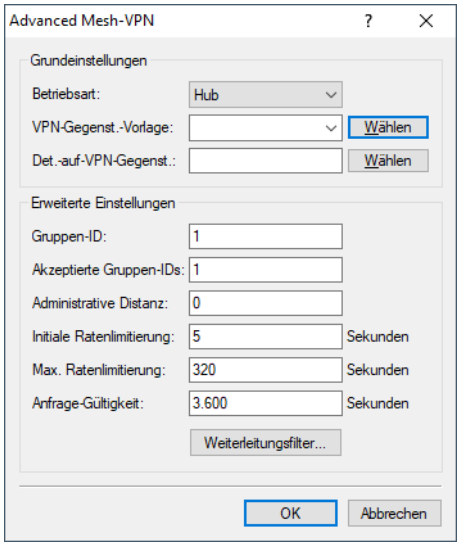


Abbildung 7: Beispiel für die Advanced Mesh VPN-Einstellungen in der Zentrale

Wenn Sie nun Daten von der Filiale A an Filiale B übertragen, so gehen die ersten Pakete über den Umweg der Zentrale. Daraufhin wird der dynamische Mesh-Tunnel zwischen den Filialen aufgebaut.

Ein Ping auf die IP-Adresse des Routers der gegenüberliegenden Seite wird keinen Mesh-Tunnel aufbauen. Es muss eine (ggf. nichtexistierende) Station im LAN der anderen Seite als Ziel verwendet werden.

5.1.4 Ergänzungen im Setup-Menü

Mesh

Hier werden die Einstellungen für LANCOM Advanced Mesh VPN (AMVPN) vorgenommen.

SNMP-ID:

2.19.36.35

Pfad Konsole:

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

Betriebsart

Dieser Parameter beeinflusst die Arbeitsweise des Mesh-VPNs und aktiviert das Verhalten als Spoke oder Hub oder beide Rollen gleichzeitig.

SNMP-ID:

2.19.36.35.1

Pfad Konsole:

Setup > **VPN** > **IKEv2** > **Mesh**

Mögliche Werte:

Inaktiv
Spoke
Hub

Default-Wert:

Inaktiv

Admin-Distanz

Die Distanz, mit der die über den Mesh-Tunnel erhaltenen Routen beim IP-Router eingetragen werden.

SNMP-ID:

2.19.36.35.2

Pfad Konsole:

Setup > **VPN** > **IKEv2** > **Mesh**

Mögliche Werte:

0 … 255

Besondere Werte:

0

Gleichbedeutend mit dem internen Default von „15“

Default-Wert:

0

VPN-Gegenstellen-Template

Dieser Parameter verweist auf einen Eintrag in der IKEv2-Gegenstellen-Tabelle. Dieser Eintrag wird als Konfigurationsvorlage für die Mesh-VPN-Tunnel verwendet.

SNMP-ID:

2.19.36.35.3

Pfad Konsole:

Setup > **VPN** > **IKEv2** > **Mesh**

Mögliche Werte:

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

Default-Wert:

leer

Initiale-Ratenlimitierung-Sek

Um das Netzwerk zu schonen, werden angeforderte Netze (Adressen) mit einer zeitlichen Sperre versehen. Hier wird die initiale Sperrzeit in Sekunden angegeben.

SNMP-ID:

2.19.36.35.4

Pfad Konsole:

Setup > **VPN** > **IKEv2** > **Mesh**

Mögliche Werte:

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

Default-Wert:

5

Max-Ratenlimitierung-Sek

Die Sperrzeit aus *2.19.36.35.4 Initiale-Ratenlimitierung-Sek* auf Seite 43 wird jeweils verdoppelt, bis der hier eingestellte Wert erreicht wird.

SNMP-ID:

2.19.36.35.5

Pfad Konsole:

Setup > **VPN** > **IKEv2** > **Mesh**

Mögliche Werte:

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

Default-Wert:

320

Anfrage-Gueltigkeit-Sek

Nach Ablauf der Sperrzeit werden bereits angefragte Netze (Adressen) weiter vorgehalten. Diese Gültigkeit beginnt immer mit Ablauf der Sperre und bricht ab, wenn das Gerät einen Request für dieses Netzwerk (diese Adresse) sendet oder empfängt.

SNMP-ID:

2.19.36.35.6

Pfad Konsole:

Setup > **VPN** > **IKEv2** > **Mesh**

Mögliche Werte:

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

Default-Wert:

3600

Gruppen-ID

Jedes Gerät kann einer Gruppe zugeordnet werden, mit der die eigenen Requests versendet werden. Damit wird es möglich das Mesh in kleinere Gruppen zu unterteilen, z. B. regionale Mesh-Strukturen.

SNMP-ID:

2.19.36.35.7

Pfad Konsole:

Setup > **VPN** > **IKEv2** > **Mesh**

Mögliche Werte:

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

Default-Wert:

1

Akzeptierte-Gruppen-IDs

Eine kommaseparierte Liste, die angibt, welche Mesh-Gruppen-IDs akzeptiert werden. Eine Anfrage von einer Gruppen-ID, die nicht unter diesem Punkt aufgeführt ist, wird verworfen.

SNMP-ID:

2.19.36.35.8

Pfad Konsole:

Setup > **VPN** > **IKEv2** > **Mesh**

Mögliche Werte:

max. 253 Zeichen aus `[0-9],`

Default-Wert:

1

Detektiere-auf-VPN-Gegenstellen

Eine kommaseparierte Liste von VPN-Gegenstellen, auf die der (Firewall-)Detektor reagieren soll. Dieser Eintrag wird auf Filialen benötigt, um eingehende Sessions zu detektieren. Kann leer gelassen werden bspw. auf Filialen, die hinter einem NAT (ohne Portforwarding) stehen und daher nicht als Responder eines Mesh-Tunnels fungieren können.

SNMP-ID:

2.19.36.35.9

Pfad Konsole:

Setup > **VPN** > **IKEv2** > **Mesh**

Mögliche Werte:

max. 253 Zeichen aus `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default-Wert:

leer

Weiterleitungs-Filter

Mithilfe dieser Filterliste können Anfragen an bestimmte Netzwerke auf dem Hub gefiltert werden. Wenn das angefragte Netzwerk aus einer Anfrage per herstellerspezifischer IKEv2-Nachricht mit keiner Tabellenzeile übereinstimmt, wird die Anfrage durchgelassen (Allow-All).

SNMP-ID:

2.19.36.35.10

Pfad Konsole:

Setup > **VPN** > **IKEv2** > **Mesh**

IP-Adressen-Praefix

Definiert das Präfix, für das eine Regel gelten soll, z. B. 10.0.0.0/24 oder 2001:db8::/32.

SNMP-ID:

2.19.36.35.10.1

Pfad Konsole:

Setup > **VPN** > **IKEv2** > **Mesh** > **Weiterleitungs-Filter**

Mögliche Werte:

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

Rtg-Tag

Definiert das zugehörige Routing Tag bzw. den Routing-Kontext zu dem die Filterregel gehört.

SNMP-ID:

2.19.36.35.10.2

Pfad Konsole:

Setup > **VPN** > **IKEv2** > **Mesh** > **Weiterleitungs-Filter**

Mögliche Werte:

0 … 65535

Default-Wert:

0

Filter-Aktion

Definiert die Aktion für diesen Filtereintrag.

SNMP-ID:

2.19.36.35.10.3

Pfad Konsole:

Setup > **VPN** > **IKEv2** > **Mesh** > **Weiterleitungs-Filter**

Mögliche Werte:

erlaubt
verboten

Kommentar

Vergeben Sie diesem Eintrag einen aussagekräftigen Kommentar.

SNMP-ID:

2.19.36.35.10.4

Pfad Konsole:

Setup > **VPN** > **IKEv2** > **Mesh** > **Weiterleitungs-Filter**

Mögliche Werte:

max. 253 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default-Wert:

leer

5.2 Zwei-Faktor-Authentifizierung im VPN

Ab LCOS 10.70 unterstützt LCOS die VPN-Zwei-Faktor-Authentifizierung (EAP-OTP) mit dem LANCOM Advanced VPN Client. Dazu kann der interne RADIUS-Server OTP-Benutzer verwalten.

Der VPN-Benutzer hat neben seinem normalen VPN-Benutzernamen und Passwort (EAP-MSCHAPv2) eine Authenticator-App z. B. auf seinem Smartphone, auf der ein zweiter Faktor generiert wird und zusätzlich zum Benutzernamen / Passwort verwendet wird. Zwei-Faktor-Authentifizierung ist bei IKEv2 laut RFC nur mit EAP möglich, so dass einfache PSK oder RSA-Signature-Verfahren nicht verwendet werden können. LCOS unterstützt eine herstellerspezifische Implementierung zusammen mit dem LANCOM Advanced VPN Client.

Als Authenticator können beliebige Apps verwendet werden, z. B. von Google, Microsoft oder NCP. Diese Apps finden Sie im Appstore Ihres mobilen Geräts.

Die Vorgehensweise zur Einrichtung ist wie folgt: Zunächst muss EAP-VPN mit IKEv2 im LANCOM Gerät konfiguriert werden. Dazu wird der interne RADIUS-Server mit seinen Benutzerkonten verwendet. Zusätzlich zu einem RADIUS-Benutzerkonto muss ein OTP-Benutzer anlegt werden. Im Anschluss kann in der WEBconfig unter **Extras** > **EAP-OTP-Benutzer** ein QR-Code abgerufen werden, der von der Authenticator-App eingescannt werden muss. Dieser QR-Code gilt pro Benutzer und muss jedes Mal verwendet werden, wenn eine Authenticator-App eingerichtet werden soll. Die WEBconfig generiert aus den Parametern der Tabelle **OTP-Benutzerkonten** einen QR-Code pro Benutzer der

von Authenticator-Apps eingescannt werden kann. Alternativ kann in den meisten Apps der Schlüssel manuell hinzugefügt werden.

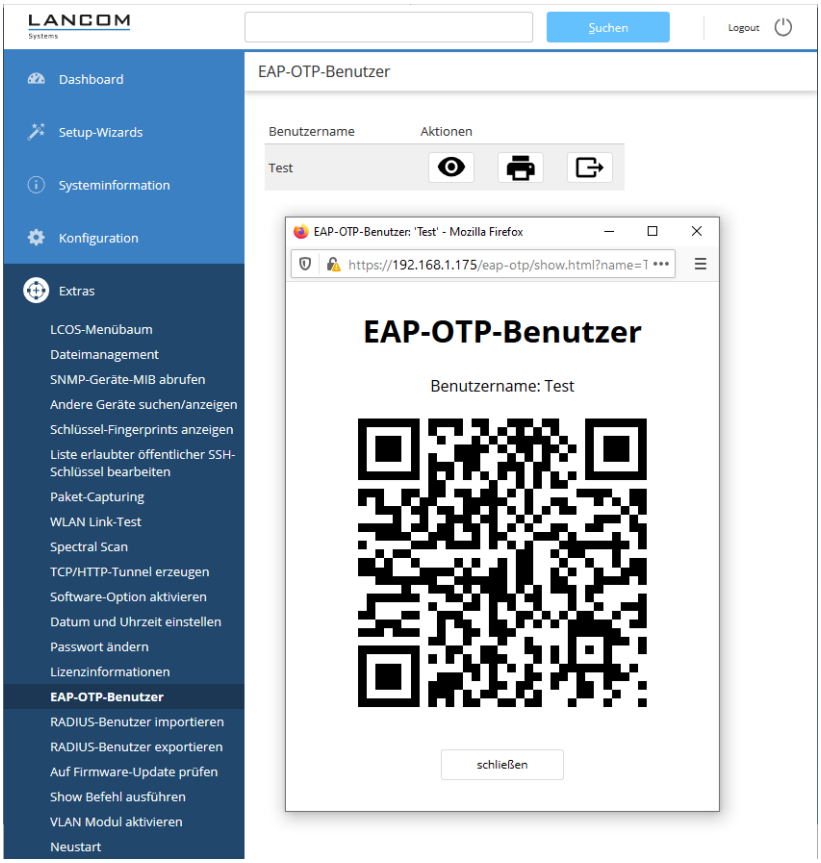


Abbildung 8: WEBconfig: Extras > EAP-OTP-Benutzer

Eine Anleitung zur Einrichtung des gesamten Szenarios finden Sie in der *LANCOM Support Knowledge Base*.

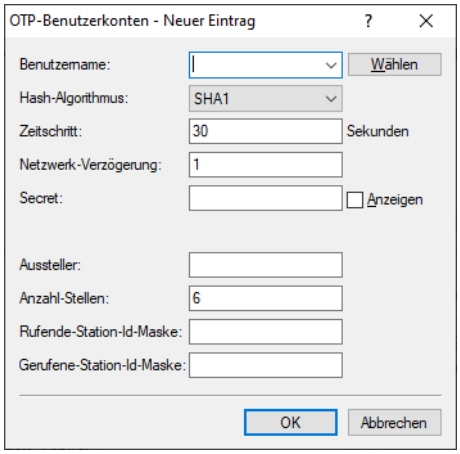
Bitte beachten Sie, dass für eine korrekte zeitliche Synchronisierung mit dem Authenticator der Router über die aktuelle Uhrzeit verfügen muss. Aktivieren Sie dazu den NTP-Client im Router unter **Datum/Zeit** > **Synchronisierung** > **NTP-Client-Einstellungen**.

5.2.1 Konfiguration mit LANconfig

OTP-Benutzerkonten

In der Tabelle OTP-Benutzerkonten werden die OTP-Benutzer definiert. Für EAP-OTP muss der Benutzer mit seinem normalen Passwort in der Tabelle der RADIUS-Benutzerkonten angelegt werden, sowie zusätzlich in dieser Tabelle mit dem OTP-Secret angelegt werden.

Die Konfiguration der OTP-Benutzerkonten erfolgt über **RADIUS** > **Server** > **Benutzer-Datenbank** > **OTP-Benutzerkonten**.



Benutzername

Geben Sie hier den Namen des OTP-Benutzers ein. Dieser muss in der Tabelle RADIUS-Benutzerkonten bereits mit gleichem Namen enthalten sein.

Hash-Algorithmus

Definiert den verwendeten Hash-Algorithmus.

Beachten Sie, dass die Authenticator-App den maximal möglichen Hash-Algorithmus unterstützt. Der Google Authenticator unterstützt aktuell z. B. auf bestimmten Android-Plattformen nur SHA1.

Zeitschritt

Definiert das Intervall in Sekunden, nach dem ein neues OTP berechnet wird. Default: 30 Sekunden

Netzwerk-Verzögerung

Definiert, um wie viele Zeitschritte die Uhr des Clients maximal abweichen darf. Der RADIUS-Server prüft das um diesen Wert ältere bzw. neuere OTP.

Secret

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

Base32 (Default)

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

Hexadezimal

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

Plain text passphrase

Präfix „ascii:“ und danach die Zeichen.

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

Aussteller

Frei definierbarer Text, der im Authenticator dazu dient, mehrere Schlüssel auseinanderzuhalten, wenn der gleiche Benutzername verwendet wird. Darf keinen Doppelpunkt enthalten.

Anzahl Stellen

Länge der OTPs. Default: 6.

Für den Google-Authenticator sollte der Wert 6 verwendet werden.

Rufende Station

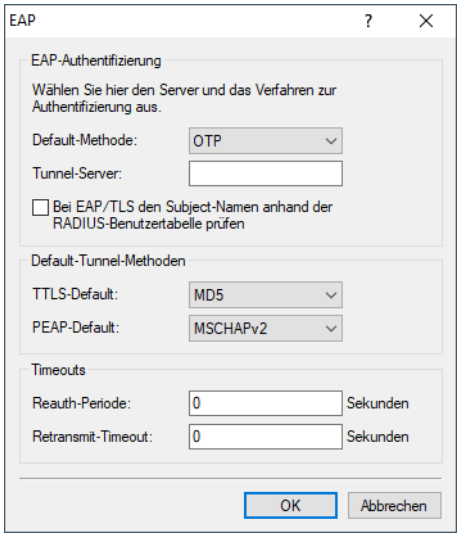
Diese Maske schränkt die Gültigkeit des Eintrags auf bestimmte IDs ein, die die rufende Station übermittelt.

Gerufene Station

Diese Maske schränkt die Gültigkeit des Eintrags auf bestimmte IDs ein, die die gerufene Station übermittelt.

EAP-OTP

RADIUS > **Server** > **Erweiterte Einstellungen** > **EAP**



Die **Default-Methode** wurde um den Wert OTP erweitert.

OTP

One Time Password. Dieser Wert muss bei EAP-OTP für die *Zwei-Faktor-Authentifizierung im VPN* verwendet werden, da beim LANCOM Advanced VPN-Client die EAP-Methode vom EAP-Server vorgegeben wird.

5.2.2 Ergänzungen im Setup-Menü

Vorgabe-Methode

Gibt an, welche Methode der RADIUS-Server dem Client außerhalb eines eventuellen TTLS/PEAP-Tunnels anbieten soll.

SNMP-ID:

2.25.10.10.7

Pfad Konsole:

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

Mögliche Werte:

Keine
MD5
GTC
MSCHAPv2
TLS
TTLS
PEAP
WFA-Unauth
OTP

Default-Wert:

MD5

EAP-OTP

Hier werden die Parameter für EAP-OTP festgelegt.

SNMP-ID:

2.25.10.10.20

Pfad Konsole:

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

Benutzer

In dieser Tabelle werden die OTP-Benutzer definiert.

SNMP-ID:

2.25.10.10.20.1

Pfad Konsole:

Setup > **RADIUS** > **Server** > **EAP** > **EAP-OTP**

Benutzername

Geben Sie hier den Namen des OTP-Benutzers ein. Dieser muss in der Tabelle RADIUS-Benutzerkonten bereits mit gleichem Namen enthalten sein.

SNMP-ID:

2.25.10.10.20.1.1

Pfad Konsole:

Setup > **RADIUS** > **Server** > **EAP** > **EAP-OTP** > **Benutzer**

Mögliche Werte:

max. 48 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default-Wert:

leer

Rufende-Station-Id-Maske

Diese Maske schränkt die Gültigkeit des Eintrags auf bestimmte IDs ein, die die rufende Station übermittelt.

SNMP-ID:

2.25.10.10.20.1.2

Pfad Konsole:

Setup > **RADIUS** > **Server** > **EAP** > **EAP-OTP** > **Benutzer**

Mögliche Werte:

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

Default-Wert:

leer

Gerufene-Station-Id-Maske

Diese Maske schränkt die Gültigkeit des Eintrags auf bestimmte IDs ein, die die gerufene Station übermittelt.

SNMP-ID:

2.25.10.10.20.1.3

Pfad Konsole:

Setup > **RADIUS** > **Server** > **EAP** > **EAP-OTP** > **Benutzer**

Mögliche Werte:

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

Default-Wert:

leer

Hash-Algorithmus

Definiert den verwendeten Hash-Algorithmus.

Beachten Sie, dass die Authenticator-App den maximal möglichen Hash-Algorithmus unterstützt. Der Google Authenticator unterstützt aktuell z. B. auf bestimmten Android-Plattformen nur SHA1.

SNMP-ID:

2.25.10.10.20.1.4

Pfad Konsole:

Setup > **RADIUS** > **Server** > **EAP** > **EAP-OTP** > **Benutzer**

Mögliche Werte:

SHA1
SHA256
SHA512

Default-Wert:

SHA1

Zeitschritt

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

SNMP-ID:

2.25.10.10.20.1.5

Pfad Konsole:

Setup > **RADIUS** > **Server** > **EAP** > **EAP-OTP** > **Benutzer**

Mögliche Werte:

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

Default-Wert:

30

Netzwerk-Verzoegerung

Definiert, um wie viele Zeitschritte die Uhr des Clients maximal abweichen darf. Der RADIUS-Server prüft das um diesen Wert ältere bzw. neuere OTP.

SNMP-ID:

2.25.10.10.20.1.6

Pfad Konsole:

Setup > **RADIUS** > **Server** > **EAP** > **EAP-OTP** > **Benutzer**

Mögliche Werte:

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

Secret

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

Base32 (Default)

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

Hexadezimal

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

Plain text passphrase

Präfix „ascii:" und danach die Zeichen.

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

SNMP-ID:

2.25.10.10.20.1.7

Pfad Konsole:

Setup > **RADIUS** > **Server** > **EAP** > **EAP-OTP** > **Benutzer**

Mögliche Werte:

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

Default-Wert:

leer

Anzahl-Stellen

Länge der OTPs.

Für den Google Authenticator sollte der Wert 6 verwendet werden.

SNMP-ID:

2.25.10.10.20.1.8

Pfad Konsole:

Setup > **RADIUS** > **Server** > **EAP** > **EAP-OTP** > **Benutzer**

Mögliche Werte:

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

Default-Wert:

6

Aussteller

Frei definierbarer Text, der im Authenticator dazu dient, mehrere Schlüssel auseinanderzuhalten, wenn der gleiche Benutzername verwendet wird. Darf keinen Doppelpunkt enthalten.

SNMP-ID:

2.25.10.10.20.1.9

Pfad Konsole:

Setup > **RADIUS** > **Server** > **EAP** > **EAP-OTP** > **Benutzer**

Mögliche Werte:

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

Default-Wert:

leer

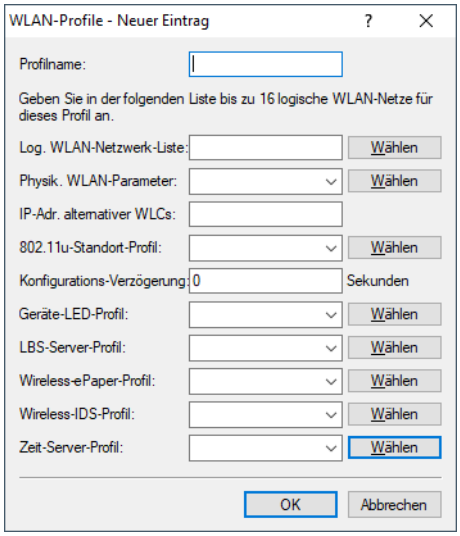
6 WLAN-Management

6.1 Unterstützung für NTP-Server im WLAN-Controller

Ab LCOS 10.70 unterstützt der WLAN-Controller die Angabe von Zeitservern (NTP) in den Profilen des WLAN-Controllers.

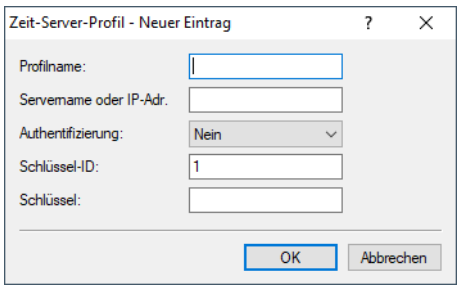
Der WLAN-Controller synchronisiert die Zeit mit einem Access Point, wenn er diesen annimmt. Hierdurch kann es vorkommen, dass ein lange verwalteter Access Point ohne neue Zeitinformationen größere Abweichungen vom WLAN-Controller hat und es dadurch ggf. zu Zertifikatsproblemen kommen kann. Durch die Verwendung eines Zeitservers kann dieses Problem nicht auftreten.

Unter **WLAN-Controller** > **Profile** > **WLAN-Profile** gibt es den neuen Parameter **Zeit-Server-Profil**:



Zeit-Server-Profil

Wählen Sie hier aus der Liste der Zeit-Server-Profile das Profil aus, das im WLAN-Profil gelten soll. Die Zeit-Server-Profile verwalten Sie unter **WLAN-Controller** > **Profile** > **Erweiterte Profile** mit der Schaltfläche **Zeit-Server-Profil**.



Profilname

Der Name dieses NTP-Profils.

Servername oder IP-Adresse

Der Servername oder die IP-Adresse des NTP-Servers.

Authentifizierung

Aktiviert bzw. deaktiviert die MD5-Authentifizierung für den Server.

Schlüssel-ID

Kennzeichnet den zur MD5-Authentifizierung verwendeten Schlüssel für den Server.

Schlüssel

Der Wert des Schlüssels für die Authentifizierung mit dem NTP-Server.

6.1.1 Ergänzungen im Setup-Menü

NTP-Profil

Der WLAN-Controller synchronisiert die Zeit mit einem Access Point, wenn er diesen annimmt. Hierdurch kann es vorkommen, dass ein lange verwalteter Access Point ohne neue Zeitinformationen größere Abweichungen vom WLAN-Controller hat und es dadurch ggf. zu Zertifikatsproblemen kommen kann. Durch die Verwendung eines Zeitservers kann dieses Problem nicht auftreten.

Wählen Sie aus der Liste der NTP-Profile unter *2.37.1.28 NTP-Profile* auf Seite 57 das Profil aus, das im WLAN-Profil gelten soll.

SNMP-ID:

2.37.1.3.12

Pfad Konsole:

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

Mögliche Werte:

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

Default-Wert:

leer

NTP-Profile

In dieser Tabelle finden Sie die definierten NTP-Profile der definierten Zeitserver.

SNMP-ID:

2.37.1.28

Pfad Konsole:

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

Name

Der Name dieses NTP-Profils.

SNMP-ID:

2.37.1.28.1

Pfad Konsole:

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

Mögliche Werte:

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

Default-Wert:

leer

RQ-Adresse

Der Servername oder die IP-Adresse des NTP-Servers.

SNMP-ID:

2.37.1.28.2

Pfad Konsole:

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

Mögliche Werte:

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

Default-Wert:

leer

Authentifizierung

Aktiviert bzw. deaktiviert die MD5-Authentifizierung für den Server.

SNMP-ID:

2.37.1.28.3

Pfad Konsole:

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

Mögliche Werte:

Nein

Deaktiviert

Ja

Aktiviert

Default-Wert:

Nein

Schluesselnummer

Kennzeichnet den zur MD5-Authentifizierung verwendeten Schlüssel für den Server.

SNMP-ID:

2.37.1.28.4

Pfad Konsole:

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

Mögliche Werte:

1 … 65535

Schluessel

Der Wert des Schlüssels für die Authentifizierung mit dem NTP-Server.

SNMP-ID:

2.37.1.28.5

Pfad Konsole:

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

Mögliche Werte:

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

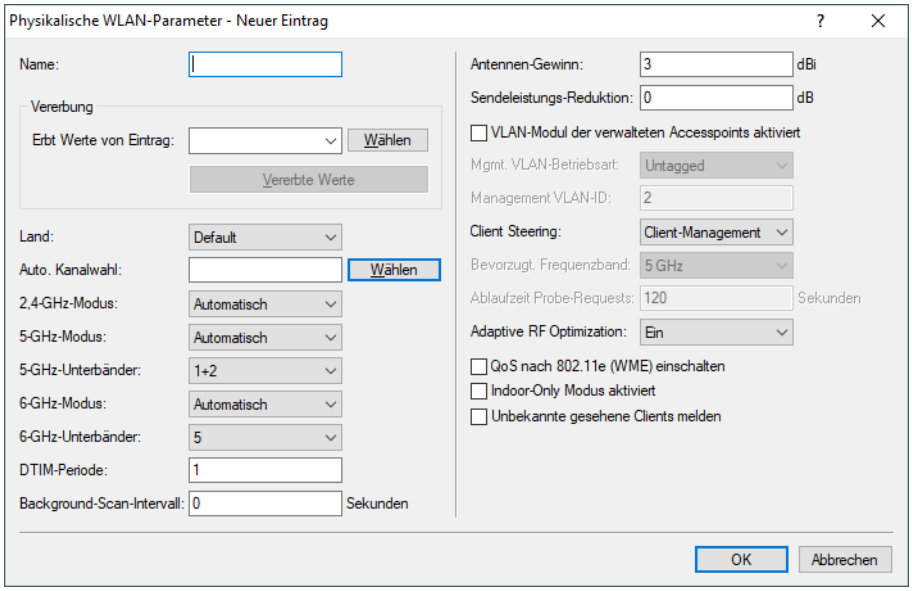
Default-Wert:

leer

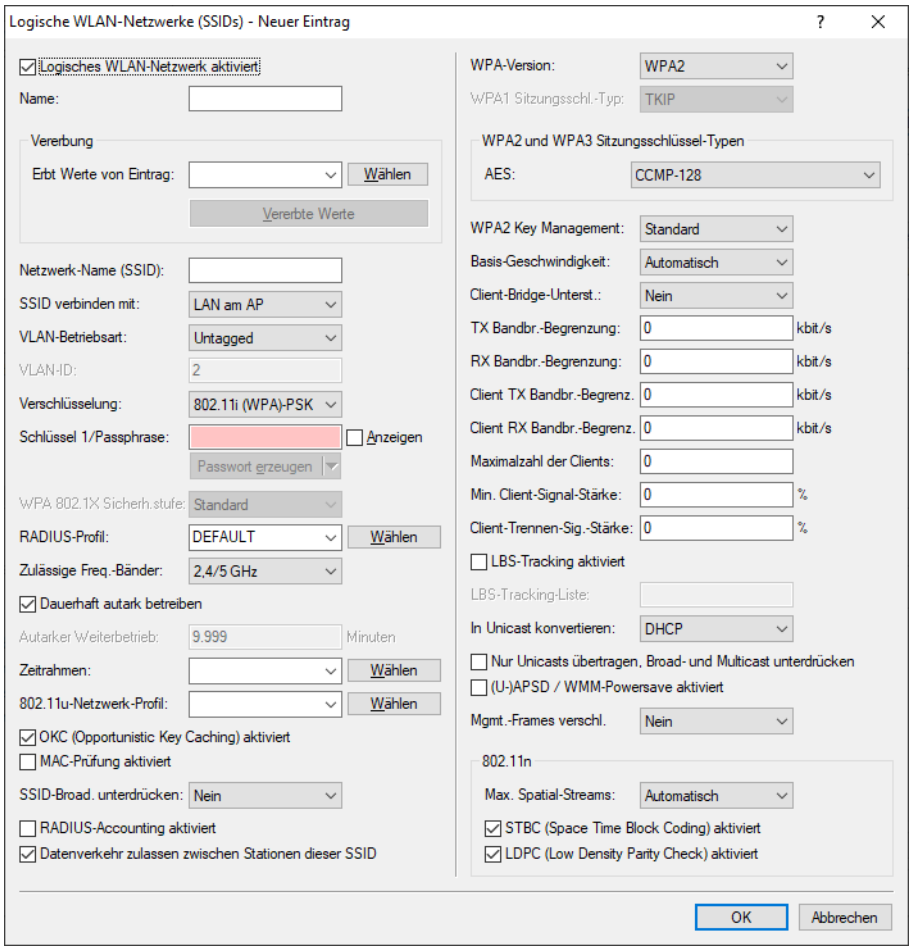
6.2 Unterstützung für drei Funkmodule und 6 GHz im WLAN-Controller

Ab LCOS 10.70 unterstützt der WLAN-Controller drei Funkmodule und das 6 GHz-Band in den Profilen des WLAN-Controllers.

Unter **WLAN-Controller** > **Profile** > **Physikalische WLAN-Parameter** wird dieser Modus und die zu verwendenden Unterbänder eingestellt.



Unter **WLAN-Controller** > **Profile** > **Logische WLAN-Netzwerke** wählen Sie bei den **Zulässige Freq.-Bänder** das 6 GHz-Band aus.



6.2.1 Ergänzungen im Setup-Menü

Band

Mit der Auswahl des Frequenzbandes legen Sie fest, ob die WLAN-Karte im 2,4 GHz-Band, 5 GHz-Band oder im 6 GHz-Band arbeitet, und damit gleichzeitig die möglichen Funkkanäle.

SNMP-ID:

2.37.1.1.10

Pfad Konsole:

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

Mögliche Werte:

Alle
2,4GHz
5GHz
6GHz

Default-Wert:

Alle

Unterbaender-6GHz

Im 6 GHz-Band kann neben dem Frequenzband ein Unterband gewählt werden, an das wiederum bestimmte Funkkanäle und maximale Sendeleistungen geknüpft sind.

SNMP-ID:

2.37.1.2.26

Pfad Konsole:

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

Mögliche Werte:

Band-5
Band-7
Band-5+7

6GHz-Modus

Geben Sie an, welche Funkstandards die von Ihnen konfigurierte physikalische WLAN-Schnittstelle gegenüber einem WLAN-Client im 6-GHz-Frequenzband unterstützt.

SNMP-ID:

2.37.1.2.27

Pfad Konsole:

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

Mögliche Werte:

Auto

Automatisch. Innerhalb des 6-GHz-Modus führt die Automatik zu 802.11ax.

Default-Wert:

Auto

WLAN-Modul-3

Frequenzband für das dritte WLAN-Modul. Mit diesem Parameter kann das WLAN-Modul auch deaktiviert werden.

SNMP-ID:

2.37.1.4.39

Pfad Konsole:

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

Mögliche Werte:

default

Dieser Wert übernimmt die Verschlüsselung von der Definition im Bereich „Optionen".

2,4GHz
5GHz
6GHz
Aus
Auto

Default-Wert:

default

Modul-3-Max.-Kanal-Bandbreite

Geben Sie an, wie und in welchem Umfang der AP die Kanal-Bandbreite für die 3. physikalische WLAN-Schnittstelle festlegt.

SNMP-ID:

2.37.1.4.40

Pfad Konsole:

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

Mögliche Werte:

Auto

Der AP erkennt automatisch die maximale Kanal-Bandbreite.

20MHz

Der AP benutzt auf 20 MHz gebündelte Kanäle.

40MHz

Der AP benutzt auf 40 MHz gebündelte Kanäle.

80MHz

Der AP benutzt auf 80 MHz gebündelte Kanäle.

80+80MHz

Der AP benutzt zwei auf 80 MHz gebündelte Kanäle.

160MHz

Der AP benutzt auf 160 MHz gebündelte Kanäle.

Default-Wert:

Auto

Module-3-Kanalliste

Mit dem Funkkanal wird ein Teil des theoretisch denkbaren Frequenzbandes für die Datenübertragung im Funknetz ausgewählt.

SNMP-ID:

2.37.1.4.41

Pfad Konsole:

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

Mögliche Werte:

max. 48 Zeichen aus `[A-Z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default-Wert:

leer

Modul-3-Ant-Gewinn-Modus

Bei der Inbetriebnahme von Access Points an einem WLAN-Controller wurden diese bisher immer mit einem Antennengewinn von 3 dBi je Modul eingerichtet, da dieser Wert für die meisten Indoor-Access Points mit Standardantennen passend ist. Insbesondere für Outdoor-Access Points mit integrierten Antennen musste der Wert aber in der Vergangenheit manuell angepasst werden, die hier häufig interne Antennen mit einem hohen Antennengewinn zum Einsatz kommen. Ab LCOS 10.30 wird der Standard-Antennengewinn eines verwalteten Access Points an den WLAN-Controller übertragen und dort automatisch verwendet. Für diese Funktion müssen sowohl der Access Point als auch der WLAN-Controller, mindestens den Firmware-Stand 10.30 aufweisen. Mit dieser Einstellung für den Modus des Antennengewinns wird verhindert, dass man nach einem Rollout einige Access Points noch manuell korrigieren muss.

SNMP-ID:

2.37.1.4.42

Pfad Konsole:

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

Mögliche Werte:

Standard

Der im Access Point voreingestellte Wert für den Antennengewinn wird verwendet.

benutzerdefiniert

Der Wert aus **Module-3-Ant-Gewinn** wird verwendet.

Default-Wert:

Standard

Module-3-Ant-Gewinn

Mit diesem Eintrag können Sie den Antennen-Verstärkungsfaktor (Gewinn in dBi) abzüglich der Dämpfungen für Kabel und ggf. Blitzschutz angeben. Hieraus errechnet Ihre Basisstation die in Ihrem Land und für das jeweilige Frequenzband maximal zulässige Sendeleistung.

Lassen Sie das Feld leer, wird die Default-Einstellung verwendet, die bei der Konfigurationsgruppe des verwendeten WLAN-Profils eingestellt ist.

Die Sendeleistung kann auf minimal 0,5 dBm im 2,4 GHz-Band bzw. 6,5 dBm im 5 GHz Band reduziert werden. Das begrenzt den maximal einzutragenden Wert im 2,4 GHz-Band auf 17,5 dBi, im 5GHz-Band auf 11,5 dBi. Bitte achten Sie darauf, dass Ihr Antennen- / Kabel- / Blitzschutz-Setup unter diesen Bedingungen den Regulierungsanforderungen des Landes entspricht, in dem Sie das System einsetzen.

Die Empfindlichkeit des Empfängers bleibt hiervon unbeeinflusst.

Beispiel:

AirLancer	Antennengewinn	Kabeldämfung:	Einzutragender Wert
O-18a	18dBi	4dB	18dBi - 4dB = 14dBi

Die aktuelle Sendeleistung können Sie mit Hilfe des Web-Interfaces des Gerätes oder per Telnet unter **Status** > **WLAN-Statistik** > **WLAN-Parameter** > **Sendeleistung** oder per LANmonitor unter **System-Informationen** > **WLAN-Karte** > **Sendeleistung** einsehen.

SNMP-ID:

2.37.1.4.43

Pfad Konsole:

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

Mögliche Werte:

0 … 999 dBi

Default-Wert:

leer

Module-3-TX-Redukt.

Wenn Sie eine Antenne mit einem hohen Verstärkungsfaktor verwenden, dann können Sie mit diesem Eintrag die Sendeleistung Ihrer Basisstation auf die in Ihrem Land und die im jeweiligen Frequenzband zulässige Sendeleistung herunterdämpfen.

Lassen Sie das Feld leer, wird die Default-Einstellung verwendet, die bei der Konfigurationsgruppe des verwendeten WLAN-Profils eingestellt ist.

Die Sendeleistung kann auf minimal 0,5 dBm im 2,4 GHz-Band bzw. 6,5 dBm im 5 GHz Band reduziert werden. Das begrenzt den maximal einzutragenden Wert im 2,4 GHz-Band auf 17,5 dBi, im 5 GHz-Band auf 11,5 dBi. Bitte achten Sie darauf, dass Ihr Antennen- / Kabel- / Blitzschutz-Setup unter diesen Bedingungen den Regulierungsanforderungen des Landes entspricht, in dem Sie das System einsetzen.

Die Empfindlichkeit des Empfängers bleibt hiervon unbeeinflusst.

Die aktuelle Sendeleistung können Sie mit Hilfe des Web-Interfaces des Gerätes oder per Telnet unter **Status** > **WLAN-Statistik** > **WLAN-Parameter** > **Sendeleistung** oder per LANmonitor unter **System-Informationen** > **WLAN-Karte** > **Sendeleistung** einsehen.

SNMP-ID:

2.37.1.4.44

Pfad Konsole:

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

Mögliche Werte:

0 … 999 dBi

Default-Wert:

leer

WLAN-Modul-3-Default

Über diese Einstellung konfigurieren Sie das Frequenzband, in dem der AP die 3. physikalische WLAN-Schnittstelle betreibt.

Sofern ein verwalteter AP lediglich über zwei oder weniger physikalische WLAN-Schnittstellen verfügt, ignoriert der AP die Einstellungen für die 3. physikalische WLAN-Schnittstelle.

SNMP-ID:

2.37.1.41

Pfad Konsole:

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

Mögliche Werte:

Auto

Der AP wählt das Frequenzband für die physikalische WLAN-Schnittstelle selbstständig aus. Dabei behandelt der AP das 6 GHz-Band bevorzugt, sofern dieses verfügbar ist.

2,4GHz

Der AP betreibt die physikalische WLAN-Schnittstelle im 2,4 GHz-Band.

5GHz

Der AP betreibt die physikalische WLAN-Schnittstelle im 5 GHz-Band.

6GHz

Der AP betreibt die physikalische WLAN-Schnittstelle im 6 GHz-Band.

Aus

Der AP deaktiviert die physikalische WLAN-Schnittstelle.

Default-Wert:

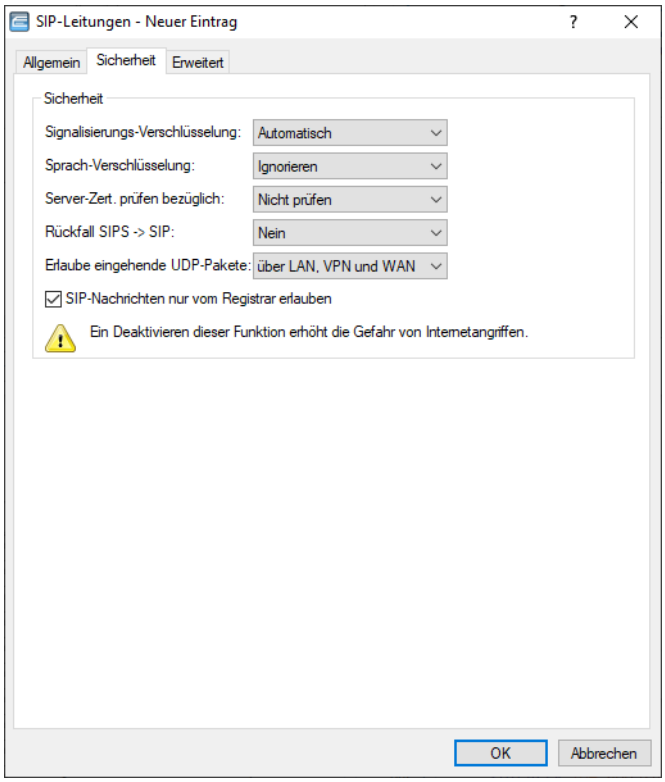
Auto

7 Voice over IP – VoIP

7.1 Unterstützung für NAPTR-Records im Voice Call Manager

Ab LCOS 10.70 unterstützt der Voice Call Manager die DNS-Auflösung von NAPTR (Naming Adress Pointer)-Records. Im NAPTR-Record kann der Telefonie-Provider das verwendete Transportprotokoll, z. B. UDP, TCP oder TLS vorgeben, das der VCM zur Auflösung des SIP-Registrars verwenden soll. Ebenso können Prioritäten bzw. Gewichtungen vergeben werden, falls es mehrere NAPTR-Records für eine Anfrage gibt. Der VCM verwendet bei neuen Konfigurationen standardmäßig NAPTR-Records für die DNS-Auflösung.

Dazu wurde in LANconfig unter **Voice Call Manager** > **Leitungen** > **SIP-Leitungen** > **Sicherheit** der Parameter **Signalisierungs-Verschlüsselung** um den neuen Default-Wert **Automatisch** erweitert.



Signalisierungs-Verschlüsselung

Diese Einstellung legt das Protokoll zur Signalisierungs-Verschlüsselung (SIP/SIPS) bei der Kommunikation mit dem Provider fest.

Automatisch

Zur DNS-Auflösung werden NAPTR (Naming Adress Pointer)-Records verwendet. Der Provider gibt in den DNS-Daten die Verwendung des Transportprotokolls wie UDP, TCP oder TLS vor. Ebenso können Gewichte bzw. Prioritäten durch den Provider vorgegeben werden.

Wenn TLS als Transportprotokoll zur Signalisierungsverschlüsselung durch NAPTR vorgegeben wird, wird automatisch auch Sprachverschlüsselung verwendet, unabhängig von der expliziten Konfigurationseinstellung der Sprachverschlüsselung.

7.1.1 Ergänzungen im Setup-Menü

Transport

Legen Sie mit diesem Eintrag fest, mit welchem Protokoll die Datenströme verschlüsselt werden.

SNMP-ID:

2.33.4.1.1.28

Pfad Konsole:

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

Mögliche Werte:

Auto

Zur DNS-Auflösung werden NAPTR (Naming Adress Pointer)-Records verwendet. Der Provider gibt in den DNS-Daten die Verwendung des Transportprotokolls wie UDP, TCP oder TLS vor. Ebenso können Gewichte bzw. Prioritäten durch den Provider vorgegeben werden.

Wenn TLS als Transportprotokoll zur Signalisierungsverschlüsselung durch NAPTR vorgegeben wird, wird automatisch auch Sprachverschlüsselung verwendet, unabhängig von der expliziten Konfigurationseinstellung der Sprachverschlüsselung.

UDP

Alle SIP Pakete werden verbindungslos übertragen. Die meisten Anbieter unterstützen diese Einstellung.

TCP

Alle SIP Pakete werden verbindungsorientiert übertragen. Das Gerät baut eine TCP Verbindung zum Provider auf und erhält diese für die Dauer der Registrierung aufrecht. Spezielle Anbieter, wie z. B. Anbieter von Trunk Anschlüssen, unterstützen oder erzwingen diese Einstellung.

TLSv1
TLSv1.1
TLSv1.2
TLSv1.3

Gleiche Übertragungsweise wie bei TCP, allerdings werden alle SIP Pakete zusätzlich durch eine Verschlüsselung bis zum Provider geheim gehalten. Die jeweils in der Konfiguration ausgewählte TLS-Version wird als minimale Anforderung für die TLS-Verschlüsselung verwendet.

Default-Wert:

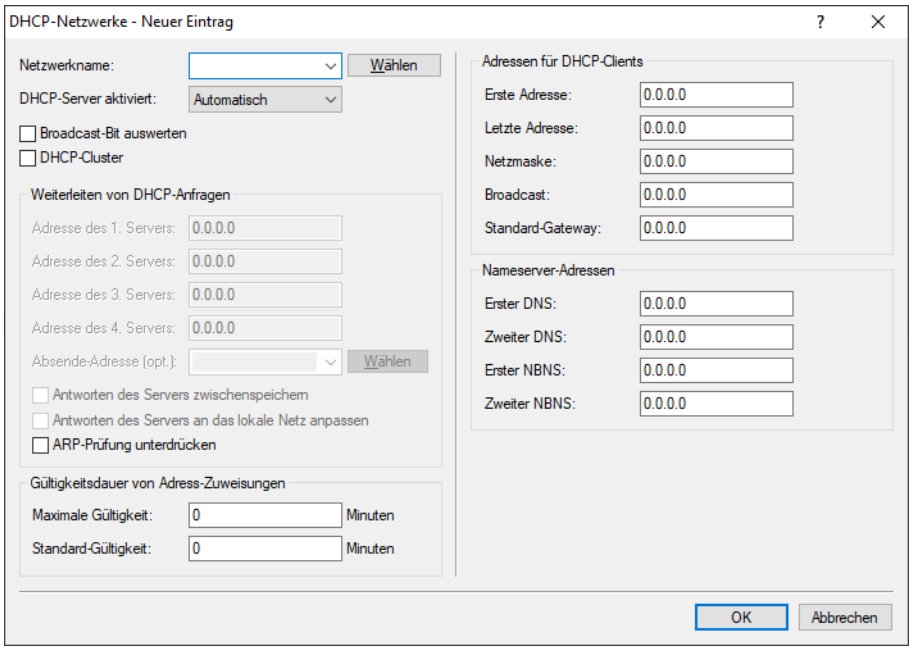
Auto

8 Weitere Dienste

8.1 Stateless DHCP-Relay Agent

Ab LCOS 10.70 unterstützt der DHCP-Relay Agent die Betriebsart „Stateless-Relay“.

Dazu wurde in LANconfig unter **IPv4** > **DHCPv4** > **DHCP-Netzwerke** der Parameter **DHCP-Server aktiviert** um den neuen Wert **Stateless Relay** erweitert.



DHCP-Server aktiviert

Der DHCP-Server kann die folgenden verschiedenen Zustände annehmen:

Stateless-Relay

Das Gerät nimmt die Anfragen der DHCP-Clients im lokalen Netz entgegen. Das Gerät beantwortet diese Anfragen jedoch nicht selbst, sondern leitet sie an einen zentralen DHCP-Server in einem anderen Netzwerkabschnitt weiter (Betriebsart DHCP-Relay-Agent).

Der Stateless Relay Agent modifiziert DHCP-Pakete vom Client zum Server und zurück nicht. Insbesondere wird der DHCP-Server Identifier, im Gegensatz zum Relay Agent, nicht modifiziert.

8.1.1 Ergänzungen im Setup-Menü

Aktiv

Betriebsart des DHCP-Servers für dieses Netzwerk. Je nach Betriebsart kann sich der DHCP-Server selbst aktivieren bzw. deaktivieren. Ob der DHCP-Server aktiv ist, kann den DHCP-Statistiken entnommen werden.

Verwenden Sie die Einstellung "Ja" nur dann, wenn sichergestellt ist, dass kein anderer DHCP-Server im LAN aktiv ist.

Verwenden Sie die Einstellung "Client-Modus" nur dann, wenn sichergestellt ist, das ein anderer DHCP-Server im LAN aktiv ist und die Zuweisung der IP-Adress-Informationen übernimmt.

SNMP-ID:

2.10.20.11

Pfad Konsole:

Setup > **DHCP** > **Netzliste**

Mögliche Werte:

Nein

Der DHCP-Server ist dauerhaft abgeschaltet.

Ja

Der DHCP-Server ist dauerhaft eingeschaltet. Bei der Eingabe dieses Wertes wird die Konfiguration des Servers (Gültigkeit des Adress-Pools) überprüft. Bei einer korrekten Konfiguration bietet das Gerät sich als DHCP-Server im Netz an. Bei einer fehlerhaften Konfiguration (z. B. ungültige Pool-Grenzen) wird der DHCP-Server für das Netzwerk deaktiviert. Verwenden Sie diese Einstellung nur dann, wenn sichergestellt ist, das kein anderer DHCP-Server im LAN aktiv ist.

Auto

In diesem Zustand sucht das Gerät regelmäßig im lokalen Netz nach anderen DHCP-Servern. Diese Suche ist erkennbar durch ein kurzes Aufleuchten der LAN-Rx/Tx-LED. Wird mindestens ein anderer DHCP-Server gefunden, schaltet das Gerät seinen eigenen DHCP-Server aus. Ist für das Gerät noch keine IP-Adresse konfiguriert, dann wechselt es in den DHCP-Client-Modus und bezieht eine IP-Adresse vom DHCP-Server. Damit wird u. a. verhindert, dass ein unkonfiguriertes Gerät nach dem Einschalten im Netz unerwünscht Adressen vergibt. Werden keine anderen DHCP-Server gefunden, schaltet das Gerät seinen eigenen DHCP-Server ein. Wird zu einem späteren Zeitpunkt ein anderer DHCP-Server im LAN eingeschaltet, wird der DHCP-Server im Gerät deaktiviert.

Relay

Der DHCP-Server ist eingeschaltet, das Gerät nimmt die Anfragen der DHCP-Clients im lokalen Netz entgegen. Das Gerät beantwortet diese Anfragen jedoch nicht selbst, sondern leitet sie an einen zentralen DHCP-Server in einem anderen Netzwerkabschnitt weiter (Betriebsart DHCP-Relay-Agent).

Client

Der DHCP-Server ist ausgeschaltet, das Gerät verhält sich als DHCP-Client und bezieht seine Adress-Informationen von einem anderen DHCP-Server im LAN. Verwenden Sie diese Einstellung nur dann, wenn sichergestellt ist, das ein anderer DHCP-Server im LAN aktiv ist und die Zuweisung der IP-Adress-Informationen übernimmt.

Stateless-Relay

Das Gerät nimmt die Anfragen der DHCP-Clients im lokalen Netz entgegen. Das Gerät beantwortet diese Anfragen jedoch nicht selbst, sondern leitet sie an einen zentralen DHCP-Server in einem anderen Netzwerkabschnitt weiter (Betriebsart DHCP-Relay-Agent).

Der Stateless Relay Agent modifiziert DHCP-Pakete vom Client zum Server und zurück nicht. Insbesondere wird der DHCP-Server Identifier, im Gegensatz zum Relay Agent, nicht modifiziert.

Default-Wert:

Nein

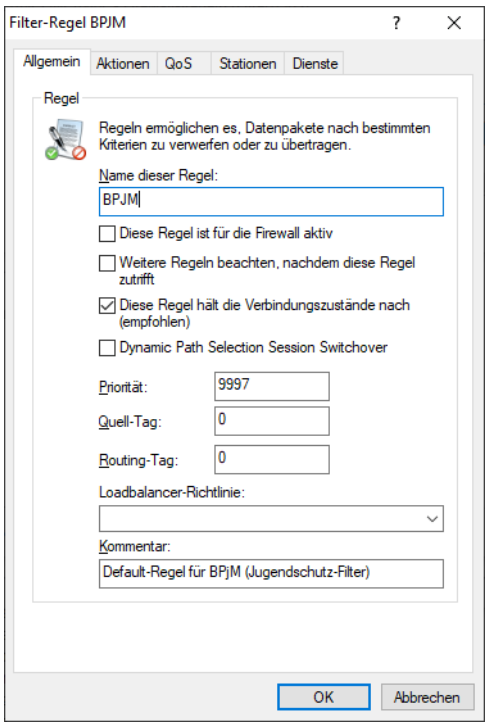
8.2 BPjM-Modul

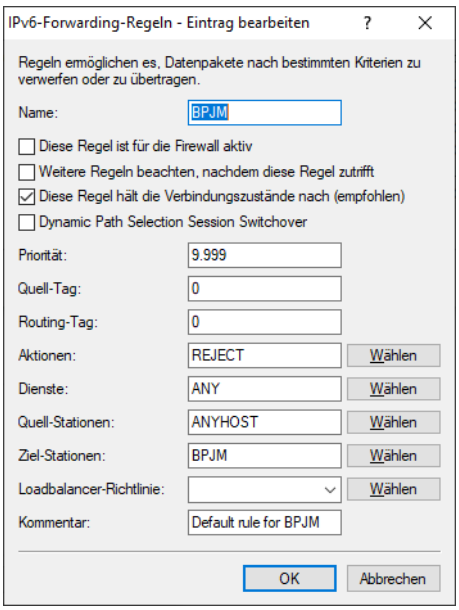
Ab LCOS 10.70 wird das BPjM-Modul unterstützt. Das BPjM-Modul wird von der Bundeszentrale für Kinder- und Jugendmedienschutz herausgegeben und sperrt Webseiten, die Kindern und Jugendlichen in Deutschland nicht zugänglich gemacht werden dürfen. Diese Funktion ist besonders für Schulen und Bildungseinrichtungen mit minderjährigen Schülern relevant. Damit sind URLs, deren Inhalte offiziell als jugendgefährdend eingestuft werden, für die entsprechende Zielgruppe in Deutschland nicht erreichbar. Eine automatische und regelmäßige Aktualisierung und Erweiterung dieser Auflistung ist dabei gewährleistet. Das BPJM-Modul sperrt URLs die auf der offiziellen Webseiten-Liste der Bundesprüfstelle für jugendgefährdende Medien (BPjM) stehen. Eine Sperrung nach Kategorie oder Override (Erlauben) ist hierbei nicht möglich.

Das BPJM-Modul ist Teil der LANCOM Content Filter Option oder separat über die Software-Option LANCOM BPjM Filter Option erhältlich.

In der IPv4- bzw. IPv6-Firewall existiert dazu eine Default-Firewall-Regel, die aktiviert werden kann und pro Netz konfiguriert werden kann. So ist beispielsweise möglich, nur das Schülernetz mit diesem Filter auszustatten, andere Netze aber davon auszunehmen.

In der IPv6-Firewall existiert eine neue Default-Regel BPJM, die standardmäßig deaktiviert ist mit dem System-Objekt „BPJM“ als Zielstation. In der IPv4-Firewall existiert dazu analog eine Regel. Definieren Sie als Quell-Stationen die Netzwerke, die durch das BPjM-Modul geschützt werden sollen.





8.2.1 Einsatzempfehlungen

Sollen Content-Filter und BPJM-Filter gemeinsam verwendet werden, müssen beide Regeln mit unterschiedlichen Prioritäten konfiguriert werden, so dass diese nacheinander durchlaufen werden.

Ebenso muss bei der ersten Regel darauf geachtet werden, dass der Punkt „Weitere Regeln beachten, nachdem diese Regel zutrifft“ aktiviert ist.

In seltenen Fällen kann es dazu kommen, dass das BPJM-Modul gewünschte Domains blockiert, da nur (DNS-)Domains und keine URL-Verzeichnisebenen aufgrund von TLS geprüft werden können. In diesem Fall können diese gewünschten Domains in der „BPJM-Allow-Liste“ hinzugefügt werden, z. B. *.example.com.

Der LANCOM Router muss als DNS-Server bzw. DNS-Forwarder im Netz dienen, d. h. Clients im lokalen Netzwerk müssen den Router als DNS-Server verwenden. Zusätzlich muss die direkte Nutzung von DNS-over-TLS und DNS-over-HTTPS (ggf. browserintern) mit externen DNS-Servern durch Clients verhindert werden.

Dies kann wie folgt erreicht werden:

- Der DHCP-Server muss die IP-Adresse des Routers als DNS-Server verteilen (wird standardmäßig vom Internet-Wizard eingerichtet)
- Einrichtung von Firewall-Regeln, die die direkte Nutzung von externen DNS-Servern verhindern, z. B. durch Sperrung des ausgehenden Ports 53 (UDP) für Clients aus dem entsprechenden Quellnetzwerk
- Einrichtung von Firewall-Regeln, die die direkte Nutzung von externen DNS-Servern mit Unterstützung von DNS-over-TLS verhindern, z. B. durch Sperrung des ausgehenden Ports 853 (TCP) für Clients aus dem entsprechenden Quellnetzwerk
- DNS-over-HTTPS (DoH) im Browser deaktivieren

Hinweise zur Synchronisierung der DNS-Datenbank der Firewall:

Da die Firewall ihre Informationen aus den DNS-Anfragen der Clients lernt, kann es in bestimmten Situationen dazu kommen, dass die DNS-Datenbank noch nicht vollständig ist. Dies kann in folgenden Situationen passieren:

- Es wird eine neue Firewall-Regel hinzugefügt, der Client hat aber noch einen DNS-Eintrag zwischengespeichert
- Kurz nach Neustart des Routers und der Client hat aber noch einen DNS-Eintrag zwischengespeichert

In diesen Fällen hilft ein Leeren des DNS-Cache auf dem Client, ein Reboot des Clients oder ein Timeout des DNS-Eintrags auf dem Client.

Wenn unterschiedliche DNS-Namen auf dieselbe IP-Adresse aufgelöst werden, dann können diese nicht unterschieden werden. In diesem Fall trifft immer die erste Regel zu, die einen dieser DNS-Namen referenziert. Das sollte bei großen Dienstanbietern kein Problem sein. Bei kleinen Webseiten, die vom selben Anbieter gehostet werden, könnte es jedoch auftreten.

9 Ergänzungen im Menüsystem

9.1 Ergänzungen im Setup-Menü

9.1.1 ARP-Bridge-Optimierung

Schalter zur Optimierung des Bridge-Handlings bei IPv4 und ARP.

SNMP-ID:

2.7.33

Pfad Konsole:

Setup > **TCP-IP**

Mögliche Werte:

nein

Das ARP speichert für ein auf einem Bridge-Link empfangenes Paket nur die Bridge-Information. Der Switch-Port wird zu 0 gesesetzt. Das erzwingt, dass die Bridge einen MAC-Address-Lookup macht um den wirklichen Link (und Switchport) zu finden.

ja

Das ARP speichert die LAN-Information und den Switchport des empfangenen ARP-Request / Replies in der ARP-Tabelle, unabhängig davon, ob das Paket auf einem Bridge-Link empfangen wurde.

Default-Wert:

ja

9.1.2 LAN-Client-ID-Typ

Dieser Schalter steuert, wie die Client-ID-Option in DHCPv4-Client DHCPDISCOVER- und DHCPREQUEST-Messages im LAN aufgebaut wird.

SNMP-ID:

2.10.31

Pfad Konsole:

Setup > **DHCP**

Mögliche Werte:

MAC

Die Client ID enthält nur die MAC-Adresse des Geräts. Vor LCOS 10.70 wurde immer die MAC-Adresse als Client ID automatisch ohne eigene Konfigurationsmöglichkeit verwendet. Bei einer Aktualisierung der Firmware bleibt dieser Wert erhalten.

DUID

Konform zu *RFC 4361* wird die Client ID als DUID (DHCP Unique IDentifier) aus der IAID und der MAC-Adresse des Geräts gebildet. Dies ist der Default bei neuen Installationen ab LCOS 10.70.

Default-Wert:

DUID

9.1.3 WAN-Client-ID-Typ

Dieser Schalter steuert, wie die Client-ID-Option in DHCPv4-Client DHCPDISCOVER- und DHCPREQUEST-Messages im WAN aufgebaut wird.

SNMP-ID:

2.10.32

Pfad Konsole:

Setup > **DHCP**

Mögliche Werte:

MAC

Die Client ID enthält nur die MAC-Adresse des Geräts. Vor LCOS 10.70 wurde immer die MAC-Adresse als Client ID automatisch ohne eigene Konfigurationsmöglichkeit verwendet. Bei einer Aktualisierung der Firmware bleibt dieser Wert erhalten.

DUID

Konform zu *RFC 4361* wird die Client ID als DUID (DHCP Unique IDentifier) aus der IAID und der MAC-Adresse des Geräts gebildet. Dies ist der Default bei neuen Installationen ab LCOS 10.70.

Default-Wert:

DUID

9.1.4 MAC-Algorithmen

Ab LCOS-Version 10.70 werden Encrypt-then-MAC HMAC-SHA-Algorithmen bei SSH unterstützt.

Die Message Authentication Code (MAC)-Algorithmen dienen der Integritätsprüfung von Nachrichten. Wählen Sie aus den verfügbaren Encrypt-and-MAC- bzw. Encrypt-then-MAC-Algorithmen einen oder mehrere aus.

Bei SSH-Algorithmen gilt grundsätzlich Client-Präferenz. Somit bestimmt der Client den Algorithmus und nimmt normalerweise den ersten passenden aus seiner Liste möglicher Algorithem. Passen Sie ggf. die Liste ihres Clients an.

SNMP-ID:

2.11.28.2

Pfad Konsole:

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

Mögliche Werte:

hmac-md5-96
hmac-md5
hmac-sha1-96
hmac-sha1
hmac-sha2-256-96
hmac-sha2-256
hmac-sha2-512-96
hmac-sha2-512
hmac-md5-96-etm
hmac-md5-etm
hmac-sha1-96-etm
hmac-sha1-etm
hmac-sha2-256-96-etm
hmac-sha2-256-etm
hmac-sha2-512-96-etm
hmac-sha2-512-etm
hmac-sha2-256,hmac-sha2-512,hmac-sha2-256-etm,hmac-sha2-512-etm

Default-Wert:

hmac-sha2-256,hmac-sha2-512,hmac-sha2-256-etm,hmac-sha2-512-etm

9.1.5 Schluesselaustausch-Algorithmen

Ab LCOS-Version 10.70 wird sntrup761x25519-sha512 bei SSH unterstützt.

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

SNMP-ID:

2.11.28.3

Pfad Konsole:

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

Mögliche Werte:

diffie-hellman-group1-sha1
diffie-hellman-group14-sha1
diffie-hellman-group-exchange-sha1
diffie-hellman-group-exchange-sha256
ecdh-sha2
curve25519-sha256
curve448-sha512
sntrup761x25519-sha512
diffie-hellman-group14-sha256
diffie-hellman-group16-sha512

Default-Wert:

diffie-hellman-group-exchange-sha256

ecdh-sha2

curve25519-sha256

curve448-sha512

sntrup761x25519-sha512

diffie-hellman-group14-sha256

diffie-hellman-group16-sha512

9.1.6 Frequenzband

Hier lässt sich das DECT-Fequenzband einer Gigaset-Basisstation N670 oder N870 bei der Provisionierung setzen.

SNMP-ID:

2.33.10.1.6

Pfad Konsole:

Setup > **Voice-Call-Manager** > **DECT** > **Basisstationen**

Mögliche Werte:

Unchanged
Das in der Basisstation konfigurierte Frequenzband wird nicht geändert.

Europa
Einstellung für Europa.

Lateinamerica
Einstellung für Lateinamerika.

Brasilien
Einstellung für Brasilien.

Default-Wert:

Unchanged

9.1.7 Admin-Passwort

Hier lässt sich das Administrator-Passwort einer Gigaset-Basisstation N670 oder N870 bei der Provisionierung setzen.

SNMP-ID:

2.33.10.1.7

Pfad Konsole:

Setup > **Voice-Call-Manager** > **DECT** > **Basisstationen**

Mögliche Werte:

mind. 8 und max. 15 Zeichen aus

```
[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.0123456789abcdefghijklmnopqrstuvwxyz
`
```

Besondere Werte:

leer

Ist der Eintrag leer, wird kein Passwort in der XML übermittelt. So bleibt das bisher gesetzte Passwort unverändert.

Default-Wert:

leer

9.1.8 NDP-Bridge-Optimierung

Schalter zur Optimierung des Bridge-Handlings bei IPv6 und dem Neighbor Discovery Protokoll (NDP).

SNMP-ID:

2.70.16.3

Pfad Konsole:

Setup > **IPv6** > **NDP**

Mögliche Werte:

nein

Die Neighbor-Discovery speichert für ein auf einem Bridge-Link empfangenes Paket nur die Bridge-Information. Der Switch-Port wird zu 0 gesesetzt. Das erzwingt, dass die Bridge einen MAC-Address-Lookup macht um den wirklichen Link (und Switchport) zu finden.

ja

Die Neighbor-Discovery speichert die LAN-Information und den Switchport des empfangenen Neighbor-Solicitation / Advertisement im Neigbor-Cache, unabhängig davon, ob das Paket auf einem Bridge-Link empfangen wurde.

Default-Wert:

ja