# LCOS 10.50

## Addendum

05/2024

LANCOM SYSTEMS

# Inhalt

# Copyright



LANCOM Systems GmbH

A Rohde & Schwarz Company

Adenauerstr. 20/B2

52146 Würselen

Deutschland

*www.lancom-systems.de*

# 1 Addendum zur LCOS-Version 10.50

Dieses Dokument beschreibt die Änderungen und Ergänzungen in der LCOS-Version 10.50 gegenüber der vorherigen Version.

# 2 Konfiguration

## 2.1 Neuer Kommandozeilenbefehl ikectl

Ab LCOS 10.50 gibt es den Befehl ikectl.

| Befehl | Beschreibung |
|---|---|
| `ikectl [-[r\|d\|D] <peer-name-list>] [-[e\|r\|d] <ipsec-name-list>] [-[r\|d] [<ike-cookies-list>\|<esp-spi-list>]] [-R <peer-name-list> <redirect-target>]` | Dieser Befehl erweitert die Analyse-Möglichkeiten, indem z. B. in einem Fehlerfall gezielt Aktionen durchgeführt werden, mit denen sich ein Problem eingrenzen lässt. Diese Funktion erlaubt es u. a., ein VPN schnell automatisiert zu modifizieren und zu testen.<br>› `-e <ipsec-name-list>`: Erzeugt eine Phase 2-SA / CHILD_SA unter Angabe des VPN-Regelnamens<br>› `-r <peer-name-list>`: Führt ein Rekeying der Phase 1-SA / IKE_SA unter Angabe des Namens der VPN-Gegenstelle durch<br>› `-r <ike-cookies-list>`: Führt ein Rekeying unter Angabe des IKE-Cookies durch<br>› `-r <ipsec-name-list>`: Führt ein Rekeying der Phase 2-SA / Child_SA unter Angabe des VPN-Regelnamens durch<br>› `-r <esp-spi-list>`: Führt ein Rekeying der Phase 2-SA / Child_SA unter Angabe der eingehenden oder ausgehenden ESP-SPI durch<br>› `-d <peer-name-list>`: Löscht eine Phase 1-SA / IKE_SA unter Angabe des Namens der VPN-Gegenstelle<br>› `-d <ike-cookies-list>`: Löscht eine Phase 1-SA / IKE_SA unter Angabe von IKEv1-Cookies / IKEv2 SPIs<br>› `-d <ipsec-name-list>`: Löscht eine Phase 2-SA / CHILD_SA unter Angabe des VPN-Regelnamens<br>› `-d <esp-spi-list>`: Löscht eine Phase 2-SA / Child_SA unter Angabe der eingehenden bzw. ausgehenden ESP-SPI<br>› `-D <peer-name-list>`: Start der Liveness-Check-Prozedur (Dead Peer Detection – DPD) unter Angabe des Namens der VPN-Gegenstelle<br>› `-R <peer-name-list> <redirect-target`: Leitet IKEv2-Gegenstellen per IKEv2-Redirect-Mechanismus zu einem neuen Ziel um. Falls die Gegenstellen-Liste leer ist, werden alle Gegenstellen umgeleitet. Mit diesem Befehl können VPN-Gegenstellen zu Wartungszwecken von dem aktuellen VPN-Gateway auf ein anderes Gateway sicher verschoben werden.<br>› `<peer-name-list>`: Durch Leerzeichen getrennte Liste von Gegenstellennamen aus aus max. 16 Zeichen<br>› `<ipsec-name-list>`: Durch Leerzeichen getrennte Liste von Namen der VPN-Regeln, wie sie in „show vpn“ als ipsec-0-PEER-pr0-l0-r0 angezeigt werden.<br>Um eine bestimmte CHILD_SA / Phase 2-SA eines road-warrior zu finden, ist es wichtig, auch den Gegenstellennamen wie folgt anzugeben: "`peer-name ipsec-name`".<br>› `<ike-cookies-list>`: Besteht aus einer durch Leerzeichen getrennten Liste von jeweils 16 hexadezimalen Werten, z. B. 0x0001020304050607080 90A0B0C0D0E0F |

| Befehl | Beschreibung |
|---|---|
| | › `<esp-spi-list>`: Besteht aus einer durch Leerzeichen getrennten Liste von jeweils 4 hexadezimalen Werten, z. B. 0x00010203<br>› `<redirect-target>`: Ziel, zu dem die Gegenstelle(n) umgeleitet werden sollen. Ziel kann eine IPv4-Adresse, IPv6-Adresse oder ein DNS-Name sein<br>Beispiel: `ikectl -r peer ipsec-name-peer-2 -D peer3 -d peer4 0x12345678 -e "RoadWarrior IPSEC-0-DEFAULT-PR0-L0-R0"` |

## 2.2 Neuer Kommandozeilenbefehl dnsquery

Ab LCOS 10.50 gibt es den Befehl dnsquery, über den analog zu bekannten Programmen unter anderen Betriebssystemen. auf der CLI DNS-Anfragen aufgelöst werden können.

| Befehl | Beschreibung |
|---|---|
| `dnsquery [-t <type>] [-d <destination>] name[@rtg-tag]` | Löst DNS-Anfragen auf. Mögliche Parameter:<br>› `name`: Der aufzulösende DNS-Name.<br>› `@rtg-tag`: Optionales Routing Tag, um die DNS-Server erreichen zu können.<br>› `-t <type>`: Typ: A, AAAA, PTR, SRV, NAPTR<br>› `-d <destination>`: Ziel, über das die DNS-Server erreicht werden können.<br>Wie in der Weiterleitungs-Tabelle kann auch ein Routing-Tag mit angegeben werden, wenn das Weiterleitungsziel eine IP-Adresse ist (z. B. 8.8.8.8@4095). Außerdem können auch zwei kommaseparierte IP-Adressen (mit optionalem Routing-Tag) angegeben werden (z. B. 8.8.4.4@4095,8.8.8.8@4095). Der DNS-Client wechselt dann zwischen den Servern, wenn einer nicht antwortet<br>Wird das Kommando ohne Optionen, also nur mit dem obligatorischen Domainnamen, aufgerufen, dann wird sowohl eine Anfrage vom Typ AAAA als auch eine vom Typ A gemacht. Beispiel:<br>`> dnsquery www.lancom.de`<br>`DNS result:`<br>`==========`<br>`www.lancom.de: type A, class IN, ttl 1 hour, addr 176.9.82.168`<br>`www.lancom.de: type AAAA, class IN, ttl 1 hour, addr 2a01:4f8:151:20a3::2`<br>Die Antwort vom Typ AAAA wird nur ausgegeben, wenn die IPv6-Adresse auch erreichbar ist.<br>Der Typ kann auch explizit über die Option `-t` angegeben werden. Möglich sind dabei AAAA, A, PTR, SRV und NAPTR. Bei einer PTR-Anfrage muß die angefragte IP-Adresse direkt angegeben werden und darf nicht in den „ARPA"-String gewandelt werden:<br>`> dnsquery -tptr 176.9.82.168`<br>`DNS result:`<br>`==========`<br>`168.82.9.176.in-addr.arpa: type PTR, class IN, ttl 5 hours, 32 minutes, 30 seconds, www.lancom-systems.de`<br>Da das dnsquery-Kommando den DNS-Client des LANCOM Gerätes benutzt, wird sein Verhalten über die DNS-Konfiguration des Gerätes bestimmt (also Weiterleitungen, Loopback-Adressen etc.). Da sich die DNS-Konfiguration abhängig vom Routing-Tag unterscheiden kann, kann beim dnsquery Kommando das zu |

| Befehl | Beschreibung |
|---|---|
| | verwendende Tag per @-Erweiterung an den angefragten Namen (oder bei PTR-Anfragen an die angefragte Adresse) angehängt werden:<br>`> dnsquery www.lancom.de@4095`<br><br>`DNS result:`<br>`==========`<br>`www.lancom.de: type A, class IN, ttl 1 hour, addr 176.9.82.168`<br>`www.lancom.de: type AAAA, class IN, ttl 1 hour, addr 2a01:4f8:151:20a3::2`<br><br>Es ist aber auch möglich, die Anfragen an der Weiterleitungskonfiguration vorbei zu senden, indem über den Parameter -d eine Zialangabe gemacht wrid. Als Zielangabe ist alles möglich, was auch in der Weiterleitungs-Tabelle als Ziel angegeben werden kann. Zudem wird auch bei einer manuellen Zielvorgabe die Loopback-Adresse entsprechend der Loopback-Konfiguration bestimmt. Beispiel: AAAA+A Anfrage über WAN-Verbindung INTERNET<br>`> dnsquery -dinternet www.lancom.de`<br><br>`DNS result:`<br>`==========`<br>`www.lancom.de: type A, class IN, ttl 1 hour, addr 176.9.82.168`<br>`www.lancom.de: type AAAA, class IN, ttl 1 hour, addr 2a01:4f8:151:20a3::2`<br><br>Dazu muß der WAN-Verbindung INTERNET natürlich ein DNS-Server zuigewiesen worden sein, z. B. per PPP, DHCP oder manuell in der IP-Parameter-Liste.<br><br>Beispiel: PTR-Anfrage über Google-Server<br>`> dnsquery -d8.8.8.8 -tptr 176.9.82.168`<br><br>`DNS result:`<br>`==========`<br>`168.82.9.176.in-addr.arpa: type PTR, class IN, ttl 5 hours, 32 minutes, 30 seconds, www.lancom-systems.de`<br><br>Wenn kein Server andwortet macht der Client drei Wiederholungen mit sich erhöhender Wartezeit, d. h. nach jeder gesendeten Anfrage wartert er 1, 2, 4 und beim letzten Mal 8 Sekunden. Kommt bis dann keine Antwort, so wird die Anfrage abgebrochen. Wenn während einer laufenden Anfrage <CR> gedrückt wird, so wird diese abgebrochen. |

## 2.3 Load-Balancer-Selektoren für Ping verwenden

Ab LCOS 10.50 gibt es eine neue Kommandozeilenoption für ping, um Load-Balancer-Selektoren zu nutzen.

Auf der Kommandozeile nutzen Sie bei ping den neuen optionalen Parameter `-l <Load-Balancer-Policy>`.

| Parameter | Bedeutung |
|---|---|
| `-l <Load-Balancer-Policy>` | Wenn das Ping-Ziel über einen Load Balancer erreichbar ist, wird beim Versand der Pings anhand der Policy eine Load-Balancer-Entscheidung getroffen. Mögliche Werte sind Traffic, Bandwidth, Round-Robin, sowie alle definierten Dynamic-Path-Selection-Policies. Die Angabe einer ungültigen Policy sorgt dafür, dass keine Pings versendet werden können<br><br>Es ist nicht möglich, diese Kommandozeilen-Option zusammen mit der Angabe eines Scopes oder einer Interface-Bindung in der Destination zu verwenden. |

# 2.4 Konfigurationsmöglichkeit für IPv4/IPv6-Auflösung bei DNS-Auflösungen

Ab LCOS 10.50 können bei Parametern, bei denen DNS-Hostnamen konfiguriert werden können, mit einem Schalter übergeben werden, wie IPv4 bzw. IPv6 beim Verbindungsaufbau priorisiert werden sollen.

Konkrete Anwendungsfälle sind beispielsweise die Verwendung von DNS-Namen bei VPN-Verbindungen oder SIP-Registraren, wo gesteuert werden soll, ob die Verbindung über IPv4 oder IPv6 aufgebaut werden soll.

**Beispiel 1:** Wird der Hostname `vpn.example.org` auf eine IPv4- und eine IPv6-Adresse aufgelöst, so bevorzugt ein Host normalerweise IPv6 vor IPv4. Soll nun aber IPv4 verwendet werden, so kann dies durch Anhängen von `?4` an den Hostnamen gesteuert werden, d. h. hier: `vpn.example.org?4`.

**Beispiel 2:** Soll beim CLI-Ping IPv4 bei einem IPv4/IPv6 DNS-Hostnamen bevorzugt werden, so kann die folgende Syntax verwendet werden: `ping www.example.org?4`.

Die folgenden Suffixe sind erlaubt:

- `?4`: Auflösung nur über IPv4
- `?6`: Auflösung nur über IPv6
- `?46`: IPv4 vor IPv6 bevorzugen, d. h. falls IPv4 nicht aufgelöst werden kann, so wird IPv6 verwendet.
- `?64`: IPv6 vor IPv4 bevorzugen, d. h. falls IPv6 nicht aufgelöst werden kann, so wird IPv4 verwendet.

# 3 Routing und WAN-Verbindungen

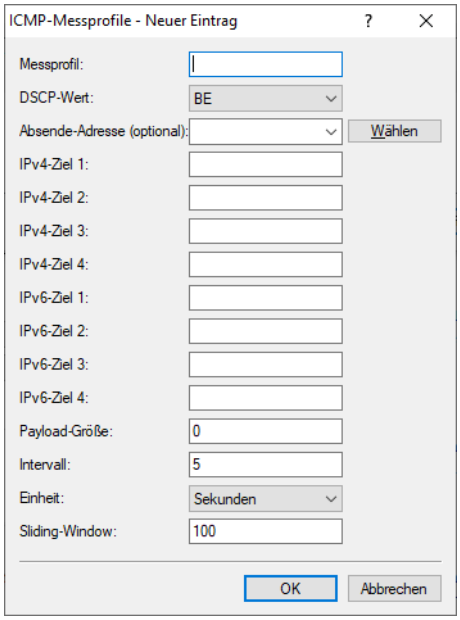
## 3.1 Dynamic Path Selection

Ab LCOS 10.50 werden bei Dynamic Path Selection die folgenden neuen Funktionen unterstützt:

- Session Switchover: Eine aktive Session kann zur Laufzeit auf eine bessere Leitung verschoben werden (nur bei unmaskierten Verbindungen, z. B. VPN / Overlay-Tunnel)
- Neben ICMP wird auch HTTP(S) als Messmethode unterstützt
- ICMP-Messintervalle unterstützen nun Intervalle mit einer Zeitauflösung in Millisekunden
- IPv6

### 3.1.1 Ergänzungen in der Tabelle ICMP-Messprofile

Zur Konfiguration der ICMP-Messprofile wechseln Sie in die Ansicht **IP-Router** > **Routing** > **SD-WAN Dynamic Path Selection** > **ICMP-Messprofile**.




**IPv6-Ziel 1-4**

Bis zu 4 Messziele als gültige IPv6-Unicast-Adressen oder DNS Hostnamen. Wird :: eingetragen, wird das Messziel dynamisch vom VPN festgelegt. Wird das Feld leer gelassen, erfolgt keine Messung für die entsprechende Adressfamilie.

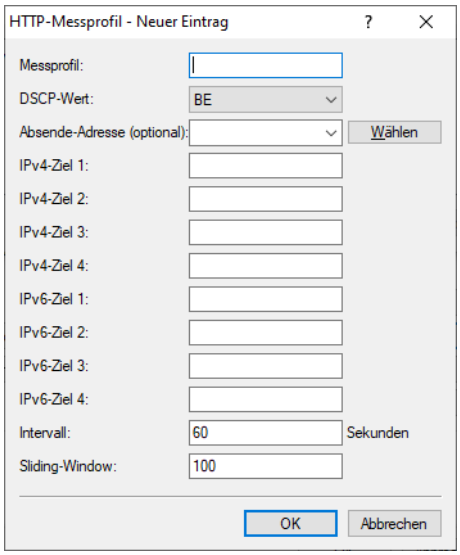
**Einheit**

Gibt an, ob die ICMP-Messungen für den Wert in der Einheit Sekunden oder Millisekunden durchgeführt werden sollen. Mögliche Werte: Sekunden (Default), Millisekunden.

## 3.1.2 Neue Tabelle HTTP-Messprofile

HTTP-Messprofile definieren einen Parametersatz, nach dem Messungen auf Basis von HTTP(S)-Verbindungsaufbauten durchgeführt werden. Aus den Messungen werden Interface-Metriken abgeleitet, welche die Verbindungsqualität quantifizieren sollen. Diese Metriken sind: Mittlere Zeit bis zum Aufbau einer HTTP(S)-Verbindung (Latenz), Jitter, und Verbindungsfehler (Paketverlust)-Rate.

Zur Konfiguration der HTTP-Messprofile wechseln Sie in die Ansicht **IP-Router** > **Routing** > **SD-WAN Dynamic Path Selection** > **HTTP-Messprofil**.




**Messprofil**

Der Name des Profils. Über diesen Namen wird das Profil in DPS-Richtlinien referenziert.

**DSCP-Wert**

Definiert den DSCP-Wert, der im IP-Header der Messpakete gesetzt wird. DSCP (Differentiated Services Code Point) wird für QoS (Quality of Service) verwendet.

**Absende-Adresse (optional)**

Referenziert eine benamte Loopback-Adresse, die bei den Messpaketen als Absender verwendet wird. Wenn das Feld leer gelassen wird, wählt der Router selbstständig eine Adresse aus, die zum Absende-Interface passt.

**IPv4-Ziel 1-4**

Bis zu 4 Messziele als gültige IPv4-Unicast-Adressen oder DNS Hostnamen. Wird 0.0.0.0 eingetragen, wird das Messziel dynamisch vom VPN festgelegt. Wird das Feld leer gelassen, erfolgt keine Messung für die entsprechende Adressfamilie.

**IPv6-Ziel 1-4**

Bis zu 4 Messziele als gültige IPv6-Unicast-Adressen oder DNS Hostnamen. Wird :: eingetragen, wird das Messziel dynamisch vom VPN festgelegt. Wird das Feld leer gelassen, erfolgt keine Messung für die entsprechende Adressfamilie.

**Payload-Größe**

Gibt die Größe der Daten nach dem ICMP-Header (Payload-Größe) der versendeten Pings an.

**Intervall**

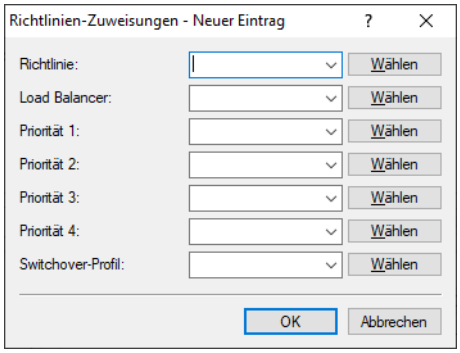
Der Abstand in Sekunden zwischen 2 Messungen. Außerdem wird die maximale Round Trip Time vorgegeben. Pakete, die binnen eines Messintervalls nicht beantwortet wurden, zählen als Packet Loss.

**Sliding-Window**

Maximale Anzahl an Messwerten, die für die Bestimmung der Interface-Metriken benutzt werden. Wird ein Messwert empfangen, obwohl bereits die hier angegebene Anzahl an Messwerten aufgezeichnet wurde, dann wird der älteste Messwert verworfen.

## 3.1.3 Ergänzungen in der Tabelle Richtlinienzuweisungen

Zur Konfiguration der Richtlinien-Zuweisungen wechseln Sie in die Ansicht **IP-Router** > **Routing** > **SD-WAN Dynamic Path Selection** > **Richtlinien-Zuweisungen**.




**Switchover-Profil**

Geben Sie hier den Namen des Switchover-Profils an, dass für diese Richtlinie verwendet werden soll. Siehe hierzu *Neue Tabelle Switchover-Profile* auf Seite 12.

## 3.1.4 Neue Tabelle Switchover-Profile

Standardmäßig werden bei Dynamic Path Selection nur neue Sessions auf eine bessere Leitung verteilt. Sollen existierende Sessions auf eine bessere Leitung aktiv verschoben werden, so muss Session Switchover aktiviert werden. Ein Session Switchover ist nur für unmaskierte Verbindungen wie z. B. VPN oder SD-WAN-Overlays sinnvoll möglich. Bei maskierten Verbindungen würde sich während der Session die öffentliche WAN-Adresse ändern, was z. B. bei SIP-Sessions oder Online Banking vom Server abgelehnt wird. Um Session Switchover zu aktivieren sind zwei Konfigurationsschritte notwendig:

1. Die Firewall-Regeln für Dynamic Path Selection müssen Session Switchover aktiviert haben.

   Dazu muss der Schalter **Dynamic Path Selection Session Failover** für IPv4 unter **Firewall/QoS** > **IPv4-Regeln** > **Regeln** > **Allgemein** bzw. für IPv6 unter **Firewall/QoS** > **IPv6-Regeln** > **IPv6-Forwarding-Regeln** gesetzt werden.

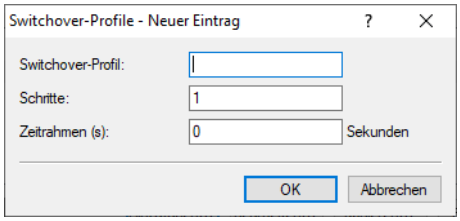
2. Ein Switchover-Profil muss mit der entsprechenden Richtlinie in der Tabelle Richtlinien-Zuweisungen verlinkt werden

Mit Hilfe des Switchover-Profils kann gesteuert werden, wie schnell die Menge der Sessions auf die neue Leitung bzw. Interface des gleichen Load Balancers umgezogen werden soll.

Um eine Konzentration umziehender Sessions auf einer einzelnen Schnittstelle zu verhindern, werden Sessions i. A. schrittweise in mehreren Gruppen umgezogen, die gleichmäßig auf den konfigurierten Zeitrahmen verteilt werden. Vor jedem Schritt wird geprüft, ob der Switchover noch notwendig ist, da sich in der Zwischenzeit die Policy-Scores und damit die Rangfolge der Interfaces bzgl. einer Policy verändert haben können. Wenn er nicht mehr notwendig ist, wird der Switchover abgebrochen, und die noch nicht verschobenen Sessions bleiben auf ihrer aktuellen Schnittstelle. Wenn er noch notwendig ist, wird für jede Session zufällig bestimmt, ob sie Teil der in diesem Schritt umziehenden Gruppe ist, oder nicht.

Wenn die Anzahl der Schritte = 1 oder die Gesamtzeit = 0 ist, dann ziehen alle Sessions sofort um.

Zur Konfiguration der HTTP-Messprofile wechseln Sie in die Ansicht **IP-Router** > **Routing** > **SD-WAN Dynamic Path Selection** > **Switchover-Profile**.




**Name**

Der Name des Switchover-Profils. Über diesen Namen wird das Profil referenziert.

**Schritte**

Anzahl der Schritte bzw. Gruppen, in der die Menge der Sessions auf die neue Leitung verschoben werden soll.

**Zeitrahmen**

Zeitrahmen in Sekunden innerhalb dessen die Menge der Sessions auf die neue Leitung verschoben werden soll.

## 3.1.5 Ergänzungen im Setup-Menü

### IPv6-Ziel-1

Das erste von bis zu 4 Messzielen als gültige IPv6-Unicast-Adressen oder DNS Hostnamen. Wird :: eingetragen, wird das Messziel dynamisch vom VPN festgelegt. Wird das Feld leer gelassen, erfolgt keine Messung für die entsprechende Adressfamilie.

**SNMP-ID:**

2.110.4.1.5

**Pfad Konsole:**

**Setup** > **Firewall** > **Dynamische-Pfadauswahl** > **ICMP-Messprofile**

**Mögliche Werte:**

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

### IPv6-Ziel-2

Das zweite von bis zu 4 Messzielen als gültige IPv6-Unicast-Adressen oder DNS Hostnamen. Wird :: eingetragen, wird das Messziel dynamisch vom VPN festgelegt. Wird das Feld leer gelassen, erfolgt keine Messung für die entsprechende Adressfamilie.

**SNMP-ID:**

2.110.4.1.12

**Pfad Konsole:**

**Setup** > **Firewall** > **Dynamische-Pfadauswahl** > **ICMP-Messprofile**

**Mögliche Werte:**

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

## IPv6-Ziel-3

Das dritte von bis zu 4 Messzielen als gültige IPv6-Unicast-Adressen oder DNS Hostnamen. Wird :: eingetragen, wird das Messziel dynamisch vom VPN festgelegt. Wird das Feld leer gelassen, erfolgt keine Messung für die entsprechende Adressfamilie.

**SNMP-ID:**

2.110.4.1.13

**Pfad Konsole:**

**Setup** > **Firewall** > **Dynamische-Pfadauswahl** > **ICMP-Messprofile**

**Mögliche Werte:**

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

## IPv6-Ziel-4

Das vierte von bis zu 4 Messzielen als gültige IPv6-Unicast-Adressen oder DNS Hostnamen. Wird :: eingetragen, wird das Messziel dynamisch vom VPN festgelegt. Wird das Feld leer gelassen, erfolgt keine Messung für die entsprechende Adressfamilie.

**SNMP-ID:**

2.110.4.1.14

**Pfad Konsole:**

**Setup** > **Firewall** > **Dynamische-Pfadauswahl** > **ICMP-Messprofile**

**Mögliche Werte:**

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

## Einheit

Gibt an, ob die ICMP-Messungen für den Wert in der Einheit Sekunden oder Millisekunden durchgeführt werden sollen.

**SNMP-ID:**

2.110.4.1.15

**Pfad Konsole:**

**Setup** > **Firewall** > **Dynamische-Pfadauswahl** > **ICMP-Messprofile**

**Mögliche Werte:**

**Sekunden**
**Millisekunden**

**Default-Wert:**

Sekunden

## HTTP-Messprofile

HTTP-Messprofile definieren einen Parametersatz, nach dem Messungen auf Basis von HTTP(S)-Verbindungsaufbauten durchgeführt werden. Aus den Messungen werden Interface-Metriken abgeleitet, welche die Verbindungsqualität quantifizieren sollen. Diese Metriken sind: Mittlere Zeit bis zum Aufbau einer HTTP(S)-Verbindung (Latenz), Jitter, und Verbindungsfehler (Paketverlust)-Rate.

**SNMP-ID:**

2.110.4.2

**Pfad Konsole:**

**Setup** > **Firewall** > **Dynamische-Pfadauswahl**

**Messprofil**

Der Name des Profils. Über diesen Namen wird das Profil in DPS-Richtlinien referenziert.

**SNMP-ID:**

2.110.4.2.1

**Pfad Konsole:**

**Setup** > **Firewall** > **Dynamische-Pfadauswahl** > **HTTP-Messprofile**

**Mögliche Werte:**

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

**DSCP-Wert**

Definiert den DSCP-Wert, der im IP-Header der Messpakete gesetzt wird. DSCP (Differentiated Services Code Point) wird für QoS (Quality of Service) verwendet.

**SNMP-ID:**

2.110.4.2.2

**Pfad Konsole:**

**Setup** > **Firewall** > **Dynamische-Pfadauswahl** > **HTTP-Messprofile**

**Mögliche Werte:**

**BE**
**CS0**
**CS1**
**CS2**
**CS3**
**CS4**
**CS5**
**CS6**
**CS7**
**AF11**
**AF12**
**AF13**
**AF21**
**AF22**
**AF23**
**AF31**
**AF32**
**AF33**
**AF41**
**AF42**
**AF43**
**EF**

**Loopback-Addr.**

Referenziert optional eine benamte Loopback-Adresse, die bei den Messpaketen als Absender verwendet wird. Wenn das Feld leer gelassen wird, wählt der Router selbstständig eine Adresse aus, die zum Absende-Interface passt.

**SNMP-ID:**

2.110.4.2.3

**Pfad Konsole:**

**Setup** > **Firewall** > **Dynamische-Pfadauswahl** > **HTTP-Messprofile**

**Mögliche Werte:**

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

**IPv4-Ziel-1**

Das erste von bis zu 4 Messzielen als gültige IPv4-Unicast-Adresse oder DNS Hostname. Wird „0.0.0.0“ eingetragen, wird das Messziel dynamisch vom VPN festgelegt. Wird das Feld leer gelassen, erfolgt keine Messung für die entsprechende Adressfamilie.

**SNMP-ID:**

2.110.4.2.4

**Pfad Konsole:**

**Setup** > **Firewall** > **Dynamische-Pfadauswahl** > **HTTP-Messprofile**

**Mögliche Werte:**

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

**IPv6-Ziel-1**

Das erste von bis zu 4 Messzielen als gültige IPv6-Unicast-Adressen oder DNS Hostnamen. Wird :: eingetragen, wird das Messziel dynamisch vom VPN festgelegt. Wird das Feld leer gelassen, erfolgt keine Messung für die entsprechende Adressfamilie.

**SNMP-ID:**

2.110.4.2.5

**Pfad Konsole:**

**Setup** > **Firewall** > **Dynamische-Pfadauswahl** > **HTTP-Messprofile**

**Mögliche Werte:**

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

**Intervall**

Der Abstand in Sekunden zwischen 2 Messungen. Außerdem wird die maximale Round Trip Time vorgegeben. Pakete, die binnen eines Messintervalls nicht beantwortet wurden, zählen als Packet Loss.

**SNMP-ID:**

2.110.4.2.6

**Pfad Konsole:**

**Setup** > **Firewall** > **Dynamische-Pfadauswahl** > **HTTP-Messprofile**

**Mögliche Werte:**

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

**Sliding-Window**

Maximale Anzahl an Messwerten, die für die Bestimmung der Interface-Metriken benutzt werden. Wird ein Messwert empfangen, obwohl bereits die hier angegebene Anzahl an Messwerten aufgezeichnet wurde, dann wird der älteste Messwert verworfen.

**SNMP-ID:**

2.110.4.2.7

**Pfad Konsole:**

**Setup** > **Firewall** > **Dynamische-Pfadauswahl** > **HTTP-Messprofile**

**Mögliche Werte:**

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

**IPv4-Ziel-2**

Das zweite von bis zu 4 Messzielen als gültige IPv4-Unicast-Adresse oder DNS Hostname. Wird „0.0.0.0" eingetragen, wird das Messziel dynamisch vom VPN festgelegt. Wird das Feld leer gelassen, erfolgt keine Messung für die entsprechende Adressfamilie.

**SNMP-ID:**

2.110.4.2.8

**Pfad Konsole:**

**Setup** > **Firewall** > **Dynamische-Pfadauswahl** > **HTTP-Messprofile**

**Mögliche Werte:**

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

**IPv4-Ziel-3**

Das dritte von bis zu 4 Messzielen als gültige IPv4-Unicast-Adresse oder DNS Hostname. Wird „0.0.0.0" eingetragen, wird das Messziel dynamisch vom VPN festgelegt. Wird das Feld leer gelassen, erfolgt keine Messung für die entsprechende Adressfamilie.

**SNMP-ID:**

2.110.4.2.9

**Pfad Konsole:**

**Setup** > **Firewall** > **Dynamische-Pfadauswahl** > **HTTP-Messprofile**

**Mögliche Werte:**

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

**IPv4-Ziel-4**

Das vierte von bis zu 4 Messzielen als gültige IPv4-Unicast-Adresseoder DNS Hostname. Wird „0.0.0.0" eingetragen, wird das Messziel dynamisch vom VPN festgelegt. Wird das Feld leer gelassen, erfolgt keine Messung für die entsprechende Adressfamilie.

**SNMP-ID:**

2.110.4.2.10

**Pfad Konsole:**

**Setup** > **Firewall** > **Dynamische-Pfadauswahl** > **HTTP-Messprofile**

**Mögliche Werte:**

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

**IPv6-Ziel-2**

Das zweite von bis zu 4 Messzielen als gültige IPv6-Unicast-Adressen oder DNS Hostnamen. Wird :: eingetragen, wird das Messziel dynamisch vom VPN festgelegt. Wird das Feld leer gelassen, erfolgt keine Messung für die entsprechende Adressfamilie.

**SNMP-ID:**

2.110.4.2.11

**Pfad Konsole:**

**Setup** > **Firewall** > **Dynamische-Pfadauswahl** > **HTTP-Messprofile**

**Mögliche Werte:**

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

**IPv6-Ziel-3**

Das dritte von bis zu 4 Messzielen als gültige IPv6-Unicast-Adressen oder DNS Hostnamen. Wird :: eingetragen, wird das Messziel dynamisch vom VPN festgelegt. Wird das Feld leer gelassen, erfolgt keine Messung für die entsprechende Adressfamilie.

**SNMP-ID:**

2.110.4.2.12

**Pfad Konsole:**

**Setup** > **Firewall** > **Dynamische-Pfadauswahl** > **HTTP-Messprofile**

**Mögliche Werte:**

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

**IPv6-Ziel-4**

Das vierte von bis zu 4 Messzielen als gültige IPv6-Unicast-Adressen oder DNS Hostnamen. Wird :: eingetragen, wird das Messziel dynamisch vom VPN festgelegt. Wird das Feld leer gelassen, erfolgt keine Messung für die entsprechende Adressfamilie.

**SNMP-ID:**

2.110.4.2.13

**Pfad Konsole:**

**Setup** > **Firewall** > **Dynamische-Pfadauswahl** > **HTTP-Messprofile**

**Mögliche Werte:**

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

## Switchover-Profil

Der Name eines Switchover-Profils, dass für diese Richtlinie verwendet werden soll. Siehe auch *2.110.4.32.1 Switchover-Profil* auf Seite 21.

**SNMP-ID:**

2.110.4.17.7

**Pfad Konsole:**

**Setup** > **Firewall** > **Dynamische-Pfadauswahl** > **Richtlinien-Zuweisungen**

**Mögliche Werte:**

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

## Switchover-Profile

Standardmäßig werden bei Dynamic Path Selection nur neue Sessions auf eine bessere Leitung verteilt. Sollen existierende Sessions auf eine bessere Leitung aktiv verschoben werden, so muss Session Switchover aktiviert werden. Ein Session Switchover ist nur für unmaskierte Verbindungen wie z. B. VPN oder SD-WAN-Overlays sinnvoll möglich. Bei maskierten Verbindungen würde sich während der Session die öffentliche WAN-Adresse ändern, was z. B. bei SIP-Sessions oder Online Banking vom Server abgelehnt wird. Um Session Switchover zu aktivieren sind zwei Konfigurationsschritte notwendig:

1. Die Firewall-Regeln für Dynamic Path Selection müssen Session Switchover aktiviert haben
2. Ein Switchover-Profil muss mit der entsprechenden Richtlinie in der Tabelle Richtlinien-Zuweisungen verlinkt werden

Mit Hilfe des Switchover-Profils kann gesteuert werden, wie schnell die Menge der Sessions auf die neue Leitung bzw. Interface des gleichen Load Balancers umgezogen werden soll.

Um eine Konzentration umziehender Sessions auf einer einzelnen Schnittstelle zu verhindern, werden Sessions i. A. schrittweise in mehreren Gruppen umgezogen, die gleichmäßig auf den konfigurierten Zeitrahmen verteilt werden. Vor jedem Schritt wird geprüft, ob der Switchover noch notwendig ist, da sich in der Zwischenzeit die Policy-Scores und damit die Rangfolge der Interfaces bzgl. einer Policy verändert haben können. Wenn er nicht mehr notwendig ist, wird der Switchover abgebrochen, und die noch nicht verschobenen Sessions bleiben auf ihrer aktuellen Schnittstelle. Wenn er noch notwendig ist, wird für jede Session zufällig bestimmt, ob sie Teil der in diesem Schritt umziehenden Gruppe ist, oder nicht.

Wenn die Anzahl der Schritte = 1 oder die Gesamtzeit = 0 ist, ziehen alle Sessions sofort um.

**SNMP-ID:**

2.110.4.32

**Pfad Konsole:**

**Setup** > **Firewall** > **Dynamische-Pfadauswahl**

**Switchover-Profil**

Der Name des Switchover-Profils. Über diesen Namen wird das Profil referenziert.

**SNMP-ID:**

2.110.4.32.1

**Pfad Konsole:**

**Setup** > **Firewall** > **Dynamische-Pfadauswahl** > **Switchover-Profile**

**Mögliche Werte:**

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

**Schritte**

Anzahl der Schritte bzw. Gruppen, in der die Menge der Sessions auf die neue Leitung verschoben werden soll.

**SNMP-ID:**

2.110.4.32.2

**Pfad Konsole:**

**Setup** > **Firewall** > **Dynamische-Pfadauswahl** > **Switchover-Profile**

**Mögliche Werte:**

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

**Zeitrahmen(s)**

Zeitrahmen in Sekunden innerhalb dessen die Menge der Sessions auf die neue Leitung verschoben werden soll.

**SNMP-ID:**

2.110.4.32.3

**Pfad Konsole:**

**Setup** > **Firewall** > **Dynamische-Pfadauswahl** > **Switchover-Profile**

**Mögliche Werte:**

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

## LB-Switchover

Gibt an, ob die Sessions dieser Regeln im Falle einer besseren Leitung bei Verwendung von Dynamic Path Selection auf diese verschoben werden sollen. Dies ist nur für umaskierte Verbindungen, z. B. VPN-Verbindungen möglich.

**SNMP-ID:**

2.8.10.2.17

**Pfad Konsole:**

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

**Mögliche Werte:**

**nein**
**ja**

**Default-Wert:**

nein

### Flags

Diese Optionen bestimmen, wie die Firewall die Regel behandelt.

Sie können mehrere Optionen gleichzeitig auswählen.

**SNMP-ID:**

2.70.5.2.2

**Pfad Konsole:**

**Setup** > **IPv6** > **Firewall** > **Forwarding-Regeln**

**Mögliche Werte:**

**deaktiviert**
Die Regel ist deaktiviert. Die Firewall überspringt diese Regel.

**verkettet**
Nach dem Abarbeiten der Regel sucht die Firewall nach weiteren Regeln, die für die Ausführung in Frage kommen.

**zustandslos**
Diese Regel beachtet die Zustände von TCP-Sessions nicht.

**LB-Switchover**
Gibt an, ob die Sessions dieser Regeln im Falle einer besseren Leitung bei Verwendung von Dynamic Path Selection auf diese verschoben werden sollen. Dies ist nur für umaskierte Verbindungen, z. B. VPN-Verbindungen möglich.

## 3.2 Bidirectional Forwarding Detection (BFD)

Ab LCOS 10.50 wird das Protokoll Bidirectional Forwarding Detection unterstützt.

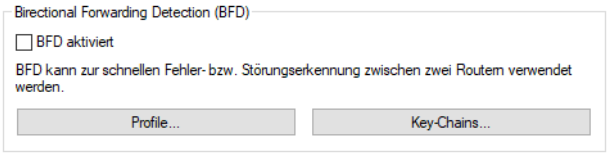
Bidirectional Forwarding Detection nach *RFC 5880* ist ein einfach Hello-Protokoll um den Verlust einer Verbindung zwischen zwei Routern festzustellen. Hello-Pakete werden in einem definierten Intervall von beiden Routern gesendet. Werden in einem bestimmten Intervall diese Hello-Pakete nicht empfangen, so wird angenommen, dass die Verbindung

unterbrochen ist. Im Zusammenspiel mit BGP bietet BFD die Möglichkeit schneller einen Verbindungsverlust zu erkennen, da die BFD-Timer deutlich kleiner gewählt werden können als die BGP-Timer.

Durch das Anpassen des Timer-Intervalls kann die Erkennung von Verbindungsverlusten schneller bzw. langsamer gesteuert werden. Je geringer das Timer-Intervall, umso schneller werden Verbindungsverluste erkannt.

- BFD unterstützt IPv4 und IPv6.
- Ein Echo-Modus wird nicht unterstützt.
- BFD ist ein Protokoll, welches deutlich System-Ressourcen verbraucht bzw. CPU-Zeit und Bandbreite benötigt. BFD wird ausschließlich in Software verarbeitet. Hardware-Verarbeitung wird für BFD nicht unterstützt.
- Wird das Hello-Intervall sehr klein gewählt, so kann es zu BFD-Flapping bzw. zur Erkennung von False-Positives kommen. Treten False-Positives auf, so wird empfohlen das Hello-Intervall zu vergrößern.
- Es wird empfohlen, dass Hello-Intervall nicht unter 250ms zu verwenden.

In LANconfig konfigurieren Sie BFD unter **Routing Protokolle** > **Allgemein** > **Bidirectional Forwarding Detection (BFD)**.

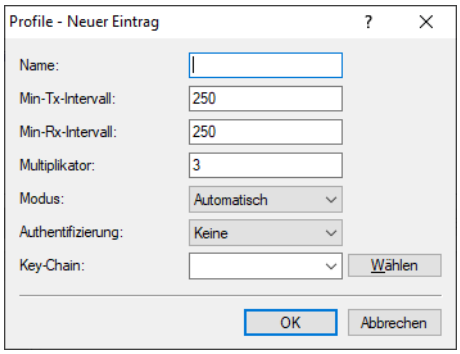



**BFD aktiviert**

Aktiviert bzw. Deaktiviert BFD global.

## 3.2.1 Profile

Zur Konfiguration der BFD-Profile wechseln Sie in die Ansicht **IP-Router** > **Allgemein** > **Bidirectional Forwarding Detection (BFD)** > **Profile**.




**Name**

Vergeben Sie einen aussagekräftigen Namen für dieses BFD-Profil. Der Name wird, falls BFD zusammen mit BGP verwendet werden soll, bei dem entsprechenden BGP-Nachbarn verlinkt.

**Min-Tx-Intervall**

Minimum Intervall in Millisekunden zwischen gesendeten BFD-Kontrollnachrichten. (Wertebereich 1-9999 Millisekunden, Default 250)

**Min-Rx-Intervall**

Minimum Intervall in Millisekunden zwischen empfangenen BFD-Kontrollnachrichten. (Wertebereich 1-9999 Millisekunden, Default 250)

**Multiplikator**

Anzahl von nicht empfangenen Paketen bis ein Interface als Down deklariert wird. Wird der Multiplikator mit dem Intervall multipliziert, so ergibt sich die Zeit, bis eine Verbindung als unterbrochen erkannt wird. (Wertebereich 1-255, Default 3)

**Modus**

Definiert, ob der BFD-Nachbar Single-Hop oder Multi-Hop verbunden ist. Im Single-Hop-Modus wird UDP-Zielport 3784 und Time-to-Live von 1 im IP-Header verwendet. Der Multi-Hop-Modus verwendet UDP-Port 4784. Bei Automatisch wird der Single-Hop-Modus verwendet, falls die Route zum Nachbarn vom Typ Connected LAN oder WAN ist, sonst Multi-Hop. Standardmäßig sind eBGP-Sessions Single-Hop. iBGP-Sessions können Multi-Hop sein. Mögliche Werte:

- Automatisch
- Single-Hop
- Multi-Hop

Default: Automatisch

**Authentifizierung**

Definiert die für BFD-Nachrichten verwendete Art der Authentifizierung. Mögliche Werte:

- Keine
- Passwort
- MD5
- MD5-Meticulous
- SHA1
- SHA1-Meticulous

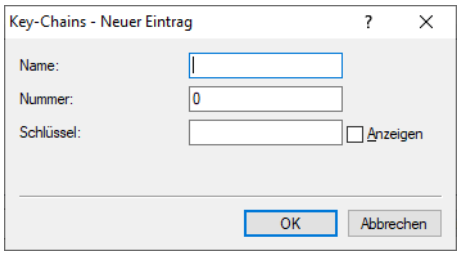
Default: Keine

**Key-Chain**

Name der Key-Chain aus der Tabelle *Key-Chain*. Definiert den verwendeten Schlüssel für die BFD-Nachrichten. Beim Parameter **Authentifizierung** muss ein anderer Wert außer „Keiner" konfiguriert sein.

## 3.2.2 Key-Chains

Zur Konfiguration der Key-Chains wechseln Sie in die Ansicht **IP-Router** > **Allgemein** > **Bidirectional Forwarding Detection (BFD)** > **Key-Chains**.




**Name**

Vergeben Sie einen aussagekräftigen Namen für diese Key-Chain. Über diesen wird diese Key-Chain in den *BFD-Profilen* referenziert.

**Nummer**

Nummer der Key-Chain.

**Schlüssel**

Schlüssel bzw. Passwort für diese Key-Chain.

## 3.2.3 Show-Commands über CLI

Ihnen stehen folgende Show-Kommandos zur Verfügung:

- **show BFD-v4-details**

  Zeigt Details zu den IPv4-BFD-Verbindungen an.

- **show BFD-v6-details**

  Zeigt Details zu den IPv6-BFD-Verbindungen an an.

- **show BFD-v4-status**

  Zeigt den Status der IPv4-BFD-Verbindungen an.

- **show BFD-v6-status**

  Zeigt den Status der IPv6-BFD-Verbindungen an.

## 3.2.4 Ergänzungen im Setup-Menü

### BFD-Profil

Enthält den Namen eines BFD-Profils aus **Setup** > **Routing-Protokolle** > **BFD** > **Profile**. Im Zusammenspiel mit BGP bietet BFD die Möglichkeit schneller einen Verbindungsverlust zu erkennen, da die BFD-Timer deutlich kleiner gewählt werden können als die BGP-Timer.

**SNMP-ID:**

2.93.1.2.17

**Pfad Konsole:**

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

**Mögliche Werte:**

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

### BFD

In diesem Verzeichnis konfigurieren Sie das Protokoll Bidirectional Forwarding Detection (BFD). BFD nach *RFC 5880* ist ein einfach Hello-Protokoll um den Verlust einer Verbindung zwischen zwei Routern festzustellen. Hello-Pakete werden in einem definierten Intervall von beiden Routern gesendet. Werden in einem bestimmten Intervall diese Hello-Pakete nicht empfangen, so wird angenommen, dass die Verbindung unterbrochen ist. Im Zusammenspiel mit BGP bietet BFD die Möglichkeit schneller einen Verbindungsverlust zu erkennen, da die BFD-Timer deutlich kleiner gewählt werden können als die BGP-Timer.

Durch das Anpassen des Timer-Intervalls kann die Erkennung von Verbindungsverlusten schneller bzw. langsamer gesteuert werden. Je geringer das Timer-Intervall, umso schneller werden Verbindungsverluste erkannt.

- BFD unterstützt IPv4 und IPv6.
- Ein Echo-Modus wird nicht unterstützt.

- BFD ist ein Protokoll, welches deutlich System-Ressourcen verbraucht bzw. CPU-Zeit und Bandbreite benötigt. BFD wird ausschließlich in Software verarbeitet. Hardware-Verarbeitung wird für BFD nicht unterstützt.
- Wird das Hello-Intervall sehr klein gewählt, so kann es zu BFD-Flapping bzw. zur Erkennung von False-Positives kommen. Treten False-Positives auf, so wird empfohlen das Hello-Intervall zu vergrößern.
- Es wird empfohlen, dass Hello-Intervall nicht unter 250ms zu verwenden.

**SNMP-ID:**

2.93.6

**Pfad Konsole:**

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

### Key-Chains

Konfigurieren Sie hier die Key-Chains für BFD.

**SNMP-ID:**

2.93.6.1

**Pfad Konsole:**

**Setup** > **Routing-Protokolle** > **BFD**

### Name

Vergeben Sie einen aussagekräftigen Namen für diese Key-Chain. Über diesen wird diese Key-Chain in den BFD-Profilen referenziert.

**SNMP-ID:**

2.93.6.1.1

**Pfad Konsole:**

**Setup** > **Routing-Protokolle** > **BFD** > **Key-Chains**

**Mögliche Werte:**

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

### Nummer

Nummer der Key-Chain.

**SNMP-ID:**

2.93.6.1.2

**Pfad Konsole:**

**Setup** > **Routing-Protokolle** > **BFD** > **Key-Chains**

**Mögliche Werte:**

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

### Key

Schlüssel bzw. Passwort für diese Key-Chain.

**SNMP-ID:**

2.93.6.1.3

**Pfad Konsole:**

**Setup** > **Routing-Protokolle** > **BFD** > **Key-Chains**

**Mögliche Werte:**

max. 80 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

### Profile

Konfigurieren Sie hier die BFD-Profile.

**SNMP-ID:**

2.93.6.2

**Pfad Konsole:**

**Setup** > **Routing-Protokolle** > **BFD**

### Name

Vergeben Sie einen aussagekräftigen Namen für dieses BFD-Profil. Der Name wird, falls BFD zusammen mit BGP verwendet werden soll, bei dem entsprechenden BGP-Nachbarn verlinkt.

**SNMP-ID:**

2.93.6.2.1

**Pfad Konsole:**

**Setup** > **Routing-Protokolle** > **BFD** > **Profile**

**Mögliche Werte:**

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

**Min-Tx-Intervall**

Minimum Intervall in Millisekunden zwischen gesendeten BFD-Kontrollnachrichten.

**SNMP-ID:**

2.93.6.2.2

**Pfad Konsole:**

**Setup** > **Routing-Protokolle** > **BFD** > **Profile**

**Mögliche Werte:**

1 … 9999

**Default-Wert:**

250

**Min-Rx-Intervall**

Minimum Intervall in Millisekunden zwischen empfangenen BFD-Kontrollnachrichten.

**SNMP-ID:**

2.93.6.2.3

**Pfad Konsole:**

**Setup** > **Routing-Protokolle** > **BFD** > **Profile**

**Mögliche Werte:**

1 … 9999

**Default-Wert:**

250

**Multiplikator**

Anzahl von nicht empfangenen Paketen bis ein Interface als Down deklariert wird. Wird der Multiplikator mit dem Intervall multipliziert, so ergibt sich die Zeit, bis eine Verbindung als unterbrochen erkannt wird.

**SNMP-ID:**

2.93.6.2.4

**Pfad Konsole:**

**Setup** > **Routing-Protokolle** > **BFD** > **Profile**

**Mögliche Werte:**

1 … 255

**Default-Wert:**

3

#### Authentifizierung

Definiert die für BFD-Nachrichten verwendete Art der Authentifizierung.

**SNMP-ID:**

2.93.6.2.6

**Pfad Konsole:**

**Setup** > **Routing-Protokolle** > **BFD** > **Profile**

**Mögliche Werte:**

**Keine**
**Passwort**
**MD5**
**MD5-Meticulous**
**SHA1**
**SHA1-Meticulous**

**Default-Wert:**

Keine

#### Key-Chain

Name der Key-Chain aus der Tabelle *2.93.6.1 Key-Chains* auf Seite 26. Definiert den verwendeten Schlüssel für die BFD-Nachrichten. Beim Parameter *2.93.6.2.6 Authentifizierung* auf Seite 29 muss ein anderer Wert außer „Keiner" konfiguriert sein.

**SNMP-ID:**

2.93.6.2.7

**Pfad Konsole:**

**Setup** > **Routing-Protokolle** > **BFD** > **Profile**

**Mögliche Werte:**

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

#### Modus

Definiert, ob der BFD-Nachbar Single-Hop oder Multi-Hop verbunden ist. Im Single-Hop-Modus wird UDP-Zielport 3784 und Time-to-Live von 1 im IP-Header verwendet. Der Multi-Hop-Modus verwendet UDP-Port 4784. Bei Automatisch wird der Single-Hop-Modus verwendet, falls die Route zum Nachbarn vom Typ Connected LAN oder WAN ist, sonst Multi-Hop. Standardmäßig sind eBGP-Sessions Single-Hop. iBGP-Sessions können Multi-Hop sein.

**SNMP-ID:**

2.93.6.2.8

**Pfad Konsole:**

**Setup** > **Routing-Protokolle** > **BFD** > **Profile**

**Mögliche Werte:**

**Automatisch**
**Single-Hop**
**Multi-Hop**

**Default-Wert:**

Automatisch

**Aktiv**

Aktiviert bzw. Deaktiviert BFD global.

**SNMP-ID:**

2.93.6.3

**Pfad Konsole:**

**Setup** > **Routing-Protokolle** > **BFD**

**Mögliche Werte:**

**nein**
**ja**

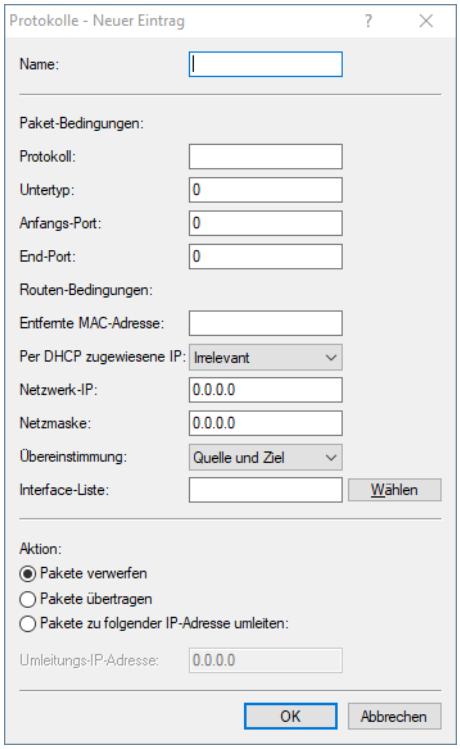
**Default-Wert:**

nein

## 3.3 Einschränkung von Protokollfiltern auf Quell- oder Zieladressen

Die (W)LAN-Protokollfilter unter **Schnittstellen** > **LAN** > **LAN-Bridge** > **Protokolle** erlauben es, eine Regel an ein IP-Netz zu binden. Dabei wird geschaut, ob entweder die Quell- oder Zieladresse eines Pakets auf das konfigurierte

IP-Netz matcht. Bisher wurde sowohl auf die Quell-, als auch auf die Zieladresse geprüft. Ab LCOS 10.50 lässt sich nun festlegen, ob auf die Quell- oder Zieladresse geprüft werden soll. Standardmäßig ist das bisherige Verhalten aktiv.




**Übereinstimmung**

Per Voreinstellung wird sowohl auf die Quell- als auch auf die Zieladresse geprüft. Hier können Sie festlegen, ob stattdessen nur auf die Quell- oder Zieladresse geprüft werden soll.

## 3.3.1 Ergänzungen im Setup-Menü

### IP-Vergleich

Per Voreinstellung wird sowohl auf die Quell- als auch auf die Zieladresse geprüft. Hier können Sie festlegen, ob stattdessen nur auf die Quell- oder Zieladresse geprüft werden soll.

**SNMP-ID:**

2.20.10.14

**Pfad Konsole:**

**Setup** > **LAN-Bridge** > **Protokoll-Tabelle**

**Mögliche Werte:**

**beide**

Es wird sowohl auf die Quell- als auch auf die Zieladresse geprüft.

**Quelle**

Es wird nur auf die Quelladresse geprüft.

**Ziel**

Es wird nur auf die Zieladresse geprüft.

**Default-Wert:**

beide

# 3.4 Netzwerkname bei IPv6-Variablen der Aktionstabelle

Ab LCOS 10.50 RU5 wurden neue Variablen für die Syntax in der Aktionstabelle hinzugefügt. Bei den IPv6-Variablen %x und %y können nun auch der LAN-Netzwerkname übergeben werden, der für diese Variable verwendet wird. Die Variablen %x und %y übertragen nur die Werte des Netzwerks mit dem festen Namen INTRANET.

- `%{xNetzwerkname}` – z. B. `%{xTESTNETZ}` für das aktuelle IPv6-LAN-Präfix des Netzwerks TESTNETZ als String im Format „fd00:0:0:1::/64“.

  Die Variable `%x` überträgt nur die Werte des Netzwerks mit dem festen Namen INTRANET. Hiermit kann auch der LAN-Netzwerkname übergeben werden, der für diese Variable verwendet wird.

- `%{yNetzwerkname}` – z. B. `%{yTESTNETZ}` für die aktuelle IPv6-LAN-Adresse des Geräts im Netzwerk TESTNETZ als String im Format „fd00::1:2a0:57ff:fa1b:9d7b“.

  Die Variable `%y` überträgt nur die Werte des Netzwerks mit dem festen Namen INTRANET. Hiermit kann auch der LAN-Netzwerkname übergeben werden, der für diese Variable verwendet wird.

## 3.4.1 Ergänzungen im Setup-Menü

### Aktion

Hier beschreiben Sie die Aktion, die beim Zustandswechsel der WAN-Verbindung ausgeführt werden soll. In jedem Eintrag darf nur eine Aktionen ausgeführt werden. Das Ergebnis der Aktionen kann im Feld 'Pruefen-auf' ausgewertet werden.

Prefixe:

- exec: – Mit diesem Prefix leiten Sie alle Befehle ein, wie sie an der Telnet-Konsole eingegeben würden. Sie können z. B. mit der Aktion 'exec:do /o/m/d' alle bestehenden Verbindungen beenden.
- `dnscheck:` – Mit diesem Präfix leiten Sie eine IPv4-DNS-Namensauflösung ein. Sie können z. B. mit der Aktion `dnscheck:myserver.dyndns.org` die IPv4-Adresse des angegebenen Servers ermitteln.
- `dnscheck6:` – Mit diesem Präfix leiten Sie eine IPv6-DNS-Namensauflösung ein. Sie können z. B. mit der Aktion `dnscheck6:myserver.dyndns.org` die IPv6-Adresse des angegebenen Servers ermitteln.
- http: – Mit diesem Prefix lösen Sie eine HTTP-Get-Anfrage aus. Sie können z. B. mit der folgenden Aktion eine DynDNS-Aktualisierung bei dyndns.org durchführen:

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

  Die Bedeutung der Platzhalter %h und %a wird im folgenden Absatz beschrieben.)
- https: – Wie 'http:', nur über eine verschlüsselte Verbindung.
- `gnudip:` – Mit diesem Präfix lösen Sie eine Anfrage über das GnuDIP-Protokoll an einen entsprechenden DynDNS-Server aus. Sie können z. B. mit der folgenden Aktion eine DynDNS-Aktualisierung bei einem DynDNS-Anbieter über das GnuDIP-Protokoll durchführen:

  ```
  gnudip://gnudipsrv?method=tcp&user=myserver&domn=mydomain.org&pass=password&reqc=0&addr=%a
  ```

  Die Bedeutung des Platzhalters `%a` erfahren Sie in den folgenden Absätzen.

- repeat: – Mit diesem Prefix und der Angabe einer Zeit in Sekunden werden alle Aktionen mit der Bedingung "Aufbau" wiederholt ausgeführt, sobald die Verbindung aufgebaut ist. Mit der Aktion 'repeat:300' werden z. B. alle Aufbau-Aktionen alle fünf Minuten wiederholt.
- mailto: – Mit diesem Prefix lösen Sie den Versand einer E-Mail aus. Sie können z. B. mit der folgenden Aktion eine E-Mail an den Systemadministrator versenden, wenn eine Verbindung beendet wurde: mailto:admin@mycompany.de?subject=VPN-Verbindung abgebrochen um %t?body=VPN-Verbindung zu Filiale 1 wurde unterbrochen.

Mögliche Variablen zur Erweiterung der Aktionen:

- `%a` – WAN-IPv4-Adresse der WAN-Verbindung, in deren Kontext diese Aktion erfolgt.
- `%x` – das aktuelle IPv6-LAN-Präfix als String im Format „fd00:0:0:1::/64".
- `%{x`*`Netzwerkname`*`}` – z. B. `%{xTESTNETZ}` für das aktuelle IPv6-LAN-Präfix des Netzwerks TESTNETZ als String im Format „fd00:0:0:1::/64".

  Die Variable `%x` überträgt nur die Werte des Netzwerks mit dem festen Namen INTRANET. Hiermit kann auch der LAN-Netzwerkname übergeben werden, der für diese Variable verwendet wird.
- `%y` – die aktuelle IPv6-LAN-Adresse des Geräts als String im Format „fd00::1:2a0:57ff:fa1b:9d7b".
- `%{y`*`Netzwerkname`*`}` – z. B. `%{yTESTNETZ}` für die aktuelle IPv6-LAN-Adresse des Geräts im Netzwerk TESTNETZ als String im Format „fd00::1:2a0:57ff:fa1b:9d7b".

  Die Variable `%y` überträgt nur die Werte des Netzwerks mit dem festen Namen INTRANET. Hiermit kann auch der LAN-Netzwerkname übergeben werden, der für diese Variable verwendet wird.
- `%z` – WAN-IPv6-Adresse der WAN-Verbindung, in deren Kontext diese Aktion erfolgt.
- `%H` – Hostname der WAN-Verbindung, in deren Kontext diese Aktion erfolgt.
- `%h` – wie `%H`, nur Hostname in Kleinbuchstaben.
- `%c` – Verbindungsname der WAN-Verbindung, in deren Kontext diese Aktion erfolgt.
- `%n` – Gerätename
- `%s` – Seriennummer des Gerätes
- `%m` – MAC-Adresse des Gerätes (wie im Sysinfo)
- `%t` – Uhrzeit und Datum, im Format `YYYY-MM-DD hh:mm:ss`
- `%e` – Bezeichnung des Fehlers, der bei einem nicht erfolgreichen Verbindungsaufbau gemeldet wurde.

**SNMP-ID:**

2.2.25.6

**Pfad Konsole:**

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

**Mögliche Werte:**

max. 250 Zeichen

**Default-Wert:**

*leer*

# 4 IPv6

## 4.1 NPTv6

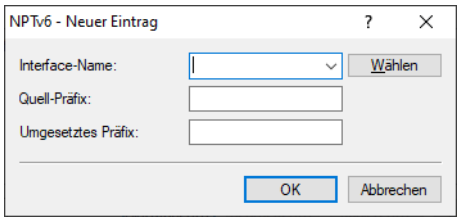
NPTv6 (Network Prefix Translation) nach *RFC 6296* erlaubt die Umsetzung eines IPv6-Präfixes auf ein anderes IPv6-Präfix. Die Umsetzung erfolgt 1:1, d. h. eine Adresse aus Präfix A wird auf eine Adresse aus Präfix B umgesetzt. Es wird dabei nur der Präfix-Teil umgesetzt, der Host-Teil bleibt erhalten. Dieses Verfahren arbeitet somit „Stateless“. Mit NPTv6 ist es nicht möglich, wie bei IPv4, ein ganzes Netzwerk hinter einer Adresse zu maskieren.

Anwendungsszenarien für NPTv6 sind z. B. VPNs oder Netzwerke mit dynamischen Präfixen wo Adressunabhängigkeit erreicht werden soll. Teilt der Provider ein dynamisches Präfix zu, so ändert sich in der Regel das Präfix bei jedem Verbindungsaufbau. Dies ist aber nicht gewünscht, wenn bestimmte Ressourcen feste IP-Adressen benötigen. Mit NPTv6 werden dann Adressen aus dem (privaten) ULA-Bereich fd00::/8 an die Clients im Netzwerk vergeben und durch eine NPTv6-Regel diese Adressen auf das Provider-Präfix umgesetzt.

Ein weiterer Anwendungsfall ist ein Load Balancer-Szenario mit mehreren Internetprovidern, wobei jeder Provider ein eigenes Präfix vergibt. Mit NPTv6 werden dann Adressen aus dem ULA-Bereich fd00::/8 an die Clients im Netzwerk vergeben und durch mehrere NPTv6-Regeln diese Adressen auf die Provider-Präfixe umgesetzt.

Die IPv6-Firewall muss für NPTv6 grundsätzlich aktiviert sein.

In LANconfig erfolgt die Konfiguration unter **Firewall/QoS** > **IPv6-Regeln** > **NPTv6**.




**Interface-Name**

Name des Netzwerks bzw. der Gegenstelle, auf der NPTv6 gemacht werden soll. Soll ein Präfix für ein dynamisches Provider-Präfix umgesetzt werden, so muss hier der Name der Internet-Verbindung bzw. Gegenstelle, z. B. INTERNET, konfiguriert werden.

**Quell-Präfix**

Präfix des Quellnetzwerks, z. B. ein explizites Präfix fd00::/64.

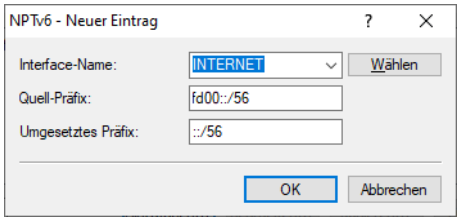
**Umgesetztes Präfix**

Präfix auf das das Quell-Präfix umgesetzt werden soll. Es kann entweder ein explizites Präfix wie 2001:db8::/32 oder der Platzhalter :: mit entsprechender Präfixlänge, falls der Provider ein dynamisches Präfix vergibt, konfiguriert werden.

## 4.1.1 Beispiele

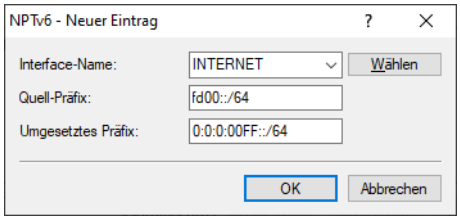
### Beispiel 1

Der Provider (Gegenstelle INTERNET) vergibt ein dynamisches Präfix mit Länge /56. Im Intranet ist das Präfix fd00::/64 konfiguriert. Das Quell-Präfix fd00::/56 soll auf das gesamte Provider-Präfix (::/56) 1:1 umgesetzt werden.



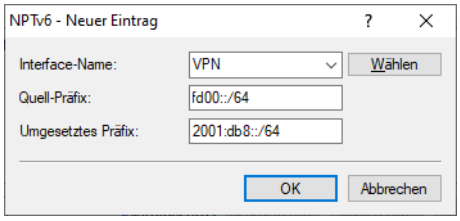

### Beispiel 2

Der Provider (Gegenstelle INTERNET) vergibt ein dynamisches Präfix mit Länge /56. Im Intranet ist das Präfix fd00::/64 konfiguriert. Das Quell-Präfix fd00::/64 soll auf das spezielle Subnetz „FF" aus dem dynamischen Provider-Präfix umgesetzt werden. Als umgesetztes Präfix wird der Platzhalter :: mit Subnetz-ID FF konfiguriert, d. h. 0:0:0:00FF::/64.




### Beispiel 3

Für ein VPN-Szenario soll das interne Quell-Präfix fd00::/64 auf das Präfix 2001:db8::/64 umgesetzt werden.




## 4.1.2 Show-Commands über CLI

Ihnen stehen folgende Show-Kommandos zur Verfügung:

- **show ipv6-npt**

  Zeigt die NPTv6-Umsetzungsregel an.

## 4.1.3 Ergänzungen im Setup-Menü

### NPTv6

NPTv6 (Network Prefix Translation) nach *RFC 6296* erlaubt die Umsetzung eines IPv6-Präfixes auf ein anderes IPv6-Präfix. Die Umsetzung erfolgt 1:1, d. h. eine Adresse aus Präfix A wird auf eine Adresse aus Präfix B umgesetzt. Es wird dabei nur der Präfix-Teil umgesetzt, der Host-Teil bleibt erhalten. Dieses Verfahren arbeitet somit „Stateless". Mit NPTv6 ist es nicht möglich, wie bei IPv4, ein ganzes Netzwerk hinter einer Adresse zu maskieren.

Anwendungsszenarien für NPTv6 sind z. B. VPNs oder Netzwerke mit dynamischen Präfixen wo Adressunabhängigkeit erreicht werden soll. Teilt der Provider ein dynamisches Präfix zu, so ändert sich in der Regel das Präfix bei jedem Verbindungsaufbau. Dies ist aber nicht gewünscht, wenn bestimmte Ressourcen feste IP-Adressen benötigen. Mit NPTv6 werden dann Adressen aus dem (privaten) ULA-Bereich fd00::/8 an die Clients im Netzwerk vergeben und durch eine NPTv6-Regel diese Adressen auf das Provider-Präfix umgesetzt.

Ein weiterer Anwendungsfall ist ein Load Balancer Szenario mit mehreren Internetprovidern, wobei jeder Provider ein eigenes Präfix vergibt. Mit NPTv6 werden dann Adressen aus dem ULA-Bereich fd00::/8 an die Clients im Netzwerk vergeben und durch mehrere NPTv6-Regeln diese Adressen auf die Provider-Präfixe umgesetzt.

Die IPv6-Firewall muss für NPTv6 grundsätzlich aktiviert sein.

**SNMP-ID:**

2.70.5.30

**Pfad Konsole:**

**Setup** > **IPv6** > **Firewall**

**Interface-Name**

Name des Netzwerks bzw. der Gegenstelle, auf der NPTv6 gemacht werden soll. Soll ein Präfix für ein dynamisches Provider-Präfix umgesetzt werden, so muss hier der Name der Internet-Verbindung bzw. Gegenstelle, z. B. INTERNET, konfiguriert werden.

**SNMP-ID:**

2.70.5.30.1

**Pfad Konsole:**

**Setup** > **IPv6** > **Firewall** > **NPTV6**

**Mögliche Werte:**

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

**Quell-Prefix**

Präfix des Quellnetzwerks, z. B. ein explizites Präfix fd00::/64.

**SNMP-ID:**

2.70.5.30.2

**Pfad Konsole:**

**Setup** > **IPv6** > **Firewall** > **NPTV6**

**Mögliche Werte:**

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

**Umgesetztes-Prefix**

Präfix auf das das Quell-Präfix umgesetzt werden soll. Es kann entweder ein explizites Präfix wie 2001:db8::/32 oder der Platzhalter :: mit entsprechender Präfixlänge, falls der Provider ein dynamisches Präfix vergibt, konfiguriert werden.

**SNMP-ID:**

2.70.5.30.3

**Pfad Konsole:**

**Setup** > **IPv6** > **Firewall** > **NPTV6**

**Mögliche Werte:**

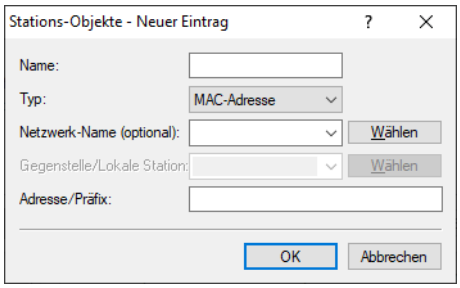
max. 43 Zeichen aus `[A-F][a-f][0-9]:./`

## 4.2 MAC-Adressen als Stations-Objekte

Ab LCOS 10.50 können MAC-Adressen als Stations-Objekte in der IPv6-Firewall verwendet werden. Damit können Regeln für Ressourcen im internen Netzwerk angelegt werden, die anhand ihrer MAC-Adresse identifiziert werden. In Dual-Stack-Netzwerken erleichtert dies die Korrelation zu IPv4-Stationsobjekten, die ebenfalls anhand ihrer MAC-Adresse mit einer IPv4-Regel behandelt werden.

MAC-Adressen sind nur in Regeln als Quelle erlaubt, nicht jedoch als Ziel.

LANconfig: **Firewall/QoS** > **IPv6-Regeln** > **Stations-Objekte**




**Typ**

Bestimmt den Stationstyp. Von der Auswahl hängt ab, welche der nachfolgenden Tabellenspalten (**Netzwerk-Name**, **Gegenstelle/Lokale Station** und **Adresse/Präfix**) ausgefüllt werden müssen. Neuer Wert:

**MAC-Adresse**

Damit können Regeln für Ressourcen im internen Netzwerk angelegt werden, die anhand ihrer MAC-Adresse identifiziert werden. In Dual-Stack-Netzwerken erleichtert dies die Korrelation zu IPv4-Stationsobjekten, die ebenfalls anhand ihrer MAC-Adresse mit einer IPv4-Regel behandelt werden.

- Die Spalte **Netzwerk-Name** ist optional und kann einen Netzwerknamen enthalten, in dem sich das Stations-Objekt befindet.
- Die Spalte **Adresse/Präfix** enthält die MAC-Adresse anhand derer das Objekt identifiziert werden soll.

## 4.2.1 Ergänzungen im Setup-Menü

### Typ

Bestimmt den Stationstyp. Von der Auswahl hängt ab, welche der nachfolgenden Tabellenspalten (*>Lokales-Netzwerk*, *Gegenstelle/Host-Name* und *Adresse/Praefix*) ausgefüllt werden müssen.

**SNMP-ID:**

2.70.5.9.2

**Pfad Konsole:**

**Setup** > **IPv6** > **Firewall** > **Stationen**

**Mögliche Werte:**

**Lokales-Netzwerk**

Name eines lokalen Netzwerks z. B. INTRANET.

- Nur die Spalte *Lokales-Netzwerk* ist auszufüllen.
- Sie kann einen Interface-Namen enthalten, dann besteht die Station aus allen Netzen an diesem Interface.
- Falls Sie eine Netzwerk-Gruppe eintragen, dann besteht die Station aus allen Präfixen unter *Adressen* mit dieser Gruppe.

**Gegenstelle**

Name einer WAN-Gegenstelle z. B. INTERNET.

- Nur die Spalte *Gegenstelle/Host-Name* ist auszufüllen.
- Sie kann ein WAN-Interface oder ein RAS-Template enthalten und löst zu allen Präfixen / Netzen auf, zu denen eine Route über dieses WAN-Interface oder über ein RAS-Interface zu diesem Template existiert.

**Praefix**

IPv6-Präfix

- Nur die Spalte *Adresse/Praefix* ist auszufüllen.
- Sie enthält ein IPv6-Präfix, z. B. „2001:db8::/32“.

**Identifier**

- Die Spalten *Lokales-Netzwerk* und *Adresse/Praefix* sind beide auszufüllen
- *Lokales-Netzwerk* enthält ein WAN-Interface oder ein RAS-Template.
- *Adresse/Praefix* enthält einen IPv6-Identifier. Dies sind die letzten 64 Bit der IPv6-Adresse eines IPv6-Hosts, z. B. „::2a0:57ff:fe1b:3a6a“. Der Wert muss zwei führende Doppelpunkte enthalten.
- Dieser Identfier wird mit allen Netzen des Interfaces unter *Lokales-Netzwerk* bzw. den Netzwerken des RAS-Interfaces zum angegebenen Template zu einer Adresse kombiniert.
- Außerdem wird zu jedem dieser Interfaces eine link-lokale Adresse mit diesem Identifier gebildet.

**IP-Adresse**

- Nur die Spalte *Adresse/Praefix* ist auszufüllen.
- Sie enthält eine IPv6-Adresse, z. B. „2001:db8::1“

**benamter-Host**

Name eines lokalen IPv6-Hosts bzw. einer lokalen Station.

- Die Spalte *Gegenstelle/Host-Name* ist auszufüllen und enthält einen Hostnamen.
- Die Spalte *Lokales-Netzwerk* ist optional und kann ein LAN-Interface enthalten.

- Der Hostname wird mit Hilfe des DHCPv6-Servers oder des DNS-Servers im Gerät zu einer Hostadresse aufgelöst.
- Wenn ein Interface angegeben wurde, dann wird die Adresse nur genommen, falls sie über dieses Interface erreicht wird.

**MAC-Adresse**

Damit können Regeln für Ressourcen im internen Netzwerk angelegt werden, die anhand ihrer MAC-Adresse identifiziert werden. In Dual-Stack-Netzwerken erleichtert dies die Korrelation zu IPv4-Stationsobjekten, die ebenfalls anhand ihrer MAC-Adresse mit einer IPv4-Regel behandelt werden.

- Die Spalte *Lokales-Netzwerk* ist optional und kann einen Netzwerknamen enthalten, in dem sich das Stations-Objekt befindet.
- Die Spalte *Adresse/Praefix* enthält die MAC-Adresse anhand derer das Objekt identifiziert werden soll.

MAC-Adressen sind nur in Regeln als Quelle erlaubt, nicht jedoch als Ziel.

**Delegiertes-Praefix**

Damit kann insbesondere im Falle eines dynamischen Provider-Präfixes eine Regel für nachgeschaltete Router oder Ressourcen definiert werden.

- Die Spalte *Lokales-Netzwerk* ist optional und kann einen Netzwerknamen enthalten, in dem sich das Stations-Objekt befindet. Dies kann als Einschränkung auf das lokale Netzwerk verwendet werden.
- Die Spalte *Gegenstelle/Host-Name* ist erforderlich und sollte die Gegenstelle enthalten, von der das delegierte Präfix bezogen bzw. abgeleitet wird.
- Die Spalte *Adresse/Praefix* enthält ein Präfix oder eine Adresse, die mit dem vom Provider bezogenen Präfix verknüpft (Oder-Verknüpfung) wird. Wenn sich das Objekt auf das gesamte Präfix beziehen soll, so kann entweder ::/0 konfiguriert werden oder der Eintrag leer gelassen werden.

  **Beispiel:** Der Provider delegiert das Präfix 2001:db8:1234::/48 auf der Gegenstelle INTERNET.

  - Soll das Subnetz abcd verwendet werden, so muss als *Adresse/Praefix* der Wert 0:0:0:abcd::/48 konfiguriert werden.
  - Soll nur die Adresse 2001:db8:0:23::dead:beef/128 verwendet werden, so muss als *Adresse/Praefix* 0:0:0:23::dead:beef/128 konfiguriert werden.
  - Soll das gesamte Präfix verwendet werden, so muss als *Adresse/Praefix* ::/0 konfiguriert werden oder der Eintrag leer gelassen werden.

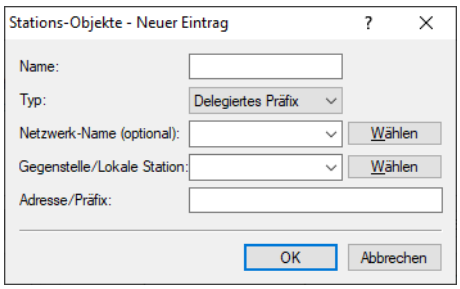
**Default-Wert:**

Lokales-Netzwerk

## 4.3 Delegiertes Präfix als Stations-Objekte

Ab LCOS 10.50 kann das vom Provider delegierte Präfix als Stations-Objekt in der IPv6-Firewall verwendet werden. Damit kann insbesondere im Falle eines dynamischen Provider-Präfixes eine Regel für nachgeschaltete Router oder Ressourcen definiert werden.

LANconfig: **Firewall/QoS** > **IPv6-Regeln** > **Stations-Objekte**




**Delegiertes Präfix**

Damit kann insbesondere im Falle eines dynamischen Provider-Präfixes eine Regel für nachgeschaltete Router oder Ressourcen definiert werden.

- Die Spalte **Netzwerk-Name** ist optional und kann einen Netzwerknamen enthalten, in dem sich das Stations-Objekt befindet. Dies kann als Einschränkung auf das lokale Netzwerk verwendet werden.
- Die Spalte **Gegenstelle/Lokale Station** ist erforderlich und sollte die Gegenstelle enthalten, von der das delegierte Präfix bezogen bzw. abgeleitet wird.
- Die Spalte **Adresse/Präfix** enthält ein Präfix oder eine Adresse, die mit dem vom Provider bezogenen Präfix verknüpft (Oder-Verknüpfung) wird. Wenn sich das Objekt auf das gesamte Präfix beziehen soll, so kann entweder ::/0 konfiguriert werden oder der Eintrag leer gelassen werden.

  **Beispiel:** Der Provider delegiert das Präfix 2001:db8:1234::/48 auf der Gegenstelle INTERNET.

  - Soll das Subnetz abcd verwendet werden, so muss als**Adresse/Präfix** der Wert 0:0:0:abcd::/48 konfiguriert werden.
  - Soll nur die Adresse 2001:db8:0:23::dead:beef/128 verwendet werden, so muss als **Adresse/Präfix** 0:0:0:23::dead:beef/128 konfiguriert werden.
  - Soll das gesamte Präfix verwendet werden, so muss als **Adresse/PräfixAdresse/Präfix** ::/0 konfiguriert werden oder der Eintrag leer gelassen werden.

## 4.3.1 Ergänzungen im Setup-Menü

### Typ

Bestimmt den Stationstyp. Von der Auswahl hängt ab, welche der nachfolgenden Tabellenspalten (*>Lokales-Netzwerk*, *Gegenstelle/Host-Name* und *Adresse/Praefix*) ausgefüllt werden müssen.

**SNMP-ID:**

2.70.5.9.2

**Pfad Konsole:**

**Setup** > **IPv6** > **Firewall** > **Stationen**

**Mögliche Werte:**

**Lokales-Netzwerk**

Name eines lokalen Netzwerks z. B. INTRANET.

- Nur die Spalte *Lokales-Netzwerk* ist auszufüllen.
- Sie kann einen Interface-Namen enthalten, dann besteht die Station aus allen Netzen an diesem Interface.

- Falls Sie eine Netzwerk-Gruppe eintragen, dann besteht die Station aus allen Präfixen unter *Adressen* mit dieser Gruppe.

**Gegenstelle**

Name einer WAN-Gegenstelle z. B. INTERNET.

- Nur die Spalte *Gegenstelle/Host-Name* ist auszufüllen.
- Sie kann ein WAN-Interface oder ein RAS-Template enthalten und löst zu allen Präfixen / Netzen auf, zu denen eine Route über dieses WAN-Interface oder über ein RAS-Interface zu diesem Template existiert.

**Praefix**

IPv6-Präfix

- Nur die Spalte *Adresse/Praefix* ist auszufüllen.
- Sie enthält ein IPv6-Präfix, z. B. „2001:db8::/32“.

**Identifier**

- Die Spalten *Lokales-Netzwerk* und *Adresse/Praefix* sind beide auszufüllen
- *Lokales-Netzwerk* enthält ein WAN-Interface oder ein RAS-Template.
- *Adresse/Praefix* enthält einen IPv6-Identifier. Dies sind die letzten 64 Bit der IPv6-Adresse eines IPv6-Hosts, z. B. „::2a0:57ff:fe1b:3a6a“. Der Wert muss zwei führende Doppelpunkte enthalten.
- Dieser Identfier wird mit allen Netzen des Interfaces unter *Lokales-Netzwerk* bzw. den Netzwerken des RAS-Interfaces zum angegebenen Template zu einer Adresse kombiniert.
- Außerdem wird zu jedem dieser Interfaces eine link-lokale Adresse mit diesem Identifier gebildet.

**IP-Adresse**

- Nur die Spalte *Adresse/Praefix* ist auszufüllen.
- Sie enthält eine IPv6-Adresse, z. B. „2001:db8::1“

**benamter-Host**

Name eines lokalen IPv6-Hosts bzw. einer lokalen Station.

- Die Spalte *Gegenstelle/Host-Name* ist auszufüllen und enthält einen Hostnamen.
- Die Spalte *Lokales-Netzwerk* ist optional und kann ein LAN-Interface enthalten.
- Der Hostname wird mit Hilfe des DHCPv6-Servers oder des DNS-Servers im Gerät zu einer Hostadresse aufgelöst.
- Wenn ein Interface angegeben wurde, dann wird die Adresse nur genommen, falls sie über dieses Interface erreicht wird.

**MAC-Adresse**

Damit können Regeln für Ressourcen im internen Netzwerk angelegt werden, die anhand ihrer MAC-Adresse identifiziert werden. In Dual-Stack-Netzwerken erleichtert dies die Korrelation zu IPv4-Stationsobjekten, die ebenfalls anhand ihrer MAC-Adresse mit einer IPv4-Regel behandelt werden.

- Die Spalte *Lokales-Netzwerk* ist optional und kann einen Netzwerknamen enthalten, in dem sich das Stations-Objekt befindet.
- Die Spalte *Adresse/Praefix* enthält die MAC-Adresse anhand derer das Objekt identifiziert werden soll.



MAC-Adressen sind nur in Regeln als Quelle erlaubt, nicht jedoch als Ziel.

**Delegiertes-Praefix**

Damit kann insbesondere im Falle eines dynamischen Provider-Präfixes eine Regel für nachgeschaltete Router oder Ressourcen definiert werden.

- Die Spalte *Lokales-Netzwerk* ist optional und kann einen Netzwerknamen enthalten, in dem sich das Stations-Objekt befindet. Dies kann als Einschränkung auf das lokale Netzwerk verwendet werden.
- Die Spalte *Gegenstelle/Host-Name* ist erforderlich und sollte die Gegenstelle enthalten, von der das delegierte Präfix bezogen bzw. abgeleitet wird.
- Die Spalte *Adresse/Praefix* enthält ein Präfix oder eine Adresse, die mit dem vom Provider bezogenen Präfix verknüpft (Oder-Verknüpfung) wird. Wenn sich das Objekt auf das gesamte Präfix beziehen soll, so kann entweder ::/0 konfiguriert werden oder der Eintrag leer gelassen werden.

  **Beispiel:** Der Provider delegiert das Präfix 2001:db8:1234::/48 auf der Gegenstelle INTERNET.

  - Soll das Subnetz abcd verwendet werden, so muss als *Adresse/Praefix* der Wert 0:0:0:abcd::/48 konfiguriert werden.
  - Soll nur die Adresse 2001:db8:0:23::dead:beef/128 verwendet werden, so muss als *Adresse/Praefix* 0:0:0:23::dead:beef/128 konfiguriert werden.
  - Soll das gesamte Präfix verwendet werden, so muss als *Adresse/Praefix* ::/0 konfiguriert werden oder der Eintrag leer gelassen werden.

**Default-Wert:**

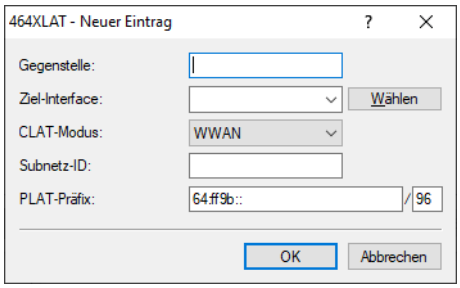
Lokales-Netzwerk

## 4.4 464XLAT

Ab LCOS 10.50 wird die CLAT-Funktion (Customer-Side Translator) von 464XLAT unterstützt.

464XLAT nach *RFC 6877* ist ein Übersetzungsverfahren von IPv4 zu IPv6 und wieder zu IPv4. Das Verfahren wird häufig von Mobilfunkprovidern eingesetzt, um in einem IPv6-Only-APN auf Basis von NAT64 Zugang zu IPv4 zu ermöglichen. An 464XLAT sind zwei Seiten beteiligt: Die Client-Seite bzw. der Client-Translator (CLAT – Customer-Side Translator) sowie der Provider-Translator (PLAT – Provider-Side Translator) bzw. das NAT64-Gateway des Providers. Das LCOS unterstützt die CLAT-Seite, um einem Netzwerk hinter einem Router Zugang zu IPv4-Netzwerken zu ermöglichen. Im Unterschied zu DS-Lite, bei dem ein 4in6-Tunnel zum AFTR-Gateway aufgebaut wird, verwendet 464XLAT eine Übersetzung (Translation) des IPv4-Pakets nach IPv6. Auf der PLAT-Seite wird das Paket zurück in IPv4 übersetzt. Aufgrund der zweifachen Übersetzung ergibt sich der Name 464. In der Regel wird das NAT64-Präfix 64:ff9b::/96 auf der Provider-Seite zur Übersetzung verwendet. Um 464XLAT zu verwenden, muss zunächst eine IPv6-Verbindung konfiguriert werden. Anschließend wird eine 464XLAT-Gegenstelle hinzugefügt. Auf diese Gegenstelle zeigt dann die IPv4-Default-Route.

In LANconfig erfolgt die Konfiguration unter **IPv6** > **Tunnel** > **464XLAT**.




**Gegenstelle**

Vergeben Sie einen eindeutigen Namen für diese Gegenstelle. Max. 16 Zeichen in Großbuchstaben.

**Ziel-Interface**

Name des darunterliegenden WAN-Interface bzw. der darunterliegenden Gegenstelle, z. B. INTERNET. Max. 16 Zeichen in Großbuchstaben.

**CLAT-Modus**

Definiert, mit welcher Methode das CLAT-Präfix erzeugt werden soll.

**DHCPv6-PD**

Verwendet der Internetprovider DHCPv6 Präfix Delegation, z. B. bei DSL oder Kabelverbindungen, so muss der CLAT-Modus DHCPv6-PD verwendet werden. Über die Subnet ID kann gesteuert werden, welches Subnetz des delegierten Präfixes für das CLAT-Präfix verwendet werden soll. Die Subnetz ID kann z. B. als „0“, „1“ oder „FF“ konfiguriert werden.

**WWAN (Default)**

Ist die Internetverbindung eine Mobilfunkverbindung (WWAN), so muss der CLAT-Modus WWAN verwendet werden. Das CLAT-Präfix wird aus dem /64 WAN-Präfix gebildet. Die Subnet-ID muss 0 oder leer sein. In der IPv4-Routing-Tabelle muss für die WAN-Verbindung NAT aktiviert werden.

**Statisch**

Verwendet der Internetprovider ein statisches Präfix, so kann im Feld Subnet-ID das statische /64 Präfix für das CLAT-Präfix verwendet werden, z. B. 2001:db8:: (ohne die Angabe /64). Dieser Modus kann auch verwendet werden, falls 464XLAT auf einer VPN-Verbindung oder einem Tunnel-Interface verwendet werden soll. In diesem Fall muss das VPN-Interface eine statische IPv6-Adresse konfiguriert haben.

**Subnetz-ID**

Subnetz-ID die mit dem delegierten DHCPv6-Präfix des Providers verknüpft wird. In das resultierende Präfix wird die IPv4-Quelladresse eingebettet, wenn das Paket ins WAN gesendet wird. Im Falle einer WWAN-Verbindung (/64-Präfix) kann entweder der Wert 0 konfiguriert werden, oder der Parameter kann leer gelassen werden (Default). Wird für CLAT-Modus der Wert statisch verwendet, so kann im Feld Subnetz-ID das statische /64 Präfix als CLAT-Präfix konfiguriert werden, z. B. 2001:db8:: (ohne die Angabe /64).

Beispiel für Subnetz-IDs: 0, 1, 12, 1f3b oder 2001:db8::

**PLAT-Präfix**

IPv6-Präfix, das auf der Providerseite zur Übersetzung verwendet wird. Wenn der Wert leer gelassen wird, wird eine DNS Präfix-Discovery nach *RFC 7050* durchgeführt, um das PLAT-Präfix automatisch zu ermitteln. Default: 64:ff9b::/96

## 4.4.1 Ergänzungen im Setup-Menü

### 464XLAT

464XLAT nach *RFC 6877* ist ein Übersetzungsverfahren von IPv4 zu IPv6 und wieder zu IPv4. Das Verfahren wird häufig von Mobilfunkprovidern eingesetzt um in einem IPv6-Only-APN auf Basis von NAT64 Zugang zu IPv4 zu ermöglichen. An 464XLAT sind zwei Seiten beteiligt: Die Client-Seite bzw. der Client-Translator (CLAT – Customer-Side Translator) sowie der Provider-Translator (PLAT – Provider-Side Translator) bzw. das NAT64-Gateway des Providers. Das LCOS unterstützt die CLAT-Seite um einem Netzwerk hinter einem Router Zugang zu IPv4-Netzwerken zu ermöglichen. Im Unterschied zu DS-Lite, bei dem ein 4in6-Tunnel zum AFTR-Gateway aufgebaut wird, verwendet 464XLAT eine Übersetzung (Translation) des IPv4-Pakets nach IPv6. Auf der PLAT-Seite wird das Paket zurück in IPv4 übersetzt. Aufgrund der zweifachen Übersetzung ergibt sich der Name 464. In der Regel wird das NAT64-Präfix 64:ff9b::/96 auf der Provider-Seite zur Übersetzung verwendet. Um 464XLAT zu verwenden muss zunächst eine IPv6-Verbindung konfiguriert werden. Anschließend wird eine 464XLAT-Gegenstelle hinzugefügt. Auf diese Gegenstelle zeigt dann die IPv4-Default-Route.

**SNMP-ID:**

2.2.63

**Pfad Konsole:**

**Setup** > **WAN**

**Gegenstelle**

Vergeben Sie einen eindeutigen Namen für diese Gegenstelle.

**SNMP-ID:**

2.2.63.1

**Pfad Konsole:**

**Setup** > **WAN** > **464XLAT**

**Mögliche Werte:**

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

**ZielInterface**

Name des darunterliegenden WAN-Interface bzw. der darunterliegenden Gegenstelle, z. B. INTERNET.

**SNMP-ID:**

2.2.63.2

**Pfad Konsole:**

**Setup** > **WAN** > **464XLAT**

**Mögliche Werte:**

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

**Subnetz-ID**

Subnetz-ID die mit dem delegierten DHCPv6-Präfix des Providers verknüpft wird. In das resultierende Präfix wird die IPv4-Quelladresse eingebettet, wenn das Paket ins WAN gesendet wird. Im Falle einer WWAN-Verbindung (/64-Präfix) kann entweder der Wert 0 konfiguriert werden, oder der Parameter kann leer gelassen werden (Default). Wird für CLAT-Modus der Wert statisch verwendet, so kann im Feld Subnetz-ID das statische /64 Präfix als CLAT-Präfix konfiguriert werden, z. B. 2001:db8:: (ohne die Angabe /64).

Beispiel für Subnetz-IDs: 0, 1, 12, 1f3b oder 2001:db8::

**SNMP-ID:**

2.2.63.3

**Pfad Konsole:**

**Setup** > **WAN** > **464XLAT**

**Mögliche Werte:**

max. 19 Zeichen aus `[A-F][a-f][0-9]:./`

**Default-Wert:**

*leer*

### PLAT-Praefix

IPv6-Präfix, das auf der Providerseite zur Übersetzung verwendet wird. Wenn der Wert leer gelassen wird, wird eine DNS Präfix-Discovery nach *RFC 7050* durchgeführt, um das PLAT-Präfix automatisch zu ermitteln.

**SNMP-ID:**

2.2.63.4

**Pfad Konsole:**

**Setup** > **WAN** > **464XLAT**

**Mögliche Werte:**

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

**Default-Wert:**

64:ff9b::/96

### CLAT-Modus

Definiert, mit welcher Methode das CLAT-Präfix erzeugt werden soll.

**SNMP-ID:**

2.2.63.6

**Pfad Konsole:**

**Setup** > **WAN** > **464XLAT**

**Mögliche Werte:**

**DHCPv6-PD**

Verwendet der Internetprovider DHCPv6 Präfix Delegation, z. B. bei DSL oder Kabelverbindungen, so muss der CLAT-Modus DHCPv6-PD verwendet werden. Über die Subnet ID kann gesteuert werden, welches Subnetz des delegierten Präfixes für das CLAT-Präfix verwendet werden soll. Die Subnetz ID kann z. B. als „0“, „1“ oder „FF“ konfiguriert werden.

**WWAN**

Ist die Internetverbindung eine Mobilfunkverbindung (WWAN), so muss der CLAT-Modus WWAN verwendet werden. Das CLAT-Präfix wird aus dem /64 WAN-Präfix gebildet. Die Subnet-ID muss 0 oder leer sein. In der IPv4-Routing-Tabelle muss für die WAN-Verbindung NAT aktiviert werden.

**Statisch**

Verwendet der Internetprovider ein statisches Präfix, so kann im Feld Subnet-ID das statische /64 Präfix für das CLAT-Präfix verwendet werden, z. B. 2001:db8:: (ohne die Angabe /64). Dieser Modus kann auch verwendet werden, falls 464XLAT auf einer VPN-Verbindung oder einem Tunnel-Interface verwendet werden soll. In diesem Fall muss das VPN-Interface eine statische IPv6-Adresse konfiguriert haben.

**Default-Wert:**

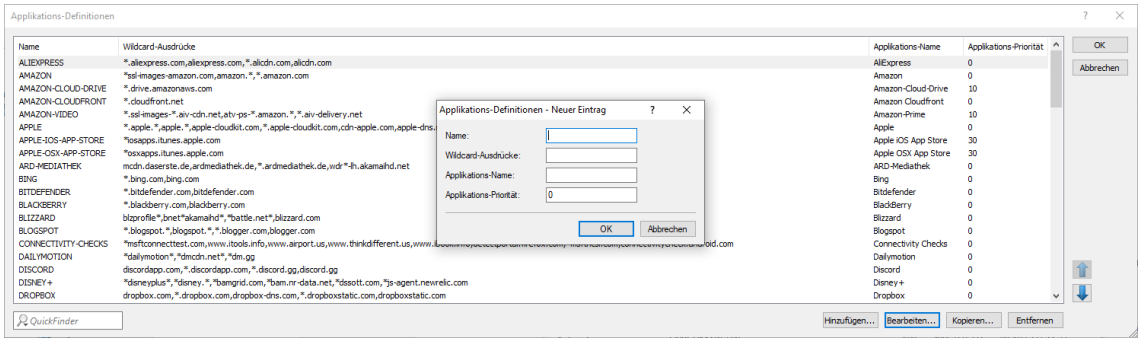
WWAN

# 5 Firewall

## 5.1 Zentrale Tabelle für DNS-basierte Anwendungen (Layer-7 App)

Bisher befanden sich die Applikationsdefinitionen für die Layer-7-Erkennung und die Layer-7-Applikationskontrolle in separaten Konfigurationstabellen. Zur Verbesserung der Benutzbarkeit wurden diese ab LCOS 10.50 zusammengeführt. Dies ermöglicht auch die einfache Benutzbarkeit der für die Layer-7-Erkennung bereits hinterlegten Definitionen auch für die Layer-7-Applikationskontrolle.

Die bisherigen Tabellen **Konfiguration** > **Firewall/QoS** > **Allgemein** > **Layer-7-Anwendungserkennung** (Konsole: **Setup** > **Layer-7-Anwendungserkennung** > **HTTP-HTTPS-Erfassung**) und **Konfiguration** > **Firewall/QoS** > **Allgemein** > **DNS-Ziele** (Konsole: **Setup** > **Firewall** > **DNS-Ziele**) wurden in der neuen Tabelle **Konfiguration** > **Firewall/QoS** > **Allgemein** > **Applikations-Definitionen** (Konsole: **Setup** > **App-Definitionen**) zusammengefasst.




### Name

Der Name für das Ziel. Der Name wird verwendet, um auf dieses Objekt zu verweisen.

Es kann mehrere Einträge für einen Namen geben, indem dem Namen des Ziels das Zeichen # angehängt und eine maximal dreistellige Zahl hinzugefügt wird (z. B. „LANCOM“, „LANCOM#1“, „LANCOM#2“ usw.).

Für die Verwendung dieses Eintrags in der Firewall muss dieser unter **Konfiguration** > **Firewall/QoS** > **Allgemein** > **DNS-Ziel Listen** referenziert werden.

### Wildcard-Ausdrücke

Enthält eine mittels Kommata oder Leerzeichen separierte Liste von Wildcardausdrücken. Die Ausdrücke können beliebig viele ? (ein beliebiges Zeichen) und * (mehrere beliebige Zeichen) enthalten, z. B. „*.lancom.*“. Die Eingabe ist auf 252 Zeichen beschränkt. Wenn Sie für einen Dienst mehr DNS-Wildcard-Ausdrücke benötigen, dann können Sie mehrere DNS-Ziele in der **DNS-Ziel-Liste** zu einem referenzierbaren Objekt zusammenfassen.

Unicodezeichen für internationalisierte Domainnamen können wie folgt eingegeben werden:

- UTF-8: Hier müssen ein bis vier Bytes einzeln als '\x', gefolgt von zwei hexadezimalen Ziffern, eintragen werden.
- UTF-16: Hier müssen ein oder zwei Doppelbytes als '\u', gefolgt von vier hexadezimalen Ziffern, eintragen werden.
- UTF-32: Hier muss der Wert als '\U', gefolgt von acht hexadezimalen Ziffern, eintragen werden.

Für die Layer-7-Applikationserkennung legen Sie mit dieser Tabelle die zu überwachenden HTTP / HTTPS-Dienste fest. Geben Sie dazu zusätzlich die Hostnamen-Bestandteile der Anwendung an.

**Applikations-Name**

Name für die Überwachung von HTTP / HTTPS-Verbindungen im Rahmen der Layer-7-Applikationserkennung (z. B. Youtube). Mit der Angabe dieses Namens wird die Layer-7-Applikationserkennung aktiviert.

**Applikations-Priorität**

Mit der Angabe der Priorität können Sie festlegen, in welcher Reihenfolge die jeweiligen Dienste ausgewertet werden, wenn bestimmte Hostnamen-Bestandteile in mehreren Einträgen definiert sind (z. B. *google).

## 5.1.1 Ergänzungen im Setup-Menü

### App-Definitionen

Einstellungen für die Applikationsdefinitionen für die Layer-7-Erkennung und die Layer-7-Applikationskontrolle.

**SNMP-ID:**

2.112

**Pfad Konsole:**

**Setup**

**Ziele**

Tabelle mit den Zielen für die Applikationsdefinitionen für die Layer-7-Erkennung und die Layer-7-Applikationskontrolle. Sobald sich in der neuen Tabelle ein Eintrag befindet, für den die Spalte *2.112.1.3 Anwendungs-Name* auf Seite 49 gesetzt ist, wird der Eintrag von der Layer-7-Erkennung verwendet. Für die Verwendung in der Firewall muss der Name des Eintrags explizit noch unter *2.110.2 DNS-Ziel-Liste* eingetragen werden.

**SNMP-ID:**

2.112.1

**Pfad Konsole:**

**Setup** > **App-Definitionen**

**Name**

Der Name für das Ziel. Der Name wird verwendet, um auf dieses Objekt zu verweisen.

Es kann mehrere Einträge für einen Namen geben, indem dem Namen des Ziels das Zeichen # angehängt und eine maximal dreistellige Zahl hinzugefügt wird (z. B. „LANCOM“, „LANCOM#1“, „LANCOM#2“ usw.).

**SNMP-ID:**

2.112.1.1

**Pfad Konsole:**

**Setup** > **App-Definitionen** > **Ziele**

**Mögliche Werte:**

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

max. 36 Zeichen (mit #) aus `[A-Z][0-9]#@{|}~!$%&'()+-,/:;<=>?[\]^_.`

**Default-Wert:**

*leer*

**Wildcard-Ausdruecke**

Enthält eine mittels Kommata oder Leerzeichen separierte Liste von Wildcardausdrücken. Die Ausdrücke können beliebig viele ? (ein beliebiges Zeichen) und * (mehrere beliebige Zeichen) enthalten, z. B. „*.lancom.*“. Die Eingabe ist auf 252 Zeichen beschränkt. Wenn Sie für einen Dienst mehr DNS-Wildcard-Ausdrücke benötigen, dann können Sie mehrere DNS-Ziele in der **DNS-Ziel-Liste** zu einem referenzierbaren Objekt zusammenfassen.

Unicodezeichen für internationalisierte Domainnamen können wie folgt eingegeben werden:

- UTF-8: Hier müssen ein bis vier Bytes einzeln als '\x', gefolgt von zwei hexadezimalen Ziffern, eintragen werden.
- UTF-16: Hier müssen ein oder zwei Doppelbytes als '\u', gefolgt von vier hexadezimalen Ziffern, eintragen werden.
- UTF-32: Hier muss der Wert als '\U', gefolgt von acht hexadezimalen Ziffern, eintragen werden.

Für die Layer-7-Applikationserkennung legen Sie mit dieser Tabelle die zu überwachenden HTTP/HTTPS-Dienste fest. Geben Sie dazu zusätzlich die Hostnamen-Bestandteile der Anwendung an.

**SNMP-ID:**

2.112.1.2

**Pfad Konsole:**

**Setup** > **App-Definitionen** > **Ziele**

**Mögliche Werte:**

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

**Default-Wert:**

*leer*

**Anwendungs-Name**

Name für die Überwachung von HTTP / HTTPS-Verbindungen im Rahmen der Layer-7-Applikationserkennung (z. B. Youtube).

**SNMP-ID:**

2.112.1.3

**Pfad Konsole:**

**Setup** > **App-Definitionen** > **Ziele**

**Mögliche Werte:**

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

**Default-Wert:**

*leer*

**Anwendungs-Prio**

Legen Sie hier die Priorität der HTTP/HTTPS-Erfassung durch die Layer-7-Anwendungserkennung fest.

**SNMP-ID:**

2.112.1.4

**Pfad Konsole:**

**Setup** > **App-Definitionen** > **Ziele**

**Mögliche Werte:**

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

**Default-Wert:**

0

## 5.2 Unterstützung für H.323 ALG in der Firewall entfallen

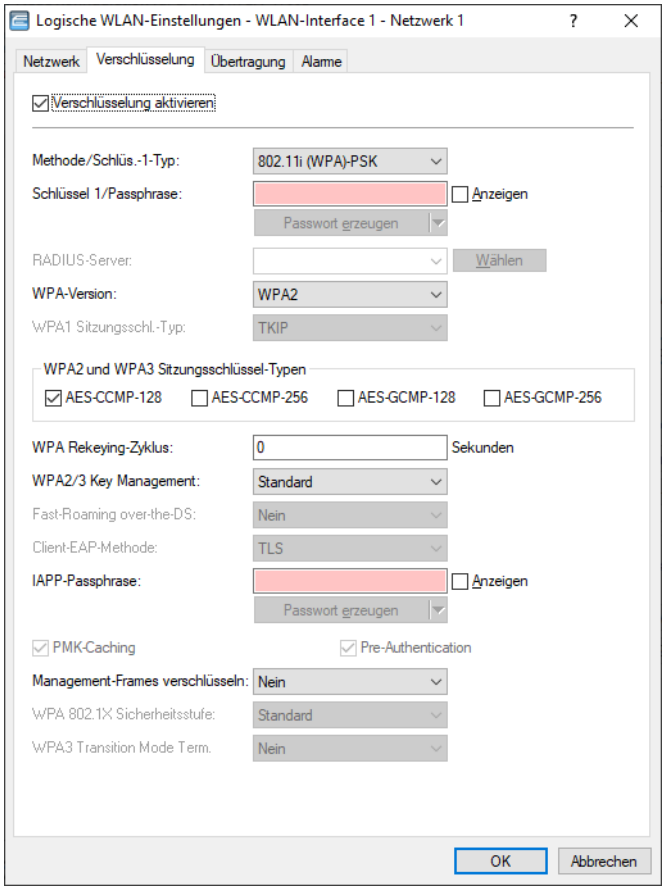
Ab LCOS 10.50 entfällt die Unterstützung für die Behandlung von H.323-Sitzungen in der Firewall. Diese Funktionalität wird auch als H.323 Application Layer Gateway (ALG) bezeichnet. Auf der Kommandozeile fällt somit der Zweig unterhalb von **Setup** > **IP-Router** > **Firewall** > **Anwendungen** > **H.323** weg.

# 6 Wireless LAN – WLAN

## 6.1 Fast Roaming over-the-DS

Ab LCOS 10.50 kann durch Setzen eines Schalters WLAN-Clients signalisiert werden, dass Fast Roaming over-the-DS vom Access Point unterstützt wird.

In LANconfig konfigurieren Sie die Option unter **Wireless-LAN** > **Allgemein** > **Logische WLAN-Einstellungen** > **Verschlüsselung** ein.




### Fast-Roaming over-the-DS

Mit Fast Roaming over-the-DS (Distribution System) können Sie eine Option des Standards IEEE 801.11r aktivieren, der sich die Verbindung der Access Points über LAN zunutze macht. Der Wechselwunsch wird an den Access Point gesendet, mit dem der Client noch verbunden ist. Dieser leitet den Wunsch an den neuen Access Point weiter und der Wechsel wird durchgeführt. Dies beschleunigt den Wechsel im Vergleich zur normalen „Over-the-Air fast transition" nochmals deutlich, was insbesondere Echtzeitanwendungen wie z. B. VoIP zugute kommt.

## 6.1.1 Ergänzungen im Setup-Menü

### Schnelles-Roaming-ueber-DS

Mit Fast Roaming over-the-DS (Distribution System) können Sie eine Option des Standards IEEE 801.11r aktivieren, der sich die Verbindung der Access Points über LAN zunutze macht. Der Wechselwunsch wird an den Access Point gesendet, mit dem der Client noch verbunden ist. Dieser leitet den Wunsch an den neuen Access Point weiter und der Wechsel wird durchgeführt. Dies beschleunigt den Wechsel im Vergleich zur normalen „Over-the-Air fast transition" nochmals deutlich, was insbesondere Echtzeitanwendungen wie z. B. VoIP zugute kommt.

**SNMP-ID:**

2.23.20.3.30

**Pfad Konsole:**

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

**Mögliche Werte:**

**ja**
**nein**

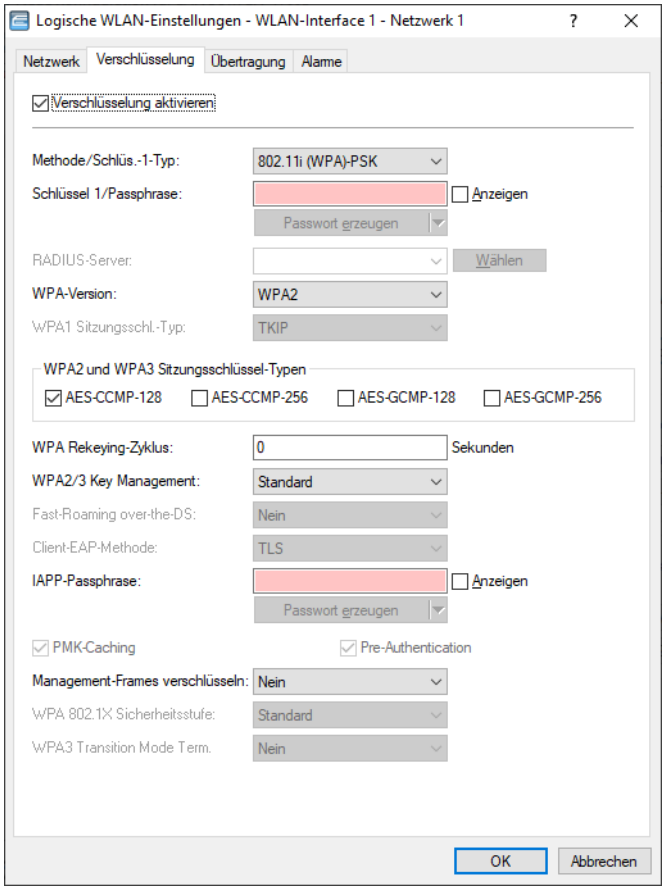
**Default-Wert:**

nein

# 6.2 WPA3 Transition Mode Termination

Ab LCOS 10.50 kann durch Setzen eines Schalters WLAN-Clients über ein zusätzliches Info-Element explizit signalisiert werden, dass im gemischten WPA2/3-Modus die WPA3-PSK (SAE)-Verschlüsselungsmethode unterstützt wird. Unterstützt der Client seinerseits das „Transition Mode Termination"-Feature, wird er für das Einbuchen an dieser SSID immer WPA3-PSK (SAE) verwenden. So wird ein Downgrade auf WPA2-PSK, was im gemischten WPA2/3-Modus ansonsten ebenfalls erlaubt ist, ausgeschlossen.

In LANconfig konfigurieren Sie die Option unter **Wireless-LAN** > **Allgemein** > **Logische WLAN-Einstellungen** > **Verschlüsselung** ein.




**WPA3 Transition Mode Term.**

Durch Setzen des Schalters wird WLAN-Clients über ein zusätzliches Info-Element explizit signalisiert, dass im gemischten WPA2/3-Modus die WPA3-PSK (SAE)-Verschlüsselungsmethode unterstützt wird. Unterstützt der Client seinerseits das „Transition Mode Termination"-Feature, wird er für das Einbuchen an dieser SSID immer WPA3-PSK (SAE) verwenden. So wird ein Downgrade auf WPA2-PSK, was im gemischten WPA2/3-Modus ansonsten ebenfalls erlaubt ist, ausgeschlossen.

## 6.2.1 Ergänzungen im Setup-Menü

### Transition-beenden

Durch Setzen des Schalters wird WLAN-Clients über ein zusätzliches Info-Element explizit signalisiert, dass im gemischten WPA2/3-Modus die WPA3-PSK (SAE)-Verschlüsselungsmethode unterstützt wird. Unterstützt der Client seinerseits das „Transition Mode Termination"-Feature, wird er für das Einbuchen an dieser SSID immer WPA3-PSK (SAE) verwenden. So wird ein Downgrade auf WPA2-PSK, was im gemischten WPA2/3-Modus ansonsten ebenfalls erlaubt ist, ausgeschlossen.

**SNMP-ID:**

2.23.20.3.31

**Pfad Konsole:**

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

**Mögliche Werte:**

**ja**
**nein**

**Default-Wert:**

nein

## 6.3 WLAN-Data-Trace in LANconfig an neuer Stelle

Ab LCOS 10.50 finden Sie den WLAN-Data-Trace nicht mehr unter **Wireless-LAN** > **Trace**, sondern nun unter **Wireless-LAN** > **Allgemein** > **Erweiterte Einstellungen** > **Trace**.

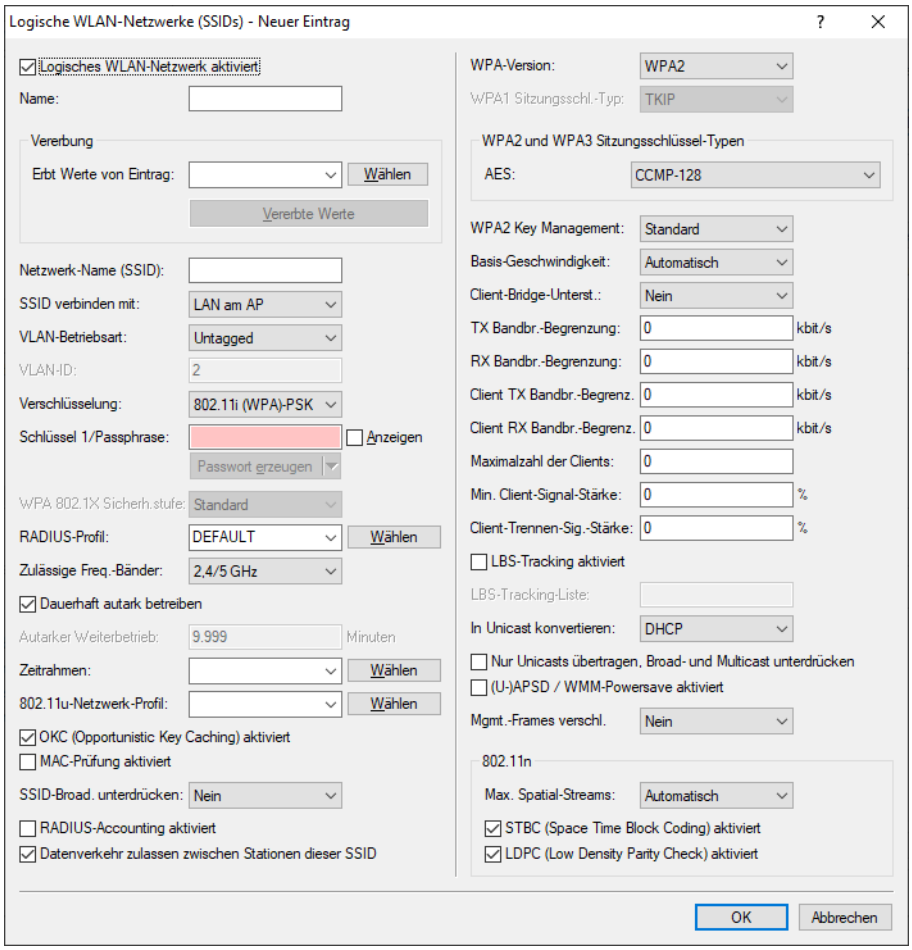
# 7 WLAN-Management

## 7.1 WLC: Auskoppeln von WLAN-SSIDs in L2TP-Ethernet-Tunnel

Ab LCOS 10.50 ist die automatische Konfiguration von L2TPv3-Ethernet-Tunneln zum Auskoppeln von WLAN-SSIDs möglich.

Allgemeine Informationen zum Thema L2TPv3 finden Sie im Referenzhandbuch im Abschnitt „Layer 2 Tunneling Protocol (L2TP)“.

Die Verwendung von L2TPv3-Tunneln als Alternative zum klassischen WLC-Layer-3-Tunnel empfiehlt sich, wenn der WLAN-Durchsatz durch diesen begrenzt wird, da mittels L2TPv3 ein höherer Maximaldurchsatz erzielt werden kann. Konfigurieren Sie die Verwendung von L2TPv3-Ethernet-Tunneln im Dialog zur Konfiguration der logischen WLAN-Netzwerke unter **WLAN-Controller** > **Profile** > **Logische WLAN-Netzwerke** unter **SSID verbinden mit**.




Sowohl der WLC als auch die verwalteten Access Points müssen LCOS 10.50 unterstützen.

Passen Sie anschließend noch die Verwendung der gewählten L2TP-ETHERNET-x-Schnittstelle auf dem WLC an, z. B. zur weiteren Verwendung im IP-Router oder in der LAN-Bridge.

## 7.1.1 Ergänzungen im Setup-Menü

### Verbinde-SSID-mit

Stellen Sie hier ein, an welche logische Schnittstelle der AP die Nutzdaten aus diesem WLAN-Netzwerk (SSID) überträgt.

Die Weiterleitung der Nutzdaten aus mehreren SSIDs an den WLC steigert die CPU-Last und die benötigte Bandbreite der zentralen Geräte. Berücksichtigen Sie die erforderlichen Leistungswerte beim zentralen WLAN-Management mit Layer-3-Tunneling.

Sie können für jeden AP bis zu 7 SSIDs mit einem WLC-Tunnel verbinden. Der WLC verbindet auf dem jeweiligen AP den WLC-Tunnel und damit die verbundene SSID mit einer freien Bridge-Gruppe. Da eine der verfügbaren 8 Bridge-Gruppen für andere Zwecke reserviert ist, verbleiben 7 Bridge-Gruppen für die Zuordnung der WC-Tunnel.

**SNMP-ID:**

2.37.1.1.32

**Pfad Konsole:**

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

**Mögliche Werte:**

**LAN**

Der AP leitet die Nutzdaten aus diesem WLAN-Netzwerk über die Bridge an die eigene lokale LAN-Schnittstelle weiter. Konfigurieren Sie in diesem Fall die weitere Verarbeitung der Datenpakete durch entsprechende Routen direkt auf dem AP, z B. durch einen separaten Internet-Zugang.

**WLC-Tunnel-1 … WLC-Tunnel-x (modellabhängig)**

Der AP leitet die Nutzdaten aus diesem WLAN-Netzwerk über die Bridge an eine der virtuellen Schnittstellen für den WLC weiter (WLC-Tunnel). Konfigurieren Sie in diesem Fall die weitere Verarbeitung der Datenpakete durch entsprechende Routen zentral auf dem WLC, z B. durch einen gemeinsam genutzten Internet-Zugang.

**L2TP-ETHERNET-1 … L2TP-ETHERNET-x (modellabhängig)**

Die SSID ist mit einem L2TPv3-Ethernet-Tunnel verbunden. Dies ermöglicht ein automatisches Auskoppeln von WLAN-SSIDs in L2TP-Ethernet-Tunnel. Die Verwendung von L2TPv3-Tunneln als Alternative zum klassischen WLC-Layer-3-Tunnel empfiehlt sich, wenn der WLAN-Durchsatz durch diesen begrenzt wird, da mittels L2TPv3 ein höherer Maximaldurchsatz erzielt werden kann. Passen Sie anschließend noch die Verwendung der gewählten L2TP-ETHERNET-x-Schnittstelle auf dem WLC an, z. B. zur weiteren Verwendung im IP-Router oder in der LAN-Bridge.

**Default-Wert:**

LAN

# 8 Public Spot

## 8.1 Public Spot-Anmeldung mit Name, Passwort und MAC-Adresse: Konfigurierbares MAC-Adress-Format

Bei der Anmelde-Methode „Anmeldung mit Name, Passwort und MAC-Adresse“ kann die MAC-Adresse des Public Spot-Clients durch einen externen RADIUS-Server geprüft werden. Das Format, in dem die MAC-Adresse an den RADIUS-Server übermittelt wird, ist ab LCOS 10.50 einstellbar. Dies geschieht im LCOS-Menübaum unter dem Menüpunkt **Setup** > **Public-Spot-Modul** > **MAC-Adresse-Benutzername-Format**.

### 8.1.1 Ergänzungen im Setup-Menü

#### MAC-Adresse-Benutzername-Format

Bei der Anmelde-Methode „Anmeldung mit Name, Passwort und MAC-Adresse“ kann die MAC-Adresse des Public Spot-Clients durch einen externen RADIUS-Server geprüft werden. Das Format, in dem die MAC-Adresse an den RADIUS-Server übermittelt wird, ist hier einstellbar.

Die einzelnen Bytes der MAC-Adresse sind hierbei als Variablen %a bis %f repräsentiert. In der hier angegebenen Standardeinstellung (%a%b%c-%d%e%f) werden die Bytes der MAC-Adresse nacheinander ausgegeben mit „-“ als Trennzeichen. Zusätzlich zu diesen Variablen können beliebige vom LCOS unterstützte Zeichen hinzugefügt werden.

**SNMP-ID:**

2.24.62

**Pfad Konsole:**

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

**Mögliche Werte:**

max. 30 Zeichen aus `[]A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

**Default-Wert:**

%a%b%c-%d%e%f

# 9 Backup-Lösungen

Ab LCOS 10.50 steht mit dem ICMPv6-Polling eine weitere Methode zur Erkennung der Störung einer Netzwerkverbindung zur Verfügung.

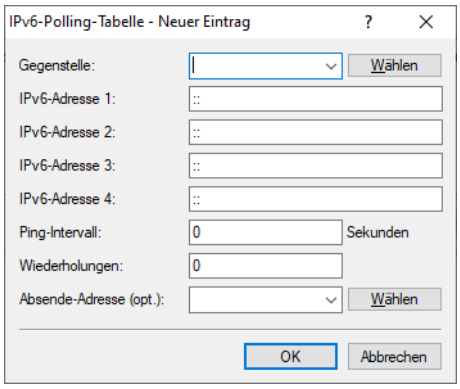
## 9.1 ICMPv6-Polling

Beim ICMPv6-Polling werden ähnlich dem LCP-Monitoring oder ICMP-Polling für IPv4 regelmäßig Anfragen an eine Gegenstelle geschickt. Hier werden ping-Befehle abgesetzt, deren Beantwortung überwacht wird. Anders als beim LCP-Monitoring kann für die ICMPv6-Pings jedoch die Ziel-Gegenstelle frei definiert werden. Mit einem Ping auf einen Router in einem entfernten Netz kann man so die gesamte Verbindung überwachen, nicht nur bis zum Internet-Provider.

In der IPv6-Polling-Tabelle wird für die Gegenstelle ein Ping-Intervall definiert, in dem die Anfragen an die Gegenstelle verschickt werden. Außerdem wird die Anzahl der Wiederholungen definiert, mit der bei Ausbleiben der Antworten erneut eine Anfrage gesendet wird. Erhält der Absender auch auf alle Wiederholungen keine Antwort, gilt das Ziel der Ping-Anfragen als nicht erreichbar.

Zu jeder Gegenstelle können dabei bis zu vier verschiedene IPv6-Adressen eingetragen werden, die parallel im entfernten Netz geprüft werden. Nur wenn alle eingetragenen IPv6-Adressen nicht erreichbar sind, gilt die Leitung als gestört.

Die Einstellungen für das ICMPv6-Polling finden Sie in LANconfig unter **Kommunikation** > **Protokolle** > **IPv6-Polling-Tabelle**.




**Gegenstelle**

Wählen Sie hier den Namen einer Gegenstelle aus der Gegenstellen-Liste.

**IPv6-Adresse 1-4**

Geben Sie hier bis zu 4 IPv6-Adressen an, welche der Reihe nach für diese Gegenstelle angepingt werden, um die Verbindung zu prüfen. Die Verbindung wird als intakt gewertet, wenn auch nur eine der angegebenen IPv6-Adressen erreicht werden kann.

Wählen Sie auf jeden Fall IPv6-Adressen, die zuverlässig erreichbar sind, da ansonsten unnötige Backup-Verbindungen initiiert würden.

Wenn Sie für alle vier IPv6-Adressen „::" eingeben, wird der per DHCPv6 oder Router Advertisement zugewiesene DNS-Server angepingt.

**Ping-Intervall**

Geben Sie hier das Ping-Intervall in Sekunden ein.

Wenn sie sowohl hier als auch bei den Wiederholungen 0 eingeben, wird ein Standardintervall von 20 Sekunden bei 5 Wiederholungen verwendet.

**Wiederholungen**

Geben Sie hier die Anzahl der Wiederholungen ein, die im Sekundentakt durchgeführt werden, wenn auf ein Ping keine Antwort empfangen wurde. Werden auch die wiederholten Pings nicht beantwortet, wird die Verbindung abgebaut.

Wenn sie sowohl hier als auch beim Ping-Intervall 0 eingeben, wird ein Standardintervall von 20 Sekunden bei 5 Wiederholungen verwendet.

**Absende-Adresse (opt.)**

Hier können Sie optional eine Absende-Adresse konfigurieren, die statt der ansonsten automatisch für die Zieladresse gewählten Absende-Adresse verwendet wird.

## 9.1.1 Ergänzungen im Setup-Menü

### Polling-Tabelle

In dieser Tabelle legen Sie die Einstellungen für ICMPv6-Polling fest. Beim ICMPv6-Polling werden ähnlich dem LCP-Monitoring oder ICMP-Polling für IPv4 regelmäßig Anfragen an eine Gegenstelle geschickt. Hier werden ping-Befehle abgesetzt, deren Beantwortung überwacht wird. Anders als beim LCP-Monitoring kann für die ICMPv6-Pings jedoch die Ziel-Gegenstelle frei definiert werden. Mit einem Ping auf einen Router in einem entfernten Netz kann man so die gesamte Verbindung überwachen, nicht nur bis zum Internet-Provider.

In dieser Tabelle wird für die Gegenstelle ein Ping-Intervall definiert, in dem die Anfragen an die Gegenstelle verschickt werden. Außerdem wird die Anzahl der Wiederholungen definiert, mit der bei Ausbleiben der Antworten erneut eine Anfrage gesendet wird. Erhält der Absender auch auf alle Wiederholungen keine Antwort, gilt das Ziel der Ping-Anfragen als nicht erreichbar.

Zu jeder Gegenstelle können dabei bis zu vier verschiedene IPv6-Adressen eingetragen werden, die parallel im entfernten Netz geprüft werden. Nur wenn alle eingetragenen IPv6-Adressen nicht erreichbar sind, gilt die Leitung als gestört.

**SNMP-ID:**

2.70.15

**Pfad Konsole:**

**Setup** > **IPv6**

**Gegenstelle**

Geben Sie hier den Namen einer Gegenstelle aus der Gegenstellen-Liste an.

**SNMP-ID:**

2.70.15.1

**Pfad Konsole:**

**Setup** > **IPv6** > **Polling-Tabelle**

**Mögliche Werte:**

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

**Default-Wert:**

*leer*

**IPv6-Adresse-1**

Geben Sie hier die erste von bis zu 4 IPv6-Adressen an, welche der Reihe nach für diese Gegenstelle angepingt werden, um die Verbindung zu prüfen. Die Verbindung wird als intakt gewertet, wenn auch nur eine der angegebenen IPv6-Adressen erreicht werden kann.

Wählen Sie auf jeden Fall IPv6-Adressen, die zuverlässig erreichbar sind, da ansonsten unnötige Backup-Verbindungen initiiert würden.

Wenn Sie für alle vier IPv6-Adressen „::" eingeben, wird der per DHCPv6 oder Router Advertisement zugewiesene DNS-Server angepingt.

**SNMP-ID:**

2.70.15.2

**Pfad Konsole:**

**Setup** > **IPv6** > **Polling-Tabelle**

**Mögliche Werte:**

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

**Default-Wert:**

*leer*

**IPv6-Adresse-2**

Geben Sie hier die zweite von bis zu 4 IPv6-Adressen an, welche der Reihe nach für diese Gegenstelle angepingt werden, um die Verbindung zu prüfen. Die Verbindung wird als intakt gewertet, wenn auch nur eine der angegebenen IPv6-Adressen erreicht werden kann.

Wählen Sie auf jeden Fall IPv6-Adressen, die zuverlässig erreichbar sind, da ansonsten unnötige Backup-Verbindungen initiiert würden.

Wenn Sie für alle vier IPv6-Adressen „::" eingeben, wird der per DHCPv6 oder Router Advertisement zugewiesene DNS-Server angepingt.

**SNMP-ID:**

2.70.15.3

**Pfad Konsole:**

**Setup** > **IPv6** > **Polling-Tabelle**

**Mögliche Werte:**

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

**Default-Wert:**

*leer*

**IPv6-Adresse-3**

Geben Sie hier die dritte von bis zu 4 IPv6-Adressen an, welche der Reihe nach für diese Gegenstelle angepingt werden, um die Verbindung zu prüfen. Die Verbindung wird als intakt gewertet, wenn auch nur eine der angegebenen IPv6-Adressen erreicht werden kann.

Wählen Sie auf jeden Fall IPv6-Adressen, die zuverlässig erreichbar sind, da ansonsten unnötige Backup-Verbindungen initiiert würden.

Wenn Sie für alle vier IPv6-Adressen „::" eingeben, wird der per DHCPv6 oder Router Advertisement zugewiesene DNS-Server angepingt.

**SNMP-ID:**

2.70.15.4

**Pfad Konsole:**

**Setup** > **IPv6** > **Polling-Tabelle**

**Mögliche Werte:**

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

**Default-Wert:**

*leer*

**IPv6-Adresse-4**

Geben Sie hier die vierte von bis zu 4 IPv6-Adressen an, welche der Reihe nach für diese Gegenstelle angepingt werden, um die Verbindung zu prüfen. Die Verbindung wird als intakt gewertet, wenn auch nur eine der angegebenen IPv6-Adressen erreicht werden kann.

Wählen Sie auf jeden Fall IPv6-Adressen, die zuverlässig erreichbar sind, da ansonsten unnötige Backup-Verbindungen initiiert würden.

Wenn Sie für alle vier IPv6-Adressen „::" eingeben, wird der per DHCPv6 oder Router Advertisement zugewiesene DNS-Server angepingt.

**SNMP-ID:**

2.70.15.5

**Pfad Konsole:**

**Setup** > **IPv6** > **Polling-Tabelle**

**Mögliche Werte:**

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

**Default-Wert:**

*leer*

**Zeit**

Geben Sie hier das Ping-Intervall in Sekunden ein.

Wenn sie sowohl hier als auch bei *2.70.15.7 Wdh.* auf Seite 62 0 eingeben, wird ein Standardintervall von 20 Sekunden bei 5 Wiederholungen verwendet.

**SNMP-ID:**

2.70.15.6

**Pfad Konsole:**

**Setup** > **IPv6** > **Polling-Tabelle**

**Mögliche Werte:**

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

**Default-Wert:**

*leer*

**Wdh.**

Geben Sie hier die Anzahl der Wiederholungen ein, die im Sekundentakt durchgeführt werden, wenn auf ein Ping keine Antwort empfangen wurde. Werden auch die wiederholten Pings nicht beantwortet, wird die Verbindung abgebaut.

Wenn sie sowohl hier als auch bei *2.70.15.6 Zeit* auf Seite 62 0 eingeben, wird ein Standardintervall von 20 Sekunden bei 5 Wiederholungen verwendet.

**SNMP-ID:**

2.70.15.7

**Pfad Konsole:**

**Setup** > **IPv6** > **Polling-Tabelle**

**Mögliche Werte:**

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

**Default-Wert:**

*leer*

**Loopback-Addr.**

Hier können Sie optional eine Absende-Adresse konfigurieren, die statt der ansonsten automatisch für die Zieladresse gewählten Absende-Adresse verwendet wird.

**SNMP-ID:**

2.70.15.8

**Pfad Konsole:**

**Setup** > **IPv6** > **Polling-Tabelle**

**Mögliche Werte:**

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

**Default-Wert:**

*leer*

**Typ**

Über diese Einstellung schalten Sie das Verhalten des Pollings.

**SNMP-ID:**

2.70.15.9

**Pfad Konsole:**

**Setup** > **IPv6** > **Polling-Tabelle**

**Mögliche Werte:**

**auto**

Das Gerät pollt nur dann aktiv, wenn keine Daten empfangen wurden. Empfangene ICMP-Pakete gelten nicht als Daten und werden auch weiterhin ignoriert.

**erzwungen**

Das Gerät pollt im vorgegebenen Intervall.

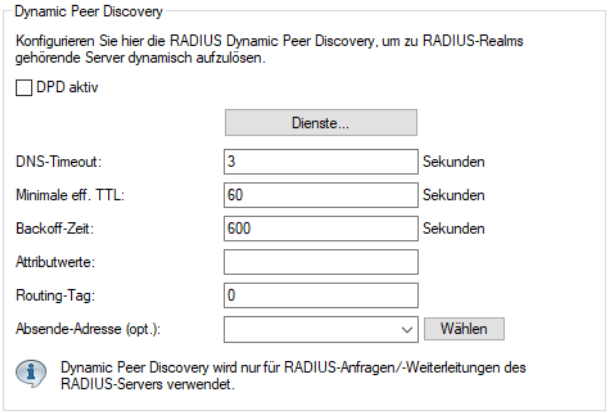
**Default-Wert:**

auto

# 10 RADIUS

## 10.1 Dynamic Peer Discovery

Unterstützung für das *RFC 7585* „Dynamic Peer Discovery for RADIUS/TLS and RADIUS/DTLS Based on the Network Access Identifier (NAI)". Statt RADIUS-Requests statisch zu einem oder mehreren RADIUS-Servern weiterzuleiten ermöglicht Dynamic Peer Discovery dynamisch anhand des Realms / NAIs den richtigen RADIUS-Server zu finden. Kommt ein Request, so wird per DNS NAPTR/SRV-Record der richtige Server gefunden.




LANconfig: **RADIUS** > **Dyn. Peer Discovery**

Konsole: **Setup** > **RADIUS** > **Dynamic-Peer-Discovery**

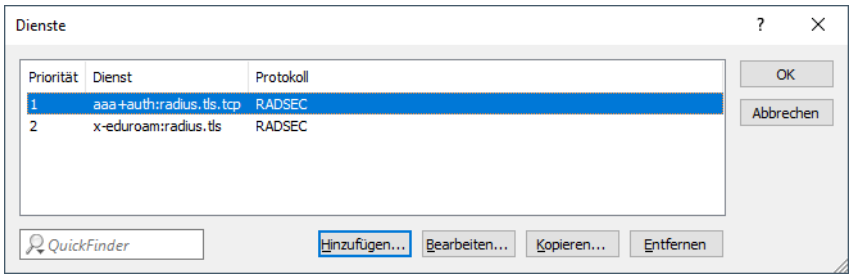
**DPD aktiv**

Dynamic Peer Discovery ein- bzw. ausschalten. Sobald Dynamic Peer Discovery eingeschaltet ist, verzweigt der RADIUS-Server zur dynamischen Auflösung, falls ein bestimmter Realm / NAI nicht in seiner Weiterleitungs-Tabelle definiert ist. Lokale Definitionen für Realms haben also immer Vorrang.

**Dienste**

Tabelle mit den Diensten. Der Dienst ist das, was in der NAPTR-Antwort im Service geliefert wird. Es werden alle NAPTR-Einträge extrahiert und weiter aufgelöst, die als Service den mit der höchsten Priorität aus dieser Tabelle haben. Werden mit der Default-Einstellung z. B. NAPTR-Records für beide Service-Typen geliefert, so werden die für „x-eduroam:radius.tls" ignoriert. Die Tabelle wird vom LCOS automatisch sortiert, so dass höher priorisierte Services weiter oben stehen. Das Protokoll, das zu so einem Server genutzt werden muss (RADIUS oder RADSEC), wird explizit vorgegeben. Für den Fall, daß die NAPTR-Anfrage keine verwendbaren Records liefert, hat diese Tabelle noch die Bedeutung, welcher Präfix dem NAI für die Fallback-SRV-Anfrage vorangestellt wird. Es wird der höchspriorisierte Eintrag aus der Tabelle genommen, für den in einer intern

fix definierten Tabelle ein Präfix definiert ist. Aktuell sind die Services radius.tls, radius.tls.tcp, radsec.tcp und radius.udp definiert, die auf ein Präfix von _radiustls._tcp., _radsec.tcp. bzw. _radius._udp. mappen.




**Priorität**

Die Priorität dieses Dienstes.

**Dienst**

Die Dienste selbst. Voreingestellt sind „aaa+auth:radius.tls.tcp“ und „x-eduroam:radius.tls“.

**Protokoll**

Das Protokoll (RADIUS oder RADSEC), das zu diesem Dienst genutzt wird.

**DNS-Timeout**

Die Zeitspanne in Sekunden, innerhalb der alle DNS-Anfragen für einen NAI abgehandelt sein müssen. Das schließt auch die zweistufige Variante über NAPTR- und nachfolgende SRV-Anfragen ein. Default: 3 Sekunden

**Minimale eff. TTL**

Vom DNS-Server gemeldete TTL-Werte, die kürzer als diese Zeit sind, werden auf diesen Wert angehoben. Default: 60 Sekunden

**Backoff-Zeit**

Falls eine Auflösung in einem Fehler endet (DNS-Antwort mit Fehler, Timeout…), ist dies die Zeit in Sekunden, für die keine neuen Auflöseversuche für diesen Realm gemacht werden sollen. Default: 600 Sekunden

**Attributwerte**

RADIUS-Attribute, die bei Weiterleitungen an per Dynamic Peer Discovery ermittelte Server hinzugefügt oder geändert werden sollen.

**Routing-Tag**

Das Routing-Tag, welches Dynamic Peer Discovery für seine DNS-Anfragen nutzen soll. Default: 0

**Abesende-Adresse (opt.)**

Die Loopback-Adresse, die bei den Weiterleitungen der per Dynamic Peer Discovery ermittelten RADIUS-Server benutzt werden soll.

## 10.1.1 Ergänzungen im Setup-Menü

### Dynamic-Peer-Discovery

Unterstützung für das *RFC 7585* „Dynamic Peer Discovery for RADIUS/TLS and RADIUS/DTLS Based on the Network Access Identifier (NAI)“. Statt RADIUS-Requests statisch zu einem oder mehreren RADIUS-Servern weiterzuleiten ermöglicht Dynamic Peer Discovery dynamisch anhand des Realms / NAIs den richtigen RADIUS-Server zu finden. Kommt ein Request, so wird per DNS NAPTR/SRV-Record der richtige Server gefunden.

**SNMP-ID:**

2.25.23

**Pfad Konsole:**

**Setup** > **RADIUS**

**In-Betrieb**

Dynamic Peer Discovery ein- bzw. ausschalten. Sobald Dynamic Peer Discovery eingeschaltet ist, verzweigt der RADIUS-Server zur dynamischen Auflösung, falls ein bestimmter Realm / NAI nicht in seiner Weiterleitungs-Tabelle definiert ist. Lokale Definitionen für Realms haben also immer Vorrang.

**SNMP-ID:**

2.25.23.1

**Pfad Konsole:**

**Setup** > **RADIUS** > **Dynamic-Peer-Discovery**

**Mögliche Werte:**

**nein**
**ja**

**Default-Wert:**

nein

**Routing-Tag**

Das Routing-Tag, welches Dynamic Peer Discovery für seine DNS-Anfragen nutzen soll.

**SNMP-ID:**

2.25.23.2

**Pfad Konsole:**

**Setup** > **RADIUS** > **Dynamic-Peer-Discovery**

**Mögliche Werte:**

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

**Default-Wert:**

0

**Loopback-Adresse**

Die Loopback-Adresse, die bei den Weiterleitungan der per Dynamic Peer Discovery ermittelten RADIUS-Server benutzt werden soll.

**SNMP-ID:**

2.25.23.3

**Pfad Konsole:**

**Setup** > **RADIUS** > **Dynamic-Peer-Discovery**

**Mögliche Werte:**

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

**Default-Wert:**

*leer*

**Attribut-Werte**

RADIUS-Attribute, die bei Weiterleitungen an per Dynamic Peer Discovery ermittelte Server hinzugefügt oder geändert werden sollen.

**SNMP-ID:**

2.25.23.4

**Pfad Konsole:**

**Setup** > **RADIUS** > **Dynamic-Peer-Discovery**

**Mögliche Werte:**

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

**Default-Wert:**

*leer*

**Services**

Tabelle mit den Services. Der Service ist das, was in der NAPTR-Antwort im Service geliefert wird. Es werden alle NAPTR-Einträge extrahiert und weiter aufgelöst, die als Service den mit der höchsten Priorität aus dieser Tabelle haben. Werden mit der Default-Einstellung z. B. NAPTR-Records für beide Service-Typen geliefert, so werden die für „x-eduroam:radius.tls“ ignoriert. Die Tabelle wird vom LCOS automatisch sortiert, so dass höher priorisierte Services weiter oben stehen. Das Protokoll, das zu so einem Server genutzt werden muss (RADIUS oder RADSEC), wird explizit vorgegeben. Für den Fall, daß die NAPTR-Anfrage keine verwendbaren Records liefert, hat diese Tabelle noch die Bedeutung, welcher Präfix dem NAI für die Fallback-SRV-Anfrage vorangestellt wird. Es wird der höchspriorisierte Eintrag aus der Tabelle genommen, für den in einer intern fix definierten Tabelle ein Präfix definiert ist. Aktuell sind die Services radius.tls, radius.tls.tcp, radsec.tcp und radius.udp definiert, die auf ein Präfix von _radiustls._tcp., _radsec.tcp. bzw. _radius._udp. mappen.

**SNMP-ID:**

2.25.23.5

**Pfad Konsole:**

**Setup** > **RADIUS** > **Dynamic-Peer-Discovery**

**Prioritaet**

Die Priorität dieses Services.

**SNMP-ID:**

2.25.23.5.1

**Pfad Konsole:**

**Setup** > **RADIUS** > **Dynamic-Peer-Discovery** > **Services**

**Mögliche Werte:**

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

**Service**

Die Services selbst. Voreingestellt sind „aaa+auth:radius.tls.tcp" und „x-eduroam:radius.tls".

**SNMP-ID:**

2.25.23.5.2

**Pfad Konsole:**

**Setup** > **RADIUS** > **Dynamic-Peer-Discovery** > **Services**

**Mögliche Werte:**

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

**Protokoll**

Das Protokoll, das zu diesem Service genutzt wird.

**SNMP-ID:**

2.25.23.5.3

**Pfad Konsole:**

**Setup** > **RADIUS** > **Dynamic-Peer-Discovery** > **Services**

**Mögliche Werte:**

**RADIUS**
**RADSEC**

**DNS-Zeitlimit**

Die Zeitspanne in Sekunden, innerhalb der alle DNS-Anfragen für einen NAI abgehandelt sein müssen. Das schließt auch die zweistufige Variante über NAPTR- und nachfolgende SRV-Anfragen ein.

**SNMP-ID:**

2.25.23.6

**Pfad Konsole:**

**Setup** > **RADIUS** > **Dynamic-Peer-Discovery**

**Mögliche Werte:**

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

**Default-Wert:**

3

**Min.-Eff.-TTL**

Vom DNS-Server gemeldete TTL-Werte, die kürzer als diese Zeit sind, werden auf diesen Wert angehoben.

**SNMP-ID:**

2.25.23.7

**Pfad Konsole:**

**Setup** > **RADIUS** > **Dynamic-Peer-Discovery**

**Mögliche Werte:**

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

**Default-Wert:**

60

**Backoff-Zeit**

Falls eine Auflösung in einem Fehler endet (DNS-Antwort mit Fehler, Timeout…), ist dies die Zeit in Sekunden, für die keine neuen Auflöseversuche für diesen Realm gemacht werden sollen.

**SNMP-ID:**

2.25.23.8

**Pfad Konsole:**

**Setup** > **RADIUS** > **Dynamic-Peer-Discovery**

**Mögliche Werte:**

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

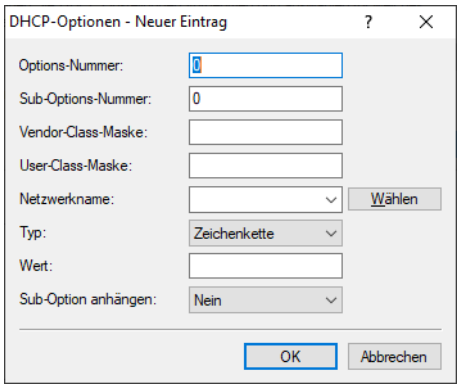
**Default-Wert:**

600

# 11 Weitere Dienste

## 11.1 Zusammenfassen mehrerer DHCP Option 43-Suboptionen im DHCP-Server

Bisher sendete der LCOS-DHCP-Server für Optionen, die über **IPv4** > **DHCPv4** > **DHCP-Optionen** konfiguriert wurden, immer eine separate DHCP-Option 43 an anfragende DHCP-Clients. Ab LCOS 10.50 ist es nun möglich, mehrere DHCP Option 43-Suboptionen zusammenzufassen.




**Sub-Option anhängen**

Für jede Sub-Option der Option 43 wird eine eigene Option angelegt und übermittelt. Über diesen Schalter ist es möglich, mehrere DHCP-Option-43-Sub-Optionen zusammenzufassen. Dazu hier auf **Ja** stellen. Das Zusammenfassen geschieht, wenn:

- **Options-Nummer** gleich 43 ist
- **Sub-Options-Nummer** ungleich Null ist
- Davor in der Tabelle bereits eine Option 43 mit Sub-Options-Nummer ungleich Null steht

Beachten Sie die maximale Länge von 255 Zeichen für eine Option.

### 11.1.1 Ergänzungen im Setup-Menü

#### Sub-Option-anhaengen

Für jede Sub-Option der Option 43 wird eine eigene Option angelegt und übermittelt. Über diesen Schalter ist es möglich, mehrere DHCP-Option-43-Suboptionen zusammenzufassen. Dazu hier auf „Ja“ stellen. Das Zusammenfassen geschieht, wenn:

- **Options-Nummer** gleich 43 ist
- **Sub-Options-Nummer** ungleich Null ist
- Davor in der Tabelle bereits eine Option 43 mit Sub-Options-Nummer ungleich Null steht

Beachten Sie die maximale Länge von 255 Zeichen für eine Option.

**SNMP-ID:**

2.10.26.8

**Pfad Konsole:**

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

**Mögliche Werte:**

**Ja**

Wenn möglich, Sub-Optionen der DHCP-Option 43 zusammenfassen.

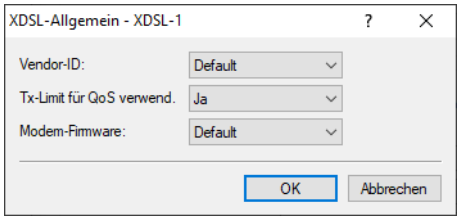
**Nein**

Diese Sub-Option der DHCP-Option 43 als eigene Option übermitteln.

## 11.2 Funktion zur Umschaltung auf alternative DSL-Modem-Firmware

In dieser Tabelle finden Sie die Einstellungen zur Modem-Firmware. Da es keine „beste" DSL-Firmware für jede Situation gibt, kann hier ab LCOS 10.50 ggf. auf eine andere im LCOS vorhandene Modem-Firmware umgeschaltet werden.

Dazu wurden die Einstellungen in LANconfig unter **Schnittstellen** > **WAN** > **XDSL-Allgemein** zur Verfügung gestellt. Dabei wurden auch weitere generische Einstellungen zu xDSL hierhin verschoben, sodass diese nun individuell pro xDSL-Interface eingestellt werden können.




LANconfig: **Schnittstellen** > **WAN** > **XDSL-Allgemein**

Konsole: **Setup** > **xDSL** > **Allgemein**

**Vendor-ID**

Die von der deutschen Bundesnetzagentur vorgegebene Kennung für LANCOM Geräte funktioniert nicht in allen Ländern. Für diese wie z. B. die Schweiz muss die Alternativkennung ausgewählt werden.

**Tx-Limit für QoS verwenden**

Dieser Schalter verändert die Verwendung der Sync-Datenrate als QoS-Datenrate. Wenn aktiviert (Default), dann wird die Sync-Datenrate als QoS-Datenrate verwendet. Sonst wird die Sync-Datenrate nicht verwendet und die Schnittstelle verhält sich bezüglich der QoS-Datenrate wie eine DSL-Schnittstelle.

**Modem-Firmware**

Mit diesem Schalter kann zwischen zwei im LCOS hinterlegten Versionen der Modem-Firmware gewählt werden.

Diese Spalte ist nur bei Geräten vorhanden, bei denen das LCOS eine alternative Modem-Firmware enthält.

## 11.2.1 Ergänzungen im Setup-Menü

### Allgemein

In dieser Tabelle finden Sie die Einstellungen zur Modem-Firmware. Da es keine „beste" DSL-Firmware für jede Situation gibt, kann hier ggf. auf eine andere im LCOS vorhandene Modem-Firmware umgeschaltet werden.

**SNMP-ID:**

2.42.5

**Pfad Konsole:**

**Setup** > **xDSL**

**Interface**

Fester Wert für dieses Interface: 1 für XDSL-1, 2 für XDSL-2 usw.

**SNMP-ID:**

2.42.5.1

**Pfad Konsole:**

**Setup** > **xDSL** > **Allgemein**

**Herstellerkennung**

Die von der deutschen Bundesnetzagentur vorgegebene Kennung für LANCOM Geräte funktioniert nicht in allen Ländern. Für diese wie z. B. die Schweiz muss die Alternativkennung ausgewählt werden.

**SNMP-ID:**

2.42.5.2

**Pfad Konsole:**

**Setup** > **xDSL** > **Allgemein**

**Mögliche Werte:**

**Standardkennung**
**Alternativkennung**

**Default-Wert:**

Standardkennung

**Sync-limitiert-TX-Rate**

Diese Einstellung gestattet es, die Begrenzung der Sendedatenrate auf die Sync-Datenrate zu deaktivieren. Dies wird in der Qualitätssicherung für Tests verwendet, wenn z. B. festgestellt werden soll, ab welcher Datenrate das Modem den Durchsatz begrenzt.

**SNMP-ID:**

2.42.5.3

**Pfad Konsole:**

**Setup** > **xDSL** > **Allgemein**

**Mögliche Werte:**

**Ja**

Die Sync-Datenrate wird als QoS-Datenrate verwendet.

**Nein**

Die Sync-Datenrate wird nicht verwendet und die Schnittstelle verhält sich bezüglich der QoS-Datenrate wie eine DSL-Schnittstelle.

**Default-Wert:**

Ja

**Modem-Firmware**

Mit diesem Schalter kann zwischen zwei im LCOS hinterlegten Versionen der Modem-Firmware gewählt werden.

Diese Spalte ist nur bei Geräten vorhanden, bei denen das LCOS eine alternative Modem-Firmware enthält.

**SNMP-ID:**

2.42.5.4

**Pfad Konsole:**

**Setup** > **xDSL** > **Allgemein**

**Mögliche Werte:**

**Standard**

Dies wählt die von LANCOM bevorzugte Version aus.

**Alternativ**

Diese Einstellung wählt eine Version aus, die an manchen Anschlüssen zu einer Verbesserung des Verhaltens führt.

**Default-Wert:**

Standard

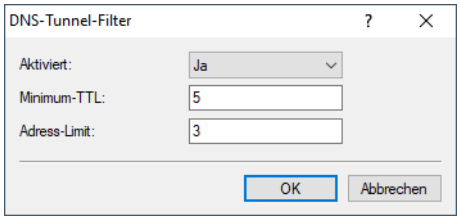
## 11.3 DNS-Einstellungen in eigenen Bereich verschoben

Ab LCOS 10.50 finden Sie die DNS-Einstellungen nicht mehr unter **IPv4** > **DNS** bzw. **IPv4** > **DNS-Filter/Aliase**, sondern in einem eigenen Bereich unter **DNS** > **Allgemein** und **DNS** > **Filter/Aliase**.

## 11.4 DNS-Filter für DNS-Datentunnel

Es gibt Verfahren und Tools, mit denen man durch DNS-Pakete Daten schleusen kann, um so bestimmte Prüfungen z. B. in der Firewall zu umgehen. Durch diesen Datentunnel können dann beliebige Daten über das DNS-Protokoll transportiert werden. Diese Methode ist zwar laut Protokoll standardkonform, in bestimmten Szenarien soll der Aufbau dieser Tunnel aber verhindert werden. Die Datentunnel werden an bestimmten Merkmalen bzw. Eigenschaften der DNS-Pakete erkannt.

Ab LCOS 10.50 können Sie diesen DNS-Filter für DNS-Datentunnel einrichten.




LANconfig: **DNS** > **Filter/Aliase** > **DNS-Tunnel-Filter**

Konsole: **Setup** > **DNS** > **Tunnel-Filter**

**Aktiviert**

Über diesen Schalter kann der Tunnel-Filter aus- bzw. eingeschaltet werden.

**Minimum-TTL**

Minimale TTL ab der Ressource-Records akzeptiert werden. Wenn ein Record (mit Ausnahme von A und AAAA) eine kleinere TTL hat, so wird das komplette Paket verworfen.

Bereich: 0-99; Default: 5

**Adress-Limit**

Maximale Anzahl von A und AAAA Recordes mit einer TTL kleiner als Minimum-TTL, die noch akzeptiert werden, bevor das komplette Paket verworfen wird.

Bereich: 0-99; Default: 3

### 11.4.1 Ergänzungen im Setup-Menü

#### Tunnel-Filter

Es gibt Verfahren und Tools, mit denen man durch DNS-Pakete Daten schleusen kann, um so bestimmte Prüfungen z. B. in der Firewall zu umgehen. Durch diesen Datentunnel können dann beliebige Daten über das DNS-Protokoll transportiert werden.

Diese Methode ist zwar laut Protokoll standardkonform, in bestimmten Szenarien soll der Aufbau dieser Tunnel aber verhindert werden. Die Datentunnel werden an bestimmten Merkmalen bzw. Eigenschaften der DNS-Pakete erkannt.

**SNMP-ID:**

2.17.21

**Pfad Konsole:**

**Setup** > **DNS**

**Aktiv**

Über diesen Schalter kann der Tunnel-Filter aus- bzw. eingeschaltet werden.

**SNMP-ID:**

2.17.21.1

**Pfad Konsole:**

**Setup** > **DNS** > **Tunnel-Filter**

**Mögliche Werte:**

**nein**

Tunnelfilter ist nicht aktiv.

**ja**

Tunnelfilter ist aktiv.

**Default-Wert:**

ja

**Minimum-TTL**

Minimale TTL ab der Ressource-Records akzeptiert werden. Wenn ein Record (mit Ausnahme von A und AAAA) eine kleinere TTL hat, so wird das komplette Paket verworfen.

**SNMP-ID:**

2.17.21.2

**Pfad Konsole:**

**Setup** > **DNS** > **Tunnel-Filter**

**Mögliche Werte:**

0 … 99

**Default-Wert:**

5

**Adress-Limit**

Maximale Anzahl von A und AAAA Recordes mit einer TTL kleiner als Minimum-TTL, die noch akzeptiert werden, bevor das komplette Paket verworfen wird.

**SNMP-ID:**

2.17.21.3

**Pfad Konsole:**

**Setup** > **DNS** > **Tunnel-Filter**

**Mögliche Werte:**

0 … 99

**Default-Wert:**

3

## 11.5 GPON-Unterstützung

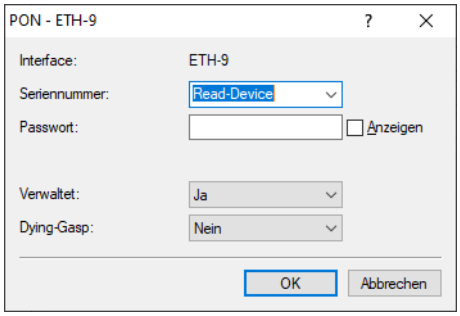
GPON (Gigabit Passive Optical Network) ist ein optischer Übertragungsstandard für Glasfaseranschlüsse (FTTH). LANCOM bietet hierzu GPON-SFP-Module an, die in LANCOM Routern mit SFP-Schnittstelle betrieben werden können. Die Liste der kompatiblen Geräte befindet sich im jeweiligen GPON-SFP-Datenblatt.

Mit einem GPON-Modul kann der LANCOM Router direkt am Glasfaseranschluss des Providers ohne separates Modem betrieben werden. Bitte kontaktieren Sie ihren Provider ob ein Betrieb ohne Modem und mit SFP-Modul unterstützt wird. In der Regel werden GPON-Modems anhand der Seriennummer und / oder mit einem GPON-Passwort authentifiziert, so dass ein Betrieb ohne Unterstützung des Providers nicht möglich ist.

In der Regel muss für den GPON-Betrieb nichts im Gerät konfiguriert werden.


LANconfig: **Interfaces** > **WAN** > **PON**

Konsole: **Setup** > **Schnittstellen** > **PON**




**Interface**

Wählen Sie hier das SFP-Interface aus, in dem das PON-Modul gesteckt ist, z. B. SFP-1.

**Seriennummer**

Jedes Modul besitzt vom Hersteller ab Werk bereits eine eindeutige Seriennummer im Format Herstellerkennung+Nummer, z. B. GPON12345678. Die Seriennummer besteht aus 8 Oktetten. Die Oktette 1 bis 4 beinhalten die Vendor-ID, die Oktette 5 bis 8 eine herstellerspezifische Seriennummer. Die Darstellung ist normalerweise gemischt ASCII / Hex. Dabei wird die Vendor-ID in ASCII dargestellt, die herstellerspezifische Seriennummer in Hex. Die Länge ist 12 Zeichen. Die Seriennummer wird aus dem Modul ausgelesen bzw. in das Modul geschrieben.

Teilen Sie diese Seriennummer ihrem Internetprovider mit, um das Modul zu registrieren.

Ändern Sie diese Seriennummer nur, falls Sie ein vorhandenes Gerät ersetzen möchten, das bereits am OLT ihres Providers registriert ist und keine neue Registrierung beim Provider gewünscht ist.

Ein Provider kann einen GPON-Modem eindeutig mit Seriennummer, Seriennummer und Passwort oder nur durch Passwort authentifizieren.

Im Falle eines Modultausch setzen Sie die Konfiguration bitte auf Default zurück, sonst werden die alte Seriennummer und Passwort auch für das neue Modul übernommen. Gehen Sie daher wie folgt vor: entfernen Sie das alte Modul, setzen Sie die Konfigurationszeile zurück, danach das neue Modul einsetzen.

Default ist der spezielle Wert **Read-Device**. Ist dieser gesetzt, wird die Konfiguration aus dem Modul gelesen und in die LCOS-Konfiguration übernommen.

**Passwort**

Geben Sie hier das PON-Passwort ein, falls Ihr Provider eine Authentifizierung per Passwort durchführt. Andere Begriffe für PON-Passwort sind „ONT-Installationskennung" oder „PLOAM-Passwort". Das Passwort besteht aus 10 Oktetten in ASCII-Darstellung. Die Länge ist 10 Zeichen. Das Passwort ist im Default leer.

Das PON-Passwort für Ihren Anschluss erhalten Sie von Ihrem Internet-Provider.

**Verwaltet**

Konfigurieren Sie hier, ob das Modem durch das Betriebssystem verwaltet werden soll. In diesem Fall schreibt das System die konfigurierte Seriennummer und das PON-Passwort (empfohlen).

**Dying-Gasp**

Konfigurieren Sie hier, ob das PON-Modem Dying Gasp aktivieren soll. Dying Gasp ist ein Signal, dass das Modem an den Provider sendet um den Verlust der Stromversorgung zu signalisieren.

## 11.5.1 Ergänzungen im Setup-Menü

### PON

Dieses Menü enthält die Einstellungen für die PON-Schnittstellen (Passive Optical Network).

GPON (Gigabit Passive Optical Network) ist ein optischer Übertragungsstandard für Glasfaseranschlüsse (FTTH). LANCOM bietet hierzu GPON-SFP-Module an, die in LANCOM Routern mit SFP-Schnittstelle betrieben werden können. Die Liste der kompatiblen Geräte befindet sich im jeweiligen GPON-SFP-Datenblatt.

Mit einem GPON-Modul kann der LANCOM Router direkt am Glasfaseranschluss des Providers ohne separates Modem betrieben werden. Bitte kontaktieren Sie ihren Provider ob ein Betrieb ohne Modem und mit SFP-Modul unterstützt wird. In der Regel werden GPON-Modems anhand der Seriennummer und / oder mit einem GPON-Passwort authentifiziert, so dass ein Betrieb ohne Unterstützung des Providers nicht möglich ist.

**SNMP-ID:**

2.23.23

**Pfad Konsole:**

**Setup** > **Schnittstellen**

**Interface**

Die am Gerät vorhanden PON-Interfaces. Wählen Sie hier das SFP-Interface aus, in dem das PON-Modul gesteckt ist, z. B. SFP-1.

**SNMP-ID:**

2.23.23.1

**Pfad Konsole:**

**Setup** > **Schnittstellen** > **PON**

**Seriennummer**

Jedes Modul besitzt vom Hersteller ab Werk bereits eine eindeutige Seriennummer im Format Herstellerkennung+Nummer, z. B. GPON12345678. Die Seriennummer besteht aus 8 Oktetten. Die Oktette 1 bis 4 beinhalten die Vendor-ID, die Oktette 5 bis 8 eine herstellerspezifische Seriennummer. Die Darstellung ist normalerweise gemischt ASCII / Hex. Dabei wird die Vendor-ID in ASCII dargestellt, die herstellerspezifische Seriennummer in Hex. Die Länge ist 12 Zeichen. Die Seriennummer wird aus dem Modul ausgelesen bzw. in das Modul geschrieben.

Teilen Sie diese Seriennummer ihrem Internetprovider mit, um das Modul zu registrieren.

Ändern Sie diese Seriennummer nur, falls Sie ein vorhandenes Gerät ersetzen möchten, das bereits am OLT ihres Providers registriert ist und keine neue Registrierung beim Provider gewünscht ist.

Ein Provider kann einen GPON-Modem eindeutig mit Seriennummer, Seriennummer und Passwort oder nur durch Passwort authentifizieren.

Im Falle eines Modultausch setzen Sie die Konfiguration bitte auf Default zurück, sonst werden die alte Seriennummer und Passwort auch für das neue Modul übernommen. Gehen Sie daher wie folgt vor: entfernen Sie das alte Modul, setzen Sie die Konfigurationszeile zurück, danach das neue Modul einsetzen.

**SNMP-ID:**

2.23.23.2

**Pfad Konsole:**

**Setup** > **Schnittstellen** > **PON**

**Mögliche Werte:**

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

**Besondere Werte:**

**Read-Device**

Liest die Konfiguration aus dem Modul und übernommt diese in die LCOS-Konfiguration.

### Passwort

Geben Sie hier das PON-Passwort ein, falls Ihr Provider eine Authentifizierung per Passwort durchführt. Andere Begriffe für PON-Passwort sind „ONT-Installationskennung“ oder „PLOAM-Passwort“. Das Passwort besteht aus 10 Oktetten in ASCII-Darstellung. Die Länge ist 10 Zeichen. Das Passwort ist im Default leer.

Das PON-Passwort für Ihren Anschluss erhalten Sie von Ihrem Internet-Provider.

**SNMP-ID:**

2.23.23.3

**Pfad Konsole:**

**Setup** > **Schnittstellen** > **PON**

**Mögliche Werte:**

max. 10 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

### Managed

Konfigurieren Sie hier, ob das Modem durch das Betriebssystem verwaltet werden soll. In diesem Fall schreibt das System die konfigurierte Seriennummer und das PON-Passwort (empfohlen).

**SNMP-ID:**

2.23.23.4

**Pfad Konsole:**

**Setup** > **Schnittstellen** > **PON**

**Mögliche Werte:**

**nein**
**ja**

### Dying-Gasp

Konfigurieren Sie hier, ob das PON-Modem Dying Gasp aktivieren soll. Dying Gasp ist ein Signal, dass das Modem an den Provider sendet um den Verlust der Stromversorgung zu signalisieren.

**SNMP-ID:**

2.23.23.5

**Pfad Konsole:**

**Setup** > **Schnittstellen** > **PON**

**Mögliche Werte:**

**nein**
**ja**

# 11.6 802.1X-Authenticator für Ethernet-Ports

Mittels des 802.1X-Authenticators können die an die Ethernet-Ports eines LANCOM Gerätes angeschlossenen Geräte mittels 802.1X authentifiziert werden. Dies kann dazu dienen, die Sicherheit vor ungefugtem Zugriff auf das Netzwerk auch im kabelgebundenen Bereich zu erhöhen.

Ab LCOS 10.50 RU4 gibt es die Möglichkeit, einen eigenen RADIUS-Server nur für den MAC-Authentisierungs-Bypass anzugeben. Hierdurch können getrennte RADIUS-Server für 802.1X und den MAC-Authentisierungs-Bypass verwendet werden. Dies erfolgt über den Eintrag **Setup** > **LAN** > **IEEE802.1X** > **Authenticator-Ifc-Setup** > **Umgehung-RADIUS-Server** auf der Kommandozeile.

## 11.6.1 Ergänzungen im Setup-Menü

### Umgehung-RADIUS-Server

Der hier angegebene RADIUS-Server wird nur für den MAC-Authentisierungs-Bypass verwendet. Hierdurch können getrennte RADIUS-Server für 802.1X und den MAC-Authentisierungs-Bypass verwendet werden. Refernzieren Sie dazu einen der Einträge unter *2.30.3 Radius-Server* oder legen dort ggfs. einen neuen Eintrag an. Das Format der übermittelten MAC-Adresse können Sie unter *2.4.10.4 Benutzername-Attribut-Format* anpassen.

**SNMP-ID:**

2.4.10.3.6

**Pfad Konsole:**

**Setup** > **LAN** > **IEEE802.1X** > **Authenticator-Ifc-Setup**

**Mögliche Werte:**

**Name** aus **Setup** > **IEEE802.1X** > **RADIUS-Server**

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

# 12 Ergänzungen im Menüsystem

## 12.1 Msg-Authenticator-erforderlich

Neuer Schalter ab LCOS 10.50 RU14. Definiert, ob das Vorhandensein des Message-Authenticator-Attributs in RADIUS-Nachrichten auf Client-Seite erzwingt. Die Client-Seite ist die Seite, die den RADIUS-Accept/Fail empfängt.

**SNMP-ID:**

2.2.22.28

**Pfad Konsole:**

**Setup** > **WAN** > **RADIUS**

**Mögliche Werte:**

**nein**

Access-Requests müssen keinen Message-Authenticator enthalten.

**ja**

Access-Requests müssen immer einen Message-Authenticator enthalten.

**Default-Wert:**

nein

## 12.2 L2TP-Msg-Authenticator-erforderlich

Neuer Schalter ab LCOS 10.50 RU14. Definiert, ob das Vorhandensein des Message-Authenticator-Attributs in RADIUS-Nachrichten auf Client-Seite erzwingt. Die Client-Seite ist die Seite, die den RADIUS-Accept/Fail empfängt.

**SNMP-ID:**

2.2.22.29

**Pfad Konsole:**

**Setup** > **WAN** > **RADIUS**

**Mögliche Werte:**

**nein**

Access-Requests müssen keinen Message-Authenticator enthalten.

**ja**

Access-Requests müssen immer einen Message-Authenticator enthalten.

**Default-Wert:**

nein

## 12.3 Msg-Authenticator-erforderlich

Neuer Schalter ab LCOS 10.50 RU14. Definiert, ob das Vorhandensein des Message-Authenticator-Attributs in RADIUS-Nachrichten auf Client-Seite erzwingt. Die Client-Seite ist die Seite, die den RADIUS-Accept/Fail empfängt.

**SNMP-ID:**

2.11.81.1.10

**Pfad Konsole:**

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

**Mögliche Werte:**

**nein**

Access-Requests müssen keinen Message-Authenticator enthalten.

**ja**

Access-Requests müssen immer einen Message-Authenticator enthalten.

**Default-Wert:**

nein

## 12.4 Msg-Authenticator-erforderlich

Neuer Schalter ab LCOS 10.50 RU14. Definiert, ob das Vorhandensein des Message-Authenticator-Attributs in RADIUS-Nachrichten auf Client-Seite erzwingt. Die Client-Seite ist die Seite, die den RADIUS-Accept/Fail empfängt.

**SNMP-ID:**

2.12.29.21

**Pfad Konsole:**

**Setup** > **WLAN** > **RADIUS-Zugriffspruefung**

**Mögliche Werte:**

**nein**

Access-Requests müssen keinen Message-Authenticator enthalten.

**ja**

Access-Requests müssen immer einen Message-Authenticator enthalten.

**Default-Wert:**

nein

## 12.5 Backup-Msg-Authenticator-erforderlich

Neuer Schalter ab LCOS 10.50 RU14. Definiert, ob das Vorhandensein des Message-Authenticator-Attributs in RADIUS-Nachrichten auf Client-Seite erzwingt. Die Client-Seite ist die Seite, die den RADIUS-Accept/Fail empfängt.

**SNMP-ID:**

2.12.29.22

**Pfad Konsole:**

**Setup** > **WLAN** > **RADIUS-Zugriffspruefung**

**Mögliche Werte:**

**nein**

Access-Requests müssen keinen Message-Authenticator enthalten.

**ja**

Access-Requests müssen immer einen Message-Authenticator enthalten.

**Default-Wert:**

nein

## 12.6 Msg-Authenticator-erforderlich

Neuer Schalter ab LCOS 10.50 RU14. Definiert, ob das Vorhandensein des Message-Authenticator-Attributs in RADIUS-Nachrichten auf Client-Seite erzwingt. Die Client-Seite ist die Seite, die den RADIUS-Accept/Fail empfängt.

**SNMP-ID:**

2.19.36.9.1.1.11

**Pfad Konsole:**

**Setup** > **VPN** > **IKEv2** > **RADIUS** > **Autorisierung** > **Server**

**Mögliche Werte:**

**nein**
Access-Requests müssen keinen Message-Authenticator enthalten.

**ja**
Access-Requests müssen immer einen Message-Authenticator enthalten.

**Default-Wert:**

nein

## 12.7 Msg-Authenticator-erforderlich

Neuer Schalter ab LCOS 10.50 RU14. Definiert, ob das Vorhandensein des Message-Authenticator-Attributs in RADIUS-Nachrichten auf Client-Seite erzwingt. Die Client-Seite ist die Seite, die den RADIUS-Accept/Fail empfängt.

**SNMP-ID:**

2.25.10.2.6

**Pfad Konsole:**

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

**Mögliche Werte:**

**nein**
Access-Requests müssen keinen Message-Authenticator enthalten.

**ja**
Access-Requests müssen immer einen Message-Authenticator enthalten.

**Nur-Proxy**
Falls ein Access-Request ein Proxy-State-Attribut enthält, muss ein Message-Authenticator enthalten sein.

**Default-Wert:**

nein

## 12.8 Msg-Authenticator-erforderlich

Neuer Schalter ab LCOS 10.50 RU14. Definiert, ob das Vorhandensein des Message-Authenticator-Attributs in RADIUS-Nachrichten auf Client-Seite erzwingt. Die Client-Seite ist die Seite, die den RADIUS-Accept/Fail empfängt.

**SNMP-ID:**

2.25.10.3.18

**Pfad Konsole:**

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

**Mögliche Werte:**

**nein**

Access-Requests müssen keinen Message-Authenticator enthalten.

**ja**

Access-Requests müssen immer einen Message-Authenticator enthalten.

**Default-Wert:**

nein

## 12.9 Msg-Authenticator-erforderlich

Neuer Schalter ab LCOS 10.50 RU14. Definiert, ob das Vorhandensein des Message-Authenticator-Attributs in RADIUS-Nachrichten auf Client-Seite erzwingt. Die Client-Seite ist die Seite, die den RADIUS-Accept/Fail empfängt.

**SNMP-ID:**

2.25.10.16.6

**Pfad Konsole:**

**Setup** > **RADIUS** > **Server** > **IPv6-Clients**

**Mögliche Werte:**

**nein**

Access-Requests müssen keinen Message-Authenticator enthalten.

**ja**

Access-Requests müssen immer einen Message-Authenticator enthalten.

**Nur-Proxy**

Falls ein Access-Request ein Proxy-State-Attribut enthält, muss ein Message-Authenticator enthalten sein.

**Default-Wert:**

nein