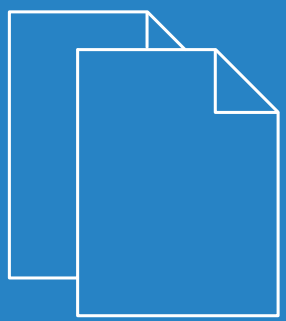
SICHER. **VERNETZT.**

LCOS 10.40

Addendum



05/2020

LANCOM Systems

Inhalt

Copyright

LANCOM Systems GmbH

Adenauerstr. 20/B2

52146 Würselen

Deutschland

www.lancom-systems.de

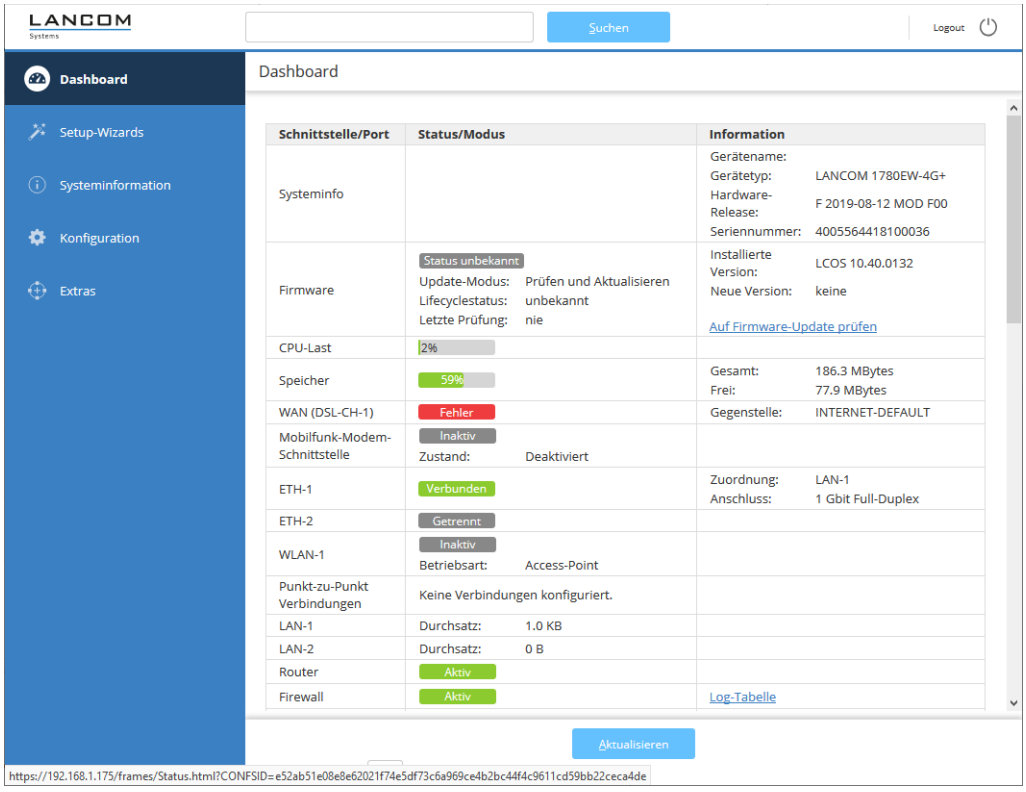
1 Addendum zur LCOS-Version 10.40

Dieses Dokument beschreibt die Änderungen und Ergänzungen in der LCOS-Version 10.40 gegenüber der vorherigen Version.

2 Konfiguration

2.1 Modernes Look & Feel: Neue WEBconfig

Ab LCOS 10.40 erfreuen Sie sich nun an einem ganz neuen Look & Feel in der LANCOM WEBconfig. Angelehnt an das moderne und helle Design der LANCOM Management Cloud wurde die Benutzeroberfläche komplett neu überarbeitet. Die attraktive Optik und Nutzerführung steigert die Usability.



Im **Dashboard** erhalten Sie die Informationen Ihres Gerätes angezeigt. **Systeminformation**, **Konfiguration** und **Extras** sind wie gewohnt vorhanden. Den **LCOS-Menübaum** und das **Dateimanagement** finden Sie nun unter **Extras**.

2.2 TLS 1.3 Client-Modus

Ab LCOS 10.40 unterstützt Ihr Gerät TLS 1.3 für den Zugriff auf Webserver. Dies wird z. B. verwendet, um eine aktualisierte Firmware herunterzuladen. TLS 1.3 stellt die neueste Weiterentwicklung des TLS-Standards dar und bietet z. B. durch die ausschließliche Verwendung moderner Cipher-Suiten und Perfect Forward Secrecy eine verbesserte Sicherheit im Vergleich zu den Vorgängerversionen.

Bei einem LCOS-Update wird die TLS 1.3-Unterstützung für den Client-Betrieb automatisch zur Konfiguration hinzugefügt. Entfernen Sie gegebenenfalls ältere Verfahren, die LCOS nicht mehr verwenden soll.

Die Unterstützung für TLS 1.3 im Server-Betrieb ist bereits seit LCOS 10.30 enthalten.

2.2.1 Ergänzungen im Setup-Menü

Versionen

Dieser Eintrag definiert die erlaubten Protokoll-Versionen.

SNMP-ID:

2.2.53.1

Pfad Konsole:

Setup > **WAN** > **SSL-fuer-Aktions-Tabelle**

Mögliche Werte:

SSLv3
TLSv1
TLSv1.1
TLSv1.2
TLSv1.3

Default-Wert:

TLSv1

TLSv1.1

TLSv1.2

TLSv1.3

Versionen

Dieser Eintrag definiert die erlaubten Protokoll-Versionen.

SNMP-ID:

2.11.29.2

Pfad Konsole:

Setup > **Config** > **Telnet-SSL**

Mögliche Werte:

SSLv3
TLSv1
TLSv1.1
TLSv1.2
TLSv1.3

Default-Wert:

TLSv1.2

TLSv1.3

Versionen

Dieser Eintrag definiert die erlaubten Protokoll-Versionen.

SNMP-ID:

2.11.55.1

Pfad Konsole:

Setup > **Config** > **SSL-fuer-Cron-Tabelle**

Mögliche Werte:

SSLv3
TLSv1
TLSv1.1
TLSv1.2
TLSv1.3

Default-Wert:

TLSv1

TLSv1.1

TLSv1.2

TLSv1.3

Versionen

Dieser Eintrag definiert die erlaubten Protokoll-Versionen für den Rollout Agent.

SNMP-ID:

2.11.92.15.1

Pfad Konsole:

Setup > **Config** > **Rollout-Agent** > **SSL**

Mögliche Werte:

SSLv3
TLSv1
TLSv1.1
TLSv1.2
TLSv1.3

Default-Wert:

TLSv1

TLSv1.1

TLSv1.2

TLSv1.3

Versionen

Wählen Sie hier die Verschlüsselungsversion(en) aus, die verwendet werden soll(en).

SNMP-ID:

2.21.20.11.1

Pfad Konsole:

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

Mögliche Werte:

SSLv3
TLSv1
TLSv1.1
TLSv1.2
TLSv1.3

Default-Wert:

TLSv1

TLSv1.1

TLSv1.2

TLSv1.3

Versionen

Dieser Eintrag definiert die erlaubten Protokoll-Versionen.

SNMP-ID:

2.21.40.3

Pfad Konsole:

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

Mögliche Werte:

SSLv3
TLSv1
TLSv1.1
TLSv1.2
TLSv1.3

Default-Wert:

TLSv1

TLSv1.1

TLSv1.2

TLSv1.3

Versionen

Dieser Eintrag definiert die erlaubten Protokoll-Versionen.

SNMP-ID:

2.24.41.2.19.1

Pfad Konsole:

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

Mögliche Werte:

SSLv3
TLSv1
TLSv1.1
TLSv1.2
TLSv1.3

Default-Wert:

TLSv1

TLSv1.1

TLSv1.2

TLSv1.3

Versionen

Dieser Eintrag definiert die erlaubten Protokoll-Versionen.

SNMP-ID:

2.24.41.5.4.1

Pfad Konsole:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **Radius-Server** > **SSL**

Mögliche Werte:

SSLv3
TLSv1
TLSv1.1
TLSv1.2
TLSv1.3

Default-Wert:

TLSv1

TLSv1.1

TLSv1.2

TLSv1.3

Versionen

Dieser Eintrag definiert die erlaubten Protokoll-Versionen.

SNMP-ID:

2.24.53.1

Pfad Konsole:

Setup > **Public-Spot-Modul** > **SSL-fuer-Seitentabelle**

Mögliche Werte:

SSLv3
TLSv1
TLSv1.1
TLSv1.2
TLSv1.3

Default-Wert:

TLSv1

TLSv1.1

TLSv1.2

TLSv1.3

Versionen

Dieser Eintrag definiert die erlaubten Protokoll-Versionen.

SNMP-ID:

2.27.14.1

Pfad Konsole:

Setup > **Mail** > **SSL**

Mögliche Werte:

SSLv3
TLSv1
TLSv1.1
TLSv1.2
TLSv1.3

Default-Wert:

TLSv1

TLSv1.1

TLSv1.2

TLSv1.3

Versionen

Dieser Eintrag definiert die erlaubten Protokoll-Versionen.

SNMP-ID:

2.37.27.39.1

Pfad Konsole:

Setup > **WLAN-Management** > **Zentrales-Firmware-Management** > **SSL**

Mögliche Werte:

SSLv3
TLSv1
TLSv1.1
TLSv1.2
TLSv1.3

Default-Wert:

TLSv1.2

TLSv1.3

Versionen

Dieser Eintrag definiert die erlaubten Protokoll-Versionen.

SNMP-ID:

2.44.26.1

Pfad Konsole:

Setup > **CWMP** > **SSL**

Mögliche Werte:

SSLv3
TLSv1
TLSv1.1
TLSv1.2
TLSv1.3

Default-Wert:

TLSv1

TLSv1.1

TLSv1.2

TLSv1.3

Versionen

Dieser Eintrag definiert die erlaubten Protokoll-Versionen.

SNMP-ID:

2.60.1.5.1

Pfad Konsole:

Setup > **Automatisches-Laden** > **Netzwerk** > **SSL**

Mögliche Werte:

SSLv3
TLSv1
TLSv1.1
TLSv1.2
TLSv1.3

Default-Wert:

TLSv1

TLSv1.1

TLSv1.2

TLSv1.3

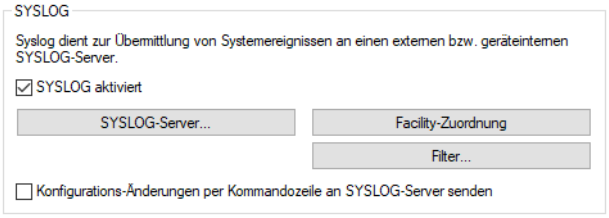
3 Diagnose

3.1 Filter für Syslog-Meldungen

Ab LCOS 10.40 unterstützt Ihr Gerät Filter für Syslog-Meldungen. Werden die Syslog-Meldungen an einen oder mehrere Server übertragen, indem Einstellungen für den Empfang bestimmter Meldungen konfiguriert wurden, so werden alle konfigurierten Meldungen mit der konfigurierten Quelle und Priorität an die Server übertragen. Mitunter ist es jedoch wünschenswert, bestimmte Meldungen für die Server auszufiltern, nur bestimmte Meldungen überhaupt zu schicken oder auch deren Quelle und Priorität zu verändern, falls sie im Serverlog eine andere Gewichtung erhalten sollen. Der Syslog-Filter erlaubt es, Meldungen in Abhängigkeit von Quelle, Priorität und / oder Meldungstext zu filtern.

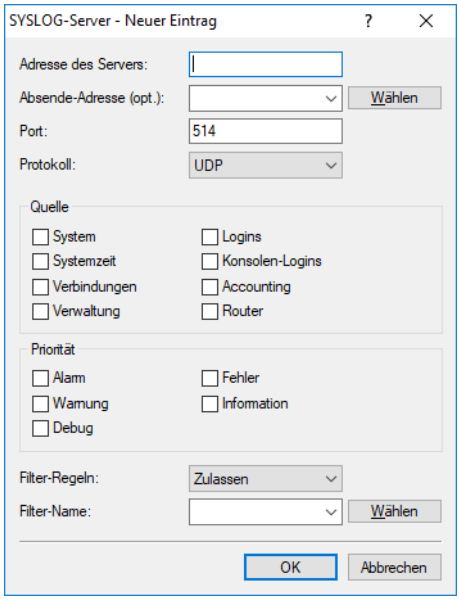
3.1.1 SYSLOG konfigurieren

In LANconfig konfigurieren Sie SYSLOG unter **Meldungen/Monitoring** > **Protokolle** im Abschnitt **SYSLOG**.



SYSLOG-Server

In LANconfig konfigurieren Sie die Einstellungen zum SYSLOG-Server unter **Meldungen/Monitoring** > **Protokolle** > **SYSLOG** über **SYSLOG-Server**.



Filter-Regeln

Werden die Syslog-Meldungen an einen oder mehrere Server übertragen, indem Einstellungen für den Empfang bestimmter Meldungen konfiguriert wurden, so werden alle konfigurierten Meldungen mit der konfigurierten Quelle und Priorität an die Server übertragen. Mitunter ist es jedoch wünschenswert, bestimmte Meldungen für die Server auszufiltern, nur bestimmte Meldungen überhaupt zu schicken oder auch deren Quelle und Priorität zu verändern, falls sie im Serverlog eine andere Gewichtung erhalten sollen. Der Syslog-Filter erlaubt es, Meldungen in Abhängigkeit von Quelle, Priorität und / oder Meldungstext zu filtern. Dabei stellen Sie hier ein, ob die Meldungen, die über den im folgenden Feld eingestellten Filter bestimmt werden, zugelassen oder abgelehnt werden.

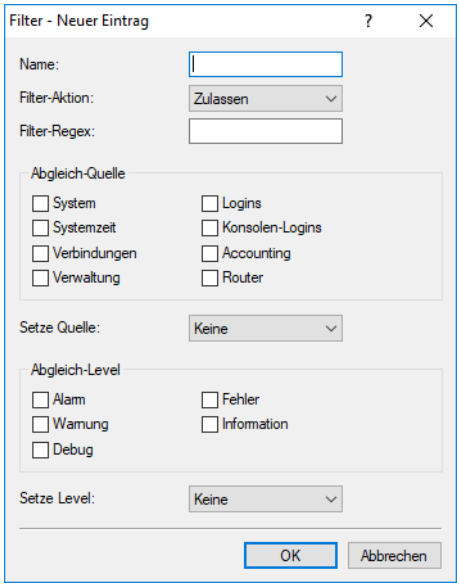
Filter-Name

Wählen Sie einen der konfigurierten Filter aus.

Filter

Werden die Syslog-Meldungen an einen oder mehrere Server übertragen, indem Einstellungen für den Empfang bestimmter Meldungen konfiguriert wurden, so werden alle konfigurierten Meldungen mit der konfigurierten Quelle und Priorität an die Server übertragen. Mitunter ist es jedoch wünschenswert, bestimmte Meldungen für die Server auszufiltern, nur bestimmte Meldungen überhaupt zu schicken oder auch deren Quelle und Priorität zu verändern, falls sie im Serverlog eine andere Gewichtung erhalten sollen. Der Syslog-Filter erlaubt es, Meldungen in Abhängigkeit von Quelle, Priorität und / oder Meldungstext zu filtern. Konfigurieren Sie hier diese Filter, die Sie dann bei Einträgen des SYSLOG-Servers verwenden können.

In LANconfig konfigurieren Sie die Filtereinstellungen zum SYSLOG-Server unter **Meldungen/Monitoring** > **Protokolle** > **SYSLOG** über **Filter**.



Name

Geben Sie diesem Filter einen aussagekräftigen Namen. Es können mehrere Regeln mit demselben Filter-Namen angelegt werden. Diese werden dann in der Reihenfolge, in der sie in der Filter-Tabelle angelegt werden, beim Versenden der Nachrichten geprüft. Trifft keine Regel in dieser Filterkette zu, wird die Nachricht gemäß der in der Server-Tabelle eingetragenen Default-Policy für den Server versendet oder verworfen.

Filter-Aktion

Aktion, falls die Regel zutrifft; „Zulassen" erlaubt das Versenden der Meldung an den Server, „Ablehnen" verwirft die Meldung.

Filter-Regex

Regulärer Ausdruck in Perl-Syntax (siehe z. B. *Regular expressions in Perl*), auf den der Meldungstext zutreffen muss. Ein leerer String bedeutet, dass der Meldungstext nicht betrachtet wird und daher alle Meldungstexte zutreffen.

Abgleich-Quelle

Quelle der Meldung, für die diese Regel gilt. Der Wert „keine“ steht für eine beliebige Quelle.

Setze Quelle

Neue Quelle der Meldung, falls die Regel zutrifft. Der Wert „Keine“ bedeutet, dass die Quelle nicht verändert wird.

Abgleich-Level

Priorität der Meldung, für die diese Regel gilt. Der Wert „keine“ steht für eine beliebige Priorität.

Setze Level

Neue Priorität der Meldung, falls die Regel zutrifft. Der Wert „Keine“ bedeutet, dass die Priorität nicht verändert wird.

3.1.2 Ergänzungen im Setup-Menü

Filter-Name

Referenziert einen SYSLOG-Filter.

SNMP-ID:

2.17.20.6

Pfad Konsole:

Setup > **DNS** > **SYSLOG**

Mögliche Werte:

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

Filter-Regel

Werden die Syslog-Meldungen an einen oder mehrere Server übertragen, indem Einstellungen für den Empfang bestimmter Meldungen konfiguriert wurden, so werden alle konfigurierten Meldungen mit der konfigurierten Quelle und Priorität an die Server übertragen. Mitunter ist es jedoch wünschenswert, bestimmte Meldungen für die Server auszufiltern, nur bestimmte Meldungen überhaupt zu schicken oder auch deren Quelle und Priorität zu verändern, falls sie im Serverlog eine andere Gewichtung erhalten sollen. Der Syslog-Filter erlaubt es, Meldungen in Abhängigkeit von Quelle, Priorität und / oder Meldungstext zu filtern. Dabei stellen Sie hier ein, ob die Meldungen, die über den im Feld **Filter-Name** eingestellten Filter bestimmt werden, zugelassen oder abgelehnt werden.

SNMP-ID:

2.17.20.7

Pfad Konsole:

Setup > **DNS** > **SYSLOG**

Mögliche Werte:

Erlauben
Ablehnen

Default-Wert:

Ablehnen

Filter-Regel

Werden die Syslog-Meldungen an einen oder mehrere Server übertragen, indem Einstellungen für den Empfang bestimmter Meldungen konfiguriert wurden, so werden alle konfigurierten Meldungen mit der konfigurierten Quelle und Priorität an die Server übertragen. Mitunter ist es jedoch wünschenswert, bestimmte Meldungen für die Server auszufiltern, nur bestimmte Meldungen überhaupt zu schicken oder auch deren Quelle und Priorität zu verändern, falls sie im Serverlog eine andere Gewichtung erhalten sollen. Der Syslog-Filter erlaubt es, Meldungen in Abhängigkeit von Quelle, Priorität und / oder Meldungstext zu filtern. Dabei stellen Sie hier ein, ob die Meldungen, die über den im Feld **Filter-Name** eingestellten Filter bestimmt werden, zugelassen oder abgelehnt werden.

SNMP-ID:

2.22.2.10

Pfad Konsole:

Setup > **SYSLOG** > **Tabelle-SYSLOG**

Mögliche Werte:

Erlauben
Ablehnen

Default-Wert:

Ablehnen

Filter-Name

Referenziert einen SYSLOG-Filter.

SNMP-ID:

2.22.2.11

Pfad Konsole:

Setup > **SYSLOG** > **Tabelle-SYSLOG**

Mögliche Werte:

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

Filter

In dieser Tabelle werden die Filter-Regeln definiert.

SNMP-ID:

2.22.13

Pfad Konsole:

Setup > **SYSLOG**

Idx.

Position des Eintrags in der Tabelle.

SNMP-ID:

2.22.13.1

Pfad Konsole:

Setup > **SYSLOG** > **Filter**

Mögliche Werte:

max. 4 Zeichen aus `[A_Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default-Wert:

leer

Filter-Name

Name der Filter-Regel; die Server-Tabelle verweist auf diesen Namen. Es können mehrere Regeln mit demselben Filter-Namen angelegt werden. Diese werden dann in der Reihenfolge ihrer Position in der Filter-Tabelle beim Versenden der Nachrichten geprüft. Trifft keine Regel in dieser Filterkette zu, wird die Nachricht gemäß der in der Server-Tabelle eingetragenen Default-Policy für den Server versendet oder verworfen.

SNMP-ID:

2.22.13.2

Pfad Konsole:

Setup > **SYSLOG** > **Filter**

Mögliche Werte:

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

Passende Quelle

Quelle der Meldung, für die diese Regel gilt. Der Wert „keine“ steht für eine beliebige Quelle.

SNMP-ID:

2.22.13.3

Pfad Konsole:

Setup > **SYSLOG** > **Filter**

Mögliche Werte:

keine
System
Login
Systemzeit
Konsole-Login
Verbindungen
Accounting
Administration
Router

Default-Wert:

keine

Passender Level

Priorität der Meldung, für die diese Regel gilt. Der Wert „keine“ steht für eine beliebige Priorität.

SNMP-ID:

2.22.13.4

Pfad Konsole:

Setup > **SYSLOG** > **Filter**

Mögliche Werte:

keine
Alarm
Fehler
Warnung
Info
Debug

Default-Wert:

keine

Reg. Ausdruck

Regulärer Ausdruck in Perl-Syntax, auf den der Meldungstext zutreffen muss. Ein leerer String bedeutet, dass der Meldungstext nicht betrachtet wird und daher alle Meldungstexte zutreffen.

SNMP-ID:

2.22.13.5

Pfad Konsole:

Setup > **SYSLOG** > **Filter**

Mögliche Werte:

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

Neue Quelle

Neue Quelle der Meldung, falls die Regel zutrifft. Der Wert „keine“ bedeutet, dass die Quelle nicht verändert wird.

SNMP-ID:

2.22.13.6

Pfad Konsole:

Setup > **SYSLOG** > **Filter**

Mögliche Werte:

keine
System
Login
Systemzeit
Konsole-Login
Verbindungen
Accounting
Administration
Router

Default-Wert:

keine

Neuer Level

Neue Priorität der Meldung, falls die Regel zutrifft. Der Wert „keine“ bedeutet, dass die Priorität nicht verändert wird.

SNMP-ID:

2.22.13.7

Pfad Konsole:

Setup > **SYSLOG** > **Filter**

Mögliche Werte:

keine
Alarm
Fehler
Warnung
Info
Debug

Default-Wert:

keine

Filter-Aktion

Aktion, falls die Regel zutrifft. Entweder das Versenden der Meldung an den Server erlauben oder ablehnen.

SNMP-ID:

2.22.13.8

Pfad Konsole:

Setup > **SYSLOG** > **Filter**

Mögliche Werte:

Erlauben
Ablehnen

Default-Wert:

Ablehnen

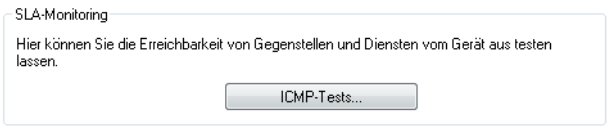
3.2 Unterstützung für DSCP-Tagging im SLA-Monitor

Ab LCOS 10.40 unterstützt Ihr Gerät DSCP-Tagging sowohl im Ping auf der Kommandozeile als auch im SLA-Monitor.

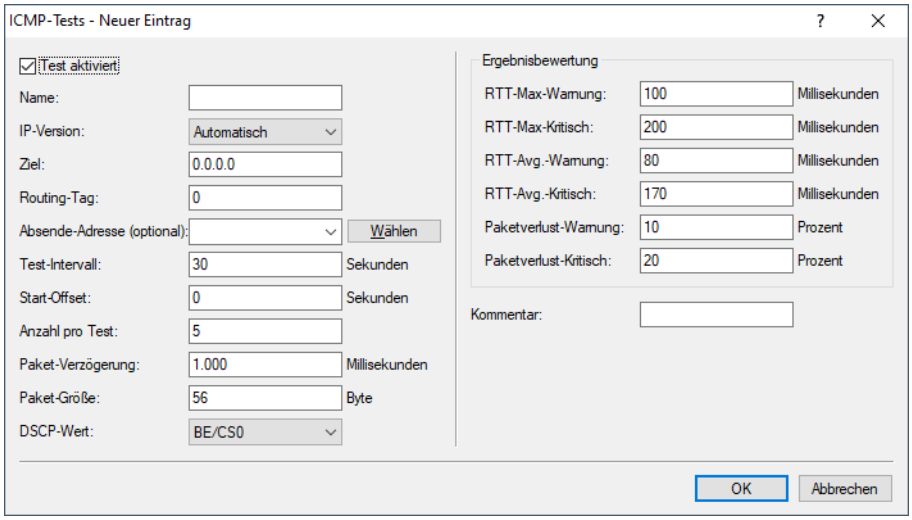
Auf der Kommandozeile nutzen Sie bei ping den neuen optionalen Parameter `[-p <DSCP>]`.

Parameter	Bedeutung
`[-p <dscp>]`	Verwende einen spezifischen DSCP-Wert für diesen Ping. DSCP (Differentiated Services Code Point) wird für QoS (Quality of Service) verwendet. Mögliche DSCP-Werte: BE/CS0, CS1, CS2, CS3, CS4, CS5, CS6, CS7, AF11, AF12, AF13, AF21, AF22, AF23, AF31, AF32, AF33, AF41, AF42, AF43, EF

Die Parameter zur Konfiguration des SLA-Monitors finden Sie bei LANconfig unter **Meldungen/Monitoring** > **Allgemein** im Abschnitt **SLA-Monitoring**.



Klicken Sie auf die Schaltfläche **ICMP-Tests**, um neue Abfragen hinzuzufügen und Richtwerte für die Verbindungstests zu definieren.



DSCP-Wert

Definiert den DSCP-Wert der ICMP-Nachricht. DSCP (Differentiated Services Code Point) wird für QoS (Quality of Service) verwendet. Mögliche Werte: BE/CS0, CS1, CS2, CS3, CS4, CS5, CS6, CS7, AF11, AF12, AF13, AF21, AF22, AF23, AF31, AF32, AF33, AF41, AF42, AF43, EF

3.2.1 Ergänzungen im Setup-Menü

DSCP

Definiert den DSCP-Wert der ICMP-Nachricht. DSCP (Differentiated Services Code Point) wird für QoS (Quality of Service) verwendet.

SNMP-ID:

2.45.1.22

Pfad Konsole:

Setup > **SLA-Monitor** > **ICMP**

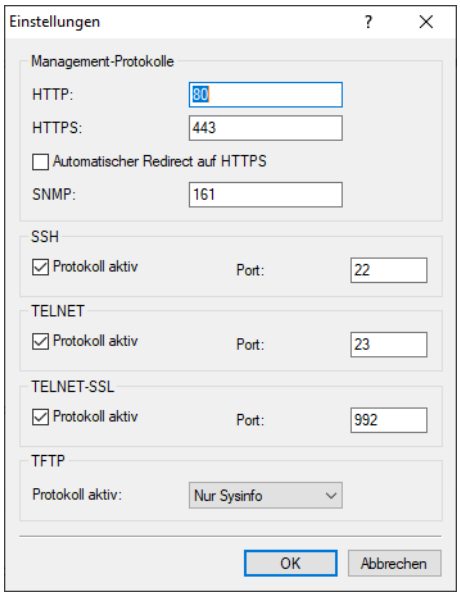
Mögliche Werte:

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

4 Sicherheit

4.1 TFTP nur noch für Sysinfo

Ab LCOS 10.40 unterstützt Ihr Gerät die Einstellung **Nur Sysinfo** für das Management-Protokoll TFTP. Sie finden die Einstellung unter **Management** > **Admin** > **Management-Protokolle**.



TFTP

Zugriff über TFTP. Das Trivial File Transfer Protocol (TFTP) ist eine einfachere Variante des File Transfer Protokolls (FTP). Im Gegensatz zu FTP ist mit TFTP lediglich das Lesen oder Schreiben von Dateien über UDP möglich. Die Einstellung **Nur Sysinfo** lässt den Port zwar offen, aber das Gerät antwortet nur auf einen Sysinfo-Request. Dadurch wird es in LANconfig angezeigt und insbesondere bei einer Suche nach Geräten gefunden. Es lässt sich aber keine Konfiguration zum Gerät hochladen. Da dieses Protokoll unverschlüsselt überträgt könnten sonst evtl. sensitive Daten im Netzwerk mitgelesen werden.

4.1.1 Ergänzungen im Setup-Menü

TFTP-aktiv

Das Trivial File Transfer Protocol (TFTP) ist eine einfachere Variante des File Transfer Protokolls (FTP). Im Gegensatz zu FTP ist mit TFTP lediglich das Lesen oder Schreiben von Dateien über UDP möglich.

Mit diesem Eintrag aktivieren oder deaktivieren Sie TFTP.

SNMP-ID:

2.11.36

Pfad Konsole:

Setup > **Config**

Mögliche Werte:

nein
ja
Sysinfo-only
Hier bleibt der Port offen und das Gerät antwortet auf einen Sysinfo-Request. Dadurch wird es in LANconfig angezeigt und insbesondere bei einer Suche nach Geräten gefunden. Es lässt sich aber keine Konfiguration zum Gerät hochladen. Da dieses Protokoll unverschlüsselt überträgt könnten sonst evtl. sensitive Daten im Netzwerk mitgelesen werden.

Default-Wert:

Sysinfo-only

4.2 Verschlüsselte Passwörter

Ab LCOS 10.40 können das Hauptgerätepasswort und die Passwörter weiterer Administratoren mittels der Hash-Verfahren SHA-256 und SHA-512 verschlüsselt gespeichert werden.

Aus Kompatibilitätsgründen wird in LCOS 10.40 im Default das Passwort weiterhin so gespeichert, das es im Klartext dargestellt werden kann. Mit der Option *2.11.89.1 Klartext-behalten* auf Seite 29 könnern Sie dies abschalten.

In zukünftigen LCOS-Versionen wird die Speicherung im Klartext abgeschaltet werden.

Protokolle wie LL2M und LCOSCap wurden angepasst, damit diese mit den verschlüsselten Passwörtern arbeiten können.

Wenn Sie Klartextpasswörter auf einem WLAN-Controller abschalten und gleichzeitig die Passwortsynchronisierung aktiviert haben, dann können nur Access Points verwaltet werden, welche ebenfalls mindestens mit LCOS 10.40 betrieben werden. Access Points mit einer LCOS-Version kleiner als 10.40 werden dann nicht mehr vom WLAN-Controller angenommen.

Wenn Sie Klartextpasswörter abschalten, so darf kein Firmware-Downgrade auf eine LCOS-Version kleiner als 10.40 durchgeführt werden, da ältere Versionen diese Funktion noch nicht unterstützen.

Wenn Sie Klartextpasswörter wieder aktivieren, so muss das Hauptgerätepasswort erneut über den Passwort-Ändern-Dialog eingegeben werden.

4.2.1 Ergänzungen im Setup-Menü

Passwoerter

Hier finden Sie Einstellungen zum Algorithmus, der zur Erzeugung des Passwort-Hashes verwendet wird.

SNMP-ID:

2.11.89

Pfad Konsole:

Setup > **Config**

Klartext-behalten

Ab LCOS 10.40 werden das Hauptgerätepasswort und die Passwörter der Administratoren über einen Algorithmus als Hashwert verschlüsselt abgelegt. Hier legen Sie fest, ob das Klartextpasswort ebenfalls behalten wird.

SNMP-ID:

2.11.89.1

Pfad Konsole:

Setup > **Config** > **Passwoerter**

Mögliche Werte:

ja

Das Hauptgerätepasswort und die Passwörter der Administratoren werden intern auch im Klartext abgelegt. Dadurch kann das Passwort weiterhin in LANconfig angezeigt werden und es können weiterhin mittels eines WLCs oder der WLC-Option Access Points mit einer LCOS-Version unter 10.40 verwaltet werden. In der CLI ist das Passwort nicht sichtbar.

Wenn die Möglichkeit erhalten werden soll, ein Firmware-Downgrade auf eine LCOS-Version vor 10.40 durchzuführen, dann muss diese Option gesetzt sein.

Erfolgt ein Firmware-Downgrade auf eine LCOS-Version vor 10.40, die keine verschlüsselten Passwörter unterstützt, dann wird das Passwort gelöscht. Ein Zugriff auf den Router ist aus dem LAN bzw. WLAN dann ohne Passwort möglich! Ein Zugriff aus dem WAN ist ohne Vergabe eines Passworts nicht möglich!

nein

Das Hauptgerätepasswort und die Passwörter der Administratoren werden intern nur in gehashter Form abgelegt.

Default-Wert:

ja

Krypto-Algorithmus

Der für die Verschlüsselung der Passwörter verwendete Algorithmus.

SNMP-ID:

2.11.89.2

Pfad Konsole:

Setup > **Config** > **Passwoerter**

Mögliche Werte:

SHA-256
SHA-512

Default-Wert:

SHA-512

Runden

Dieser Wert bestimmt, wie oft der Verschlüsselungsalgorithmus angewendet wird. Je mehr Runden durchgerechnet werden, um so höher ist die Widerstandsfähigkeit gegen Brute-Force-Angriffe. Gleichzeitig wird die eigentliche Arbeit mit den Passwörtern verlangsamt. Die Konfigurationsvorgabe von 5000 Runden bietet eine hohe Sicherheit bei gleichzeitig guter Arbeitsgeschwindigkeit.

SNMP-ID:

2.11.89.3

Pfad Konsole:

Setup > **Config** > **Passwoerter**

Mögliche Werte:

1000 … 999999999

Default-Wert:

5000

Verschluesseltes-Passwort

Verschlüsseltes Passwort für diesen Eintrag.

Dieses Passwort wird automatisch durch den in *2.11.89.2 Krypto-Algorithmus* auf Seite 29 vorgegebenen Algorithmus verschlüsselt.

SNMP-ID:

2.11.21.6

Pfad Konsole:

Setup > **Config** > **Admins**

Mögliche Werte:

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

Default-Wert:

leer

SNMP-Verschluesseltes-Passwort

Verschlüsseltes SNMP-Passwort für diesen Eintrag.

Dieses Passwort wird automatisch durch den in *2.11.89.2 Krypto-Algorithmus* auf Seite 29 vorgegebenen Algorithmus verschlüsselt.

SNMP-ID:

2.11.21.7

Pfad Konsole:

Setup > **Config** > **Admins**

Mögliche Werte:

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

Default-Wert:

leer

Krypto-Algorithmen

Hier können Sie die für LL2M-Verbindungen zu verwendenden Verschlüsselungsalgorithmen einschränken. Diese Einstellung gilt sowohl für den Server- als auch für den Clientmodus. Der Simple-Algorithmus verwendet das Klartext-Passwort als Basis für die Schlüsselableitung, während die beiden anderen Algorithmen ein verschlüsseltes Passwort als Basis verwenden, das entweder mit SHA-256 oder mit SHA-512 verschlüsselt ist. Simple muss aktiviert bleiben, wenn die Kommunikation mit LCOS-Versionen vor LCOS 10.40 gewünscht wird.

Beachten Sie, dass die Auswahl des Algorithmus mit dem verwendeten Passwort-Verschlüsselungsalgorithmus konsistent sein muss: Wenn zum Beispiel SHA-512 zur Verschlüsselung von Admin-Passwörtern verwendet wird (siehe *2.11.89.2 Krypto-Algorithmus* auf Seite 29) und Klartext-Passwörter nicht aufbewahrt werden (siehe *2.11.89.1 Klartext-behalten* auf Seite 29), darf SHA-512 an dieser Stelle nicht deaktiviert werden, da sonst das Gerät nicht über LL2M erreichbar ist.

SNMP-ID:

2.11.50.3

Pfad Konsole:

Setup > **Config** > **LL2M**

Mögliche Werte:

Simple
SHA-256
SHA-512

Default-Wert:

Simple

SHA-256

SHA-512

LCOSCap-Algorithmen

Hier können Sie die für LCOSCap-Verbindungen zu verwendenden Verschlüsselungsalgorithmen einschränken. Der Simple-Algorithmus verwendet das Klartext-Passwort als Basis für die Schlüsselableitung, während die beiden anderen Algorithmen ein verschlüsseltes Passwort als Basis verwenden, das entweder mit SHA-256 oder mit SHA-512 verschlüsselt ist. Simple muss aktiviert bleiben, wenn die Kommunikation mit LCOSCap-Versionen vor LCOS 10.40 gewünscht wird.

Beachten Sie, dass die Auswahl des Algorithmus mit dem verwendeten Passwort-Verschlüsselungsalgorithmus konsistent sein muss: Wenn zum Beispiel SHA-512 zur Verschlüsselung von Admin-Passwörtern verwendet wird (siehe *2.11.89.2 Krypto-Algorithmus* auf Seite 29) und Klartext-Passwörter nicht aufbewahrt werden (siehe *2.11.89.1 Klartext-behalten* auf Seite 29), darf SHA-512 an dieser Stelle nicht deaktiviert werden, da sonst das Gerät nicht über LL2M erreichbar ist.

SNMP-ID:

2.63.4

Pfad Konsole:

Setup > **Paket-Capture**

Mögliche Werte:

Simple
SHA-256
SHA-512

Default-Wert:

Simple

SHA-256

SHA-512

Klartext-behalten

Ab LCOS 10.40 werden die Passwörter der SNMP-Benutzer über einen Algorithmus als Hashwert verschlüsselt abgelegt. Hier legen Sie fest, ob das Klartextpasswort ebenfalls behalten wird.

SNMP-ID:

2.9.44

Pfad Konsole:

Setup > **Config**

Mögliche Werte:

ja

Die Passwörter der SNMP-Benutzer werden intern auch im Klartext abgelegt.

Wenn die Möglichkeit erhalten werden soll, ein Firmware-Downgrade auf eine LCOS-Version vor 10.40 durchzuführen, dann muss diese Option gesetzt sein.

nein

Die Passwörter der SNMP-Benutzer werden intern nur in gehashter Form abgelegt.

Default-Wert:

ja

Authentication-Key

Verschlüsseltes Authentifizierungs-Passwort für diesen Eintrag.

Dieses Passwort wird automatisch durch den in *2.11.89.2 Krypto-Algorithmus* auf Seite 29 vorgegebenen Algorithmus verschlüsselt.

SNMP-ID:

2.9.32.14

Pfad Konsole:

Setup > **SNMP** > **Benutzer**

Mögliche Werte:

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

Default-Wert:

leer

Verschluesselungs-Schluessel

Verschlüsseltes Verschlüsselungs-Passwort für diesen Eintrag.

Dieses Passwort wird automatisch durch den in *2.11.89.2 Krypto-Algorithmus* auf Seite 29 vorgegebenen Algorithmus verschlüsselt.

SNMP-ID:

2.9.32.15

Pfad Konsole:

Setup > **SNMP** > **Benutzer**

Mögliche Werte:

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

Default-Wert:

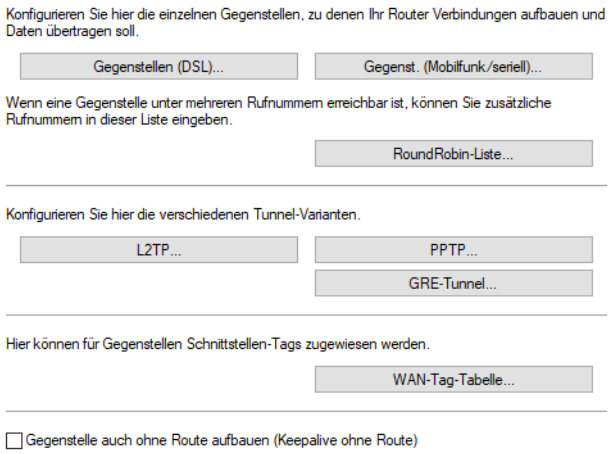
leer

5 Routing und WAN-Verbindungen

5.1 Gegenstellen auch ohne Route aufbauen

Ab LCOS 10.40 unterstützt Ihr Gerät den Aufbau von Gegenstellen auch ohne bestehende Route.

Die entsprechende Option finden Sie unter **Kommunikation** > **Gegenstellen**.



Gegenstelle auch ohne Route aufbauen (Keepalive ohne Route)

Definiert, ob eine Gegenstelle, z. B. ein VPN-Tunnel oder eine Internetverbindung, auch ohne Route aufgebaut werden soll. Der Aufbau der Gegenstelle ohne explizite Route in der Routing-Tabelle ist inbesondere dann erforderlich, wenn die Gegenseite die Routen übermittelt, z. B. durch DHCP (Classless-Static-Route-Option) oder ein dynamisches Routing-Protokoll.

5.1.1 Ergänzungen im Setup-Menü

Keepalive-ohne-Route

Definiert, ob eine Gegenstelle, z. B. ein VPN-Tunnel oder eine Internetverbindung, auch ohne Route aufgebaut werden soll. Der Aufbau der Gegenstelle ohne explizite Route in der Routing-Tabelle ist inbesondere dann erforderlich, wenn die Gegenseite die Routen übermittelt, z. B. durch DHCP (Classless-Static-Route-Option) oder ein dynamisches Routing-Protokoll.

SNMP-ID:

2.2.15

Pfad Konsole:

Setup > **WAN**

Mögliche Werte:

Nein

Gegenstellen werden erst aufgebaut, wenn eine Route existiert. Dies entspricht dem Standardverhalten bis LCOS 10.40.

Ja

Ab LCOS 10.40 kann über diese Option der Aufbau von Gegenstellen bereits ohne existierende Route erfolgen.

Default-Wert:

Nein

5.2 Feature „Zeitgesteuerte Default-Route“ entfernt

Ab LCOS 10.40 unterstützt Ihr Gerät das Feature „Zeitgesteuerte Default-Route“ nicht mehr. Dieses stammt noch aus der Zeit, als der Router ein reiner ISDN-Router war. Die entsprechenden Optionen in LANconfig unter **IP-Router** > **Routing** > **Zeitsteuerung** wurden entfernt. Ebenso auf der Konsole die Tabelle Default-Zeit-Liste und der Eintrag Nutzung-Default-Listen unter **Setup** > **IP-Router**.

5.3 Backup über die Routing-Tabelle

Ab LCOS 10.40 unterstützt Ihr Gerät eine konfigurierbare administrative Distanz bei statischen Routen und ermöglicht so einen Backup-Mechanismus über die Routing-Tabelle.

5.3.1 Administrative Distanz

Über die administrative Distanz ist es möglich mehrere gleiche statische Routen bzw. Präfixe zu unterschiedlichen Gegenstellen zu konfigurieren. Die Route mit der geringsten administrativen Distanz ist die bevorzugt aktive Route. Über diesen Mechanismus lassen sich beispielsweise einfache Backup-Mechanismen konfigurieren.

Die Manipulation der administrativen Distanz für Routen von dynamischen Routen erfolgt bei dem jeweiligen dynamischen Routing-Protokoll.

Beispiel 1: Es sollen zwei VPN-Tunnel mit Route 192.168.2.0/24 konfiguriert werden. Der zweite VPN-Tunnel soll als „Always-On“ Backup für den ersten VPN-Tunnel konfiguriert werden.

Für den ersten Tunnel wird das Präfix 192.168.2.0/24 auf die Gegenstellen VPN-1 mit einer administrativen Distanz von 10 eingerichtet, für den zweiten Tunnel wird das Präfix 192.168.2.0/24 auf die Gegenstellen VPN-2 mit einer administrativen Distanz von 20 eingerichtet. Beide VPN-Tunnel werden aufgebaut, aber nur für den ersten VPN-Tunnel wird die Route aktiv, da diese die bessere / niedrigere administrative Distanz hat. Ist der erste VPN-Tunnel nicht verbunden, so setzt das Betriebssystem diese Route auf die administrative Distanz von 255 (Interface Down), womit die Route über den zweiten Tunnel automatisch aktiv wird.

Beispiel 2: Es existiert eine statische Route für 192.168.1.0/24 zur Gegenstellen VPN-Tunnel1. Wird das gleiche Präfix 192.168.1.0/24 nun über BGP empfangen, so hat die statische Route im Default eine bessere / niedrigere administrative Distanz, so dass diese verwendet wird und nicht die Route über BGP.

Setzt man nun die administrative Distanz der statischen Route auf den Wert 210, so wird die über BGP gelernte Route bevorzugt und aktiv, da (e)BGP eine administrative Distanz von 20 bzw. 200 (iBGP) hat. Somit dient die statische Route als Backup für die dynamische BGP-Route.

Diese Funktion ersetzt nicht die Funktion der Backup-Tabelle, sondern stellt eine andere Art von „Backup" zur Verfügung. Bei Verwendung der Backup-Tabelle ist immer nur eine Verbindung aktiv. Im Backup-Fall wird versucht die Backup-Verbindung zu aktivieren. Wenn die Backup-Verbindung aktiv ist, wird versucht, im Hintergrund die primäre Verbindung wieder aufzubauen und im Erfolgsfall wieder umzuschalten. Die Backup-Strategie über die administrative Distanz geht davon aus, dass alle Gegenstellen immer aufgebaut sind. Dies ist in bestimmten Szenarien, z. B. Backup über Mobilfunk nicht immer gewünscht und die Backup-Tabelle ist dann die bevorzugte Wahl.

Die Backup-Funktion über die Backuptabelle und ein Backup über administrative Distanzen schließen sich gegenseitig aus.

Das Kommando `show ipv4-static-routes` bzw. `show ipv6-static-routes` zeigt alle aktiven und inaktiven statischen Routen an. Die gültigen administrativen Distanzen für die entsprechenden Routen-Quellen sind auf der Konsole über das Kommando `show admin-distance` abrufbar.

Die wichtigsten administrativen Distanzen sind:

Tabelle 1: Administrative Distanzen

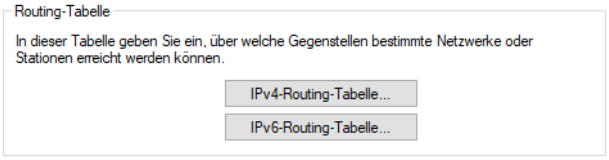
Art der Route	Administrative Distanz
Statische Routen	5
VPN	15
eBGP	20
OSPF	110
RIP	120
iBGP	200
LISP	240
Interface Down	255

Statische Routen sind definiert als Routen, die in der IPv4- bzw. IPv6-Routing-Tabelle vom Benutzer konfiguriert werden.

VPN-Routen sind definiert als Routen, die vom VPN automatische in die Routing-Tabelle eingetragen werden, z. B. durch IKEv2-Routing.

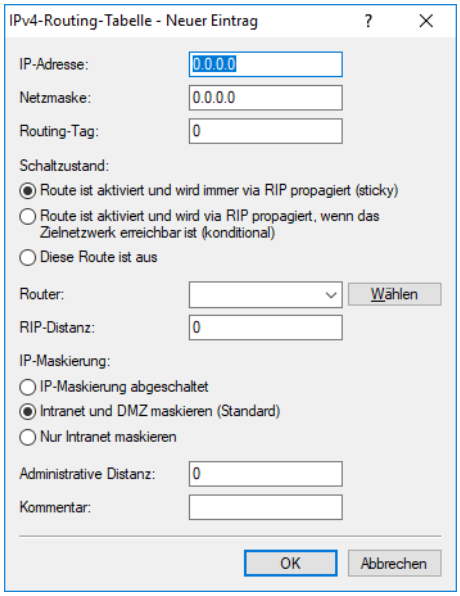
5.3.2 Routing-Tabellen für IPv4 / IPv6

Statische Routing-Einträge werden für IPv4 und IPv6 in getrennten Tabellen konfiguriert. Die Tabellen finden Sie in LANconfig unter **IP-Router** > **Routing** > **Routing-Tabelle**.



IPv4

Die Routing-Tabelle für das statische Routing von IPv4-Paketen finden Sie unter **IP-Router** > **Routing** > **Routing-Tabelle** > **IPv4-Routing-Tabelle**.



Router

An diese Gegenstelle bzw. IPv4-Adresse überträgt der Router die zur IP-Adresse und Netzmaske passenden Datenpakete.

› Ab LCOS 10.40 kann die Syntax 'IP-Adresse@Tag' verwendet werden, falls der Router bzw. Next-Hop in einem anderem Routing-Kontext aufgelöst werden soll.

Dies ist beispielsweise der Fall, wenn eine statische Route mit einem Tag angelegt wurde, bei welcher dieses Tag nur durch eine Firewallregel zugewiesen werden kann.

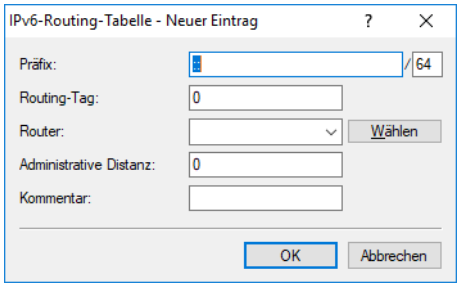
Beispiel: Soll der Router 192.168.1.1 im Routing Kontext 1 aufgelöst werden, so lautet die Eingabe '192.168.1.1@1'.

Administrative Distanz

Administrative Distanz für diese Route. Default ist 0 (wird automatisch vom Betriebssystem vergeben). Über den Parameter administrative Distanz ist es möglich mehrere gleiche Routen bzw. Präfixe zu unterschiedlichen Gegenstellen zu konfigurieren. Die Route mit der geringsten administrativen Distanz ist die bevorzugt aktive Route. Siehe *Administrative Distanz* auf Seite 36.

IPv6

Die Routing-Tabelle für das statische Routing von IPv6-Paketen finden Sie unter **IP-Router** > **Routing** > **Routing-Tabelle** > **IPv6-Routing-Tabelle**.



Router

Wählen Sie hier das Ziel bzw. die Gegenstelle für diese Route aus.

Ab LCOS 10.40 kann die Syntax 'IP-Adresse@Tag' verwendet werden, falls der Router bzw. Next-Hop in einem anderem Routing-Kontext aufgelöst werden soll.

Dies ist beispielsweise der Fall, wenn eine statische Route mit einem Tag angelegt wurde, bei welcher dieses Tag nur durch eine Firewallregel zugewiesen werden kann.

Beispiel: Soll der Router 2001:db8::1 im Routing Kontext 1 aufgelöst werden, so lautet die Eingabe '2001:db8::1@1'.

Administrative Distanz

Definieren Sie hier die administrative Distanz dieser Route. Über diesen Parameter ist es möglich mehrere gleiche Routen bzw. Präfixe zu unterschiedlichen Gegenstellen zu konfigurieren. Die Route mit der geringsten administrativen Distanz ist die bevorzugt aktive Route. Der Default ist 0, d. h. der Wert wird automatisch vom Betriebssystem vergeben. Siehe *Administrative Distanz* auf Seite 36.

5.3.3 Ergänzungen im Setup-Menü

Admin-Distanz

Administrative Distanz für diese Route. Default ist 0 (wird automatisch vom Betriebssystem vergeben). Über den Parameter administrative Distanz ist es möglich mehrere gleiche Routen bzw. Präfixe zu unterschiedlichen Gegenstellen zu konfigurieren. Die Route mit der geringsten administrativen Distanz ist die bevorzugt aktive Route.

SNMP-ID:

2.8.2.9

Pfad Konsole:

Setup > **IP-Router** > **IP-Routing-Tabelle**

Mögliche Werte:

0 … 255

Default-Wert:

0

Admin-Distanz

Administrative Distanz dieser Route. Über diesen Parameter ist es möglich mehrere gleiche Routen bzw. Präfixe zu unterschiedlichen Gegenstellen zu konfigurieren. Die Route mit der geringsten administrativen Distanz ist die bevorzugt aktive Route. Der Default ist 0, d. h. der Wert wird automatisch vom Betriebssystem vergeben.

SNMP-ID:

2.70.12.1.5

Pfad Konsole:

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

Mögliche Werte:

0 … 255

Default-Wert:

0

5.4 Load-Balancing

5.4.1 Dynamisches Load-Balancing

Load-Balancer aus RADIUS-Konfiguration

Ab LCOS 10.40 unterstützt Ihr Gerät neben der bereits vorhandenen Möglichkeit, einen Load-Balancer über die Konfigurationstabelle des Load-Balancers zu konfigurieren, auch die Möglichkeit, einen Load-Balancer aus übermittelten RADIUS-Attributen für IKEv2 VPN-Tunnel zu erzeugen.

In großen VPN-Szenarien werden zentralseitige Konfigurationen nicht durch Konfigurationseinträge aller notwendigen Parameter eines VPN-Tunnels im Gerät selbst abgelegt, sondern auf einen oder mehrere zentrale RADIUS-Server ausgelagert. Dies dient der besseren Skalierbarkeit und Administration. Sollen in diesen Szenarien auf den zentralseitigen VPN-Gateway mehrere eingehende IKEv2-VPN-Tunnel zu einem Load Blancer zusammengefasst werden, so kann dies über zusätzliche RADIUS-Attribute realisiert werden.

Die Bündel-Gegenstellen eines dynamischen Load-Balancers sind IKEv2-VPN-Clients, die RADIUS-Authorization nutzen. Dabei wird ein VPN-Client dann in einem dynamischen Load-Balancer-Verbund aufgenommen, wenn die RADIUS-Antwort ein entsprechendes RADIUS-Attribut (LCS-Load-Balancer) enthält. Dieses Attribut gibt den Namen des Load-Balancer-Verbundes an und entscheidet zusätzlich darüber, ob Client-Binding aktiv sein soll.

Wenn eine solche VPN-Verbindung abbricht, wird der Client wieder aus seinem Load-Balancer-Verbund entfernt. Ein erneuter Verbindungsaufbau muss durch den Client erfolgen.

Ein dynamischer Load-Balancer-Verbund darf nicht denselben Namen wie ein statisch konfigurierter Verbund haben, man kann also statische und dynamische Clients nicht im selben Load-Balancer vermischen.

Für die Konfiguration über einen RADIUS-Server wird die Syntax der Standard-Attribute „Framed-Route“ und „Framed-IPv6-Route“ erweitert, damit dynamisch Routen übermittelt werden können, die auf einen Load-Balancer zeigen. Routen des IKEv2-Routing zeigen automatisch auf den Load-Balancer statt auf das Einwahlinterface, wenn das Attribut „LCS-Load-Balancer“ verwendet wird.

Das Feature wird auch im Zusammenhang mit IKEv2-Routing unterstützt. Die Route auf dem VPN-Gateway wird dann dynamisch von der Gegenseite übermittelt statt die Route per Framed-Route-Attribut vom RADIUS-Server zu empfangen. In diesem Fall muss lediglich das Attribut „LCS-Load-Balancer“ vom RADIUS-Server übermittelt werden.

Tabelle 2: RADIUS-Attribute

ID	Bezeichnung	Bedeutung
22	Framed-Route	IPv4-Routen, die in Richtung des Clients (Next-Hop-Client) auf dem VPN-Gateway in der Routing-Tabelle eingetragen werden sollen. Format (String): <Präfix> [ifc=<Zielinterface>] [rtg_tag=<Routing-Tag>] [admin_distance=<Distanz>] **<Präfix>** IPv4-Adresse + '/' + Präfixlänge oder Netzmaske **ifc=<Zielinterface>** Name des IP-Interfaces oder eines Load-Balancers, auf den die Route zeigen soll, oder „#Ifc". Wenn kein Zielinterface angegeben ist oder es „#Ifc" lautet, dann zeigt die Route auf das VPN-Interface für den betreffenden Einwahlclient. Der Interfacename kann bis zu 16 Zeichen enthalten. **rtg_tag=<Routing-Tag>** Routing-Tag für die Route. Wenn es nicht angegeben wird, bekommt die Route das Tag des Einwahlinterfaces. **admin_distance=<Distanz>** Administrative Distanz der Route als Zahl von 0 bis 255. Wenn sie nicht angegeben wird, bekommt die Route die standardmäßige Distanz für VPN-Routen.
99	Framed-IPv6-Route	IPv6-Routen, die in Richtung des Clients (Next-Hop-Client) auf dem VPN-Gateway in der Routing-Tabelle eingetragen werden sollen. Format (String): <Präfix> [ifc=<Zielinterface>] [rtg_tag=<Routing-Tag>] [admin_distance=<Distanz>] **<Präfix>** IPv6-Adresse + '/' + Präfixlänge **ifc=<Zielinterface>** Name des IP-Interfaces oder eines Load-Balancers, auf den die Route zeigen soll, oder „#Ifc". Wenn kein Zielinterface angegeben ist oder es „#Ifc" lautet, dann zeigt die Route auf das VPN-Interface für den betreffenden Einwahlclient. Der Interfacename kann bis zu 16 Zeichen enthalten. **rtg_tag=<Routing-Tag>** Routing-Tag für die Route. Wenn es nicht angegeben wird, bekommt die Route das Tag des Einwahlinterfaces.

ID	Bezeichnung	Bedeutung
		admin_distance=<Distanz> Administrative Distanz der Route als Zahl von 0 bis 255. Wenn sie nicht angegeben wird, bekommt die Route die standardmäßige Distanz für VPN-Routen.
LANCOM 28	LCS-Load-Balancer	Format (String): <Load-Balancer-Name> [client_binding={no|yes}] Der <Load-Balancer-Name> kann bis zu 16 Zeichen lang sein und gibt eine entsprechende Load-Balancing-Gegenstelle auf den LANCOM Routern an. Diese Gegenstelle wird für das dynamische IKEv2-VPN-Load-Balancing verwendet und darf daher nicht unter **IP-Router** > **Load Balancing** bereits für statisches Load-Balancing verwendet werden. Die Option „client_binding“ schaltet das Client Binding ein oder aus. Ohne diese Angabe ist Client Binding aus. Der erste sich verbindende IKEv2-VPN-Client gibt diese Einstellung vor. Danach erfolgende andere Einstellungen für das Client Binding in Verbindung mit dieser Load-Balancing-Gegenstelle werden ignoriert.

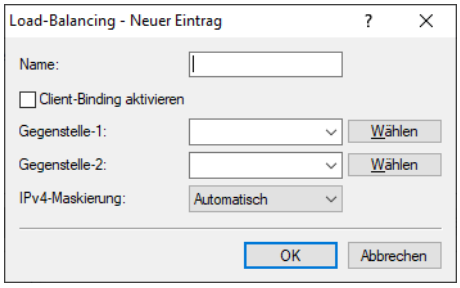
Beispiel: RADIUS-Attribute für einen einfachen Loadbalancer aus IKEv2-VPN-Tunneln auf der Zentrale

```
LCS-Load-Balancer=LB1
Framed-Route=192.168.45.0/24 ifc=LB1;
```

5.4.2 Übernahme der Maskierungseinstellung der Load-Balancer-Verbindung

Ab LCOS 10.40 unterstützt Ihr Gerät die Konfiguration der Maskierungseinstellung der Load-Balancer-Verbindung, sodass diese für alle einzelnen Kanäle übernommen wird.

In LANconfig finden Sie die Einstellung unter **IP-Router** > **Routing** > **Load-Balancing**.



IPv4-Maskierung

Stellen Sie hier die IPv4-Maskierung des Load-Balancers ein. Mögliche Werte:

Automatisch

Übernimmt die Maskierungsoption jeder einzelnen Leitung aus der Routing-Tabelle.

Ein

Aktiviert NAT auf allen Gegenstellen im Loadbalancer.

Nein

Deaktiviert NAT auf allen Gegenstellen im Loadbalancer.

Nur Intranet

Aktiviert NAT für Netze vom Typ INTRANET. Die DMZ wird nicht maskiert.

Ergänzungen im Setup-Menü

IPv4-Masq.

Stellen Sie hier die IPv4-Maskierung des Load-Balancers ein.

SNMP-ID:

2.8.20.2.11

Pfad Konsole:

Setup > **IP-Router** > **Load-Balancer** > **Buendel-Gegenstellen**

Mögliche Werte:

auto

Übernimmt die Maskierungsoption jeder einzelnen Leitung aus der Routing-Tabelle.

Nein

Deaktiviert NAT auf allen Gegenstellen im Load-Balancer.

Ein

Aktiviert NAT auf allen Gegenstellen im Load-Balancer

intranet

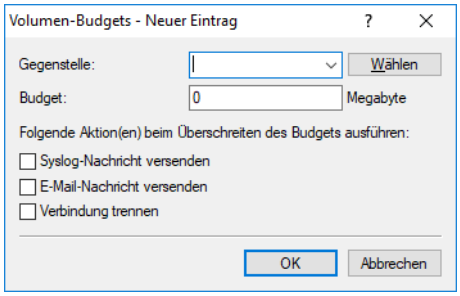
Aktiviert NAT für Netze vom Typ INTRANET. Die DMZ wird nicht maskiert.

Default-Wert:

auto

5.5 Weitere Benachrichtigung bei Volumenbudget

Ab LCOS 10.40 sendet Ihr Gerät nicht nur bei 100% des Volumenbudgets eine Benachrichtigung, sondern eine weitere Benachrichtigung über Syslog und / oder E-Mail, wenn der Schwellenwert von 80% des unter **Management** > **Budget** > **Budget-Überwachung** > **Volumen-Budgets** einstellbaren Volumenbudgets erreicht wird.



5.6 PPP-Bandbreite anzeigen

Ab LCOS 10.40 unterstützt Ihr Gerät die automatischen Übernahme der tatsächlichen Down- und Upstream-Raten bei einem Login aus der PAP-ACK-Nachricht. Bestimmte Provider übermitteln nach erfolgreichem PPP-Login (PPP PAP-ACK) die tatsächlich zur Verfügung stehende Layer 3-Bandbreite. Diese ist dann relevant, wenn die synchronisierte DSL-Bandbreite von der Bandbreite des gebuchten Internettarifs abweicht oder wenn die tatsächliche Bandbreite wie bei Glasfaser- bzw. Ethernet-basierten Anschlüssen nicht bekannt ist. In diesem Fall wird das Minimum zwischen übermittelter Bandbreite und DSL-Information als QoS-Wert verwendet. Mit diesen Informationen kann dann Quality-of Service effizient betrieben werden.

Dazu wird eine Tabelle verwendet, welche zu einer Login-Kennung eines Providers jeweils einen passenden Parameter-String mit Platzhaltern für die Raten enthält. Bei einem Login wird dann geprüft, ob der Provider in der Tabelle enthalten ist und danach die entsprechenden Raten ermittelt. Falls kein Provider-String passt, dann werden alle definierten Formate nacheinander durchgegangen, ob eines übereinstimmt. Der erste Treffer wird dann verwendet und die Up- / Downstream-Raten entsprechend übernommen.

5.6.1 Ergänzungen im Setup-Menü

Provider-Spezifika

Bestimmte Provider übermitteln nach erfolgreichem PPP-Login (PPP PAP-ACK) die tatsächlich zur Verfügung stehende Layer 3-Bandbreite. Diese ist dann relevant, wenn die synchronisierte DSL-Bandbreite von der Bandbreite des gebuchten Internettarifs abweicht oder wenn die tatsächliche Bandbreite wie bei Glasfaser- bzw. Ethernet-basierten Anschlüssen nicht bekannt ist. In diesem Fall wird das Minimum zwischen übermittelter Bandbreite und DSL-Information als QoS-Wert verwendet. Mit diesen Informationen kann dann Quality-of Service effizient betrieben werden.

Diese Tabelle enthält dazu Login-Kennungen mit Platzhaltern, um z. B. bei einem Login aus der PAP-ACK-Nachricht die tatsächlichen Up- und Downstream-Geschwindigkeiten zu extrahieren.

Wird in der Tabelle keine passende Login-Kennung gefunden, dann werden alle in der Tabelle definierten Parameter-Strings geprüft, ob einer übereinstimmt. Der erste Treffer wird dann verwendet und die Up- / Download-Raten entsprechend übernommen.

Die Anzeige der ermittelten Werte erfolgt im Status-Menü unter **Status** > **WAN** > **Connection-Bandwidth**. Dort wird die per DSL synchronisierte Bandbreite sowie die vom Provider übertragene Bandbreite angezeigt, sowie die resultierende Bandbreite, die vom QoS dann verwendet wird.

SNMP-ID:

2.2.62

Pfad Konsole:

Setup > **WAN**

Provider

Provider-Login-Kennung, die Wildcards enthalten darf.

SNMP-ID:

2.2.62.1

Pfad Konsole:

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

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9]/?.-;:@&=$_+!*'(),%`

Default-Wert:

leer

Parameter-Format

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

- {txrate} – Upstream-Rate
- {rxrate} – Downstream-Rate

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

SNMP-ID:

2.2.62.2

Pfad Konsole:

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

Mögliche Werte:

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

Default-Wert:

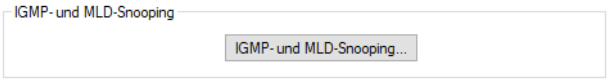
leer

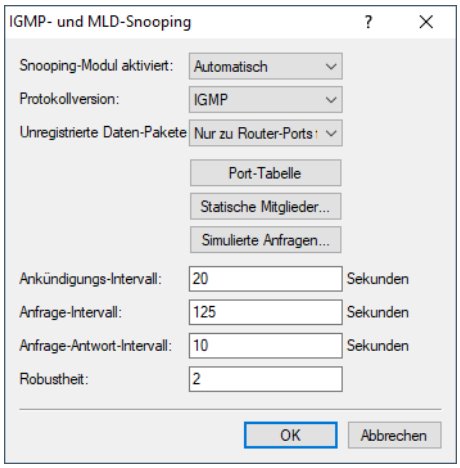
5.7 MLD-Snooping

Ab LCOS 10.40 unterstützen alle Geräte mit LAN-Bridge MLD-Snooping (Multicast Listener Discovery). Dieses funktioniert für IPv6 analog zum IGMP-Snooping für IPv4.

5.7.1 Konfiguration

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





Snooping-Modul aktiviert

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

Mögliche Werte:

- Ein
- Aus
- Automatisch

Default:

- Automatisch

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

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

Protokollversion

Geben Sie die unterstützten Protokolle an: IGMP, MLD oder beide.

Unregistrierte Datenpakete

Diese Option definiert die Verarbeitung von Multicast-Paketen mit Ziel-Adressen außerhalb des reservierten Adress-Bereiches „224.0.0.x" bzw. bzw. bei IPv6 „FF02::1", für die weder dynamisch gelernte noch statisch konfigurierte Mitgliedschaften vorhanden sind.

Mögliche Werte:

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

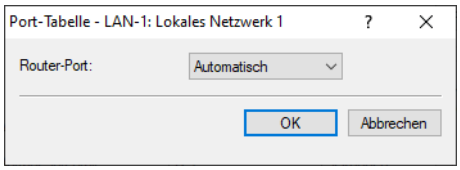
- Verwerfen: Verwirft diese Pakete.

Default:

- Nur-Router-Ports

Port-Tabelle

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



Port

Auf diesen Port beziehen sich die Einstellungen.

Mögliche Werte:

- Auswahl aus der Liste der im Gerät verfügbaren Ports.

Default:

- N/A

Router-Port

Diese Option definiert das Verhalten des Ports.

Mögliche Werte:

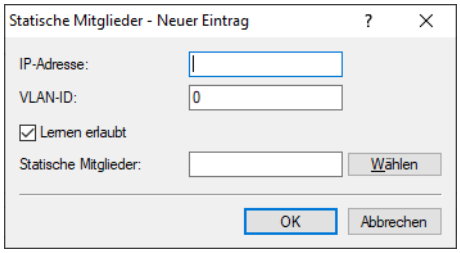
- Ja: Dieser Port verhält sich immer wie ein Router-Port, unabhängig von den IGMP-Anfragen oder Router-Meldungen, die die Bridge auf diesem Port evtl. empfängt.
- Nein: Dieser Port verhält sich nie wie ein Router-Port, unabhängig von den IGMP-Anfragen oder Router-Meldungen, die die Bridge auf diesem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

Default:

- Automatisch

Statische Mitglieder

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



IP-Adresse

Die IP-Adresse der manuell definierten Multicast-Gruppe.

Mögliche Werte:

- Gültige IP-Multicast-Adresse.

VLAN-ID

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

Mögliche Werte:

- 0 bis 4096.

Default:

- 0

Besondere Werte:

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

Lernen erlaubt

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

Statische Mitglieder

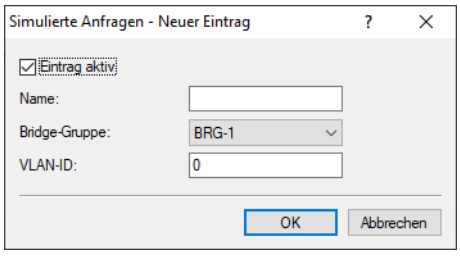
An diese Ports stellt die Bridge die Pakete mit der entsprechenden IP-Multicast-Adresse immer zu, unabhängig von empfangenen Join-Nachrichten.

Mögliche Werte:

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

Simulierte Anfragen

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



Eintrag aktiv

Aktiviert oder deaktiviert die Querier-Instanz.

Name

Name der Querier-Instanz.

Mögliche Werte:

- 8 alphanumerische Zeichen.

Bridge-Gruppe

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

Mögliche Werte:

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

Default:

- BRG-1

Besondere Werte:

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

VLAN-ID

Schränkt die Querier-Instanz auf ein bestimmtes VLAN ein.

Mögliche Werte:

- 0 bis 4096

Default:

- 0

Besondere Werte:

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

Ankündigungs-Intervall

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

Mögliche Werte:

- 4 bis 180 Sekunden

Default:

- 20 Sekunden

Anfrage-Intervall

Intervall in Sekunden, in dem ein Multicast-fähiger Router (oder ein simulierter Querier) IGMP- / MLD-Anfragen an die Multicast-Adresse `224.0.0.1` bzw. bei IPv6 „FF02::1" schickt und damit Rückmeldungen der Stationen über die Mitgliedschaft in Multicast-Gruppen auslöst. Diese regelmäßigen Abfragen beeinflussen den Zeitpunkt, nach dem die Bridge die Mitgliedschaft in bestimmten Multicast-Gruppen „altern" lässt und löscht.

- Ein Querier sendet nach der Anfangsphase IGMP- / MLD-Anfragen in diesem Intervall.

- Ein Querier kehrt zurück in den Querier-Status nach einer Zeit von „Robustheit*Anfrage-Intervall+(Anfrage-Antwort-Intervall/2)“.
- Ein Router-Port verliert seine Eigenschaften nach einer Alterungszeit von „Robustheit*Anfrage-Intervall+(Anfrage-Antwort-Intervall/2)“.

Mögliche Werte:

- Zahl aus 10 Ziffern größer als 0.

Default:

- 125

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

Anfrage-Antwort-Intervall

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

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

Mögliche Werte:

- Zahl aus 10 Ziffern größer als 0.

Default:

- 10

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

Robustheit

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

Mögliche Werte:

- Zahl aus 10 Ziffern größer als 0.

Default:

- 2

5.7.2 Ergänzungen im Setup-Menü

IGMP-Snooping

Dieses Menü enthält die Konfigurationsmöglichkeiten für das IGMP- / MLD-Snooping.

SNMP-ID:

2.20.30

Pfad Konsole:

Setup > LAN-Bridge

In-Betrieb

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

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

SNMP-ID:

2.20.30.1

Pfad Konsole:

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

Mögliche Werte:

nein
ja
Auto

Default-Wert:

Auto

Port-Einstellungen

In dieser Tabelle werden die Port-bezogenen Einstellungen für IGMP / MLD-Snooping vorgenommen.

SNMP-ID:

2.20.30.2

Pfad Konsole:

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

Router-Port

Diese Option definiert das Verhalten des Ports.

SNMP-ID:

2.20.30.2.2

Pfad Konsole:

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

Mögliche Werte:

nein

Dieser Port verhält sich nie wie ein Router-Port, unabhängig von den IGMP / MLD-Anfragen oder Router-Meldungen, die auf diesem Port evtl. empfangen werden.

ja

Dieser Port verhält sich immer wie ein Router-Port, unabhängig von den IGMP / MLD-Anfragen oder Router-Meldungen, die auf diesem Port evtl. empfangen werden.

Auto

Dieser Port verhält sich wie ein Router-Port, wenn eine IGMP / MLD-Anfragen oder Router-Meldung empfangen wurde. Der Port verliert diese Eigenschaft wieder, wenn für die Dauer von „Robustheit*Anfrage-Intervall+(Anfrage-Antwort-Intervall/2)" keine entsprechenden Pakete empfangen wurden.

Default-Wert:

Auto

Unregistrierte-Datenpakete-Behandlung

Diese Option definiert die Verarbeitung von Multicast-Paketen mit Ziel-Adressen außerhalb der reservierten Adress-Bereiche „224.0.0.x" und „FF02::1", für die weder dynamisch gelernte noch statisch konfigurierte Mitgliedschaften vorhanden sind.

SNMP-ID:

2.20.30.3

Pfad Konsole:

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

Mögliche Werte:

Nur-Router-Ports

Sendet diese Pakete an alle Router-Ports.

Fluten

Sendet diese Pakete an alle Ports.

Verwerfen

Verwirft diese Pakete.

Default-Wert:

Nur-Router-Ports

Simulierte-Anfrager

Diese Tabelle enthält alle im Gerät definierten simulierten Querier. Diese Einheiten werden eingesetzt, wenn kein Multicast-Router im Netzwerk vorhanden ist, aber dennoch die Funktionen des IGMP- / MLD-Snooping benötigt werden.

Um die Querier auf bestimmte Bridge-Gruppen oder VLANs einzuschränken, können mehrere unabhängige Querier definiert werden, welche dann die entsprechenden VLAN-IDs nutzen.

SNMP-ID:

2.20.30.4

Pfad Konsole:

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

Bridge-Gruppe

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

SNMP-ID:

2.20.30.4.3

Pfad Konsole:

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

Mögliche Werte:

BRG-1
BRG-2
BRG-3
BRG-4
BRG-5
BRG-6
BRG-7
BRG-8
keine

Mit dieser Einstellung werden die IGMP-Anfragen auf allen Brigde-Gruppen ausgegeben.

Default-Wert:

BRG-1

VLAN-Id

Schränkt die Querier-Instanz auf ein bestimmtes VLAN ein.

SNMP-ID:

2.20.30.4.4

Pfad Konsole:

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

Mögliche Werte:

0 … 4096

Default-Wert:

0

Besondere Werte:

0

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

Protokoll

Schränkt die Querier-Instanz auf ein bestimmtes Protokoll ein.

SNMP-ID:

2.20.30.4.6

Pfad Konsole:

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

Mögliche Werte:

IGMP
MLD

Anfrage-Intervall

Intervall in Sekunden, in dem ein Multicast-fähiger Router (oder ein simulierter Querier) IGMP- / MLD-Anfragen an die Multicast-Adresse 224.0.0.1 bzw. FF02::1 schickt und damit Rückmeldungen der Stationen über die Mitgliedschaft in Multicast-Gruppen auslöst. Diese regelmäßigen Abfragen beeinflussen den Zeitpunkt, nach dem die Mitgliedschaft in bestimmten Multicast-Gruppen „altern" und gelöscht werden.

Ein Querier sendet nach der Anfangsphase IGMP- / MLD-Anfragen in diesem Intervall.

Ein Querier kehrt zurück in den Querier-Status nach einer Zeit von „Robustheit*Anfrage-Intervall+(Anfrage-Antwort-Intervall/2)".

Ein Router-Port verliert seine Eigenschaften nach einer Alterungszeit von „Robustheit*Anfrage-Intervall+(Anfrage-Antwort-Intervall/2)".

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

SNMP-ID:

2.20.30.5

Pfad Konsole:

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

Mögliche Werte:

max. 10 Zeichen aus `[1-9]`

Default-Wert:

125

Anfrage-Antwort-Intervall

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

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

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

SNMP-ID:

2.20.30.6

Pfad Konsole:

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

Mögliche Werte:

max. 10 Zeichen aus `[1-9]`

Default-Wert:

10

Robustheit

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

SNMP-ID:

2.20.30.7

Pfad Konsole:

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

Mögliche Werte:

max. 10 Zeichen aus `[1-9]`

Default-Wert:

2

Statische-Mitglieder

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

SNMP-ID:

2.20.30.8

Pfad Konsole:

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

Adresse

Die IP-Adresse der manuell definierten Multicast-Gruppe.

SNMP-ID:

2.20.30.8.1

Pfad Konsole:

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

Mögliche Werte:

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

VLAN-Id

Die VLAN-ID, auf welche diese statische Mitgliedschaft angewendet werden soll. Für eine IP-Multicast-Adresse können durchaus mehrere Einträge mit unterschiedlichen VLAN-IDs gemacht werden.

SNMP-ID:

2.20.30.8.3

Pfad Konsole:

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

Mögliche Werte:

0 … 4096

Default-Wert:

0

Besondere Werte:

0

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

Werbe-Intervall

Das Intervall in Sekunden, in dem die Geräte Pakete aussenden, mit denen sie sich als Multicast-fähige Router bekanntmachen. Aufgrund dieser Information können andere IGMP- / MLD-Snooping-fähige Geräte schneller lernen, welche ihrer Ports als Router-Ports verwendet werden sollen. Beim Aktivieren von Ports kann ein Switch z. B. eine entsprechende Anfrage nach Multicast-Routern versenden, die der Router mit einer solchen Bekanntmachung beantworten

kann. Diese Methode ist je nach Situation ggf. deutlich schneller als die alternative Lernmöglichkeit über die IGMP- / MLD-Anfragen.

SNMP-ID:

2.20.30.9

Pfad Konsole:

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

Mögliche Werte:

4 … 180 Sekunden

Default-Wert:

20

Protokolle

Geben Sie die unterstützten Protokolle an: IGMP, MLD oder beide.

SNMP-ID:

2.20.30.10

Pfad Konsole:

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

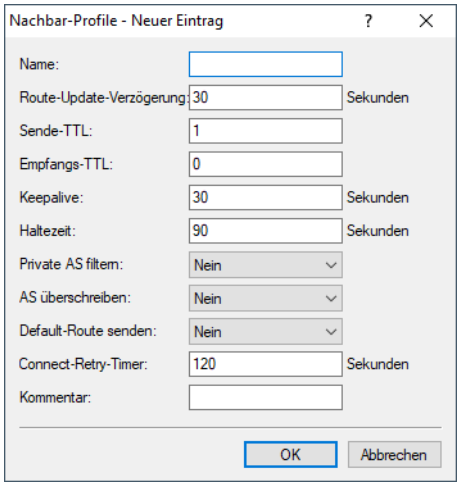
Mögliche Werte:

IGMP
MLD
IGMP-und-MLD

5.8 BGP: Schalter für Default-Route propagieren

Ab LCOS 10.40 unterstützt Ihr Gerät die Möglichkeit, Default Routen bei BGP wie normale Routen zu behandeln.

In LANconfig konfigurieren Sie diese Option unter **Routing Protokolle** > **BGP** > **Nachbar-Profile**



Default-Route senden

Dieser Schalter bestimmt das Verhalten der Propagation von Default Routen. Mögliche Werte:

Ja

Default Routen werden in BGP Phase 3 (Bestimmung der Routen zur Redistribution) wie normale Routen behandelt.

Nein

Default Routen werden ignoriert, die nicht als Quelle die Tabelle der statischen BGP Routen haben (*IPv4-Netzwerke* oder *IPv6-Netzwerke*).

5.8.1 Ergänzungen im Setup-Menü

Default-Route-Senden

Dieser Schalter bestimmt das Verhalten der Propagation von Default Routen.

SNMP-ID:

2.93.1.3.11

Pfad Konsole:

Setup > **Routing-Protokolle** > **BGP** > **Nachbar-Profile**

Mögliche Werte:

Ja

Default Routen werden in BGP Phase 3 (Bestimmung der Routen zur Redistribution) wie normale Routen behandelt.

Nein

Default Routen werden ignoriert, die nicht als Quelle die Tabelle der statischen BGP Routen haben.

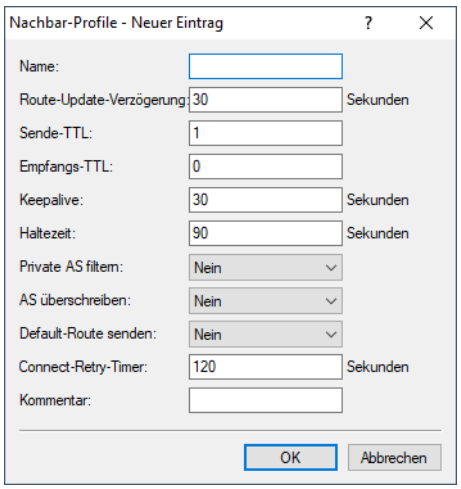
Default-Wert:

Nein

5.9 BGP: Connection Retry Timer einstellbar

Ab LCOS 10.40 unterstützt Ihr Gerät die Möglichkeit, den Connection Retry Timer für BGP zu konfigurieren

In LANconfig konfigurieren Sie diese Option unter **Routing Protokolle** > **BGP** > **Nachbar-Profile**



Connect-Retry Timer

Definiert die Zeit in Sekunden, die der Router bei einem fehlgeschlagenen BGP-Verbindungsaufbau wartet bis zum nächsten Verbindungsversuch. In der Regel wird dieser Schalter nur benötigt, wenn die Gegenseite im Verbindungsmodus „passiv" ist, um den Verbindungsaufbau zu beschleunigen. Default: 120 Sekunden

5.9.1 Ergänzungen im Setup-Menü

Connect-Retry-Zeit

Definiert die Zeit in Sekunden, die der Router bei einem fehlgeschlagenen BGP-Verbindungsaufbau wartet bis zum nächsten Verbindungsversuch. In der Regel wird dieser Schalter nur benötigt, wenn die Gegenseite im Verbindungsmodus „passiv" ist, um den Verbindungsaufbau zu beschleunigen.

SNMP-ID:

2.93.1.3.12

Pfad Konsole:

Setup > **Routing-Protokolle** > **BGP** > **Nachbar-Profile**

Mögliche Werte:

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

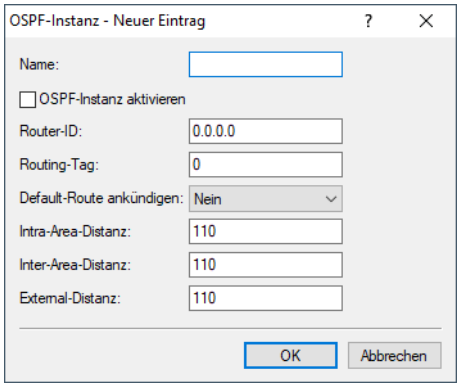
Default-Wert:

120

5.10 Administrative Distanz bei OSPF konfigurierbar

Ab LCOS 10.40 können bei OSPF jetzt die Administrativen Distanzen konfiguriert werden, mit der OSPF-Routen in die Routing-Tabelle eingetragen werden. Die Administrative Distanz kann dabei je nach OSPF-Routen-Typ definiert werden.

Um die administrative Distanz bei OSPF mit LANconfig zu konfigurieren, wechseln Sie in die Ansicht **Routing Protokolle** > **OSPF** > **OSPF-Instanz**.



Intra-Area-Distanz

Definiert die Administrative Distanz, mit der OSPF empfangende Routen des Typs Intra-Area in die Routing-Tabelle einfügt.

Inter-Area-Distanz

Definiert die Administrative Distanz, mit der OSPF empfangende Routen des Typs Inter-Area in die Routing-Tabelle einfügt.

External-Distanz

Definiert die Administrative Distanz, mit der OSPF empfangende Routen des Typs External in die Routing-Tabelle einfügt.

5.10.1 Ergänzungen im Setup-Menü

Intra-Area-Distance

Definiert die Administrative Distanz, mit der OSPF empfangende Routen des Typs Intra-Area in die Routing-Tabelle einfügt.

SNMP-ID:

2.93.3.1.7

Pfad Konsole:

Setup > **Routing-Protokolle** > **OSPF** > **OSPF-Instanz**

Mögliche Werte:

0 … 255

Default-Wert:

110

Inter-Area-Distance

Definiert die Administrative Distanz, mit der OSPF empfangende Routen des Typs Inter-Area in die Routing-Tabelle einfügt.

SNMP-ID:

2.93.3.1.8

Pfad Konsole:

Setup > **Routing-Protokolle** > **OSPF** > **OSPF-Instanz**

Mögliche Werte:

0 … 255

Default-Wert:

110

External-Distance

Definiert die Administrative Distanz, mit der OSPF empfangende Routen des Typs External in die Routing-Tabelle einfügt.

SNMP-ID:

2.93.3.1.9

Pfad Konsole:

Setup > **Routing-Protokolle** > **OSPF** > **OSPF-Instanz**

Mögliche Werte:

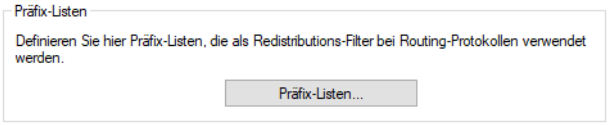
0 … 255

Default-Wert:

110

5.11 Filterliste für Redistribution in OSPF

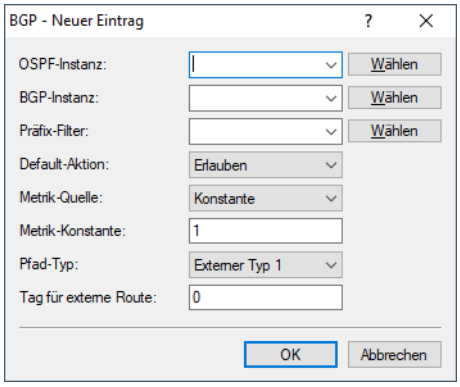
Mit Hilfe von Filterlisten für die Redistribution bei OSPF können bestimmte Präfixe für die Redistribution erlaubt oder verweigert werden. Dazu legen Sie die Präfix-Filterliste wie bisher bereits für BGP unter **IP-Router** > **Allgemein** > **Präfix-Listen** an.



Verwendung der Präfix-Listen bei OSPF

Diese **Präfix-Listen** können Sie dann für die Redistribution von statischen Routen, BGP und verbundenen Routen des OSPF-Protokolls referenzieren sowie definieren, ob diese Präfix-Listen erlaubt oder abgelehnt werden sollen.

Routing Protokolle > OSPF > BGP



Präfix-Filter

Name der Präfix-Filterliste aus *Präfix-Listen*.

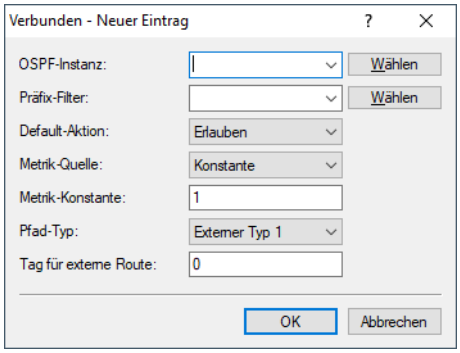
Default-Aktion

Definiert, wie Präfixe standardmäßig behandelt werden sollen, die in der Präfix-Liste konfiguriert sind. Mögliche Werte:

Erlauben

Verweigern

Routing Protokolle > OSPF > Verbunden



Präfix-Filter

Name der Präfix-Filterliste aus *Präfix-Listen*.

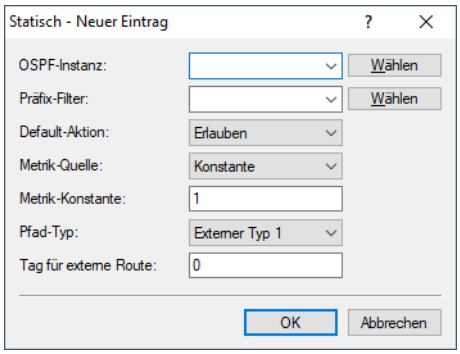
Default-Aktion

Definiert, wie Präfixe standardmäßig behandelt werden sollen, die in der Präfix-Liste konfiguriert sind. Mögliche Werte:

Erlauben

Verweigern

Routing Protokolle > **OSPF** > **Statisch**



Präfix-Filter

Name der Präfix-Filterliste aus *Präfix-Listen*.

Default-Aktion

Definiert, wie Präfixe standardmäßig behandelt werden sollen, die in der Präfix-Liste konfiguriert sind. Mögliche Werte:

Erlauben

Verweigern

5.11.1 Ergänzungen im Setup-Menü

Filter-Liste

Name der Präfix-Filterliste aus **Setup** > **Routing-Protokolle** > **Filter** > **Praefix-Liste**.

SNMP-ID:

2.93.3.9.1.3

Pfad Konsole:

Setup > **Routing-Protokolle** > **OSPF** > **Route-Weiterverteilen** > **BGP**

Mögliche Werte:

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

Default-Wert:

leer

Default-Aktion

Definiert, wie Präfixe standardmäßig behandelt werden sollen, die in der Präfix-Liste konfiguriert sind.

SNMP-ID:

2.93.3.9.1.8

Pfad Konsole:

Setup > **Routing-Protokolle** > **OSPF** > **Route-Weiterverteilen** > **BGP**

Mögliche Werte:

Erlauben
Ablehnen

Default-Wert:

Erlauben

Filter-Liste

Name der Präfix-Filterliste aus **Setup** > **Routing-Protokolle** > **Filter** > **Praefix-Liste**.

SNMP-ID:

2.93.3.9.2.2

Pfad Konsole:

Setup > **Routing-Protokolle** > **OSPF** > **Route-Weiterverteilen** > **Verbunden**

Mögliche Werte:

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

Default-Wert:

leer

Default-Aktion

Definiert, wie Präfixe standardmäßig behandelt werden sollen, die in der Präfix-Liste konfiguriert sind.

SNMP-ID:

2.93.3.9.2.7

Pfad Konsole:

Setup > **Routing-Protokolle** > **OSPF** > **Route-Weiterverteilen** > **Verbunden**

Mögliche Werte:

Erlauben
Ablehnen

Default-Wert:

Erlauben

Filter-Liste

Name der Präfix-Filterliste aus **Setup** > **Routing-Protokolle** > **Filter** > **Praefix-Liste**.

SNMP-ID:

2.93.3.9.4.2

Pfad Konsole:

Setup > **Routing-Protokolle** > **OSPF** > **Route-Weiterverteilen** > **Statisch**

Mögliche Werte:

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

Default-Wert:

leer

Default-Aktion

Definiert, wie Präfixe standardmäßig behandelt werden sollen, die in der Präfix-Liste konfiguriert sind.

SNMP-ID:

2.93.3.9.4.7

Pfad Konsole:

Setup > **Routing-Protokolle** > **OSPF** > **Route-Weiterverteilen** > **Statisch**

Mögliche Werte:

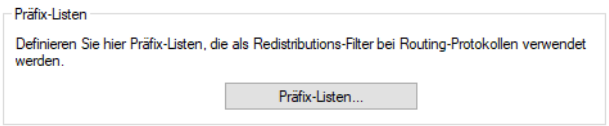
Erlauben
Ablehnen

Default-Wert:

Erlauben

5.12 Filterliste für Redistribution in LISP

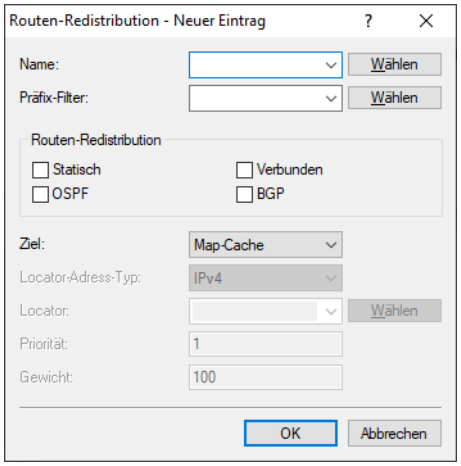
Mit Hilfe von Filterlisten für die Redistribution bei LISP können bestimmte Präfixe für die Redistribution erlaubt werden. Dazu legen Sie die Präfix-Filterliste wie bisher bereits für BGP unter **IP-Router** > **Allgemein** > **Präfix-Listen** an.



Verwendung der Präfix-Listen bei LISP

Diese **Präfix-Listen** können Sie dann für die Redistribution von statischen Routen, BGP, OSPF und verbundenen Routen verwenden.

Routing Protokolle > **LISP** > **Routen-Redistribution**



Präfix-Filter

Name der Präfix-Filterliste aus *Präfix-Listen*. Für die Präfixe aus dieser Liste wird die Routen-Redistribution erlaubt.

5.12.1 Ergänzungen im Setup-Menü

Filter-Liste

Name der Präfix-Filterliste aus **Setup** > **Routing-Protokolle** > **Filter** > **Praefix-Liste**. Für die Präfixe aus dieser Liste wird die Routen-Redistribution erlaubt.

SNMP-ID:

2.93.4.10.8

Pfad Konsole:

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

Mögliche Werte:

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

Default-Wert:

leer

6 Firewall

6.1 Keine MAC-Adressen als Ziel in Firewallregeln

Ab LCOS 10.40 werden MAC-Adressen als Ziel in Firewallregeln nicht mehr unterstützt. Ein entsprechendes Stationsobjekt, das unter **Firewall/QoS** > **IPv4-Regeln** > **Firewall-Objekte** > **Stations-Objekte** angelegt wurde, lässt sich nicht als Zielobjekt in einer Firewallregel verwenden.

6.2 DNS-Cache-Zeit konfigurierbar

Ab LCOS 10.40 können Sie die DNS-Cache-Zeit für die Verwendung von DNS-Objekten in der Firewall konfigurieren. Über den Schalter DNS-Minimum-Cache-Zeit wird die Zeit in Sekunden definiert, die ein DNS-Eintrag minimal gespeichert werden soll, falls die TTL im DNS-Paket kleiner als der konfigurierte Wert ist. Hierbei wird ein Puffer von 10 Sekunden hinzuaddiert. Es wird somit das Maximum des Parameters DNS-Minimum-Cache-Zeit und der um 10 Sekunden erhöhten TTL aus dem DNS-Paket verwendet.

6.2.1 Ergänzungen im Setup-Menü

DNS-Minimum-Cache-Zeit

Über diesen Schalter wird die Zeit in Sekunden definiert, die ein DNS-Eintrag minimal gespeichert werden soll, falls die TTL im DNS-Paket kleiner als der konfigurierte Wert ist. Hierbei wird ein Puffer von 10 Sekunden hinzuaddiert. Es wird somit das Maximum des Parameters **DNS-Minimum-Cache-Zeit** und der um 10 Sekunden erhöhten TTL aus dem DNS-Paket verwendet.

SNMP-ID:

2.110.3

Pfad Konsole:

Setup > **Firewall**

Mögliche Werte:

max. 11 Zeichen aus `[0-9]`

Default-Wert:

180

7 Multicast Routing

In der Datenkommunikation unterscheidet man grundsätzlich vier Kategorien von Kommunikationsbeziehungen: Unicast, Broadcast, Multicast und Anycast. Unter Unicast versteht man die 1:1-Kommunikation, d. h. ein Sender kommuniziert mit einem Empfänger. Bei Broadcast sendet ein Sender Daten an alle angeschlossenen Geräte (1:n-Beziehung, bzw. „einer an alle"). Diese Kommunikationsmethode ist für bestimmte Dienste wie IPTV ineffizient, da alle Clients die Daten erhalten würden, also auch die Clients die kein Interesse daran haben. Daher gibt es mit Multicast eine weitere Methode, um Sender / Empfänger-Beziehungen herzustellen.. Multicast ist eine effiziente Kommunikationsmethode bei der ein Sender die Daten nur an die Geräte sendet, die Interesse an den Daten haben (1:m Beziehung, bzw. „einer an viele"). Empfänger müssen daher, bevor sie Daten empfangen, ihr Interesse durch Signalisierungsnachrichten bekunden. Bei der Kommunikationsbeziehung Anycast sendet ein Sender die Daten an einen beliebigen Empfänger aus einer Gruppe. In diesem Kapitel wird das Thema Multicast weiter behandelt.

Bei Multicast unterscheidet man grundsätzlich zwischen den folgenden Rollen: Sender und Empfänger. Ein Empfänger ist beispielsweise ein IPTV-Receiver oder ein mobiles Endgerät / PC. Unter einem Sender versteht man die Multicast-Quelle, z. B. einen IPTV-Sender. Wenn ein Client Multicast-Daten erhalten möchte, z. B. einen IPTV-Kanal, so bekundet er sein Interesse durch das Senden eines IGMP (Internet Group Management Protocol) Membership Reports bzw. bei IPv6 eines MLD (Multicast Listener Discovery) Membership Reports. Ein Multicast-Router erzeugt daraufhin automatisch einen Multicast-Routing Eintrag für diese Gruppe. Die Daten fließen dann „rückwärts" von der Quelle zum Empfänger. Besteht beim Client kein Interesse mehr an den Multicast-Daten, so sendet dieser eine entsprechen Membership Report zum Verlassen der Gruppe.

Der IP-Adressbereich für Multicast ist definiert von 224.0.0.0 bis 239.255.255.255 bei IPv4 bzw. als Präfix FF00::/8 bei IPv6. Man unterscheidet bei Multicast grundsätzlich in verschiedene Gültigkeitsbereiche, z. B. Link Local, Source Specific Multicast (232.0.0.0 bis 232.255.255.255) oder Organization-Local Scope (239.0.0.0 bis 239.255.255.255).

Weiterhin unterscheidet man zwei Kategorien von Multicast: Any Source Multicast (ASM) sowie Source Specific Multicast (SSM). Bei Any Source Multicast, dargestellt als (*,G), gibt der Empfänger nur die Multicast-Gruppe G an, und akzeptiert diese von beliebigen Quellen *. Any Source Multicast ist die ältere Variante der beiden Verfahren. Source Specific Multicast ist die moderne Variante bei der ein Empfänger neben der gewünschten Gruppe auch eine oder mehrere Quellen S anfordert. SSM setzt allerdings IGMPv3 bzw. MLDv2 voraus. Nach Möglichkeit sollte grundsätzlich SSM mit IGMPv3 eingesetzt werden, da dies besser skaliert. In der Regel basieren IPTV-Architekturen auf SSM.

Multicast-Routen werden nicht in der normalen (Unicast-)Routing-Tabelle verwaltet, sondern in einer separaten Multicast-Routing-Tabelle. Die Routing-Einträge dort werden in der Regel nicht statisch konfiguriert, sondern von Multicast-Routing-Protokollen wie PIM (Protocol Independent Multicast) oder einem Proxy, z. B. IGMP-Proxy, dynamisch erzeugt. Grundsätzlich setzt Multicast eine funktionierende Unicast-Routing-Tabelle voraus, da beim Reverse Path Forward Check (RPF-Check) geprüft wird, ob es eine Route zur Multicast-Quelle gibt. In der Regel wird neben einem Multicast Routing Protokoll wie PIM auch immer ein Unicast Routing-Protokoll verwendet, beispielsweise OSPF.

Für ein Szenario mit Multicast-Routing stehen drei Ansätze zur Verfügung:

1. Für ein einfaches Multicast-Routing-Szenario: Einsatz des IGMP- / MLD-Proxies.
2. Für ein komplexes Multicast-Routing-Szenario: PIM SSM.
3. Konfiguration von statischen Gruppeneinträgen wird nur empfohlen, wenn Clients kein IGMP / MLD beherrschen.

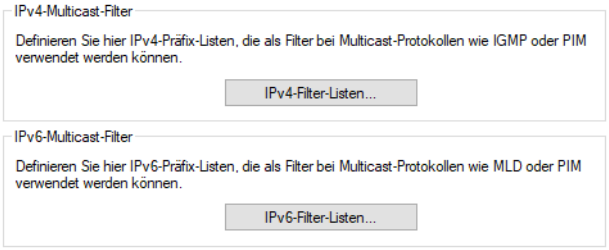
PIM Sparse Mode kann ebenfalls statt PIM SSM zum Einsatz kommen, allerdings muss sowohl die Rolle des Rendezvous Points als auch die des First-Hop-Routers direkt vor der Multicast-Quelle von einem Dritthersteller übernommen werden.

7.1 Allgemeine Multicast Show-Kommandos

- `show IPv4-mfib` / `show IPv4-mfib` (als alias gibt es `ipv4-mroute` / `ipv6-mroute`): Zeigt den Inhalt der Multicast Forwarding Information Base / Routing-Tabelle an.
- `show iPv4-tib` / `show iPv6-tib`: Zeigt den Inhalt der Tree Information Base an. Enthält Informationen über den Multicast Gruppenstatus sowie zusätzliche Informationen aus PIM.
- `show igmp-groups`: Zeigt Informationen über Multicast-Gruppen, bei denen der Router selbst beigetreten ist.

7.2 Allgemeine Einstellungen

Um allgemeine Einstellungen zu Multicast mit LANconfig zu konfigurieren, wechseln Sie in die Ansicht **Multicast** > **Allgemein**.

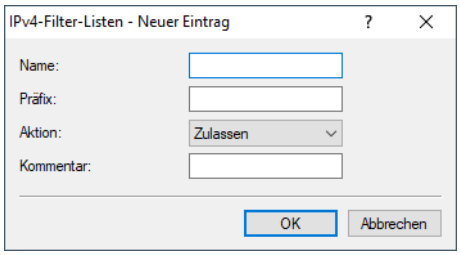


7.2.1 IPv4-Filter-Listen

In LANconfig konfigurieren Sie die IPv4-Filter-Listen für Muilticast unter **Multicast** > **Allgemein** > **IPv4-Multicast-Filter** über **IPv4-Filter-Listen**.

In dieser Tabelle können Listen von gewünschten oder unerwünschten IPv4 Multicast-Adressen bzw. Präfixen definiert werden. Verschiedene einzelne Filterregeln können durch einen gleichen Namen zu einer Regelliste zusammengefasst werden. In einer Regelliste können sowohl Präfixe verboten als auch erlaubt werden.

Die Namen der Filterlisten können an verschiedenen Stellen referenziert werden und über diese Tabelle global verwaltet werden.



Name

Geben Sie diesem Eintrag einen Namen. Eine Liste wird durch mehrere Einträge mit gleichem Namen definiert.

Präfix

Geben Sie hier die IPv4-Adresse des Netzwerkes gefolgt von der Präfix-Länge des Netzwerkes an (CIDR-Notation). Diese legt fest, wie viele höchstwertige Bits (Most Significant Bit, MSB) der IP-Adresse für eine Übereinstimmung notwendig sind.

Aktion

Geben Sie an, ob die Präfixe dieses Filtereintrags zugelassen oder abgewiesen werden sollen.

Kommentar

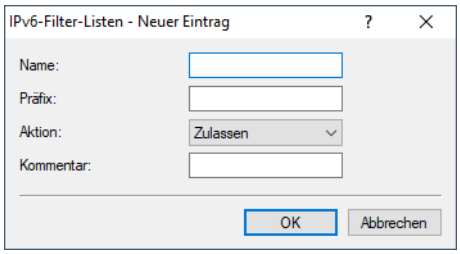
Kommentar zu diesem Eintrag.

7.2.2 IPv6-Filter-Listen

In LANconfig konfigurieren Sie die IPv4-Filter-Listen für Muilticast unter **Multicast** > **Allgemein** > **IPv6-Multicast-Filter** über **IPv6-Filter-Listen**.

In dieser Tabelle können Listen von gewünschten oder unerwünschten IPv6 Multicast-Adressen bzw. Präfixen definiert werden. Verschiedene einzelne Filterregeln können durch einen gleichen Namen zu einer Regelliste zusammengefasst werden. In einer Regelliste können sowohl Präfixe verboten als auch erlaubt werden.

Die Namen der Filterlisten können an verschiedenen Stellen referenziert werden und über diese Tabelle global verwaltet werden.



Name

Geben Sie diesem Eintrag einen Namen. Eine Liste wird durch mehrere Einträge mit gleichem Namen definiert.

Präfix

Geben Sie hier die IPv6-Multicast-Adresse bzw. das Präfix an.

Aktion

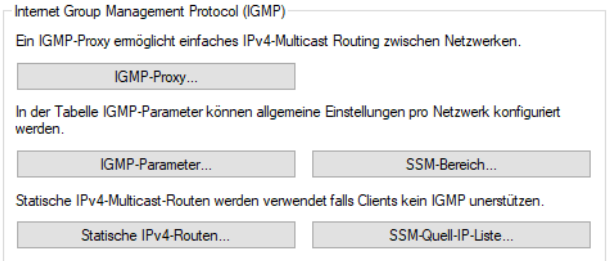
Geben Sie an, ob die Präfixe dieses Filtereintrags zugelassen oder abgewiesen werden sollen.

Kommentar

Kommentar zu diesem Eintrag.

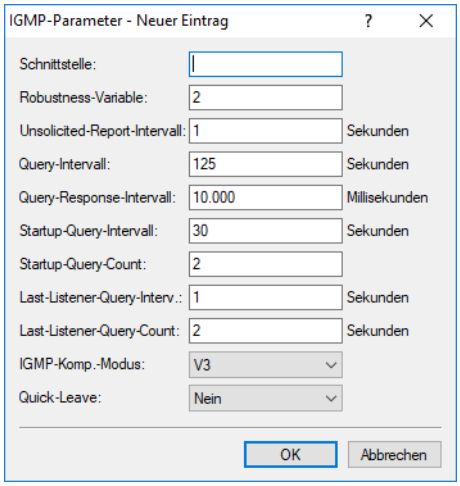
7.3 IGMP (Internet Group Management Protocol)

Um IGMP mit LANconfig zu konfigurieren, wechseln Sie in die Ansicht **Multicast** > **IGMP / MLD** > **Internet Group Management Protocol (IGMP)**.



7.3.1 IGMP-Parameter

In LANconfig konfigurieren Sie die allgemeinen IGMP-Parameter unter **Multicast** > **IGMP / MLD** > **Internet Group Management Protocol (IGMP)** über **IGMP-Parameter**.



Schnittstelle

Schnittstellenname, für den die IGMP-Konfiguration gilt. Der Eintrag mit dem Namen DEFAULT gilt für alle Schnittstellen, die keinen spezifischen Eintrag haben. Falls der Eintrag DEFAULT nicht vorhanden ist, gelten interne Default-Werte die den Werten des DEFAULT-Eintrags entsprechen. Mögliche Werte sind DEFAULT, IPv4-Netzwerke, z. B. INTRANET oder IPv4-(WAN)-Gegenstellen. Ebenfalls sind Wildcard-Einträge mit * für RAS-Interfaces erlaubt, z. B. „VPN*".

Robustness-Variable

Anzahl der Wiederholungen von IGMP-Nachrichten. (1-10; Default: 2)

Unsolicited-Report-Intervall

Definiert die Zeit zwischen den Wiederholungen von Membership-Reports nach dem das Gerät in der Host-Rolle den erstmaligen Membership-Report in einer Gruppe gesendet hat. (1-25 Sekunden; Default: 2)

Query-Intervall

Intervall zwischen IGMP General-Query-Nachrichten. (2-99999 Sekunden; Default: 125)

Query-Response-Intervall

Maximale Antwortzeit. Aus dieser wird der Wert Maximum Response Time berechnet, der in periodischen General-Query-Nachrichten gesetzt wird. Der Wert Query-Response-Intervall muss kleiner als der Wert für Query-Intervall sein. (1-999999 Millisekunden; Default: 10000)

Startup-Query-Intervall

Intervall zwischen IGMP General-Query-Nachrichten beim Start des IGMP-Queriers. (1-99998 Sekunden; Default: 30)

Startup-Query-Count

Anzahl an IGMP General-Query-Nachrichten, die beim Start gesendet werden, unterbrochen bzw. zeitlich verzögert vom Startup-Query-Intervall. (1-10; Default: 2)

Last-Listener-Query-Intervall

Definiert den Wert der Maximum Response Time in Multicast-Address-Specific Queries, die als Antwort auf Done-Nachrichten gesendet werden. Der Parameter definiert ebenso die Zeit zwischen Multicast-Address-Specific-Query-Nachrichten. (1-25 Sekunden; Default: 2)

Last-Listener-Query-Count

Anzahl von gesendeten Nachrichten vom Typ Multicast-Address-Specific Query bevor der Router annimmt, dass es keine lokalen Empfänger mehr gibt. Definiert ebenso die Anzahl an gesendeten Nachrichten vom Typ Multicast-Address-Specific-Query bevor der Router annimmt, dass es keine weiteren Empfänger für eine spezielle Quelle gibt. (1-10; Default: 2)

IGMP-Kompatibilitäts-Modus

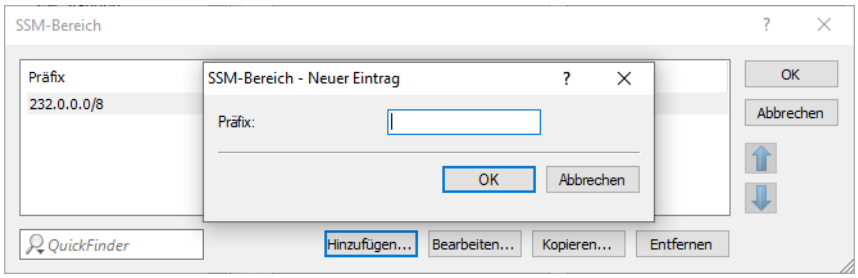
IGMP-Version, in der das Gerät in der Rolle als Multicast-Router arbeitet. Mögliche Werte: Aus, V1, V2, V3. (Default: V3)

Quick-Leave

Erlaubt das schnelle Verlassen von Multicast Gruppen. Sollte nur verwendet werden, falls es nur einen Empfänger pro Gruppe auf dem Interface gibt. Intern wird der Parameter Last-Listener-Query-Count auf 1 und das Last-Listener-Query-Intervall auf 20 ms gesetzt. Mögliche Werte: Ja, Nein (Default: Nein)

7.3.2 SSM-Bereich

In LANconfig konfigurieren Sie die SSM-Bereiche unter **Multicast** > **IGMP / MLD** > **Internet Group Management Protocol (IGMP)** über **SSM-Bereich**.



Präfix

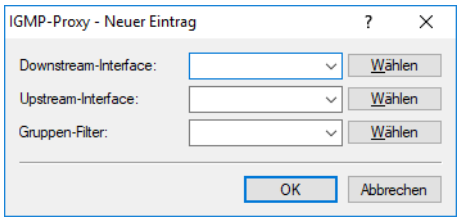
Definiert den IP-Adressbereich in Präfixschreibweise, der für SSM verwendet wird.

7.3.3 IGMP-Proxy

Ein IGMP-Proxy wird in der Regel bei Interzugängen mit Multicast IPTV verwendet. Dabei senden Clients bzw. IPTV Set-Top-Boxen (STBs) im lokalen Netz IGMP-Nachrichten, um einen bestimmten TV-Kanal zu empfangen. Dazu treten sie bestimmten Multicast-Gruppen bei und verlassen diese auch wieder. Der Router bzw. die IGMP-Proxy-Funktionalität empfängt die IGMP-Nachrichten und leitet sie an das Provider-Netzwerk weiter bzw. filtert die Gruppen bei Bedarf. Der IGMP-Proxy arbeitet dabei als Stellvertreter für das lokale Netzwerk mit seinen Clients.

Ein IGMP-Proxy kann auch in einfachen Multicast-Routing Szenarien beispielsweise über VPN verwendet werden ohne dass PIM verwendet werden muss. Durch die Konfiguration des IGMP-Proxies wird eine statische (Baum-)Struktur ohne alternative Pfade bzw. Redundanz sowie Loop-Verhinderung erzeugt. IGMP-Proxies können durch eine Reihenschaltung mehrerer Router „kaskadiert“ werden.

In LANconfig konfigurieren Sie den IGMP-Proxy unter **Multicast** > **IGMP / MLD** > **Internet Group Management Protocol (IGMP)** über **IGMP-Proxy**.



Downstream-Interface

Interface-Name auf dem IGMP-Clients Gruppen beitreten können und IGMP-Nachrichten vom Proxy empfangen werden. Mögliche Werte sind IPv4-Netzwerke, z. B. INTRANET, IPv4-(WAN)-Gegenstellen. Ebenfalls sind Wildcard-Einträge mit * für RAS-Interfaces erlaubt, z. B. „VPN*“.

Bei Provider-basierten IPTV-Szenarien muss hier das lokale Netzwerk, z. B. INTRANET, konfiguriert werden.

Upstream-Interface

Interface Name auf dem IGMP-Nachrichten vom Proxy stellvertretend für Clients gesendet werden. Die Quelle der Multicast-Nachrichten muss über dieses Interface erreicht werden. Mögliche Werte sind IPv4-Netzwerke, z. B. INTRANET sowie IPv4-(WAN)-Gegenstellen.

Bei Provider-basierten IPTV-Szenarien muss hier die WAN-Gegenstelle, z. B. INTERNET, konfiguriert werden.

Gruppenfilter

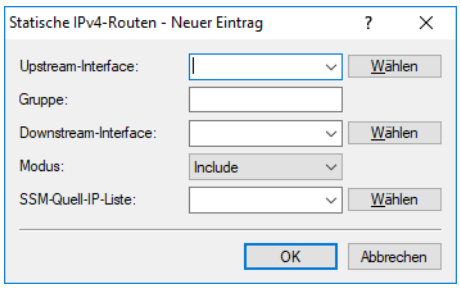
Name des Gruppenfilters der für diesen Proxy gelten soll. Referenziert die Tabelle IPv4-Filter-Listen unter **Multicast** > **Allgemein**. Standardmäßig ist der Filtereintrag leer bzw. verweist auf die Filterliste „ANY“, die alle Multicast-Gruppen erlaubt. Mit Hilfe des Gruppenfilters können die möglichen Multicast-Gruppen für Clients eingeschränkt werden.

7.3.4 Statisches IPv4-Multicast Routing

Statisches Multicast Routing kann verwendet werden, wenn Multicast Clients kein IGMP beherrschen bzw. für Szenarien, in dem Multicast-Datenverkehr immer fließen muss, ohne dass Clients die entsprechende Gruppe anfordern. Der Router erzeugt ab dem Anlegen des Eintrags auf dem Upstream-Interface IGMP Joins bzw. Gruppenreporte.

Bitte beachten Sie, dass ein statisches Multicast Routing hohen Datenverkehr und Last verursachen kann, da die Multicast-Daten immer weitergeleitet werden.

In LANconfig konfigurieren Sie die statischen IPv4-Multicast-Routen unter **Multicast** > **IGMP / MLD** > **Internet Group Management Protocol (IGMP)** über **Statische IVv4-Routen**.



Upstream-Interface

Interface Name auf dem die Multicast-Pakete den Router erreichen. Mögliche Werte sind IPv4-Netzwerke, z. B. INTRANET sowie IPv4-(WAN)-Gegenstellen.

Gruppe

Multicast-Gruppe für die das statische Weiterleiten von Multicast-Daten angelegt werden soll, z. B. 239.0.0.1.

Downstream-Interface

Interface Name auf dem die Multicast-Pakete den Router verlassen sollen. Mögliche Werte sind IPv4-Netzwerke, z. B. INTRANET sowie IPv4-(WAN)-Gegenstellen.

Modus

Falls SSM verwendet werden soll: Steuert, über welche Methode Quelladressen der Multicast-Quellen in einem IGMP-Membership-Report angefordert werden sollen. Mögliche Werte:

Include

Es wird ein IGMP-Membership Report mit Record-Type „Change to Include Mode" gesendet. Die Einträge aus der SSM-Quell-IP-Liste werden als gewünschte Quelladressen gesendet. Eine Kombination mit Einstellung „Include" und SSM-Quell-IP-Liste mit Eintrag „ANY" führt zu keinem sinnvollen Ergebnis und wird als Konfiguration intern nicht akzeptiert, da alle Quell-IP-Adressen abgelehnt werden würden.

Exclude

Es wird ein IGMP-Membership Report mit Record-Type „Change to Exclude Mode" gesendet. Wenn die Quell-Liste den Eintrag „ANY" bzw. „0.0.0.0" enthält, d. h. alle Quellen erlaubt, so wird ein IGMP-Membership Report mit Join Group für „any sources" gesendet. Wenn die Liste einen anderen Eintrag als 0.0.0.0 enthält wird ein IGMP Membership Report „block sources" mit der entsprechenden IP-Adresse gesendet.

Wenn eine SSM-Gruppe mit beliebigen Quelladressen verwendet werden soll, so muss bei Modus „Exclude" und SSM-Quell-IP-Liste „ANY" verlinkt werden.

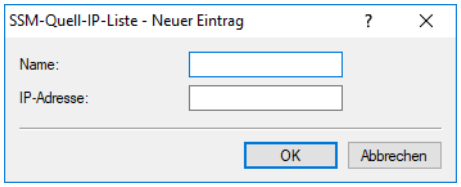
SSM-Quell-IP-Liste

Falls SSM verwendet werden soll, kann hier eine Liste von gewünschten Quellen zusätzlich zur Multicast-Gruppe definiert werden. Sollen alle Quellen zugelassen werden, kann die vordefinierte Liste „ANY" mit dem Eintrag „0.0.0.0" verwendet werden.

7.3.5 SSM-Quell-IP-Liste

In dieser Tabelle können Listen von gewünschten oder unerwünschten (Unicast) Quell-IP-Adressen definiert werden. Diese können an verschiedenen Stellen referenziert werden und über diese Tabelle global verwaltet werden. Eine Liste wird durch den mehrere Einträge mit gleichem Namen definiert.

In LANconfig konfigurieren Sie die SSM-Quell-IP-Liste unter **Multicast** > **IGMP / MLD** > **Internet Group Management Protocol (IGMP)** über **SSM-Quell-IP-Liste**.



Name

Vergeben Sie einen Namen für den Eintrag. Eine Liste wird durch den mehrere Einträge mit gleichem Namen definiert.

IP-Adresse

Unicast Quell-IPv4-Adresse. Multicast-Adressen sind an dieser Stelle keine gültige Eingabe, da hier die Quell-IP-Adressen (Source) eines Multicast-Eintrag (S,G) definiert werden.

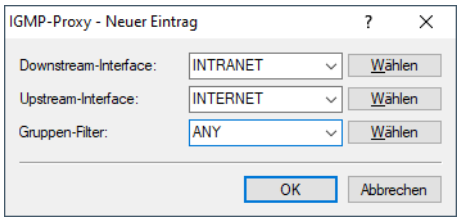
7.3.6 Tutorial: IGMP-Proxy einrichten

Im folgenden Tutorial werden die notwendigen Schritte zur Einrichtung eines IGMP-Proxies für Multicast-Routing beschrieben.

In diesem Beispiel befinden sich Multicast-Clients im Netzwerk „INTRANET", die Multicast-Quellen sind über die WAN-Gegenstelle „INTERNET" zu erreichen. Der IGMP-Proxy leitet IGMP-Nachrichten vom INTRANET ins INTERNET stellvertretend für die Clients weiter. Zusätzlich ist es möglich, dass bestimmte Multicast-Gruppen gefiltert werden können.

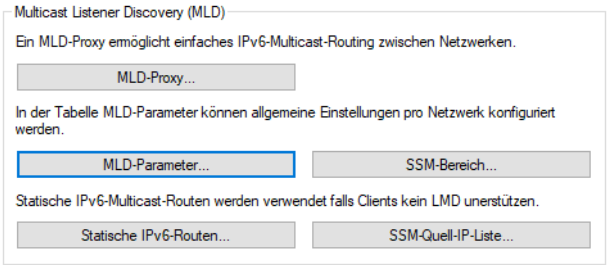
1. Neuen Tabelleneintrag erstellen unter **Multicast** > **IGMP / MLD** > **Internet Group Management Protocol (IGMP)** > **IGMP-Proxy** erstellen:
   - **Downstream-Interface**: Interface-Name, auf dem IGMP-Clients Gruppen beitreten können und IGMP-Nachrichten vom Proxy empfangen werden. Konfigurieren Sie hier den Namen des Client-Netzwerks, z. B. „INTRANET".
   - **Upstream-Interface**: Interface Name, auf dem IGMP-Nachrichten vom Proxy stellvertretend für Clients gesendet werden. Die Quelle der Multicast-Nachrichten muss über dieses Interface erreicht werden. Konfigurieren Sie hier den Namen der Gegenstelle der Internetverbindung, z. B. „INTERNET".
   - **Gruppen-Filter**: Name des Gruppenfilters der für diesen Proxy gelten soll. Referenziert die Tabelle **IPv4-Filter-Listen** unter **Multicast** > **Allgemein**. Mit Hilfe des Gruppenfilters können die möglichen Multicast-Gruppen für Clients eingeschränkt werden. Eintrag „ANY" auswählen, dieser erlaubt alle Multicast-Gruppen.

Weitere Einstellungen, z. B. in der Firewall sind ab LCOS 10.40 nicht mehr erforderlich.



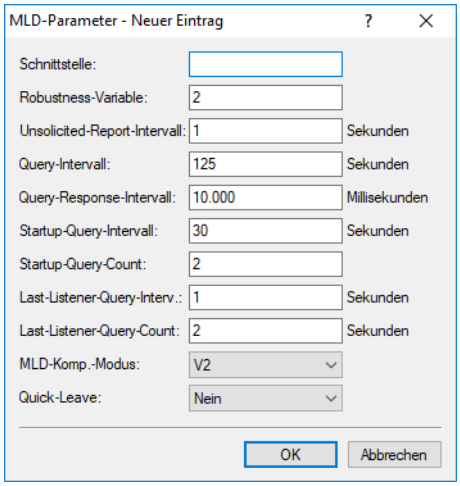
7.4 MLD (Multicast Listener Discovery)

Um MLD mit LANconfig zu konfigurieren, wechseln Sie in die Ansicht **Multicast** > **IGMP / MLD** > **Multicast Listener Discovery (MLD)**.



7.4.1 MLD-Parameter

In LANconfig konfigurieren Sie die allgemeinen MLD-Parameter unter **Multicast** > **IGMP / MLD** > **Multicast Listener Discovery (MLD)** über **MLD-Parameter**.



Schnittstelle

Schnittstellenname, für den die MLD-Konfiguration gilt. Der Eintrag mit dem Namen DEFAULT gilt für alle Schnittstellen, die keinen spezifischen Eintrag haben. Falls der Eintrag DEFAULT nicht vorhanden ist, gelten interne Default-Werte, die den Werten des DEFAULT-Eintrags entsprechen. Mögliche Werte sind DEFAULT, IPv6-Netzwerke, z. B. INTRANET, IPv6-(WAN)-Gegenstellen oder IPv6 RAS-Templates.

Robustness-Variable

Anzahl der Wiederholungen von MLD-Nachrichten. (1-10; Default: 2)

Unsolicited-Report-Intervall

Definiert die Zeit zwischen den Wiederholungen von Membership-Reports nach dem das Gerät in der Host-Rolle den erstmaligen Membership-Report in einer Gruppe gesendet hat. (1-25 Sekunden; Default: 2)

Query-Intervall

Intervall zwischen MLD General-Query-Nachrichten. (2-99999 Sekunden; Default: 125)

Query-Response-Intervall

Maximale Antwortzeit aus der der Wert Maximum Response Code berechnet wird, der in periodischen MLD General-Query-Nachrichten gesetzt wird. Der Wert Query-Response-Intervall muss kleiner als der Wert für Query-Intervall sein. (1-999999 Millisekunden; Default: 10000)

Startup-Query-Intervall

Intervall zwischen MLD General-Query-Nachrichten beim Start des MLD-Queriers. (1-99998 Sekunden; Default: 30)

Startup-Query-Count

Anzahl an MLD-General-Nachrichten die beim Start gesendet werden, unterbrochen bzw. zeitlich verzögert vom Startup-Query-Intervall. (1-10; Default: 2)

Last-Listener-Query-Intervall

Definiert den Wert des Maximum Response Code (bei IPv6) in Multicast-Address-Specific Queries, die als Antwort auf Done-Nachrichten gesendet werden. Der Parameter definiert ebenso die Zeit zwischen Multicast-Address-Specific-Query-Nachrichten. (1-25 Secunden; Default: 2)

Last-Listener-Query-Count

Anzahl von gesendeten Nachrichten vom Typ Multicast-Address-Specific Query bevor der Router annimmt, dass es keine lokalen Empfänger mehr gibt. Definiert ebenso die Anzahl an gesendeten Nachrichten vom Typ Multicast-Address-Specific-Query bevor der Router annimmt, dass es keine weiteren Empfänger für eine spezielle Quelle gibt. (1-10; Default: 2)

MLD-Kompatibilitäts-Modus

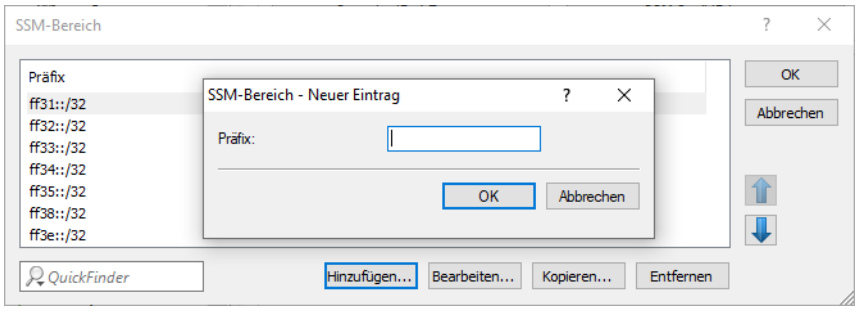
MLD-Version, in der das Gerät in der Rolle als Multicast-Router arbeitet. Mögliche Werte: Aus, V1, V2 (Default: V2)

Quick-Leave

Erlaubt das schnelle Verlassen von Multicast Gruppen. Sollte nur verwendet werden, falls es nur einen Empfänger pro Gruppe auf dem Interface gibt. Intern wird der Parameter Last-Listener-Query-Count auf 1 und das Last-Listener-Query-Intervall auf 20 ms gesetzt. Mögliche Werte: Ja, Nein (Default: Nein)

7.4.2 SSM-Bereich

In LANconfig konfigurieren Sie die SSM-Bereiche unter **Multicast** > **IGMP / MLD** > **Multicast Listener Discovery (MLD)** über **SSM-Bereich**.



Präfix

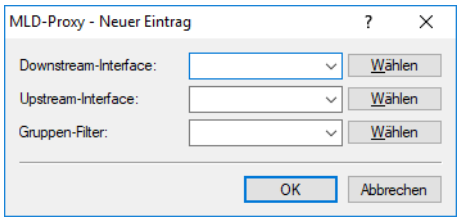
Definiert den IP-Adressbereich in Präfixschreibweise, der für SSM verwendet wird.

7.4.3 MLD-Proxy

Ein MLD-Proxy wird in der Regel bei Interzugängen mit Multicast IPTV über IPv6 verwendet. Dabei senden Clients bzw. IPTV Set-Top-Boxen (STBs) im lokalen Netz MLD-Nachrichten um einen bestimmten TV-Kanal zu empfangen. Dazu treten sie bestimmten Multicast-Gruppen bei und verlassen diese auch wieder. Der Router bzw. die MLD-Proxy-Funktionalität empfängt die MLD-Nachrichten und leitet sie an das Provider-Netzwerk weiter bzw. filtert die Gruppen bei Bedarf. Der MLD-Proxy arbeitet dabei als Stellvertreter für das lokale Netzwerk mit seinen Clients.

Ein MLD-Proxy kann auch in einfachen Multicast-Routing Szenarien beispielsweise über VPN verwendet werden ohne dass PIM verwendet werden muss. Durch die Konfiguration des MLD-Proxies wird eine statische (Baum-)Struktur ohne alternative Pfade bzw. Redundanz sowie Loop-Verhinderung erzeugt. MLD-Proxies können durch eine Reihenschaltung mehrerer Router „kaskadiert“ werden.

In LANconfig konfigurieren Sie den MLD-Proxy unter **Multicast** > **IGMP / MLD** > **Multicast Listener Discovery (MLD)** über **MLD-Proxy**.



Downstream-Interface

Interface-Name auf dem MLD-Clients Gruppen beitreten können und MLD-Nachrichten vom Proxy empfangen werden. Mögliche Werte sind IPv6-Netzwerke, z. B. INTRANET, IPv6-(WAN)-Gegenstellen oder RAS-Templates.

Bei Provider-basierten IPTV-Szenarien muss hier das lokale Netzwerk, z. B. INTRANET, konfiguriert werden.

Upstream-Interface

Interface Name auf dem MLD-Nachrichten vom Proxy stellvertretend für Clients gesendet werden. Die Quelle der Multicast-Nachrichten muss über dieses Interface erreicht werden. Mögliche Werte sind IPv6-Netzwerke, z. B. INTRANET sowie IPv6-(WAN)-Gegenstellen.

Bei Provider-basierten IPTV-Szenarien muss hier die WAN-Gegenstelle, z. B. INTERNET, konfiguriert werden.

Gruppenfilter

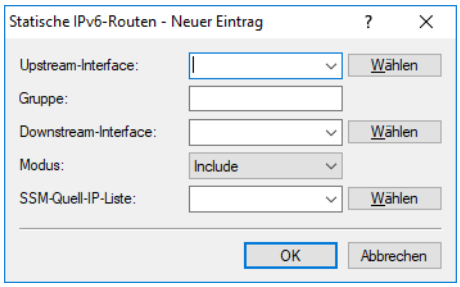
Name des Gruppenfilters, der für diesen Proxy gelten soll. Referenziert die Tabelle IPv6-Filter-Listen unter **Multicast** > **Allgemein**. Standardmäßig ist der Filtereintrag leer bzw. verweist auf die Filterliste „ANY", die alle Multicast-Gruppen erlaubt. Mit Hilfe des Gruppenfilters können die möglichen Multicast-Gruppen für Clients eingeschränkt werden.

7.4.4 Statisches IPv6-Multicast Routing

Statisches Multicast Routing kann verwendet werden, wenn Multicast Clients kein MLD beherrschen bzw. für Szenarien, in dem Multicast-Datenverkehr immer fließen muss, ohne dass Clients die entsprechende Gruppe anfordern. Der Router erzeugt ab dem Anlegen des Eintrags auf dem Upstream-Interface MLD Gruppenreporte.

Bitte beachten Sie, dass ein statisches Multicast Routing hohen Datenverkehr und Last verursachen kann, da die Multicast-Daten immer weitergeleitet werden.

In LANconfig konfigurieren Sie die statischen IPv6-Multicast-Routen unter **Multicast** > **IGMP / MLD** > **Multicast Listener Discovery (MLD)** über **Statische IVv6-Routen**.



Upstream-Interface

Interface Name auf dem die Multicast-Pakete den Router erreichen. Mögliche Werte sind IPv6-Netzwerke, z. B. INTRANET sowie IPv6-(WAN)-Gegenstellen.

Gruppe

Multicast-Gruppe für die das statische Weiterleiten von Multicast-Daten angelegt werden soll, beispielsweise „ff09::1“.

Downstream-Interface

Interface Name auf dem die Multicast-Pakete den Router verlassen sollen. Mögliche Werte sind IPv6-Netzwerke, z. B. INTRANET sowie IPv6-(WAN)-Gegenstellen.

Modus

Falls SSM verwendet werden soll: Steuert, über welche Methode Quelladressen der Multicast-Quellen in einem MLD-Membership-Report angefordert werden sollen. Mögliche Werte:

Include

Es wird ein MLD-Membership Report mit Record-Type „Change to Include Mode“ gesendet. Die Einträge aus der SSM-Quell-IP-Liste werden als gewünschte Quelladressen gesendet. Eine Kombination mit Einstellung „Include“ und SSM-Quell-IP-Liste mit Eintrag „ANY“ führt zu keinem sinnvollen Ergebnis und wird als Konfiguration intern nicht akzeptiert, da alle Quell-IP-Adressen abgelehnt werden würden.

Exclude

Es wird ein MLD-Membership Report mit Record-Type „Change to Exclude Mode“ gesendet. Wenn die Quell-Liste den Eintrag „ANY“ bzw. „::“ enthält, d. h. alle Quellen erlaubt, so wird ein MLD-Membership Report mit Join Group für „any sources“ gesendet. Wenn die Liste einen anderen Eintrag als „::“ enthält wird ein MLD Membership Report „block sources“ mit der entsprechenden IP-Adresse gesendet.

Wenn eine SSM-Gruppe mit beliebigen Quelladressen verwendet werden soll, so muss bei Modus „Exclude“ und SSM-Quell-IP-Liste „ANY“ verlinkt werden.

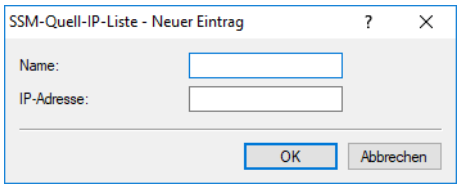
SSM-Quell-IP-Liste

Falls SSM verwendet werden soll, kann hier eine Liste von gewünschten Quellen zusätzlich zur Multicast-Gruppe definiert werden. Sollen alle Quellen zugelassen werden, kann die vordefinierte Liste „ANY“ mit dem Eintrag „::“ verwendet werden.

7.4.5 SSM-Quell-IP-Liste

In dieser Tabelle können Listen von gewünschten oder unerwünschten (Unicast) Quell-IPv6-Adressen definiert werden. Diese können an verschiedenen Stellen referenziert werden und über diese Tabelle global verwaltet werden. Eine Liste wird durch mehrere Einträge mit gleichem Namen definiert.

In LANconfig konfigurieren Sie die SSM-Quell-IP-Liste unter **Multicast** > **IGMP / MLD** > **Multicast Listener Discovery (MLD)** über **SSM-Quell-IP-Liste**.



Name

Vergeben Sie einen Namen für den Eintrag. Eine Liste wird durch den mehrere Einträge mit gleichem Namen definiert.

IP-Adresse

Unicast Quell-IPv6-Adresse. Multicast-Adressen sind an dieser Stelle keine gültige Eingabe, da hier die Quell-IPv6-Adressen (Source) eines Multicast-Eintrag (S,G) definiert werden.

7.5 PIM (Protocol Independent Multicast)

PIM (*RFC 7761*) ermöglicht dynamisches Routing von Multicast-Paketen. Dabei nutzt PIM die Routinginformationen des im Router aktiven Unicast-Routing-Protokolls mit, funktioniert aber grundsätzlich unabhängig von dem verwendeten Routingprotokoll wie z. B. RIP, OSPF oder BGP.

Für ein PIM-Szenario mit ausschließlich LANCOM Router wird nur die Betriebsart PIM SSM (Source Specific Multicast) vollständig unterstützt. Für den Betrieb des PIM Sparse Mode werden Router bzw. Komponenten von Drittherstellern benötigt. PIM SSM hat den Vorteil, dass es dank einfacherer Architektur deutlich besser skaliert und ideal geeignet ist für moderne Multicast-Anwendungen wie etwa IPTV. PIM SSM setzt auf der Clientseite IGMPv3 bzw. MLDv2 (bei IPv6) voraus und kommt ohne zusätzlichen Rendezvous Point (RP) aus, da Clients neben der gewünschten Multicast Gruppe (G) auch die Multicast Source (S) direkt anfragen.

Grundsätzlich wird bei PIM SSM zwischen zwei Router-Rollen unterschieden: First-Hop-Router und Last-Hop-Router. Ein First-Hop-Router ist definiert als Router, der direkt mit Multicast IGMP- bzw. MLD-Clients bzw. Empfängern verbunden ist. Ein Last-Hop-Router ist definiert als Router, der direkt mit der Multicast-Quelle verbunden ist. Darüber hinaus gibt es noch Router, die zwischen den beiden anderen Router-Rollen geschaltet sein können. PIM muss grundsätzlich auf allen Interfaces aktiviert werden, auf denen Multicast-Routing durchgeführt werden soll. Auf Client-Interfaces muss IGMP bzw. MLD aktiviert sein.

Die folgenden PIM-Funktionen werden vom LCOS unterstützt:

- PIM Sparse Mode (ASM) mit externem RP von einem Drittheersteller
- Statische Konfiguration des RPs bei PIM Sparse Mode
- PIM SSM in den Rollen als Last-Hop-Router sowie First-Hop-Router
- Unterstützung von IPv4 und IPv6 PIM
- SSM Mapping, wobei aus IGMPv2- bzw. MLD-Nachrichten PIM SSM-Joins erzeugt werden
- PIM nativ über IPSec VPN ohne GRE-Tunnel

Die folgenden PIM-Funktionen werden nicht unterstützt:

- Rolle als Rendezvous Point (RP)
- Rolle als First-Hop-Router bei PIM Sparse, der einen automatischen Register-Unicast-Tunnel erzeugt, um beim RP eine Multicast-Quelle zu registrieren
- Dense Mode, Bi-Dir Mode
- Dynamische RP-Konfiguration, z. B. über Bootstrap Router (BSR) Funktion

PIM Show-Kommandos

Die folgenden Show Kommandos stehen für PIM zur Verfügung:

- PIM IPv4-Groups: Zeigt Informationen über beigetretene IPv4 Multicast Gruppen
- PIM IPv6-Groups: Zeigt Informationen über beigetretene IPv6 Multicast Gruppen
- PIM IPv4-Hello: Zeigt erweiterte Informationen über PIM-Nachbarn und PIM Hello-State auf IPv4-Interfaces
- PIM IPv6-Hello: Zeigt erweiterte Informationen über PIM-Nachbarn und PIM Hello-State auf IPv6-Interfaces
- PIM IPv4-Neighbors: Zeigt einen kompakten Überblick über PIM-Nachbarn auf IPv4-Interfaces. Optional kann über den Parameter `[-s] [--skip-own-info]` die Ausgabe des eigenen Interfaces in der Ausgabe weggelassen werden.

- PIM IPv6-Neighbors: Zeigt einen kompakten Überblick über PIM-Nachbarn auf IPv6-Interfaces. Optional kann über den Parameter `[-s] [--skip-own-info]` die Ausgabe des eigenen Interfaces in der Ausgabe weggelassen werden.

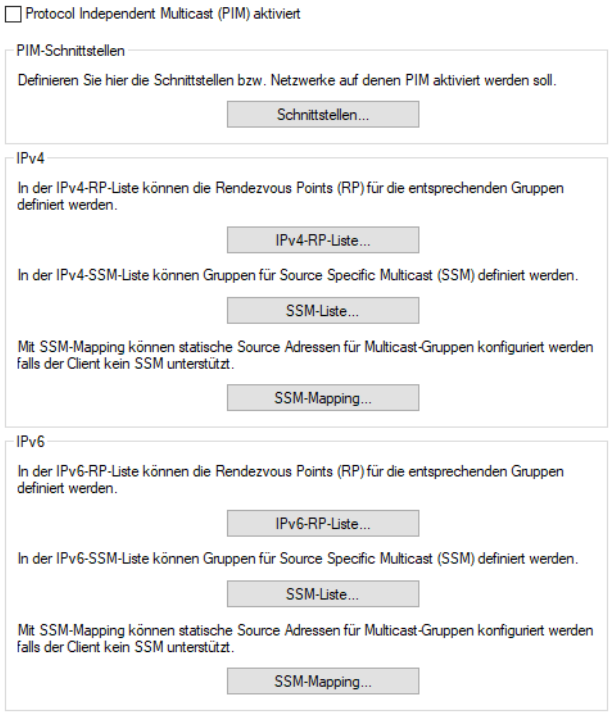
Beispiel für notwendige Konfigurationsschritte

Für ein einfaches Szenario mit PIM SSM sind folgende Konfigurationsschritte notwendig:

1. PIM global aktivieren
2. Für alle Interfaces, die am Multicast-Routing beteiligt sind, inkl. Client-Interfaces und Source-Interface, muss ein Eintrag in der PIM-Schnittstellen-Tabelle erfolgen. Die Default-Werte können übernommen werden.
3. Um SSM zu aktivieren, muss ein Eintrag in der IPv4- bzw. IPv6-SSM-Tabelle angelegt werden. Die Default-Werte können übernommen werden.

Konfiguration

Um PIM mit LANconfig zu konfigurieren, wechseln Sie in die Ansicht **Multicast** > **PIM**.



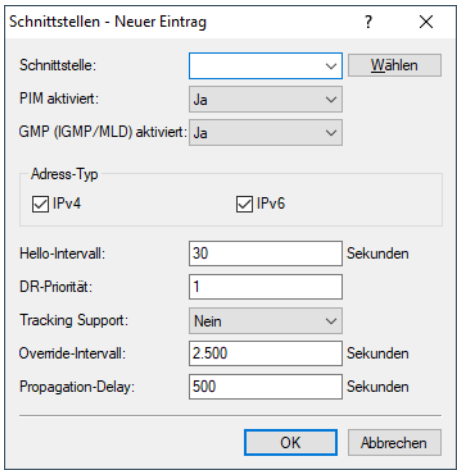
Protocol Independent Multicast (PIM) aktiviert

Aktiviert bzw. deaktiviert PIM auf dem Gerät.

7.5.1 Schnittstellen

In LANconfig konfigurieren Sie die Schnittstellen unter **Multicast** > **PIM** > **PIM-Schnittstellen** über **Schnittstellen**. In dieser Tabelle werden die Interfaces bzw. logischen Netzwerke definiert, auf denen PIM aktiviert werden soll. Ebenso werden die Interfaces definiert, auf denen Clients per IGMP bzw. MLD Multicast-Gruppen beitreten können. Für alle

Interfaces, die am Multicast-Routing beteiligt sind, inkl. Client-Interfaces und Source-Interface, muss ein Eintrag in der PIM-Schnittstellen-Tabelle erfolgen.



Schnittstelle

Name des logischen Interfaces auf dem PIM bzw. GMP (Group Management Protokoll wie IGMP oder MLD) aktiviert werden soll. Mögliche Werte sind IPv4-Netzwerke, z. B. INTRANET, WAN-Gegenstellen, Wildcard-Einträge mit * für IPv4-RAS-Interfaces, z. B. „VPN*“. Weitere mögliche Werte sind IPv6-Interfaces sowie IPv6 RAS-Templates.

PIM aktiviert

Aktiviert PIM sowie das Senden und Empfangen von PIM-Nachrichten auf diesem logischen Interface. Wenn nur IGMP- / MLD-Clients bzw. Multicast-Empfänger auf dieser Schnittstelle vorhanden sind, kann somit das Senden bzw. Empfangen von PIM-Nachrichten explizit deaktiviert werden. In diesem Fall muss nur GMP (IGMP / MLD) aktiviert sein.

GMP (IGMP / MLD) aktiviert

Aktiviert die IGMP- bzw. MLD-Routerrolle auf diesem logischen Interface. In diesem Fall werden IGMP- bzw. MLD-Joins von Clients akzeptiert. Auf Interfaces bei denen keine Clients im Netzwerk, sondern nur PIM-Nachbar-Router vorhanden sind, kann GMP deaktiviert werden. IGMP- / MLD-Joins werden in diesem Fall dann nicht akzeptiert.

Adress-Typ

Hier definieren Sie, für welche Adressfamilie PIM bzw. GMP auf diesem Interface aktiviert werden soll. Bei Bedarf können Sie auch beide Adressfamilienn gleichzeitig aktivieren. Mögliche Werte: IPv4, IPv6

Hello-Intervall

Definiert die Zeit in Sekunden zwischen der Wiederholung von regelmäßigen PIM Hello-Nachrichten. Die Haltezeit ist automatisch das 3,5-fache des PIM-Hello-Intervalls und nicht separat konfigurierbar.

Mögliche Werte: 0-255 Sekunden, Default: 30. Der Wert 0 deaktiviert das Senden von Hello-Nachrichten.

DR-Priorität

Definiert die Priorität als Designated Router (DR) im Prozess der DR-Wahl von PIM. Ein höherer Wert bedeutet eine höhere Priorität im DR-Wahlverfahren zum Designated Router (DR).

Mögliche Werte: 0 bis 2^{32}, Default: 1.

Tracking Support

Beeinflusst das Setzen des „T-Bits“ in der LAN-Prune-Delay-Option in ausgehenden Hello-Nachrichten.

Mögliche Werte: Ja, Nein, Default: Nein.

Override Intervall

Beeinflusst das Setzen des Override-Intervall-Felds in der LAN-Prune-Delay-Option in ausgehenden Hello-Nachrichten. Definiert die maximale Verzögerung für die Übertragung von Override-Join-Nachrichten für Multicast-Netzwerke, die Join-Supression aktiviert haben.

Mögliche Werte: 0 bis 2^{32}, Default: 0.

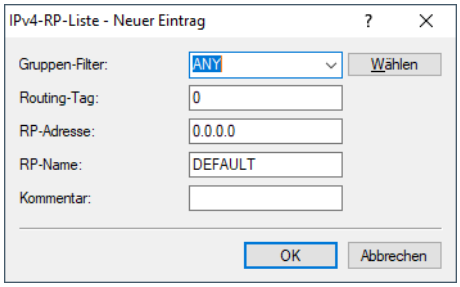
Propagation-Delay

Konfiguriert das Setzen des Propagation-Delay-Felds in gesendeten Hello-Nachrichten der LAN-Prune-Delay-Option. Definiert die Verzögerung für das Versenden von PIM Prune-Nachrichten auf dem Upstream-Router in einem Multicast-Netzwerk, in dem Join-Unterdrückung aktiviert ist.

Mögliche Werte: 250-2000 Millisekunden, Default: 500.

7.5.2 IPv4-RP-Liste

In LANconfig konfigurieren Sie die IPv4-RP-Liste unter **Multicast** > **PIM** > **IPv4** über **IPv4-RP-Liste**. In dieser Tabelle werden die IPv4 Rendezvous Points (RPs) sowie die zugehörigen Multicastgruppen für den PIM Sparse Mode konfiguriert.



Gruppen-Filter

Definiert die Multicast-Gruppen, für die der Rendezvous Points zuständig sein soll. Adressen, die auf den Gruppen-Filter passen, werden von diesem Rendezvous Point verwaltet. Referenziert eine Filterliste aus der Tabelle **Multicast** > **Allgemein** > **IPv4-Filterlisten**.

Routing-Tag

Routing-Tag, das verwendet werden soll um diesen Rendezvous Point zu erreichen.

RP-Adresse

IPv4-Adresse des externen Rendezvous Points. Das Gerät selbst unterstützt nicht die Rolle eines Rendezvous Points.

RP-Name

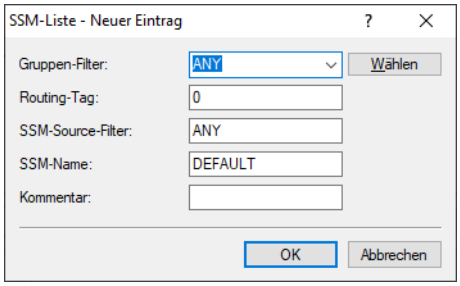
Name des Rendezvous Points.

Kommentar

Vergeben Sie optional einen sinnvollen Kommentar als Beschreibung.

7.5.3 IPv4-SSM-Liste

In LANconfig konfigurieren Sie die IPv4-SSM-Liste unter **Multicast** > **PIM** > **IPv4** über **SSM-Liste**. In dieser Tabelle werden die Parameter für PIM SSM (Source Specific Multicast) Mode konfiguriert.



Gruppen-Filter

Definiert die Multicast-Gruppen, für die diese SSM-Konfiguration gelten soll. Adressen, die auf den Gruppen-Filter passen, werden auf diese SSM-Konfiguration angewendet. Referenziert eine Filterliste aus der Tabelle **Multicast** > **Allgemein** > **IPv4-Filterlisten**.

Routing-Tag

Routing-Tag, für den diese Konfiguration gelten soll.

SSM-Source-Filter

Definiert den SSM-Source-Filter für diesen Tabellen-Eintrag. Nur Multicast-Quell-Adressen, die auf den SSM-Source-Filter passen, werden auf diese SSM-Konfiguration angewendet. Referenziert eine Filterliste aus der Tabelle **Multicast** > **IGMP / MLD** > **Internet Group Management Protocol (IGMP)** > **SSM-Quell-IP-Liste**.

SSM-Name

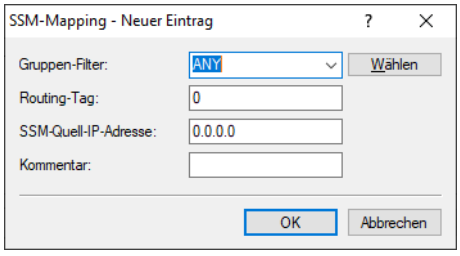
Name dieser SSM-Konfiguration.

Kommentar

Vergeben Sie optional einen sinnvollen Kommentar als Beschreibung.

7.5.4 IPv4-SSM-Mapping

In LANconfig konfigurieren Sie das IPv4-SSM-Mapping unter **Multicast** > **PIM** > **IPv4** über **SSM-Mapping**. In dieser Tabelle können IPv4 Multicast Quell-Adressen (S) konfiguriert werden, die automatisch in PIM-Join-Nachrichten eingefügt werden sollen, falls in empfangenen IGMP-Nachrichten keine Quell-Adressen (S) vorhanden sind. Somit werden (*,G)-Einträge vom Router automatisch zu (S,G)-Einträgen ergänzt.



Gruppen-Filter

Definiert die Multicast-Gruppen (G) für die dieses SSM-Mapping durchgeführt werden soll. Referenziert eine Filterliste aus der Tabelle **Multicast** > **Allgemein** > **IPv4-Filterlisten**.

Routing-Tag

Routing-Tag für das diese Konfiguration gelten soll.

SSM-Quell-IP-Adresse

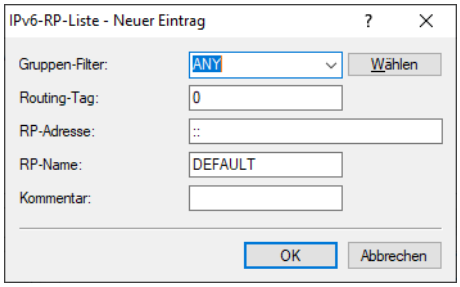
Definiert eine Quell-IPv4-Adresse (S), die automatisch in PIM-Join-Nachrichten für (*,G)-Einträge eingefügt werden soll und automatisch zu (S,G)-Einträge ergänzt werden soll.

Kommentar

Vergeben Sie optional einen sinnvollen Kommentar als Beschreibung.

7.5.5 IPv6-RP-Liste

In LANconfig konfigurieren Sie die IPv6-RP-Liste unter **Multicast** > **PIM** > **IPv6** über **IPv6-RP-Liste**. In dieser Tabelle werden die Rendezvous Points (RPs) sowie die zugehörigen Multicastgruppen für den PIM Sparse Mode konfiguriert.



Gruppen-Filter

Definiert die Multicast-Gruppen, für die der Rendezvous Points zuständig sein soll. Adressen, die auf den Gruppen-Filter passen, werden von diesem Rendezvous Point verwaltet. Referenziert eine Filterliste aus der Tabelle **Multicast** > **Allgemein** > **IPv6-Filterlisten**.

Routing-Tag

Routing-Tag, das verwendet werden soll um diesen Rendezvous Point zu erreichen.

RP-Adresse

IPv6-Adresse des externen Rendezvous Points. Das Gerät selbst unterstützt die Rolle eines Rendezvous Points nicht.

RP-Name

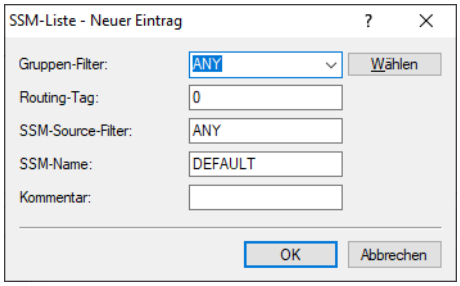
Name des Rendezvous Points.

Kommentar

Vergeben Sie optional einen sinnvollen Kommentar als Beschreibung.

7.5.6 IPv6-SSM-Liste

In LANconfig konfigurieren Sie die IPv6-SSM-Liste unter **Multicast** > **PIM** > **IPv6** über **SSM-Liste**. In dieser Tabelle werden die Parameter für PIM IPv6 SSM (Source Specific Multicast) Mode konfiguriert.



Gruppen-Filter

Definiert die Multicast-Gruppen, für die diese SSM-Konfiguration gelten soll. Adressen, die auf den Gruppen-Filter passen, werden auf diese SSM-Konfiguration angewendet. Referenziert eine Filterliste aus der Tabelle **Multicast** > **Allgemein** > **IPv6-Filterlisten**.

Routing-Tag

Routing-Tag, für den diese Konfiguration gelten soll.

SSM-Source-Filter

Definiert den SSM-Source-Filter für diesen Tabellen-Eintrag. Nur Multicast-Quell-Adressen, die auf den SSM-Source-Filter passen, werden auf diese SSM-Konfiguration angewendet. Referenziert eine Filterliste aus der Tabelle **Multicast** > **IGMP / MLD** > **Internet Group Management Protocol (IGMP)** > **SSM-Quell-IP-Liste**.

SSM-Name

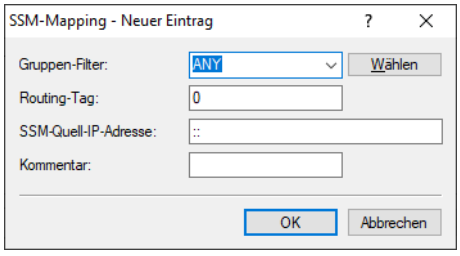
Name dieser SSM-Konfiguration.

Kommentar

Vergeben Sie optional einen sinnvollen Kommentar als Beschreibung.

7.5.7 IPv6-SSM-Mapping

In LANconfig konfigurieren Sie das IPv6-SSM-Mapping unter **Multicast** > **PIM** > **IPv6** über **SSM-Mapping**. In dieser Tabelle können IPv6 Multicast Quell-Adressen (S) konfiguriert werden, die automatisch in PIM-Join-Nachrichten eingefügt werden sollen, falls in empfangenen MLD-Nachrichten keine Quell-Adressen vorhanden sind. Somit werden (*,G) Einträge vom Router automatisch zu (S,G) ergänzt.



Gruppen-Filter

Definiert die Multicast-Gruppen (G) für die dieses SSM-Mapping durchgeführt werden soll. Referenziert eine Filterliste aus der Tabelle **Multicast** > **Allgemein** > **IPv6-Filterlisten**.

Routing-Tag

Routing-Tag für das diese Konfiguration gelten soll.

SSM-Quell-IP-Adresse

Definiert eine Quell-IPv6-Adresse (S), die automatisch in PIM-Join-Nachrichten für (*,G)-Einträge eingefügt werden soll und automatisch zu (S,G)-Einträge ergänzt werden soll.

Kommentar

Vergeben Sie optional einen sinnvollen Kommentar als Beschreibung.

7.6 Ergänzungen im Setup-Menü

7.6.1 Multicast

Hier finden Sie die Einstellungen zu Mulitcast-Protokollen.

SNMP-ID:

2.108

Pfad Konsole:

Setup

IGMP

Hier finden Sie die Einstellungen zum Internet Group Management Protocol (IGMP).

SNMP-ID:

2.108.1

Pfad Konsole:

Setup > **Multicast**

IGMP-Proxy

Ein IGMP-Proxy wird in der Regel bei Interzugängen mit Multicast IPTV verwendet. Dabei senden Clients bzw. IPTV Set-Top-Boxen (STBs) im lokalen Netz IGMP-Nachrichten, um einen bestimmten TV-Kanal zu empfangen. Dazu treten sie bestimmten Multicast-Gruppen bei und verlassen diese auch wieder. Der Router bzw. die IGMP-Proxy-Funktionalität empfängt die IGMP-Nachrichten und leitet sie an das Provider-Netzwerk weiter bzw. filtert die Gruppen bei Bedarf. Der IGMP-Proxy arbeitet dabei als Stellvertreter für das lokale Netzwerk mit seinen Clients.

Ein IGMP-Proxy kann auch in einfachen Multicast-Routing Szenarien beispielsweise über VPN verwendet werden ohne dass PIM verwendet werden muss. Durch die Konfiguration des IGMP-Proxies wird eine statische (Baum-)Struktur ohne alternative Pfade bzw. Redundanz sowie Loop-Verhinderung erzeugt. IGMP-Proxies können durch eine Reihenschaltung mehrerer Router „kaskadiert“ werden.

SNMP-ID:

2.108.1.1

Pfad Konsole:

Setup > **Multicast** > **IGMP**

Downstream-Interface

Interface-Name auf dem IGMP-Clients Gruppen beitreten können und IGMP-Nachrichten vom Proxy empfangen werden. Mögliche Werte sind IPv4-Netzwerke, z. B. INTRANET, IPv4-(WAN)-Gegenstellen. Ebenfalls sind Wildcard-Einträge mit * für RAS-Interfaces erlaubt, z. B. „VPN*“.

Bei Provider-basierten IPTV-Szenarien muss hier das lokale Netzwerk, z. B. INTRANET, konfiguriert werden.

SNMP-ID:

2.108.1.1.1

Pfad Konsole:

Setup > **Multicast** > **IGMP** > **IGMP-Proxy**

Mögliche Werte:

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

Upstream-Interface

Interface Name auf dem IGMP-Nachrichten vom Proxy stellvertretend für Clients gesendet werden. Die Quelle der Multicast-Nachrichten muss über dieses Interface erreicht werden. Mögliche Werte sind IPv4-Netzwerke, z. B. INTRANET sowie IPv4-(WAN)-Gegenstellen.

Bei Provider-basierten IPTV-Szenarien muss hier die WAN-Gegenstelle, z. B. INTERNET, konfiguriert werden.

SNMP-ID:

2.108.1.1.2

Pfad Konsole:

Setup > **Multicast** > **IGMP** > **IGMP-Proxy**

Mögliche Werte:

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

Gruppen-Filter

Name des Gruppenfilters der für diesen Proxy gelten soll. Referenziert die Tabelle *IPv4-Filter-Tabelle*. Standardmäßig ist der Filtereintrag leer bzw. verweist auf die Filterliste „ANY“, die alle Multicast-Gruppen erlaubt. Mit Hilfe des Gruppenfilters können die möglichen Multicast-Gruppen für Clients eingeschränkt werden.

SNMP-ID:

2.108.1.1.3

Pfad Konsole:

Setup > **Multicast** > **IGMP** > **IGMP-Proxy**

Mögliche Werte:

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

SSM-Bereiche

Definiert den IP-Adressbereich in Präfixschreibweise der für SSM verwendet wird.

SNMP-ID:

2.108.1.3

Pfad Konsole:

Setup > **Multicast** > **IGMP**

Praefix

Diese Präfixe definieren den IPv4-Adressbereich, der für SSM verwendet wird.

SNMP-ID:

2.108.1.3.1

Pfad Konsole:

Setup > **Multicast** > **IGMP** > **SSM-Bereiche**

Mögliche Werte:

max. 18 Zeichen aus `[0-9]./`

SSM-Quell-IP-Liste

In dieser Tabelle können Listen von gewünschten oder unerwünschten (Unicast) Quell-IP-Adressen definiert werden. Diese können an verschiedenen Stellen referenziert werden und über diese Tabelle global verwaltet werden. Eine Liste wird durch den mehrere Einträge mit gleichem Namen definiert.

SNMP-ID:

2.108.1.4

Pfad Konsole:

Setup > **Multicast** > **IGMP**

Name

Vergeben Sie einen Namen für den Eintrag. Eine Liste wird durch den mehrere Einträge mit gleichem Namen definiert.

SNMP-ID:

2.108.1.4.1

Pfad Konsole:

Setup > **Multicast** > **IGMP** > **SSM-Quell-IP-Liste**

Mögliche Werte:

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

IP-Adresse

Unicast Quell-IP-Adresse. Multicast-Adressen sind an dieser Stelle keine gültige Eingabe, da hier die Quell-IP-Adressen (Source) eines Multicast-Eintrag (S,G) definiert werden.

SNMP-ID:

2.108.1.4.2

Pfad Konsole:

Setup > **Multicast** > **IGMP** > **SSM-Quell-IP-Liste**

Mögliche Werte:

max. 15 Zeichen aus `[0-9].`

Statische-Routen

Statisches Multicast Routing kann verwendet werden, wenn Multicast Clients kein IGMP beherrschen bzw. für Szenarien, in dem Multicast-Datenverkehr immer fließen muss, ohne dass Clients die entsprechende Gruppe anfordern. Der Router erzeugt ab dem Anlegen des Eintrags auf dem Upstream-Interface IGMP Joins bzw. Gruppenreporte.

Bitte beachten Sie, dass ein statisches Multicast Routing hohen Datenverkehr und Last verursachen kann, da die Multicast-Daten immer weitergeleitet werden.

SNMP-ID:

2.108.1.5

Pfad Konsole:

Setup > **Multicast** > **IGMP**

Upstream-Interface

Interface Name auf dem die Multicast-Pakete den Router erreichen. Mögliche Werte sind IPv4-Netzwerke, z. B. INTRANET sowie IPv4-(WAN)-Gegenstellen.

SNMP-ID:

2.108.1.5.1

Pfad Konsole:

Setup > **Multicast** > **IGMP** > **Statische-Routen**

Mögliche Werte:

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

Gruppe

Multicast-Gruppe für die das statische Weiterleiten von Multicast-Daten angelegt werden soll, z. B. 239.0.0.1.

SNMP-ID:

2.108.1.5.2

Pfad Konsole:

Setup > **Multicast** > **IGMP** > **Statische-Routen**

Mögliche Werte:

max. 15 Zeichen aus `[0-9].`

Downstream-Interface

Interface Name auf dem die Multicast-Pakete den Router verlassen sollen. Mögliche Werte sind IPv4-Netzwerke, z. B. INTRANET sowie IPv4-(WAN)-Gegenstellen.

SNMP-ID:

2.108.1.5.3

Pfad Konsole:

Setup > **Multicast** > **IGMP** > **Statische-Routen**

Mögliche Werte:

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

Modus

Falls SSM verwendet werden soll: Steuert, über welche Methode Quelladressen der Multicast-Quellen in einem IGMP-Membership-Report angefordert werden sollen.

Wenn eine SSM-Gruppe mit beliebigen Quelladressen verwendet werden soll, so muss bei Modus „Exclude“ und SSM-Quell-IP-Liste „ANY“ verlinkt werden.

SNMP-ID:

2.108.1.5.4

Pfad Konsole:

Setup > **Multicast** > **IGMP** > **Statische-Routen**

Mögliche Werte:

Include

Es wird ein IGMP-Membership Report mit Record-Type „Change to Include Mode“ gesendet. Die Einträge aus der SSM-Quell-IP-Liste werden als gewünschte Quelladressen gesendet. Eine Kombination mit Einstellung „Include“ und SSM-Quell-IP-Liste mit Eintrag „ANY“ führt zu keinem sinnvollen Ergebnis und wird als Konfiguration intern nicht akzeptiert, da alle Quell-IP-Adressen abgelehnt werden würden.

Exclude

Es wird ein IGMP-Membership Report mit Record-Type „Change to Exclude Mode“ gesendet. Wenn die Quell-Liste den Eintrag „ANY“ bzw. „0.0.0.0“ enthält, d. h. alle Quellen erlaubt, so wird ein IGMP-Membership Report mit Join Group für „any sources“ gesendet. Wenn die Liste einen anderen Eintrag als 0.0.0.0 enthält wird ein IGMP Membership Report „block sources“ mit der entsprechenden IP-Adresse gesendet.

SSM-Quell-IP-Liste

Falls SSM verwendet werden soll, kann hier eine Liste von gewünschten Quellen zusätzlich zur Multicast-Gruppe definiert werden. Sollen alle Quellen zugelassen werden, kann die vordefinierte Liste „ANY“ mit dem Eintrag „0.0.0.0“ verwendet werden.

SNMP-ID:

2.108.1.5.5

Pfad Konsole:

Setup > **Multicast** > **IGMP** > **Statische-Routen**

Mögliche Werte:

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

Parameter

Hier finden Sie die Einstellungen zu den allgemeinen IGMP-Parametern.

SNMP-ID:

2.108.1.6

Pfad Konsole:

Setup > **Multicast** > **IGMP**

Interface

Schnittstellenname, für den die IGMP-Konfiguration gilt. Der Eintrag mit dem Namen DEFAULT gilt für alle Schnittstellen, die keinen spezifischen Eintrag haben. Falls der Eintrag DEFAULT nicht vorhanden ist, gelten interne Default-Werte die den Werten des DEFAULT-Eintrags entsprechen. Mögliche Werte sind DEFAULT, IPv4-Netzwerke, z. B. INTRANET oder IPv4-(WAN)-Gegenstellen. Ebenfalls sind Wildcard-Einträge mit * für RAS-Interfaces erlaubt, z. B. „VPN*“.

SNMP-ID:

2.108.1.6.1

Pfad Konsole:

Setup > **Multicast** > **IGMP** > **Parameter**

Mögliche Werte:

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

Robustness-Variable

Anzahl der Wiederholungen von IGMP-Nachrichten.

SNMP-ID:

2.108.1.6.2

Pfad Konsole:

Setup > **Multicast** > **IGMP** > **Parameter**

Mögliche Werte:

1 … 10

Default-Wert:

2

Unsolicited-Report-Interval

Definiert die Zeit in Sekunden zwischen den Wiederholungen von Membership-Reports nach dem das Gerät in der Host-Rolle den erstmaligen Membership-Report in einer Gruppe gesendet hat.

SNMP-ID:

2.108.1.6.3

Pfad Konsole:

Setup > **Multicast** > **IGMP** > **Parameter**

Mögliche Werte:

1 … 25

Default-Wert:

2

Query-Interval

Intervall zwischen IGMP General-Query-Nachrichten.

SNMP-ID:

2.108.1.6.4

Pfad Konsole:

Setup > **Multicast** > **IGMP** > **Parameter**

Mögliche Werte:

2 … 99999

Default-Wert:

125

Query-Response-Interval

Maximale Antwortzeit in Millisekunden. Aus dieser wird der Wert Maximum Response Time berechnet, der in periodischen General-Query-Nachrichten gesetzt wird. Der Wert Query-Response-Intervall muss kleiner als der Wert für Query-Intervall sein.

SNMP-ID:

2.108.1.6.5

Pfad Konsole:

Setup > **Multicast** > **IGMP** > **Parameter**

Mögliche Werte:

1 … 999999

Default-Wert:

10000

Startup-Query-Interval

Intervall in Sekunden zwischen IGMP General-Query-Nachrichten beim Start des IGMP-Queriers.

SNMP-ID:

2.108.1.6.6

Pfad Konsole:

Setup > **Multicast** > **IGMP** > **Parameter**

Mögliche Werte:

1 … 99998

Default-Wert:

30

Startup-Query-Count

Anzahl an IGMP General-Query-Nachrichten, die beim Start gesendet werden, unterbrochen bzw. zeitlich verzögert vom Startup-Query-Intervall.

SNMP-ID:

2.108.1.6.7

Pfad Konsole:

Setup > **Multicast** > **IGMP** > **Parameter**

Mögliche Werte:

1 … 10

Default-Wert:

2

Last-Listener-Query-Interval

Definiert den Wert in Sekunden der Maximum Response Time in Multicast-Address-Specific Queries, die als Antwort auf Done-Nachrichten gesendet werden. Der Parameter definiert ebenso die Zeit zwischen Multicast-Address-Specific-Query-Nachrichten.

SNMP-ID:

2.108.1.6.8

Pfad Konsole:

Setup > **Multicast** > **IGMP** > **Parameter**

Mögliche Werte:

1 … 25

Default-Wert:

2

Last-Listener-Query-Count

Anzahl von gesendeten Nachrichten vom Typ Multicast-Address-Specific Query bevor der Router annimmt, dass es keine lokalen Empfänger mehr gibt. Definiert ebenso die Anzahl an gesendeten Nachrichten vom Typ Multicast-Address-Specific-Query bevor der Router annimmt, dass es keine weiteren Empfänger für eine spezielle Quelle gibt.

SNMP-ID:

2.108.1.6.9

Pfad Konsole:

Setup > **Multicast** > **IGMP** > **Parameter**

Mögliche Werte:

1 … 10

Default-Wert:

2

IGMP-Kompatibilitaets-Modus

IGMP-Version, in der das Gerät in der Rolle als Multicast-Router arbeitet.

SNMP-ID:

2.108.1.6.10

Pfad Konsole:

Setup > **Multicast** > **IGMP** > **Parameter**

Mögliche Werte:

Aus
V1
V2
V3

Default-Wert:

V3

Quick-Leave

Erlaubt das schnelle Verlassen von Multicast Gruppen. Sollte nur verwendet werden, falls es nur einen Empfänger pro Gruppe auf dem Interface gibt. Intern wird der Parameter Last-Listener-Query-Count auf 1 und das Last-Listener-Query-Intervall auf 20 ms gesetzt.

SNMP-ID:

2.108.1.6.11

Pfad Konsole:

Setup > **Multicast** > **IGMP** > **Parameter**

Mögliche Werte:

Nein
Ja

Default-Wert:

Nein

Check-Router-Alert

Definiert, ob in empfangenen IGMP-Nachrichten überprüft werden soll, ob die Router-Alert-Option vorhanden ist. Laut RFC sollen IGMP-Pakete verworfen werden, bei denen die Router-Alert-Option fehlt. Der Schalter dient zur Herstellung der Kompatibilität mit fehlerhaften Client-Implementierungen.

SNMP-ID:

2.108.1.7

Pfad Konsole:

Setup > **Multicast** > **IGMP**

Mögliche Werte:

Nein
Ja

Default-Wert:

Ja

Statistiken-Erfassen

Definiert, ob erweiterte IPv4-Multicast-Statistiken gesammelt werden sollen. Das Sammeln dieser Statistiken beeinflusst ggf. die Performance des Geräts.

SNMP-ID:

2.108.1.8

Pfad Konsole:

Setup > **Multicast** > **IGMP**

Mögliche Werte:

Nein
Ja

Default-Wert:

Nein

Static-Join

In dieser Tabelle können IPv4-Multicast-Gruppen definiert werden, denen das Gerät zu Testzwecken auf Client-Interfaces durch IGMP beitreten kann. Damit können im Test Multicast-Clients simuliert werden, die bestimmten IGMP-Gruppen beitreten. Das entsprechende Client-Interface muss Teil der IGMP-Proxy oder PIM-Konfiguration sein. Der eingehende Multicast-Datenverkehr wird dann vom Gerät verarbeitet und verworfen. Diese Funktion ist nicht für den dauerhaften Betrieb in produktiven Szenarien geeignet.

SNMP-ID:

2.108.1.9

Pfad Konsole:

Setup > **Multicast** > **IGMP**

Interface

(Client-)Interface-Name auf dem der Multicast Client simuliert werden soll.

SNMP-ID:

2.108.1.9.1

Pfad Konsole:

Setup > **Multicast** > **IGMP** > **Static-Join**

Mögliche Werte:

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

Gruppe

IPv4-Multicast-Gruppe der das Gerät statisch beitreten soll.

SNMP-ID:

2.108.1.9.2

Pfad Konsole:

Setup > **Multicast** > **IGMP** > **Static-Join**

Mögliche Werte:

max. 15 Zeichen aus `[0-9].`

Kommentar

Vergeben Sie optional einen sinnvollen Kommentar als Beschreibung.

SNMP-ID:

2.108.1.9.3

Pfad Konsole:

Setup > **Multicast** > **IGMP** > **Static-Join**

Mögliche Werte:

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

MLD

Hier finden Sie die Einstellungen zum Multicast Listener Discovery (MLD).

SNMP-ID:

2.108.2

Pfad Konsole:

Setup > **Multicast**

MLD-Proxy

Ein MLD-Proxy wird in der Regel bei Interzugängen mit Multicast IPTV über IPv6 verwendet. Dabei senden Clients bzw. IPTV Set-Top-Boxen (STBs) im lokalen Netz MLD-Nachrichten um einen bestimmten TV-Kanal zu empfangen. Dazu treten sie bestimmten Multicast-Gruppen bei und verlassen diese auch wieder. Der Router bzw. die MLD-Proxy-Funktionalität empfängt die MLD-Nachrichten und leitet sie an das Provider-Netzwerk weiter bzw. filtert die Gruppen bei Bedarf. Der MLD-Proxy arbeitet dabei als Stellvertreter für das lokale Netzwerk mit seinen Clients.

Ein MLD-Proxy kann auch in einfachen Multicast-Routing Szenarien beispielsweise über VPN verwendet werden ohne dass PIM verwendet werden muss. Durch die Konfiguration des MLD-Proxies wird eine statische (Baum-)Struktur ohne alternative Pfade bzw. Redundanz sowie Loop-Verhinderung erzeugt. MLD-Proxies können durch eine Reihenschaltung mehrerer Router „kaskadiert" werden.

SNMP-ID:

2.108.2.1

Pfad Konsole:

Setup > **Multicast** > **MLD**

Downstream-Interface

Interface-Name auf dem MLD-Clients Gruppen beitreten können und MLD-Nachrichten vom Proxy empfangen werden. Mögliche Werte sind IPv6-Netzwerke, z. B. INTRANET, IPv6-(WAN)-Gegenstellen oder RAS-Templates.

Bei Provider-basierten IPTV-Szenarien muss hier das lokale Netzwerk, z. B. INTRANET, konfiguriert werden.

SNMP-ID:

2.108.2.1.1

Pfad Konsole:

Setup > **Multicast** > **MLD** > **MLD-Proxy**

Mögliche Werte:

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

Upstream-Interface

Interface Name auf dem MLD-Nachrichten vom Proxy stellvertretend für Clients gesendet werden. Die Quelle der Multicast-Nachrichten muss über dieses Interface erreicht werden. Mögliche Werte sind IPv6-Netzwerke, z. B. INTRANET sowie IPv6-(WAN)-Gegenstellen.

Bei Provider-basierten IPTV-Szenarien muss hier die WAN-Gegenstelle, z. B. INTERNET, konfiguriert werden.

SNMP-ID:

2.108.2.1.2

Pfad Konsole:

Setup > **Multicast** > **MLD** > **MLD-Proxy**

Mögliche Werte:

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

Gruppen-Filter

Name des Gruppenfilters, der für diesen Proxy gelten soll. Referenziert die Tabelle *IPv6-Filter-Tabelle*. Standardmäßig ist der Filtereintrag leer bzw. verweist auf die Filterliste „ANY“, die alle Multicast-Gruppen erlaubt. Mit Hilfe des Gruppenfilters können die möglichen Multicast-Gruppen für Clients eingeschränkt werden.

SNMP-ID:

2.108.2.1.3

Pfad Konsole:

Setup > **Multicast** > **MLD** > **MLD-Proxy**

Mögliche Werte:

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

SSM-Bereiche

Definiert den IP-Adressbereich in Präfixschreibweise der für SSM verwendet wird.

SNMP-ID:

2.108.2.3

Pfad Konsole:

Setup > **Multicast** > **MLD**

Praefix

Diese Präfixe definieren den IP-Adressbereich, der für SSM verwendet wird.

SNMP-ID:

2.108.2.3.1

Pfad Konsole:

Setup > **Multicast** > **MLD** > **SSM-Bereiche**

Mögliche Werte:

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

SSM-Quell-IP-Liste

In dieser Tabelle können Listen von gewünschten oder unerwünschten (Unicast) Quell-IP-Adressen definiert werden. Diese können an verschiedenen Stellen referenziert werden und über diese Tabelle global verwaltet werden. Eine Liste wird durch mehrere Einträge mit gleichem Namen definiert.

SNMP-ID:

2.108.2.4

Pfad Konsole:

Setup > **Multicast** > **MLD**

Name

Vergeben Sie einen Namen für den Eintrag. Eine Liste wird durch den mehrere Einträge mit gleichem Namen definiert.

SNMP-ID:

2.108.2.4.1

Pfad Konsole:

Setup > **Multicast** > **MLD** > **SSM-Quell-IP-Liste**

Mögliche Werte:

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

IP-Adresse

Unicast Quell-IP-Adresse. Multicast-Adressen sind an dieser Stelle keine gültige Eingabe, da hier die Quell-IP-Adressen (Source) eines Multicast-Eintrag (S,G) definiert werden.

SNMP-ID:

2.108.2.4.2

Pfad Konsole:

Setup > **Multicast** > **MLD** > **SSM-Quell-IP-Liste**

Mögliche Werte:

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

Statische-Routen

Statisches Multicast Routing kann verwendet werden, wenn Multicast Clients kein MLD beherrschen bzw. für Szenarien, in dem Multicast-Datenverkehr immer fließen muss, ohne dass Clients die entsprechende Gruppe anfordern. Der Router erzeugt ab dem Anlegen des Eintrags auf dem Upstream-Interface MLD Gruppenreporte.

Bitte beachten Sie, dass ein statisches Multicast Routing hohen Datenverkehr und Last verursachen kann, da die Multicast-Daten immer weitergeleitet werden.

SNMP-ID:

2.108.2.5

Pfad Konsole:

Setup > **Multicast** > **MLD**

Upstream-Interface

Interface Name auf dem die Multicast-Pakete den Router erreichen. Mögliche Werte sind IPv6-Netzwerke, z. B. INTRANET sowie IPv6-(WAN)-Gegenstellen.

SNMP-ID:

2.108.2.5.1

Pfad Konsole:

Setup > **Multicast** > **MLD** > **Statische-Routen**

Mögliche Werte:

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

Gruppe

Multicast-Gruppe für die das statische Weiterleiten von Multicast-Daten angelegt werden soll, beispielsweise „ff09::1".

SNMP-ID:

2.108.2.5.2

Pfad Konsole:

Setup > **Multicast** > **MLD** > **Statische-Routen**

Mögliche Werte:

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

Downstream-Interface

Interface Name auf dem die Multicast-Pakete den Router verlassen sollen. Mögliche Werte sind IPv6-Netzwerke, z. B. INTRANET sowie IPv6-(WAN)-Gegenstellen.

SNMP-ID:

2.108.2.5.3

Pfad Konsole:

Setup > **Multicast** > **MLD** > **Statische-Routen**

Mögliche Werte:

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

Modus

Falls SSM verwendet werden soll: Steuert, über welche Methode Quelladressen der Multicast-Quellen in einem MLD-Membership-Report angefordert werden sollen.

Wenn eine SSM-Gruppe mit beliebigen Quelladressen verwendet werden soll, so muss bei Modus „Exclude“ und SSM-Quell-IP-Liste „ANY“ verlinkt werden.

SNMP-ID:

2.108.2.5.4

Pfad Konsole:

Setup > **Multicast** > **MLD** > **Statische-Routen**

Mögliche Werte:

Include

Es wird ein MLD-Membership Report mit Record-Type „Change to Include Mode“ gesendet. Die Einträge aus der SSM-Quell-IP-Liste werden als gewünschte Quelladressen gesendet. Eine Kombination mit Einstellung „Include“ und SSM-Quell-IP-Liste mit Eintrag „ANY“ führt zu keinem sinnvollen Ergebnis und wird als Konfiguration intern nicht akzeptiert, da alle Quell-IP-Adressen abgelehnt werden würden.

Exclude

Es wird ein MLD-Membership Report mit Record-Type „Change to Exclude Mode“ gesendet. Wenn die Quell-Liste den Eintrag „ANY“ bzw. „0.0.0.0“ enthält, d. h. alle Quellen erlaubt, so wird ein MLD-Membership Report mit Join Group für „any sources“ gesendet. Wenn die Liste einen anderen Eintrag als 0.0.0.0 enthält wird ein MLD Membership Report „block sources“ mit der entsprechenden IP-Adresse gesendet.

SSM-Quell-IP-Liste

Falls SSM verwendet werden soll, kann hier eine Liste von gewünschten Quellen zusätzlich zur Multicast-Gruppe definiert werden. Sollen alle Quellen zugelassen werden, kann die vordefinierte Liste „ANY“ mit dem Eintrag „0.0.0.0“ verwendet werden.

SNMP-ID:

2.108.2.5.5

Pfad Konsole:

Setup > **Multicast** > **MLD** > **Statische-Routen**

Mögliche Werte:

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

Parameter

Hier finden Sie die Einstellungen zu den allgemeinen MLD-Parametern.

SNMP-ID:

2.108.2.6

Pfad Konsole:

Setup > **Multicast** > **MLD**

Interface

Schnittstellenname, für den die MLD-Konfiguration gilt. Der Eintrag mit dem Namen DEFAULT gilt für alle Schnittstellen, die keinen spezifischen Eintrag haben. Falls der Eintrag DEFAULT nicht vorhanden ist, gelten interne Default-Werte, die den Werten des DEFAULT-Eintrags entsprechen. Mögliche Werte sind DEFAULT, IPv6-Netzwerke, z. B. INTRANET, IPv6-(WAN)-Gegenstellen oder IPv6 RAS-Templates.

SNMP-ID:

2.108.2.6.1

Pfad Konsole:

Setup > **Multicast** > **MLD** > **Parameter**

Mögliche Werte:

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

Robustness-Variable

Anzahl der Wiederholungen von MLD-Nachrichten.

SNMP-ID:

2.108.2.6.2

Pfad Konsole:

Setup > **Multicast** > **MLD** > **Parameter**

Mögliche Werte:

1 … 10

Default-Wert:

2

Unsolicited-Report-Interval

Definiert die Zeit in Sekunden zwischen den Wiederholungen von Membership-Reports nach dem das Gerät in der Host-Rolle den erstmaligen Membership-Report in einer Gruppe gesendet hat.

SNMP-ID:

2.108.2.6.3

Pfad Konsole:

Setup > **Multicast** > **MLD** > **Parameter**

Mögliche Werte:

1 … 25

Default-Wert:

2

Query-Interval

Intervall in Sekunden zwischen MLD General-Query-Nachrichten.

SNMP-ID:

2.108.2.6.4

Pfad Konsole:

Setup > **Multicast** > **MLD** > **Parameter**

Mögliche Werte:

2 … 99999

Default-Wert:

125

Query-Response-Interval

Maximale Antwortzeit aus der der Wert Maximum Response Code berechnet wird, der in periodischen MLD General-Query-Nachrichten gesetzt wird. Der Wert Query-Response-Intervall muss kleiner als der Wert für Query-Intervall sein.

SNMP-ID:

2.108.2.6.5

Pfad Konsole:

Setup > **Multicast** > **MLD** > **Parameter**

Mögliche Werte:

1 … 999999

Default-Wert:

10000

Startup-Query-Interval

Intervall in Sekunden zwischen MLD General-Query-Nachrichten beim Start des MLD-Queriers.

SNMP-ID:

2.108.2.6.6

Pfad Konsole:

Setup > **Multicast** > **MLD** > **Parameter**

Mögliche Werte:

1 … 99998

Default-Wert:

30

Startup-Query-Count

Anzahl an MLD General-Nachrichten die beim Start gesendet werden, unterbrochen bzw. zeitlich verzögert vom Startup-Query-Intervall.

SNMP-ID:

2.108.2.6.7

Pfad Konsole:

Setup > **Multicast** > **MLD** > **Parameter**

Mögliche Werte:

1 … 10

Default-Wert:

2

Last-Listener-Query-Interval

Definiert den Wert in Sekunden des Maximum Response Code (bei IPv6) in Multicast-Address-Specific Queries, die als Antwort auf Done-Nachrichten gesendet werden. Der Parameter definiert ebenso die Zeit zwischen Multicast-Address-Specific-Query-Nachrichten.

SNMP-ID:

2.108.2.6.8

Pfad Konsole:

Setup > **Multicast** > **MLD** > **Parameter**

Mögliche Werte:

1 … 25

Default-Wert:

2

Last-Listener-Query-Count

Anzahl von gesendeten Nachrichten vom Typ Multicast-Address-Specific Query bevor der Router annimmt, dass es keine lokalen Empfänger mehr gibt. Definiert ebenso die Anzahl an gesendeten Nachrichten vom Typ Multicast-Address-Specific-Query bevor der Router annimmt, dass es keine weiteren Empfänger für eine spezielle Quelle gibt.

SNMP-ID:

2.108.2.6.9

Pfad Konsole:

Setup > **Multicast** > **MLD** > **Parameter**

Mögliche Werte:

1 … 10

Default-Wert:

2

MLD-Kompatibilitaets-Modus

MLD-Version, in der das Gerät in der Rolle als Multicast-Router arbeitet.

SNMP-ID:

2.108.2.6.10

Pfad Konsole:

Setup > **Multicast** > **MLD** > **Parameter**

Mögliche Werte:

Aus
V1
V2

Default-Wert:

V2

Quick-Leave

Erlaubt das schnelle Verlassen von Multicast Gruppen. Sollte nur verwendet werden, falls es nur einen Empfänger pro Gruppe auf dem Interface gibt. Intern wird der Parameter Last-Listener-Query-Count auf 1 und das Last-Listener-Query-Intervall auf 20 ms gesetzt.

SNMP-ID:

2.108.2.6.11

Pfad Konsole:

Setup > **Multicast** > **MLD** > **Parameter**

Mögliche Werte:

Nein
Ja

Default-Wert:

Nein

Statistiken-Erfassen

Definiert, ob erweiterte IPv6-Multicast-Statistiken gesammelt werden sollen. Das Sammeln dieser Statistiken beeinflusst ggf. die Performance des Geräts.

SNMP-ID:

2.108.2.8

Pfad Konsole:

Setup > **Multicast** > **MLD**

Mögliche Werte:

Nein
Ja

Default-Wert:

Nein

Static-Join

In dieser Tabelle können IPv6-Multicast-Gruppen definiert werden, denen das Gerät zu Testzwecken auf Client-Interfaces durch MLD beitreten kann. Damit können im Test Multicast-Clients simuliert werden, die bestimmten MLD-Gruppen beitreten. Das entsprechende Client-Interface muss Teil der IGMP-Proxy oder PIM-Konfiguration sein. Der eingehende Multicast-Datenverkehr wird dann vom Gerät verarbeitet und verworfen. Diese Funktion ist nicht für den dauerhaften Betrieb in produktiven Szenarien geeignet.

SNMP-ID:

2.108.2.9

Pfad Konsole:

Setup > **Multicast** > **MLD**

Interface

(Client-)Interface-Name auf dem der Multicast Client simuliert werden soll.

SNMP-ID:

2.108.2.9.1

Pfad Konsole:

Setup > **Multicast** > **MLD** > **Static-Join**

Mögliche Werte:

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

Gruppe

IPv6-Multicast-Gruppe der das Gerät statisch beitreten soll.

SNMP-ID:

2.108.2.9.2

Pfad Konsole:

Setup > **Multicast** > **MLD** > **Static-Join**

Mögliche Werte:

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

Kommentar

Vergeben Sie optional einen sinnvollen Kommentar als Beschreibung.

SNMP-ID:

2.108.2.9.3

Pfad Konsole:

Setup > **Multicast** > **MLD** > **Static-Join**

Mögliche Werte:

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

Aktiviere-Lancom-Gruppe

Definiert, ob das Gerät auf die Multicast-Adresse ff02::139 reagieren soll. Diese Multicast-Gruppe wird zum Finden von LANCOM Geräten durch die LANtools verwendet.

SNMP-ID:

2.108.2.127

Pfad Konsole:

Setup > **Multicast** > **MLD**

Mögliche Werte:

Nein
Ja

Default-Wert:

Ja

PIM

Hier finden Sie die Einstellungen zu PIM (Protocol Independent Multicast).

SNMP-ID:

2.108.4

Pfad Konsole:

Setup > **Multicast**

IPv4

Hier finden Sie die Einstellungen zu PIM (Protocol Independent Multicast) bei IPv4.

SNMP-ID:

2.108.4.1

Pfad Konsole:

Setup > **Multicast** > **PIM**

RP-Liste

In dieser Tabelle werden die Rendezvous Points (RPs) sowie die zugehörigen Multicastgruppen für den PIM Sparse Mode konfiguriert.

SNMP-ID:

2.108.4.1.1

Pfad Konsole:

Setup > **Multicast** > **PIM** > **IPv4**

Gruppen-Filter

Definiert die Multicast-Gruppen, für die der Rendezvous Points zuständig sein soll. Adressen, die auf den Gruppen-Filter passen, werden von diesem Rendezvous Point verwaltet. Referenziert eine Filterliste aus der Tabelle *2.108.5 IPv4-Filter-Tabelle* auf Seite 125.

SNMP-ID:

2.108.4.1.1.1

Pfad Konsole:

Setup > **Multicast** > **PIM** > **IPv4** > **RP-Liste**

Mögliche Werte:

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

Rtg-Tag

Routing-Tag, das verwendet werden soll um diesen Rendezvous Point zu erreichen.

SNMP-ID:

2.108.4.1.1.2

Pfad Konsole:

Setup > **Multicast** > **PIM** > **IPv4** > **RP-Liste**

Mögliche Werte:

0 … 65535

Default-Wert:

0

RP-Adresse

IPv4-Adresse des externen Rendezvous Points. Das Gerät selbst unterstützt die Rolle eines Rendezvous Points nicht.

SNMP-ID:

2.108.4.1.1.3

Pfad Konsole:

Setup > **Multicast** > **PIM** > **IPv4** > **RP-Liste**

Mögliche Werte:

max. 15 Zeichen aus `[0-9].`

RP-Name

Name des Rendezvous Points.

SNMP-ID:

2.108.4.1.1.5

Pfad Konsole:

Setup > **Multicast** > **PIM** > **IPv4** > **RP-Liste**

Mögliche Werte:

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

Kommentar

Vergeben Sie optional einen sinnvollen Kommentar als Beschreibung.

SNMP-ID:

2.108.4.1.1.6

Pfad Konsole:

Setup > **Multicast** > **PIM** > **IPv4** > **RP-Liste**

Mögliche Werte:

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

SSM-Liste

In dieser Tabelle werden die Parameter für PIM SSM (Source Specific Multicast) Mode konfiguriert.

SNMP-ID:

2.108.4.1.2

Pfad Konsole:

Setup > **Multicast** > **PIM** > **IPv4**

Gruppen-Filter

Definiert die Multicast-Gruppen, für die diese SSM-Konfiguration gelten soll. Adressen, die auf den Gruppen-Filter passen, werden auf diese SSM-Konfiguration angewendet. Referenziert eine Filterliste aus der Tabelle *2.108.5 IPv4-Filter-Tabelle* auf Seite 125.

SNMP-ID:

2.108.4.1.2.1

Pfad Konsole:

Setup > **Multicast** > **PIM** > **IPv4** > **SSM-Liste**

Mögliche Werte:

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

Rtg-Tag

Routing-Tag, für den diese Konfiguration gelten soll.

SNMP-ID:

2.108.4.1.2.2

Pfad Konsole:

Setup > **Multicast** > **PIM** > **IPv4** > **SSM-Liste**

Mögliche Werte:

0 … 65535

Default-Wert:

0

SSM-Quellen-Filter

Definiert den SSM-Source-Filter für diesen Tabellen-Eintrag. Nur Multicast-Quell-Adressen, die auf den SSM-Source-Filter passen, werden auf diese SSM-Konfiguration angewendet. Referenziert eine Filterliste aus der Tabelle *2.108.1.4 SSM-Quell-IP-Liste* auf Seite 89.

SNMP-ID:

2.108.4.1.2.3

Pfad Konsole:

Setup > **Multicast** > **PIM** > **IPv4** > **SSM-Liste**

Mögliche Werte:

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

SSM-Name

Name dieser SSM-Konfiguration.

SNMP-ID:

2.108.4.1.2.5

Pfad Konsole:

Setup > **Multicast** > **PIM** > **IPv4** > **SSM-Liste**

Mögliche Werte:

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

Kommentar

Vergeben Sie optional einen sinnvollen Kommentar als Beschreibung.

SNMP-ID:

2.108.4.1.2.6

Pfad Konsole:

Setup > **Multicast** > **PIM** > **IPv4** > **SSM-Liste**

Mögliche Werte:

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

SSM-Zuordnung

In dieser Tabelle können IPv4 Multicast Quell-Adressen (S) konfiguriert werden, die automatisch in PIM-Join-Nachrichten eingefügt werden sollen, falls in empfangenen IGMP-Nachrichten keine Quell-Adressen (S) vorhanden sind. Somit werden (*,G)-Einträge vom Router automatisch zu (S,G)-Einträgen ergänzt.

SNMP-ID:

2.108.4.1.3

Pfad Konsole:

Setup > **Multicast** > **PIM** > **IPv4**

Gruppen-Filter

Definiert die Multicast-Gruppen (G) für die dieses SSM-Mapping durchgeführt werden soll. Referenziert eine Filterliste aus der Tabelle *2.108.5 IPv4-Filter-Tabelle* auf Seite 125.

SNMP-ID:

2.108.4.1.3.1

Pfad Konsole:

Setup > **Multicast** > **PIM** > **IPv4** > **SSM-Zuordnung**

Mögliche Werte:

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

Rtg-Tag

Routing-Tag, für den diese Konfiguration gelten soll.

SNMP-ID:

2.108.4.1.3.2

Pfad Konsole:

Setup > **Multicast** > **PIM** > **IPv4** > **SSM-Zuordnung**

Mögliche Werte:

0 … 65535

Default-Wert:

0

SSM-Quell-IP

Definiert eine Quell-IPv4-Adresse (S), die automatisch in PIM-Join-Nachrichten für (*,G)-Einträge eingefügt werden soll und automatisch zu (S,G)-Einträge ergänzt werden soll.

SNMP-ID:

2.108.4.1.3.3

Pfad Konsole:

Setup > **Multicast** > **PIM** > **IPv4** > **SSM-Zuordnung**

Mögliche Werte:

max. 15 Zeichen aus `[0-9].`

Kommentar

Vergeben Sie optional einen sinnvollen Kommentar als Beschreibung.

SNMP-ID:

2.108.4.1.3.4

Pfad Konsole:

Setup > **Multicast** > **PIM** > **IPv4** > **SSM-Zuordnung**

Mögliche Werte:

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

IPv6

Hier finden Sie die Einstellungen zu PIM (Protocol Independent Multicast) bei IPv6.

SNMP-ID:

2.108.4.2

Pfad Konsole:

Setup > **Multicast** > **PIM**

RP-Liste

In dieser Tabelle werden die Rendezvous Points (RPs) sowie die zugehörigen Multicastgruppen für den PIM Sparse Mode konfiguriert.

SNMP-ID:

2.108.4.2.1

Pfad Konsole:

Setup > **Multicast** > **PIM** > **IPv6**

Gruppen-Filter

Definiert die Multicast-Gruppen, für die der Rendezvous Points zuständig sein soll. Adressen, die auf den Gruppen-Filter passen, werden von diesem Rendezvous Point verwaltet. Referenziert eine Filterliste aus der Tabelle *2.108.6 IPv6-Filter-Tabelle* auf Seite 127.

SNMP-ID:

2.108.4.2.1.1

Pfad Konsole:

Setup > **Multicast** > **PIM** > **IPv6** > **RP-Liste**

Mögliche Werte:

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

Rtg-Tag

Routing-Tag, das verwendet werden soll um diesen Rendezvous Point zu erreichen.

SNMP-ID:

2.108.4.2.1.2

Pfad Konsole:

Setup > **Multicast** > **PIM** > **IPv6** > **RP-Liste**

Mögliche Werte:

0 … 65535

Default-Wert:

0

RP-Adresse

IPv6-Adresse des externen Rendezvous Points. Das Gerät selbst unterstützt die Rolle eines Rendezvous Points nicht.

SNMP-ID:

2.108.4.2.1.3

Pfad Konsole:

Setup > **Multicast** > **PIM** > **IPv6** > **RP-Liste**

Mögliche Werte:

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

RP-Name

Name des Rendezvous Points.

SNMP-ID:

2.108.4.2.1.5

Pfad Konsole:

Setup > **Multicast** > **PIM** > **IPv6** > **RP-Liste**

Mögliche Werte:

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

Kommentar

Vergeben Sie optional einen sinnvollen Kommentar als Beschreibung.

SNMP-ID:

2.108.4.2.1.6

Pfad Konsole:

Setup > **Multicast** > **PIM** > **IPv6** > **RP-Liste**

Mögliche Werte:

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

SSM-Liste

In dieser Tabelle werden die Parameter für PIM IPv6 SSM (Source Specific Multicast) Mode konfiguriert.

SNMP-ID:

2.108.4.2.2

Pfad Konsole:

Setup > **Multicast** > **PIM** > **IPv6**

Gruppen-Filter

Definiert die Multicast-Gruppen, für die diese SSM-Konfiguration gelten soll. Adressen, die auf den Gruppen-Filter passen, werden auf diese SSM-Konfiguration angewendet. Referenziert eine Filterliste aus der Tabelle *2.108.6 IPv6-Filter-Tabelle* auf Seite 127.

SNMP-ID:

2.108.4.2.2.1

Pfad Konsole:

Setup > **Multicast** > **PIM** > **IPv6** > **SSM-Liste**

Mögliche Werte:

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

Rtg-Tag

Routing-Tag, für den diese Konfiguration gelten soll.

SNMP-ID:

2.108.4.2.2.2

Pfad Konsole:

Setup > **Multicast** > **PIM** > **IPv6** > **SSM-Liste**

Mögliche Werte:

0 … 65535

Default-Wert:

0

SSM-Quellen-Filter

Definiert den SSM-Source-Filter für diesen Tabellen-Eintrag. Nur Multicast-Quell-Adressen, die auf den SSM-Source-Filter passen, werden auf diese SSM-Konfiguration angewendet. Referenziert eine Filterliste aus der Tabelle *2.108.1.4 SSM-Quell-IP-Liste* auf Seite 89.

SNMP-ID:

2.108.4.2.2.3

Pfad Konsole:

Setup > **Multicast** > **PIM** > **IPv6** > **SSM-Liste**

Mögliche Werte:

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

SSM-Name

Name dieser SSM-Konfiguration.

SNMP-ID:

2.108.4.2.2.5

Pfad Konsole:

Setup > **Multicast** > **PIM** > **IPv6** > **SSM-Liste**

Mögliche Werte:

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

Kommentar

Vergeben Sie optional einen sinnvollen Kommentar als Beschreibung.

SNMP-ID:

2.108.4.2.2.6

Pfad Konsole:

Setup > **Multicast** > **PIM** > **IPv6** > **SSM-Liste**

Mögliche Werte:

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

SSM-Zuordnung

In dieser Tabelle können IPv6 Multicast Quell-Adressen (S) konfiguriert werden, die automatisch in PIM-Join-Nachrichten eingefügt werden sollen, falls in empfangenen MLD-Nachrichten keine Quell-Adressen vorhanden sind. Somit werden (*,G) Einträge vom Router automatisch zu (S,G) ergänzt.

SNMP-ID:

2.108.4.2.3

Pfad Konsole:

Setup > **Multicast** > **PIM** > **IPv6**

Gruppen-Filter

Definiert die Multicast-Gruppen (G) für die dieses SSM-Mapping durchgeführt werden soll. Referenziert eine Filterliste aus der Tabelle *2.108.6 IPv6-Filter-Tabelle* auf Seite 127.

SNMP-ID:

2.108.4.2.3.1

Pfad Konsole:

Setup > **Multicast** > **PIM** > **IPv6** > **SSM-Zuordnung**

Mögliche Werte:

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

Rtg-Tag

Routing-Tag für das diese Konfiguration gelten soll.

SNMP-ID:

2.108.4.2.3.2

Pfad Konsole:

Setup > **Multicast** > **PIM** > **IPv6** > **SSM-Zuordnung**

Mögliche Werte:

0 … 65535

Default-Wert:

0

SSM-Quell-IP

Definiert eine Quell-IPv6-Adresse (S), die automatisch in PIM-Join-Nachrichten für (*,G)-Einträge eingefügt werden soll und automatisch zu (S,G)-Einträge ergänzt werden soll.

SNMP-ID:

2.108.4.2.3.3

Pfad Konsole:

Setup > **Multicast** > **PIM** > **IPv6** > **SSM-Zuordnung**

Mögliche Werte:

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

Kommentar

Vergeben Sie optional einen sinnvollen Kommentar als Beschreibung.

SNMP-ID:

2.108.4.2.3.4

Pfad Konsole:

Setup > **Multicast** > **PIM** > **IPv6** > **SSM-Zuordnung**

Mögliche Werte:

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

Interfaces

In dieser Tabelle werden die Interfaces bzw. logischen Netzwerke definiert, auf denen PIM aktiviert werden soll. Ebenso werden die Interfaces definiert, auf denen Clients per IGMP bzw. MLD Multicast-Gruppen beitreten können.

SNMP-ID:

2.108.4.3

Pfad Konsole:

Setup > **Multicast** > **PIM**

Interface

Name des logischen Interfaces auf dem PIM bzw. GMP (Group Management Protokoll wie IGMP oder MLD) aktiviert werden soll. Mögliche Werte sind IPv4-Netzwerke, z. B. INTRANET, WAN-Gegenstellen, Wildcard-Einträge mit * für IPv4-RAS-Interfaces, z. B. „VPN*“. Weitere mögliche Werte sind IPv6-Interfaces sowie IPv6 RAS-Templates.

SNMP-ID:

2.108.4.3.1

Pfad Konsole:

Setup > **Multicast** > **PIM** > **Interfaces**

Mögliche Werte:

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

PIM-Active

Aktiviert PIM sowie das Senden und Empfangen von PIM-Nachrichten auf diesem logischen Interface. Wenn nur IGMP- / MLD-Clients bzw. Multicast-Empfänger auf dieser Schnittstelle vorhanden sind, kann somit das Senden bzw. Empfangen von PIM-Nachrichten explizit deaktiviert werden. In diesem Fall muss nur GMP (IGMP / MLD) aktiviert sein.

SNMP-ID:

2.108.4.3.2

Pfad Konsole:

Setup > **Multicast** > **PIM** > **Interfaces**

Mögliche Werte:

Nein

PIM ist nicht aktiv.

Ja

PIM ist aktiv.

GMP-Active

Aktiviert die IGMP- bzw. MLD-Routerrolle auf diesem logischen Interface. In diesem Fall werden IGMP- bzw. MLD-Joins von Clients akzeptiert. Auf Interfaces bei denen keine Clients im Netzwerk, sondern nur PIM-Nachbar-Router vorhanden sind, kann GMP deaktiviert werden. IGMP- / MLD-Joins werden in diesem Fall dann nicht akzeptiert.

SNMP-ID:

2.108.4.3.3

Pfad Konsole:

Setup > **Multicast** > **PIM** > **Interfaces**

Mögliche Werte:

Nein

IGMP- bzw. MLD-Routerrolle ist nicht aktiv.

Ja

IGMP- bzw. MLD-Routerrolle ist aktiv.

Adresstyp

Hier definieren Sie, für welche Adressfamilie PIM bzw. GMP auf diesem Interface aktiviert werden soll.

SNMP-ID:

2.108.4.3.4

Pfad Konsole:

Setup > **Multicast** > **PIM** > **Interfaces**

Mögliche Werte:

IPv4
IPv6

Hello-Intervall

Definiert die Zeit in Sekunden zwischen der Wiederholung von regelmäßigen PIM Hello-Nachrichten. Die Haltezeit ist automatisch das 3,5-fache des PIM-Hello-Intervalls und nicht separat konfigurierbar.

SNMP-ID:

2.108.4.3.5

Pfad Konsole:

Setup > **Multicast** > **PIM** > **Interfaces**

Mögliche Werte:

0 … 255

Default-Wert:

30

Besondere Werte:

0

Der Wert 0 deaktiviert das Senden von Hello-Nachrichten.

DR-Priority

Definiert die Priorität als Designated Router (DR) im Prozess der DR-Wahl von PIM. Ein höherer Wert bedeutet eine höhere Priorität im DR-Wahlverfahren zum Designated Router (DR).

SNMP-ID:

2.108.4.3.6

Pfad Konsole:

Setup > **Multicast** > **PIM** > **Interfaces**

Mögliche Werte:

0 … 4294967296

Default-Wert:

1

Tracking-Support

Beeinflusst das Setzen des „T-Bits“ in der LAN-Prune-Delay-Option in ausgehenden Hello-Nachrichten.

SNMP-ID:

2.108.4.3.7

Pfad Konsole:

Setup > **Multicast** > **PIM** > **Interfaces**

Mögliche Werte:

Ja
Nein

Default-Wert:

Nein

Override-Intervall

Beeinflusst das Setzen des Override-Intervall-Felds in der LAN-Prune-Delay-Option in ausgehenden Hello-Nachrichten. Definiert die maximale Verzögerung für die Übertragung von Override-Join-Nachrichten für Multicast-Netzwerke, die Join-Supression aktiviert haben.

SNMP-ID:

2.108.4.3.8

Pfad Konsole:

Setup > **Multicast** > **PIM** > **Interfaces**

Mögliche Werte:

0 … 4294967296

Default-Wert:

0

Propagation-Delay

Konfiguriert das Setzen des Propagation-Delay-Felds in gesendeten Hello-Nachrichten der LAN-Prune-Delay-Option. Definiert die Verzögerung in Millisekunden für das Versenden von PIM Prune-Nachrichten auf dem Upstream-Router in einem Multicast-Netzwerk, in dem Join-Unterdrückung aktiviert ist.

SNMP-ID:

2.108.4.3.9

Pfad Konsole:

Setup > **Multicast** > **PIM** > **Interfaces**

Mögliche Werte:

250 … 2000

Default-Wert:

500

Aktiv

Aktiviert bzw. deaktiviert PIM auf dem Gerät.

SNMP-ID:

2.108.4.6

Pfad Konsole:

Setup > **Multicast** > **PIM**

Mögliche Werte:

Nein

PIM ist nicht aktiv.

Ja

PIM ist aktiv.

Default-Wert:

Nein

IPv4-Filter-Tabelle

In dieser Tabelle können Listen von gewünschten oder unerwünschten IPv4 Multicast-Adressen bzw. Präfixen definiert werden.

Diese können an verschiedenen Stellen referenziert werden und über diese Tabelle global verwaltet werden. Eine Liste wird durch mehrere Einträge mit gleichem Namen definiert.

SNMP-ID:

2.108.5

Pfad Konsole:

Setup > **Multicast**

Name

Geben Sie diesem Eintrag einen Namen. Eine Liste wird durch mehrere Einträge mit gleichem Namen definiert.

SNMP-ID:

2.108.5.1

Pfad Konsole:

Setup > **Multicast** > **IPv4-Filter-Tabelle**

Mögliche Werte:

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

Praefix

Geben Sie hier die IPv4-Adresse des Netzwerkes gefolgt von der Präfix-Länge des Netzwerkes an (CIDR-Notation). Diese legt fest, wie viele höchstwertige Bits (Most Significant Bit, MSB) der IP-Adresse für eine Übereinstimmung notwendig sind.

SNMP-ID:

2.108.5.2

Pfad Konsole:

Setup > **Multicast** > **IPv4-Filter-Tabelle**

Mögliche Werte:

max. 18 Zeichen aus `[0-9]./`

Aktion

Geben Sie an, ob die Präfixe dieses Filtereintrags zugelassen oder abgewiesen werden sollen.

SNMP-ID:

2.108.5.3

Pfad Konsole:

Setup > **Multicast** > **IPv4-Filter-Tabelle**

Mögliche Werte:

Erlauben
Ablehnen

Kommentar

Vergeben Sie optional einen sinnvollen Kommentar als Beschreibung.

SNMP-ID:

2.108.5.4

Pfad Konsole:

Setup > **Multicast** > **IPv4-Filter-Tabelle**

Mögliche Werte:

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

IPv6-Filter-Tabelle

In dieser Tabelle können Listen von gewünschten oder unerwünschten IPv6 Multicast-Adressen bzw. Präfixen definiert werden.

Diese können an verschiedenen Stellen referenziert werden und über diese Tabelle global verwaltet werden. Eine Liste wird durch mehrere Einträge mit gleichem Namen definiert.

SNMP-ID:

2.108.6

Pfad Konsole:

Setup > **Multicast**

Name

Geben Sie diesem Eintrag einen Namen. Eine Liste wird durch mehrere Einträge mit gleichem Namen definiert.

SNMP-ID:

2.108.6.1

Pfad Konsole:

Setup > **Multicast** > **IPv6-Filter-Tabelle**

Mögliche Werte:

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

Praefix

Geben Sie hier die IPv6-Multicast-Adresse bzw. das Präfix an.

SNMP-ID:

2.108.6.2

Pfad Konsole:

Setup > **Multicast** > **IPv6-Filter-Tabelle**

Mögliche Werte:

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

Aktion

Geben Sie an, ob die Präfixe dieses Filtereintrags zugelassen oder abgewiesen werden sollen.

SNMP-ID:

2.108.6.3

Pfad Konsole:

Setup > **Multicast** > **IPv6-Filter-Tabelle**

Mögliche Werte:

Erlauben
Ablehnen

Kommentar

Vergeben Sie optional einen sinnvollen Kommentar als Beschreibung.

SNMP-ID:

2.108.6.4

Pfad Konsole:

Setup > **Multicast** > **IPv6-Filter-Tabelle**

Mögliche Werte:

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

8 Virtual Private Networks – VPN

8.1 High Scalability VPN (HSVPN)

In SD-WAN-Szenarien, bei denen Filialen Verbindungen zu einer oder mehreren Zentralen aufbauen, sind in der Regel mehrere logische Netze vorhanden, die sicher über VLAN und ARF voneinander getrennt werden müssen, z. B. Zahlungsverkehr, Warenwirtschaft oder Hotspot. Diese lokalen Netze wurden bisher entweder als „gestapelte" Tunnel, d. h. PPTP oder L2TP innerhalb eines VPN-Tunnels oder als einzelne IPSec-VPN-Tunnel mit der Zentrale verbunden. Diese Architekturen skalieren aber bei einer großen Anzahl von Filialen und vielen ARF-Netzen nicht besonders gut. Beispielsweise ergibt sich bei 1.000 Filialen und 8 ARF-Netzen eine Anzahl von 8.000 Tunneln bei einer Architektur mit einem Tunnel pro ARF-Netz. Gestapelte Tunnel haben aufgrund des Protokoll-Overheads Performance- und MTU-Einschränkungen.

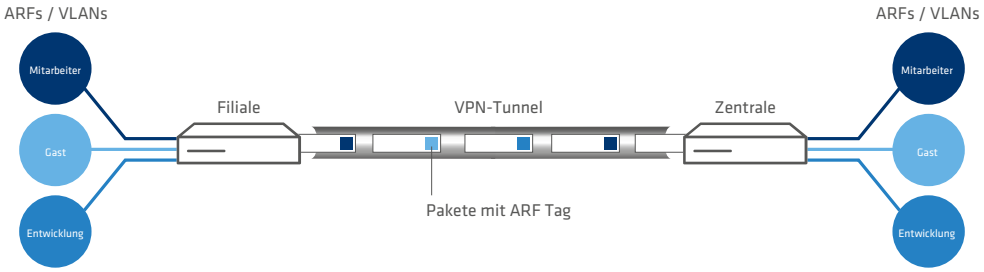


Abbildung 1: LANCOM HSVPN-Szenario für SD-WAN

Die neue Architektur LANCOM HSVPN („LANCOM High Scalability VPN") löst diese Herausforderungen. Bei HSVPN werden Pakete aus ARF-Netzen innerhalb eines IPSec-Tunnels mit einem ARF-Tag markiert und ohne Overhead im VPN-Tunnel transportiert. Diese Tagging-Methode auf Layer 3 entspricht dem VLAN-Ansatz für Layer 2 und bietet somit das gleiche Sicherheitsniveau wie VLAN. Dadurch, das insgesamt weniger Tunnel benötigt werden, verbessern sich die Tunnelaufbauzeiten insbesondere im Fail-over-Fall. Auch bzgl. MTU gibt es keine großen Einschränkungen.

Die folgenden groben Konfigurationsschritte sind dafür notwendig:

1. Anlegen der einzelnen ARF-Netze
2. Anlegen eines IKEv2-Tunnels
3. Im HSVPN-Konfigurationsprofil des IKEv2-Tunnels werden die erlaubten ARF-Netze als Tag-Liste konfiguriert
4. Für die gewünschten ARF-Netze müssen entsprechende Routen auf den HSVPN-Tunnel angelegt werden

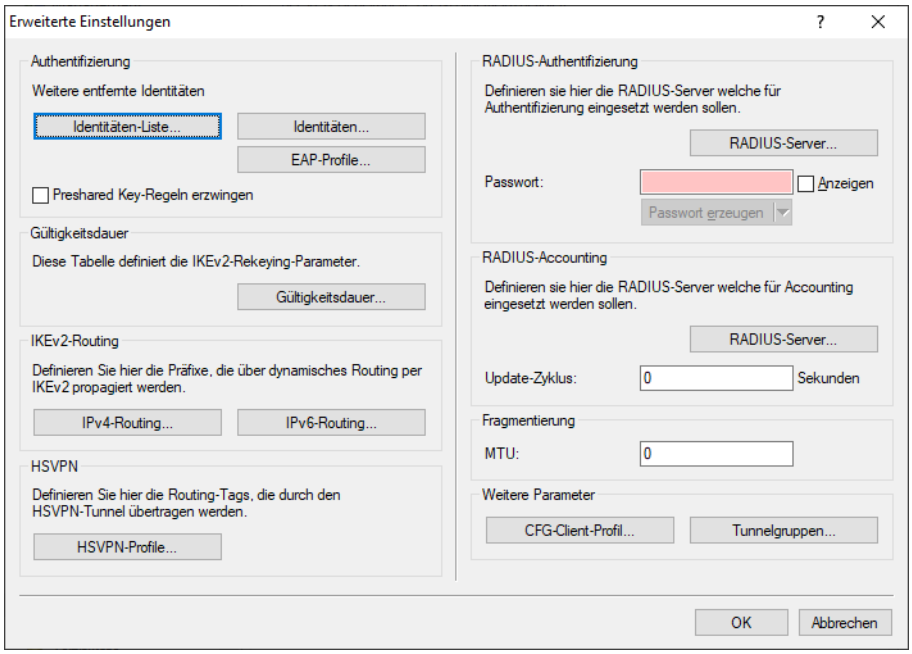
Grundsätzlich unterstützt LANCOM HSVPN zwei Betriebsarten:

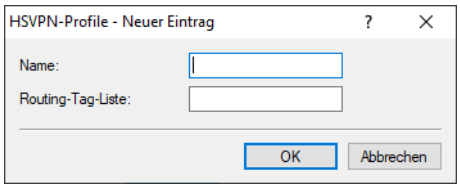
- Betrieb als klassisches Site-to-Site VPN
- Betrieb im CFG-Mode mit IKEv2-Routing, wobei neben den Routen auch die zugehörigen Routing-Tags übertragen werden

Aktuelle Einschränkungen:

- Multicast Routing über HSVPN wird derzeit nicht unterstützt. Hierzu ist ein separater VPN-Tunnel für Multicast erforderlich.
- OSPF über HSVPN wird nicht unterstützt

In LANconfig erfolgt die Konfiguration der HSVPN-Profile unter **VPN** > **IKEv2/IPSec** > **Erweiterte Einstellungen** > **HSVPN** über **HSVPN-Profile**.





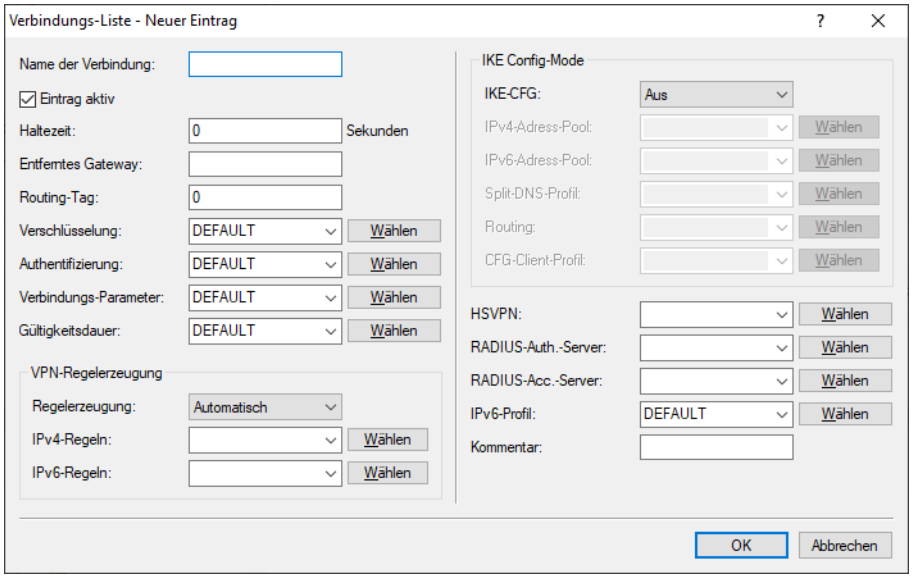
Name

Vergeben Sie einen Namen für das HSVPN-Profil.

Routing-Tag-Liste

Definieren Sie hier die Routing-Tags als kommaseparierte Liste (z. B. 1,2,3), die über HSVPN übertragen werden sollen. Die Rtg-Tag-Liste muss zwischen beiden VPN-Partnern identisch sein, damit alle gewünschten ARF-Netze transportiert werden.

Diese Profile können Sie dann bei den VPN-Verbindungen unter **VPN** > **IKEv2/IPSec** > **Verbindungs-Liste** auswählen.



HSVPN

Definieren Sie hier den Namen des HSVPN-Profils aus der Tabelle *HSVPN-Profile*.

Neue RADIUS-Attribute für HSPVN

ID	Bezeichnung	Bedeutung
LANCOM 29	LCS-IKEv2-Routing-Tag-List	Format (String): #, z. B. `0,3,7` Beinhaltet die Routing-Tags, die über HSVPN übertragen werden sollen.
LANCOM 30	LCS-IKEv2-IPv4-Tagged-Route	Format (String): <Präfix> rtg_tag=<Routing-Tag> **<Präfix>** HSVPN IPv4-Route die der CFG-Mode-Server im Rahmen des IKEv2-Routings an den Client übermittelt. **rtg_tag=<Routing-Tag>** Das hierbei verwendete Routing-Tag. Z. B. `192.168.1.0/24 rtg_tag=1` Ein Präfix mit Routing-Tag kann mehrfach im Attribut vorkommen und wird durch ein Komma getrennt.
LANCOM 31	LCS-IKEv2-IPv6-Tagged-Route	Format (String), <Präfix> rtg_tag=<Routing-Tag> **<Präfix>** HSVPN IPv6-Route die der CFG-Mode-Server im Rahmen des IKEv2-Routings an den Client übermittelt. **rtg_tag=<Routing-Tag>** Das hierbei verwendete Routing-Tag.

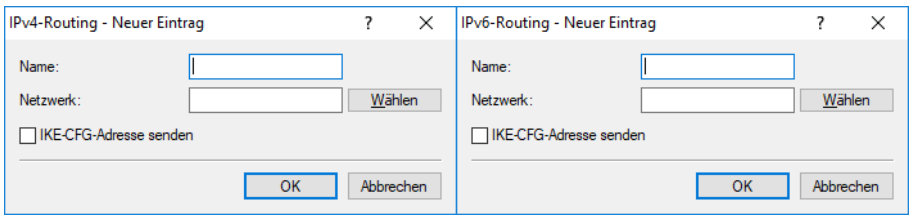
ID	Bezeichnung	Bedeutung
		Z. B. `2001:db8::/64 rtg_tag=1` Ein Präfix mit Routing-Tag kann mehrfach im Attribut vorkommen und wird durch ein Komma getrennt.

Beispiel:

```
LCS-IKEv2-Routing-Tag-List=1,2,3
LCS-IKEv2-IPv4-Tagged-Route=10.11.0.0/24 rtg_tag=1,10.12.0.0/24 rtg_tag=2,10.13.0.0/24 rtg_tag=3
```

8.1.1 HSVPN und IKEv2-Routing

In den Tabellen **VPN** > **IKEv2/IPSec** > **Erweiterte Einstellungen** > **IPv4-Routing** und **VPN** > **IKEv2/IPSec** > **Erweiterte Einstellungen** > **IPv6-Routing** wurde die Eingabesyntax für HSVPN erweitert. Hier kann zusätzlich zum Netzwerknamen oder Präfix auch das entsprechende Routing Tag angegeben werden, falls HSVPN verwendet werden soll. Z. B. 'INTRANET@1' oder '192.168.1.0/24@1', wobei in diesem Beispiel „1“ das entsprechende Routing Tag ist.



Konsole: **Setup** > **VPN** > **IKEv2** > **Routing** > **IPv4** bzw. **Setup** > **VPN** > **IKEv2** > **Routing** > **IPv6**

8.1.2 Ergänzungen im Setup-Menü

HSVPN

Definieren Sie hier den Namen des HSVPN-Profils aus der Tabelle *HSVPN-Profile*.

SNMP-ID:

2.19.36.1.23

Pfad Konsole:

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

Mögliche Werte:

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

HSVPN-Profil

In dieser Tabelle werden die HSVPN-Profile konfiguriert.

SNMP-ID:

2.19.36.15

Pfad Konsole:

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

Name

Vergeben Sie einen Namen für das HSVPN-Profil.

SNMP-ID:

2.19.36.15.1

Pfad Konsole:

Setup > **VPN** > **IKEv2** > **HSVPN-Profil**

Mögliche Werte:

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

Rtg-Tag-Liste

Definieren Sie hier die Routing-Tags als kommaseparierte Liste (z. B. 1,2,3), die über HSVPN übertragen werden sollen. Die Rtg-Tag-Liste muss zwischen beiden VPN-Partnern identisch sein, damit alle gewünschten ARF-Netze transportiert werden.

SNMP-ID:

2.19.36.15.2

Pfad Konsole:

Setup > **VPN** > **IKEv2** > **HSVPN-Profile**

Mögliche Werte:

max. 100 Zeichen aus `[0-9] ,`

Netze

Enthält die kommaseparierte Liste von IPv4-Subnetzen.

Die Angabe der Netze ist in den folgenden Formaten möglich:

- IP-Adresse
- IP-Adresse/Netzmaske
- IP-Adresse/Netzmaske@Tag
- IP-Adresse/Präfixlänge
- IP-Adresse/Präfixlänge@Tag
- IP-Schnittstellen-Name
- IP-Schnittstellen-Name@Tag

Die Angabe mit Routing Tag wird bei HSVPN verwendet.

SNMP-ID:

2.19.36.6.1.2

Pfad Konsole:

Setup > **VPN** > **IKEv2** > **Routing** > **IPv4**

Mögliche Werte:

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

Netze

Enthält die kommaseparierte Liste von IPv6-Subnetzen.

Die Angabe der Netze ist in den folgenden Formaten möglich:

- IPv6-Adresse
- IPv6-Adresse/Präfixlänge
- IPv6-Adresse/Präfixlänge@Tag
- IPv6-Schnittstellen-Name
- IPv6-Schnittstellen-Name@Tag

Die Angabe mit Routing Tag wird bei HSVPN verwendet.

SNMP-ID:

2.19.36.6.2.2

Pfad Konsole:

Setup > **VPN** > **IKEv2** > **Routing** > **IPv6**

Mögliche Werte:

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

8.2 Support für IP Compression und Authentication Header bei IKEv1 beendet

Ab LCOS 10.40 unterstützt Ihr Gerät die Features IP Compression (IPCOMP) und Authentication Header (AH) bei IKEv1 nicht mehr. IPCOMP ist ein Protokoll zur Datenkompression im VPN-Tunnel, welches in der Praxis durch ESP abgelöst wurde. Der Authentication Header (AH) sollte die Authentizität und Integrität der übertragenen Pakete sicherstellen und den Sender authentifizieren. Da er allerdings nicht in Kombination mit NAT verwendet werden kann wird er praktisch nie verwendet. Daher kommt auch hier seit längerem ESP zur Anwendung.

Dadurch entfallen in der Konfiguration unter **VPN** > **IKE/IPSec** > **IPSec-Proposals** die Optionen zur Auswahl des **Modus**, des **AH-Proposals** und des **IPCOMP-Proposals**.

8.3 Gruppierung und Priorisierung von alternativen Gateways

Ab LCOS 10.40 unterstützt Ihr Gerät die Möglichkeit der Gruppierung und Priorisierung von alternativen VPN-Gateways. Dies erweitert die bereits vorhandene Möglichkeit, bis zu 32 zusätzliche Gateways zu konfigurieren, die alternativ nach einem konfigurierbaren Schema (Erstes, Zuletzt benutzt, Zufall) als Einwahlpunkt verwendet wurden, sobald das primäre VPN-Gateway nicht erreichbar war.

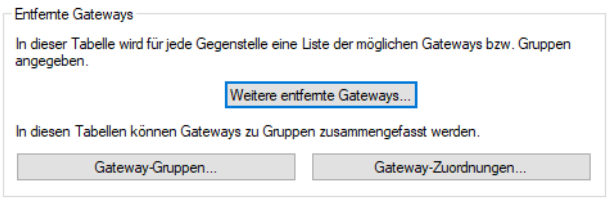
Nun können Gateways optional in Gruppen zusammengefasst werden, wobei Gruppen gleicher Priorität auf einer Ebene nebeneinander angesiedelt werden. Die höchste Priorität ist 0, die niedrigste 65535. Der primäre Gateway wird automatisch in einer eigenen Gruppe mit Priorität 0 angelegt. Wenn der primäre Gateway selbst eine Gateway-Gruppe referenziert, so wird diese Gruppe unabhängig von ihrer konfigurierten Priorität mit der Priorität 0 der Ebenenstruktur hinzugefügt. Alle Gateways aus der Tabelle der **weiteren entfernten Gateways**, die keinen Gruppennamen referenzieren, werden

ebenfalls der Gruppe der primären Gateways hinzugefügt. Die Auswahl-Strategie innerhalb der Gruppe der primären Gateways wird durch die folgenden Regeln definiert:

- Gibt es zusätzliche Gateways, so wird die Auswahl-Strategie durch die Spalte **Anfangen mit** aus der Tabelle der **weiteren entfernten Gateways** festgelegt.
- Gibt es keine zusätzlichen Gateways:
  - Gibt es nur einen primären Gateway, so ist die Auswahl-Strategie „Erstes".
  - Ist der primäre Gateway eine Gateway-Gruppe, so wird die Auswahl-Strategie der Gruppe verwendet.

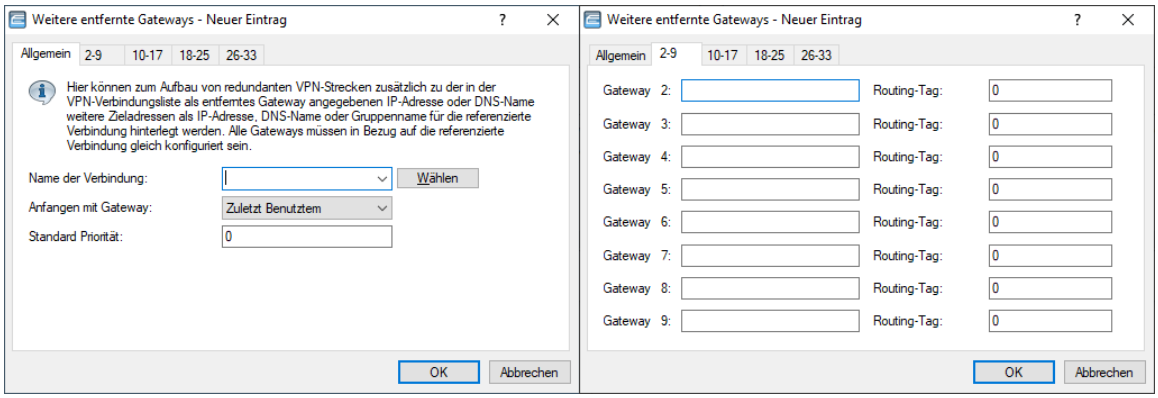
Alle definierten Gruppen werden dann in der Reihenfolge der Gateways aus der Tabelle der **weiteren entfernten Gateways** der Ebenenstruktur mit ihrer in der Tabelle **Gateway-Gruppen** hinterlegten Priorität hinzugefügt. Die Auswahl-Strategie zwischen den Gruppen gleicher Priorität wird durch die Spalte **Anfangen mit** aus der Tabelle **Weitere entfernte Gateways** festgelegt, die Auswahl-Strategie innerhalb einer Gruppe durch die Spalte **Beginne mit** in der Tabelle **Gateway-Gruppen**. Die verschiedenen Ebenen werden immer in aufsteigender Reihenfolge ihrer Priorität nach beginnend mit 0 verwendet.

Die Konfiguration erfolgt unter **VPN** > **Allgemein** > **Entfernte Gateways**.



8.3.1 Weitere entfernte Gateways

Unter **Weitere entfernte Gateways** können zum Aufbau von redundanten VPN-Strecken zusätzlich zu der in der VPN-Verbindungsliste als entferntes Gateway angegebenen IP-Adresse oder DNS-Name weitere Zieladressen als IP-Adresse, DNS-Name oder Gruppenname für die referenzierte Verbindung hinterlegt werden. Alle Gateways müssen in Bezug auf die referenzierte Verbindung gleich konfiguriert sein.



Name der Verbindung

Wählen Sie aus der Liste der definierten VPN-Verbindungen den Namen der VPN-Verbindung aus, für welche die hier definierten zusätzlichen Gateways gelten sollen.

Anfangen mit Gateway

Auswahl des Gateways, über das zuerst der Aufbau der VPN-Verbindung versucht werden soll. Mögliche Werte:

Zuletzt Benutztem

Beginnt mit dem Gateway, über den zuletzt eine Verbindung erfolgreich aufgebaut werden konnte.

Erstem

Beginnt mit dem ersten Eintrag in der Liste.

Zufall

Wählt zufällig einen Eintrag aus der Liste.

Standard-Priorität

Dies ist die Standard-Priorität für alle hier definierten Gateways. Die höchste Priorität ist 0, die niedrigste 65535. Alle Gateways werden jeweils in Gruppen zusammengefasst, wobei Gruppen gleicher Priorität auf einer Ebene nebeneinander angesiedelt werden.

Der primäre Gateway wird automatisch in einer eigenen Gruppe mit Priorität 0 angelegt. Wenn der primäre Gateway selbst eine Gateway-Gruppe referenziert, so wird diese Gruppe unabhängig von ihrer konfigurierten Priorität mit der Priorität 0 der Ebenenstruktur hinzugefügt. Werden hier alternative Gateways definiert, die keine Gateway-Gruppe referenzieren, dann werden diese ebenfalls der Gruppe der primären Gateways hinzugefügt.

Gateway 2-33

Für jeden der bis zu 32 alternativen Gateways können Sie drei mögliche Einträge vornehmen:

1. Der Name einer Gateway-Gruppe
2. Der DNS-Name eines Gateways
3. Die IP-Adresse eines Gateways

Beim Auswerten der Tabelle wird nun zuerst geprüft, ob der eingetragene Gateway der Name einer Gruppe ist, die in der Tabelle **Gateway-Grupen** definiert ist. In diesem Fall werden alle Gateways, die über die Tabelle **Gateway-Zuordnungen** dieser Gruppe zugeordnet sind, in die Gateway-Liste aufgenommen.

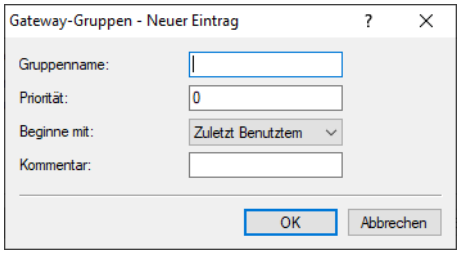
Routing-Tag

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

Wenn Sie hier kein Routing-Tag angeben (d. h. das Routing-Tag ist 0), dann wird für den zugehörigen Gateway das in der VPN-Verbindungs-Liste für diese Gegenstelle konfigurierte Routing-Tag verwendet.

8.3.2 Gateway-Gruppen

Unter **Gateway-Gruppen** können Sie Gateway-Gruppen einrichten, die Sie dann unter *Weitere entfernte Gateways* referenzieren können.



Gruppenname

Geben Sie dieser Gateway-Gruppe einen eindeutigen Namen, über den Sie diese Gruppe referenzieren können.

Priorität

Die Priorität dieser Gruppe. Die höchste Priorität ist 0, die niedrigste 65535.

Beginne mit

Auswahl-Strategie innerhalb der Gruppe. Mögliche Werte:

Zuletzt Benutztem

Beginnt mit dem Gateway in der Gruppe, über den zuletzt eine Verbindung erfolgreich aufgebaut werden konnte.

Erstem

Beginnt mit dem ersten Eintrag in der Liste.

Zufall

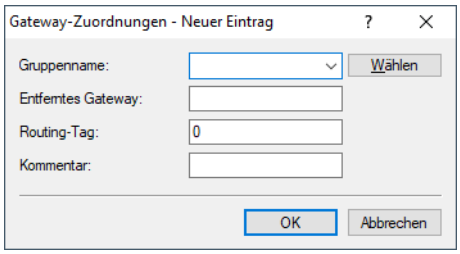
Wählt zufällig einen Eintrag aus der Liste.

Kommentar

Vergeben Sie optional einen sinnvollen Kommentar als Beschreibung.

8.3.3 Gateway-Zuordnungen

Unter **Gateway-Zuordnungen** können Sie Gateway-Gruppen einrichten, die Sie dann unter *Weitere entfernte Gateways* referenzieren können. **Entferntes Gateway** und **Gruppenname** bilden zusammen den Primärschlüssel der Tabelle, d. h. die Kombination aus beiden muss innerhalb der Tabelle eindeutig sein. Damit kann ein einzelner Gateway aber auch mehreren Gruppen zugeordnet werden, insofern das gewünscht ist.



Gruppenname

Name der Gruppe, zu dem der Gateway gehört.

Entferntes Gateway

DNS-Name oder IP-Adresse eines Gateways.

Routing-Tag

Routing-Tag des Gateways.

Kommentar

Vergeben Sie optional einen sinnvollen Kommentar als Beschreibung.

8.3.4 Beispiel eines alternativen Gateways mit priorisierten Gruppen

Der Kunde „Telekom“ nutze den primären Gateway 1.1.1.1 und den zusätzlichen Gateway 1.1.1.2 ohne spezielle Gruppenzugehörigkeit. Darüber hinaus werden unter **VPN** > **Allgemein** > **Entfernte Gateways** die folgenden weiteren entfernten Gateways, Gateway-Gruppen und Gateway-Zuordnungen angegeben:

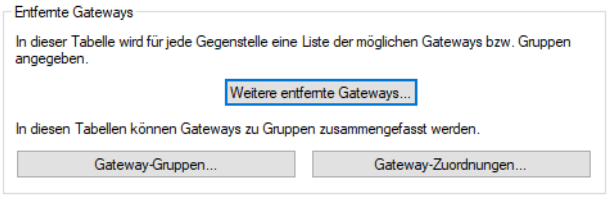


Abbildung 2: Entfernte Gateways

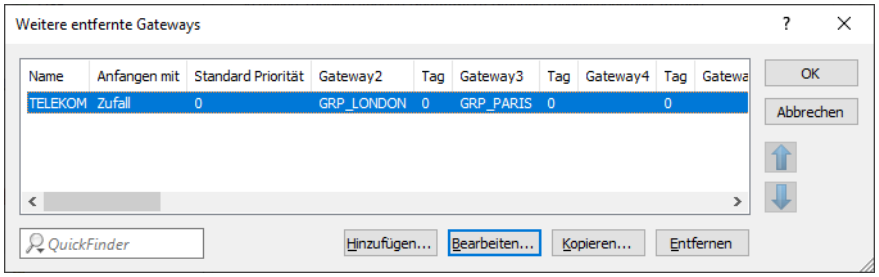


Abbildung 3: Weitere entfernte Gateways

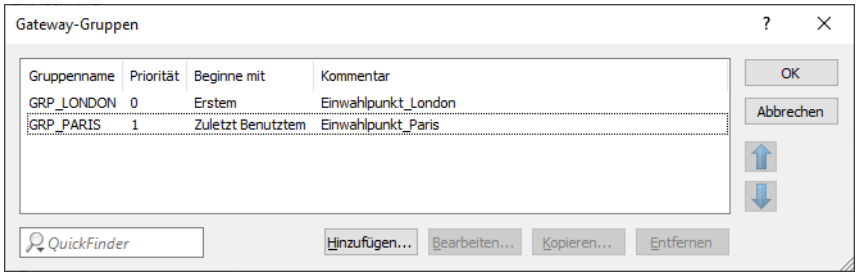


Abbildung 4: Gateway-Gruppen

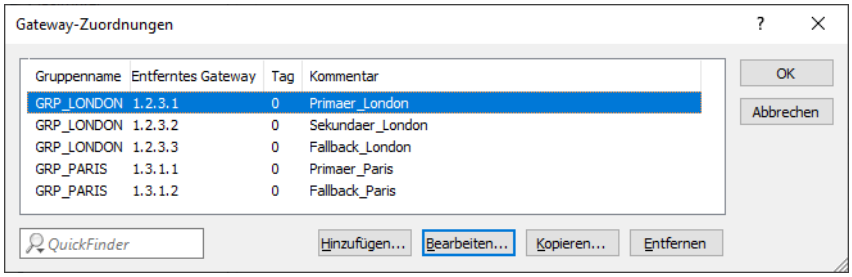


Abbildung 5: Gateway-Zuordnungen

Dadurch würde sich die folgende Ebenenstruktur ergeben:

Priorität	Gruppe 1	Gruppe 2
0	1.1.1.1, 1.1.1.2	GRP_LONDON
1	GRP_PARIS	

Die Gateways würden dann in der folgenden Reihenfolge angesprochen:

1. Priorität 0: Es wird nach dem Zufallsprinzip eine Gruppe ausgewählt, weil in der Tabelle **Weitere entfernte Gateways** die Spalte **Anfangen** mit auf „Zufall" gesetzt ist:
   - 1.1.1.1, 1.1.1.2 (Primärer Gateway sowie zusätzlicher Gateway, der keiner Gruppe angehört)
   - 1.2.3.1, 1.2.3.2, 1.2.3.3 (GRP_LONDON) beginnend mit dem ersten Gateway in dieser Gruppe
2. Priorität 1: Es wird nach dem Zufallsprinzip eine Gruppe ausgewählt, weil in der Tabelle **Weitere entfernte Gateways** die Spalte **Anfangen mit** auf „Zufall" gesetzt ist:
   - 1.3.1.1, 1.3.1.2 (GRP_PARIS) beginnend mit dem letzten Gateway in dieser Gruppe, der zuvor erreicht werden konnte.

8.3.5 Ergänzungen im Setup-Menü

Default-Prio

Dies ist die Standard-Priorität für alle hier definierten Gateways. Die höchste Priorität ist 0, die niedrigste 65535. Alle Gateways werden jeweils in Gruppen zusammengefasst, wobei Gruppen gleicher Priorität auf einer Ebene nebeneinander angesiedelt werden.

Der primäre Gateway wird automatisch in einer eigenen Gruppe mit Priorität 0 angelegt. Wenn der primäre Gateway selbst eine Gateway-Gruppe referenziert, so wird diese Gruppe unabhängig von ihrer konfigurierten Priorität mit der Priorität 0 der Ebenenstruktur hinzugefügt. Werden hier alternative Gateways definiert, die keine Gateway-Gruppe referenzieren, dann werden diese ebenfalls der Gruppe der primären Gateways hinzugefügt.

SNMP-ID:

2.19.12.67

Pfad Konsole:

Setup > **VPN** > **Zusaetzliche-Gateway-Liste**

Mögliche Werte:

0 … 65535

Default-Wert:

0

Gateway-Gruppen

In dieser Tabelle finden Sie die Einstellungen für Gateway-Gruppen, die Sie dann in der Liste der zusätzlichen Gateways referenzieren können.

SNMP-ID:

2.19.65

Pfad Konsole:

Setup > **VPN**

Gruppen-Name

Geben Sie dieser Gateway-Gruppe einen eindeutigen Namen, über den Sie diese Gruppe referenzieren können.

SNMP-ID:

2.19.65.1

Pfad Konsole:

Setup > **VPN** > **Gateway-Gruppen**

Mögliche Werte:

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

Prioritaet

Die Priorität dieser Gruppe.

SNMP-ID:

2.19.65.2

Pfad Konsole:

Setup > **VPN** > **Gateway-Gruppen**

Mögliche Werte:

0 … 65535

Anfangen-mit

Auswahl-Strategie innerhalb der Gruppe.

SNMP-ID:

2.19.65.3

Pfad Konsole:

Setup > **VPN** > **Gateway-Gruppen**

Mögliche Werte:

zuletzt-verwendetem

Beginnt mit dem Gateway in der Gruppe, über den zuletzt eine Verbindung erfolgreich aufgebaut werden konnte.

erstem

Beginnt mit dem ersten Eintrag in der Liste.

zufaelligem

Wählt zufällig einen Eintrag aus der Liste.

Kommentar

Vergeben Sie optional einen sinnvollen Kommentar als Beschreibung.

SNMP-ID:

2.19.65.4

Pfad Konsole:

Setup > **VPN** > **Gateway-Gruppen**

Mögliche Werte:

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

Gateway-Zuordnungen

In dieser Tabelle finden Sie die Einstellungen zu den Gateway-Zuordnungen. Über Gateway-Zuordnungen können Sie Gateway-Gruppen (siehe auch *2.19.65 Gateway-Gruppen* auf Seite 139) einrichten, die Sie dann unter *2.19.12 Zusaetzliche-Gateway-Liste* referenzieren können. Gateway und Gruppenname bilden zusammen den Primärschlüssel der Tabelle, d. h. die Kombination aus beiden muss innerhalb der Tabelle eindeutig sein. Damit kann ein einzelner Gateway aber auch mehreren Gruppen zugeordnet werden, insofern das gewünscht ist.

SNMP-ID:

2.19.66

Pfad Konsole:

Setup > **VPN**

Gruppen-Name

Name der Gruppe, zu dem der Gateway gehört.

SNMP-ID:

2.19.66.1

Pfad Konsole:

Setup > **VPN** > **Gateway-Zuordnungen**

Mögliche Werte:

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

Gateway

DNS-Name oder IP-Adresse eines Gateways.

SNMP-ID:

2.19.66.2

Pfad Konsole:

Setup > **VPN** > **Gateway-Zuordnungen**

Mögliche Werte:

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

Rtg-Tag

Routing-Tag des Gateways.

SNMP-ID:

2.19.66.3

Pfad Konsole:

Setup > **VPN** > **Gateway-Zuordnungen**

Mögliche Werte:

0 … 65535

Default-Wert:

0

Kommentar

Vergeben Sie optional einen sinnvollen Kommentar als Beschreibung.

SNMP-ID:

2.19.66.4

Pfad Konsole:

Setup > **VPN** > **Gateway-Zuordnungen**

Mögliche Werte:

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

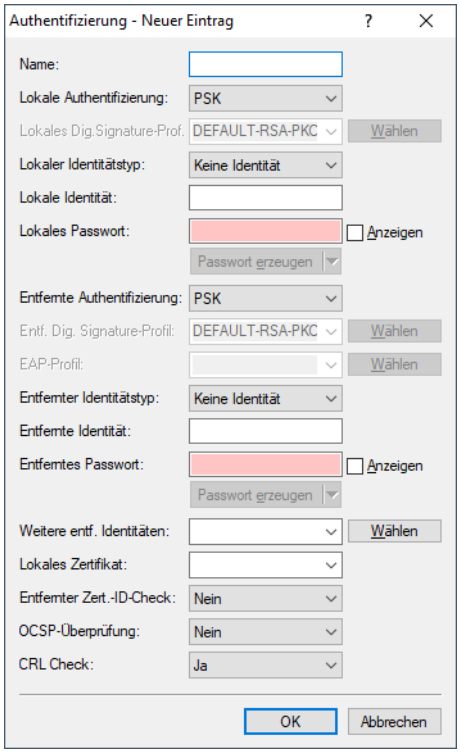
8.4 Unterstützung für Extensible Authentication Protocol (EAP) bei IKEv2

Ab LCOS-Version 10.40 wird die Authentifizierung von IKEv2-Clients durch EAP (Extensible Authentication Protocol) unterstützt. EAP ist kein festes Authentifizierungsverfahren, sondern es bietet einen Rahmen für beliebige Authentifizierungsverfahren, wie beispielsweise TLS (Authentifizierung per Zertifikat) oder MSCHAP (Authentifizierung per Benutzername / Passwort).

Die EAP-Authentifizierung übernimmt dabei ein externer RADIUS-Server wie z. B. der LANCOM RADIUS Server, FreeRADIUS oder Microsoft Network Policy Server (NPS). Das VPN-Gateway übernimmt dabei nur die Vermittlerrolle zwischen Client und RADIUS-Server. Das VPN-Gateway muss sich gegenüber dem Client mit einem gültigen Zertifikat per RSA-Signature-Verfahren authentifizieren. Der RADIUS-Server muss ebenso ein gültiges Zertifikat vorweisen. Die notwendigen Zertifikate können beispielsweise mit der LANCOM SCEP CA im Router erstellt werden. Nach der Erstellung müssen die jeweiligen Zertifikatsconatiner in das VPN-Gateway sowie in den RADIUS-Server importiert werden.

Die Nutzung des Features IKEv2 EAP-Authentifizierung benötigt auf LANCOM Routern die VPN-25 Option oder einen Router mit 25 oder mehr VPN-Tunneln. Ob der Router IKEv2 EAP unterstützt, kann im LCOS Status-Menü unter **Status** > **Software-Info** > **IKEv2-EAP-License** überprüft werden.

Unter **VPN** > **IKEv2/IPSec** > **Authentifizierung** können Sie für die **entfernte Authentifizierung** die Methode EAP auswählen. In diesem Fall geben Sie dann optional das zu verwendende EAP-Profil an.



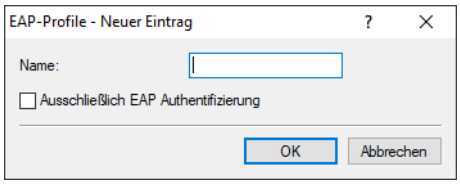
EAP-Profil

Geben Sie ein EAP-Profil an, wenn als Methode für die **Entfernte Authentifizierung** EAP ausgewählt wurde. Die EAP-Profile werden unter *EAP-Profile* definiert.

Unter **VPN** > **IKEv2/IPSec** > **Erweiterte Einstellungen** > **Authentifizierung** > **EAP-Profile** können Sie die EAP-Profile definieren.

EAP-Profile

In dieser Tabelle konfigurieren Sie EAP-Profile. Diese wählen Sie bei der **Authentifizierung** aus, wenn Sie als Methode für die **entfernte Authentifizierung** EAP auswählen.



Name

Geben Sie diesem EAP-Profil einen Namen, über den es referenziert werden kann.

Ausschließlich EAP-Authentifzierung

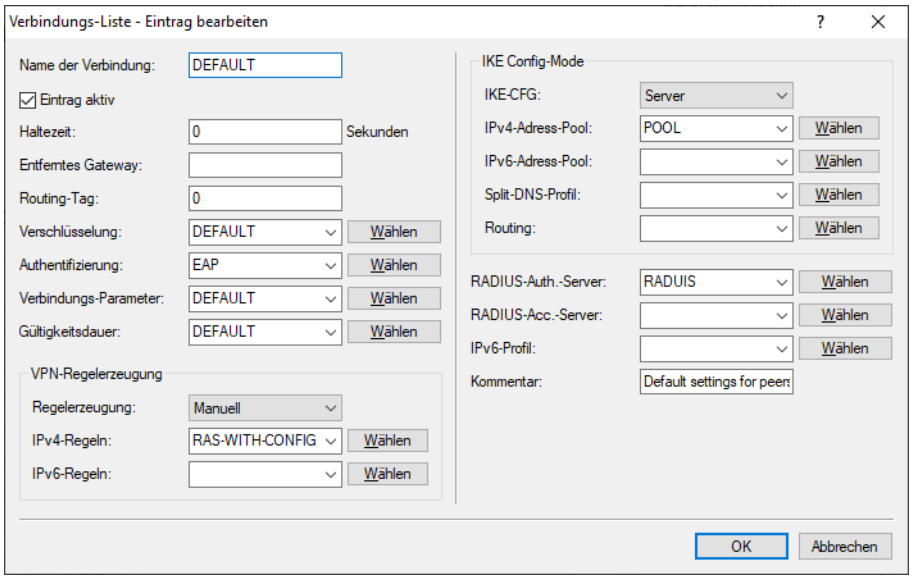
Erlaubt optional die gegenseitige Authentifizierung der Gegenstellen innerhalb des EAP. Die Authentifizierung außerhalb des EAP entfällt dann. Siehe auch *RFC 5998*.

8.4.1 Tutorial – EAP-Client gegen einen EAP-Server

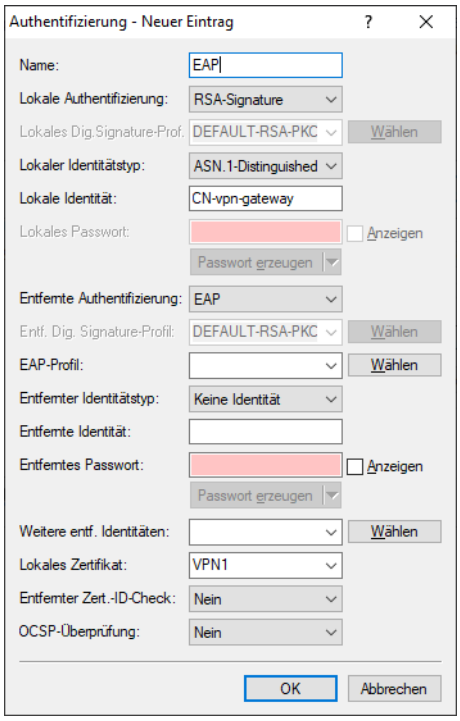
Im folgenden Tutorial soll ein EAP-Client gegen einen EAP-Server konfiguriert werden.

1. Erstellen Sie zwei Zertifikate bzw. Zertifikatscontainer, z. B. mit der LANCOM SCEP CA oder OpenSSL.
2. Importieren Sie sowohl ein Zertifikat in das VPN-Gateway als auch ein Zertifikat in den RADIUS-Server.

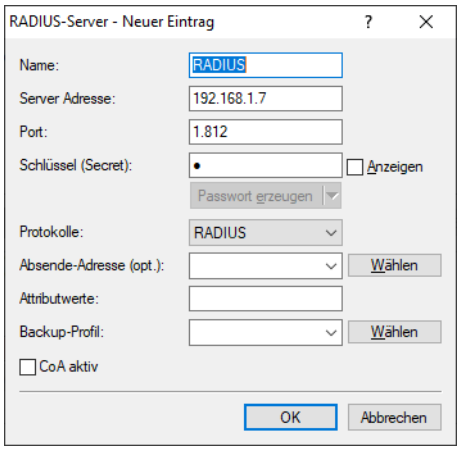
   Achten Sie darauf, dass der Subject Alternative Name (SAN) dem gültigen DNS-Namen des VPN-Gateways entspricht und der VPN-Client das Gateway unter diesem DNS-Namen kontaktiert.
3. Zur Herstellung der Vertrauensbeziehung importieren Sie zusätzlich das gültige CA-Zertifikat in den IKEv2-EAP-Client.
4. Editieren Sie den DEFAULT-Eintrag der IKEv2-Gegenstellen-Tabelle unter **VPN** > **IKEv2/IPSec** > **VPN-Verbindungen** > **Verbindungs-Liste** wie folgt:



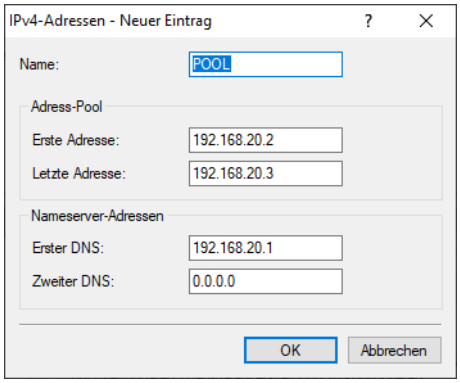
5. Legen Sie eine neue Zeile in der Tabelle IKEv2-Authentifizierung unter **VPN** > **IKEv2/IPSec** > **Authentifizierung** an. Die Lokale Authentifizierung des VPN-Gateways erfolgt über Zertifikat (RSA-Signature), die Entfernte Authentifizierung der Clients erfolgt per EAP.



6. Konfigurieren Sie den RADIUS-Server unter **VPN** > **IKEv2/IPSec** > **Erweiterte Einstellungen** > **RADIUS-Authentifizierung** > **RADIUS-Server**.



7. Konfigurieren Sie einen Adress-Pool unter **VPN** > **IKEv2/IPSec** > **IPv4-Adressen**.



8.4.2 Ergänzungen im Setup-Menü

Remote-Auth

Legt die Authentifizierungsmethode für die entfernte Identität fest.

SNMP-ID:

2.19.36.3.1.6

Pfad Konsole:

Setup > **VPN** > **IKEv2** > **Auth** > **Parameter**

Mögliche Werte:

RSA-Signature
Die Authentifizierung erfolgt über eine RSA-Signatur.

PSK
Die Authentifizierung erfolgt über Pre-shared Key (PSK).

Digital-Signature
Verwendung von konfigurierbaren Authentifizierungsmethoden mit digitalen Zertifikaten nach *RFC 7427*.

EAP
Die Authentifizierung erfolgt über das Extensible Authentication Protocol (EAP) nach *RFC 3748*.

ECDSA-256
Elliptic Curve Digital Signature Algorithm (ECDSA) nach *RFC 4754* mit SHA-256 auf der P-256-Kurve.

ECDSA-384
Elliptic Curve Digital Signature Algorithm (ECDSA) nach *RFC 4754* mit SHA-384 auf der P-384-Kurve.

ECDSA-521
Elliptic Curve Digital Signature Algorithm (ECDSA) nach *RFC 4754* mit SHA-512 auf der P-521-Kurve.

Default-Wert:

PSK

Remote-EAP-Profil

Referenziert ein *EAP-Profil*.

SNMP-ID:

2.19.36.3.1.16

Pfad Konsole:

Setup > **VPN** > **IKEv2** > **Auth** > **Parameter**

Mögliche Werte:

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

Default-Wert:

DEFAULT

EAP-Profile

In dieser Tabelle konfigurieren Sie die EAP-Profile.

SNMP-ID:

2.19.36.3.5

Pfad Konsole:

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

Name

Geben Sie diesem EAP-Profil einen Namen, über den es referenziert werden kann.

SNMP-ID:

2.19.36.3.5.1

Pfad Konsole:

Setup > **VPN** > **IKEv2** > **EAP-Profile**

Mögliche Werte:

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

EAP-Only-Authentication

Erlaubt optional die gegenseitige Authentifizierung der Gegenstellen innerhalb des EAP. Die Authentifizierung außerhalb des EAP entfällt dann. Siehe auch *RFC 5998*

SNMP-ID:

2.19.36.3.5.4

Pfad Konsole:

Setup > **VPN** > **IKEv2** > **EAP-Profile**

Mögliche Werte:

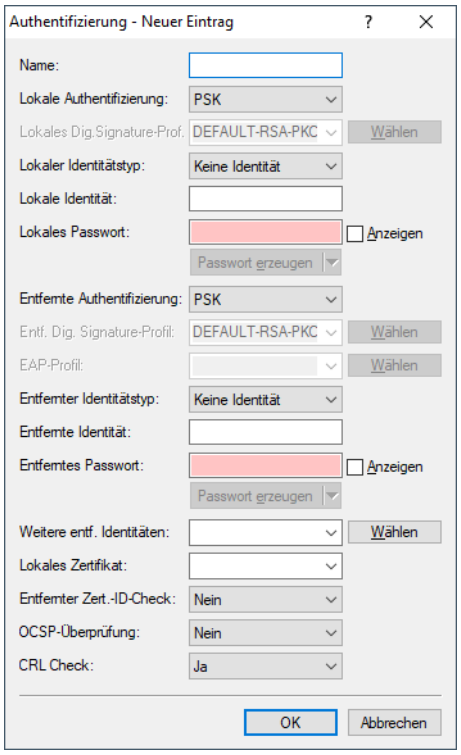
Nein
Ja

Optionale Authentifizierung der Gegenstellen innerhalb des EAP möglich.

8.5 Überprüfung von Zertifikatssperrlisten bei IKEv2 abschaltbar

Ab LCOS-Version 10.40 kann die Überprüfung des Gültigkeitsstatus von X.509-Zertifikaten via Zertifikatssperrlisten (Certificate Revocation List, CRL) abgeschaltet werden.

Unter **VPN** > **IKEv2/IPSec** > **Authentifizierung** können Sie über die Option **CRL Check** die Überprüfung abschalten.



CRL Check

Mit dieser Einstellung aktivieren Sie die Überprüfung eines X.509-Zertifikats via Zertifikatssperrlisten (Certificate Revocation List, CRL), welche den Gültigkeitsstatus des Zertifikats der Gegenstelle abfragt.

Schalten Sie diese Überprüfung nur ab, wenn Sie die Überprüfung auf einem anderen Weg durchführen, z. B. über OSCP.

8.5.1 Ergänzungen im Setup-Menü

CRL-Check

Mit dieser Einstellung aktivieren Sie die Überprüfung eines X.509-Zertifikats via Zertifikatssperrlisten (Certificate Revocation List, CRL), welche den Gültigkeitsstatus des Zertifikats der Gegenstelle abfragt.

Schalten Sie diese Überprüfung nur ab, wenn Sie die Überprüfung auf einem anderen Weg durchführen, z. B. über OSCP.

SNMP-ID:

2.19.36.3.1.17

Pfad Konsole:

Setup > **VPN** > **IKEv2** > **Auth** > **Parameter**

Mögliche Werte:

nein
ja

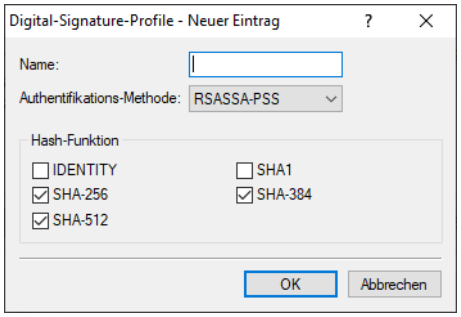
Default-Wert:

ja

8.6 Digitale Signatur-Profile

Ab LCOS-Version 10.40 unterstützt Ihr Gerät die Verfahren Elliptic Curve Digital Signature Algorithm (ECDSA), Edwards Curve 2551 (EdDSA25519) und Edwards Curve 448 (EdDSA448) als Authentifizierungs-Methoden bei den digitalen Signatur-Profilen.

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



Authentifizierungs-Methode

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

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

- EdDSA25519: Edwards Curve 2551 (EdDSA25519) nach *RFC 8420*
- EdDSA448: Edwards Curve 448 (EdDSA448) nach *RFC 8420*

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

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

8.6.1 Ergänzungen im Setup-Menü

Auth-Methode

Legt die Authentifizierungsmethode für die Digitale Signatur fest.

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

SNMP-ID:

2.19.36.3.4.2

Pfad Konsole:

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

Mögliche Werte:

RSASSA-PSS
RSASSA-PKCS1-v1_5
ECDSA
Elliptic Curve Digital Signature Algorithm
EdDSA25519
Authentifzierung nach EdDSA25519 (Edwards Curve 2551) nach *RFC 8420*.
EdDSA448
Authentifzierung nach EdDSA448 (Edwards Curve 448) nach *RFC 8420*.

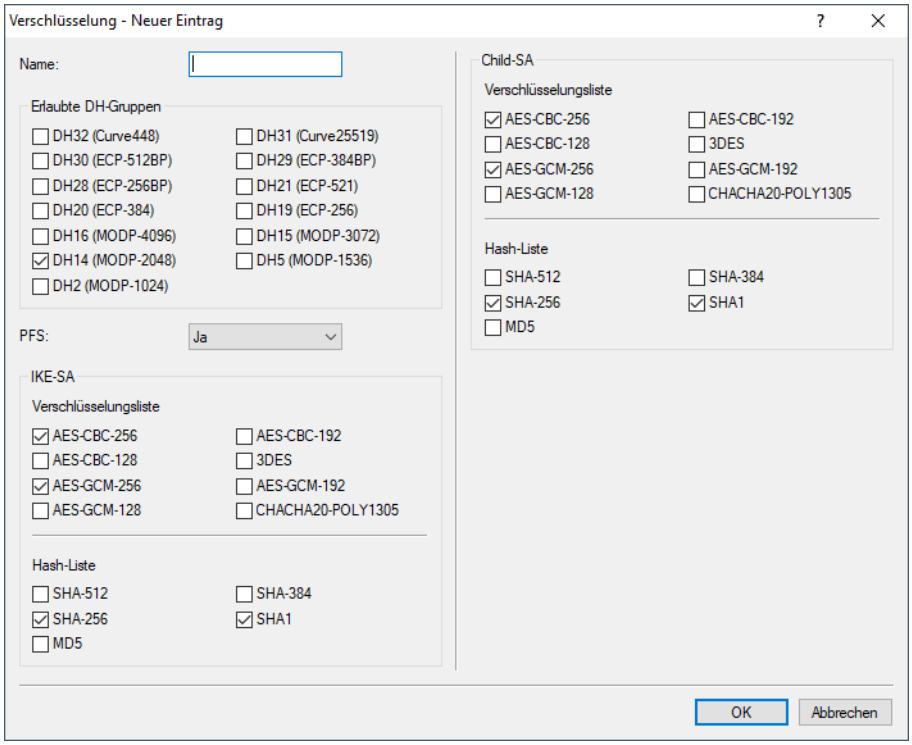
Default-Wert:

RSASSA-PSS

8.7 Erweiterung der DH-Gruppen und Verschlüsselungsalgorithmen bei IKEv2

Ab LCOS-Version 10.40 werden die DH-Gruppen DH-31 (Curve25519) und DH-32 (Curve448) unterstützt. Zudem wird mit Chacha20-Poly1305 die ChaCha20 Datenstromverschlüsselung zusammen mit dem Poly1305 Authentifikator unterstützt, siehe *RFC 7634*.

Bitte beachten Sie, dass ChaCha20-Poly1305 derzeit nicht durch Hardware beschleunigt wird und daher nicht für VPN-Szenarien empfohlen wird, in denen eine hohe Verschlüsselungsleistung benötigt wird.



8.7.1 Ergänzungen im Setup-Menü

DH-Gruppen

Enthält die Auswahl der Diffie-Hellman-Gruppen.

SNMP-ID:

2.19.36.2.2

Pfad Konsole:

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

Mögliche Werte:

DH32

Curve448 (ab LCOS-Version 10.40)

DH31

Curve25519 (ab LCOS-Version 10.40)

DH30

(ab LCOS-Version 10.12)

DH29

(ab LCOS-Version 10.12)

DH28

(ab LCOS-Version 10.12)

DH21
(ab LCOS-Version 10.12)
DH20
(ab LCOS-Version 10.12)
DH19
(ab LCOS-Version 10.12)
DH16
DH15
DH14
DH5
DH2

Default-Wert:

DH14

IKE-SA-Verschlüsselungsliste

Gibt an, welche Verschlüsselungsalgorithmen aktiviert sind.

SNMP-ID:

2.19.36.2.4

Pfad Konsole:

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

Mögliche Werte:

AES-CBC-256
AES-CBC-192
AES-CBC-128
3DES
AES-GCM-256
Advanced Encryption Standard (AES) 256 in Galois / Counter Mode (GCM)
AES-GCM-192
Advanced Encryption Standard (AES) 192 in Galois / Counter Mode (GCM)
AES-GCM-128
Advanced Encryption Standard (AES) 128 in Galois / Counter Mode (GCM)
Chacha20-Poly1305
ChaCha20 Datenstromverschlüsselung zusammen mit dem Poly1305 Authentifikator, siehe *RFC 7634*, wird ab LCOS-Version 10.40 unterstützt.


Bitte beachten Sie, dass ChaCha20-Poly1305 derzeit nicht durch Hardware beschleunigt wird und daher nicht für VPN-Szenarien empfohlen wird, in denen eine hohe Verschlüsselungsleistung benötigt wird.

Default-Wert:

AES-CBC-256

AES-GCM-256

Child-SA-Verschlüsselungsliste

Gibt an, welche Verschlüsselungsalgorithmen in der Child-SA aktiviert sind.

SNMP-ID:

2.19.36.2.6

Pfad Konsole:

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

Mögliche Werte:

AES-CBC-256
AES-CBC-192
AES-CBC-128
3DES
AES-GCM-256

Advanced Encryption Standard (AES) 256 in Galois / Counter Mode (GCM)

AES-GCM-192

Advanced Encryption Standard (AES) 192 in Galois / Counter Mode (GCM)

AES-GCM-128

Advanced Encryption Standard (AES) 128 in Galois / Counter Mode (GCM)

Chacha20-Poly1305

ChaCha20 Datenstromverschlüsselung zusammen mit dem Poly1305 Authentifikator, siehe *RFC 7634*, wird ab LCOS-Version 10.40 unterstützt.

Bitte beachten Sie, dass ChaCha20-Poly1305 derzeit nicht durch Hardware beschleunigt wird und daher nicht für VPN-Szenarien empfohlen wird, in denen eine hohe Verschlüsselungsleistung benötigt wird.

Default-Wert:

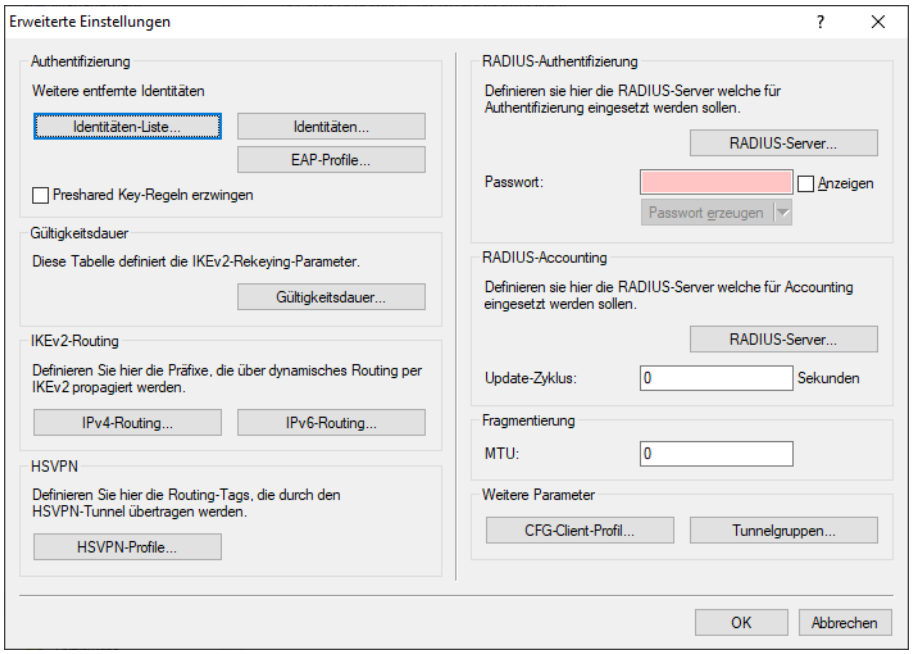
AES-CBC-256

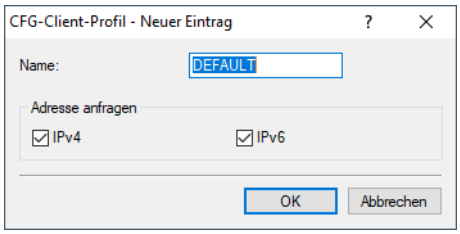
AES-GCM-256

8.8 Anfragen der Adresse im IKEv2-CFG-Mode konfigurierbar

Ab LCOS-Version 10.40 unterstützt Ihr Gerät die Option, die Anfrage der Adresse im IKEv2-CFG-Mode zu konfigurieren.

In LANconfig erfolgt die Konfiguration der CFG-Client-Profile unter **VPN** > **IKEv2/IPSec** > **Erweiterte Einstellungen** > **Weitere Parameter** über **CFG-Client-Profile**.





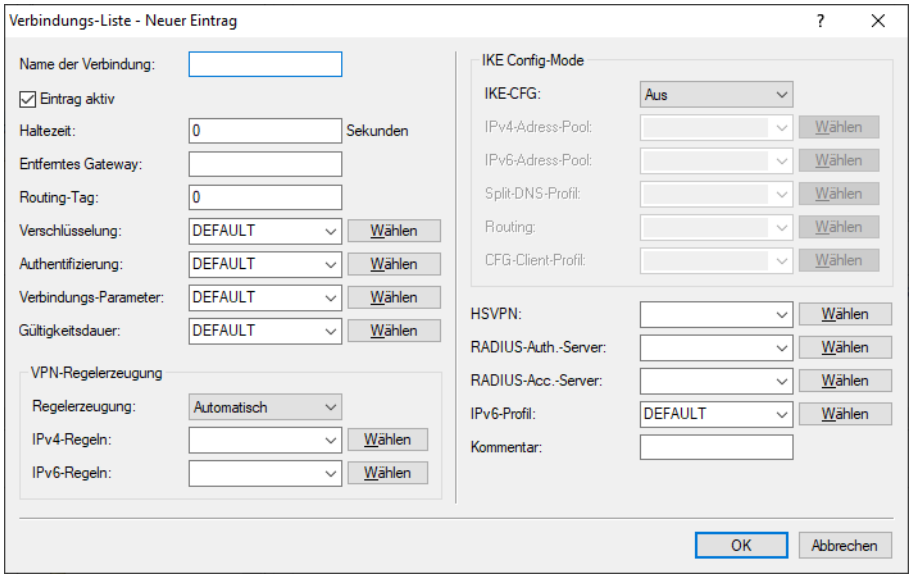
Name

Eindeutiger Name für das CFG-Client-Profil.

Adresse anfragen

Bestimmen Sie, ob für dieses Profil Adressen für IPv4 und / oder IPv6 angefragt werden sollen.

Diese Profile können Sie dann bei den VPN-Verbindungen unter **VPN** > **IKEv2/IPSec** > **Verbindungs-Liste** auswählen.



CFG-Client-Profil

Wählen Sie ein CFG-Client-Profil aus, welches Sie unter *CFG-Client-Profil* angelegt haben. Dieses Profil bestimmt, ob das Gerät in der Rolle CFG-Mode Client eine Adresse beim CFG-Mode-Server anfragen soll.

8.8.1 Ergänzungen im Setup-Menü

CFG-Client-Profil

Definieren Sie hier den Namen des Client-Profils aus der Tabelle *Client-Profil*. Dieses bestimmt, ob das Gerät in der Rolle CFG-Mode Client eine Adresse beim CFG-Mode-Server anfragen soll.

SNMP-ID:

2.19.36.1.24

Pfad Konsole:

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

Mögliche Werte:

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

Client-Profil

In dieser Tabelle können Sie definieren, ob das Gerät in der Rolle CFG-Mode Client eine Adresse beim CFG-Mode-Server anfragen soll. Diese Funktion wird in der Regel in Zusammenhang mit IKEv2-Routing verwendet.

SNMP-ID:

2.19.36.7.4

Pfad Konsole:

Setup > **VPN** > **IKEv2** > **IKE-CFG**

Name

Vergeben Sie einen Namen für das Client-Profil.

SNMP-ID:

2.19.36.7.4.1

Pfad Konsole:

Setup > **VPN** > **IKEv2** > **IKE-CFG** > **Client-Profil**

Mögliche Werte:

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

Request-Address

Definiert welcher Adresstyp im Config-Mode angefragt werden soll.

SNMP-ID:

2.19.36.7.4.2

Pfad Konsole:

Setup > **VPN** > **IKEv2** > **IKE-CFG** > **Client-Profil**

Mögliche Werte:

None
IPv4
IPv6

Default-Wert:

IPv4

IPv6

8.9 IKEv2-Tunnelgruppen

In bestimmten VPN-Szenarien ist es erforderlich, dass eine bestimmte Gruppe von VPN-Tunneln eines Geräts immer auf einem gemeinsamen VPN-Gateway terminiert wird bzw. zu diesem aufbaut. Dies ist beispielsweise dann erforderlich, wenn VPN-Tunnel in einem Load-Balancer-Verbund konfiguriert sind und VPN-Tunnel die alternative Gateway-Liste verwenden und ggf. unterschiedliche Wege bzw. ausgehende Internetverbindungen (DSL, LTE, Ethernet) zum Ziel nutzen.

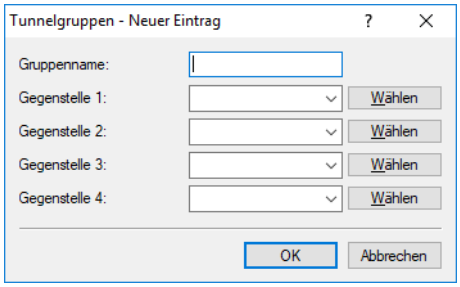
Voraussetzung für einen VPN-Load-Balancer ist, dass alle VPN-Tunnel immer auf einem gemeinsamen VPN-Gateway terminieren.

Die Funktion IKEv2-Tunnelgruppen stellt sicher, dass alle VPN-Tunnel einer Gruppe immer auf einem gemeinsamen VPN-Gateway terminieren. Der erste funktionierend aufgebaute VPN-Tunnel einer Gruppe gibt das gemeinsame VPN-Gateway vor und es werden VPN-Remote-Gateways aller anderen Tunnelgruppenmitglieder auf dieses Ziel umgeschrieben. In der Regel ist das der VPN-Tunnel, der am schnellsten zu Stande kommt. Eine neue Auswahl eines Gateways findet nur statt, wenn alle Tunnelgruppen-Mitglieder das Gateway nicht erreichen können.

Die Funktion der IKEv2-Tunnelgruppen kann grundsätzlich unabhängig von einem Load-Balancer genutzt werden.

Tunnelgruppen werden nicht in Zusammenhang mit IKEv2-Redirect und dem IKEv2 Redirect Load-Balancer unterstützt.

Wechseln Sie zur Konfiguration in LANconfig in die Ansicht **VPN** > **IKEv2/IPSec** > **Erweiterte Einstellungen** und konfigurieren Sie im Abschnitt **Weitere Parameter** die **Tunnelgruppen**.



Gruppenname

Eindeutiger Name für die Tunnelgruppe.

Gegenstelle 1-4

Jeweiliger Gegenstellenname des IKEv2 VPN-Tunnels, der in der Tunnelgruppe terminiert.

8.9.1 Ergänzungen im Setup-Menü

Tunnel-Gruppen

In bestimmten VPN-Szenarien ist es erforderlich, dass eine bestimmte Gruppe von VPN-Tunneln eines Geräts immer auf einem gemeinsamen VPN-Gateway terminiert wird bzw. zu diesem aufbaut. Dies ist beispielsweise dann erforderlich, wenn VPN-Tunnel in einem Load-Balancer-Verbund konfiguriert sind und VPN-Tunnel die alternative Gateway-Liste verwenden und ggf. unterschiedliche Wege bzw. ausgehende Internetverbindungen (DSL, LTE, Ethernet) zum Ziel nutzen.

Voraussetzung für einen VPN-Load-Balancer ist, dass alle VPN-Tunnel immer auf einem gemeinsamen VPN-Gateway terminieren.

Die Funktion IKEv2-Tunnelgruppen stellt sicher, dass alle VPN-Tunnel einer Gruppe immer auf einem gemeinsamen VPN-Gateway terminieren. Der erste funktionierend aufgebaute VPN-Tunnel einer Gruppe gibt das gemeinsame VPN-Gateway vor und es werden VPN-Remote-Gateways aller anderen Tunnelgruppenmitglieder auf dieses Ziel umgeschrieben. In der Regel ist das der VPN-Tunnel, der am schnellsten zu Stande kommt. Eine neue Auswahl eines Gateways findet nur statt, wenn alle Tunnelgruppen-Mitglieder das Gateway nicht erreichen können.

Die Funktion der IKEv2-Tunnelgruppen kann grundsätzlich unabhängig von einem Load-Balancer genutzt werden.

Tunnelgruppen werden nicht in Zusammenhang mit IKEv2-Redirect und dem IKEv2 Redirect Load-Balancer unterstützt.

SNMP-ID:

2.19.36.13

Pfad Konsole:

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

Gruppen-Name

Eindeutiger Name für die Tunnelgruppe.

SNMP-ID:

2.19.36.13.1

Pfad Konsole:

Setup > **VPN** > **IKEv2** > **Tunnel-Gruppen**

Mögliche Werte:

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

Gegenstelle-1

Ein Gegenstellenname des IKEv2 VPN-Tunnels, der in der Tunnelgruppe terminiert.

SNMP-ID:

2.19.36.13.2

Pfad Konsole:

Setup > **VPN** > **IKEv2** > **Tunnel-Gruppen**

Mögliche Werte:

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

Gegenstelle-2

Ein Gegenstellenname des IKEv2 VPN-Tunnels, der in der Tunnelgruppe terminiert.

SNMP-ID:

2.19.36.13.3

Pfad Konsole:

Setup > **VPN** > **IKEv2** > **Tunnel-Gruppen**

Mögliche Werte:

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

Gegenstelle-3

Ein Gegenstellenname des IKEv2 VPN-Tunnels, der in der Tunnelgruppe terminiert.

SNMP-ID:

2.19.36.13.4

Pfad Konsole:

Setup > **VPN** > **IKEv2** > **Tunnel-Gruppen**

Mögliche Werte:

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

Gegenstelle-4

Ein Gegenstellenname des IKEv2 VPN-Tunnels, der in der Tunnelgruppe terminiert.

SNMP-ID:

2.19.36.13.5

Pfad Konsole:

Setup > **VPN** > **IKEv2** > **Tunnel-Gruppen**

Mögliche Werte:

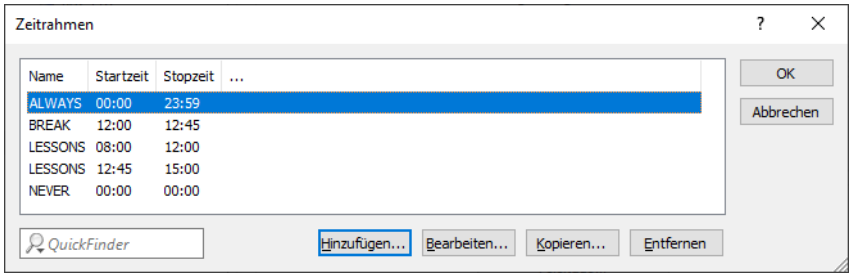
max. 16 Zeichen aus `[A-Z][0-9]@{|}~!$%&'()+-,/:;< =>?[\]^_.`

9 Wireless LAN – WLAN

9.1 Zeitsteuerung für SSIDs

Ab LCOS 10.40 lassen sich einzelne SSIDs anhand eines Zeitplans ein- und ausschalten. Somit lässt sich z. B. in einer Schule ein WLAN nur während der Unterrichtszeiten aktivieren. Oder ein Hotspot wird nur während der Geschäftszeiten aktiviert oder in einer Schule nur während der Pausen für die Schüler zur Verfügung gestellt.

Dazu definieren Sie im ersten Schritt die zu verwendenden Zeitrahmen in der Zeitrahmen-Tabelle unter **Datum/Zeit** > **Allgemein** > **Zeitrahmen**.



Name

Hier muss der Name des Zeitrahmens angegeben werden, über den dieser im Content-Filter-Profil oder bei einer WLAN-SSID referenziert wird. Mehrere Einträge gleichen Namens ergeben dabei ein gemeinsames Profil.

Mögliche Werte:

- Name eines Zeitrahmens

Startzeit

Hier kann die Startzeit (Tageszeit) angegeben werden, ab der das gewählte Profil gelten soll.

Mögliche Werte:

- Format HH:MM (Default: 00:00)

Stoppzeit

Hier kann die Stoppzeit (Tageszeit) angegeben werden, ab der das gewählte Profil nicht mehr gültig sein soll.

Mögliche Werte:

- Format HH:MM (Default: 23:59)

Eine Stoppzeit von HH:MM geht normalerweise bis HH:MM:00. Eine Ausnahme ist die Stoppzeit 00:00, die als 23:59:59 interpretiert wird.

Wochentage

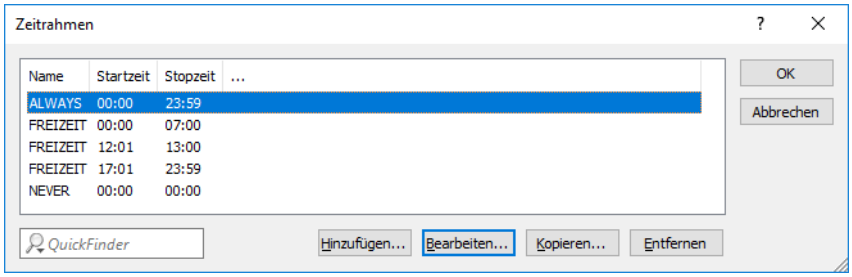
Hier können Sie die Wochentage auswählen, an denen der Zeitrahmen gültig sein soll.

Mögliche Werte:

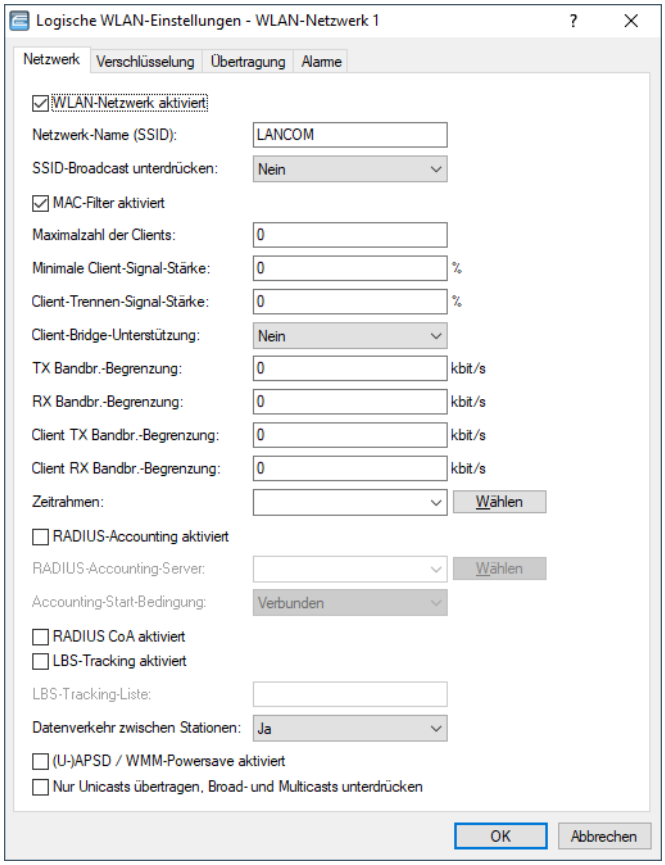
- Montag, Dienstag, Mittwoch, Donnerstag, Freitag, Samstag, Sonntag, Feiertag

Die Feiertage werden unter **Datum/Zeit** > **Allgemein** > **Feiertage** eingestellt.

Zeitschemata lassen sich mit gleichem Namen, aber unterschiedlichen Zeiten auch über mehrere Zeilen hinweg definieren:



Im zweiten Schritt wählen Sie dann unter **Wireless-LAN** > **Allgemein** > **Logische WLAN-Einstellungen** > **Netzwerk** den **Zeitrahmen** aus.



Zeitrahmen

Wählen Sie hier einen der in *Zeitrahmen* definierten Zeitrahmen aus. Über diesen kann die Ausstrahlung dieser SSID auf die dort definierten Zeiten eingeschränkt werden. Somit lässt sich z. B. in einer Schule ein WLAN nur während der Unterrichtszeiten aktivieren.

9.1.1 Ergänzungen im Setup-Menü

Stopp

Hier kann die Endzeit (Tageszeit) im Format HH:MM angegeben werden, bis zu der das gewählte Profil gelten soll.

Eine Stoppzeit von HH:MM geht normalerweise bis HH:MM:00. Eine Ausnahme ist die Stoppzeit 00:00, die als 23:59:59 interpretiert wird.

SNMP-ID:

2.14.16.3

Pfad Konsole:

Setup > **Zeit** > **Zeitrahmen**

Mögliche Werte:

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

Default-Wert:

00:00

Zeitrahmen

Wählen Sie hier einen der in *2.14.16 Zeitrahmen* definierten Zeitrahmen aus. Über diesen kann die Ausstrahlung dieser SSID auf die dort definierten Zeiten eingeschränkt werden. Somit lässt sich z. B. in einer Schule ein WLAN nur während der Unterrichtszeiten aktivieren.

SNMP-ID:

2.23.20.1.31

Pfad Konsole:

Setup > **Schnittstellen** > **WLAN** > **Netzwerk**

Mögliche Werte:

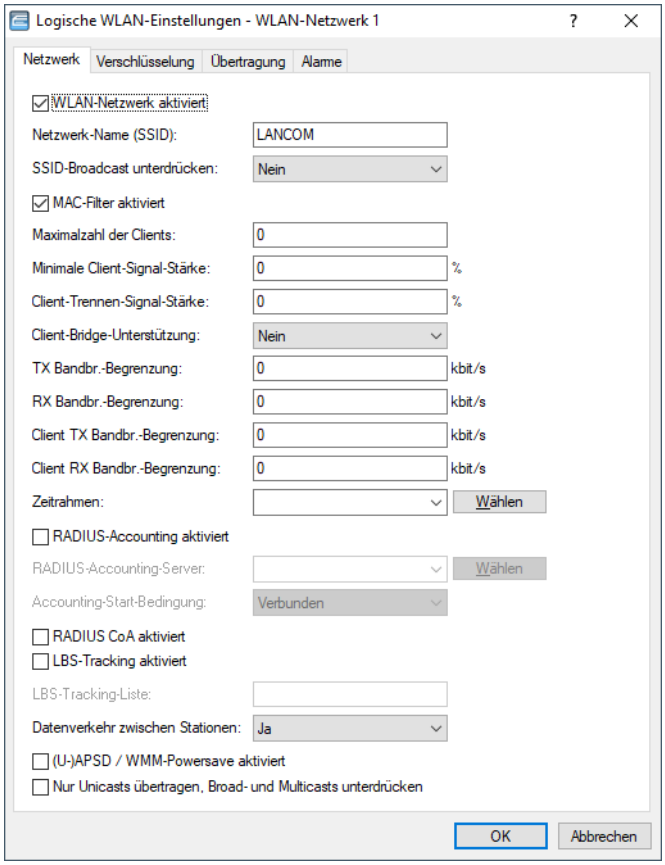
max. 16 Zeichen aus `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default-Wert:

leer

9.2 Signalstärke, ab der ein Client getrennt wird

Ab LCOS 10.40 ist es möglich, einen Client bei zu geringer Signalstärke zu disassoziieren.



Client-Trennen-Signal-Stärke

Wenn dieser Schwellenwert unterschritten wird, dann wird der Client disassoziiert. Dadurch lässt sich vermeiden, dass der Client an einer aufgrund der geringen Signalstärke de facto bereits unbrauchbaren WLAN-Verbindung hängen bleibt anstatt auf eine am Client oft ebenfalls verfügbare Mobiltelefon-Verbindung umzuschalten – ein Verhalten, welches sich bei Mobiltelefonen immer wieder beobachten lässt und für den Benutzer ärgerlich ist.

Dieser Schwellenwert funktioniert nur, wenn auch der Wert **Minimale Client-Signal-Stärke** gesetzt ist und außerdem **Client-Trennen-Signal-Stärke** kleiner als dieser Wert ist.

9.2.1 Ergänzungen im Setup-Menü

Min-Stations-Disassoc-Staerke

Wenn dieser Schwellenwert unterschritten wird, dann wird der Client disassoziiert. Dadurch lässt sich vermeiden, dass der Client an einer aufgrund der geringen Signalstärke de facto bereits unbrauchbaren WLAN-Verbindung hängen bleibt anstatt auf eine am Client oft ebenfalls verfügbare Mobiltelefon-Verbindung umzuschalten – ein Verhalten, welches sich bei Mobiltelefonen immer wieder beobachten lässt und für den Benutzer ärgerlich ist.

Dieser Schwellenwert funktioniert nur, wenn auch der Wert *2.23.20.1.16 Minimal-Stations-Staerke* gesetzt ist und außerdem Min-Stations-Disassoc-Staerke kleiner als dieser Wert ist.

SNMP-ID:

2.23.20.1.32

Pfad Konsole:

Setup > **Schnittstellen** > **WLAN** > **Netzwerk**

Mögliche Werte:

0 … 100

Default-Wert:

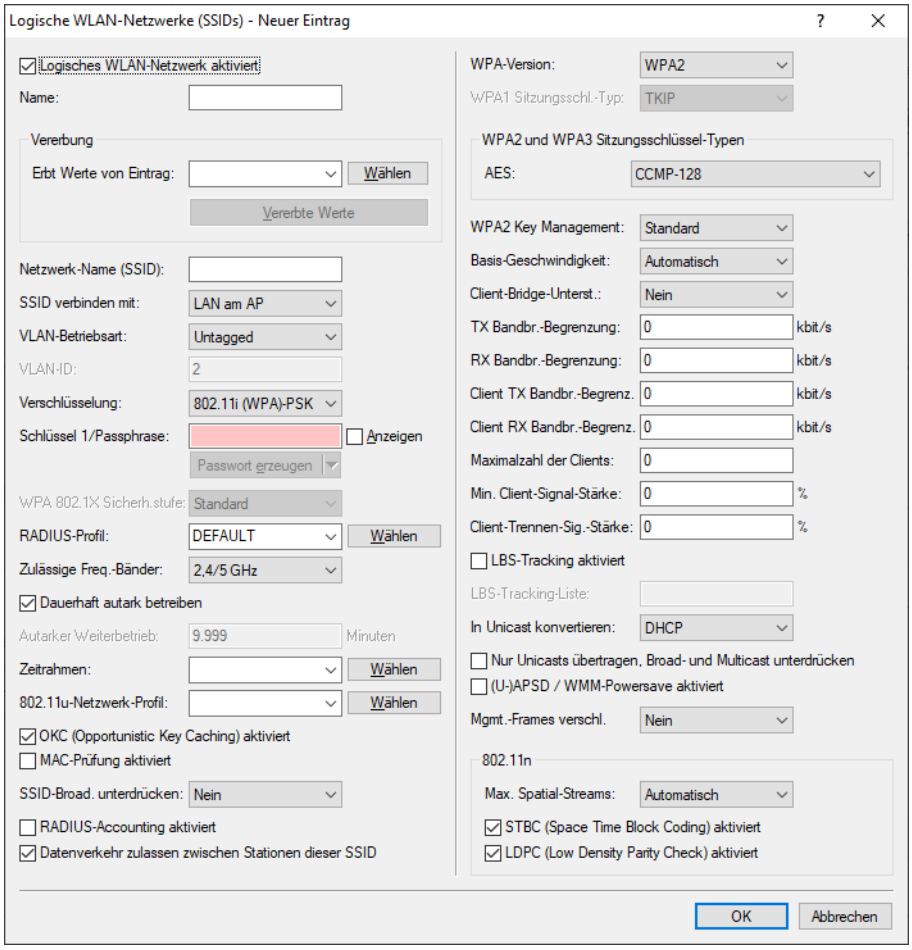
0

10 WLAN-Management

10.1 Client-Bandbreitenbegrenzung

Ab LCOS 10.40 können Sie die Bandbreite für Clients begrenzen.

Dazu wechseln Sie in LANconfig in die Ansicht **WLAN-Controller** > **Profile** > **Logische WLAN-Netzwerke**.



Client TX Bandbr.-Begrenzung

Hier begrenzen Sie die Bandbreite (Limit in kBit/s) in Senderichtung, die jedem WLAN-Client auf dieser SSID zur Verfügung steht. Der Wert `0` deaktiviert die Begrenzung.

Client RX Bandbr.-Begrenzung

Hier begrenzen Sie die Bandbreite (Limit in kBit/s) in Empfangsrichtung, die jedem WLAN-Client auf dieser SSID zur Verfügung steht. Der Wert `0` deaktiviert die Begrenzung.

10.1.1 Ergänzungen im Setup-Menü

Pro-Client-Tx-Limit

Hier begrenzen Sie die Bandbreite (Limit in kBit/s) in Senderichtung, die jedem WLAN-Client auf dieser SSID zur Verfügung steht. Der Wert 0 deaktiviert die Begrenzung.

SNMP-ID:

2.37.1.1.55

Pfad Konsole:

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

Mögliche Werte:

max. 10 Zeichen aus `0123456789`

Default-Wert:

0

Besondere Werte:

0

Deaktiviert die Begrenzung.

Pro-Client-Rx-Limit

Hier begrenzen Sie die Bandbreite (Limit in kBit/s) in Empfangsrichtung, die jedem WLAN-Client auf dieser SSID zur Verfügung steht. Der Wert 0 deaktiviert die Begrenzung.

SNMP-ID:

2.37.1.1.56

Pfad Konsole:

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

Mögliche Werte:

max. 10 Zeichen aus `0123456789`

Default-Wert:

0

Besondere Werte:

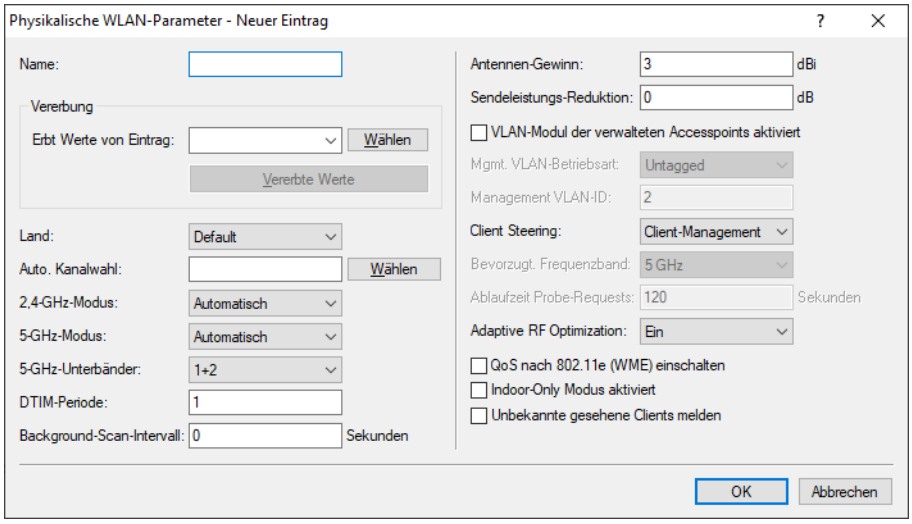
0

Deaktiviert die Begrenzung.

10.2 Default für „Unbekannte gesehene Clients melden“ geändert

Ab LCOS 10.40 wurde die Voreinstellung des Parameters **Unbekannte gesehene Clients melden** auf „Aus“ geändert.

Sie finden diesen Parameter in LANconfig in der Ansicht **WLAN-Controller** > **Profile** > **Physikalische WLAN-Parameter**.



Unbekannte gesehene Clients melden

Der Access-Point meldet standardmäßig nur bekannte (also assoziierte) Clients an den WLC. Sollen darüber hinaus auch alle übrigen gesehenen (also unbekannte und nicht assoziierte) Clients gemeldet werden, so können Sie diesen Schalter aktivieren. Dies erhöht natürlich den Datenverkehr im Netz. Sie sollten diesen Schalter daher nur vorübergehend oder zu Testzwecken aktivieren.

Wenn mit einer Vielzahl von unbekannten Clients zu rechnen ist (z. B. bei einem Public Spot oder in Bereichen mit regem Publikumsverkehr), sollten Sie diesen Schalter nicht aktivieren, da Sie ansonsten von den eingehenden Meldungen überflutet werden.

10.2.1 Ergänzungen im Setup-Menü

Melde-gesehene-Clients

Der Access-Point meldet standardmäßig nur bekannte (also assoziierte) Clients an den WLC. Sollen darüber hinaus auch alle übrigen gesehenen (also unbekannte und nicht assoziierte) Clients gemeldet werden, so können Sie diesen Schalter aktivieren. Dies erhöht natürlich den Datenverkehr im Netz. Sie sollten diesen Schalter daher nur vorübergehend oder zu Testzwecken aktivieren.

Wenn mit einer Vielzahl von unbekannten Clients zu rechnen ist (z. B. bei einem Public Spot oder in Bereichen mit regem Publikumsverkehr), sollten Sie diesen Schalter nicht aktivieren, da Sie ansonsten von den eingehenden Meldungen überflutet werden.

SNMP-ID:

2.37.1.2.20

Pfad Konsole:

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

Mögliche Werte:

nein
ja

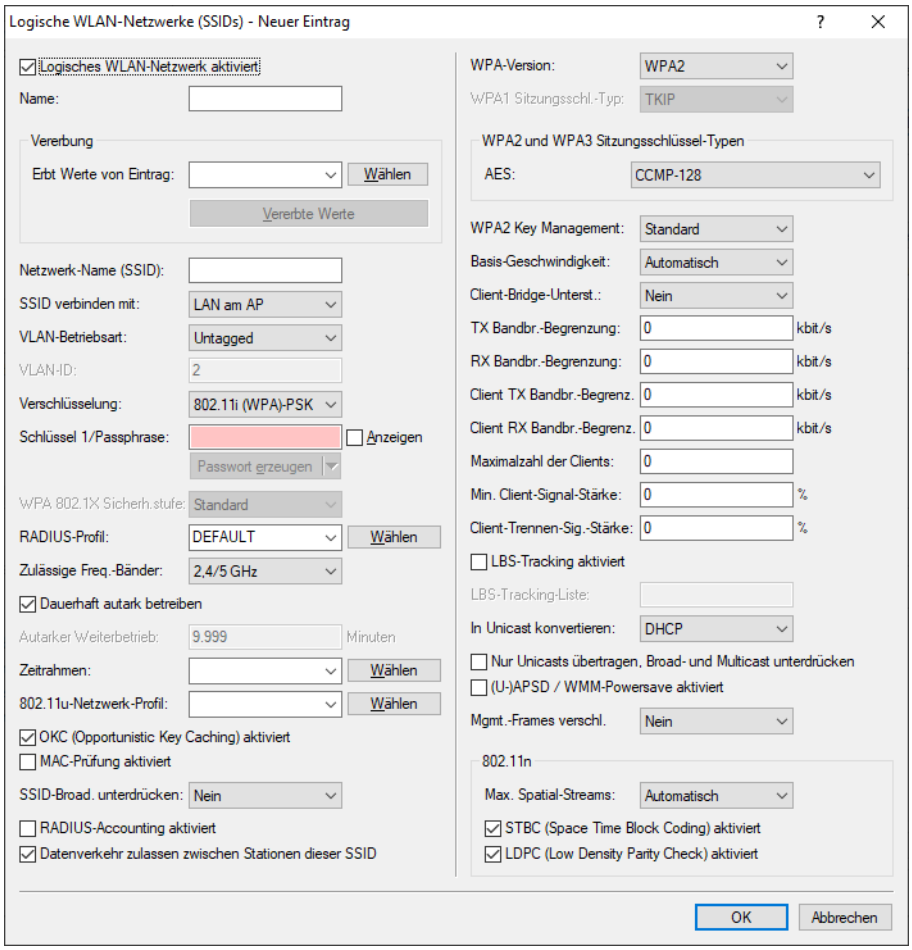
Default-Wert:

nein

10.3 Zeitsteuerung für SSIDs

Analog zu der in *Zeitsteuerung für SSIDs* auf Seite 160 beschriebenen Funktionalität gibt es diese Option auch für WLAN-Controller.

Hier geben Sie den Zeitrahmen unter **WLAN-Controller** > **Profile** > **Logische WLAN-Netzwerke** an.



Zeitrahmen

Wählen Sie hier einen der in **WLAN-Controller** > **Allgemein** > **Zeitrahmen** definierten Zeitrahmen aus. Über diesen kann die Ausstrahlung dieser SSID auf die dort definierten Zeiten eingeschränkt werden. Somit lässt sich z. B. in einer Schule ein WLAN nur während der Unterrichtszeiten aktivieren. Die Konfiguration der Zeitrahmen für den WLAN-Controller erfolgt analog zu den Einstellungen in *Zeitrahmen*.

10.3.1 Ergänzungen im Setup-Menü

Zeitrahmen

Wählen Sie hier einen der in *2.37.1.26 Zeitrahmen* auf Seite 169 definierten Zeitrahmen aus. Über diesen kann die Ausstrahlung dieser SSID auf die dort definierten Zeiten eingeschränkt werden. Somit lässt sich z. B. in einer Schule ein WLAN nur während der Unterrichtszeiten aktivieren.

SNMP-ID:

2.37.1.1.57

Pfad Konsole:

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

Mögliche Werte:

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

Default-Wert:

leer

Zeitrahmen

Zeitrahmen werden verwendet, um um eine WLAN-SSID nicht dauerhaft auszustrahlen. Zu einem Profil kann es auch mehrere Zeilen mit unterschiedlichen Zeitrahmen geben. Dabei sollten sich die Zeitrahmen unterschiedlicher Zeilen ergänzen, d. h. wenn Sie eine ARBEITSZEIT festlegen, wollen Sie wahrscheinlich auch einen Zeitrahmen FREIZEIT festlegen, der die Zeit außerhalb der Arbeitszeit umfasst.

SNMP-ID:

2.37.1.26

Pfad Konsole:

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

Name

Hier muss der Name des Zeitrahmens angegeben werden, über den er referenziert wird.

SNMP-ID:

2.37.1.26.1

Pfad Konsole:

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

Mögliche Werte:

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

Default-Wert:

leer

Start

Hier kann die Startzeit (Tageszeit) im Format HH:MM angegeben werden, ab der das gewählte Profil gelten soll.

SNMP-ID:

2.37.1.26.2

Pfad Konsole:

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

Mögliche Werte:

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

Default-Wert:

00:00

Stopp

Hier kann die Endzeit (Tageszeit) im Format HH:MM angegeben werden, bis zu der das gewählte Profil gelten soll.

Eine Stoppzeit von HH:MM geht normalerweise bis HH:MM:00. Eine Ausnahme ist die Stoppzeit 00:00, die als 23:59:59 interpretiert wird.

SNMP-ID:

2.37.1.26.3

Pfad Konsole:

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

Mögliche Werte:

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

Default-Wert:

00:00

Wochentage

Hier können Sie die Wochentage auswählen, an denen der Zeitrahmen gültig sein soll.

SNMP-ID:

2.37.1.26.4

Pfad Konsole:

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

Mögliche Werte:

Montag, Dienstag, Mittwoch, Donnerstag, Freitag, Samstag, Sonntag, Feiertag

Default-Wert:

Montag, Dienstag, Mittwoch, Donnerstag, Freitag, Samstag, Sonntag, Feiertag

Feiertage

In dieser Tabelle finden Sie die definierten Feiertage.

SNMP-ID:

2.37.1.27

Pfad Konsole:

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

Index

Index des Eintrags, der dessen Position in der Tabelle beschreibt.

SNMP-ID:

2.37.1.27.1

Pfad Konsole:

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

Mögliche Werte:

0 … 9999

Default-Wert:

leer

Datum

Wenn Sie in der Zeitsteuerungs-Tabelle Einträge angelegt haben, die an Feiertagen gelten sollen, dann tragen Sie diese Tage hier ein.

SNMP-ID:

2.37.1.27.2

Pfad Konsole:

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

Mögliche Werte:

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

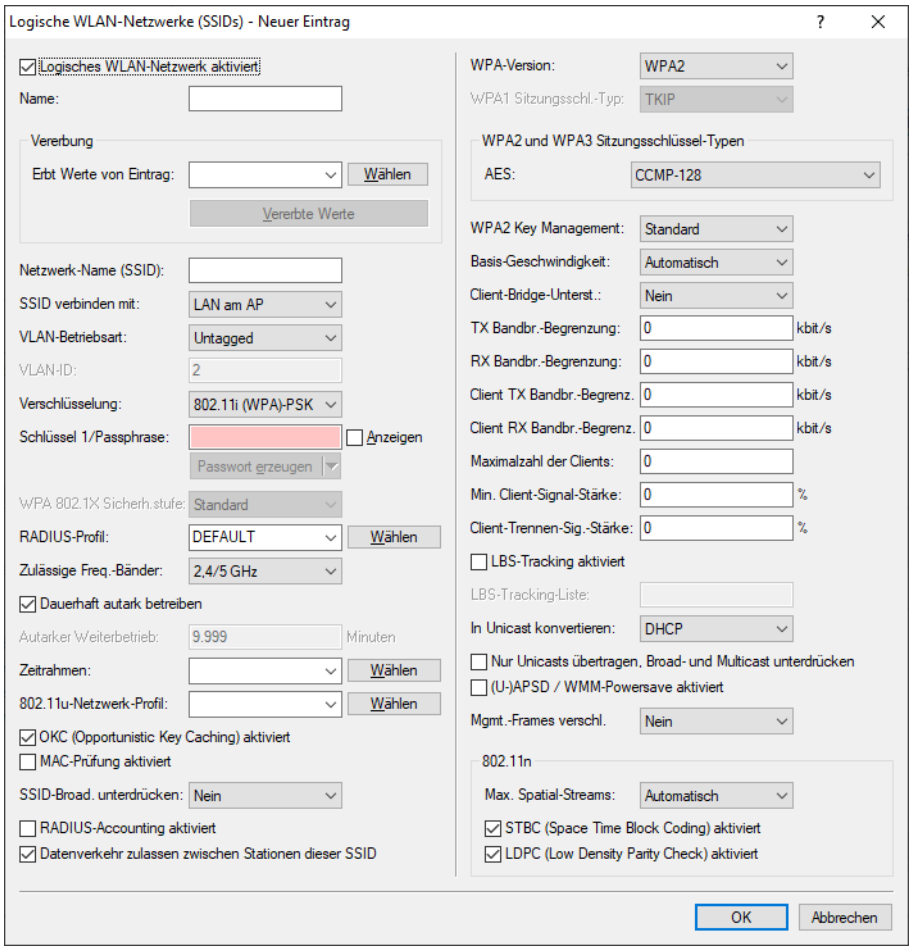
Default-Wert:

leer

10.4 Signalstärke, ab der ein Client getrennt wird

Analog zu der in *Signalstärke, ab der ein Client getrennt wird* auf Seite 163 beschriebenen Funktionalität gibt es diese Option auch für WLAN-Controller.

Hier geben Sie den Schwellenwert **Client-Trennen-Signal-Stärke** unter **WLAN-Controller** > **Profile** > **Logische WLAN-Netzwerke** an.



Client-Trennen-Signal-Stärke

Wenn dieser Schwellenwert unterschritten wird, dann wird der Client disassoziiert. Dadurch lässt sich vermeiden, dass der Client an einer aufgrund der geringen Signalstärke de facto bereits unbrauchbaren WLAN-Verbindung hängen bleibt anstatt auf eine am Client oft ebenfalls verfügbare Mobiltelefon-Verbindung umzuschalten – ein Verhalten, welches sich bei Mobiltelefonen immer wieder beobachten lässt und für den Benutzer ärgerlich ist.

Dieser Schwellenwert funktioniert nur, wenn auch der Wert **Minimale Client-Signal-Stärke** gesetzt ist und außerdem **Client-Trennen-Signal-Stärke** kleiner als dieser Wert ist.

10.4.1 Ergänzungen im Setup-Menü

Min-Stations-Disassoc-Staerke

Wenn dieser Schwellenwert unterschritten wird, dann wird der Client disassoziiert. Dadurch lässt sich vermeiden, dass der Client an einer aufgrund der geringen Signalstärke de facto bereits unbrauchbaren WLAN-Verbindung hängen bleibt anstatt auf eine am Client oft ebenfalls verfügbare Mobiltelefon-Verbindung umzuschalten – ein Verhalten, welches sich bei Mobiltelefonen immer wieder beobachten lässt und für den Benutzer ärgerlich ist.

Dieser Schwellenwert funktioniert nur, wenn auch der Wert *2.37.1.1.38 Minimal-Stations-Staerke* gesetzt ist und außerdem Min-Stations-Disassoc-Staerke kleiner als dieser Wert ist.

SNMP-ID:

2.37.1.1.58

Pfad Konsole:

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

Mögliche Werte:

0 … 100

Default-Wert:

0

11 Public Spot

11.1 Passpoint® Release 2

Ab LCOS 10.40 ist die seit LCOS 10.32 RU4 unterstützte erweiterte Hotspot 2.0-Funktionalität Ihres WLAN-Gerätes nach dem von der Wi-Fi Alliance spezifizierten Passpoint® Release 2 auch über LANconfig konfigurierbar. Der im LCOS integrierte RADIUS-Server beinhaltet ab Version 10.32 RU4 die benötigten Features.

Passpoint® Release 2 vereinfacht das Onboarding von Geräten in ein Netz mit der Verschlüsselungsmethode WPA2-Enterprise (802.1X). Mittels eigener Onboarding-SSID kann ein Benutzer sich ein Profil auf Passpoint® Release 2-fähige Endgeräte installieren und dann automatisch mit den hinterlegten Anmeldedaten ins verschlüsselte Netz wechseln. Somit lassen sich Hotspots realisieren, die verschlüsselte drahtlose Kommunikation ermöglichen. Hierbei können die Gäste über eine offene Onboarding-SSID mit zeitlich begrenzten Zugangsdaten ausgestattet werden.

Ebenso kann ein Mobilfunkanbieter sein Mobilfunknetz entlasten, indem er Wi-Fi Offloading einführt und mobile Endgeräte, die mit einer SIM-Karte ausgestattet sind, automatisch in sein WLAN-Netz einbuchen lässt. Die Endgeräte der Kunden finden das WLAN-Netz des Mobilfunkanbieters automatisch und buchen sich mit den hinterlegten Benutzerdaten der SIM-Karte automatisch in das WLAN-Netz des Betreibers ein.

Mit Passpoint® Release 2 wird die Hotspot 2.0-Funktionalität um die folgenden Features erweitert:

- Online Sign-Up (OSU) – Mit Passpoint® Release 2 bekommen Unternehmen und Netzbetreiber die Möglichkeit, Benutzerprofile über einen so genannten „Online Sign-Up"-Server (OSU-Server) zur Verfügung zu stellen. Über eine offene OSU-SSID hat der Benutzer die Möglichkeit, verschiedene OSU-Server anhand von hinterlegten Icons zu identifizieren und somit den für ihn passenden auszuwählen. Der OSU-Server kann ggf. Benutzerdaten abfragen, bevor er ein passendes Profil für das Endgerät des Benutzers bereitstellt. Neben der offenen OSU-SSID kann auch eine verschlüsselte SSID genutzt werden, welche mittels „anonymous EAP-TLS" die Benutzerdaten verschlüsselt abfragt und bereitstellt. Hierfür wird ein entsprechender RADIUS-Server mit „anonymous EAP-TLS" Unterstützung benötigt.

  Ein OSU-Server ist kein Bestandteil des LCOS. Es gibt allerdings Lösungen von LANCOM Partnern.

- OSU-Icons – Für die unterstützten OSU-Server können im LCOS über die WEBconfig im Bereich **Dateimanagement** entsprechende Icons als Datei hochgeladen werden. Als Dateiformat empfehlen wir PNG.
- Benachrichtigungsmöglichkeit – Auf Netzseite gibt es die Möglichkeit, den Benutzer zu benachrichtigen, wenn eine Abmeldung seitens RADIUS-Server kurz bevor steht. Dies kann z. B. der Fall sein, wenn die Benutzerdaten nicht mehr länger gültig sind oder die festgelegte Verbindungsdauer erreicht wurde.
- QoS Map – Ein Access Point kann über die Funktion „QoS Map Set" seine Clients anweisen, eine bestimmte QoS Map zu verwenden. Hierbei werden die Werte für das Contention Window (Medienzugriff via EDCA) der verschiedenen Access Categories für Voice, Video, Best Effort und Background-Datenpakete und deren zugehörige DSCP-Werte definiert. Gleichzeitig nutzt auch der Access Points die in der QoS Map hinterlegten Werte.

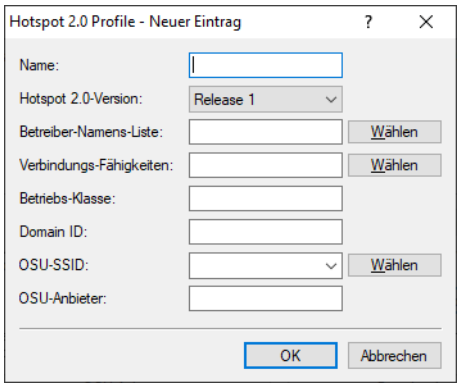
  Aktuell stehen neben den zwei durch die Wi-Fi Alliance vorgegebenen QoS Maps nur die Standard-QoS-Map des LCOS zur Verfügung.

11.1.1 Hotspot 2.0 konfigurieren

Hotspot 2.0 Profile

Über diese Tabelle verwalten Sie die Profillisten für Hotspot 2.0. **Hotspot 2.0 Profile** bieten Ihnen die Möglichkeit, bestimmte ANQP-Elemente (die der Hotspot-2.0-Spezifikation) zu gruppieren und sie in der Tabelle **Interfaces** unabhängig voneinander logischen WLAN-Schnittstellen zuzuweisen. Zu diesen Elementen gehören z. B. der betreiberfreundliche

Name, die Verbindungs-Fähigkeiten, die Betriebsklasse und die WAN-Metriken. Ein Teil der Elemente ist in weitere Profillisten ausgelagert.



Hotspot 2.0 Version

Stellen Sie das in diesem Profil unterstützte Release von Hotspot 2.0 ein.

Ein Client muss das entsprechende Release beherrschen, um sich verbinden zu können.

Domain ID

Die Domain-ID gibt an, welcher ANQP-Server verwendet wird. Alle Access Points bzw. SSIDs mit gleicher Nummer / Domain-ID (16-Bit-Wert) verwenden den gleichen ANQP-Server.

Ein Client würde somit auf eine ANQP-Anfrage auf Access Points / SSIDs mit identischer Domain-ID immer die gleiche Antwort erhalten. Um unterschiedliche Antworten zu erhalten, müsste der Client nach unterschiedlichen Domain-IDs Ausschau halten.

OSU-SSID

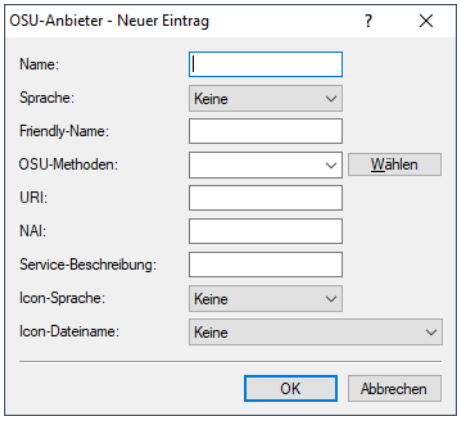
Name der SSID, die Zugang zum OSU-Server bietet.

OSU-Anbieter

Liste der OSU-Providernamen aus *OSU-Anbieter* auf Seite 175, die im Profil unterstützt werden.

OSU-Anbieter

In dieser Tabelle konfigurieren Sie die OSU-Provider für Online Sign-Up bei Passpoint® Release 2.



Name

Geben Sie diesem OSU-Provider einen Namen, über den Sie ihn später referenzieren können. Wenn der gleiche Name erneut verwendet wird, dann kann dieser Provider z. B. für mehrere Spachen verwendet werden.

Sprache

Stellen Sie die von diesem OSU-Provider unterstützte Sprache ein.

Friendly-Name

Geben Sie diesem OSU-Provider einen sprechenden Namen.

OSU-Methoden

Stellen Sie hier die von diesem OSU-Provider verwendeten OSU-Methoden ein. Möglich sind „OMA-DM“ oder „SOAP-XML-SPP“.

Mögliche Methoden innerhalb des Online Sign-Up-Servers bei Passpoint® Release 2:

- OMA – Open Mobile Alliance
- DM – Device Management
- SOAP – Simple Object Access Protocol
- XML – eXtended Markup Language
- SPP – Subscription Provisioning Protocol

URI

Geben Sie eine URI ein, unter der ein Client den OSU-Server erreicht.

NAI

Geben Sie den Network Access Identifier (NAI) für diesen OSU-Provider ein.

Service-Beschreibung

Geben Sie hier einen Beschreibungstext für diesen Dienst ein.

Icon-Sprache

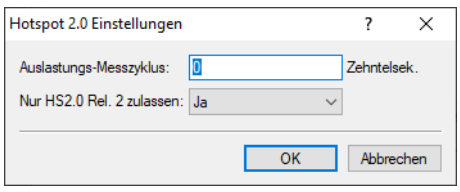
Stellen Sie hier die Sprache des ausgewählten Icons ein.

Icon-Dateiname

Wählen Sie ein Icon für diesen OSU-Provider aus. Die Icons können über die WEBconfig im Bereich ***Dateimanagement*** als Datei hochgeladen werden. Als Dateiformat empfehlen wir PNG.

Hotspot 2.0 Einstellungen

In dieser Tabelle konfigurieren Sie spezielle Einstellungen für Hotspot 2.0.



Auslastungs-Messzyklus

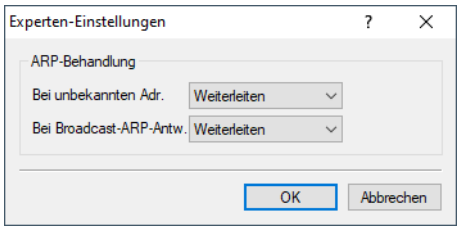
Messzyklus der WAN-Down- / Uplink-Geschwindigkeiten in Zehntelsekunden.

Nur Hotspot 2.0 Release 2 zulassen

Für HotSpot 2.0 Release 2 wird gefordert, nur Release 2-Clients zuzulassen. Dies kann durch diesen Schalter ausgeschaltet werden.

Experten-Einstellungen

In dieser Tabelle konfigurieren Sie Experten-Einstellungen für Hotspot 2.0. Die Einstellungen in diesem Menü dienen der Unterdrückung von ARP (IPv4) bzw. Neighbor Solicitation (IPv6) innerhalb der SSID zwischen den Clients. Alternativ kann dies i.d.R. auch durch die Unterdrückung von Broad- / Multicasts via **Nur Unicasts übertragen, Broad- und Multicasts unterdrücken** in den logischen WLAN-Netzwerkeinstellungen gelöst werden.



Bei unbekannten Adressen

Bei unbekannten Adressen wird das Paket entweder weitergeleitet oder verworfen.

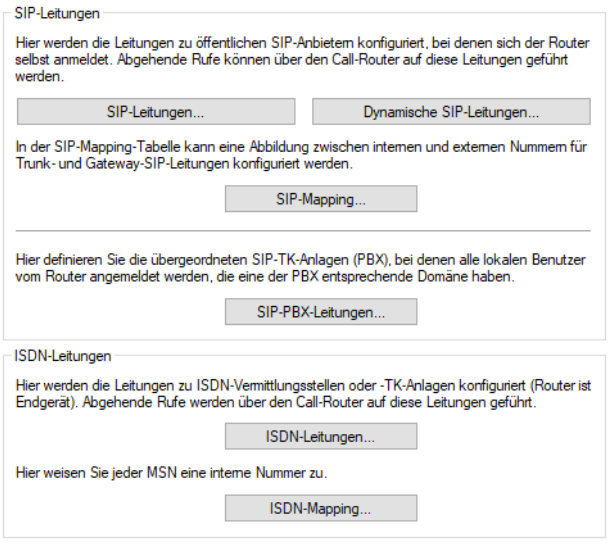
Bei Broadcast-ARP-Antworten

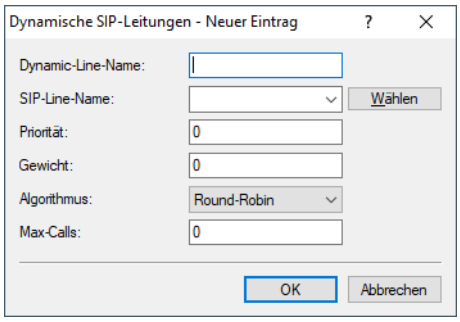
Bei Broadcasts wird das Paket entweder weitergeleitet oder verworfen.

12 Voice over IP – VoIP

12.1 Dynamische SIP-Leitungen

Ab LCOS 10.40 ist es möglich, dynamische SIP-Leitungen einzurichten. Dazu unter **Voice Call Manager** > **Leitungen** die Konfiguration mit einem Klick auf die Schaltfläche **Dynamische SIP-Leitungen** aufrufen.





Dynamic-Line-Name

Geben Sie hier den Namen der dynamischen Leitung an. Besteht die dynamische Leitung aus mehreren physikalischen Leitungen, verwenden Sie diesen dynamischen Leitungsnamen ebenfalls bei weiteren Tabelleneinträgen.Dieser dynamische Leitungsname kann später in der Callrouting Tabelle als Ziel-Leitung verwendet werden.

SIP-Line-Name

Wählen Sie hier eine der bereits konfigurierten physikalischen SIP-Verbindungen aus.

Priorität

Geben Sie hier die Priorität der physikalischen Leitung an, mit der die Leitung in der Verteilung ausgehender Rufe berücksichtigt werden soll.

Gewicht

Geben Sie hier die Gewichtung der physikalischen Leitung an, mit der die Leitung in der Verteilung ausgehender Rufe berücksichtigt werden soll.

Algorithmus

Der Algorithmus muss für alle Einträge, die zu einer dynamischen Leitung gehören, identisch konfiguriert werden. Dabei können folgende Algorithmen verwendet werden:

Gewicht

Mit diesem Algorithmus kann eine prozentuale Verteilung der Rufe auf verschiedene physikalische Leitungen bestimmt werden.

Round-Robin

Bei diesem Algorithmus werden ausgehende Rufe der Reihe nach auf die physikalischen Leitungen verteilt.

Priorität

Die physikalische Leitung mit der höchsten Priorität wird zunächst vollständig ausgelastet, bevor die physikalische Leitung mit der nächst niedrigeren Priorität verwendet wird.

Max-Calls

Geben Sie hier an, wie viele gleichzeitige Sprachkanäle auf der physikalischen SIP-Leitung möglich sind. Ist keine Beschränkung der Sprachkanäle notwendig, tragen Sie hier eine 0 ein.

12.1.1 Ergänzungen im Setup-Menü

Dynamic-Line

Konfigurieren Sie hier dynamische SIP-Leitungen.

SNMP-ID:

2.33.4.1.3

Pfad Konsole:

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

Dynamic-Line-Name

Geben Sie hier den Namen der dynamischen Leitung an. Besteht die dynamische Leitung aus mehreren physikalischen Leitungen, verwenden Sie diesen dynamischen Leitungsnamen ebenfalls bei weiteren Tabelleneinträgen.Dieser dynamische Leitungsname kann später in der Callrouting Tabelle als Ziel-Leitung verwendet werden.

SNMP-ID:

2.33.4.1.3.1

Pfad Konsole:

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

Mögliche Werte:

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

Sip-Line-Name

Geben Sie hier eine der bereits konfigurierten physikalischen SIP-Verbindungen an.

SNMP-ID:

2.33.4.1.3.2

Pfad Konsole:

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

Mögliche Werte:

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

Priority

Geben Sie hier die Priorität der physikalischen Leitung an, mit der die Leitung in der Verteilung ausgehender Rufe berücksichtigt werden soll.

SNMP-ID:

2.33.4.1.3.3

Pfad Konsole:

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

Mögliche Werte:

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

Weight

Geben Sie hier die Gewichtung der physikalischen Leitung an, mit der die Leitung in der Verteilung ausgehender Rufe berücksichtigt werden soll.

SNMP-ID:

2.33.4.1.3.4

Pfad Konsole:

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

Mögliche Werte:

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

Algorithm

Der Algorithmus muss für alle Einträge, die zu einer dynamischen Leitung gehören, identisch konfiguriert werden.

SNMP-ID:

2.33.4.1.3.5

Pfad Konsole:

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

Mögliche Werte:

Weight

Mit diesem Algorithmus kann eine prozentuale Verteilung der Rufe auf verschiedene physikalische Leitungen bestimmt werden.

Round-Robin

Bei diesem Algorithmus werden ausgehende Rufe der Reihe nach auf die physikalischen Leitungen verteilt.

Priority

Die physikalische Leitung mit der höchsten Priorität wird zunächst vollständig ausgelastet, bevor die physikalische Leitung mit der nächst niedrigeren Priorität verwendet wird.

Max-Calls

Geben Sie hier an, wie viele gleichzeitige Sprachkanäle auf der physikalischen SIP-Leitung möglich sind. Ist keine Beschränkung der Sprachkanäle notwendig, tragen Sie hier eine 0 ein.

SNMP-ID:

2.33.4.1.3.6

Pfad Konsole:

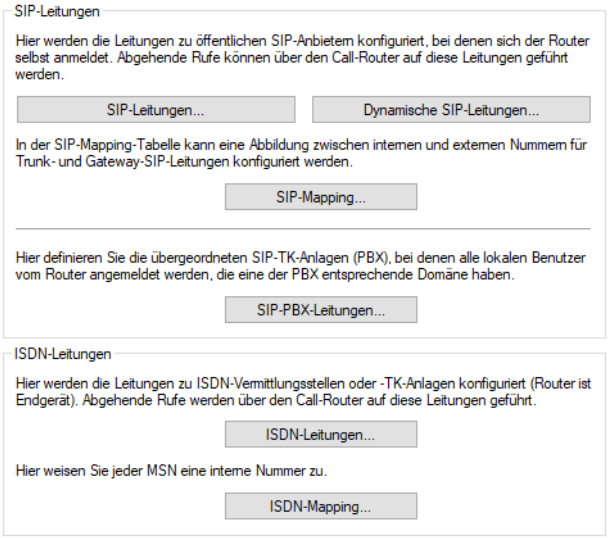
Setup > **Voice-Call-Manager** > **Line** > **SIP-Provider** > **Dynamic-Line**

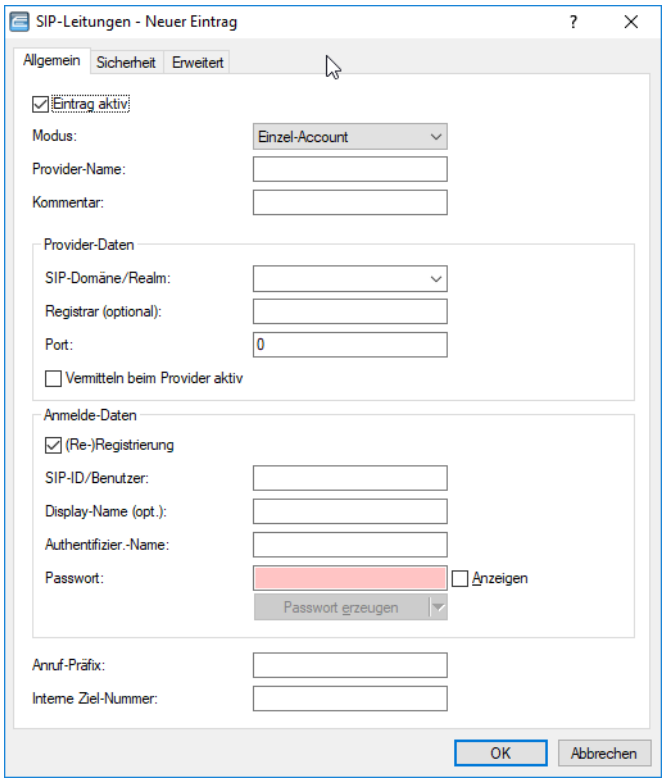
Mögliche Werte:

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

12.2 Flex-Modus

Ab LCOS 10.40 wird der neue Flex-Modus für SIP-Leitungen unterstützt. Dazu unter **Voice Call Manager** > **Leitungen** die Konfiguration mit einem Klick auf die Schaltfläche **SIP-Leitungen** aufrufen.





Modus

Flex

› Sie verhält sich nach außen wie ein handelsüblicher SIP-Account mit einer einzigen öffentlichen Nummer.

- Die Nummer wird beim Serviceprovider registriert und die Registrierung regelmäßig aufgefrischt.
- Bei ausgehenden Rufen wird die Nummer des Rufenden (Absender) nicht modifiziert.
- Bei eingehenden Rufen wird die gerufene Nummer (Ziel) nicht modifiziert.
- Die maximale Anzahl der Verbindungen zu einem bestimmten Zeitpunkt ist nur durch die zur Verfügung stehende Bandbreite begrenzt.

12.2.1 Ergänzungen im Setup-Menü

Mode

Mit dieser Auswahl bestimmen Sie die Betriebsart der SIP-Leitung.

Der "Serviceprovider" kann ein Server im Internet, eine IP-Telefonanlage oder ein Voice-Gateway sein. Bitte beachten Sie auch die Hinweise zum "SIP-Mapping".

SNMP-ID:

2.33.4.1.1.17

Pfad Konsole:

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

Mögliche Werte:

Provider

Verhält sich nach außen wie ein üblicher SIP-Account mit einer einzigen öffentlichen Nummer. Die Nummer wird beim Serviceprovider registriert und die Registrierung regelmäßig aufgefrischt (wenn eine (Re-)Registrierung für diese SIP-Provider-Line aktiviert ist). Bei ausgehenden Rufen wird die Nummer des Rufenden (Absender) durch die registrierte Nummer ersetzt (maskiert). Eingehende Rufe werden der konfigurierten internen Ziel-Nummer zugestellt. Es kann nur maximal eine Verbindung zu einem Zeitpunkt bestehen.

Trunk

Verhält sich nach außen wie ein erweiterter SIP-Account mit einer Stamm- und mehreren Durchwahlnummern. Die SIP-ID wird als Stammnummer beim Serviceprovider registriert und die Registrierung regelmäßig aufgefrischt (wenn eine (Re-)Registrierung für diese SIP-Provider-Line aktiviert ist). Bei ausgehenden Rufen fungiert die Stammnummer als Präfix, das jeder rufenden Nummer (Absender; SIP: "From:") vorangestellt wird. Bei eingehenden Rufen wird das Präfix aus der Ziel-Nummer entfernt (SIP: "To:"). Die verbleibende Nummer wird als interne Durchwahl verwendet. Im Fehlerfall (Präfix nicht auffindbar, Ziel gleich Präfix) wird der Ruf an die konfigurierte interne Ziel-Nummer geleitet. Die maximale Anzahl der Verbindungen zu einem bestimmten Zeitpunkt ist nur durch die zur Verfügung stehende Bandbreite begrenzt.

Gateway

Sie verhält sich nach außen wie ein üblicher SIP-Account mit einer einzigen öffentlichen Nummer, der SIP-ID. Die Nummer (SIP-ID) wird beim Serviceprovider registriert und die Registrierung regelmäßig aufgefrischt (wenn eine (Re-)Registrierung für diese SIP-Provider-Line aktiviert ist). Bei ausgehenden Rufen wird die Nummer des Rufenden (Absender) durch die registrierte Nummer (SIP-ID in SIP: "From:") ersetzt (maskiert) und in einem separaten Feld (SIP: "Contact:") übertragen. Bei eingehenden Rufen wird die gerufene Nummer (Ziel) nicht modifiziert. Die maximale Anzahl der Verbindungen zu einem bestimmten Zeitpunkt ist nur durch die zur Verfügung stehende Bandbreite begrenzt.

Link

Verhält sich nach außen wie ein üblicher SIP-Account mit einer einzigen öffentlichen Nummer (SIP-ID). Die Nummer wird beim Serviceprovider registriert und die Registrierung regelmäßig aufgefrischt (wenn eine (Re-)Registrierung für diese SIP-Provider-Line aktiviert ist). Bei ausgehenden Rufen wird die Nummer des Rufenden (Absender; SIP: "From:") nicht modifiziert. Bei eingehenden Rufen wird die gerufene Nummer (Ziel; SIP: "To:") nicht modifiziert. Die maximale Anzahl der Verbindungen zu einem bestimmten Zeitpunkt ist nur durch die zur Verfügung stehende Bandbreite begrenzt.

Flex

- Sie verhält sich nach außen wie ein handelsüblicher SIP-Account mit einer einzigen öffentlichen Nummer.
- Die Nummer wird beim Serviceprovider registriert und die Registrierung regelmäßig aufgefrischt.
- Bei ausgehenden Rufen wird die Nummer des Rufenden (Absender) nicht modifiziert.
- Bei eingehenden Rufen wird die gerufene Nummer (Ziel) nicht modifiziert.
- Die maximale Anzahl der Verbindungen zu einem bestimmten Zeitpunkt ist nur durch die zur Verfügung stehende Bandbreite begrenzt.

Default-Wert:

Provider

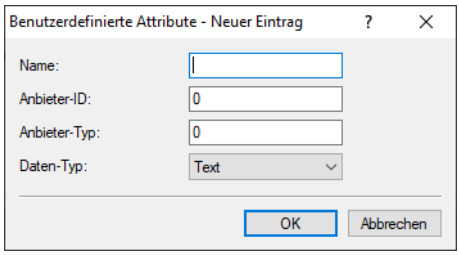
13 RADIUS

13.1 Benutzerdefinierte Attribute

Ab LCOS 10.40 unterstützt Ihr Gerät die Verwendung benutzerdefinierter RADIUS-Attribute.

RADIUS-Attribute werden in einem sog. Dictionary verwaltet. Von Haus aus unterstützt LCOS bereits viele verschiedene Attribute; allerdings gibt es eine unüberschaubare Menge von herstellerspezifischen Attributen, die hier durch durch den Administrator in die LCOS-Konfiguration eingetragen werden können. Diese Attribute können dadurch an allen Stellen im LCOS verwendet werden, an denen Attribute zu einer RADIUS-Anfrage bzw. -Antwort hinzugefügt werden können, wie z .B. in der RADIUS-Benutzerverwaltung.

Die Konfiguration der benutzerdefinierten Attribute erfolgt über **RADIUS** > **Server** > **Erweiterte Einstellungen** > **Benutzerdefinierte Attribute**



Name

Der Name, unter dem das Attribut an weiteren Stellen im LCOS referenziert wird.

Anbieter-ID

Die spezifische Anbieter-ID (Vendor-ID) des Attributs.

Anbieter-Typ

Die spezifische Typ-ID des Attributs.

Daten-Typ

Der Daten-Typ des Attributs.

13.1.1 Ergänzungen im Setup-Menü

Benutzerdefinierte-Attribute

In diesem Verzeichnis konfigurieren Sie die benutzerdefinierte Attribute.

RADIUS-Attribute werden in einem sog. Dictionary verwaltet. Von Haus aus unterstützt LCOS bereits viele verschiedene Attribute; allerdings gibt es eine unüberschaubare Menge von herstellerspezifischen Attributen, die hier durch durch den Administrator in die LCOS-Konfiguration eingetragen werden können. Diese Attribute können dadurch an allen Stellen im LCOS verwendet werden, an denen Attribute zu einer RADIUS-Anfrage bzw. -Antwort hinzugefügt werden können, wie z .B. in der RADIUS-Benutzerverwaltung.

SNMP-ID:

2.25.22

Pfad Konsole:

Setup > **RADIUS**

Attribute

Hier erstellen Sie die benutzerdefinierten Attribute zur Verwendung mit RADIUS-Servern.

SNMP-ID:

2.25.22.1

Pfad Konsole:

Setup > **RADIUS** > **Benutzerdefinierte-Attribute**

Name

Der Name, unter dem das Attribut an weiteren Stellen im LCOS referenziert wird.

SNMP-ID:

2.25.22.1.1

Pfad Konsole:

Setup > **RADIUS** > **Benutzerdefinierte-Attribute** > **Attribute**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9]-_`

Vendor-ID

Die spezifische Anbieter-ID (Vendor-ID) des Attributs.

SNMP-ID:

2.25.22.1.2

Pfad Konsole:

Setup > **RADIUS** > **Benutzerdefinierte-Attribute** > **Attribute**

Mögliche Werte:

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

Vendor-Typ

Die spezifische Typ-ID des Attributs.

SNMP-ID:

2.25.22.1.3

Pfad Konsole:

Setup > **RADIUS** > **Benutzerdefinierte-Attribute** > **Attribute**

Mögliche Werte:

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

Datentyp

Die spezifische Typ-ID des Attributs.

SNMP-ID:

2.25.22.1.4

Pfad Konsole:

Setup > **RADIUS** > **Benutzerdefinierte-Attribute** > **Attribute**

Mögliche Werte:

Text
Integer
IPv4-Adresse
IPv6-Adresse
Datum

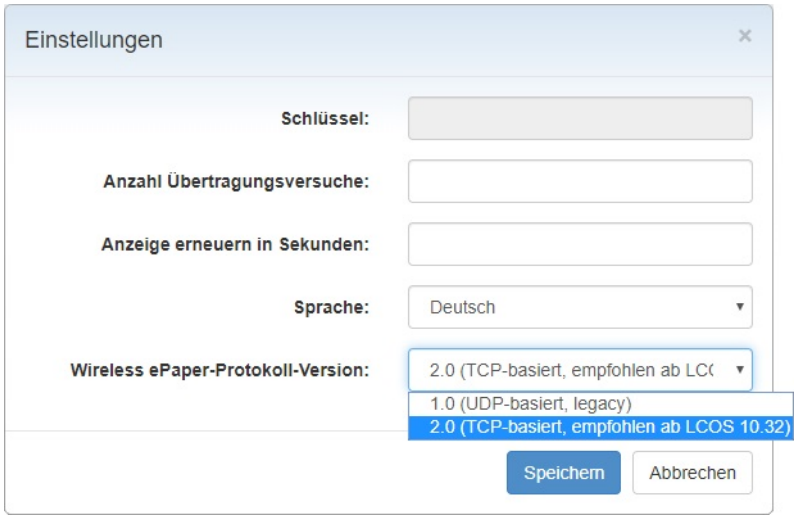
14 IoT – Das Internet der Dinge (Internet of Things – IoT)

14.1 Wireless ePaper

Zentrale Verwaltung Ihrer Wireless ePaper-Infrastruktur

Ab LCOS 10.40 unterstützen die LANCOM Access Points mit Wireless ePaper-Unterstützung eine Erweiterung des TCP-Protokolls, welches den Verbindungsaufbau (Wireless ePaper Access Point bzw. Router mit USB-Schnittstelle und Wireless ePaper USB-Stick) zum Wireless ePaper Server zulässt und die Verbindung mittels TLS verschlüsselt. Um diese Erweiterung einzusetzen sind sowohl der Wireless ePaper Server als auch auf das Wireless ePaper Gerät (Access Point bzw. Router mit Wireless ePaper USB) zu konfigurieren.

In der rechten, oberen Ecke der Wireless ePaper-Verwaltung können Sie auf das Zahnrad-Symbol und dann **Einstellungen** klicken, um allgemeine Einstellungsmöglichkeiten zum Wireless ePaper Server zu erreichen. Dort können Sie das neue Protokoll aktivieren.



Im LANmonitor in der Anzeige des entsprechenden Gerätes unter **IoT** > **Wireless ePaper** > **Protokollversion** wird das verwendete Protokoll angezeigt:

- Keine – Es besteht keine Verbindung zu einem Controller / Server
- ThinAP1.0/UDP – Protokollversion 1.0 (UDP-basiert, legacy)
- ThinAP2.0/TCP – Protokollversion 2.0 (TCP-basiert, ab LCOS 10.32)
- ThinAP2.0/TLS – Erweiterung der Protokollversion 2.0 (TCP-basiert und verschlüsselt, ab LCOS 10.40)

Aktivierung eines TCP-basierten Protokolls auf dem Wireless ePaper Server

Der Wireless ePaper Server unterstützt „Protokollversion 2.0" ab Version 1.91 und ab Version 1.101 die darauf aufbauende TLS-Verschlüsselung. Falls Sie einen unterstützten Wireless ePaper Server bereits einsetzen und trotzdem hier nur „Protokollversion 1.0" oder ab Version 1.101 nur „Protokollversion 2.0" sehen, dann wurde ggf. das Protokoll in den Einstellungen des Wireless ePaper Servers nicht aktiviert. In diesem Fall müssen Sie die Protokollversion erst aktivieren.

Gehen Sie wie folgt vor, um „Protokollversion 2.0 (ThinAP2.0/TCP)" zu aktivieren:

1. Überprüfen Sie die folgenden Voraussetzungen:

- LANCOM Wireless ePaper Server in der Version 1.91 oder höher ist installiert
- cURL ist installiert

2. Öffnen Sie in Ihrem Betriebsystem eine Kommandozeile und geben Sie den folgenden Befehl ein:

   ```
   curl -X PUT http://<server-ip>:8001/service/configuration/lancomUseTcpThinMode?value=true
   ```

3. Starten Sie den Wireless ePaper Server neu.
4. Geben Sie anschließend den folgenden Befehl ein, um zu überprüfen, ob die Aktivierung erfolgreich war:

   ```
   curl -X GET http://<server-ip>:8001/service/configuration/lancomUseTcpThinMode
   ```

Eine erfolgreiche Aktivierung liefert die Ausgabe:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Configuration key="lancomUseTcpThinMode" type="BOOLEAN" defaultValue="false" value="true"/>
```

Gehen Sie wie folgt vor, um „Protokollversion 2.0 (ThinAP2.0/TLS)“ zu aktivieren:

1. Überprüfen Sie die folgenden Voraussetzungen:

   - LANCOM Wireless ePaper Server in der Version 1.101 oder höher ist installiert
   - cURL ist installiert
   - „Protokollversion 2.0 (ThinAP2.0/TCP)“ ist aktiviert

2. Öffnen Sie in Ihrem Betriebsystem eine Kommandozeile und geben Sie die folgenden Befehle ein:

   ```
   curl -X PUT http://<server-ip>:8001/service/configuration/accessPointUseThinMode?value=true
   curl -X PUT http://<server-ip>:8001/service/configuration/lancomUseTcpThinOutboundMode?value=true
   curl -X PUT http://<server-ip>:8001/service/configuration/accessPointThinUseOutboundMode?value=true
   ```

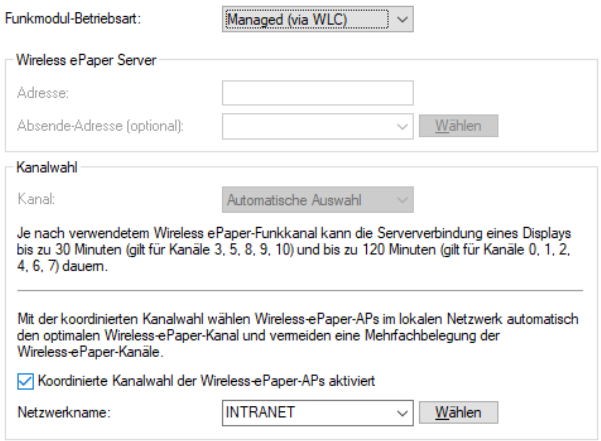
3. Starten Sie den Wireless ePaper Server neu.
4. Geben Sie anschließend analog zur Überprüfung beim TCP-Protokoll alle drei Parameter mit „GET“ als Befehl ein, um zu überprüfen, ob die Aktivierung erfolgreich war. Als Ausgabe muss jeweils „`value="true"`“ angezeigt werden

Um die Funktion zu deaktivieren sind auf der Kommandozeile die Befehle mit dem Parameter „`value=false`“ anstelle des Parameters „`value=true`“ aufzurufen. Der Befehl sieht dann z. B. so aus:

```
curl -X PUT http://<server-ip>:8001/service/configuration/lancomUseTcpThinMode?value=false
```

14.1.1 Einstellungen für Wireless ePaper

Aktivieren Sie das Wireless ePaper Funkmodul in LANconfig unter **IoT** > **Wireless ePaper**.



Wireless ePaper Server

Ab LCOS 10.40 unterstützen die LANCOM Access Points mit Wireless ePaper-Unterstützung eine Erweiterung des TCP-Protokolls, welches den Verbindungsaufbau (Wireless ePaper Access Point bzw. Router mit USB-Schnittstelle und Wireless ePaper USB-Stick) zum Wireless ePaper Server zulässt und die Verbindung mittels TLS verschlüsselt. Dazu muss auf dem Wireless ePaper Server das Protokoll ThinAP2.0/TLS eingerichtet sein und die IP-Adresse des Wireless ePaper Servers hier angegeben werden.

Adresse

IP-Adresse des Wireless ePaper Servers.

Absende-Adresse

Geben Sie hier die Loopback-Adresse an.

14.2 Ergänzungen im Setup-Menü

14.2.1 Outbound-Server

IP-Adresse des Wireless ePaper Servers.

SNMP-ID:

2.111.88.5

Pfad Konsole:

Setup > **IoT** > **Wireless-ePaper**

Mögliche Werte:

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

14.2.2 SSL

Dieses Menü enthält die Parameter für die TLS-Authentifizierung.

SNMP-ID:

2.111.88.6

Pfad Konsole:

Setup > **IoT** > **Wireless-ePaper**

Versionen

Dieser Eintrag definiert die erlaubten Protokoll-Versionen.

SNMP-ID:

2.111.88.6.1

Pfad Konsole:

Setup > **IoT** > **Wireless-ePaper** > **SSL**

Mögliche Werte:

SSLv3
TLSv1
TLSv1.1
TLSv1.2

Default-Wert:

TLSv1.2

Schluesselaustausch-Algorithmen

Dieser Eintrag legt fest, welche Verfahren zum Schlüsselaustausch zur Verfügung stehen.

SNMP-ID:

2.111.88.6.2

Pfad Konsole:

Setup > **IoT** > **Wireless-ePaper** > **SSL**

Mögliche Werte:

RSA
DHE
ECDHE

Default-Wert:

RSA

DHE

ECDHE

Krypto-Algorithmen

Diese Bitmaske legt fest, welche Krypto-Algorithmen erlaubt sind.

SNMP-ID:

2.111.88.6.3

Pfad Konsole:

Setup > **IoT** > **Wireless-ePaper** > **SSL**

Mögliche Werte:

RC4-40
RC4-56
RC4-128
DES40
DES
3DES
AES-128
AES-256
AESGCM-128
AESGCM-256
Chacha20-Poly1305

ChaCha20 Datenstromverschlüsselung zusammen mit dem Poly1305 Authentifikator, siehe *RFC 7634*.

Default-Wert:

3DES

AES-128

AES-256

AESGCM-128

AESGCM-256

Chacha20-Poly1305

Hash-Algorithmen

Dieser Eintrag legt fest, welche Hash-Algorithmen erlaubt sind und impliziert, welche HMAC-Algorithmen zum Schutz der Nachrichten-Integrität genutzt werden.

SNMP-ID:

2.111.88.6.4

Pfad Konsole:

Setup > **IoT** > **Wireless-ePaper** > **SSL**

Mögliche Werte:

MD5
SHA1
SHA2-256
SHA2-384

Default-Wert:

MD5

SHA1

SHA2-256

SHA2-384

PFS-bevorzugen

Bei der Auswahl der Chiffrier-Methode (Cipher-Suite) richtet sich das Gerät normalerweise nach der Einstellung des anfragenden Clients. Bestimmte Anwendungen auf dem Client verlangen standardmäßig eine Verbindung ohne Perfect Forward Secrecy (PFS), obwohl Gerät und Client durchaus PFS beherrschen.

Mit dieser Option legen Sie fest, dass das Gerät immer eine Verbindung über PFS bevorzugt, unabhängig von der Standard-Einstellung des Clients.

SNMP-ID:

2.111.88.6.5

Pfad Konsole:

Setup > **IoT** > **Wireless-ePaper** > **SSL**

Mögliche Werte:

nein
ja

Default-Wert:

ja

Neuverhandlungen

Mit dieser Einstellung steuern Sie, ob der Client eine Neuverhandlung von SSL / TLS auslösen kann.

SNMP-ID:

2.111.88.6.6

Pfad Konsole:

Setup > **IoT** > **Wireless-ePaper** > **SSL**

Mögliche Werte:

verboten

Das Gerät bricht die Verbindung zur Gegenstelle ab, falls diese eine Neuverhandlung anfordert.

erlaubt

Das Gerät lässt Neuverhandlungen mit der Gegenstelle zu.

ignoriert

Das Gerät ignoriert die Anforderung der Gegenseite zur Neuverhandlung.

Default-Wert:

ignoriert

Elliptische-Kurven

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

SNMP-ID:

2.111.88.6.7

Pfad Konsole:

Setup > **IoT** > **Wireless-ePaper** > **SSL**

Mögliche Werte:

secp256r1

secp256r1 wird zur Verschlüsselung verwendet.

secp384r1

secp384r1 wird zur Verschlüsselung verwendet.

secp521r1

secp521r1 wird zur Verschlüsselung verwendet.

ecdh_x25519

ecdh_x25519 wird zur Verschlüsselung verwendet.

Default-Wert:

secp256r1

secp384r1

secp521r1

ecdh_x25519

Signatur-Hash-Algorithmen

Bestimmen Sie mit diesem Eintrag, mit welchem Hash-Algorithmus die Signatur verschlüsselt werden soll.

SNMP-ID:

2.111.88.6.21

Pfad Konsole:

Setup > **IoT** > **Wireless-ePaper** > **SSL**

Mögliche Werte:

MD5-RSA
SHA1-RSA
SHA224-RSA
SHA256-RSA
SHA384-RSA
SHA512-RSA
SHA256-ECDSA
SHA384-ECDSA
SHA512-ECDSA

Default-Wert:

SHA256-RSA

SHA384-RSA

SHA512-RSA

SHA256-ECDSA

SHA384-ECDSA

SHA512-ECDSA

14.2.3 Loopback-Adresse

Geben Sie hier die Loopback-Adresse an.

SNMP-ID:

2.111.88.7

Pfad Konsole:

Setup > **IoT** > **Wireless-ePaper**

Mögliche Werte:

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

Default-Wert:

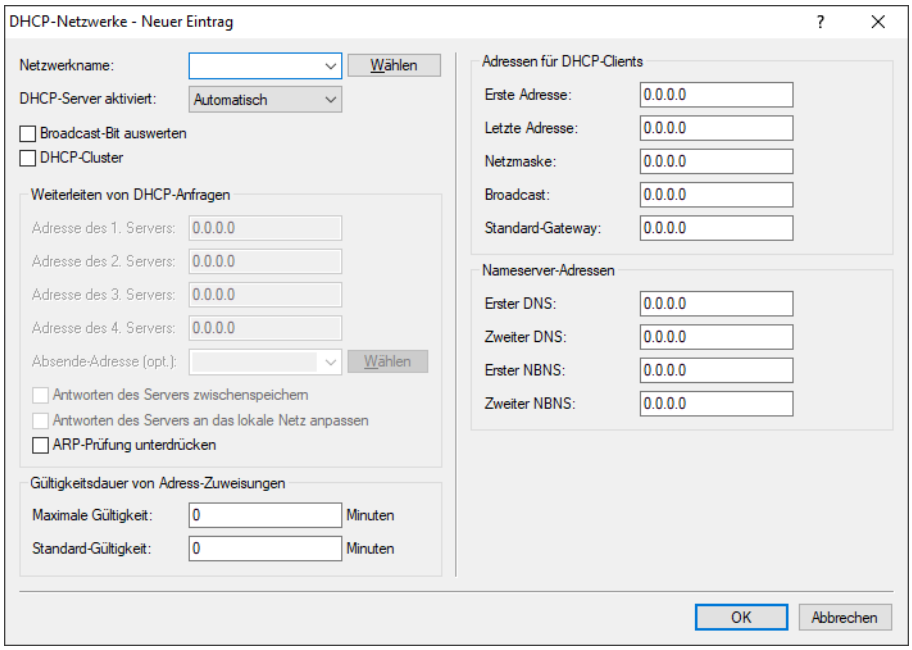
leer

15 Weitere Dienste

15.1 DHCP-Server – ARP-Request unterdrücken

Ab LCOS 10.40 ist die seit LCOS 10.32 RU4 in der CLI verfügbare Option, den ARP-Request vor Vergabe einer IP-Adresse nicht durchzuführen, auch über LANconfig einstellbar.

Den entsprechenden Parameter finden Sie unter **IPv4** > **DHCPv4** > **DHCP-Netzwerke**.



ARP-Prüfung unterdrücken

Normalerweise wird vor der Zuweisung einer IP-Adresse durch den DHCP-Server über einen ARP-Request überprüft, ob diese Adresse bereits vergeben ist. Nach 3 Sekunden ohne Antwort auf den ARP-Request wird dann die Zuweisung durchgeführt. In normalen Netzen, gerade wenn Rechner hochgefahren werden, ist diese Abfrage sinnvoll, da dort auch mit festen IP-Adressen gearbeitet wird. Bei einem Public Spot Netzwerk, in dem z. B. ein Smartphone noch erkennen muss, dass keine Internetverbindung besteht, um dann das Login-Popup anzuzeigen, verzögert dieser ARP-Request diese Zeit unnötig. Gerade für solche Szenarien lässt sich diese Überprüfung hier abschalten.

15.2 DHCP-Client-Option Classless Static Route

Über die Classless Static Route DHCPv4-Option kann ein DHCP-Server eine Liste von statischen Routen an einen DHCP-Client übermitteln, der diese Routen dann in seine Routing-Tabelle einträgt. Die Routen dieser Liste sind „Classless", d. h. zu jeder Route wird eine Subnetzmaske bzw. Präfixlänge übermittelt. Nach *RFC 3442* wird hierzu die Optionsnummer 121 verwendet.

Der DHCP-Client installiert dann beim Empfang keine Default-Route zum spezifizierten Router, sondern nur die Liste der statischen Route in die Routing-Tabelle.

Diese Funktion wird beispielsweise von Internet-Providern in Szenarien verwendet, bei denen mehrere virtuelle Verbindungen nach Dienst über VLAN getrennt werden, z. B. jeweils ein VLAN für Internet, VoIP und IPTV. In diesem Fall wird für die Internetverbindung (z. B. über PPPoE oder DHCP) die Default-Route verwendet, die notwendigen Routen für IPTV über ein anderes VLAN per DHCP als Classless Static Route Option.

Der LANCOM DHCPv4-Client fragt standardmäßig sowohl Router als auch die Option „Classless Static Routes" an. Wird vom DHCP-Server eine Option „Classless Static Routes" ausgeliefert, so wird eine ggf. vorhandene Router-Option ignoriert und nur die Liste der Routen installiert. Dieses Verhalten ist RFC-konform nach RFC 3442.

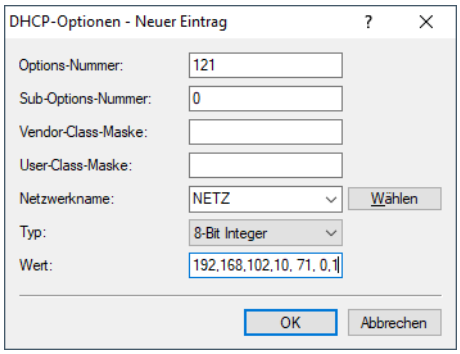
Für ein Provider-Szenario mit IPTV legen Sie dazu eine neue DSL-Gegenstelle mit Haltezeit 9999, Layer DHCPOE sowie dem entsprechenden VLAN nach Providervorgaben an. Aktivieren Sie den Schalter **Gegenstelle auch ohne Route aufbauen (Keepalive ohne Route)** unter **Kommunikation** > **Gegenstellen**. Es ist kein Eintrag in der Routing-Tabelle nötig, da der DHCP-Client die notwendigen Routen per Option „Classless Static Route" empfängt.

Der LANCOM DHCP-Server kann die Option „Classless Static Route" per benutzerdefinierter Option ebenfalls an DHCP-Clients vergeben.

Beispiel: Option „Classless Static Route" im DHCP-Server übertragen

Um die Route 192.168.102.0/24 via 10.71.0.1 als Classless Static Route Option (121) im DHCP-Server zu übertragen, legen Sie folgenden Eintrag in der Tabelle **IPv4** > **DHCPv4** > **DHCP-Optionen** an:

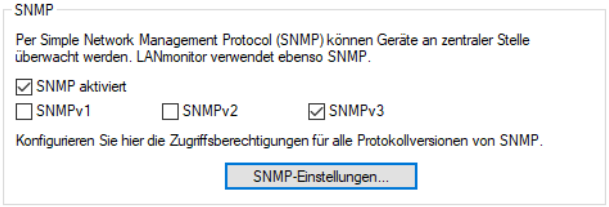
- **Options-Nummer** – 121
- **Netzwerkname** – Name des Netzes, in dem die Option an Clients übertragen werden soll.
- **Typ** – 8 Bit Integer
- **Wert** – 24,192,168,102,10, 71, 0,1



15.3 Simple Network Management Protocol (SNMP)

15.3.1 SNMP konfigurieren

In LANconfig konfigurieren Sie SNMP unter **Meldungen/Monitoring** > **Protokolle** im Abschnitt **SNMP**.



SNMP aktiviert

Aktivieren Sie SNMP für die im Folgenden angegebenen SNMP-Protokollversionen, die das Gerät bei SNMP-Anfragen und SNMP-Traps unterstützen soll.

SNMPv1

Aktiviert SNMPv1.

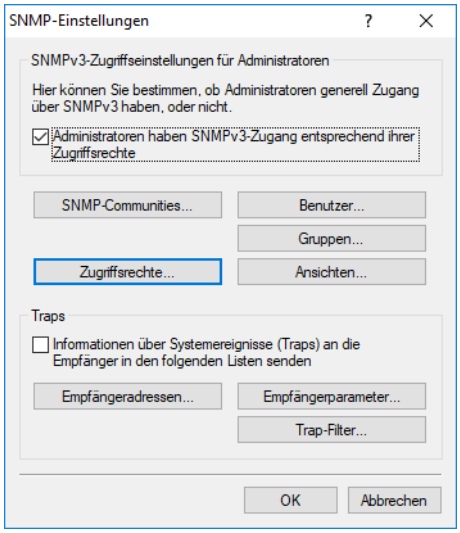
SNMPv2

Aktiviert SNMPv2c.

SNMPv3

Aktiviert SNMPv3.

Mit einem Klick auf **SNMP-Einstellungen** öffnen Sie die Konfigurationeinstellungen.



SNMP-Einstellungen

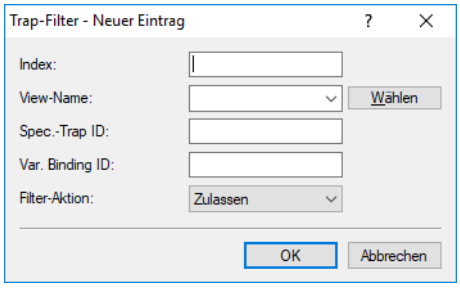
Traps

Wenn Sie die Option **Informationen über Systemereignisse (Traps) an die Empfänger in den folgenden Listen senden** aktivieren, dann bekommen die unter **Empfängeradressen** und **Empfängerparameter** konfigurierten Empfänger entsprechende Informationen. Die Systemereignisse, die eine Meldung auslösen, lassen sich über Trap-Filter einschränken.

Trap-Filter

Bestimmte SNMP-Traps bzw. eine große Anzahl von SNMP-Traps können auf den empfangenden Servern mitunter ungewünscht sein. Daher lässt sich ab LCOS 10.40 eine SNMP-Filterliste hinzufügen, die es erlaubt, SNMP-Traps basierend auf ihren Hersteller-spezifischen OIDs oder den in den Variable Bindings enthaltenen OIDs wahlweise durchzulassen oder zurückzuhalten.

Traps für den Benutzer „root" können nicht gefiltert werden. Für die Filterung muss ein separater SNMP-Benutzer verwendet werden.



Index

Die Position dieses Eintrags in der Filterliste. Die Liste wird vom kleinsten zum größten Wert überprüft bis zum ersten

Treffer.

View-Name

Der **View-Name** ist der Name einer **Ansicht**, für den diese Filterregel gültig ist. Ist der **Zugriff auf Teilbaum** der betreffenden Ansicht auf „hinzugefügt" gesetzt, dann lassen sich mit einer zugehörigen Filterregel mit der **Filter-Aktion** „Ablehnen" die entsprechenden Traps verhindern. Ist der **Zugriff auf Teilbaum** der betreffenden Ansicht hingegen auf „entfernt" gesetzt, so lassen sich mit der **Filter-Aktion** „Zulassen" die Meldungen dennoch als Ausnahme senden. Da in den **Ansichten** mehrere Eintrgäge gleichen Namens mit verschiedenen Zugriffseinstellungen erlaubt sind, muss die **Filter-Aktion** unabhängig vom Wert der jeweiligen Einstellung des **Zugriff auf Teilbaum** gesetzt werden können.

Spec.-Trap ID

Gibt eine spezifische Trap-ID an, die Wildcards und Bereiche enthalten darf. Ein leerer Eintrag gilt für alle spezifischen Trap IDs des Gerätes. Siehe Beispiele in der folgenden Tabelle.

OID	Beschreibung
	Trifft auf jede OID zu.
1.2.3	Trifft auf alle OIDs zu, die mit „1.2.3" beginnen.
1.*.3	Trifft auf alle OIDs zu, die mit „1" beginnen, dann einen beliebigen Wert haben und dann mit „3" fortgesetzt werden.
1.2-3.4	Trifft auf alle OIDs zu, die mit „1" beginnen, dann mit einer Stelle im Bereich „2 bis 3" gefolgt von einer „4" fortgesetzt werden.
1.2.3-4,7-8	Trifft auf alle OIDs zu, die mit „1.2" beginnen und dann mit einer Stelle im Bereich „3 bis 4" oder „7 bis 8" fortgesetzt werden.

Wildcards und Bereichsangaben dürfen an jeder beliebigen Stelle einer OID vorkommen und eine OID darf auch mehrere Wildcards oder Bereichsangaben enthalten. An jeder Stelle darf aber nur entweder eine Wildcard oder eine Bereichsangabe stehen.

Ein LANCOM Gerät bildet die generischen Trap-OIDs des SNMP-Protokolls auf bestimmte Herstellerspezifische OIDs ab:

Bezeichnung	Generische OID	OID bei LANCOM
Kaltstart (coldStart)	0	1.3.6.1.6.3.1.1.5.1

Bezeichnung	Generische OID	OID bei LANCOM
Warmstart (warmStart)	1	1.3.6.1.6.3.1.1.5.2
Link Down (linkDown)	2	1.3.6.1.6.3.1.1.5.3
Link Up (linkUp)	3	1.3.6.1.6.3.1.1.5.4
Authentifizierungsfehler (authenticationFailure)	4	1.3.6.1.6.3.1.1.5.5
EGP-Nachbar (Exterior Gateway Protocol) verloren (egpNeighborLoss)	5	1.3.6.1.6.3.1.1.5.6

Var. Binding ID

Gibt eine OID an, die in den Variable Bindings des Traps enthalten sein muss und die wiederum Wildcards und Bereiche enthalten darf. Siehe hierzu auch **Spec.-Trap ID**. Ein leerer Eintrag gilt für alle variablen Bindings des Gerätes.

Filter-Aktion

Bei einer Übereinstimmung mit den oben eingestellten IDs können Sie den Trap entweder „Zulassen", also senden oder „Ablehnen", also verwerfen.

Ergänzungen im Setup-Menü

Filter

Bestimmte SNMP-Traps bzw. eine große Anzahl von SNMP-Traps können auf den empfangenden Servern mitunter ungewünscht sein. Daher lässt sich eine SNMP-Filterliste hinzufügen, die es erlaubt, SNMP-Traps basierend auf ihren Hersteller-spezifischen OIDs oder den in den Variable Bindings enthaltenen OIDs wahlweise durchzulassen oder zurückzuhalten.

Traps für den Benutzer „root" können nicht gefiltert werden. Für die Filterung muss ein separater SNMP-Benutzer verwendet werden.

SNMP-ID:

2.9.42

Pfad Konsole:

Setup > SNMP

Index

Die Position dieses Eintrags in der Filterliste. Die Liste wird vom kleinsten zum größten Wert überprüft bis zum ersten Treffer.

SNMP-ID:

2.9.42.1

Pfad Konsole:

Setup > SNMP > Filter

Mögliche Werte:

max. 4 Zeichen aus `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

View-Name

Geben Sie hier den Name einer Ansicht aus **Setup** > **SNMP** > **Ansichten** > **View-Name** ein, für den diese Filterregel gültig ist. Ist der Zugriff im Wert **Setup** > **SNMP** > **Ansichten** > **Type** dieser Ansicht auf „Included" gesetzt, dann lassen sich mit einer zugehörigen Filterregel mit der **Filter-Aktion** „Verbieten" die entsprechenden Traps verhindern. Ist der entsprechende Zugriff hingegen auf „Excluded" gesetzt, so lassen sich mit der Filter-Aktion „Erlauben" die Meldungen dennoch als Ausnahme senden. Da in den Ansichten mehrere Eintrgäge gleichen Namens mit verschiedenen Zugriffseinstellungen erlaubt sind, muss die Filter-Aktion unabhängig vom Wert der jeweiligen Einstellung im Wert **Setup** > **SNMP** > **Ansichten** > **Type** gesetzt werden können.

SNMP-ID:

2.9.42.2

Pfad Konsole:

Setup > **SNMP** > **Filter**

Mögliche Werte:

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

Spez.-TrapID

Gibt eine spezifische Trap-ID an, die Wildcards und Bereiche enthalten darf. Ein leerer Eintrag gilt für alle spezifischen Trap IDs des Gerätes. Siehe Beispiele in der folgenden Tabelle.

OID	Beschreibung
	Trifft auf jede OID zu.
1.2.3	Trifft auf alle OIDs zu, die mit „1.2.3" beginnen.
1.*.3	Trifft auf alle OIDs zu, die mit „1" beginnen, dann einen beliebigen Wert haben und dann mit „3" fortgesetzt werden.
1.2-3.4	Trifft auf alle OIDs zu, die mit „1" beginnen, dann mit einer Stelle im Bereich „2 bis 3" gefolgt von einer „4" fortgesetzt werden.
1.2.3-4,7-8	Trifft auf alle OIDs zu, die mit „1.2" beginnen und dann mit einer Stelle im Bereich „3 bis 4" oder „7 bis 8" fortgesetzt werden.

Wildcards und Bereichsangaben dürfen an jeder beliebigen Stelle einer OID vorkommen und eine OID darf auch mehrere Wildcards oder Bereichsangaben enthalten. An jeder Stelle darf aber nur entweder eine Wildcard oder eine Bereichsangabe stehen.

Ein LANCOM Gerät bildet die generischen Trap-OIDs des SNMP-Protokolls auf bestimmte Herstellerspezifische OIDs ab:

Bezeichnung	Generische OID	OID bei LANCOM
Kaltstart (coldStart)	0	1.3.6.1.6.3.1.1.5.1
Warmstart (warmStart)	1	1.3.6.1.6.3.1.1.5.2

Bezeichnung	Generische OID	OID bei LANCOM
Link Down (linkDown)	2	1.3.6.1.6.3.1.1.5.3
Link Up (linkUp)	3	1.3.6.1.6.3.1.1.5.4
Authentifizierungsfehler (authenticationFailure)	4	1.3.6.1.6.3.1.1.5.5
EGP-Nachbar verloren (egpNeighborLoss)	5	1.3.6.1.6.3.1.1.5.6

SNMP-ID:

2.9.42.3

Pfad Konsole:

Setup > **SNMP** > **Filter**

Mögliche Werte:

max. 128 Zeichen aus `[0-9],-*.`

Var.BindingID

Gibt eine OID an, die in den Variable Bindings des Traps enthalten sein muss und die wiederum Wildcards und Bereiche enthalten darf. Ein leerer Eintrag gilt für alle variablen Bindings des Gerätes. Siehe Beispiele in der folgenden Tabelle.

OID	Beschreibung
	Trifft auf jede OID zu.
1.2.3	Trifft auf alle OIDs zu, die mit „1.2.3“ beginnen.
1.*.3	Trifft auf alle OIDs zu, die mit „1“ beginnen, dann einen beliebigen Wert haben und dann mit „3“ fortgesetzt werden.
1.2-3.4	Trifft auf alle OIDs zu, die mit „1“ beginnen, dann mit einer Stelle im Bereich „2 bis 3“ gefolgt von einer „4“ fortgesetzt werden.
1.2.3-4,7-8	Trifft auf alle OIDs zu, die mit „1.2“ beginnen und dann mit einer Stelle im Bereich „3 bis 4“ oder „7 bis 8“ fortgesetzt werden.

Wildcards und Bereichsangaben dürfen an jeder beliebigen Stelle einer OID vorkommen und eine OID darf auch mehrere Wildcards oder Bereichsangaben enthalten. An jeder Stelle darf aber nur entweder eine Wildcard oder eine Bereichsangabe stehen.

SNMP-ID:

2.9.42.4

Pfad Konsole:

Setup > **SNMP** > **Filter**

Mögliche Werte:

max. 128 Zeichen aus `[0-9],-*.`

Filter-Aktion

Bei einer Übereinstimmung mit den eingestellten OID können Sie den Trap entweder „Erlauben“, also senden oder „Verbieten“, also verwerfen.

SNMP-ID:

2.9.42.5

Pfad Konsole:

Setup > **SNMP** > **Filter**

Mögliche Werte:

Erlauben
Verbieten

15.4 Netflow / IPFIX

NetFlow ist eine Technik, bei der Netzwerkgeräte wie Router oder Switches Informationen über den ein- und ausgehenden IP-Datenverkehr innerhalb des Geräts per UDP als sogenannte IP-Flows exportieren. Ein IP-Flow enthält u. a. Informationen über Quell-IP-Adresse, Ziel-IP-Adresse, Ports, Zeitstempel sowie Paketzähler. Diese Informationen werden auf einem NetFlow-Kollektor empfangen, gespeichert und verarbeitet. NetFlow kann entweder dauerhaft oder temporär zur Netzwerkanalyse eingesetzt werden.

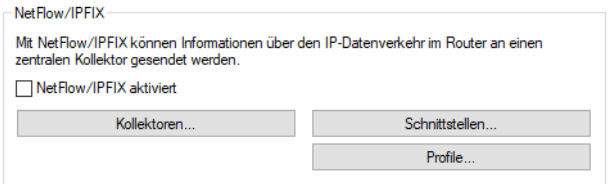
LANCOM unterstützt die Standards NetFlow 9 (*RFC 3954*) sowie IPFIX (*RFC 7011*), welches eine Erweiterung von Netflow Version 9 darstellt, über das Transportprotokoll UDP.

Hinweise zum Einsatz:

- Es wird ein externer NetFlow-Kollektor benötigt, der NetFlow 9 oder IPFIX unterstützt.
- Die Firewall muss grundsätzlich aktiviert sein.
- Bei IPv4 werden nur Flow-Informationen gesammelt, die von einer logischen Schnittstelle zu einer anderen logischen Schnittstelle weitergeleitet werden. Pakete, die der Router selbst erzeugt bzw. an den Router selbst gerichtet sind, werden nicht erfasst. Bei IPv6 gilt diese Einschränkung nicht.
- Es werden nur Unicast IP-Flow-Informationen gesammelt, Multicast (z. B. IPTV) wird nicht unterstützt.
- Je nach Szenario erhöht die Verwendung von NetFlow / IPFIX die CPU-Auslastung und reduziert die Gesamt-Performance des Routers.

15.4.1 NetFlow / IPFIX konfigurieren

In LANconfig konfigurieren Sie NetFlow / IPFIX unter **Meldungen/Monitoring** > **Protokolle** im Abschnitt **NetFlow / IPFIX**.

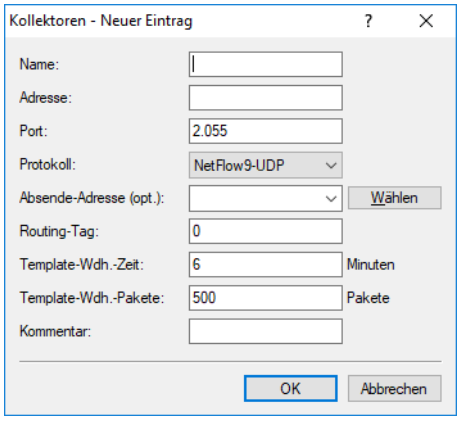


NetFlow / IPFIX aktiviert

Aktivieren Sie NetFlow / IPFIX auf dem Gerät.

Kollektoren

Die Kollektoren für NetFlow / IPFIX konfigurieren Sie unter **Meldungen/Monitoring** > **Protokolle** > **NetFlow / IPFIX** > **Kollektoren**.



Name

Eindeutiger Name des NetFlow-Kollektors. Der Name wird in weiteren Tabellen referenziert.

Adresse

IPv4-, IPv6-Adresse oder Hostname des Kollektors.

Port

Port des NetFlow-Kollektors. Meistens Port 2055 für NetFlow 9 und 4739 für IPFIX.

Protokoll

Protokollversion, die vom NetFlow-Kollektor verwendet wird. Mögliche Werte sind NetFlow 9 über UDP oder IPFIX über UDP.

Absende-Adresse

Geben Sie optional eine Absendeadresse an.

Routing-Tag

Geben Sie ein Routing-Tag an, falls eine bestimmte Route zum Kollektor verwendet werden soll.

Template-Wdh.-Zeit

Definiert die Zeit in Minuten, nach der ein NetFlow-Template-Record wiederholt übertragen wird. Der Wert 0 deaktiviert das regelmäßige Senden von Template-Records basierend auf einem Zeitintervall.

Eine Wiederholung der Übertragung des Netflow-Template-Pakets findet entweder nach der definierten Zeit in Minuten oder nach der entsprechenden Anzahl von Flow-Paketen statt, je nachdem welches Ereignis früher eintritt.

Template-Wdh.-Pakete

Definiert die Anzahl von Paketen, nach der ein NetFlow-Template-Record wiederholt übertragen wird. Der Wert 0 deaktiviert das regelmäßige Senden von Template-Records basierend auf einem Paketzähler.

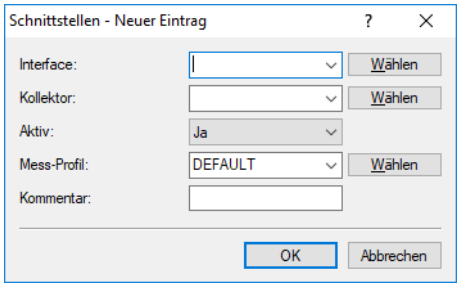
Eine Wiederholung der Übertragung des Netflow-Template-Pakets findet entweder nach der definierten Zeit in Minuten oder nach der entsprechenden Anzahl von Flow-Paketen statt, je nachdem welches Ereignis früher eintritt.

Kommentar

Vergeben Sie optional einen sinnvollen Kommentar als Beschreibung.

Schnittstellen

Die Schnittstellen für NetFlow / IPFIX konfigurieren Sie unter **Meldungen/Monitoring** > **Protokolle** > **NetFlow / IPFIX** > **Schnittstellen**.



Interface

Logische Schnittstelle, auf der NetFlow / IPFIX aktiviert werden soll. Mögliche Werte: IPv4-, IPv6-LAN-Schnittstellen, Gegenstellen, IPv6-RAS-Template. Für IPv4-Gegenstellen kann eine Wildcard verwendet werden, z. B. Firma*

Kollektor

Referenziert einen Eintrag aus der Tabelle Kollektoren.

Aktiv

Aktiviert / Deaktiviert NetFlow / IPFIX für diesen Eintrag für die Schnittstelle und den Kollektor.

Mess-Profil

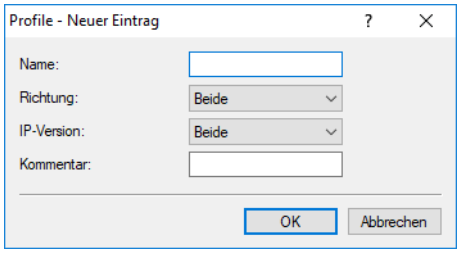
Referenziert einen Eintrag aus der Tabelle Profile.

Kommentar

Vergeben Sie optional einen sinnvollen Kommentar als Beschreibung.

Profile

Die Profile für NetFlow / IPFIX konfigurieren Sie unter **Meldungen/Monitoring** > **Protokolle** > **NetFlow / IPFIX** > **Profile**.



Name

Eindeutiger Name des Mess-Profils. Der Name wird in weiteren Tabellen referenziert.

Richtung

IP-Flow-Richtung, die von NetFlow / IPFIX berücksichtigt werden soll. Mögliche Werte jeweils aus der Sicht von NetFlow / IPFIX: Eingehend, Ausgehend, Beide

IP-Version

IP-Protokoll-Version(en), die von NetFlow / IPFIX berücksichtigt werden soll, Mögliche Werte: IPv4, IPv6, Beide

Kommentar

Vergeben Sie optional einen sinnvollen Kommentar als Beschreibung.

15.4.2 Ergänzungen im Setup-Menü

NetFlow

NetFlow ist eine Technik, bei der Netzwerkgeräte wie Router oder Switches Informationen über den ein- und ausgehenden IP-Datenverkehr innerhalb des Geräts per UDP als sogenannte IP-Flows exportieren. Ein IP-Flow enthält u. a. Informationen über Quell-IP-Adresse, Ziel-IP-Adresse, Ports, Zeitstempel sowie Paketzähler. Diese Informationen werden auf einem NetFlow-Kollektor empfangen, gespeichert und verarbeitet. NetFlow kann entweder dauerhaft oder temporär zur Netzwerkanalyse eingesetzt werden.

LANCOM unterstützt die Standards NetFlow 9 (*RFC 3954*) sowie IPFIX (*RFC 7011*), welches eine Erweiterung von Netflow Version 9 darstellt, über das Transportprotokoll UDP.

Hinweise zum Einsatz:

- Es wird ein externer NetFlow-Kollektor benötigt, der NetFlow 9 oder IPFIX unterstützt.
- Die Firewall muss grundsätzlich aktiviert sein.
- Bei IPv4 werden nur Flow-Informationen gesammelt, die von einer logischen Schnittstelle zu einer anderen logischen Schnittstelle weitergeleitet werden. Pakete, die der Router selbst erzeugt bzw. an den Router selbst gerichtet sind, werden nicht erfasst. Bei IPv6 gilt diese Einschränkung nicht.
- Es werden nur Unicast IP-Flow-Informationen gesammelt, Multicast (z. B. IPTV) wird nicht unterstützt.
- Je nach Szenario erhöht die Verwendung von NetFlow / IPFIX die CPU-Auslastung und reduziert die Gesamt-Performance des Routers.

SNMP-ID:

2.109

Pfad Konsole:

Setup

Collectors

Konfigurieren Sie hier die Kollektoren für NetFlow / IPFIX.

SNMP-ID:

2.109.1

Pfad Konsole:

Setup > **NetFlow**

Name

Eindeutiger Name des NetFlow-Kollektors. Der Name wird in weiteren Tabellen referenziert.

SNMP-ID:

2.109.1.1

Pfad Konsole:

Setup > **NetFlow** > **Collectors**

Mögliche Werte:

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

Adresse

IPv4-, IPv6-Adresse oder Hostname des Kollektors.

SNMP-ID:

2.109.1.2

Pfad Konsole:

Setup > **NetFlow** > **Collectors**

Mögliche Werte:

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

Port

Port des NetFlow-Kollektors. Meistens Port 2055 für NetFlow 9 und 4739 für IPFIX.

SNMP-ID:

2.109.1.3

Pfad Konsole:

Setup > **NetFlow** > **Collectors**

Mögliche Werte:

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

Protokoll

Protokollversion, die vom NetFlow-Kollektor verwendet wird.

SNMP-ID:

2.109.1.4

Pfad Konsole:

Setup > **NetFlow** > **Collectors**

Mögliche Werte:

IPFIX-UDP
NetFlow9-UDP

Loopback-Addr.

Geben Sie optional eine Absendeadresse an.

SNMP-ID:

2.109.1.5

Pfad Konsole:

Setup > **NetFlow** > **Collectors**

Mögliche Werte:

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

Rtg-Tag

Geben Sie ein Routing-Tag an, falls eine bestimmte Route zum Kollektor verwendet werden soll.

SNMP-ID:

2.109.1.6

Pfad Konsole:

Setup > **NetFlow** > **Collectors**

Mögliche Werte:

0 … 65535

Default-Wert:

0

Template-Refresh-Zeit

Definiert die Zeit in Minuten, nach der ein NetFlow-Template-Record wiederholt übertragen wird. Der Wert 0 deaktiviert das regelmäßige Senden von Template-Records basierend auf einem Zeitintervall.

Eine Wiederholung der Übertragung des Netflow-Template-Pakets findet entweder nach der definierten Zeit in Minuten oder nach der entsprechenden Anzahl von Flow-Paketen statt, je nachdem welches Ereignis früher eintritt.

SNMP-ID:

2.109.1.7

Pfad Konsole:

Setup > **NetFlow** > **Collectors**

Mögliche Werte:

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

Template-Refresh-Pakete

Definiert die Anzahl von Paketen, nach der ein NetFlow-Template-Record wiederholt übertragen wird. Der Wert 0 deaktiviert das regelmäßige Senden von Template-Records basierend auf einem Paketzähler.

Eine Wiederholung der Übertragung des Netflow-Template-Pakets findet entweder nach der definierten Zeit in Minuten oder nach der entsprechenden Anzahl von Flow-Paketen statt, je nachdem welches Ereignis früher eintritt.

SNMP-ID:

2.109.1.8

Pfad Konsole:

Setup > **NetFlow** > **Collectors**

Mögliche Werte:

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

Kommentar

Vergeben Sie optional einen sinnvollen Kommentar als Beschreibung.

SNMP-ID:

2.109.1.99

Pfad Konsole:

Setup > **NetFlow** > **Collectors**

Mögliche Werte:

max. 50 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Schnittstellen

Konfigurieren Sie hier die Schnittstellen für NetFlow / IPFIX.

SNMP-ID:

2.109.2

Pfad Konsole:

Setup > **NetFlow**

Ifc

Logische Schnittstelle, auf der NetFlow / IPFIX aktiviert werden soll. Mögliche Werte: IPv4-, IPv6-LAN-Schnittstellen, Gegenstellen, IPv6-RAS-Template. Für IPv4-Gegenstellen kann eine Wildcard verwendet werden, z. B. Firma*

SNMP-ID:

2.109.2.1

Pfad Konsole:

Setup > **NetFlow** > **Schnittstellen**

Mögliche Werte:

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

Collector

Referenziert einen Eintrag aus der Tabelle Kollektoren.

SNMP-ID:

2.109.2.2

Pfad Konsole:

Setup > **NetFlow** > **Schnittstellen**

Mögliche Werte:

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

Aktiv

Aktiviert / Deaktiviert NetFlow / IPFIX für diesen Eintrag für die Schnittstelle und den Kollektor.

SNMP-ID:

2.109.2.3

Pfad Konsole:

Setup > **NetFlow** > **Schnittstellen**

Mögliche Werte:

ja

NetFlow / IPFIX ist für diese Schnittstelle aktiviert.

nein

NetFlow / IPFIX ist für diese Schnittstelle nicht aktiviert.

Metering-Profil

Referenziert einen Eintrag aus der Tabelle Metering-Profile.

SNMP-ID:

2.109.2.4

Pfad Konsole:

Setup > **NetFlow** > **Schnittstellen**

Mögliche Werte:

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

Kommentar

Vergeben Sie optional einen sinnvollen Kommentar als Beschreibung.

SNMP-ID:

2.109.2.99

Pfad Konsole:

Setup > **NetFlow** > **Schnittstellen**

Mögliche Werte:

max. 50 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Aktiv

Aktivieren Sie NetFlow / IPFIX auf dem Gerät.

SNMP-ID:

2.109.3

Pfad Konsole:

Setup > **NetFlow**

Mögliche Werte:

ja

NetFlow / IPFIX ist aktiviert.

nein

NetFlow / IPFIX ist nicht aktiviert.

Metering-Profile

Konfigurieren Sie hier die Profile für NetFlow / IPFIX.

SNMP-ID:

2.109.4

Pfad Konsole:

Setup > **NetFlow**

Name

Eindeutiger Name des Mess-Profils. Der Name wird in weiteren Tabellen referenziert.

SNMP-ID:

2.109.4.1

Pfad Konsole:

Setup > **NetFlow** > **Metering-Profil**

Mögliche Werte:

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

Richtung

IP-Flow-Richtung, die von NetFlow / IPFIX berücksichtigt werden soll.

SNMP-ID:

2.109.4.2

Pfad Konsole:

Setup > **NetFlow** > **Metering-Profil**

Mögliche Werte:

Eingang

Eingehende IP-Datenströme aus der Sicht von NetFlow / IPFIX.

Ausgang

Ausgehende IP-Datenströme aus der Sicht von NetFlow / IPFIX.

Alle

Ein- und ausgehende IP-Datenströme.

IP-Version

IP-Protokoll-Version(en), die von NetFlow / IPFIX berücksichtigt werden soll,

SNMP-ID:

2.109.4.3

Pfad Konsole:

Setup > **NetFlow** > **Metering-Profil**

Mögliche Werte:

IPv4
IPv6
Alle

Kommentar

Vergeben Sie optional einen sinnvollen Kommentar als Beschreibung.

SNMP-ID:

2.109.4.99

Pfad Konsole:

Setup > **NetFlow** > **Metering-Profil**

Mögliche Werte:

max. 50 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``