

# LCOS 10.90

## Addendum

03/2025



**LANCOM**  
SYSTEMS

# Inhalt

<b>1 Addendum zur LCOS-Version 10.90.....</b>	<b>5</b>
<b>2 Konfiguration.....</b>	<b>6</b>
2.1 Änderung des automatischen Ladens von USB.....	6
2.2 Erweiterungen bei iperf.....	6
2.3 Automatische Ermittlung der PMTU im Ping-Kommando.....	7
2.4 TCP- / HTTP-Tunnel per CLI erzeugen.....	7
2.4.1 Ergänzungen im Setup-Menü.....	8
<b>3 Diagnose.....</b>	<b>9</b>
3.1 Unterstützung von TLS beim Syslog-Client.....	9
3.1.1 Ergänzungen im Setup-Menü.....	10
3.2 Syslog-Nachrichten nach dem Standard RFC 5424.....	11
3.2.1 Ergänzungen im Setup-Menü.....	11
<b>4 Sicherheit.....</b>	<b>12</b>
4.1 Konfigurierbare Passwortpolicy.....	12
4.1.1 Ergänzungen im Setup-Menü.....	12
<b>5 Routing und WAN-Verbindungen.....</b>	<b>15</b>
5.1 DHCP-Client Broadcast-Bit schaltbar.....	15
5.1.1 Ergänzungen im Setup-Menü.....	15
5.2 Erweiterung der MTU-Liste.....	16
5.2.1 Ergänzungen im Setup-Menü.....	16
<b>6 IPv6.....</b>	<b>18</b>
6.1 Stabil-Private IPv6-Autoconfig-Adressen.....	18
6.1.1 Ergänzungen im Setup-Menü.....	19
<b>7 Quality-of-Service.....</b>	<b>22</b>
7.1 Quality-of-Service (QoS) mit 8 Queues.....	22
7.1.1 Queues.....	22
7.1.2 Queue-Listen.....	24
7.1.3 Schnittstellen.....	25
7.1.4 Paketstau-Aktion.....	25
7.1.5 Beispiel 1: Konfiguration eines QoS-Konzepts mit vier Klassen.....	26
7.1.6 Beispiel 2: Konfiguration eines QoS-Konzepts am VDSL-Anschluss mit zwei QoS-Klassen.....	29
7.1.7 Queue-Nutzung in der Firewall.....	31
7.1.8 Ergänzungen im Setup-Menü.....	34
<b>8 Virtual Private Networks – VPN.....</b>	<b>45</b>
8.1 MOBIKE.....	45
8.1.1 Ergänzungen im Setup-Menü.....	45
8.2 IKEv2 Post-quantum Preshared Keys (PPK).....	46
8.2.1 Ergänzungen im Setup-Menü.....	49

8.3 Null-Verschlüsselung in der IKEv2 Child-SA.....	51
8.3.1 Ergänzungen im Setup-Menü.....	52
8.4 IKE-CFG schickt Subnetzmaske für die verhandelte IP-Adresse mit.....	53
8.4.1 Ergänzungen im Setup-Menü.....	54
8.5 VLB IPv6-Support.....	55
8.5.1 Ergänzungen im Setup-Menü.....	56
<b>9 WLAN-Management.....</b>	<b>58</b>
9.1 WLAN-Management mit Wi-Fi 7.....	58
9.1.1 Ergänzungen im Setup-Menü.....	58
<b>10 Public Spot.....</b>	<b>64</b>
10.1 Public Spot Captive Portal API.....	64
10.1.1 Ergänzungen im Setup-Menü.....	66
<b>11 Backup-Lösungen.....</b>	<b>68</b>
11.1 VRRPv3.....	68
11.1.1 Interaktion mit dem WAN-Backup-Modul.....	68
11.1.2 Steuerung des WAN/WAN-Backup durch das VRRP.....	68
11.1.3 Konfiguration von VRRPv3.....	68
11.1.4 Ergänzungen im Setup-Menü.....	72
<b>12 RADIUS.....</b>	<b>82</b>
12.1 RADIUS-Message-Authenticator-Prüfung.....	82
12.1.1 Ergänzungen im Setup-Menü.....	82
<b>13 Weitere Dienste.....</b>	<b>88</b>
13.1 Unterstützung für MTU 1500 im PPPoE nach RFC 4638.....	88
13.1.1 Ergänzungen im Setup-Menü.....	89
13.2 Operations, Administration und Management (OAM).....	89
13.2.1 Ethernet Link OAM (IEEE 802.3ah).....	90
13.2.2 Connectivity Fault Management (IEEE 802.1ag / ITU-T Y.1731).....	93
13.3 Eingabemöglichkeiten bei der Cron-Tabelle bereinigt.....	107
13.3.1 Ergänzungen im Setup-Menü.....	107
13.4 Erweiterungen beim Alive-Test.....	110
13.4.1 Ergänzungen im Setup-Menü.....	110
<b>14 Ergänzungen im Menüsystem.....</b>	<b>113</b>
14.1 Ergänzungen im Setup-Menü.....	113
14.1.1 Max-Auth-Versuche.....	113
14.1.2 Kommentar.....	113
14.1.3 SFP-Ports.....	113
14.1.4 Datenmodell.....	114
14.1.5 System-Boot.....	115
14.1.6 Kaltstart.....	115
<b>15 Entfallene Features.....</b>	<b>117</b>

# Copyright

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

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

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

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

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

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

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

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

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

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

LANCOM Systems GmbH

A Rohde & Schwarz Company

Adenauerstr. 20/B2

52146 Würselen

Deutschland

[www.lancom-systems.de](http://www.lancom-systems.de)

# 1 Addendum zur LCOS-Version 10.90

Dieses Dokument beschreibt die Änderungen und Ergänzungen in der LCOS-Version 10.90 gegenüber der vorherigen Version.

## 2 Konfiguration

### 2.1 Änderung des automatischen Ladens von USB

Ab LCOS 10.90 wurde die Option zum automatischen Laden von Konfigurations- und / oder Skript-Dateien verändert. Die Option zur Konfiguration unter **Management > Erweitert** wurde genau wie der CLI-Wert **Setup > Automatisches-Laden > USB > Konfiguration-und-Skript** (2.60.56.2) entfernt.

Die Konfigurations- und / oder Skript-Dateien werden nur dann automatisch in das Gerät geladen, wenn sich das Gerät im Auslieferungszustand befindet. Durch einen Konfigurations-Reset kann ein Gerät jederzeit wieder auf den Auslieferungszustand zurückgesetzt werden.

### 2.2 Erweiterungen bei iperf

Ab LCOS 10.90 wurde das Kommando iperf um Optionen erweitert, um die Gegenstellenbandbreite zu vermessen und dieses auch aus z. B. der Aktionstabelle automatisiert aufrufen zu können. Mit LCOS 10.90 RU2 wurden die Optionen `--ratediffperc` und `--expbandwidth` hinzugefügt.

Mit diesen Optionen lässt sich folgendes Problem lösen: Bei wiederkehrenden Messungen wird aus den unterschiedlichsten Gründen nicht die zu erwartende Geschwindigkeit gemessen. Beispiel: Ein Kunde vermisst eine Aussenstelle, an welcher normalerweise 40 Down / 10 Up anliegen. Nun wird an einem Sonntag plötzlich eine Rate von 2 Down / 1 Up ermittelt (Server ausgelastet, Kundenbackup läuft unerwartet, usw...). Dann steht der Kunde Montags plötzlich mit einer sehr eingeschränkten Internet-Anbindung da und läuft unerwartet in Performance-Probleme, da die Werte für die Gegenstelle gesetzt bzw. übernommen werden. Lösung: Unterschreiten die ermittelten Down- und Upstream Werte 20% der vorherigen Werte, dann sollen die Messergebnisse verworfen werden und die alten Werte weiter Bestand haben. Falls die RxTx-Rate nicht geändert wurde, so wird dies in das Syslog geschrieben.

**Tabelle 1: Übersicht aller auf der Kommandozeile eingebbaren Befehle**

Befehl	Beschreibung
<code>iperf [-s -c &lt;Host&gt;] [options]</code>	<p>Startet iPerf auf dem Gerät, um eine Bandbreitenmessung mit einer iPerf2-Gegenstelle durchzuführen. Mögliche Optionsschalter sind:</p> <ul style="list-style-type: none"> <li>&gt; <b>Client/Server</b> <ul style="list-style-type: none"> <li>&gt; <code>-q, --quiet</code>: Setzt den quiet-Modus bei dem der CLI-Output unterdrückt wird, da der Befehl auch über die Aktionstabelle aufgerufen werden kann. Außerdem wird im Client-Modus verhindert, dass die Ausführung abgebrochen werden kann.</li> </ul> </li> <li>&gt; <b>Client-spezifisch</b> <ul style="list-style-type: none"> <li>&gt; <code>-R, --reverse</code>: Kehrt die Messrichtung um.</li> <li>&gt; <code>-E, --peer &lt;Interface&gt;</code>: Verbindung über die mit dem Peer-Namen angegebene Schnittstelle herstellen und rx/tx-Grenzwerte auf der Grundlage des Ergebnisses/der Ergebnisse festlegen. Wenn nicht im Dual- oder Tradeoff-Modus ausgeführt, wird der Wert der nicht gemessenen Richtung entsprechend der letzten Messung festgelegt, sofern verfügbar.</li> </ul> </li> </ul>

Befehl	Beschreibung
	<p>Das Ergebnis wird in der Statustabelle <b>Status &gt; Iperf &gt; Last-Results &gt; Peer-Result (1.96.1.3)</b> in den Werten <b>Peer</b>, <b>Server-Bandwidth-kbps</b> und <b>Client-Bandwidth-kbps</b> eingetragen.</p> <ul style="list-style-type: none"> <li>&gt; <code>--retry</code>: Anzahl der Wiederholungsversuche, wenn keine Verbindung möglich ist. Maximum: 99.</li> <li>&gt; <code>--ratediffperc #</code>: Maximal erlaubte Ratenabweichung in Prozent im Peer-Modus (Maximum: 99).</li> <li>&gt; <code>--expbandwidth #/#{kKmM}</code>: Erwartete Down- / Up-Stream-Bandbreite im Peer-Modus. Werte für nicht gemessene Richtungen werden ignoriert. Beispiel: 10/10M</li> </ul>

## 2.3 Automatische Ermittlung der PMTU im Ping-Kommando

Ab LCOS 10.90 gibt es eine neue Kommandozeilenoption für ping, um über den Tracepath-Modus die Pfad-MTU zu ermitteln.

Auf der Kommandozeile nutzen Sie bei ping den neuen optionalen Parameter `-m`.

Parameter	Bedeutung
<code>-m</code>	Wechselt in den tracepath-Modus zur Ermittlung der Pfad-MTU zu der angegebenen IP-Adresse.

## 2.4 TCP- / HTTP-Tunnel per CLI erzeugen

Ab LCOS 10.90 kann der TCP-HTTP-Tunnel auch über ein CLI-Kommando erzeugt werden. Dies war vorher nur über die WEBconfig möglich.

Einen TCP- / HTTP-Tunnel richten Sie über die CLI Ihres Gerätes ein.

1. Melden Sie sich z. B. per SSH an dem Gerät an, hinter dem das freizugebende Gerät erreichbar ist.
2. Gehen Sie über `cd /setup/http` in dieses Verzeichnis
3. Rufen Sie das Kommando `do start-TCP-HTTP-Tunnel -r <Routing Tag> -h <IP-Adresse> -p <Lokaler Port> [-a <Remote-Adresse>]` auf.

**-r**

Routing-Tag.

**-h**

Host-Adresse, auf die über den Tunnel zugegriffen werden soll.

**-p**

Lokaler Port.

**-a**

Optionale Remote-Adresse

Der TCP- / HTTP-Tunnel wurde erzeugt.

## 2.4.1 Ergänzungen im Setup-Menü

### Start-TCP-HTTP-Tunnel

Über diese Aktion können Sie einen TCP- / HTTP-Tunnel erzeugen.

#### SNMP-ID:

2.21.50

#### Pfad Konsole:

Setup > HTTP

#### Mögliche Argumente:

- r  
Routing-Tag.
- h  
Host-Adresse, auf die über den Tunnel zugegriffen werden soll.
- p  
Lokaler Port.
- a  
Optionale Remote-Adresse



## 3 Diagnose

### 3.1 Unterstützung von TLS beim Syslog-Client

Ab LCOS 10.90 unterstützt der Syslog-Client neben den Transportprotokollen UDP und TCP auch die verschlüsselte Übertragung mit TLS.

Die entsprechende Einstellung finden Sie in LANconfig unter **Meldungen/Monitoring > Protokolle > SYSLOG** über **Protokoll**.

SYSLOG-Server - Neuer Eintrag

Adresse des Servers:

Absende-Adresse (opt.):  Wählen

Port:

Protokoll:

RFC5424-Format:

Quelle

System  Logins

Systemzeit  Konsolen-Logins

Verbindungen  Accounting

Verwaltung  Router

Priorität

Alarm  Fehler

Warnung  Information

Debug

Filter-Regeln:

Filter-Name:  Wählen

OK Abbrechen

#### Protokoll

Definiert das verwendete Protokoll. Mögliche Werte:

##### UDP

User Datagram Protocol

##### TCP

Transmission Control Protocol

##### TLS

Der Syslog-Client unterstützt drei Szenarien im TLS-Modus:

1. Der Syslog-Client akzeptiert alle TLS-Server-Zertifikate des Syslog-Servers. Dazu wird im Router kein vertrauenswürdigen CA-Zertifikat hinterlegt.
2. Der Syslog-Client akzeptiert nur Server-Zertifikate, die von einer vertrauenswürdigen CA signiert wurden. Dazu muss das CA-Zertifikat in den entsprechenden Zertifikatsslot des Routers hochgeladen werden.
3. Der Syslog-Client authentifiziert sich mit einem TLS-Client-Zertifikat beim Syslog-Server und der Syslog-Server authentifiziert sich mit seinem CA-Zertifikat. Dazu muss sowohl das TLS-Client-Zertifikat für den Router

und das CA-Zertifikat in den entsprechenden Zertifikatsslot des Routers hochgeladen werden, z. B. in einem Container als PKCS#12-Datei.

Zertifikate für Syslog können entweder über die WEBconfig oder per LANconfig in das Gerät geladen werden.

- > **LANconfig: Rechtsklick auf das Gerät > Konfigurationsverwaltung > Zertifikat oder Datei hochladen**
  - > Syslog - Container als PKCS12-Datei oder
  - > Syslog - Root CA Zertifikat
- > **WEBconfig: Extras > Dateimanagement > Zertifikat oder Datei hochladen > Dateityp**
  - > Syslog - Container als PKCS12-Datei oder
  - > Syslog - Root CA Zertifikat

### 3.1.1 Ergänzungen im Setup-Menü

#### Protokoll

Definiert, über welches Transportprotokoll der Syslog-Client die Syslog-Nachrichten an den Server übertragen soll.

#### SNMP-ID:

2.22.2.9

#### Pfad Konsole:

**Setup > SYSLOG > Tabelle-SYSLOG**

#### Mögliche Werte:

##### TCP

Transmission Control Protocol

##### UDP

User Datagram Protocol

##### TLS

Der Syslog-Client unterstützt drei Szenarien im TLS-Modus:

1. Der Syslog-Client akzeptiert alle TLS-Server-Zertifikate des Syslog-Servers. Dazu wird im Router kein vertrauenswürdiges CA-Zertifikat hinterlegt.
2. Der Syslog-Client akzeptiert nur Server-Zertifikate, die von einer vertrauenswürdigen CA signiert wurden. Dazu muss das CA-Zertifikat in den entsprechenden Zertifikatsslot des Routers hochgeladen werden.
3. Der Syslog-Client authentifiziert sich mit einem TLS-Client-Zertifikat beim Syslog-Server und der Syslog-Server authentifiziert sich mit seinem CA-Zertifikat. Dazu muss sowohl das TLS-Client-Zertifikat für den Router und das CA-Zertifikat in den entsprechenden Zertifikatsslot des Routers hochgeladen werden, z. B. in einem Container als PKCS#12-Datei.

#### Default-Wert:

UDP

## 3.2 Syslog-Nachrichten nach dem Standard RFC 5424

Ab LCOS 10.90 unterstützt der Syslog-Client auch die Formatierung der Syslog-Nachrichten nach dem Standard RFC 5424.

Die entsprechende Einstellung finden Sie in LANconfig unter **Meldungen/Monitoring > Protokolle > SYSLOG** über **SYSLOG-Server**.

### RFC5424-Format

Definiert, ob der Syslog-Client Nachrichten im RFC5424-Format an den Syslog-Server senden soll.

### 3.2.1 Ergänzungen im Setup-Menü

#### RFC5424-Format

Definiert, ob der Syslog-Client Nachrichten im RFC5424-Format an den Syslog-Server senden soll.

#### SNMP-ID:

2.22.2.12

#### Pfad Konsole:

Setup > SYSLOG > Tabelle-SYSLOG

#### Mögliche Werte:

Ja  
Nein

#### Default-Wert:

Nein

## 4 Sicherheit

### 4.1 Konfigurierbare Passwortpolicy

Ab LCOS 10.90 können Sie die Richtlinie für die Geräte-Passwörter konfigurieren. Dazu gehen Sie in LANconfig unter **Management > Admin > Geräte-Konfiguration > Geräte-Passwort-Richtlinie erzwingen** und passen diese an.

Geräte-Konfiguration

Geräte-Passwort-Richtlinie erzwingen

Komplexitätsklassen:

Min. Anzahl versch. Zeichen:  Zeichen

Minimale Länge:  Zeichen

Administrator-Name (optional):

Hauptgerätepassewort:   Anzeigen

Sie können auch weitere Geräte-Administratoren einrichten:

---

Konfigurations-Login-Sperre

Sperre aktivieren nach:  Fehl-Logins

Dauer der Sperre:  Minuten

#### Komplexitätsklassen

Konfigurieren Sie hier die notwendige Anzahl an unterschiedlichen Komplexitätsklassen für Passwörter. Komplexitätsklassen sind Klein- bzw. Großbuchstaben, Zahlen und Sonderzeichen. Bei einer Einstellung von 2 müsste das Passwort somit Zeichen aus mindestens zweien dieser Komplexitätsklassen enthalten.

#### Minimale Anzahl verschiedener Zeichen

Konfigurieren Sie hier die notwendige Anzahl an unterschiedlichen Zeichen für Passwörter.

#### Minimale Länge

Konfigurieren Sie hier die minimale Anzahl an Zeichen für Passwörter.

#### 4.1.1 Ergänzungen im Setup-Menü

##### Passwortkomplexität

Konfigurieren Sie in diesem Menü die Längen- und Komplexitätsanforderungen an Passwörter.

##### SNMP-ID:

2.11.89.4

##### Pfad Konsole:

Setup > Config > Passwoerter

**Minimallaenge**

Konfigurieren Sie hier die minimale Anzahl an Zeichen für Passwörter.

**SNMP-ID:**

2.11.89.4.1

**Pfad Konsole:**

**Setup > Config > Passwoerter > Passwortkomplexitaet**

**Mögliche Werte:**

max. 3 Zeichen aus [0-9]

**Default-Wert:**

8

**Unterschiedliche-Zeichen**

Konfigurieren Sie hier die notwendige Anzahl an unterschiedlichen Zeichen für Passwörter.

**SNMP-ID:**

2.11.89.4.2

**Pfad Konsole:**

**Setup > Config > Passwoerter > Passwortkomplexitaet**

**Mögliche Werte:**

max. 3 Zeichen aus [0-9]

**Default-Wert:**

3

**Komplexitaetsklassen**

Konfigurieren Sie hier die notwendige Anzahl an unterschiedlichen Komplexitätsklassen für Passwörter. Komplexitätsklassen sind Klein- bzw. Großbuchstaben, Zahlen und Sonderzeichen. Bei einer Einstellung von 2 müsste das Passwort somit Zeichen aus mindestens zweien dieser Komplexitätsklassen enthalten.

**SNMP-ID:**

2.11.89.4.3

**Pfad Konsole:**

**Setup > Config > Passwoerter > Passwortkomplexitaet**

**Mögliche Werte:**

0 ... 4

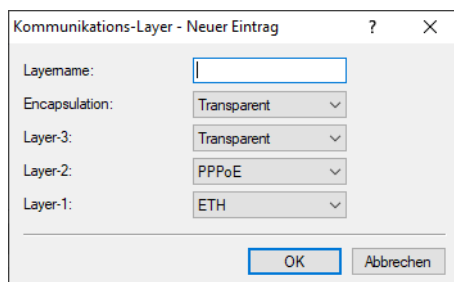
**Default-Wert:**

3

## 5 Routing und WAN-Verbindungen

### 5.1 DHCP-Client Broadcast-Bit schaltbar

Ab LCOS 10.90 kann bei dem Parameter **Layer-3** in LANconfig unter **Kommunikation > Allgemein > Kommunikations-Layer** das DHCP-Client Broadcast-Bit gesetzt werden.



#### Layer-3

Folgende neue Option steht für die Vermittlungsschicht (oder Netzwerkschicht) zur Verfügung:

##### **DHCP (Broadcast-Flag)**

Der Verbindungsaufbau erfolgt mit DHCP-Client und gesetztem Broadcast-Flag im DHCP.

#### 5.1.1 Ergänzungen im Setup-Menü

##### Lay-3

Folgende Optionen stehen für die Vermittlungsschicht (oder Netzwerkschicht) zur Verfügung:

##### **SNMP-ID:**

2.2.4.3

##### **Pfad Konsole:**

**Setup > WAN > Layer**

##### **Mögliche Werte:**

##### **PPP**

Der Verbindungsaufbau erfolgt nach dem PPP-Protokoll (im synchronen Modus, d. h. bitorientiert). Die Konfigurationsdaten werden der PPP-Tabelle entnommen.

##### **DHCP**

Zuordnung der Netzwerkparameter über DHCP.

##### **B-DHCP**

Der Verbindungsaufbau erfolgt mit DHCP-Client und gesetztem Broadcast-Flag im DHCP.

**TRANS**

Transparent: Es wird kein zusätzlicher Header eingefügt.

**Default-Wert:**

PPP

## 5.2 Erweiterung der MTU-Liste

Ab LCOS 10.90 können bei der MTU-Liste Wildcards verwendet werden.

LANconfig: **Kommunikation > Protokolle > MTU-Liste**

**Gegenstelle**

Geben Sie hier den Namen der Gegenstelle ein. Dieser Name muss mit einem Eintrag in der Liste der Gegenstellen übereinstimmen. Sie können auch direkt einen Namen aus der Liste der Gegenstellen auswählen.

Es können dabei die Wildcards „?“ und „\*“ an beliebiger Stelle im Namen der Gegenstelle eingegeben werden. „?“ steht für genau ein Zeichen. „\*“ steht für beliebig viele oder auch kein Zeichen. Die MTU-Liste wird dazu absteigend nach Länge des Gegenstellen-Namens und bei gleicher Länge absteigend in alphabetischer Ordnung sortiert. Dadurch stehen vollständige Namen immer vor Namen mit Wildcards.

### 5.2.1 Ergänzungen im Setup-Menü

**Gegenstelle**

Geben Sie hier den Namen der Gegenstelle ein. Dieser Name muss mit einem Eintrag in der Liste der Gegenstellen übereinstimmen. Sie können auch direkt einen Namen aus der Liste der Gegenstellen auswählen.

Es können dabei die Wildcards „?“ und „\*“ an beliebiger Stelle im Namen der Gegenstelle eingegeben werden. „?“ steht für genau ein Zeichen. „\*“ steht für beliebig viele oder auch kein Zeichen. Die MTU-Liste wird dazu absteigend nach Länge des Gegenstellen-Namens und bei gleicher Länge absteigend in alphabetischer Ordnung sortiert. Dadurch stehen vollständige Namen immer vor Namen mit Wildcards.

**SNMP-ID:**

2.2.26.1

**Pfad Konsole:**

**Setup > WAN > MTU-Liste**

**Mögliche Werte:**

Auswahl aus der Liste der definierten Gegenstellen

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



**Default-Wert:**

*leer*

## 6 IPv6

### 6.1 Stabil-Private IPv6-Autoconfig-Adressen

Ab LCOS 10.90 gibt es den neuen Parameter **Identifizier-Modus** in LANconfig sowohl unter **IPv6 > Allgemein > LAN-Schnittstellen** als auch unter **IPv6 > Allgemein > WAN-Profil**

LAN-Schnittstellen - Neuer Eintrag

Schnittstelle aktiv

Interface-Name:

Schnittstellen-Zuordnung: BRG-1

VLAN-ID:

Schnittstellen-Tag:

Identifizier-Modus: EUI-64

Autokonfiguration

Router-Advertisements akzeptieren

Forwarding

MTU:

Firewall für dieses Interface aktiv

ND-Proxy

Kommentar:

OK Abbrechen

WAN-Profil - Neuer Eintrag

Eintrag aktiv

Profilname:

Schnittstellen-Tag:

Identifizier-Modus: EUI-64

Autokonfiguration

Router-Advertisements akzeptieren

Forwarding

Firewall für dieses Interface aktiv

PD-Quellentyp: DHCPv6

ND-Proxy

Kommentar:

OK Abbrechen

#### Identifizier-Modus

Definiert, wie automatisch erzeugte IPv6-Adressen auf dem jeweiligen Interface des Geräts erzeugt werden.

#### EUI-64

Automatisch erzeugte IPv6-Adressen auf dem konfigurierten Interface werden nach dem EUI-64-Prinzip generiert, d. h. die MAC-Adresse wird als Basis für den Host-Anteil der IPv6-Adresse verwendet.

**Stabil-Privat**

Automatisch erzeugte IPv6-Adressen auf dem konfigurierten Interface werden nach RFC 7217 gebildet. Die Erzeugung basiert nicht mehr auf der eindeutigen MAC-Adresse des Geräts oder der Schnittstelle, sondern aus Datenschutzgründen auf einem Teil aus Zufallswerten sowie dem empfangenen Provider-Präfix. Der erzeugte Interface Identifier ist immer stabil bzw. identisch, solange das empfangene Präfix identisch ist. Bei wechselndem Präfix ändert sich auch der Interface-Identifier und somit die gesamte IPv6-Adresse des Geräts.

Außerdem gibt es unter **IPv6 > Allgemein > IPv6-Adressen** im Parameter **Adress-Typ** die folgende neue Option:

> **Stabil-Privat**

Automatisch erzeugte IPv6-Adressen auf dem konfigurierten Interface werden nach RFC 7217 gebildet. Die Erzeugung basiert nicht mehr auf der eindeutigen MAC-Adresse des Geräts oder der Schnittstelle, sondern aus Datenschutzgründen auf einem Teil aus Zufallswerten sowie dem empfangenen Provider-Präfix. Der erzeugte Interface Identifier ist immer stabil bzw. identisch, solange das empfangene Präfix identisch ist. Bei wechselndem Präfix ändert sich auch der Interface-Identifier und somit die gesamte IPv6-Adresse des Geräts.

## 6.1.1 Ergänzungen im Setup-Menü

### Adresstyp

Bestimmen Sie den Typ der IPv6-Adresse.

#### SNMP-ID:

2.70.4.1.3

#### Pfad Konsole:

**Setup > IPv6 > Netzwerk > Adressen**

#### Mögliche Werte:

##### Unicast

Beim Adresstyp Unicast können sie eine vollständige IPv6-Adresse im Feld [2.70.4.1.2 IPv6-Adresse-Präfixlänge](#) inkl. Interface Identifier angeben, z. B. „2001:db8::1234/64“.

##### Anycast

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

##### EUI-64

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



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



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

##### Delegated-Auto-Configuration

Die IPv6-Adresse wird aus dem empfangenen Router Advertisement Präfix auf dem ausgewählten Interface (Feld [2.70.4.1.1 Interface-Name](#)) und dem Host-Identifier aus dem Feld

[2.70.4.1.2 IPv6-Adresse-Präfixlänge](#) gebildet. Im Feld [2.70.4.1.2 IPv6-Adresse-Präfixlänge](#) kann z. B. der Wert „::2/64“ eingetragen werden, zusammen mit dem Präfix „2001:db8::/64“ auf dem Interface ergibt sich dann entsprechend die Adresse „2001:db8::2/64“.

#### **Delegated-DHCPv6**

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

#### **Stabil-Privat**

Automatisch erzeugte IPv6-Adressen auf dem konfigurierten Interface werden nach RFC 7217 gebildet. Die Erzeugung basiert nicht mehr auf der eindeutigen MAC-Adresse des Geräts oder der Schnittstelle, sondern aus Datenschutzgründen auf einem Teil aus Zufallswerten sowie dem empfangenen Provider-Präfix. Der erzeugte Interface Identifizierer ist immer stabil bzw. identisch, solange das empfangene Präfix identisch ist. Bei wechselndem Präfix ändert sich auch der Interface-Identifizierer und somit die gesamte IPv6-Adresse des Geräts.

#### **Default-Wert:**

Unicast

#### **Identifizierer-Modus**

Definiert, wie automatisch erzeugte IPv6-Adressen auf dem jeweiligen Interface des Geräts erzeugt werden.

#### **SNMP-ID:**

2.70.6.15

#### **Pfad Konsole:**

**Setup > IPv6 > LAN-Interfaces**

#### **Mögliche Werte:**

##### **EUI-64**

Automatisch erzeugte IPv6-Adressen auf dem konfigurierten Interface werden nach dem EUI-64-Prinzip generiert, d. h. die MAC-Adresse wird als Basis für den Host-Anteil der IPv6-Adresse verwendet.

##### **Stabil-Privat**

Automatisch erzeugte IPv6-Adressen auf dem konfigurierten Interface werden nach RFC 7217 gebildet. Die Erzeugung basiert nicht mehr auf der eindeutigen MAC-Adresse des Geräts oder der Schnittstelle, sondern aus Datenschutzgründen auf einem Teil aus Zufallswerten sowie dem empfangenen Provider-Präfix. Der erzeugte Interface Identifizierer ist immer stabil bzw. identisch, solange das empfangene Präfix identisch ist. Bei wechselndem Präfix ändert sich auch der Interface-Identifizierer und somit die gesamte IPv6-Adresse des Geräts.

**Default-Wert:**

EUI-64

**Identifizier-Modus**

Definiert, wie automatisch erzeugte IPv6-Adressen auf dem jeweiligen Interface des Geräts erzeugt werden.

**SNMP-ID:**

2.70.7.13

**Pfad Konsole:****Setup > IPv6 > WAN-Interfaces****Mögliche Werte:****EUI-64**

Automatisch erzeugte IPv6-Adressen auf dem konfigurierten Interface werden nach dem EUI-64-Prinzip generiert, d. h. die MAC-Adresse wird als Basis für den Host-Anteil der IPv6-Adresse verwendet.

**Stabil-Privat**

Automatisch erzeugte IPv6-Adressen auf dem konfigurierten Interface werden nach RFC 7217 gebildet. Die Erzeugung basiert nicht mehr auf der eindeutigen MAC-Adresse des Geräts oder der Schnittstelle, sondern aus Datenschutzgründen auf einem Teil aus Zufallswerten sowie dem empfangenen Provider-Präfix. Der erzeugte Interface Identifier ist immer stabil bzw. identisch, solange das empfangene Präfix identisch ist. Bei wechselndem Präfix ändert sich auch der Interface-Identifier und somit die gesamte IPv6-Adresse des Geräts.

**Default-Wert:**

EUI-64

## 7 Quality-of-Service

### 7.1 Quality-of-Service (QoS) mit 8 Queues

Im Folgenden soll konzeptionell die Funktionsweise des Quality-of-Service mit acht Queues erklärt werden. Grundlegend sollen Pakete vom Router auf Basis des DSCP-Wertes im IP-Header priorisiert werden können. Hierfür stehen insgesamt acht **Queues** zur Verfügung, die strikt priorisiert werden. Das bedeutet, dass Pakete nach Verfügbarkeit von der **Queue** mit der höchsten Priorität bis zur **Queue** mit der niedrigsten Priorität versendet werden. Die Zuordnung eines Paketes zu einer **Queue** geschieht auf Basis des DSCP-Werts im IP-Header oder der Zuweisung zu einer Queue über eine Firewall-Regel. Von den acht zur Verfügung stehenden **Queues** sind zwei reserviert, einmal für die **Urgent-Queue** (höchste Priorität, für interne Dienste wie VCM und Protokollpakete) und zum anderen für die **Best-Effort-Queue** (niedrigste Priorität, für alle nicht-priorisierten Pakete). Die verbleibenden sechs **Queues** stehen dem Nutzer zur freien Verfügung. Um die Prioritätsstufen der einzelnen **Queues** festzulegen werden sie in eine **Queue-List** nach absteigender Priorität verkettet. Die interne **Urgent-Queue** und **Best-Effort-Queue** werden an diese **Queue-List** vorne und hinten eingefügt. Die fertige **Queue-List** muss dann einem physischen **WAN-Interface** zugeordnet werden. Danach werden Pakete, die dieses **WAN-Interface** zum Ziel haben, auf Basis der konfigurierten **Queues** priorisiert.

QoS basiert darauf, dass die Bandbreiten bzw. Raten einer Schnittstelle bekannt sind, damit das QoS die korrekte Verteilung übernehmen kann, z. B. in dem Fall, dass prozentual Bandbreiten zugewiesen werden. Die Bandbreiten werden in der Regel aus der Upstream- bzw. Downstream-Datenrate aus den internen DSL-Modems übernommen oder aus der übermittelten Bandbreite im PPP durch den Provider.

Bei WAN-Verbindungen über externe Modems oder reine Ethernet-Verbindungen müssen die tatsächlichen Bandbreiten in der Tabelle **Schnittstellen > WAN > Interface-Einstellungen** bei **Downstream-Rate** sowie **Upstream-Rate** für das entsprechende Interface eingetragen werden.



Bitte beachten Sie, dass bestimmte eigene Pakete automatisch vom LCOS in die Urgent-Queue sortiert werden. Dazu zählen wichtige Verhandlungspakete wie IKEv2, BGP oder Keepalive-Pakete.

Darüber hinaus werden weitergeleitete TCP SYN- und ACK-Pakete bevorzugt behandelt und ebenfalls in die Urgent-Queue einsortiert. Das Verhalten kann konfiguriert werden unter **IP-Router > Allgemein > Routing-Optionen > TCP SYN- und ACK-Pakete bevorzugt weiterleiten**.

Die Konfiguration dieser **Queues** erfolgt in LANconfig unter **Firewall/QoS > QoS**.

In dieser Tabelle werden QoS-Queues und deren Parameter definiert.

Queues...

Zuvor erstellte Queues können hier zu Queue-Listen zusammengelegt werden.

Queue-Listen...

Verknüpfen Sie hier erzeugte Queue-Listen mit Schnittstellen.

Schnittstellen...

Hier werden die Grenzwerte für Paketstau-Fälle hinterlegt.

Paketstau-Aktion...

#### 7.1.1 Queues

In dieser Tabelle werden **Queue-Vorlagen** konfiguriert. Das bedeutet, dass nicht jeder Eintrag in dieser Tabelle auch eine Queue erzeugt. Eine **Queue** wird erst dann erzeugt, wenn sie in einer **Queue-List** verwendet und diese einem **WAN-Interface** zugeordnet wurde. Das bedeutet, dass auf Basis einer hier erstellten Vorlage beliebig viele oder auch keine **Queues** erzeugt werden können.

**Beispiel:** Wenn in diese Tabelle ein Eintrag mit Namen „Test“ angelegt wird und dieser Eintrag dann in zwei **Queue-List**-Objekten genutzt und diese zwei verschiedenen **WAN-Interfaces** zugeordnet werden, dann gibt es zwei **Queues** mit Namen „Test“, die aber voneinander völlig unabhängig sind.

Die Konfiguration der Queues und deren Parameter erfolgt in LANconfig unter **Firewall/QoS > QoS > Queues**.

### Name

Hier wird der Name der **Queue-Vorlage** eingetragen. Die Vorlage wird mit diesem Namen in anderen Tabellen referenziert. Der Name muss innerhalb der Tabelle eindeutig sein.

### Metrik-Typ

Hier wird die Metrik der Spalten **Commit-Rate** und **Excess-Rate** festgelegt.

### Commit-Rate

Hier wird eingetragen, wieviel Bandbreite dieser **Queue** zur Verfügung steht. Der Wert wird allgemein auch als CIR (Committed Information Rate) bezeichnet. Die Einheit der Eingabe wird in der Spalte **Metrik-Typ** festgelegt. Es gelten folgende Wertebereiche:

- > *Prozent:*  $1 < x < 100$
- > *KBit:*  $1 < x < 4294967295$
- > *MBit:*  $1 < x < 4294967295$

### Excess-Rate

Hier wird eingetragen, wieviel Bandbreite die **Queue** zusätzlich zu ihrer **Commit-Rate** nutzen darf. Der Wert wird allgemein auch als EIR (Excess Information Rate) bezeichnet. Damit höher priorisierte **Queues** sich nicht die **Commit-Rate** der niedriger priorisierten **Queues** nehmen können, wurde folgendes Konzept verwendet:

Das QoS operiert in Zeitscheiben, in denen jede **Queue** ihre **Commit-Rate** zur Verfügung hat. Am Ende der Zeitscheibe wird die nicht genutzte **Commit-Rate** aller **Queues** bestimmt und als Pool für die **Excess-Rate** in die nächste Zeitscheibe mitgenommen. Dieser Pool limitiert dann, wie viel Bandbreite mit der **Excess-Rate** genutzt werden darf. Damit sind zwei wichtige Punkte erfüllt, nämlich erstens wird die **Excess-Rate** einer Queue nicht von der aktuellen **Commit-Rate** einer anderen Queue genommen, sondern von der ungenutzten Rate der letzten Zeitscheibe. Zweitens wird der Pool für die **Excess-Rate** am Anfang jeder Zeitscheibe neu gesetzt und nicht aufaddiert, womit die ungenutzte **Commit-Rate** einer Zeitscheibe nur in der darauf folgenden

Zeitscheibe genutzt werden kann. Damit wird ein Ansparen verhindert, was dafür sorgen könnte, dass **Queues** mit konfigurierter Excess-Rate die niedriger priorisierten Queues aushungern lassen.

**Beispiel:** Es werden zwei **Queues** konfiguriert, in eine **Queue-List** verkettet und einem **WAN-Interface** zugewiesen. **Queue A** hat eine **Commit-Rate** von 10 MBit/s und eine **Excess-Rate** von 4 MBit/s. **Queue B** hat eine **Commit-Rate** von 5 MBit/s und eine **Excess-Rate** von 0. Wenn jetzt in Zeitscheibe 1 **Queue A** 9 MBit/s und **Queue B** 4 MBit/s nutzt, dann werden 2 MBit/s als ungenutzte Rate in den Pool der **Excess-Rate** für die Zeitscheibe 2 mitgenommen. In dieser Zeitscheibe könnte **Queue A** dann seine 10 MBit/s **Commit-Rate** und zusätzlich 2 MBit/s aus dem Pool im Rahmen seiner **Excess-Rate** nutzen. Wichtig ist, dass nur soviel **Excess-Rate** genutzt werden kann wie der Pool zur Verfügung stellt.

Die Einheit der Eingabe wird in der Spalte **Metrik-Typ** festgelegt. Es gelten folgende Wertebereiche:

- > *Prozent:*  $0 < x < 100$
- > *KBit:*  $0 < x < 4294967295$
- > *MBit:*  $0 < x < 4294967295$

### Rückfall auf Best Effort

Dieser Schalter bestimmt, was mit Paketen passiert, die weder im Rahmen der Commit-Rate noch Excess-Rate versendet werden können. Bei **Ja** werden die Pakete über die Best-Effort-Queue versendet, sonst verworfen.

### Paketstau-Aktion

Hier wird ein Objekt aus der Tabelle [Paketstau-Aktion](#) auf Seite 25 referenziert, welches bestimmt wann Pakete wegen voller werdender Sendequeues verworfen werden.

### DSCP-Tags

Hier werden die DSCP-Tags (Differentiated Services Code Point) eingetragen, die dieser Queue zugeordnet werden sollen. Es können mehrere Werte übergeben werden.

## 7.1.2 Queue-Listen

Die konfigurierten **Queue-Vorlagen** werden hier zu einer **Queue-Liste** verkettet. Dafür wird eine komma-separierte Liste verwendet, wobei die Reihenfolge die Priorisierung vorgibt, von hoch nach niedrig.

! Es ist bei der Erstellung einer **Queue-Liste** darauf zu achten, dass die **Commit-Raten** der **Queues** die Bandbreite des **WAN-Interfaces** nicht überbuchen. Ansonsten kann es zu einem Aushungern der niedrig priorisierten **Queues** kommen.

! Es ist außerdem darauf zu achten, dass **DSCP-Tags** nicht mehrfach zugewiesen werden. Sollte das passieren, wird implementierungsbedingt der niedrigst priorisierten **Queue** das Tag zugeordnet.

Zuvor erstellte Queues können in LANconfig unter **Firewall/QoS > QoS > Queue-Listen** zusammengelegt werden.

### Name

Mit diesem Namen wird die **Queue-Liste** in anderen Tabellen referenziert. Er muss innerhalb der Tabelle eindeutig sein.



### Best Effort Cong. Action

Hier kann eine **Paketstau-Aktion** aus der Paketstau-Aktion-Tabelle referenziert werden, um der **Best-Effort-Queue** eine **Paketstau-Aktion** zuzuweisen. Im Default wird der DEFAULT-Eintrag genutzt.

### Sortierte Liste

Hier wird eine komma-separierte Liste aus **Queue-Vorlagen** eingetragen, deren Priorisierung sich aus der Reihenfolge von hoch nach niedrig ergibt. Es können bis zu sechs eigene **Queue-Vorlagen** verkettet werden, da zwei Plätze für die interne **Urgent-Queue** und **Best-Effort-Queue** reserviert sind.

Beispiel für eine Liste: Gold, Silber, Bronze. Die Priorität der Queues beginnt mit Gold über Silber bis zu Bronze.

## 7.1.3 Schnittstellen

In LANconfig unter **Firewall/QoS > QoS > Schnittstellen** verknüpfen Sie Queue-Listen mit Schnittstellen.

### Schnittstellen

Hier wird der Name der physischen **WAN-Schnittstelle** eingetragen. Die Eingabe ist auf ein Inputset der auf dem Gerät verfügbaren **WAN-Schnittstellen** begrenzt.

### Eintrag aktiv

Hier wird das konfigurierte QoS auf der **WAN-Schnittstelle** ein- und ausgeschaltet.

### Maximale Burst-Größe

Die Maximum Burst Size (MBS) reguliert die Anzahl der Bytes, die in einem kurzen Zeitraum (Burst) gesendet werden können. Dieser Parameter gewährleistet, dass ein massiv oder kontinuierlich überbuchter Datenverkehr die verfügbaren Pufferressourcen, z. B. auf vorgeschalteten Provider-Routern, nicht vollständig ausschöpft. Der Defaultwert 0 bedeutet, dass das Betriebssystem den Parameter intern automatisch verwaltet. In der Regel entspricht der Wert intern der MTU der verwendeten WAN-Verbindung. Der Wert sollte auf die Vorgaben des Providers für den gebuchten Anschluss gesetzt werden.

### Queue-Liste

Referenziert einen Eintrag aus der Queue-Listen-Tabelle.

## 7.1.4 Paketstau-Aktion

Die Paketstau-Aktion bestimmt, wie mit einer sich anstauenden Sendequeue umgegangen wird. Da diese Queue nicht unbegrenzt lang werden kann, müssen ab einem Punkt Pakete verworfen werden. Dafür stehen zwei Mechanismen zur Verfügung: **Taildrop** und **Random Early Detection (RED)** oder auch als **Random Early Discard** bezeichnet. Bei Taildrop wird eine Grenze bestimmt, ab der alle weiteren eingehenden Pakete verworfen werden. Bei RED werden zwei Grenzen bestimmt. Ab der ersten werden Pakete mit einer Wahrscheinlichkeit P verworfen. P steigt dabei an, je näher man an die zweite Grenze kommt. Wenn die zweite Grenze überschritten wird, werden alle eingehenden Pakete verworfen, wie beim Taildrop.



Die Tabelle **Paketstau-Aktion** ist so definiert, dass darin sowohl **RED** als auch **Taildrop** passiv konfiguriert werden kann. Ein **Taildrop** wird daran erkannt, dass der **Grenzwert-Minimum** gleich **Grenzwert-Maximum** ist. **Max-Wahrscheinlichkeit** erfüllt bei einem **Taildrop** keinen Zweck, sollte aber mit 100 eingetragen werden, um zu definieren, dass oberhalb der Grenze alles verworfen wird.

Man gibt nur den **Metrik-Typ** und **Grenzwert-Minimum** an, die weiteren Werte werden passend so gesetzt, dass ein **Taildrop** konfiguriert wird.

Für ein **RED** ist **Grenzwert-Minimum** ungleich **Grenzwert-Maximum**. Ab **Grenzwert-Minimum** wird beginnend mit Wahrscheinlichkeit  $P=0$  das Paket verworfen, wobei sich  $P$  linear **Max-Wahrscheinlichkeit** annähert, je weiter man sich **Grenzwert-Max** annähert.

In LANconfig werden die Grenzwerte für Paketstau-Fälle unter **Firewall/QoS > QoS > Paketstau-Aktion** hinterlegt.

**Name**

Hier wird der Name der **Paketstau-Aktion** eingetragen, mit dem der Eintrag in anderen Tabellen referenziert wird. Der Name muss eindeutig innerhalb dieser Tabelle sein.

**Metrik-Typ**

Hier wird angegeben, welche Metrik die Werte in den Spalten **Commit-Rate** und **Excess-Rate** haben.

**Grenzwert-Minimum**

Gibt die untere Grenze der **Paketstau-Aktion** an.

**Grenzwert-Maximum**

Gibt die obere Grenze der **Paketstau-Aktion** an. Ab hier werden alle Pakete verworfen.

**Max.-Wahrscheinlichkeit**

Gibt die maximale Drop-Wahrscheinlichkeit bei einem konfigurierten **RED** an. Wird bei einem **Taildrop** ignoriert und sollte dort auf 100 gesetzt werden.

**7.1.5 Beispiel 1: Konfiguration eines QoS-Konzepts mit vier Klassen**

Im folgenden Beispiel soll ein Router für einen Kunden bereitgestellt werden, der dem Kunden am Anschluss ein QoS-Konzept mit vier QoS-Klassen ermöglicht. Die Klassen sind definiert als VoIP, Gold, Silber und Best Effort.

Jeder Serviceklasse wird 25% der Bandbreite zugeteilt. Der Kunde markiert seine Pakete per DSCP, so dass die Pakete der korrekten Queue im Router zugewiesen werden können.

Werden in der definierten Serviceklasse mehr Daten übertragen als Bandbreite vorhanden ist, so werden diese Daten verworfen. Ein Rückfall in die Serviceklasse Best Effort wird nicht erlaubt. Die Definition ist wie folgt:

Klasse	DSCP
VOIP	EF
Gold	CS3

Klasse	DSCP
Silber	CS2
Best Effort	0

1. Starten Sie LANconfig und öffnen Sie den Konfigurationsdialog für das Gerät.
2. Wechseln Sie in den Dialog **Firewall/QoS > QoS > Queues**.
3. Legen Sie die drei Vorlagen für die Serviceklassen VOIP, GOLD und SILBER an. Die Klasse Best Effort muss nicht manuell konfiguriert werden, da diese automatisch vorhanden ist.

Queues - Neuer Eintrag ? X

Name:

Metrik-Typ:

Commit-Rate:

Excess-Rate:

Rückfall auf Best Effort:

Paketstau-Aktion:

DSCP-Tags

<input type="checkbox"/> BE/CS0	<input type="checkbox"/> CS1
<input type="checkbox"/> CS2	<input type="checkbox"/> CS3
<input type="checkbox"/> CS4	<input type="checkbox"/> CS5
<input type="checkbox"/> CS6	<input type="checkbox"/> CS7
<input type="checkbox"/> AF11	<input type="checkbox"/> AF12
<input type="checkbox"/> AF13	<input type="checkbox"/> AF21
<input type="checkbox"/> AF22	<input type="checkbox"/> AF23
<input type="checkbox"/> AF31	<input type="checkbox"/> AF32
<input type="checkbox"/> AF33	<input type="checkbox"/> AF41
<input type="checkbox"/> AF42	<input type="checkbox"/> AF43
<input checked="" type="checkbox"/> EF	<input type="checkbox"/> Voice-Admit

Queues - Neuer Eintrag ? X

Name:

Metrik-Typ:

Commit-Rate:

Excess-Rate:

Rückfall auf Best Effort:

Paketstau-Aktion:

DSCP-Tags

<input type="checkbox"/> BE/CS0	<input type="checkbox"/> CS1
<input checked="" type="checkbox"/> CS2	<input type="checkbox"/> CS3
<input type="checkbox"/> CS4	<input type="checkbox"/> CS5
<input type="checkbox"/> CS6	<input type="checkbox"/> CS7
<input type="checkbox"/> AF11	<input type="checkbox"/> AF12
<input type="checkbox"/> AF13	<input type="checkbox"/> AF21
<input type="checkbox"/> AF22	<input type="checkbox"/> AF23
<input type="checkbox"/> AF31	<input type="checkbox"/> AF32
<input type="checkbox"/> AF33	<input type="checkbox"/> AF41
<input type="checkbox"/> AF42	<input type="checkbox"/> AF43
<input type="checkbox"/> EF	<input type="checkbox"/> Voice-Admit

7 Quality-of-Service

4. Wechseln Sie in den Dialog **Firewall/QoS > QoS > Queue-Listen**.
5. Legen Sie eine Liste an, mit der Sie eine strikte Reihenfolge für die angelegten Klassen vorgeben. Die erste Klasse in der Liste hat die höchste Priorität.

6. Als letztes muss die konfigurierte Liste einer WAN-Schnittstelle zugewiesen werden. In diesem Beispiel nehmen wir DSL. Wechseln Sie in den Dialog **Firewall/QoS > QoS > Schnittstellen**.

7. (Optional): Je nach verwendeter WAN-Schnittstelle muss noch die verfügbare Datenrate im Fall einer Ethernet-Verbindung konfiguriert werden. Dies ist nicht nötig, falls ein internes xDSL-Modem verwendet wird. In

diesem Fall wird die synchronisierte DSL-Datenrate verwendet. Wechseln Sie in den Dialog **Schnittstellen > WAN > Interface-Einstellungen**.

Die Paket-Statistiken und die Verteilung in die Queues können auf der CLI unter `/status/WAN/QoS/Statistik` abgerufen werden (hier gekürzte Darstellung):

```
root@:/
> ls /Status/WAN/QoS/Statistik/
```

Interface	Prioritaet	Queue-Name	Vorab-klassifiziert	DSCP-klassifiziert	Gesamt-klassifiziert
DSL-1	0	#urgent	0	0	0
DSL-1	1	VOIP	0	0	0
DSL-1	2	GOLD	0	0	0
DSL-1	3	SILBER	0	0	0
DSL-1	4	#best-effort	0	0	0

## 7.1.6 Beispiel 2: Konfiguration eines QoS-Konzepts am VDSL-Anschluss mit zwei QoS-Klassen

Im folgenden Beispiel soll ein Router für einen Kunden bereitgestellt werden, der dem Kunden am VDSL-Anschluss ein QoS-Konzept mit zwei QoS-Klassen ermöglicht. Die Klassen sind definiert als VoIP und Best Effort. Als Gerät wird ein Router mit internem xDSL-Modem verwendet.

Der Serviceklasse VoIP wird eine absolute Bandbreite von 10 Mbit/s zugewiesen. Der Kunde markiert seine Pakete per DSCP, so dass die Pakete der korrekten Queue im Router zugewiesen werden können.

Werden in der definierten Serviceklasse mehr Daten übertragen als Bandbreite vorhanden ist, so werden diese Daten der Klasse Best Effort zugewiesen. Die Definition ist wie folgt:

Klasse	DSCP
VOIP	EF

1. Starten Sie LANconfig und öffnen Sie den Konfigurationsdialog für das Gerät.
2. Wechseln Sie in den Dialog **Firewall/QoS > QoS > Queues**.

- Legen Sie die Vorlage für die Serviceklasse VOIP an. Die Klasse Best Effort muss nicht manuell konfiguriert werden, da diese automatisch vorhanden ist.

- Wechseln Sie in den Dialog **Firewall/QoS > QoS > Queue-Listen**.
- Legen Sie eine Liste an, mit der Sie eine strikte Reihenfolge für die angelegten Klassen vorgeben. Die erste Klasse in der Liste hat die höchste Priorität.

- Als letztes muss die konfigurierte Liste einer WAN-Schnittstelle zugewiesen werden. In diesem Beispiel nehmen wir DSL-1. Wechseln Sie in den Dialog **Firewall/QoS > QoS > Schnittstellen**.

Die Paket-Statistiken und die Verteilung in die Queues können auf der CLI unter `/status/WAN/QoS/Statistik` abgerufen werden (hier gekürzte Darstellung):

```

root@:/
> ls /Status/WAN/QoS/Statistik/

```

Interface	Prioritaet	Queue-Name	Vorab-klassifiziert	DSCP-klassifiziert	Gesamt-klassifiziert
DSL-1	0	#urgent	0	0	0
DSL-1	1	VOIP	0	0	0
DSL-1	2	#best-effort	0	0	0

## 7.1.7 Queue-Nutzung in der Firewall

In der Firewall ist es möglich, die im QoS konfigurierten Queues regelbasiert zuzuweisen. Diese Zuweisung ist unabhängig vom DSCP-Wert im IP-Header. Die Zuweisung erfolgt über Aktionen, die einer Regel zugewiesen werden. Wenn eine Regel mit einer solchen Aktion übereinstimmt und in der Firewall eine Session erzeugt wird, dann wird geprüft, ob dem Ziel- oder Quell-Interface der Session eine solche Queue zugewiesen wurde und die Zuweisung in der Aktion vermerkt. Wenn Daten über die Session laufen und die Aktion ausgeführt wird, wird das jeweilige Paket mit der Zuweisung markiert und wird dadurch vom DSCP-Classifer ignoriert und in der QoS-Statistik für die jeweilige Queue als „Pre-Classified“ gezählt.

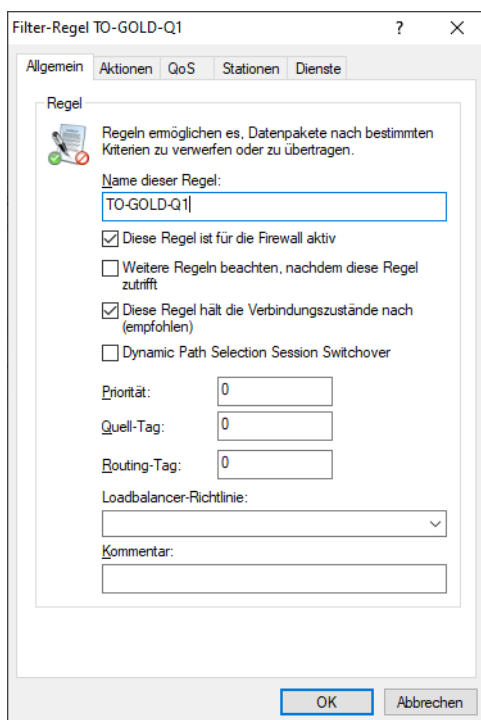
Die Queue-Zuweisung bezieht sich auf Queues, die physikalischen Interfaces zugewiesen wurden, wird aber auf darüber gestapelte Interfaces vererbt, d. h. wenn z. B. das Ziel-Interface einer Session ein VPN-Interface ist, dann propagiert sich die Queue-Zuweisung bis zum physikalischen Interface (WAN) durch und nutzt dieses dann zur Zuweisung.

Da sich die IPv4- und die IPv6-Firewall in ihrer Konfiguration unterscheiden, werden sie im Folgenden getrennt aufgeführt.

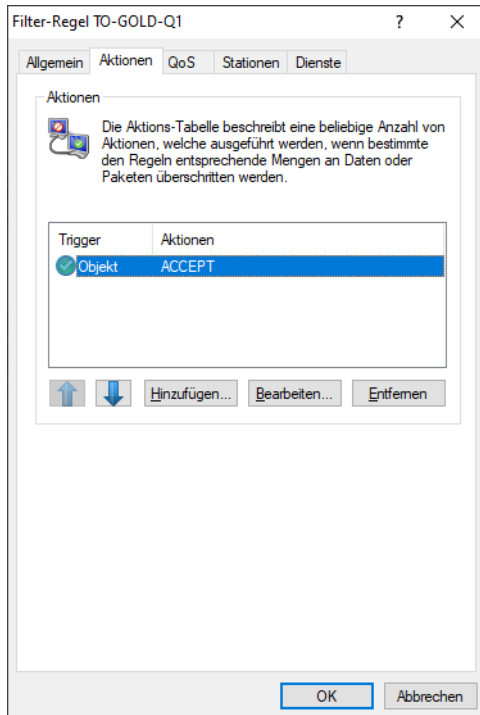
### IPv4-Firewall

Im Folgenden ein Beispiel für die Vorgehensweise für eine Queuezuweisung:

1. Eine Queuezuweisung erfolgt über eine Firewall-Regel, d. h. sie wird unter **Firewall/QoS > IPv4-Regeln > Firewall-Regeln (Filter/QoS) > Regeln** hinzugefügt. Als erstes geben Sie der Regel auf dem Reiter **Allgemein** einen Namen.

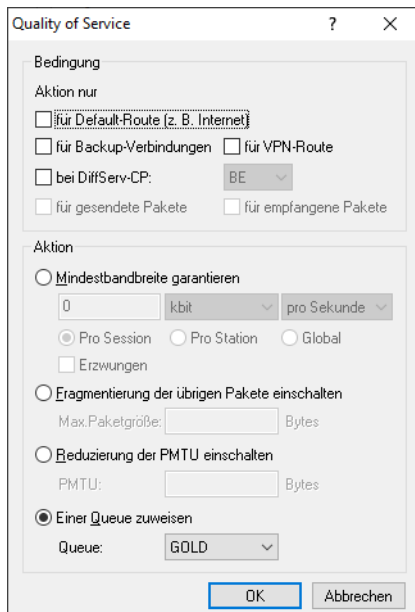


2. Danach fügen Sie auf dem Reiter **Aktionen** eine „ACCEPT“-Aktion hinzu und entfernen die voreingestellte „REJECT“-Aktion.



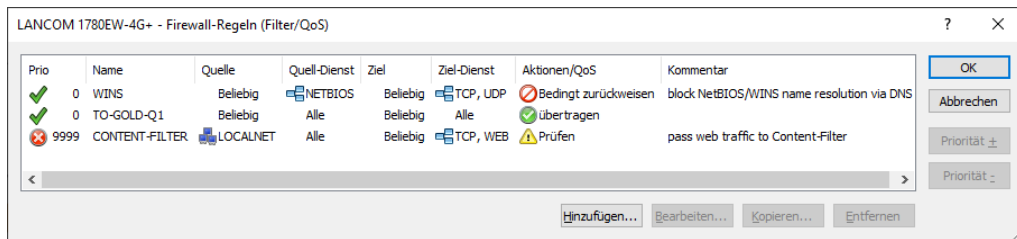
3. Als nächstes fügen Sie auf dem Reiter **QoS** ein neues QoS-Objekt an. Geben Sie diesem auf dem Reiter **Allgemein** einen Namen und weisen Sie dann auf dem Reiter **QoS** diesem die gewünschte Queue zu.

Die Aktion kann mit Bedingungen eingeschränkt werden, z. B. wenn die Zuweisung nur in einer bestimmten Richtung oder nur für einen bestimmten DSCP-Wert gelten soll.





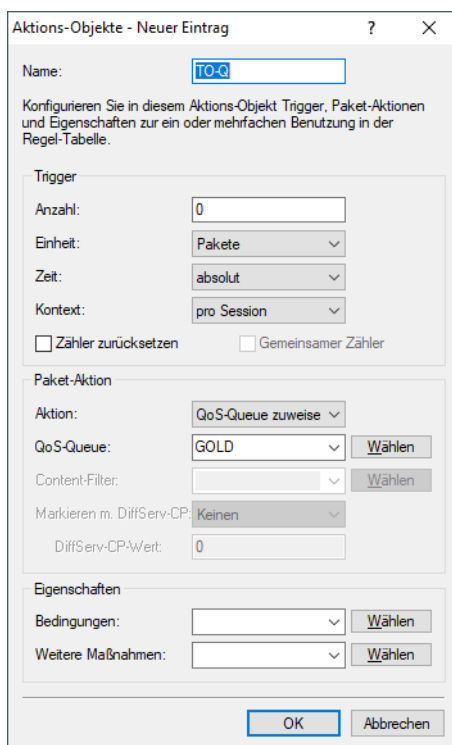
- Als Ergebnis erhalten Sie eine Regel, welche die gewünschten Pakete einer Queue – in diesem Beispiel „GOLD“ – zuweist.



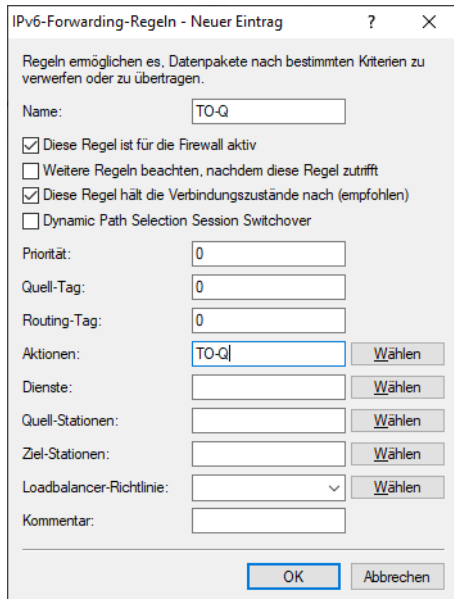
## IPv6-Firewall

Im Folgenden ein Beispiel für die Vorgehensweise für eine Queuezuweisung:

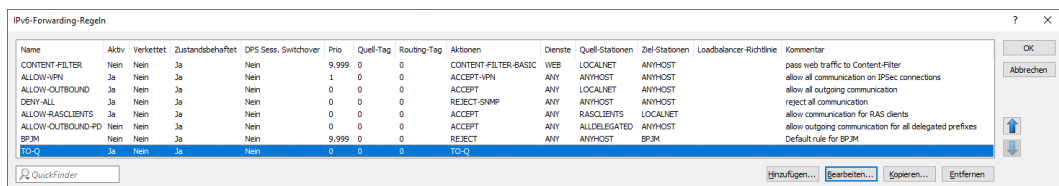
- Eine Queuezuweisung erfolgt über ein in einer IPv6-Forwarding-Regel zugewiesenes Aktions-Objekt. Legen Sie als erstes ein Aktions-Objekt unter **Firewall/QoS > IPv6-Regeln > Firewall-Objekte > Aktions-Objekte** an, in dem Sie die gewünschte Queue zuweisen.



- Danach erstellen Sie unter **Firewall/QoS > IPv6-Regeln > IPv6-Forwarding-Regeln** eine neue Regel, in der dieses Aktions-Objekt verwendet wird.



- Als Ergebnis erhalten Sie eine Regel, welche die gewünschten Pakete einer Queue – in diesem Beispiel „GOLD“ – zuweist.



## 7.1.8 Ergänzungen im Setup-Menü

### QoS

LCOS unterstützt bis zu acht verschiedene Queues (Serviceklassen) mit entsprechenden Prioritätsstufen für Anwendungen im Netzwerk wie z. B. „VoIP“, „Gold“, „Silber“ oder „Best Effort“. Datenpakete werden mithilfe von DSCP-Markierungen oder durch Firewallregeln der entsprechenden Quality of Service (QoS)-Klasse zugeordnet. Der Router sortiert anschließend die Pakete in die richtige Prioritätsstufe und stellt sicher, dass die entsprechenden Dienste nur so viel Upload-Bandbreite nutzen, wie für die Klasse zuvor in Prozent oder MBit/s konfiguriert wurden. Auf diese Weise wird sichergestellt, dass wichtige Dienste wie VoIP oder Videoanrufe stets ausreichend Bandbreite erhalten, selbst bei hoher Netzwerkauslastung.

Im Folgenden soll konzeptionell die Funktionsweise des Quality-of-Service mit acht Queues erklärt werden. Grundlegend sollen Pakete vom Router auf Basis des DSCP-Wertes im IP-Header priorisiert werden können. Hierfür stehen insgesamt acht **Queues** zur Verfügung, die strikt priorisiert werden. Das bedeutet, dass Pakete nach Verfügbarkeit von der **Queue** mit der höchsten Priorität bis zur **Queue** mit der niedrigsten Priorität versendet werden. Die Zuordnung eines Paketes zu einer **Queue** geschieht auf Basis des DSCP-Werts im IP-Header oder der Zuweisung zu einer Queue über eine Firewall-Regel. Von den acht zur Verfügung stehenden **Queues** sind zwei reserviert, einmal für die **Urgent-Queue** (höchste Priorität, für interne Dienste wie VCM und Protokollpakete) und zum anderen für die **Best-Effort-Queue** (niedrigste Priorität, für alle nicht-priorisierten Pakete). Die verbleibenden sechs **Queues** stehen dem Nutzer zur freien Verfügung. Um die Prioritätsstufen der einzelnen **Queues** festzulegen werden sie in eine **Queue-List** nach absteigender Priorität verkettet. Die interne **Urgent-Queue** und **Best-Effort-Queue** werden an diese **Queue-List** vorne und hinten eingefügt. Die fertige **Queue-List** muss dann einem physischen **WAN-Interface** zugeordnet werden. Danach werden Pakete, die dieses **WAN-Interface** zum Ziel haben, auf Basis der konfigurierten **Queues** priorisiert.

QoS basiert darauf, dass die Bandbreiten bzw. Raten einer Schnittstelle bekannt sind, damit das QoS die korrekte Verteilung übernehmen kann, z. B. in dem Fall, dass prozentual Bandbreiten zugewiesen werden. Die Bandbreiten werden in der Regel aus der Upstream- bzw. Downstream-Datenrate aus den internen DSL-Modems übernommen oder aus der übermittelten Bandbreite im PPP durch den Provider.

**SNMP-ID:**

2.2.71

**Pfad Konsole:****Setup > WAN****Paketstau-Aktion**

Die Paketstau-Aktion bestimmt, wie mit einer sich anstauenden Sendequelle umgegangen wird. Da diese Queue nicht unbegrenzt lang werden kann, müssen ab einem Punkt Pakete verworfen werden. Dafür stehen zwei Mechanismen zur Verfügung: **Taildrop** und **Random early detection (RED)** oder auch als **Random early discard** bezeichnet. Bei Taildrop wird eine Grenze bestimmt, ab der alle weiteren eingehenden Pakete verworfen werden. Bei RED werden zwei Grenzen bestimmt. Ab der ersten werden Pakete mit einer Wahrscheinlichkeit P verworfen. P steigt dabei an, je näher man an die zweite Grenze kommt. Wenn die zweite Grenze überschritten wird, werden alle eingehenden Pakete verworfen, wie beim Taildrop.



Die Tabelle **Paketstau-Aktion** ist so definiert, dass man darin sowohl **RED** als auch **Taildrop** konfigurieren kann. Diese Entscheidung sorgt einerseits für maximale Flexibilität, aber auch für ein hohes Fehlerpotential, eine nicht funktionsfähige Konfiguration zu erzeugen. Daher folgende Erklärung über die Rahmenbedingungen für beide Konzepte. Ein **Taildrop** wird daran erkannt, dass **Grenzwert-Min** gleich **Grenzwert-Max** ist. **Max-Wahrscheinlichkeit** erfüllt bei einem **Taildrop** keinen Zweck, sollte aber mit 100 eingetragen werden, um zu verstehen zu geben, dass oberhalb der Grenze alles verworfen wird. Damit ein Nutzer ein **Taildrop** möglichst einfach konfigurieren kann ist eine verkürzte Eingabe möglich:

```
root@:/Setup/WAN/QoS
> add Paketstau-Aktion/test bytes 20000
set ok:
Name           Metrik-Typ   Grenzwert-Min  Grenzwert-Max  Max-Wahrscheinlichkeit[%]
=====
TEST           Bytes        20000          20000          100
```

Man gibt nur den **Metrik-Typ** und **Grenzwert-Min** an, die weiteren Werte werden passend so gesetzt, dass ein **Taildrop** konfiguriert wird.

Für ein **RED** ist **Grenzwert-Min** ungleich **Grenzwert-Max**. Ab **Grenzwert-Min** wird beginnend mit Wahrscheinlichkeit P=0 das Paket verworfen, wobei sich P linear **Max-Wahrscheinlichkeit** annähert, je weiter man sich **Grenzwert-Max** annähert.

**SNMP-ID:**

2.2.71.1

**Pfad Konsole:****Setup > WAN > QoS****Name**

Hier wird der Name der **Paketstau-Aktion** eingetragen, mit dem der Eintrag in anderen Tabellen referenziert wird. Der Name muss eindeutig innerhalb dieser Tabelle sein.

**SNMP-ID:**

2.2.71.1.1

**Pfad Konsole:****Setup > WAN > QoS > Paketstau-Aktion****Mögliche Werte:**max. 20 Zeichen aus `[A-Z][0-9]@{ }~!$&'()*+,-./:;<=>?[\]^_.`**Metrik-Typ**

Hier wird angegeben, welche Metrik die Werte in den Spalten [2.2.71.1.3 Grenzwert-Min](#) auf Seite 36 und [2.2.71.1.4 Grenzwert-Max](#) auf Seite 36 haben

**SNMP-ID:**

2.2.71.1.2

**Pfad Konsole:****Setup > WAN > QoS > Paketstau-Aktion****Mögliche Werte:**

Frames  
Bytes  
KBytes

**Grenzwert-Min**

Gibt die untere Grenze der **Paketstau-Aktion** an.

**SNMP-ID:**

2.2.71.1.3

**Pfad Konsole:****Setup > WAN > QoS > Paketstau-Aktion****Mögliche Werte:**max. 10 Zeichen aus `[0-9]`**Grenzwert-Max**

Gibt die obere Grenze der **Paketstau-Aktion** an. Ab hier werden alle Pakete verworfen.

**SNMP-ID:**

2.2.71.1.4

**Pfad Konsole:**

Setup > WAN > QoS > Paketstau-Aktion

**Mögliche Werte:**

max. 10 Zeichen aus [0-9]

**Max-Wahrscheinlichkeit-Prozent**

Gibt die maximale Drop-Wahrscheinlichkeit bei einem konfigurierten **RED** an. Wird bei einem **Taildrop** ignoriert und sollte dort auf 100 gesetzt werden.

**SNMP-ID:**

2.2.71.1.5

**Pfad Konsole:**

Setup > WAN > QoS > Paketstau-Aktion

**Mögliche Werte:**

0 ... 100

**Queues**

In dieser Tabelle werden **Queue-Vorlagen** konfiguriert. Das bedeutet, dass nicht jeder Eintrag in dieser Tabelle auch eine Queue erzeugt. Eine **Queue** wird erst dann erzeugt, wenn sie in einer **Queue-List** verwendet und diese einem **WAN-Interface** zugeordnet wurde. Das bedeutet, dass auf Basis einer hier erstellten Vorlage beliebig viele oder auch keine **Queues** erzeugt werden können.

**Beispiel:** Wenn in diese Tabelle ein Eintrag mit Namen „Test“ angelegt wird und dieser Eintrag dann in zwei **Queue-List**-Objekten genutzt und diese zwei verschiedenen **WAN-Interfaces** zugeordnet werden, dann gibt es zwei **Queues** mit Namen „Test“, die aber voneinander völlig unabhängig sind.

**SNMP-ID:**

2.2.71.2

**Pfad Konsole:**

Setup > WAN > QoS

**Name**

Hier wird der Name der **Queue-Vorlage** eingetragen. Die Vorlage wird mit diesem Namen in anderen Tabellen referenziert. Der Name muss innerhalb der Tabelle eindeutig sein.

**SNMP-ID:**

2.2.71.2.1

**Pfad Konsole:**

Setup > WAN > QoS > Queues

**Mögliche Werte:**

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

**Metrik-Typ**

Hier wird die Metrik der Spalten [2.2.71.2.3 Commit-Rate](#) auf Seite 38 und [2.2.71.2.4 Excess-Rate](#) auf Seite 39 festgelegt.

**SNMP-ID:**

2.2.71.2.2

**Pfad Konsole:**

**Setup > WAN > QoS > Queues**

**Mögliche Werte:****Prozent**

Die Rate wird als Prozentwert angegeben. Grundwert der Berechnung ist die auf dem WAN-Interface verfügbare Bandbreite.

**KBit**

Die Rate wird nominell in Kilobit pro Sekunde angegeben.

**MBit**

Die Rate wird nominell in Megabit pro Sekunde angegeben.

**Commit-Rate**

Hier wird eingetragen, wieviel Bandbreite dieser **Queue** zur Verfügung steht. Der Wert wird allgemein auch als CIR (Committed Information Rate) bezeichnet. Die Einheit der Eingabe wird in der Spalte [2.2.71.2.2 Metrik-Typ](#) auf Seite 38 festgelegt. Es gelten folgende Wertebereiche:

- > *Prozent*:  $1 < x < 100$
- > *KBit*:  $1 < x < 4294967295$
- > *MBit*:  $1 < x < 4294967295$

**SNMP-ID:**

2.2.71.2.3

**Pfad Konsole:**

**Setup > WAN > QoS > Queues**

**Mögliche Werte:**

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

**Excess-Rate**

Hier wird eingetragen, wieviel Bandbreite die **Queue** zusätzlich zu ihrer **Commit-Rate** nutzen darf. Der Wert wird allgemein auch als EIR (Excess Information Rate) bezeichnet. Damit höher priorisierte **Queues** sich nicht die **Commit-Rate** der niedriger priorisierten **Queues** nehmen können, wurde folgendes Konzept verwendet:

Das QoS operiert in Zeitscheiben, in denen jede **Queue** ihre **Commit-Rate** zur Verfügung hat. Am Ende der Zeitscheibe wird die nicht genutzte **Commit-Rate** aller **Queues** bestimmt und als Pool für die **Excess-Rate** in die nächste Zeitscheibe mitgenommen. Dieser Pool limitiert dann, wie ivel Bandbreite mit der **Excess-Rate** genutzt werden darf. Damit sind zwei wichtige Punkte erfüllt, nämlich erstens wird die **Excess-Rate** einer Queue nicht von der aktuellen **Commit-Rate** einer anderen Queue genommen, sondern von der ungenutzten Rate der letzten Zeitscheibe. Zweitens wird der Pool für die **Excess-Rate** am Anfang jeder Zeitscheibe neu gesetzt und nicht aufaddiert, womit die ungenutzte **Commit-Rate** einer Zeitscheibe nur in der darauf folgenden Zeitscheibe genutzt werden kann. Damit wird ein Ansparen verhindert, was dafür sorgen könnte, dass **Queues** mit konfigurierter Excess-Rate die niedriger priorisierten Queues aushungern lassen.

**Beispiel:** Es werden zwei **Queues** konfiguriert, in eine **Queue-List** verkettet und einem **WAN-Interface** zugewiesen. **Queue A** hat eine **Commit-Rate** von 10 MBit/s und eine **Excess-Rate** von 4 MBit/s. **Queue B** hat eine **Commit-Rate** von 5 MBit/s und eine **Excess-Rate** von 0. Wenn jetzt in Zeitscheibe 1 **Queue A** 9 MBit/s und **Queue B** 4 MBit/s nutzt, dann werden 2 MBit/s als ungenutzte Rate in den Pool der **Excess-Rate** für die Zeitscheibe 2 mitgenommen. In dieser Zeitscheibe könnte **Queue A** dann seine 10 MBit/s **Commit-Rate** und zusätzlich 2 MBit/s aus dem Pool im Rahmen seiner **Excess-Rate** nutzen. Wichtig ist, dass nur soviel **Excess-Rate** genutzt werden kann wie der Pool zur Verfügung stellt.

Die Einheit der Eingabe wird in der Spalte [2.2.71.2.2 Metrik-Typ](#) auf Seite 38 festgelegt. Es gelten folgende Wertebereiche:

- > *Prozent:*  $0 < x < 100$
- > *KBit:*  $0 < x < 4294967295$
- > *MBit:*  $0 < x < 4294967295$

**SNMP-ID:**

2.2.71.2.4

**Pfad Konsole:**

Setup &gt; WAN &gt; QoS &gt; Queues

**Mögliche Werte:**

max. 10 Zeichen aus [0-9]

**Rueckfall-auf-Best-Effort**

Dieser Schalter bestimmt, was mit Paketen passiert, die weder im Rahmen der Commit-Rate noch Excess-Rate versendet werden können.

**SNMP-ID:**

2.2.71.2.5

**Pfad Konsole:**

Setup &gt; WAN &gt; QoS &gt; Queues

**Mögliche Werte:****Ja**

Die Pakete werden über die Best-Effort-Queue versendet.

**Nein**

Die Pakete werden verworfen.

**Paketstau-Aktion**

Hier wird ein Objekt aus der Tabelle [2.2.71.1 Paketstau-Aktion](#) auf Seite 35 referenziert, welches bestimmt wann Pakete wegen voller werdender Sendequeres verworfen werden.

**SNMP-ID:**

2.2.71.2.6

**Pfad Konsole:**

**Setup > WAN > QoS > Queues**

**DSCP-Tags**

Hier wedern die DSCP-Tags (Differentiated Services Code Point) eingetragen, die dieser Queue zugeordnet werden sollen. Es können mehrere Werte mit einer komma-separierten Liste übergeben werden.

**SNMP-ID:**

2.2.71.2.7

**Pfad Konsole:**

**Setup > WAN > QoS > Queues**





**Mögliche Werte:**

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

**Queue-Liste**

Die konfigurierten **Queue-Vorlagen** werden hier zu einer **Queue-Liste** verkettet. Dafür wird eine komma-separierte Liste verwendet, wobei die Reihenfolge die Priorisierung vorgibt, von hoch nach niedrig.

- 
-  Es ist bei der Erstellung einer **Queue-Liste** darauf zu achten, dass die **Commit-Raten** der **Queues** die Bandbreite des **WAN-Interfaces** nicht überbuchen. Ansonsten kann es zu einem Aushungern der niedrig priorisierten **Queues** kommen.
- 
-  Es ist außerdem darauf zu achten, dass **DSCP-Tags** nicht mehrfach zugewiesen werden. Sollte das passieren, wird implementierungsbedingt der niedrigst priorisierten **Queue** das Tag zugeordnet.

**SNMP-ID:**

2.2.71.3

**Pfad Konsole:**

Setup > WAN > QoS

**Name**

Mit diesem Namen wird die **Queue-Liste** in anderen Tabellen referenziert. Er muss innerhalb der Tabelle eindeutig sein.

**SNMP-ID:**

2.2.71.3.1

**Pfad Konsole:**

**Setup > WAN > QoS > Queue-Liste**

**Mögliche Werte:**

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

**Best-Effort-Paketstau-Aktion**

Hier kann eine **Paketstau-Aktion** aus der Paketstau-Aktion-Tabelle referenziert werden, um der **Best-Effort-Queue** eine **Paketstau-Aktion** zuzuweisen. Im Default wird der DEFAULT-Eintrag genutzt.

**SNMP-ID:**

2.2.71.3.2

**Pfad Konsole:**

**Setup > WAN > QoS > Queue-Liste**

**Mögliche Werte:**

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

**Sortierte-Liste**

Hier wird eine komma-separierte Liste aus **Queue-Vorlagen** eingetragen, deren Priorisierung sich aus der Reihenfolge von hoch nach niedrig ergibt. Es können bis zu sechs eigene **Queue-Vorlagen** verkettet werden, da zwei Plätze für die interne **Urgent-Queue** und **Best-Effort-Queue** reserviert sind.

Beispiel für eine Liste: Gold, Silber, Bronze. Die Priorität der Queues beginnt mit Gold über Silber bis zu Bronze.

**SNMP-ID:**

2.2.71.3.3

**Pfad Konsole:**

**Setup > WAN > QoS > Queue-Liste**

**Mögliche Werte:**

max. 120 Zeichen aus `[A-Z][0-9]@{|}~!$&'()+-./:;<=>?[\]^_.`

**Interfaces**

Hier werden konfigurierte **Queue-Listen WAN-Interfaces** zugeordnet.

**SNMP-ID:**

2.2.71.4

**Pfad Konsole:**

**Setup > WAN > QoS**

**Interface**

Hier wird der Name des physischen **WAN-Interfaces** eingetragen. Die Eingabe ist auf ein Inputset der auf dem Gerät verfügbaren **WAN-Interfaces** begrenzt.

**SNMP-ID:**

2.2.71.4.1

**Pfad Konsole:****Setup > WAN > QoS > Interfaces****Aktiv**

Hier wird das konfigurierte QoS auf dem **WAN-Interface** ein- und ausgeschaltet.

**SNMP-ID:**

2.2.71.4.2

**Pfad Konsole:****Setup > WAN > QoS > Interfaces****Mögliche Werte:****Ja**  
**Nein****Queue-Liste**

Referenziert einen Eintrag aus der Queue-List-Tabelle.

**SNMP-ID:**

2.2.71.4.3

**Pfad Konsole:****Setup > WAN > QoS > Interfaces****Mögliche Werte:**max. 20 Zeichen aus `[A-Z][0-9]@{|}~!$&'()*+,-./:;<=>?[\]^_.`**Maximale-Burst-Groesse**

Die Maximum Burst Size (MBS) reguliert die Anzahl der Bytes, die in einem kurzen Zeitraum (Burst) gesendet werden können. Dieser Parameter gewährleistet, dass ein massiv oder kontinuierlich überbuchter Datenverkehr die verfügbaren Pufferressourcen, z. B. auf vorgeschalteten Provider-Routern, nicht vollständig ausschöpft. Der Wert sollte auf die Vorgaben des Providers für den gebuchten Anschluss gesetzt werden.

**SNMP-ID:**

2.2.71.4.4

**Pfad Konsole:**

**Setup > WAN > QoS > Interfaces**

**Mögliche Werte:**

max. 5 Zeichen aus [0-9]

**Default-Wert:**

0

**Besondere Werte:**

**0**

Der Defaultwert 0 bedeutet, dass das Betriebssystem den Parameter intern automatisch verwaltet. In der Regel entspricht der Wert intern der MTU der verwendeten WAN-Verbindung.

## 8 Virtual Private Networks – VPN

### 8.1 MOBIKE

Ab LCOS 10.90 gibt es die neuen Parameter **MOBIKE** und **MOBIKE-Cookie-Challenge** in der Tabelle **VPN > IKEv2/IPSec > VPN-Verbindungen > Verbindungs-Parameter**.

Verbindungs-Parameter - Eintrag bearbeiten	
Name:	DEFAULT
Dead Peer Detection:	30 Sekunden
Encapsulation:	Keine
Ziel-Port:	0
MOBIKE:	Ja
MOBIKE-Cookie-Challenge:	Nein
<input type="button" value="OK"/> <input type="button" value="Abbrechen"/>	

#### MOBIKE

Definiert, ob MOBIKE nach [RFC 4555](#) unterstützt werden soll.

MOBIKE nach RFC 4555 für IKEv2 bietet mobilen Clients die Möglichkeit, zwischen verschiedenen Netzen zu roamen und dabei den VPN-Tunnel nicht abbauen zu müssen. Ein VPN-Client kann beispielsweise nahtlos vom Mobilfunk ins WLAN roamen und dabei wird seine externe IP-Adresse auf dem VPN-Gateway durch eine IKEv2-Update-Nachricht aktualisiert. Der Vorteil ist, dass der VPN-Tunnel bzw. die Security Associations (SAs) nicht abgebaut und wieder neu aufgebaut werden muss.

MOBIKE wird nur als Responder-Rolle unterstützt, d. h. wenn VPN-Clients Verbindungen zum LANCOM VPN-Router aufbauen. Der Aufbau von VPN-Tunneln mit MOBIKE-Erweiterung wird nicht unterstützt.

#### MOBIKE-Cookie-Challenge

Definiert, ob das Gerät eine Cookie-Challenge senden soll um festzustellen, ob der VPN-Client auch unter der neuen Adresse tatsächlich Pakete empfangen kann („Return Routability Check“).

### 8.1.1 Ergänzungen im Setup-Menü

#### MOBIKE

Definiert, ob MOBIKE nach [RFC 4555](#) unterstützt werden soll.

MOBIKE nach RFC 4555 für IKEv2 bietet mobilen Clients die Möglichkeit, zwischen verschiedenen Netzen zu roamen und dabei den VPN-Tunnel nicht abbauen zu müssen. Ein VPN-Client kann beispielsweise nahtlos vom Mobilfunk ins WLAN roamen und dabei wird seine externe IP-Adresse auf dem VPN-Gateway durch eine IKEv2-Update-Nachricht aktualisiert. Der Vorteil ist, dass der VPN-Tunnel bzw. die Security Associations (SAs) nicht abgebaut und wieder neu aufgebaut werden muss.

MOBIKE wird nur als Responder-Rolle unterstützt, d. h. wenn VPN-Clients Verbindungen zum LANCOM VPN-Router aufbauen. Der Aufbau von VPN-Tunneln mit MOBIKE-Erweiterung wird nicht unterstützt.

**SNMP-ID:**

2.19.36.4.9

**Pfad Konsole:****Setup > VPN > IKEv2 > Allgemeines****Mögliche Werte:****Ja**

MOBIKE wird unterstützt.

**Nein**

MOBIKE wird nicht unterstützt.

**Default-Wert:**

Ja

**MOBIKE-Cookie-Challenge**

Definiert, ob das Gerät eine Cookie-Challenge senden soll um festzustellen, ob der VPN-Client auch unter der neuen Adresse tatsächlich Pakete empfangen kann („Return Routability Check“).

**SNMP-ID:**

2.19.36.4.10

**Pfad Konsole:****Setup > VPN > IKEv2 > Allgemeines****Mögliche Werte:****Ja**

MOBIKE-Cookie-Challenge wird gesendet.

**Nein**

MOBIKE-Cookie-Challenge wird nicht gesendet.

**Default-Wert:**

Nein

## 8.2 IKEv2 Post-quantum Preshared Keys (PPK)

Quantencomputer stellen eine mögliche Herausforderung für aktuelle kryptografische Algorithmen dar, wie sie beispielsweise im IKEv2 VPN verwendet werden. Aktuelle Algorithmen gelten nach heutigem Stand als sehr robust, aber es besteht die Herausforderung, dass ein Angreifer heute verschlüsselte Daten aufzeichnen kann und diese mit Quantencomputern in der Zukunft entschlüsseln könnte.

Das [RFC 8784](#) „Mixing Preshared Keys in the Internet Key Exchange Protocol Version 2 (IKEv2) for Post-quantum Security“ bietet eine Möglichkeit, resistent gegen Quantencomputer zu sein, wenn Passwörter (PSKs) verwendet werden. Die

Erweiterung besteht darin, dass in das standardmäßig verwendete IKEv2 Passwort-Verfahren (PSK) ein weiterer Schlüssel in Form eines Post-quantum Preshared Key (PPK) „gemixt“ wird, um die Resistenz zu erhöhen.

Bestehende IKEv2-PSK-Tunnel können einfach um PPKs ergänzt werden. Der PPK ist unabhängig vom bereits vorhandenen PSK.

LCOS unterstützt die manuelle Konfiguration von PPKs. Automatische Verfahren zur Änderung bzw. Wechsel von PPKs werden nicht unterstützt.

### Tabelle VPN > IKEv2/IPSec > Authentifizierung

Authentifizierung - Neuer Eintrag

Name:

Lokale Authentifizierung: PSK

Lokales Dig. Signature-Profil:  Wählen

Lokaler Identitätstyp: Keine Identität

Lokale Identität:

Lokales Passwort:   Anzeigen  
Passwort erzeugen

Entfernte Authentifizierung: PSK

Entf. Dig. Signature-Profil:  Wählen

PPK-ID:  Wählen

EAP-Profil:  Wählen

Entfernter Identitätstyp: Keine Identität

Entfernte Identität:

Entferntes Passwort:   Anzeigen  
Passwort erzeugen

Weitere entf. Identitäten:  Wählen

Lokales Zertifikat:

Entfernter Zert.-ID-Check: Nein

OCSP-Überprüfung: Nein

CRL Check: Ja

OK Abbrechen

### PPK-ID

Geben Sie hier den Namen der PPK-ID (Post-quantum Preshared Keys nach [RFC 8784](#)) aus der Tabelle der PPKs ein.

**Tabelle VPN > IKEv2/IPSec > Erweiterte Einstellungen > Authentifizierung > Identitäten**

**PPK-ID**

Geben Sie hier den Namen der PPK-ID (Post-quantum Preshared Keys nach [RFC 8784](#)) ein aus der Tabelle der PPKs.

**Tabelle VPN > IKEv2/IPSec > Erweiterte Einstellungen > Authentifizierung > PPKs**

**PPK-ID**

Vergeben Sie einen eindeutigen Namen für diesen Eintrag. Eingabeformat ist möglich als Zeichenkette oder Hexadezimalzahl (identifiziert durch ein führendes 0x).

**PPK**

Vergeben Sie hier den Post-quantum Preshared Key als Zeichenkette oder Hexadezimalzahl (identifiziert durch ein führendes 0x).

**Erforderlich**

Wird die Verwendung von PPKs als erforderlich konfiguriert, so wird die entsprechende VPN-Verbindung abgelehnt, falls die Gegenseite kein PPK unterstützt oder konfiguriert hat. Wird die Verwendung von PPKs als optional konfiguriert, so werden sowohl Verbindungen mit PPK als auch ohne PPK akzeptiert.

**RADIUS-Attribute**

Analog dazu werden auch entsprechende RADIUS-Attribute unterstützt:

ID	Bezeichnung	Bedeutung
LANCOM 33	LCS-IKEv2-PPK	Gibt den Post-quantum Preshared Key als Zeichenkette oder Hexadezimalzahl (identifiziert durch ein führendes 0x) an.



ID	Bezeichnung	Bedeutung
LANCOM 34	LCS-IKEv2-PPK-MANDATORY	Gibt an, ob die Verwendung des übergebenen Post-quantum Preshared Key (PPK) gefordert wird. Falls ja, dann wird die entsprechende VPN-Verbindung abgelehnt, falls die Gegenseite kein PPK unterstützt oder konfiguriert hat. Wird die Verwendung von PPKs als optional konfiguriert, so werden sowohl Verbindungen mit PPK als auch ohne PPK akzeptiert.

## 8.2.1 Ergänzungen im Setup-Menü

### PPK-ID

Referenziert einen [PPK](#).

### SNMP-ID:

2.19.36.3.1.18

### Pfad Konsole:

Setup > VPN > IKEv2 > Auth > Parameter

### Mögliche Werte:

max. 66 Zeichen aus `[A-Z][a-z][0-9]@{|}~!$%&'()+,-./:;<=>?[\]^_`~`

### Default-Wert:

leer

### PPK-ID

Referenziert einen [PPK](#).

### SNMP-ID:

2.19.36.3.3.11

### Pfad Konsole:

Setup > VPN > IKEv2 > Auth > Addit.-Remote-IDs

### Mögliche Werte:

max. 66 Zeichen aus `[A-Z][a-z][0-9]@{|}~!$%&'()+,-./:;<=>?[\]^_`~`

### Default-Wert:

leer

## PPKs

Quantencomputer stellen eine mögliche Herausforderung für aktuelle kryptografische Algorithmen dar, wie sie beispielsweise im IKEv2 VPN verwendet werden. Aktuelle Algorithmen gelten nach heutigem Stand als sehr robust, aber es besteht die Herausforderung, dass ein Angreifer heute verschlüsselte Daten aufzeichnen kann und diese mit Quantencomputern in der Zukunft entschlüsseln könnte.

Das [RFC 8784](#) „Mixing Preshared Keys in the Internet Key Exchange Protocol Version 2 (IKEv2) for Post-quantum Security“ bietet eine Möglichkeit, resistent gegen Quantencomputer zu sein, wenn Passwörter (PSKs) verwendet werden. Die Erweiterung besteht darin, dass in das standardmäßig verwendete IKEv2 Passwort-Verfahren (PSK) ein weiterer Schlüssel in Form eines Post-quantum Preshared Key (PPK) „gemixt“ wird, um die Resistenz zu erhöhen.

Bestehende IKEv2-PSK-Tunnel können einfach um PPKs ergänzt werden. Der PPK ist unabhängig vom bereits vorhandenen PSK.

LCOS unterstützt die manuelle Konfiguration von PPKs. Automatische Verfahren zur Änderung bzw. Wechsel von PPKs werden nicht unterstützt.

In dieser Tabelle konfigurieren Sie die PPKs.

**SNMP-ID:**

2.19.36.3.6

**Pfad Konsole:**

**Setup > VPN > IKEv2**

**PPK-ID**

Vergeben Sie einen eindeutigen Namen für diesen Eintrag. Eingabeformat ist möglich als Zeichenkette oder Hexadezimalzahl (identifiziert durch ein führendes 0x).

**SNMP-ID:**

2.19.36.3.6.1

**Pfad Konsole:**

**Setup > VPN > IKEv2 > PPKs**

**Mögliche Werte:**

max. 66 Zeichen aus `[A-Z][a-z][0-9]@{|}~!$%&'()*+,-./:;<=>?[\]^_`~`

**Default-Wert:**

*leer*

**PPK**

Vergeben Sie hier den Post-quantum Preshared Key als Zeichenkette oder Hexadezimalzahl (identifiziert durch ein führendes 0x).

**SNMP-ID:**

2.19.36.3.6.2

**Pfad Konsole:**

**Setup > VPN > IKEv2 > PPKs**

**Mögliche Werte:**

max. 66 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+,-./:;<=>?[\]^_`~`

**Default-Wert:***leer***Erforderlich**

Wird die Verwendung von PPKs als erforderlich konfiguriert, so wird die entsprechende VPN-Verbindung abgelehnt, falls die Gegenseite kein PPK unterstützt oder konfiguriert hat. Wird die Verwendung von PPKs als optional konfiguriert, so werden sowohl Verbindungen mit PPK als auch ohne PPK akzeptiert.

**SNMP-ID:**

2.19.36.3.6.3

**Pfad Konsole:****Setup > VPN > IKEv2 > PPKs****Mögliche Werte:**

nein

ja

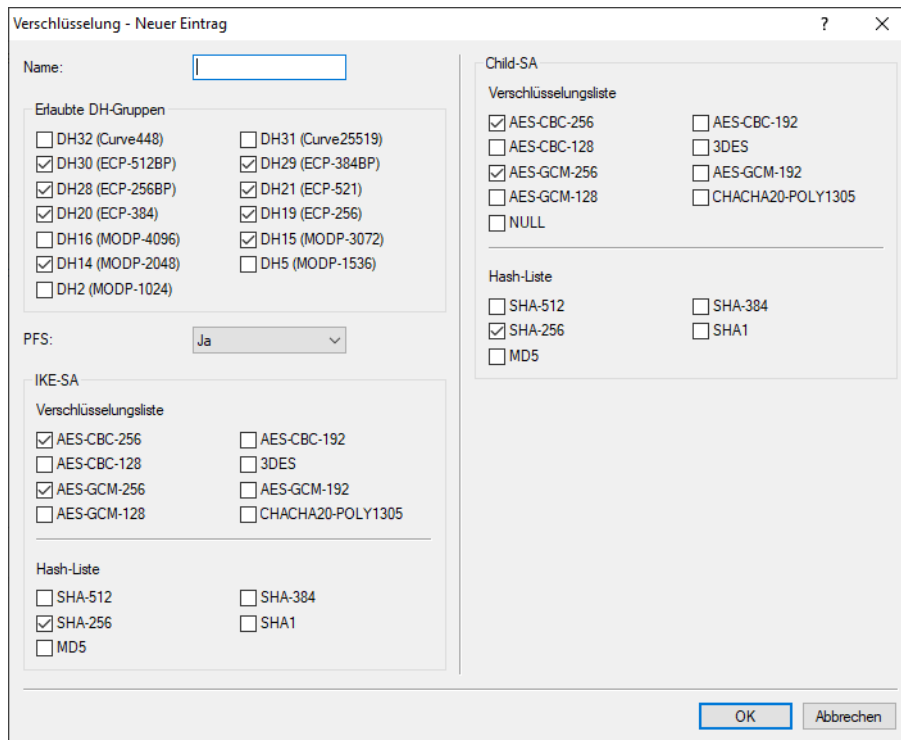
**Default-Wert:**

nein

## 8.3 Null-Verschlüsselung in der IKEv2 Child-SA

Ab LCOS 10.90 wird die Null-Verschlüsselung in der IKEv2 Child-SA unterstützt. Dabei ist zu beachten, dass keine Verschlüsselung der Datenpakete mehr erfolgt. Diese Funktion wird nur in speziellen Szenarien benötigt und generell nicht empfohlen.

Dazu wurde in LANconfig unter **VPN > IKEv2 / IPSec > Verschlüsselung** die Verschlüsselungsliste erweitert.



**Verschlüsselungsliste**

> NULL



Hier erfolgt keine Verschlüsselung der Datenpakete mehr. Diese Funktion wird nur in speziellen Szenarien benötigt und generell nicht empfohlen.

**8.3.1 Ergänzungen im Setup-Menü**

**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.

**NULL**

Hier erfolgt keine Verschlüsselung der Datenpakete mehr. Diese Funktion wird nur in speziellen Szenarien benötigt und generell nicht empfohlen.

**Default-Wert:**

AES-CBC-256

AES-GCM-256

## 8.4 IKE-CFG schickt Subnetzmaske für die verhandelte IP-Adresse mit

Ab LCOS 10.90 kann die Netzmaske (IPv4) bzw. Präfix-Länge (IPv6) für die Adressen angegeben werden, welche den Clients zugewiesen werden.

Dazu wurden in LANconfig unter **VPN > IKEv2 / IPSec > IPv4-Adressen** bzw. **VPN > IKEv2 / IPSec > IPv6-Adressen** die folgenden Parameter ergänzt.

IPv4-Adressen - Neuer Eintrag

Name:

Adress-Pool

Erste Adresse:

Letzte Adresse:

Nameserver-Adressen

Erster DNS:

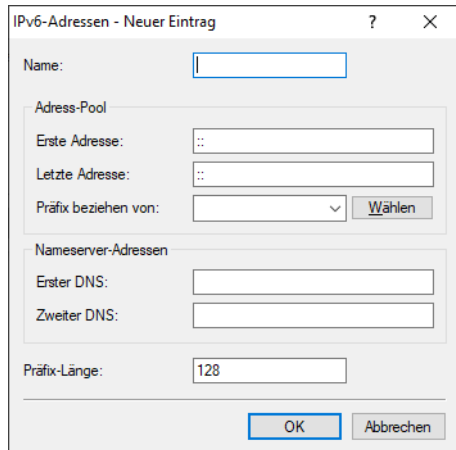
Zweiter DNS:

Netzmaske:

OK Abbrechen

**Netzmaske**

Optionale Netzmaske, die für die verhandelte IP-Adresse mitgeschickt wird.



**Präfix-Länge**

Optionale Präfix-Länge, die für die verhandelte IP-Adresse mitgeschickt wird.

Analog dazu werden auch entsprechende RADIUS-Attribute unterstützt:

ID	Bezeichnung	Bedeutung
9	Framed-IP-Netmask	Gibt die IP-Netzmaske an, die für den Client zu konfigurieren ist (im IKE-CFG-Mode „Server“). Dieser Attributwert führt dazu, dass eine statische Route für die Framed-IP-Adresse mit der angegebenen Maske hinzugefügt wird.
LANCOM 32	LCS-IPv6-Prefix-Length	Gibt die IPv6-Präfix-Länge an, die für den Client zu konfigurieren ist (im IKE-CFG-Mode „Server“).

**8.4.1 Ergänzungen im Setup-Menü**

**Netzmaske**

Optionale Netzmaske, die für die verhandelte IP-Adresse mitgeschickt wird.

**SNMP-ID:**

2.19.36.7.1.5

**Pfad Konsole:**

Setup > VPN > IKEv2 > IKE-CFG > IPv4

**Mögliche Werte:**

max. 3 Zeichen aus [0-9]

**Default-Wert:**

leer

## Praefix-Laenge

Optionale Präfix-Länge, die für die verhandelte IP-Adresse mitgeschickt wird.

### SNMP-ID:

2.19.36.7.2.7

### Pfad Konsole:

Setup > VPN > IKEv2 > IKE-CFG > IPv6

### Mögliche Werte:

max. 3 Zeichen aus [0–9]

### Default-Wert:

128

## 8.5 VLB IPv6-Support

Ab LCOS 10.90 unterstützt der IKEv2 Load Balancer zur VPN-Tunnel-Lastverteilung auf zentralseitigen Geräten IPv6 zusammen mit VRRPv3. Dazu gibt es die folgenden neuen Parameter in LANconfig unter **VPN > IKEv2 / IPsec > IKEv2 Load Balancer > Load Balancer > Instanzen**.

### VLB-Schnittstelle

Definiert die Schnittstelle bzw. das logische Netzwerk auf dem der IKEv2-Loadbalancer VPN-Tunnel annehmen soll. Auf dieser Schnittstelle muss ebenfalls VRRP konfiguriert bzw. aktiv sein.

### VLB-ID

Definiert die eindeutige Kennung der Load-Balancer-Instanz. Default: 1

### Lokales IPv6 Weiterleitungsziel

Globale IPv6-Adresse oder FQDN, auf dem das Gerät VPN-Tunnel annehmen soll. Auf diese Adresse wird ein VPN-Client durch den Master im Load-Balancer-Verbund weitergeleitet. Link-Lokale Adressen werden nicht unterstützt.




Hierbei handelt es sich nicht um die virtuelle VRRP-IP-Adresse.

## 8.5.1 Ergänzungen im Setup-Menü

### Eigenes-IPv6-Umleitungsziel

Globale IPv6-Adresse oder FQDN, auf dem das Gerät VPN-Tunnel annehmen soll. Auf diese Adresse wird ein VPN-Client durch den Master im Load-Balancer-Verbund weitergeleitet. Link-Lokale Adressen werden nicht unterstützt.

 Hierbei handelt es sich nicht um die virtuelle VRRP-IP-Adresse.

#### SNMP-ID:

2.19.50.2.3

#### Pfad Konsole:

Setup > VPN > Lastverteilung > Instanzen

#### Mögliche Werte:

max. 63 Zeichen aus `[A-Z][a-z][0-9].-:;%?`

### VLB-Schnittstelle

Definiert die Schnittstelle bzw. das logische Netzwerk auf dem der IKEv2-Loadbalancer VPN-Tunnel annehmen soll. Auf dieser Schnittstelle muss ebenfalls VRRP konfiguriert bzw. aktiv sein.

#### SNMP-ID:

2.19.50.2.8

#### Pfad Konsole:

Setup > VPN > Lastverteilung > Instanzen

#### Mögliche Werte:

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

### VLB-ID

Definiert die eindeutige Kennung der Load-Balancer-Instanz.

#### SNMP-ID:

2.19.50.2.9

#### Pfad Konsole:

Setup > VPN > Lastverteilung > Instanzen

#### Mögliche Werte:

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



**Default-Wert:**

1

# 9 WLAN-Management

## 9.1 WLAN-Management mit Wi-Fi 7

Ab LCOS 10.90 unterstützt das WLAN-Management Wi-Fi 7 Access Points wie den LANCOM LX-7300 und LANCOM LX-7500. Daher sind diese nun im **Firmware-Management** unter **WLAN-Controller > AP-Update > Access-Point Firmware- und Skriptmanagement** auswählbar. Ebenso wurde bei den Modi Wi-Fi 7 (IEEE 802.11be) hinzugefügt. Außerdem 320 MHz als mögliche maximale Bandbreite für das 3. Modul.

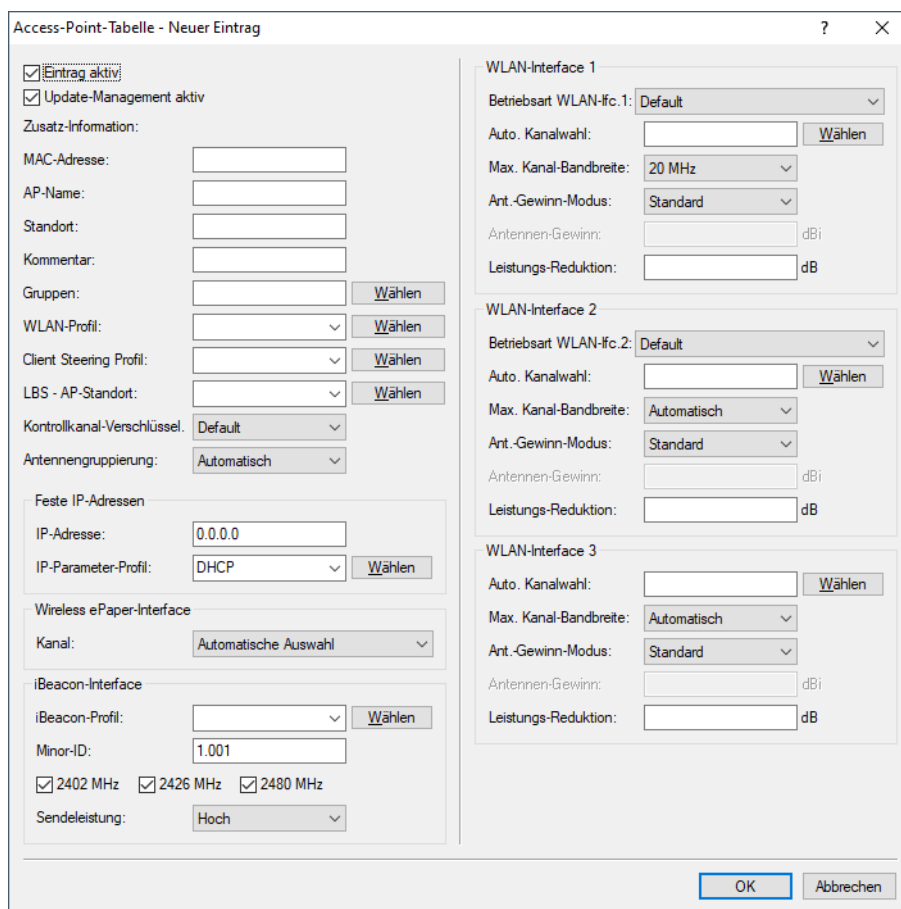


Abbildung 1: WLAN-Controller > AP-Konfiguration > Access-Point-Tabelle

### 9.1.1 Ergänzungen im Setup-Menü

#### 2.4GHz-Modus

Geben Sie an, welche(n) Funkstandard(s) die von Ihnen konfigurierte physikalische WLAN-Schnittstelle gegenüber einem WLAN-Client im 2,4-GHz-Frequenzband unterstützt. Je nach Gerätetyp und gewähltem Frequenzband haben Sie die Möglichkeit, einen AP exklusiv in einem bestimmten Modus zu betreiben oder einen der verschiedenen Kompatibilitätsmodi einzustellen.

- ⓘ Beachten Sie, dass WLAN-Clients, die lediglich einen langsameren Standard unterstützen, sich nicht mehr in Ihrem WLAN anmelden können, wenn Sie den Modus auf einen zu hohen Wert einstellen. Die Kompatibilität geht jedoch immer zu Lasten der Performance. Erlauben Sie daher ausschließlich jene Betriebsarten, die aufgrund der vorhandenen WLAN-Clients unbedingt erforderlich sind.

**SNMP-ID:**

2.37.1.2.6

**Pfad Konsole:**

Setup &gt; WLAN-Management &gt; AP-Konfiguration &gt; Radioprofile

**Mögliche Werte:****11bg-gemischt**

802.11g/b (gemischt)

**nur-11b**

Nur 802.11b (11Mbit)

**nur-11g**

Nur 802.11g (54Mbit)

**108Mbps**

802.11g++ (108MBit/s-Modus / Turbo-Modus)

**11bgn-gemischt**

802.11g/b/n

**11gn-gemischt**

802.11g/n

**Greenfield**

Nur 802.11n (Greenfield-Modus)

**11bgnax-gemischt**

802.11g/b/n/ax

**11gnax-gemischt**

802.11g/n/ax

**11bgnaxbe-gemischt**

802.11g/b/n/ax/be

**11gnaxbe-gemischt**

802.11g/n/ax/be

**Auto**

Automatisch. Innerhalb des 2,4-GHz-Modus führt die Automatik entweder zu **11bgn-gemischt** oder zu **11bg-gemischt**.

**Default-Wert:**

Auto

**5GHz-Modus**

Geben Sie an, welche(n) Funkstandard(s) die von Ihnen konfigurierte physikalische WLAN-Schnittstelle gegenüber einem WLAN-Client im 5-GHz-Frequenzband unterstützt. Je nach Gerätetyp und gewähltem Frequenzband haben Sie die

Möglichkeit, einen AP exklusiv in einem bestimmten Modus zu betreiben oder einen der verschiedenen Kompatibilitätsmodi einzustellen.

! Beachten Sie, dass WLAN-Clients, die lediglich einen langsameren Standard unterstützen, sich nicht mehr in Ihrem WLAN anmelden können, wenn Sie den Modus auf einen zu hohen Wert einstellen. Die Kompatibilität geht jedoch immer zu Lasten der Performance. Erlauben Sie daher ausschließlich jene Betriebsarten, die aufgrund der vorhandenen WLAN-Clients unbedingt erforderlich sind.

**SNMP-ID:**

2.37.1.2.7

**Pfad Konsole:****Setup > WLAN-Management > AP-Konfiguration > Radioprofile****Mögliche Werte:****normal**

802.11g (54Mbit/s-Modus)

**108Mbps**

802.11g++ (108MBit/s-Modus / Turbo-Modus)

**11an-gemischt**

802.11a/n (gemischt)

**Greenfield**

Nur 802.11n (Greenfield-Modus)

**11anac-gemischt**

802.11a/n/ac (gemischt)

**11nac-gemischt**

802.11n/ac (gemischt)

**nur-11ac**

Nur 802.11ac

**11anacax-gemischt**

802.11a/n/ac/ax (gemischt)

**11anacaxbe-gemischt**

802.11a/n/ac/ax/be (gemischt)

**Auto**

Automatisch. Innerhalb des 5-GHz-Modus führt die Automatik entweder zu **11anac-gemischt**, **11an-gemischt** oder **normal**.

**Default-Wert:**

Auto

**6GHz-Modus**

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

**SNMP-ID:**

2.37.1.2.27

**Pfad Konsole:****Setup > WLAN-Management > AP-Konfiguration > Radioprofile****Mögliche Werte:****11axbe-gemischt**

802.11ax/be

**Auto**

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

**Default-Wert:**

Auto

**Modul-2-Max.-Kanal-Bandbreite**

Geben Sie an, wie und in welchem Umfang der AP die Kanal-Bandbreite für die 2. physikalische WLAN-Schnittstelle festlegt.

Standardmäßig bestimmt die physikalische WLAN-Schnittstelle den Frequenzbereich, in dem die zu übertragenen Daten auf die Trägersignale aufmoduliert werden, automatisch. 802.11a/b/g nutzen 48 Trägersignale in einem 20 MHz-Kanal. Durch die Nutzung des doppelten Frequenzbereiches von 40 MHz können 96 Trägersignale eingesetzt werden, was zu einer Verdoppelung des Datendurchsatzes führt.

802.11n kann in einem 20 MHz-Kanal 52, in einem 40 MHz-Kanal sogar 108 Trägersignale zur Modulation nutzen. Für 802.11n bedeutet die Nutzung der 40 MHz-Option also einen Performance-Gewinn auf mehr als das Doppelte.

**SNMP-ID:**

2.37.1.4.25

**Pfad Konsole:****Setup > WLAN-Management > AP-Konfiguration > Basisstationen****Mögliche Werte:****Automatisch**

Der AP erkennt automatisch die maximale Kanal-Bandbreite.

**20MHz**

Der AP benutzt auf 20MHz gebündelte Kanäle.

**40MHz**

Der AP benutzt auf 40MHz gebündelte Kanäle.

**80MHz**

Der AP benutzt auf 80MHz gebündelte Kanäle.

**80+80MHz**

Der AP benutzt zwei auf 80 MHz gebündelte Kanäle.

**160MHz**

Der AP benutzt auf 160 MHz gebündelte Kanäle.

**Default-Wert:**

Automatisch

**Modul-1-Max.-Kanal-Bandbreite**

Geben Sie an, wie und in welchem Umfang der AP die Kanal-Bandbreite für die 1. physikalische WLAN-Schnittstelle festlegt.

Standardmäßig bestimmt die physikalische WLAN-Schnittstelle den Frequenzbereich, in dem die zu übertragene Daten auf die Trägersignale aufmoduliert werden, automatisch. 802.11a/b/g nutzen 48 Trägersignale in einem 20 MHz-Kanal. Durch die Nutzung des doppelten Frequenzbereiches von 40 MHz können 96 Trägersignale eingesetzt werden, was zu einer Verdoppelung des Datendurchsatzes führt.

802.11n kann in einem 20 MHz-Kanal 52, in einem 40 MHz-Kanal sogar 108 Trägersignale zur Modulation nutzen. Für 802.11n bedeutet die Nutzung der 40 MHz-Option also einen Performance-Gewinn auf mehr als das Doppelte.

**SNMP-ID:**

2.37.1.4.26

**Pfad Konsole:****Setup > WLAN-Management > AP-Konfiguration > Basisstationen****Mögliche Werte:****Automatisch**

Der AP erkennt automatisch die maximale Kanal-Bandbreite.

**20MHz**

Der AP benutzt auf 20MHz gebündelte Kanäle.

**40MHz**

Der AP benutzt auf 40MHz gebündelte Kanäle.

**80MHz**

Der AP benutzt auf 80MHz gebündelte Kanäle.

**80+80MHz**

Der AP benutzt zwei auf 80 MHz gebündelte Kanäle.

**160MHz**

Der AP benutzt auf 160 MHz gebündelte Kanäle.

**Default-Wert:**

Automatisch

**Modul-3-Max.-Kanal-Bandbreite**

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

**SNMP-ID:**

2.37.1.4.40

**Pfad Konsole:****Setup > WLAN-Management > AP-Konfiguration > Basisstationen****Mögliche Werte:****Auto**

Der AP erkennt automatisch die maximale Kanal-Bandbreite.

**20MHz**

Der AP benutzt auf 20 MHz gebündelte Kanäle.

**40MHz**

Der AP benutzt auf 40 MHz gebündelte Kanäle.

**80MHz**

Der AP benutzt auf 80 MHz gebündelte Kanäle.

**80+80MHz**

Der AP benutzt zwei auf 80 MHz gebündelte Kanäle.

**160MHz**

Der AP benutzt auf 160 MHz gebündelte Kanäle.

**320MHz**

Der AP benutzt auf 320 MHz gebündelte Kanäle.

**Default-Wert:**

Auto

# 10 Public Spot

## 10.1 Public Spot Captive Portal API

Ab LCOS 10.90 unterstützt der Public Spot den neuen Standard der Captive Portal API nach [RFC 8908](#). Der Standard erlaubt es WLAN-Clients, in einem Hotspot ein Captive Portal bzw. eine Login-Seite automatisch zu finden.

Der Client erhält per DHCP die URL der Portal-Seite und kann dann per API-Anfrage an den Hotspot prüfen, ob ein Login erforderlich ist oder der Zugriff für den Client schon erlaubt ist. Das beschleunigt die Benutzererfahrung in einem Hotspot deutlich und stellt durch die Definition eines Standards nun eine bessere Herstellerinteroperabilität zwischen Hotspot und Clients her.

Folgende Schritte sind dazu erforderlich:

1. Die Verwendung von TLS-Zertifikaten im Public Spot ist zwingend erforderlich. Ohne HTTPS-Login stellt der Client an das Portal keine Anfrage.
2. Der DHCP-Server muss die Captive Portal DHCP-Option an den Client ausliefern.

Die Konfiguration finden Sie in LANconfig unter **Public-Spot > Server > Captive Portal API (RFC 8908)**.

Captive Portal API (RFC 8909)

Captive Portal API aktiviert

Benutzerportal-URL:

Venue-URL:

### Captive Portal API aktiviert

Aktiviert bzw. deaktiviert die Funktion der Captive Portal API im Public Spot.

### Benutzerportal-URL

(Optional) Die Captive Portal API unterstützt laut Standard nur die Betriebsart über TLS. Deshalb muss das Gerät über ein vertrauenswürdigen Zertifikat sowie einen DNS-Namen verfügen. Im Default kann der Parameter leer gelassen werden und wird automatisch vom System eingefügt. Dazu muss der Gerätenamen in den Public Spot Betriebseinstellungen konfiguriert werden und mit dem TLS-Zertifikat übereinstimmen. Wird ein externer Hotspot-Server verwendet, kann auch eine URL des externen Servers eingetragen werden. Als weitere Voraussetzung gilt, dass die Clients im Hotspot das Captive Portal per DHCP-Option finden müssen. Dazu muss die entsprechende DHCP-Option nach [RFC 8910](#) für das Hotspot-Netzwerk konfiguriert werden.

### Venue-URL

(Optional) URL (TLS), über die der Betreiber dem Benutzer zusätzliche Informationen über die Lokation des Hotspots bereitstellen kann, z. B. die Webseite des Hotels des Hotspots.

### DHCPv4-Option konfigurieren(laut RFC 8910)

Legen Sie in LANconfig einen neuen Tabelleneintrag unter **IPv4 > DHCPv4 > DHCP-Optionen** an.

#### Options-Nummer

Nummer der Option, die an die DHCP-Clients übermittelt werden soll. Hier 114.

#### Netzwerkname

Name des Public Spot-Netzwerks (siehe IPv4-Netzwerke)



**Typ**

Typ des Eintrags. Hier Zeichenkette.

**Wert**

HTTPS-URL des LANCOM Routers im Hotspot, z. B. „https://hotspot.org/captive-portal-api“. Der DNS-Name, z. B. „hotspot.org“, ist der Gerätenamen des Routers im TLS-Zertifikat ergänzt um den internen Pfad der Public Spot Login-Seite „captive-portal-api“. Der DNS-Name muss durch den Hotspot-Clients auflösbar sein. Ebenso muss der Gerätenamen in den Public Spot-Betriebseinstellungen konfiguriert werden und mit dem TLS-Zertifikat übereinstimmen.

DHCP-Optionen - Neuer Eintrag

Options-Nummer: 114

Sub-Options-Nummer: 0

Vendor-Class-Maske:

User-Class-Maske:

Netzwerkname: HOTSPO

Typ: Zeichenkette

Wert: https://hotspot.org/capt

Sub-Option anhängen: Nein

**DHCPv6-Option konfigurieren (laut RFC8910)**

Legen Sie in LANconfig einen neuen Tabelleneintrag unter **IPv6 > DHCPv6 > DHCPv6-Server > Weitere Optionen** an.

**Interface-Name / Relay-IP**

Name des Public Spot Netzwerks (siehe IPv6-Netzwerke)

**Optionscode**

103

**Optionstyp**

String

**Optionswert**

HTTPS-URL des LANCOM Routers im Hotspot, z. B. „https://hotspot.org/captive-portal-api“. Der DNS-Name, z. B. „hotspot.org“, ist der Gerätenamen des Routers im TLS-Zertifikat ergänzt um den internen Pfad der Public Spot Login-Seite „captive-portal-api“. Der DNS-Name muss durch den Hotspot-Clients auflösbar sein. Ebenso muss der Gerätenamen in den Public Spot-Betriebseinstellungen konfiguriert werden und mit dem TLS-Zertifikat übereinstimmen.

Weitere Optionen - Eintrag bearbeiten

Interface-Name/Relay-IP: HOTSPO

Optionscode: 103

Optionstyp: String

Optionswert: https://hotspot.org/capt

## 10.1.1 Ergänzungen im Setup-Menü

### Api-Server

Der Public Spot unterstützt den neuen Standard der Captive Portal API nach [RFC 8908](#). Der Standard erlaubt es WLAN-Clients in einem Hotspot ein Captive Portal bzw. eine Login-Seite automatisch zu finden.

Der Client erhält per DHCP die URL der Portal-Seite und kann dann per API-Anfrage an den Hotspot prüfen, ob ein Login erforderlich ist oder der Zugriff für den Client schon erlaubt ist. Das beschleunigt die Benutzererfahrung in einem Hotspot deutlich und stellt durch die Definition eines Standards nun eine bessere Herstellerinteroperabilität zwischen Hotspot und Clients her.

Folgende Schritte sind dazu erforderlich:

1. Die Verwendung von TLS-Zertifikaten im Public Spot ist zwingend erforderlich. Ohne HTTPS-Login stellt der Client an das Portal keine Anfrage.
2. Der DHCP-Server muss die Captive Portal DHCP-Option an den Client ausliefern.

#### SNMP-ID:

2.24.63

#### Pfad Konsole:

**Setup > Public-Spot-Modul**

#### Aktiv

Aktiviert bzw. deaktiviert die Funktion der Captive Portal API im Public Spot.

#### SNMP-ID:

2.24.63.1

#### Pfad Konsole:

**Setup > Public-Spot-Modul > Api-Server**

#### Mögliche Werte:

nein  
ja

#### Default-Wert:

nein

### User-Portal-URL

(Optional) Die Captive Portal API unterstützt laut Standard nur die Betriebsart über TLS. Deshalb muss das Gerät über ein vertrauenswürdiges Zertifikat sowie einen DNS-Namen verfügen. Im Default kann der Parameter leer gelassen werden und wird automatisch vom System eingefügt. Dazu muss der Gerätenamen in den Public Spot Betriebseinstellungen konfiguriert werden und mit dem TLS-Zertifikat übereinstimmen. Wird ein externer Hotspot-Server verwendet, kann auch eine URL des externen Servers eingetragen werden. Als weitere Voraussetzung gilt, dass die Clients im Hotspot das

Captive Portal per DHCP-Option finden müssen. Dazu muss die entsprechende DHCP-Option nach [RFC 8910](#) für das Hotspot-Netzwerk konfiguriert werden.

**SNMP-ID:**

2.24.63.2

**Pfad Konsole:****Setup > Public-Spot-Modul > Api-Server****Mögliche Werte:**

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

**Default-Wert:***leer***Venue-Info-URL**

(Optional) URL (TLS), über die der Betreiber dem Benutzer zusätzliche Informationen über die Lokation des Hotspots bereitstellen kann, z. B. die Webseite des Hotels des Hotspots.

**SNMP-ID:**

2.24.63.3

**Pfad Konsole:****Setup > Public-Spot-Modul > Api-Server****Mögliche Werte:**

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

**Default-Wert:***leer*

# 11 Backup-Lösungen

## 11.1 VRRPv3

Ab LCOS 10.90 wird das Virtual Router Redundancy Protocol Version 3 (VRRPv3) unterstützt.

Dabei wurde die Konfiguration auf der Kommandozeile von **Setup > IP-Router > VRRP** nach **Setup > VRRP** verschoben.

### 11.1.1 Interaktion mit dem WAN-Backup-Modul


Das VRRP-Modul ist eng an das WAN-Backup-Modul angebunden, um eine Interaktion der beiden Funktionalitäten zu ermöglichen. Grundsätzlich passiert die Interaktion in beide Richtungen: Das VRRP kann einerseits abhängig vom Zustand der virtuellen Router den Aufbau von WAN-Verbindungen anfordern oder unterbinden, und andererseits kann der Verbindungszustand einer WAN-Verbindung (aufgebaut/Backup/abgebaut) einen Einfluss darauf haben, welche Priorität die virtuellen Router verwenden.

Ein virtueller Router im VRRP interagiert dabei mit maximal einer WAN-Verbindung (und ihren Backup-Verbindungen), und zwar genau dann, wenn der Name der WAN-Verbindung in der Spalte **Überwachte Gegenstelle** in der Konfigurationstabelle **Virtuelle Router** eingetragen ist. Ist dort für einen virtuellen Router kein Eintrag vorhanden, interagiert dieser Router nicht mit dem WAN-Backup-Modul.

### 11.1.2 Steuerung des WAN/WAN-Backup durch das VRRP

Wenn virtuelle Router, die ein WAN-Interface überwachen, existieren, und keiner von diesen im Zustand „Master“ ist, fordert das VRRP einen Verbindungsabbau des überwachten WAN an, und unterbindet einen Wiederaufbau. Sobald einer der Router den Zustand zu Master wechselt, wird der Verbindungsaufbau freigegeben und ein Verbindungsversuch gestartet. Da WAN-Verbindungen für IPv4 und IPv6 gemeinsam auf- und abgebaut werden, spielt hierbei die IP-Version der virtuellen Router keine Rolle. Generell gilt: Wenn der VRRP-Schalter **VRRP aktiviert** nicht eingeschaltet wurde, dann findet keinerlei Beeinflussung des WAN-Backup-Moduls durch das VRRP statt.

---

 Beachten Sie hier auch den Schalter **Setup > VRRP > WAN-Verbindungskontrolle** (2.141.7).


### 11.1.3 Konfiguration von VRRPv3

LCOS unterstützt VRRPv2 und VRRPv3 ([RFC 5798](#) sowie [RFC 9568](#)) für IPv4 und IPv6.

---

 VRRP mit IPv6 funktioniert nur mit statischen Adressen oder Network Prefix Translation (NPTv6) in Richtung des Internetproviders.

---

 VRRP arbeitet für IPv4 und IPv6 jeweils unabhängig, auch wenn es gemeinsam in einer Zeile konfiguriert wurde. Dies ist sogar empfehlenswert, damit das Advert.-Intervall und die Prioritäten konsistent sind.

Die Einstellungen für das VRRP finden Sie in LANconfig unter **IP-Router > VRRP**.

Kommandozeile: **Setup > VRRP**

Zur Konfiguration von Ausfallsicherung (Router-Redundanz) oder Load-Balancing über VRRP können folgende Parameter eingestellt werden:

**VRRP aktiviert**

Mit diesem Schalter lässt sich das VRRP-Modul ein- und ausschalten (Default: Aus).

**Virtuelle Router**

In der Tabelle Virtuelle Router können die virtuellen Router pro Interface definiert werden.

**Interface**

Logisches IPv4- oder IPv6-Interface bzw. Netzwerk, auf dem VRRP aktiviert werden soll. Grundsätzlich sind nur LAN-Interfaces sinnvoll. Andere Schnittstellen lassen sich zwar auswählen, führen aber zu einem undefinierten Verhalten.

**Router-ID**

Eindeutige ID des virtuellen Routers. Es sind Werte zwischen 1 und 255 möglich. Mit der Router-ID werden mehrere physikalische Router zu einem virtuellen Router bzw. einer Standby-Gruppe zusammengefasst. Manchmal wird die Router-ID auch VRRP-ID oder kurz VRID genannt.

**Aktiviert**

Aktiviert oder deaktiviert VRRP für diesen Konfigurationseintrag.

**Version**

Definiert welche VRRP-Version verwendet werden soll. Es werden VRRPv2, VRRPv3 oder VRRPv2 und VRRPv3 unterstützt. IPv6 wird nur bei VRRPv3 unterstützt. IPv4 wird sowohl bei VRRPv2 als auch bei VRRPv3 unterstützt.

Der Modus v2+v3 ist als Übergangslösung für die Transition von einem VRRPv2- zu einem VRRPv3-Betrieb unter IPv4 gedacht und sorgt für ein verdoppeltes Paketaufkommen, da ein so konfigurierter Virtueller Router Advertisements in beiden Protokollversionen versendet.

Ein Virtueller Router, der auf eine Protokollversion konfiguriert wurde, verwirft Advertisements anderer Router, wenn sie die falsche Protokollversion haben, und gibt eine Ausgabe auf dem VRRP-Packet Trace aus und trägt einen zugehörigen Eintrag in die Event-Log-Tabelle ein.

### **Priorität**

Gibt die Priorität an, mit der der Virtuelle Router arbeitet. Diese wird in den Advertisements übertragen und bestimmt maßgeblich, welches Gerät der zuständige Master für eine VRRP-Verbindung ist. Die angegebene Priorität muss größer als 0 sein. Der Wert 255 hat eine Sonderbedeutung:

- Der Wert 255 wird automatisch eingestellt, wenn die Adresse des virtuellen Routers gleich der Adresse des Interfaces ist, an das der Router gebunden ist. In allen anderen Fällen wird die Priorität automatisch herabgesetzt.

### **Backup-Priorität**

Die Backup-Priorität des virtuellen Routers bezieht sich auf das Interface, für das eine Backup-Verbindung konfiguriert ist, also z. B. bei Routern mit DSL- und Mobilfunk-Unterstützung auf das Mobilfunk-Interface. Es sind Werte zwischen 0 und der konfigurierten Priorität zulässig. Der Wert 0 hat eine Sonderbedeutung:

- 0 deaktiviert den virtuellen Router im Backup-Fall. Es wird in regelmäßigen Abständen geprüft, ob die Hauptverbindung wieder aufgebaut werden kann. Das Prüf-Intervall wird im Reconnect-Delay festgelegt.

Wenn im Backup-Fall auch die Backup-Verbindung nicht aufgebaut werden kann meldet sich der virtuelle Router vollständig ab und versucht ebenfalls in, über die Reconnect-Verzögerung angegebenen, Intervallen entweder die Haupt- oder die Backup-Verbindung erneut aufzubauen.

### **Advert.-Intervall**

Das Advertisement-Intervall gibt an, nach welcher Zeit ein virtueller Router neu propagiert wird. Der Defaultwert beträgt 100 Zentisekunden (1 Sekunde).

Zusätzlich muss bei Version v2 oder v2+v3 das Intervall ein Ganzzahliges von 100 sein, da bei VRRPv2 das Intervall eine ganzzahlige Sekundenzahl darstellen muss. Wird die Version nachträglich geändert, dann wird das Advert.-Intervall automatisch auf einen gültigen Wert angepasst und sollte überprüft werden.



Mit einer Propagationszeit von 1 Sekunde erzielen die Router im VRRP-Verband einen sehr schnellen Wechsel beim Ausfall eines Gerätes oder eines Interfaces. Eine Unterbrechung in dieser Größenordnung wird von den meisten Anwendungen unbemerkt bleiben, da normalerweise auch die TCP-Verbindung nicht unterbrochen wird. Andere Routingprotokolle benötigen bis zu 5 Minuten oder länger, um den Wechsel auf einen Backup-Router durchzuführen.

### **Virtuelle IPv4-Adresse**

Definiert die virtuelle IPv4-Adresse des virtuellen Routers. Die Adresse muss auf allen Router des VRRP-Verbands identisch sein.

Verwenden Sie als virtuelle IP-Adressen ausschließlich IP-Adressen, die nicht dynamisch an Endgeräte vergeben werden, die kein VRRP sprechen, um Konflikte zu vermeiden.


Wenn die vergebene Virtuelle-IPv4 der physikalischen Adresse des Geräts auf dem LAN-Interface entsprechen, werden die konfigurierten Prioritäten und Backup-Prioritäten ignoriert und stattdessen gemäß RFC immer die Priorität 255 verwendet.




Eine un spezifizierte IPv4-Adresse (0.0.0.0) deaktiviert für diesen Konfigurationseintrag IPv4.

### Virtuelle Link Lokale IPv6-Adresse

Definiert die virtuelle Link-lokale IPv6-Adresse des virtuellen Routers, z. B. fe80::1. Die Adresse muss auf allen Router des VRRP-Verbunds identisch sein. Diese Adresse wird für als Absendeadresse für das Versenden der Router Advertisements verwendet. Der Parameter wird nur im VRRPv3-Modus unterstützt.

-  Die Vergabe einer virtuellen link lokalen Adresse ist zwingend notwendig, um einen virtuellen Router für IPv6 zu definieren.

Wenn die vergebene virtuelle Link-lokale IPv6-Adresse der physikalischen Adresse des Geräts auf dem LAN-Interface entsprechen, werden die konfigurierten Prioritäten und Backup-Prioritäten ignoriert und stattdessen gemäß RFC immer die Priorität 255 verwendet.

-  Eine unspezifizierte IPv6-Adresse (::) deaktiviert für diesen Konfigurationseintrag IPv6.

### Virtuelle Globale IPv6-Adresse

Definiert die optionale globale IPv6-Adresse des virtuellen Routers, z. B. 2001:db8::1. Die Adresse muss auf allen Router des VRRP-Verbunds identisch sein. Der Parameter wird nur im VRRPv3-Modus unterstützt.

-  Für den VPN-Loadbalancer ist diese Adresse notwendig, wenn dieser mit IPv6 arbeiten soll.

### Überwachte Gegenstelle

Name der Gegenstelle, die das Verhalten des virtuellen Routers steuert. Die Gegenstelle kann auch weiteren virtuellen Routern zugeordnet werden.

Die Angabe der Gegenstelle ist optional. Mit der Bindung der Backup-Bedingung an eine Gegenstelle wird die LANCOM spezifische Erweiterung von VRRP genutzt, nicht nur den Ausfall eines Gerätes (VRRP-Standard), sondern zusätzlich auch die Störung eines Interfaces oder einer Gegenstelle abzusichern.

### Kommentar

Vergeben Sie einen Kommentar für diesen Eintrag.

### Reconnect-Verzögerung

Hier geben Sie an, nach wie vielen Minuten ein abgemeldeter virtueller Router versucht, seine Hauptverbindung wieder aufzubauen. Bei diesem Aufbauversuch bleibt der Router abgemeldet. Erst wenn die Verbindung erfolgreich aufgebaut werden konnte, meldet er sich wieder mit seiner Haupt- oder Backup-Priorität an. Der Defaultwert beträgt 30 Minuten. Eingabe erfolgt als <Minuten>:<Sekunden>

### Master-Holddown-Zeit

Wenn hier eine Zeit konfiguriert ist, wechselt der virtuelle Router in den Zustand „Hold-Down“, sobald die überwachte WAN-Verbindung mit einem Fehler abgebaut wird und das Backup-Delay abläuft (also in den Backupzustand wechselt). Im Zustand „Hold-Down“ kann die überwachte WAN-Verbindung nicht mehr aufgebaut werden. Des Weiteren werden keine VRRP-Advertisements mehr geschickt.

Sobald die „Master-Holddown-Zeit“ abläuft, wechselt der virtuelle Router in den Zustand „Standby“, in dem die überwachte WAN-Verbindung wiederaufgebaut werden kann.

Die „Master-Holddown-Time“ ist ein String von maximal 6 Zeichen, der die Ziffern 0-9 und den Doppelpunkt enthalten kann. Damit können Zeiten von maximal 999 Minuten 59 Sekunden (999:59) eingegeben werden.

Ist kein Doppelpunkt vorhanden (z. B. „30“) dann wird die Angabe als Minuten interpretiert. Hier ist dennoch maximal „999“ möglich.

Ist ein Doppelpunkt vorhanden, müssen nach dem Doppelpunkt zwei Zeichen kommen, die als Sekunden interpretiert werden. Hier sind maximal „59“ möglich.

Korrekte Zeitangaben sind also z. B. „5“ (5 Minuten), „5:30“ (5 Minuten, 30 Sekunden) oder „0:30“ (30 Sekunden).

Ein Wert von „0“ oder „0:00“ deaktiviert den Master-Holddown.


### WAN-Verbindungskontrolle

Definiert, ob VRRP den Verbindungsaufbau der überwachten WAN-Gegenstelle in der Standby-Rolle unterdrücken soll. Mögliche Werte:

#### Aktiviert

In der Rolle Standby wird der Aufbau der überwachten WAN-Gegenstelle nicht unterdrückt und die WAN-Verbindung wird aufgebaut. Desweiteren werden in diesem Fall auch die Routen zum überwachten WAN nicht umgeschaltet, wenn der virtuelle Router in den Standby wechselt.

---

 Pakete, die an die physikalische MAC-Adresse des Routers geschickt werden, werden im Standby-Zustand nicht zum Master weitergeleitet.

#### Deaktiviert

In der Rolle Standby wird der Aufbau der überwachten WAN-Gegenstelle unterdrückt.

### LAN-Link-Erkennung

Definiert, ob im Falle, dass keine LAN-Verbindung besteht, der Aufbau der WAN-Verbindung nicht unterdrückt werden soll.

Die Funktion ist für ein Szenario relevant, wo der Router noch ohne LAN-Verbindung in Betrieb ist, aber eine Verwaltung des Routers über die WAN-Verbindung möglich sein soll. In diesem Szenario muss die LAN-Link-Erkennung deaktiviert werden.

### Interne Dienste unter der virtuellen IP anbieten

Dieser Schalter steuert, ob der virtuelle Router im DHCPv4, DHCPv6 und Router-Advertisement als DNS-Server zugewiesen wird.


## 11.1.4 Ergänzungen im Setup-Menü

### VRRP

Dieses Menü enthält die Konfiguration von VRRP für ihren IP-Router.

Das Virtual-Router-Redundancy-Protocol dient dazu, mehrere physikalische Router wie einen einzigen „virtuellen“ Router erscheinen zu lassen. Von den vorhandenen physikalischen Routern ist immer einer der sogenannte Master. Dieser Master ist der einzige, der wirklich eine Verbindung z. B. ins Internet hat und Daten überträgt. Erst wenn der Master ausfällt, weil z. B. die Spannungsversorgung unterbrochen oder seine Internetanbindung ausgefallen ist, werden die anderen Router aktiv. Über das Protokoll VRRP, handeln sie nun aus, wer als nächster die Rolle des Masters zu übernehmen hat. Der neue Master übernimmt vollständig die Aufgaben des bisherigen Masters.

---

 VRRP arbeitet für IPv4 und IPv6 jeweils unabhängig, auch wenn es gemeinsam in einer Zeile konfiguriert wurde. Dies ist sogar empfehlenswert, damit das Advert.-Intervall und die Prioritäten konsistent sind.

### SNMP-ID:

2.141

### Pfad Konsole:

Setup



**Aktiv**

Mit diesem Schalter lässt sich das VRRP-Modul ein- und ausschalten.

**SNMP-ID:**

2.141.1

**Pfad Konsole:**

**Setup > VRRP**

**Mögliche Werte:**

**Ja**

**Nein**

**Default-Wert:**

Nein

**Virtuelle-Router**

In der Tabelle Virtuelle Router können die virtuellen Router pro Interface definiert werden.

**SNMP-ID:**

2.141.2

**Pfad Konsole:**

**Setup > VRRP**

**Interface**

Logisches IPv4- oder IPv6-Interface bzw. Netzwerk, auf dem VRRP aktiviert werden soll. Es werden grundsätzlich nur LAN-Interfaces unterstützt.

**SNMP-ID:**

2.141.2.1

**Pfad Konsole:**

**Setup > VRRP > Virtuelle-Router**

**Mögliche Werte:**

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

**Default-Wert:**

*leer*

**Router-ID**

Eindeutige ID des virtuellen Routers. Mit der Router-ID werden mehrere physikalische Router zu einem virtuellen Router bzw. einer Standby-Gruppe zusammengefasst. Manchmal wird die Router-ID auch VRRP-ID oder kurz VRID genannt.

**SNMP-ID:**

2.141.2.2

**Pfad Konsole:****Setup > VRRP > Virtuelle-Router****Mögliche Werte:**

1 ... 255

**Default-Wert:**

1

**Aktiv**

Aktiviert oder deaktiviert VRRP auf dem Interface.

**SNMP-ID:**

2.141.2.3

**Pfad Konsole:****Setup > VRRP > Virtuelle-Router****Mögliche Werte:****Ja**  
**Nein****Default-Wert:**

Ja

**Version**

Definiert welche VRRP-Version verwendet werden soll. Es werden VRRPv2, VRRPv3 oder VRRPv2 und VRRPv3 unterstützt. IPv6 wird nur bei VRRPv3 unterstützt. IPv4 wird sowohl bei VRRPv2 als auch bei VRRPv3 unterstützt.

Der Modus v2+v3 ist als Übergangslösung für die Transition von einem VRRPv2- zu einem VRRPv3-Betrieb unter IPv4 gedacht und sorgt für ein verdoppeltes Paketaufkommen, da ein so konfigurierter Virtueller Router Advertisements in beiden Protokollversionen versendet.

Ein Virtueller Router, der auf eine Protokollversion konfiguriert wurde, verwirft Advertisements anderer Router, wenn sie die falsche Protokollversion haben, und gibt eine Ausgabe auf dem VRRP-Packet Trace aus und trägt einen zugehörigen Eintrag in die Event-Log-Tabelle ein.

**SNMP-ID:**

2.141.2.4

**Pfad Konsole:****Setup > VRRP > Virtuelle-Router****Mögliche Werte:**

v2

v3

v2+v3

**Default-Wert:**

v3

**Prio**

Gibt die Priorität an, mit der der Virtuelle Router arbeitet. Diese wird in den Advertisements übertragen und bestimmt maßgeblich, welches Gerät der zuständige Master für eine VRRP-Verbund ist. Die angegebene Priorität muss größer als 0 sein.

Der Wert 255 hat eine Sonderbedeutung:

- > Der Wert 255 wird automatisch eingestellt, wenn die Adresse des virtuellen Routers gleich der Adresse des Interfaces ist, an das der Router gebunden ist. In allen anderen Fällen wird die Priorität automatisch herabgesetzt.

**SNMP-ID:**

2.141.2.5

**Pfad Konsole:****Setup > VRRP > Virtuelle-Router****Mögliche Werte:**

max. 3 Zeichen aus [0-9]

**Default-Wert:**

100

**Backup-Prio**

Die Backup-Priorität des virtuellen Routers bezieht sich auf das Interface, für das eine Backup-Verbindung konfiguriert ist, also z. B. bei Routern mit DSL- und Mobilfunk-Unterstützung auf das Mobilfunk-Interface. Es sind Werte zwischen 0 und der konfigurierten Priorität zulässig. Der Wert 0 hat eine Sonderbedeutung:

- > 0 deaktiviert den virtuellen Router im Backup-Fall. Es wird in regelmäßigen Abständen geprüft, ob die Hauptverbindung wieder aufgebaut werden kann. Das Prüf-Intervall wird im Reconnect-Delay festgelegt.

Wenn im Backup-Fall auch die Backup-Verbindung nicht aufgebaut werden kann meldet sich der virtuelle Router vollständig ab und versucht ebenfalls in, über die Reconnect-Verzögerung angegebenen, Intervallen entweder die Haupt- oder die Backup-Verbindung erneut aufzubauen.

**SNMP-ID:**

2.141.2.6

**Pfad Konsole:****Setup > VRRP > Virtuelle-Router****Mögliche Werte:**

max. 3 Zeichen aus [0-9]


**Default-Wert:**

0

**Ank.-Intervall**

Das Advertisement-Intervall gibt an, nach welcher Zeit ein virtueller Router neu propagiert wird. Der Defaultwert beträgt 100 Zentisekunden (1 Sekunde).

Zusätzlich muss bei Version v2 oder v2+v3 das Intervall ein Ganzzahliges von 100 sein, da bei VRRPv2 das Intervall eine ganzzahlige Sekundenzahl darstellen muss. Wird die Version nachträglich geändert, dann wird das Advert.-Intervall automatisch auf einen gültigen Wert angepasst und sollte überprüft werden.

 Mit einer Propagationszeit von 1 Sekunde erzielen die Router im VRRP-Verbund einen sehr schnellen Wechsel beim Ausfall eines Gerätes oder eines Interfaces. Eine Unterbrechung in dieser Größenordnung wird von den meisten Anwendungen unbemerkt bleiben, da normalerweise auch die TCP-Verbindung nicht unterbrochen wird. Andere Routingprotokolle benötigen bis zu 5 Minuten oder länger, um den Wechsel auf einen Backup-Router durchzuführen.

**SNMP-ID:**

2.141.2.7

**Pfad Konsole:****Setup > VRRP > Virtuelle-Router****Mögliche Werte:**

max. 5 Zeichen aus [0-9]

**Default-Wert:**

100


**Virtuelle-IPv4**

Definiert die virtuelle IPv4-Adresse des virtuellen Routers. Die Adresse muss auf allen Router des VRRP-Verbunds identisch sein.

Verwenden Sie als virtuelle IP-Adressen ausschließlich IP-Adressen, die nicht dynamisch an Endgeräte vergeben werden, die kein VRRP sprechen, um Konflikte zu vermeiden.

Wenn die vergebene Virtuelle-IPv4 der physikalischen Adresse des Geräts auf dem LAN-Interface entsprechen, werden die konfigurierten Prioritäten und Backup-Prioritäten ignoriert und stattdessen gemäß RFC immer die Priorität 255 verwendet.

---

 Eine unspezifizierte IPv4-Adresse (0.0.0.0) deaktiviert für diesen Konfigurationseintrag IPv4.

**SNMP-ID:**

2.141.2.8


**Pfad Konsole:****Setup > VRRP > Virtuelle-Router****Mögliche Werte:**

max. 15 Zeichen aus [0-9] .

**Link-Lokale-Virtuelle-IPv6**

Definiert die virtuelle Link-lokale IPv6-Adresse des virtuellen Routers, z. B. fe80::1. Die Adresse muss auf allen Router des VRRP-Verbunds identisch sein. Diese Adresse wird für als Absendeadresse für das Versenden der Router Advertisements verwendet. Der Parameter wird nur im VRRPv3-Modus unterstützt.

---

 Die Vergabe einer virtuellen link lokalen Adresse ist zwingend notwendig, um einen virtuellen Router für IPv6 zu definieren.

Wenn die vergebene virtuelle Link-lokale IPv6-Adresse der physikalischen Adresse des Geräts auf dem LAN-Interface entsprechen, werden die konfigurierten Prioritäten und Backup-Prioritäten ignoriert und stattdessen gemäß RFC immer die Priorität 255 verwendet.

---

 Eine unspezifizierte IPv6-Adresse (::) deaktiviert für diesen Konfigurationseintrag IPv6.

**SNMP-ID:**

2.141.2.9

**Pfad Konsole:****Setup > VRRP > Virtuelle-Router****Mögliche Werte:**

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

**Globale-Virtuelle-IPv6**

Definiert die optionale globale IPv6-Adresse des virtuellen Routers, z. B. 2001:db8::1. Die Adresse muss auf allen Router des VRRP-Verbunds identisch sein. Der Parameter wird nur im VRRPv3-Modus unterstützt.

---

 Für den VPN-Loadbalancer ist diese Adresse notwendig, wenn dieser mit IPv6 arbeiten soll.

**SNMP-ID:**

2.141.2.10

**Pfad Konsole:****Setup > VRRP > Virtuelle-Router****Mögliche Werte:**max. 39 Zeichen aus `[A-F] [a-f] [0-9] : .`**Ueberwachtes-WAN**

Name der Gegenstelle, die das Verhalten des virtuellen Routers steuert. Die Gegenstelle kann auch weiteren virtuellen Routern zugeordnet werden.

Die Angabe der Gegenstelle ist optional. Mit der Bindung der Backup-Bedingung an eine Gegenstelle wird die LANCOM spezifische Erweiterung von VRRP genutzt, nicht nur den Ausfall eines Gerätes (VRRP-Standard), sondern zusätzlich auch die Störung eines Interfaces oder einer Gegenstelle abzusichern.

**SNMP-ID:**

2.141.2.11

**Pfad Konsole:****Setup > VRRP > Virtuelle-Router****Mögliche Werte:**max. 16 Zeichen aus `[A-Z] [0-9] @ { | } ~ ! $ % & ' ( ) + - , / : ; < = > ? [ \ ] ^ _ .`**Default-Wert:***leer***Kommentar**

Vergeben Sie einen Kommentar für diesen Eintrag.

**SNMP-ID:**

2.141.2.12

**Pfad Konsole:****Setup > VRRP > Virtuelle-Router****Mögliche Werte:**max. 64 Zeichen aus `[A-Z] [a-z] [0-9] # @ { | } ~ ! $ % & ' ( ) + - , / : ; < = > ? [ \ ] ^ _ . ``**Default-Wert:***leer***Master-Holddown-Zeit**

Wenn hier eine Zeit konfiguriert ist, wechselt der virtuelle Router in den Zustand „Hold-Down“, sobald die überwachte WAN-Verbindung mit einem Fehler abgebaut wird und das Backup-Delay abläuft (also in den Backupzustand wechselt).

Im Zustand „Hold-Down“ kann die überwachte WAN-Verbindung nicht mehr aufgebaut werden. Des Weiteren werden keine VRRP-Advertisements mehr geschickt.

Sobald die „Master-Holddown-Zeit“ abläuft, wechselt der virtuelle Router in den Zustand „Standby“, in dem die überwachte WAN-Verbindung wiederaufgebaut werden kann.

Die „Master-Holddown-Time“ ist ein String von maximal 6 Zeichen, der die Ziffern 0-9 und den Doppelpunkt enthalten kann. Damit können Zeiten von maximal 999 Minuten 59 Sekunden (999:59) eingegeben werden.

Ist kein Doppelpunkt vorhanden (z. B. „30“) dann wird die Angabe als Minuten interpretiert. Hier ist dennoch maximal „999“ möglich.

Ist ein Doppelpunkt vorhanden, müssen nach dem Doppelpunkt zwei Zeichen kommen, die als Sekunden interpretiert werden. Hier sind maximal „59“ möglich.

Korrekte Zeitangaben sind also z. B. „5“ (5 Minuten), „5:30“ (5 Minuten, 30 Sekunden) oder „0:30“ (30 Sekunden).

Ein Wert von „0“ oder „0:00“ deaktiviert den Master-Holddown.

**SNMP-ID:**

2.141.3

**Pfad Konsole:**

**Setup > VRRP**

**Mögliche Werte:**

max. 6 Zeichen aus [0-9] :

**Default-Wert:**

0:00

**Reconnect-Verz.**

Wenn die Backup-Verbindung eines Routers nicht aufgebaut werden konnte, wird der Router nicht mehr propagiert. Das Reconnect-Delay gibt an, nach wie vielen Minuten ein solcher Router in diesem Fall versucht, seine Haupt- oder Backup-Verbindung erneut aufzubauen. Während dieses Versuchs wird dieser Router weiterhin nicht propagiert. Eingabe erfolgt als <Minuten>:<Sekunden>.

**SNMP-ID:**

2.141.4

**Pfad Konsole:**

**Setup > VRRP**

**Mögliche Werte:**

max. 6 Zeichen aus [0-9] :

**Default-Wert:**

30:00

**Interne-Dienste-Zuweisen**

Dieser Schalter steuert, ob der virtuelle Router im DHCPv4, DHCPv6 und Router-Advertisement als DNS-Server zugewiesen wird.

**SNMP-ID:**

2.141.5

**Pfad Konsole:****Setup > VRRP****Mögliche Werte:****Ja****Nein****Default-Wert:**

Ja

**Lan-Link-Detection**

Definiert, ob im Falle, dass keine LAN-Verbindung besteht, der Aufbau der WAN-Verbindung nicht unterdrückt werden soll.

Die Funktion ist für ein Szenario relevant, wo der Router noch ohne LAN-Verbindung in Betrieb ist, aber eine Verwaltung des Routers über die WAN-Verbindung möglich sein soll. In diesem Szenario muss die LAN-Link-Erkennung deaktiviert werden.

**SNMP-ID:**

2.141.6

**Pfad Konsole:****Setup > VRRP****Mögliche Werte:****Ja****Nein****Default-Wert:**

Ja

**WAN-Verbindungskontrolle**

Definiert, ob VRRP den Verbindungsaufbau der überwachten WAN-Gegenstelle in der Standby-Rolle unterdrücken soll.

**SNMP-ID:**

2.141.7



**Pfad Konsole:****Setup > VRRP****Mögliche Werte:****Inaktiv**

In der Rolle Standby wird der Aufbau der überwachten WAN-Gegenstelle nicht unterdrückt und die WAN-Verbindung wird aufgebaut. Desweiteren werden in diesem Fall auch die Routen zum überwachten WAN nicht umgeschaltet, wenn der virtuelle Router in den Standby wechselt.



Pakete, die an die physikalische MAC-Adresse des Routers geschickt werden, werden im Standby-Zustand nicht zum Master weitergeleitet.

**Aktiv**

In der Rolle Standby wird der Aufbau der überwachten WAN-Gegenstelle unterdrückt.

**Default-Wert:**

Aktiv

**V2-Checksumme-fuer-IPv4**

Definiert, wie die Checksumme von VRRPv3-Paketen bei IPv4 berechnet werden soll. Aus Kompatibilitätsgründen zu 3rd-Party-Netzwerkgeräten kann die Checksumme bei VRRPv3 IPv4 wie in VRRPv2 berechnet werden.

**SNMP-ID:**

2.141.8

**Pfad Konsole:****Setup > VRRP****Mögliche Werte:****Ja**

Checksumme bei VRRPv3 IPv4 wie in VRRPv2 berechnen.

**Nein**

Checksumme bei VRRPv3 IPv4 nicht wie in VRRPv2 berechnen.

**Default-Wert:**

Nein

# 12 RADIUS

## 12.1 RADIUS-Message-Authenticator-Prüfung

Ab LCOS 10.90 gibt es an mehreren Stellen den neuen Parameter **Message-Authenticator erforderlich**

In LANconfig finden Sie diese unter

- > **Kommunikation > RADIUS,**
- > **RADIUS > Server > RADIUS- / RADSEC-Clients > IPv4-Clients,**
- > **RADIUS > Server > RADIUS- / RADSEC-Clients > IPv6-Clients,**
- > **RADIUS > Server > Erweiterte Einstellungen > Weiterleitung > Weiterleitungs-Server,**
- > **Management > Authentifizierung > RADIUS-Authentifizierung > RADIUS-Server** und
- > **VPN > IKEv2/IPSec > Erweiterte Einstellungen > RADIUS-Authentifizierung > RADIUS-Server.**

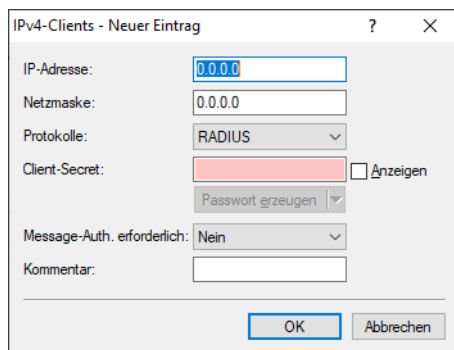


Abbildung 2: Beispiel in LANconfig

### Message-Authenticator erforderlich

Definiert, ob das Vorhandensein des Message-Authenticator-Attributs in RADIUS-Nachrichten auf Client-Seite erforderlich ist. Die Client-Seite ist die Seite, die den RADIUS-Accept/Fail empfängt.

### 12.1.1 Ergänzungen im Setup-Menü

#### Msg-Authenticator-erforderlich

Definiert, ob das Vorhandensein des Message-Authenticator-Attributs in RADIUS-Nachrichten auf Client-Seite erforderlich ist. Die Client-Seite ist die Seite, die den RADIUS-Accept/Fail empfängt.

#### SNMP-ID:

2.2.22.28

#### Pfad Konsole:

Setup > WAN > RADIUS

**Mögliche Werte:****nein**

Access-Requests müssen keinen Message-Authenticator enthalten.

**ja**

Access-Requests müssen immer einen Message-Authenticator enthalten.

**Default-Wert:**

nein

**L2TP-Msg-Authenticator-erforderlich**

Definiert, ob das Vorhandensein des Message-Authenticator-Attributs in RADIUS-Nachrichten auf Client-Seite erforderlich ist. Die Client-Seite ist die Seite, die den RADIUS-Accept/Fail empfängt.

**SNMP-ID:**

2.2.22.29

**Pfad Konsole:****Setup > WAN > RADIUS****Mögliche Werte:****nein**

Access-Requests müssen keinen Message-Authenticator enthalten.

**ja**

Access-Requests müssen immer einen Message-Authenticator enthalten.

**Default-Wert:**

nein

**Msg-Authenticator-erforderlich**

Definiert, ob das Vorhandensein des Message-Authenticator-Attributs in RADIUS-Nachrichten auf Client-Seite erforderlich ist. Die Client-Seite ist die Seite, die den RADIUS-Accept/Fail empfängt.

**SNMP-ID:**

2.11.81.1.10

**Pfad Konsole:****Setup > Config > RADIUS > Server**

**Mögliche Werte:****nein**

Access-Requests müssen keinen Message-Authenticator enthalten.

**ja**

Access-Requests müssen immer einen Message-Authenticator enthalten.

**Default-Wert:**

nein

**Msg-Authenticator-erforderlich**

Definiert, ob das Vorhandensein des Message-Authenticator-Attributs in RADIUS-Nachrichten auf Client-Seite erforderlich ist. Die Client-Seite ist die Seite, die den RADIUS-Accept/Fail empfängt.

**SNMP-ID:**

2.12.29.21

**Pfad Konsole:****Setup > WLAN > RADIUS-Zugriffspruefung****Mögliche Werte:****nein**

Access-Requests müssen keinen Message-Authenticator enthalten.

**ja**

Access-Requests müssen immer einen Message-Authenticator enthalten.

**Default-Wert:**

nein

**Backup-Msg-Authenticator-erforderlich**

Definiert, ob das Vorhandensein des Message-Authenticator-Attributs in RADIUS-Nachrichten auf Client-Seite erforderlich ist. Die Client-Seite ist die Seite, die den RADIUS-Accept/Fail empfängt.

**SNMP-ID:**

2.12.29.22

**Pfad Konsole:****Setup > WLAN > RADIUS-Zugriffspruefung**

**Mögliche Werte:****nein**

Access-Requests müssen keinen Message-Authenticator enthalten.

**ja**

Access-Requests müssen immer einen Message-Authenticator enthalten.

**Default-Wert:**

nein

**Msg-Authenticator-erforderlich**

Definiert, ob das Vorhandensein des Message-Authenticator-Attributs in RADIUS-Nachrichten auf Client-Seite erforderlich ist. Die Client-Seite ist die Seite, die den RADIUS-Accept/Fail empfängt.

**SNMP-ID:**

2.19.36.9.1.1.11

**Pfad Konsole:****Setup > VPN > IKEv2 > RADIUS > Autorisierung > Server****Mögliche Werte:****nein**

Access-Requests müssen keinen Message-Authenticator enthalten.

**ja**

Access-Requests müssen immer einen Message-Authenticator enthalten.

**Default-Wert:**

nein

**Msg-Authenticator-erforderlich**

Definiert, ob das Vorhandensein des Message-Authenticator-Attributs in RADIUS-Nachrichten auf Client-Seite erforderlich ist. Die Client-Seite ist die Seite, die den RADIUS-Accept/Fail empfängt.

**SNMP-ID:**

2.25.10.2.6

**Pfad Konsole:****Setup > RADIUS > Server > Clients**

**Mögliche Werte:****nein**

Access-Requests müssen keinen Message-Authenticator enthalten.

**ja**

Access-Requests müssen immer einen Message-Authenticator enthalten.

**Nur-Proxy**

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

**Default-Wert:**

nein

**Msg-Authenticator-erforderlich**

Definiert, ob das Vorhandensein des Message-Authenticator-Attributs in RADIUS-Nachrichten auf Client-Seite erforderlich ist. Die Client-Seite ist die Seite, die den RADIUS-Accept/Fail empfängt.

**SNMP-ID:**

2.25.10.3.18

**Pfad Konsole:**

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

**Mögliche Werte:****nein**

Access-Requests müssen keinen Message-Authenticator enthalten.

**ja**

Access-Requests müssen immer einen Message-Authenticator enthalten.

**Default-Wert:**

nein

**Msg-Authenticator-erforderlich**

Definiert, ob das Vorhandensein des Message-Authenticator-Attributs in RADIUS-Nachrichten auf Client-Seite erforderlich ist. Die Client-Seite ist die Seite, die den RADIUS-Accept/Fail empfängt.

**SNMP-ID:**

2.25.10.16.6

**Pfad Konsole:**

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

**Mögliche Werte:****nein**

Access-Requests müssen keinen Message-Authenticator enthalten.

**ja**

Access-Requests müssen immer einen Message-Authenticator enthalten.

**Nur-Proxy**

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

**Default-Wert:**

nein

## 13 Weitere Dienste

### 13.1 Unterstützung für MTU 1500 im PPPoE nach RFC 4638

Ab LCOS 10.90 wird MTU 1500 im PPPoE nach [RFC 4638](#) unterstützt.

Dazu gibt es zwei neue Parameter. Der erste bei den DSL-Breitband-Gegenstellen unter **Kommunikation > Gegenstellen > Gegenstellen (DSL)**.

#### MTU 1500 über PPPoE

Definiert, ob das Gerät im PPPoE eine MTU von 1500 nach [RFC 4638](#) verhandeln soll. Die Gegenseite muss diese Erweiterung ebenfalls unterstützen.

Den zweiten neuen Parameter finden Sie bei den Einstellungen für den PPPoE-Server. In LANconfig unter **Kommunikation > Allgemein**.

#### MTU 1500 unterstützen

Definiert, ob das Gerät im PPPoE eine MTU von 1500 nach [RFC 4638](#) verhandeln soll. Die Gegenseite muss diese Erweiterung ebenfalls unterstützen.



### 13.1.1 Ergänzungen im Setup-Menü

#### PPPoE-MTU-1500

Definiert, ob das Gerät im PPPoE eine MTU von 1500 nach [RFC 4638](#) verhandeln soll. Die Gegenseite muss diese Erweiterung ebenfalls unterstützen.

#### SNMP-ID:

2.2.19.22

#### Pfad Konsole:

Setup > WAN > DSL-Breitband-Gegenstellen

#### Mögliche Werte:

Ja  
Nein

#### Default-Wert:

Nein

#### MTU-1500

Definiert, ob das Gerät im PPPoE eine MTU von 1500 nach [RFC 4638](#) verhandeln soll. Die Gegenseite muss diese Erweiterung ebenfalls unterstützen.

#### SNMP-ID:

2.31.7

#### Pfad Konsole:

Setup > PPPoE-Server

#### Mögliche Werte:

Ja  
Nein

#### Default-Wert:

Nein

## 13.2 Operations, Administration und Management (OAM)

Ethernet OAM nach IEEE 802.3ah dient ISPs zur Überwachung einer Ethernet-basierten **letzten Meile**, zum Beispiel bei FTTH- oder VDSL2-Zugängen.

Hierzu werden von der aktiven Seite, die für gewöhnlich die ISP-Seite darstellt, regelmäßig OAM-Pakete (OAM Protocol Data Units – OAMPDUs) übertragen. Die passive Seite, welche für gewöhnlich die CPE-Seite darstellt, reagiert auf diese

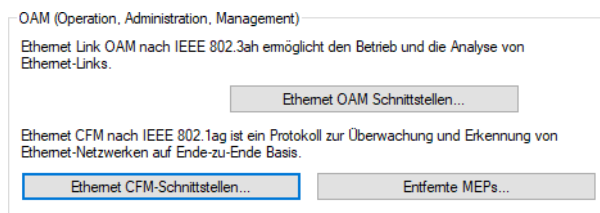
OAMPDUs und beantwortet sie. Hierdurch wird die Erreichbarkeit der Gegenseite überprüft. Dieses Verfahren wird **OAM Discovery** genannt.

Bisher gab es dieses Feature nur auf der CLI. Ab LCOS 10.90 wurden zwei Parameter ergänzt und das Feature in LANconfig exponiert.

Ab LCOS 10.90 wird außerdem Connectivity Fault Management (CFM) nach IEEE 802.1ag / ITU-T Y.1731 unterstützt.

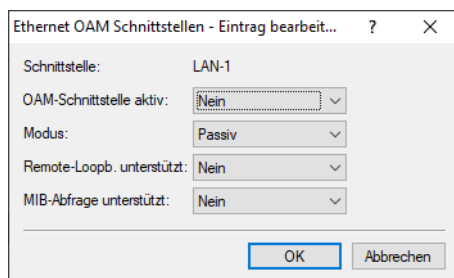
Connectivity Fault Management (CFM) nach IEEE 802.1ag / ITU-T Y.1731 ist eine Sammlung von Protokollen und Werkzeugen zur sog. OAM auf Layer 2. CFM wird verwendet zur Überwachung und Fehleranalyse in LANs, Bridges oder Ethernet-basierten WANs.

In LANconfig konfigurieren Sie OAM unter **Sonstige Dienste > Dienste > OAM (Operation, Administration, Management)**.



### 13.2.1 Ethernet Link OAM (IEEE 802.3ah)

In LANconfig konfigurieren Sie Ethernet OAM nach IEEE 802.3ah unter **Sonstige Dienste > Dienste > OAM (Operation, Administration, Management) > Ethernet OAM Schnittstellen**.



#### Schnittstelle

Name der Schnittstelle.

#### OAM-Schnittstelle aktiv

Aktiviert/deaktiviert OAM auf der jeweiligen Schnittstelle.

#### Modus

Legt den Modus (Aktiv/Passiv) für die jeweilige Schnittstelle fest.

#### Aktiv

Die passive Seite (üblicherweise die CPE-Seite) beantwortet die OAM-Pakete (OAMPDUs) des Senders.

#### Passiv (Default)

Die aktive Seite (üblicherweise der Internet-Provider) sendet die OAM-Pakete (OAMPDUs) an den Empfänger.

#### Remote-Loopback unterstützt

Definiert, ob das Geräte sich von der Gegenseite in den Loopback-Modus versetzen lassen kann. Im Loopback-Modus stellt das Gerät den Forwarding-Modus ein und sendet alle empfangenen Pakete auf der

Schnittstelle zurück. Dabei wird das Paket genau so zurückgesendet wie es empfangen wurde, es werden weder MAC-Adressen noch IP-Adressen gespiegelt.

#### **MIB-Abfrage unterstützt**

Definiert, ob das Gerät erlaubt, dass die Gegenseite bestimmte Statuswerte bzw. Zähler über Pakete vom Gerät abrufen darf.

Die folgenden beiden Kommandos werden auf der CLI unterstützt:

### **Ergänzungen im Setup-Menü**

#### **entfernter-Loopback-unterstuetzt**

Definiert, ob das Gerät sich von der Gegenseite in den Loopback-Modus versetzen lassen kann. Im Loopback-Modus stellt das Gerät den Forwarding-Modus ein und sendet alle empfangenen Pakete auf der Schnittstelle zurück. Dabei wird das Paket genau so zurückgesendet wie es empfangen wurde. Es werden weder MAC-Adressen noch IP-Adressen gespiegelt.

#### **SNMP-ID:**

2.105.1.4

#### **Pfad Konsole:**

**Setup > OAM > Schnittstellen**

#### **Mögliche Werte:**

##### **Ja**

Gerät lässt sich von der Gegenseite in den Loopback-Modus versetzen.

##### **Nein**

Gerät lässt sich von der Gegenseite nicht in den Loopback-Modus versetzen.

#### **Default-Wert:**

Nein

#### **MIB-Abfragen-unterstuetzt**

Definiert, ob das Gerät erlaubt, dass die Gegenseite bestimmte Statuswerte bzw. Zähler über Pakete vom Gerät abrufen darf.

#### **SNMP-ID:**

2.105.1.5

#### **Pfad Konsole:**

**Setup > OAM > Schnittstellen**

#### **Mögliche Werte:**

##### **Ja**

Gerät unterstützt MIB-Abfragen.

**Nein**

Gerät unterstützt keine MIB-Abfragen.

**Default-Wert:**

Nein

**Remote-Loopback**

Mit diesem Kommando sendet das Gerät eine Loopback Control OAMPDU an die Gegenseite, so dass die Gegenseite in den Loopback-Modus versetzt wird, oder entsprechend wieder beendet wird. Im Loopback-Modus stellt das Gerät auf der Gegenseite den Forwarding-Modus auf dieser Schnittstelle ein und sendet alle empfangenen Pakete zurück. Dabei wird das Paket genau so zurückgesendet wie es empfangen wurde, es werden weder MAC-Adressen noch IP-Adressen gespiegelt.

**SNMP-ID:**

2.105.4

**Pfad Konsole:**

**Setup > OAM**

**Mögliche Argumente:****-i <Schnittstelle>**

Schnittstelle, auf der der Loopback-Modus gestartet oder gestoppt werden soll. Auf dieser Schnittstelle sendet das Gerät eine Nachricht, um die Gegenseite in den Loopback-Modus zu versetzen oder diesen dort zu beenden.

Mögliche Werte aus der OAM-Setup-Tabelle wie z. B. LAN-1, DSL-1, ...

**[-?]**

Gibt eine kurze Hilfe zu den Parametern aus.

**<start|stop>**

Startet oder stoppt den Loopback-Modus.

**Variablen-Lesen**

Mit diesem Kommando sendet das Gerät eine Variable Request OAMPDU an die Gegenseite. Die Gegenseite sendet darauf den Wert der angefragten Variable auf Basis der lokalen MIB. Mit diesem Verfahren lassen sich z. B. Paketzähler der Gegenseite auslesen. Die Gegenseite muss die Funktion zum Auslesen von MIB-Variablen per OAM unterstützen.

Unterstützt werden u. A. Variablen aus IEEE 802.3.1.

**Beispiel:**

```
> do Variable-Read -i LAN-3 aFramesTransmittedOK
aFramesTransmittedOK = 8444
OK: Action Variable-Read done
```

**SNMP-ID:**

2.105.6

**Pfad Konsole:****Setup > OAM****Mögliche Argumente:****-i <Schnittstelle>**

Schnittstelle, auf der die Variable ausgelesen werden soll.

**[-?]**

Gibt eine kurze Hilfe zu den Parametern aus.

**<Variablenname> [weitere Variablenamen]**

Ein oder mehrere durch Leerzeichen getrennte Variablenamen.

## 13.2.2 Connectivity Fault Management (IEEE 802.1ag / ITU-T Y.1731)

Connectivity Fault Management (CFM) nach IEEE 802.1ag / ITU-T Y.1731 ist eine Sammlung von Protokollen und Werkzeugen zur sog. OAM auf Layer 2. CFM wird verwendet zur Überwachung und Fehleranalyse in LANs, Bridges oder Ethernet-basierten WANs.

Die Protokolle bieten insbesondere Providern oder Betreibern bzw. Administratoren von Ethernet-Leitungen die Möglichkeit diese Leitungen proaktiv zu überwachen oder im Fehlerfall zu analysieren.

LCOS unterstützt dabei die folgenden Funktionen:

- > **Continuity Check Messages (CCM):** Es werden regelmäßige Status-Nachrichten ausgetauscht, um die Verfügbarkeit der Netzelemente zu überwachen
- > **Loopback:** Es können Loopback-Nachrichten gesendet werden, die von der Gegenseite zurückgesendet werden (ethping / Layer 2). Diese Funktion ist analog zum ICMP-basierten Ping auf Layer 3. Es werden sowohl Ethernet-Unicast als auch Multicast-Adressen unterstützt.
- > **Linktrace:** Es können Linktrace-Nachrichten gesendet werden, die von der Gegenseite zurückgesendet werden und von Netzelementen auf dem Pfad beantwortet werden (Layer 2). Diese Funktion ist analog zum ICMP-basierten Traceroute auf Layer 3

Die Funktionen CCM und Loopback / Linktrace sind unabhängig nutzbar, d. h. Loopback und Linktrace können auch ohne die Nutzung von regelmäßigen CCM-Nachrichten verwendet werden.

Darüber hinaus unterstützt LCOS die folgenden Funktionen aus ITU-T Y.1731:

- > Empfang und Status-Anzeige von ETH-AIS (Alarm Indication Signal)
- > Empfang und Status-Anzeige von ETH-LCK (Ethernet Locked Signal)
- > Empfang und Verarbeitung von ETH-RDI (Remote Defect Indication)

## Ethernet CFM Schnittstellen

In LANconfig konfigurieren Sie Ethernet OAM nach IEEE 802.3ah unter **Sonstige Dienste > Dienste > OAM (Operation, Administration, Management) > Ethernet CFM Schnittstellen**.

### Schnittstelle

Schnittstelle auf der CFM aktiviert werden soll, mögliche Werte sind LAN-Schnittstellen wie z.B. LAN-1 oder WAN-Schnittstellen wie DSL-1.

### CFM-Schnittstelle aktiv

Aktiviert oder Deaktiviert CFM auf der konfigurierten Schnittstelle.

### MD-Level

Definiert das Maintenance Domain Level für diese Schnittstelle.

### VLANs

Definiert die VLANs auf der Schnittstelle, mit der CFM-Nachrichten empfangen und gesendet werden können. Bei leerem Wert werden alle VLANs akzeptiert. Es kann entweder ein VLAN oder eine komma-separierte Liste von VLANs konfiguriert werden.

### Endpunkt-Typ

Definiert den CFM-Endpunkt-Typ. Mögliche Werte:

#### MEP (Maintenance Association End Point)

Der Maintenance Association End Point stellt die Grenze einer Domain dar und führt die Fehlererkennung zwischen den Domain-Grenzen durch. Der MEP erstellt und sendet CFM-Pakete.

#### MIP (Maintenance Intermediate Point)

Der Maintenance Intermediate Point befindet sich innerhalb der Domain und führt die Pfad- und Fehler-Erkennung innerhalb der Domain-Grenzen durch. Der MIP antwortet auf CFM-Pakete.

### Wartungsdomäne

Definiert den Namen der Wartungsdomäne (Maintenance Domain (MD)).

**Wartungsassoziiierung**

Definiert den Namen der Wartungsassoziiierung (Maintenance Association (MA)).

**MEPID**

Definiert die Maintenance Endpoint ID des Geräts für diesen Eintrag (1-8191). Diese muss auf jedem Gerät eindeutig sein.

**Sender-ID**

Definiert die optionale Sender-ID in CFM-CCM-Nachrichten.

**CoS**

Definiert den Class-of-Service mit dem CFM-CCM (Continuity Check Message)-Pakete markiert werden. Mögliche Werte: Best-Effort (0), Background (1), Excellent-Effort (3), Controlled-Latency (4), Video (5), Voice (6), Network-Control (7)

**CCM-Initiator**

Definiert, ob das Gerät regelmäßige CCM-Nachrichten (Continuity Check Message) versenden soll.

**CCM-Intervall**

Definiert, mit welchem Intervall CCM-Nachrichten (Continuity Check Message) von dem Gerät versendet werden sollen. CCM-Intervalle müssen zwischen Kommunikationspartnern einheitlich sein.

**CCM niedrigste Alarm-Priorität**

Definiert, wie schwerwiegend festgestellte Fehler mindestens sein müssen, damit der MEP das RDI-Flag (Remote Defect Indication) setzt und in CCM-Paketen propagiert. Level, in aufsteigender Schwere, sind:

**RDICCM**

Von mindestens einem anderen MEP wurde ein CC-Frame mit gesetztem RDI empfangen.

**MACstatus (Default)**

Mindestens ein anderer MEP hat einen Interface-Status ungleich 'up' gemeldet (z.B. Hardware-Problem), oder alle anderen MEPs melden einen PortStatus ungleich 'up' (z.B. Netzsegment isoliert).

**RemoteCCM**

Mindestens von einem konfigurierten MEP werden keine CCM-Frames empfangen.

**ErrorCCM**

Ein weiterer MEP verwendet die gleiche MEPID wie das lokale Gerät oder es werden CCMs von einem nicht konfigurierten MEP empfangen (falls Matching ungleich none), oder ein anderer MEP verwendet ein abweichendes CCM-Intervall.

**XconCCM**

Es wurden CCs von einem anderen MEP mit niedrigerem MD-Level empfangen, oder mit einer abweichenden Domain oder Association.

**CCM-Empfänger**

Definiert, ob das Gerät CCM-Nachrichten verarbeiten bzw. empfangen soll.

**Remote MEP-Verknüpfung**

Definiert, wie das Gerät die Anwesenheit von entfernten MEPs behandeln soll. Beliebige entfernte MEPs können dynamisch gelernt werden oder es kann als Fehler gewertet werden, wenn eine konfigurierte entfernte MEP nicht gefunden wurde.

**Keine**

Nicht konfigurierte MEPs werden in die Statustabelle aufgenommen und gehen auch in die Bedingungen RDICCM und MACstatus ein.

**Ja**

Nicht konfigurierte MEPs werden in die Statustabelle aufgenommen, gehen aber nicht in die Bedingungen RDICCM und MACstatus ein. Sie lösen ErrorCCM aus.

**Streng**

Nicht konfigurierte MEPs werden nicht in die Statustabelle aufgenommen, gehen nicht in die Bedingungen RDICCM und MACstatus ein. Sie lösen ErrorCCM aus.

**LBM-Responder**

Definiert, ob das Gerät auf CFM-Loopback-Nachrichten (Ethernet-Ping) antworten soll. Die Funktion ist unabhängig vom CCM-Betriebsmodus verwendbar.

**LTM-Responder**

Definiert, ob das Gerät auf CFM-Linktrace-Nachrichten (Ethernet-Traceroute) antworten soll. Die Funktion ist unabhängig vom CCM-Betriebsmodus verwendbar.

**Entfernte MEPs**

In dieser Tabelle können optional entfernte MEPs definiert werden, die das Gerät auf der entfernten Seite erwartet. In LANconfig konfigurieren Sie diese unter **Sonstige Dienste > Dienste > OAM (Operation, Administration, Management) > Entfernte MEPs**.

The screenshot shows a dialog box titled 'Entfernte MEPs - Neuer Eintrag'. It has a standard window title bar with a question mark and a close button. Inside the dialog, there are four text input fields stacked vertically, labeled 'Wartungsdomäne:', 'Wartungsassoziierung:', 'MEPID:', and 'Entfernte MEPID:'. At the bottom of the dialog, there are two buttons: 'OK' and 'Abbrechen'.

**Wartungsdomäne**

Definiert den Namen der Wartungsdomäne (Maintenance Domain (MD)).

**Wartungsassoziierung**

Definiert den Namen der Wartungsassoziierung (Maintenance Association (MA)).

**MEPID**

Definiert die Maintenance Endpoint ID des Geräts für diesen Eintrag (1-8191). Diese muss auf jedem Gerät eindeutig sein.

**Entfernte MEPID**

Definiert die entfernte MEPID, die für diese Konfiguration erwartet wird (1-8191). Diese muss auf jedem Gerät eindeutig sein.

**Kommandos auf der Konsole****Ethping**



```
ethping -i <Schnittstelle> [-?] [-c Anzahl] [-v VLAN] [-s Groesse] [-l MD-Level] <Zieladresse>
```

**Beispiel:** Um CFM-Ethernet-Ping zu verwenden ist eine minimale Konfiguration in der Tabelle Ethernet-CFM-Schnittstellen notwendig. Auf dem zweiten Gerät ist eine entsprechende Konfiguration ebenso notwendig, die MEPID muss sich allerdings unterscheiden bzw. eindeutig sein. In diesem Beispiel wird das MD-Level 7 verwendet.

```
root@:/
> ethping -i LAN-1 -l 7 00:a0:57:9c:47:fd
 60 Byte Packet from 00:a0:57:9c:47:fd, seq.no=3109236825, time=0.130 ms
 60 Byte Packet from 00:a0:57:9c:47:fd, seq.no=3109236826, time=0.126 ms
 60 Byte Packet from 00:a0:57:9c:47:fd, seq.no=3109236827, time=0.125 ms

---00:a0:57:9c:47:fd ping statistic---
3 Packets transmitted, 3 Packets received, 0% loss
```

Statt den CFM-Ethernet-Ping an eine Ethernet-Unicast-MAC-Adresse zu senden, kann auch die standardisierte Multicast-Gruppe verwendet werden. Dabei ist der Aufbau der Multicast-Adresse wie folgt: 01:80:C2:00:00:3x. Dabei ist x ein Wert zwischen 0 und 7 und entspricht der Nummer des Domain Level für den MEP.

## Ergänzungen im Setup-Menü

### CFM-Schnittstellen

In dieser Tabelle werden die CFM-Parameter für die jeweilige Schnittstelle definiert.

#### SNMP-ID:

2.105.3

#### Pfad Konsole:

Setup > OAM

**Schnittstelle**

Schnittstelle auf der CFM aktiviert werden soll, mögliche Werte sind LAN-Schnittstellen wie z. B. LAN-1 oder WAN-Schnittstellen wie DSL-1.

**SNMP-ID:**

2.105.3.1

**Pfad Konsole:**

**Setup > OAM > CFM-Schnittstellen**

**Mögliche Werte:**

max. 18 Zeichen aus `[A-Z][0-9]@{|}~!$%&'()+-./:;<=>?[\]^_.`

**Default-Wert:**

*leer*

**MD-Ebene**

Definiert das Maintenance Domain Level für diese Schnittstelle.

**SNMP-ID:**

2.105.3.2

**Pfad Konsole:**

**Setup > OAM > CFM-Schnittstellen**

**Mögliche Werte:**

0 ... 7

**Default-Wert:**

0

**VLANs**

Definiert die VLANs auf der Schnittstelle, mit der CFM-Nachrichten empfangen und gesendet werden können. Es kann entweder ein VLAN oder eine komma-separierte Liste von VLANs konfiguriert werden.

**SNMP-ID:**

2.105.3.3

**Pfad Konsole:**

**Setup > OAM > CFM-Schnittstellen**

**Mögliche Werte:**

max. 50 Zeichen aus `[0-9],-/`

**Default-Wert:***leer***Besondere Werte:***leer*

Alle VLANs werden akzeptiert.

**In-Betrieb**

Aktiviert oder Deaktiviert CFM auf der konfigurierten Schnittstelle.

**SNMP-ID:**

2.105.3.4

**Pfad Konsole:****Setup > OAM > CFM-Schnittstellen****Mögliche Werte:****Nein**

CFM deaktiviert.

**Ja**

CFM aktiviert.

**Default-Wert:**

Nein

**Endpunkt-Typ**

Definiert den CFM-Endpunkt-Typ.

**SNMP-ID:**

2.105.3.5

**Pfad Konsole:****Setup > OAM > CFM-Schnittstellen****Mögliche Werte:****MEP**

Der Maintenance Association End Point (MEP) stellt die Grenze einer Domain dar und führt die Fehlererkennung zwischen den Domain-Grenzen durch. Der MEP erstellt und sendet CFM-Pakete.

**MIP**

Der Maintenance Intermediate Point (MIP) befindet sich innerhalb der Domain und führt die Pfad- und Fehler-Erkennung innerhalb der Domain-Grenzen durch. Der MIP antwortet auf CFM-Pakete.

**Default-Wert:**

MEP

**Wartungs-Domaene**

Definiert den Namen der Wartungsdomäne (Maintenance Domain (MD)).

**SNMP-ID:**

2.105.3.6

**Pfad Konsole:****Setup > OAM > CFM-Schnittstellen****Mögliche Werte:**max. 43 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+,-./:;<=>?[\]^_`~``**Default-Wert:***leer***Wartungs-Assoziierung**

Definiert den Namen der Wartungsassoziiierung (Maintenance Association (MA)).

**SNMP-ID:**

2.105.3.7

**Pfad Konsole:****Setup > OAM > CFM-Schnittstellen****Mögliche Werte:**max. 45 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+,-./:;<=>?[\]^_`~``**Default-Wert:***leer***MEPID**

Definiert die Maintenance Endpoint ID des Geräts für diesen Eintrag. Diese muss auf jedem Gerät eindeutig sein.

**SNMP-ID:**

2.105.3.8

**Pfad Konsole:****Setup > OAM > CFM-Schnittstellen**

**Mögliche Werte:**

1 ... 8191

**Sender-ID**

Definiert die optionale Sender-ID in CFM-CCM-Nachrichten.

**SNMP-ID:**

2.105.3.9

**Pfad Konsole:****Setup > OAM > CFM-Schnittstellen****Mögliche Werte:**

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

**Default-Wert:***leer***CoS**

Definiert den Class-of-Service mit dem CFM-CCM (Continuity Check Message)-Pakete markiert werden.

**SNMP-ID:**

2.105.3.10

**Pfad Konsole:****Setup > OAM > CFM-Schnittstellen****Mögliche Werte:****Best-Effort**  
**Background**  
**Excellent-Effort**  
**Controlled-Latency**  
**Video**  
**Voice**  
**Network-Control****Default-Wert:**

Best-Effort

**LBM-Responder**

Definiert, ob das Gerät auf CFM-Loopback-Nachrichten (Ethernet-Ping) antworten soll. Die Funktion ist unabhängig vom CCM-Betriebsmodus verwendbar.

**SNMP-ID:**

2.105.3.11

**Pfad Konsole:****Setup > OAM > CFM-Schnittstellen****Mögliche Werte:**Nein  
Ja**Default-Wert:**

Nein

**LTM-Responder**

Definiert, ob das Gerät auf CFM-Linktrace-Nachrichten (Ethernet-Traceroute) antworten soll. Die Funktion ist unabhängig vom CCM-Betriebsmodus verwendbar.

**SNMP-ID:**

2.105.3.21

**Pfad Konsole:****Setup > OAM > CFM-Schnittstellen****Mögliche Werte:**Nein  
Ja**Default-Wert:**

Nein

**CCM-Initiator**

Definiert, ob das Gerät regelmäßige CCM-Nachrichten (Continuity Check Message) versenden soll.

**SNMP-ID:**

2.105.3.31

**Pfad Konsole:****Setup > OAM > CFM-Schnittstellen**

**Mögliche Werte:**

**Nein**  
**Ja**

**Default-Wert:**

Nein

**CCM-Intervall**

Definiert, mit welchem Intervall CCM-Nachrichten (Continuity Check Message) von dem Gerät versendet werden sollen. CCM-Intervalle müssen zwischen Kommunikationspartnern einheitlich sein.

**SNMP-ID:**

2.105.3.32

**Pfad Konsole:**

**Setup > OAM > CFM-Schnittstellen**

**Mögliche Werte:**

**3.333-msek**  
Intervall von 3,333 Millisekunden.

**10-msek**  
Intervall von 10 Millisekunden.

**100-msek**  
Intervall von 100 Millisekunden.

**1-sek**  
Intervall von einer Sekunde.

**10-sek**  
Intervall von 10 Sekunden.

**1-min**  
Intervall von einer Minute.

**10-min**  
Intervall von 10 Minuten.

**Default-Wert:**

3.333-msek

**CCM-niedrigste-Alarm-Prio**

Definiert, wie schwerwiegend festgestellte Fehler mindestens sein müssen, damit der MEP das RDI-Flag (Remote Defect Indication) setzt und in CCM-Paketen propagiert. Level, in aufsteigender Schwere, sind: RDICCM, MACstatus, RemoteCCM, ErrorCCM, XconCCM.

**SNMP-ID:**

2.105.3.33

**Pfad Konsole:****Setup > OAM > CFM-Schnittstellen****Mögliche Werte:****RDICCM**

Von mindestens einem anderen MEP wurde ein CCM-Frame mit gesetztem RDI empfangen.

**MACstatus**

Mindestens ein anderer MEP hat einen Interface-Status ungleich 'up' gemeldet (z.B. Hardware-Problem), oder alle anderen MEPs melden einen PortStatus ungleich 'up' (z.B. Netzsegment isoliert).

**RemoteCCM**

Mindestens von einem konfigurierten MEP werden keine CCM-Frames empfangen.

**ErrorCCM**

Ein weiterer MEP verwendet die gleiche MEPID wie das lokale Gerät oder es werden CCMs von einem nicht konfigurierten MEP empfangen (falls Matching ungleich none), oder ein anderer MEP verwendet ein abweichendes CCM-Intervall.

**XconCCM**

Es wurden CCs von einem anderen MEP mit niedrigerem MD-Level empfangen, oder mit einer abweichenden Domain oder Association.

**Default-Wert:**

MACstatus

**CCM-Empfänger**

Definiert, ob das Gerät CCM-Nachrichten verarbeiten bzw. empfangen soll.

**SNMP-ID:**

2.105.3.41

**Pfad Konsole:****Setup > OAM > CFM-Schnittstellen****Mögliche Werte:****Nein****Ja****Default-Wert:**

Nein



### Entfernte-MEP-Verknuepfung

Definiert, wie das Gerät die Anwesenheit von entfernten MEPs behandeln soll. Beliebige entfernte MEPs können dynamisch gelernt werden oder es kann als Fehler gewertet werden, wenn eine konfigurierte entfernte MEP nicht gefunden wurde.

**SNMP-ID:**

2.105.3.42

**Pfad Konsole:****Setup > OAM > CFM-Schnittstellen****Mögliche Werte:****Keines**

Nicht konfigurierte MEPs werden in die Statustabelle aufgenommen und gehen auch in die Bedingungen RDICCM und MACstatus ein.

**Ja**

Nicht konfigurierte MEPs werden in die Statustabelle aufgenommen, gehen aber nicht in die Bedingungen RDICCM und MACstatus ein. Sie lösen ErrorCCM aus.

**Strikt**

Nicht konfigurierte MEPs werden nicht in die Statustabelle aufgenommen, gehen nicht in die Bedingungen RDICCM und MACstatus ein. Sie lösen ErrorCCM aus.

**Default-Wert:**

Keines

### Entfernte-MEPs

In dieser Tabelle können optional entfernte MEPs definiert werden, die das Gerät auf der entfernten Seite erwartet.

**SNMP-ID:**

2.105.5

**Pfad Konsole:****Setup > OAM**

### Wartungs-Domaene

Definiert den Namen der Wartungsdomäne (Maintenance Domain (MD)).

**SNMP-ID:**

2.105.5.1

**Pfad Konsole:****Setup > OAM > Entfernte-MEPs**

**Mögliche Werte:**

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

**Default-Wert:**

*leer*

**Wartungs-Assoziierung**

Definiert den Namen der Wartungsassoziierung (Maintenance Association (MA)).

**SNMP-ID:**

2.105.5.2

**Pfad Konsole:**

**Setup > OAM > Entfernte-MEPs**

**Mögliche Werte:**

max. 45 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+,-./:;<=>?[\]^_`~``

**Default-Wert:**

*leer*

**MEPID**

Definiert die Maintenance Endpoint ID des Geräts für diesen Eintrag. Diese muss auf jedem Gerät eindeutig sein.

**SNMP-ID:**

2.105.5.3

**Pfad Konsole:**

**Setup > OAM > Entfernte-MEPs**

**Mögliche Werte:**

1 ... 8191

**Entfernte-MEPID**

Definiert die entfernte MEPID, die für diese Konfiguration erwartet wird.

**SNMP-ID:**

2.105.5.4

**Pfad Konsole:**

**Setup > OAM > Entfernte-MEPs**

**Mögliche Werte:**

1 ... 8191

## 13.3 Eingabemöglichkeiten bei der Cron-Tabelle bereinigt

Ab LCOS 10.90 wurden die möglichen Eingaben bei einigen Parametern der Cron-Tabelle auf die möglichen Zeichen beschränkt. Dadurch werden fehlerhafte Eingaben verhindert.

In LANconfig finden Sie die Cron-Tabelle unter **Datum/Zeit > Allgemein > Cron-Tabelle**. In der CLI unter **Setup > Config > Cron-Tabelle**.

### 13.3.1 Ergänzungen im Setup-Menü

#### Minute

Der Wert definiert den Zeitpunkt, an dem ein Kommando ausgeführt werden soll. Wird kein Wert angegeben, so wird er auch nicht in die Steuerung einbezogen. Es kann auch eine Kommaseparierte Liste von Werten, oder aber ein Bereich eingegeben werden. Mit / kann eine Schrittweite angegeben werden. Falls ein Bereich vor der Schrittweite angegeben wird, dann bezieht sich diese auf den angegebenen Bereich. Minutenangaben erfolgen von 0 bis 59.

Beispiele:

- > /10 – Alle 10 Minuten
- > 0,10,20,30,40,50 – Alle 10 Minuten
- > 0-30/5 – Alle 5 Minuten innerhalb der ersten halben Stunde
- > 0-59 – Jede Minute
- > 25-30 – In den Minuten 25 bis 30
- > 25,26,27,28,29,30 – In den Minuten 25 bis 30
- > 55-5 – In den Minuten 55 bis 5
- > 55,56,57,58,59,0,1,2,3,4,5 – In den Minuten 55 bis 5

**SNMP-ID:**

2.11.20.2

**Pfad Konsole:****Setup > Config > Cron-Tabelle****Mögliche Werte:**

max. 50 Zeichen aus [0-9] , - /

**Default-Wert:***leer***Stunde**

Der Wert definiert den Zeitpunkt, an dem ein Kommando ausgeführt werden soll. Wird kein Wert angegeben, so wird er auch nicht in die Steuerung einbezogen. Es kann auch eine Kommaseparierte Liste von Werten, oder aber ein Bereich eingegeben werden. Mit / kann eine Schrittweite angegeben werden. Falls ein Bereich vor der Schrittweite angegeben wird, dann bezieht sich diese auf den angegebenen Bereich. Stundenangaben erfolgen von 0 bis 23.

Beispiele:

- > /4 – Alle 4 Stunden
- > 0,4,8,12,16,20 – Alle 4 Stunden
- > 8-20/2 – Alle 2 Stunden zwischen 8 und 20 Uhr
- > 0-23 – Jede Stunde
- > 13-16 – In den Stunden 13 bis 16
- > 13,14,15,16 – In den Stunden 13 bis 16
- > 22-1 – In den Stunden 22 bis 1
- > 22,23,0,1 – In den Stunden 22 bis 1

**SNMP-ID:**

2.11.20.3

**Pfad Konsole:****Setup > Config > Cron-Tabelle****Mögliche Werte:**

max. 50 Zeichen aus [0-9] , - /

**Default-Wert:***leer***Wochentag**

Der Wert definiert den Zeitpunkt, an dem ein Kommando ausgeführt werden soll. Wird kein Wert angegeben, so wird er auch nicht in die Steuerung einbezogen. Es kann auch eine Kommaseparierte Liste von Werten, oder aber ein Bereich eingegeben werden. Mit / kann eine Schrittweite angegeben werden. Falls ein Bereich vor der Schrittweite angegeben wird, dann bezieht sich diese auf den angegebenen Bereich. Wochentagsangaben erfolgen von 0 (Sonntag) bis 6 (Samstag). Für Beispiele der Syntax siehe Minute oder Stunde.

**SNMP-ID:**

2.11.20.4

**Pfad Konsole:****Setup > Config > Cron-Tabelle****Mögliche Werte:**

max. 50 Zeichen aus [0-9] , - /

**Default-Wert:***leer***Tag**

Der Wert definiert den Zeitpunkt, an dem ein Kommando ausgeführt werden soll. Wird kein Wert angegeben, so wird er auch nicht in die Steuerung einbezogen. Es kann auch eine Kommaseparierte Liste von Werten, oder aber ein Bereich eingegeben werden. Mit / kann eine Schrittweite angegeben werden. Falls ein Bereich vor der Schrittweite angegeben wird, dann bezieht sich diese auf den angegebenen Bereich. Tagesangaben erfolgen von 1 bis 31. Für Beispiele der Syntax siehe Minute oder Stunde.

**SNMP-ID:**

2.11.20.5

**Pfad Konsole:****Setup > Config > Cron-Tabelle****Mögliche Werte:**

max. 50 Zeichen aus [0-9] , - /

**Default-Wert:***leer***Monat**

Der Wert definiert den Zeitpunkt, an dem ein Kommando ausgeführt werden soll. Wird kein Wert angegeben, so wird er auch nicht in die Steuerung einbezogen. Es kann auch eine Kommaseparierte Liste von Werten, oder aber ein Bereich eingegeben werden. Mit / kann eine Schrittweite angegeben werden. Falls ein Bereich vor der Schrittweite angegeben wird, dann bezieht sich diese auf den angegebenen Bereich. Nonatsangaben erfolgen von 1 (Januar) bis 12 (Dezember). Für Beispiele der Syntax siehe Minute oder Stunde.

**SNMP-ID:**

2.11.20.6

**Pfad Konsole:****Setup > Config > Cron-Tabelle****Mögliche Werte:**

max. 50 Zeichen aus [0-9] , - /

**Default-Wert:***leer*

## 13.4 Erweiterungen beim Alive-Test

Ab LCOS 10.90 können Sie beim Alive-Test weitere Ziel-Adressen und eine Wiederherstellungs-Aktion konfigurieren.

Mit dem Alive-Test können Sie die Erreichbarkeit von IPv4-Adressen mittels Ping prüfen. Falls keine Antwort kommt oder nach Nichterreichbarkeit wieder erreichbar wird, dann kann das Gerät eine konfigurierbare Aktion ausführen.

In LANconfig konfigurieren Sie den Alive-Test unter **IPv4 > Allgemein > Alive-Test**.

**Alive-Test**

Mit dem Alive-Test kann die Erreichbarkeit einer Ziel-Adresse durch PING geprüft werden. Das Gerät führt die unten angegebene Aktion aus, wenn die Ziel-Adresse nicht antwortet.

1. Ziel-Adresse:

2. Ziel-Adresse:

3. Ziel-Adresse:

4. Ziel-Adresse:

Test-Intervall:  Sekunden

Anzahl Wiederholungen:

Wiederholungs-Intervall:  Sekunden

Anzahl Fehler für Reaktion:

Absende-Adresse (opt.):

Reaktion:

Benutzer-definierter Befehl:

Wiederherst. Ben.-def. Befehl:

### Ziel-Adresse 1-4

Bis zu vier mögliche Ziel-IPv4-Adressen, an welche das Gerät einen Ping sendet. Es muss nur eine Adresse erreichbar sein, damit der Alive-Test als erfolgreich gilt.

### Wiederherstellungs-Benutzer-definierter Befehl

Als Wiederherstellungs-Aktion kann jeder auf der Konsole ausführbare Befehl angegeben werden. Dieser wird einmalig ausgeführt, wenn das Gerät vom Fehlerzustand der Nichterreichbarkeit der Zieladresse in den Fall übergeht, wo die konfigurierte Zieladresse wieder erreichbar ist.



Die hier eingestellte Aktion wird nur ausgeführt, wenn die **Reaktion** auf den Wert **Benutzer-definierter Befehl** eingestellt ist.

### 13.4.1 Ergänzungen im Setup-Menü

#### Wiederherstellungs-Aktion

Als Wiederherstellungs-Aktion kann jeder auf der Konsole ausführbare Befehl angegeben werden. Dieser wird einmalig ausgeführt, wenn das Gerät vom Fehlerzustand der Nichterreichbarkeit der Zieladresse in den Fall übergeht, wo die konfigurierte Zieladresse wieder erreichbar ist.

**SNMP-ID:**

2.7.21.9

**Pfad Konsole:**

**Setup > TCP-IP > Alive-Test**

**Mögliche Werte:**

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

**Default-Wert:**

*leer*

**Ziel-Adresse-2**

Eine von vier möglichen Ziel-IPv4-Adressen, an welche das Gerät einen Ping sendet. Es muss nur eine Adresse erreichbar sein, damit der Alive-Test als erfolgreich gilt.

**SNMP-ID:**

2.7.21.11

**Pfad Konsole:**

**Setup > TCP-IP > Alive-Test**

**Mögliche Werte:**

max. 15 Zeichen aus [0-9].

**Ziel-Adresse-3**

Eine von vier möglichen Ziel-IPv4-Adressen, an welche das Gerät einen Ping sendet. Es muss nur eine Adresse erreichbar sein, damit der Alive-Test als erfolgreich gilt.

**SNMP-ID:**

2.7.21.12

**Pfad Konsole:**

**Setup > TCP-IP > Alive-Test**

**Mögliche Werte:**

max. 15 Zeichen aus [0-9].

**Ziel-Adresse-4**

Eine von vier möglichen Ziel-IPv4-Adressen, an welche das Gerät einen Ping sendet. Es muss nur eine Adresse erreichbar sein, damit der Alive-Test als erfolgreich gilt.

**SNMP-ID:**

2.7.21.13

**Pfad Konsole:**

**Setup > TCP-IP > Alive-Test**

**Mögliche Werte:**

max. 15 Zeichen aus [0-9].



## 14 Ergänzungen im Menüsystem

### 14.1 Ergänzungen im Setup-Menü

#### 14.1.1 Max-Auth-Versuche

Definiert, wie viele mögliche Versuche der Public Key Authentifizierung nacheinander möglich sind. Wird der konfigurierte Wert erreicht, beendet der SSH-Server die Verbindung.

**SNMP-ID:**

2.11.28.20

**Pfad Konsole:**

Setup > Config > SSH

**Mögliche Werte:**

max. 5 Zeichen aus [0-9]

**Default-Wert:**

6

**Besondere Werte:**

0

Funktion deaktiviert.

#### 14.1.2 Kommentar

Vergeben Sie optional einen sinnvollen Kommentar als Beschreibung.

**SNMP-ID:**

2.23.30.10

**Pfad Konsole:**

Setup > Schnittstellen > Ethernet-Ports

**Mögliche Werte:**

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

#### 14.1.3 SFP-Ports

Hier finden Sie Einstellungen zu den SFP-Port-Schnittstellen des Gerätes

**SNMP-ID:**

2.23.31

**Pfad Konsole:****Setup > Schnittstellen****Port**

Der Name des gewählten Ports.

**SNMP-ID:**

2.23.31.1

**Pfad Konsole:****Setup > Schnittstellen > SFP-Ports****Autoneg-Bypass**

Falls bei eingeschalteter Auto-Negotiation eine optische Gegenstelle erkannt wurde, aber die Verhandlung nicht abgeschlossen werden kann, versuche alternativ eine Verbindung ohne Auto-Negotiation.

**SNMP-ID:**

2.23.31.2

**Pfad Konsole:****Setup > Schnittstellen > SFP-Ports****Mögliche Werte:****Ja**  
**Nein**

## 14.1.4 Datenmodell

Mit diesem Eintrag definieren Sie das CWMP-Datenmodell.

**SNMP-ID:**

2.44.18

**Pfad Konsole:****Setup > CWMP**

**Mögliche Werte:**

TR-098  
TR-181

**Default-Wert:**

TR-181

## 14.1.5 System-Boot

Über diese Aktion bewirken Sie den manuellen Neustart des Gerätes. Über einen der Parameter lässt sich dieser auch zeitgesteuert später ausführen bzw. ein später erfolgender Neustart wieder löschen.

Diese Funktion kann für Szenarien verwendet werden, in denen kritische Konfigurationen auf dem Gerät geändert werden müssen, bei denen eine Fehlkonfiguration (z. B. WAN-Verbindung oder Managementverbindung) zur Nicht-Erreichbarkeit des Gerätes führen könnte. Das Kommando kann in Zusammenhang mit dem Testmodus „flash no“ verwendet werden, in dem Konfigurationsänderungen nicht persistent im Flash gespeichert werden. Anwendungsbeispiel:

1. Es wird auf der CLI zunächst „flash no“ durchgeführt.
2. Setzen eines zeitgesteuerten Reboots in 30 Minuten, z .B. `do /Sonstiges/System-Boot 30m`
3. Durchführung von kritischen Konfigurationsänderungen.
4. > Falls die Änderungen erfolgreich waren, kann der Reboot-Timer gestoppt werden mit „`do /Sonstiges/System-Boot stop`“ und anschließend wieder in „flash yes“ gewechselt werden.  
> Falls die Änderungen zu einer Nicht-Erreichbarkeit führen, bootet das Gerät nach 30 Minuten automatisch mit der alten Konfiguration wie vor dem „flash no“ neu.

**SNMP-ID:**

4.2

**Pfad Konsole:**

Sonstiges

**Mögliche Argumente:**

**<num>s**

Neustart nach vorgegebener Dauer in Sekunden, Beispiel: `do /sonstiges/system-boot 10s`

**<num>m**

Neustart nach vorgegebener Dauer in Minuten, Beispiel: `do /sonstiges/system-boot 10m`

**<num>h**

Neustart nach vorgegebener Dauer in Stunden, Beispiel: `do /sonstiges/system-boot 10h`

**stop**

Timer stoppen, Beispiel: `do /sonstiges/system-boot stop`

## 14.1.6 Kaltstart

Mit dieser Aktion können Sie das Gerät neu booten. Über einen der Parameter lässt sich der Kaltstart auch zeitgesteuert später ausführen bzw. ein später erfolgender Neustart wieder löschen.

Diese Funktion kann für Szenarien verwendet werden, in denen kritische Konfigurationen auf dem Gerät geändert werden müssen, bei denen eine Fehlkonfiguration (z. B. WAN-Verbindung oder Managementverbindung) zur Nicht-Erreichbarkeit des Gerätes führen könnte. Das Kommando kann in Zusammenhang mit dem Testmodus „flash no“ verwendet werden, in dem Konfigurationsänderungen nicht persistent im Flash gespeichert werden. Anwendungsbeispiel:

1. Es wird auf der CLI zunächst „flash no“ durchgeführt.
2. Setzen eines zeitgesteuerten Kaltstarts in 30 Minuten, z .B. do /Sonstiges/Kaltstart 30m
3. Durchführung von kritischen Konfigurationsänderungen.
4. > Falls die Änderungen erfolgreich waren, kann der Reboot-Timer gestoppt werden mit „do /Sonstiges/Kaltstart stop“ und anschließend wieder in „flash yes“ gewechselt werden.  
> Falls die Änderungen zu einer Nicht-Erreichbarkeit führen, bootet das Gerät nach 30 Minuten automatisch mit der alten Konfiguration wie vor dem „flash no“ neu.

**SNMP-ID:**

4.5

**Pfad Konsole:****Sonstiges****Mögliche Argumente:****<num>s**

Neustart nach vorgegebener Dauer in Sekunden, Beispiel: do /sonstiges/kaltstart 10s

**<num>m**

Neustart nach vorgegebener Dauer in Minuten, Beispiel: do /sonstiges/kaltstart 10m

**<num>h**

Neustart nach vorgegebener Dauer in Stunden, Beispiel: do /sonstiges/kaltstart 10h

**stop**

Timer stoppen, Beispiel: do /sonstiges/kaltstart stop

## 15 Entfallene Features

Ab LCOS 10.90 sind die folgenden Features entfallen:

- > AsyncPPP (2.2.4.5)
- > CLIP bei RAS-Einwahl (2.2.22.6, 2.2.22.7)
- > Parameter Datenrate in 2.23.7 entfernt (2.23.7.21)
- > IKEv1/VPN-Algorithmen cast128\_cbc, blowfish\_cbc und DES
- > ISDN-Gegenstellentabelle ohne Wählverbindungen (2.2.2.4, 2.2.2.6, 2.2.3, 2.2.6, 2.2.7, 2.2.8, 2.2.9, 2.2.10, 2.2.11, 2.15, 2.3.3, 2.3.4, 2.3.5, 2.3.6, 2.3.15)
- > ISDN-Standortverifikation (2.11.31.2, 2.11.31.3, 2.11.31.4, 2.11.31.6, 2.11.31.7)
- > ISDN-Zeitbezug (2.3.1, 2.3.13, 2.14.3, 2.14.5)
- > LANcapi (2.11.9, 2.13, 2.15.2)
- > Least Cost Router (2.15)
- > myVPN (2.19.28)
- > NetBIOS-Proxy (1.9.8, 2.16)
- > NetBIOS-Support bezüglich DHCP und PPP (1.6.8.3.4, 1.6.8.3.6, 1.6.9.3.4, 1.6.9.3.6, 1.9.6.20.9, 1.9.6.20.10, 1.27.9.10, 1.27.9.13, 1.32.20.7, 1.32.20.8, 1.32.21.7, 1.32.21.8, 1.84.7.11, 1.84.7.12, 2.2.20.7, 2.2.20.8, 2.7.9, 2.7.10, 2.8.23.7, 2.8.23.8, 2.10.20.9, 2.10.20.10, 2.17.4, 2.17.15.5)
- > X.25 Bridge (2.2.45)