

LCOS 10.90

Addendum

10/2024



LANCOM
SYSTEMS

Inhalt

1 Addendum zur LCOS-Version 10.90.....	5
2 Konfiguration.....	6
2.1 Änderung des automatischen Ladens von USB.....	6
3 Diagnose.....	7
3.1 Unterstützung von TLS beim Syslog-Client.....	7
3.1.1 Ergänzungen im Setup-Menü.....	8
3.2 Syslog-Nachrichten nach dem Standard RFC 5424.....	9
3.2.1 Ergänzungen im Setup-Menü.....	9
4 Sicherheit.....	10
4.1 Ergänzungen im Setup-Menü.....	10
4.1.1 Passwortkomplexität.....	10
5 Quality-of-Service.....	12
5.1 Quality-of-Service (QoS) mit 8 Queues.....	12
5.1.1 Queues.....	12
5.1.2 Queue-Listen.....	14
5.1.3 Schnittstellen.....	15
5.1.4 Paketstau-Aktion.....	15
5.1.5 Beispiel 1: Konfiguration eines QoS-Konzepts mit vier Klassen.....	16
5.1.6 Beispiel 2: Konfiguration eines QoS-Konzepts am VDSL-Anschluss mit zwei QoS-Klassen.....	19
5.1.7 Queue-Nutzung in der Firewall.....	21
5.1.8 Ergänzungen im Setup-Menü.....	24
6 Virtual Private Networks – VPN.....	34
6.1 MOBIKE.....	34
6.1.1 Ergänzungen im Setup-Menü.....	34
6.2 IKEv2 Post-quantum Preshared Keys (PPK).....	35
6.2.1 Ergänzungen im Setup-Menü.....	38
6.3 Null-Verschlüsselung in der IKEv2 Child-SA.....	40
6.3.1 Ergänzungen im Setup-Menü.....	41
6.4 IKE-CFG schickt Subnetzmaske für die verhandelte IP-Adresse mit.....	42
6.4.1 Ergänzungen im Setup-Menü.....	43
7 Public Spot.....	45
7.1 Public Spot Captive Portal API.....	45
7.1.1 Ergänzungen im Setup-Menü.....	47
8 Backup-Lösungen.....	49
8.1 VRRPv3.....	49
8.1.1 Interaktion mit dem WAN-Backup-Modul.....	49
8.1.2 Steuerung des WAN/WAN-Backup durch das VRRP.....	49
8.1.3 Konfiguration von VRRPv3.....	49

8.1.4 Ergänzungen im Setup-Menü.....	52
9 RADIUS.....	61
9.1 Ergänzungen im Setup-Menü.....	61
9.1.1 Msg-Authenticator-erforderlich.....	61
9.1.2 L2TP-Msg-Authenticator-erforderlich.....	61
9.1.3 Msg-Authenticator-erforderlich.....	62
9.1.4 Msg-Authenticator-erforderlich.....	62
9.1.5 Backup-Msg-Authenticator-erforderlich.....	63
9.1.6 Msg-Authenticator-erforderlich.....	63
9.1.7 Msg-Authenticator-erforderlich.....	64
9.1.8 Msg-Authenticator-erforderlich.....	64
9.1.9 Msg-Authenticator-erforderlich.....	65
10 Weitere Dienste.....	66
10.1 Unterstützung für MTU 1500 im PPPoE nach RFC 4638.....	66
10.1.1 Ergänzungen im Setup-Menü.....	67
11 Ergänzungen im Menüsystem.....	68
11.1 Ergänzungen im Setup-Menü.....	68
11.1.1 Kommentar.....	68
11.1.2 Datenmodell.....	68
11.1.3 System-Boot.....	68
11.1.4 Kaltstart.....	69
12 Entfallene Features.....	71

Copyright

© 2024 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).

Produkte von LANCOM Systems enthalten kryptographische Software, die von Eric Young (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

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.

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**.

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 Ergänzungen im Setup-Menü

4.1.1 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

Komplexitätsklassen

Konfigurieren Sie hier die notwendige Anzahl an unterschiedlichen Komplexitätsklassen für Passwörter. Komplexitätsklassen sind Buchstaben, Ziffern, 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 ... 3

Default-Wert:

3

5 Quality-of-Service

5.1 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...

5.1.1 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 15 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.

5.1.2 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.

5.1.3 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.

Queue-Liste

Referenziert einen Eintrag aus der Queue-Listen-Tabelle.

5.1.4 Paketstau-Aktion

Die Paketstau-Aktion bestimmt, wie mit einer sich anstauenden Sendequete 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.

5.1.5 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
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**.

- 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

5 Quality-of-Service

Queues - Neuer Eintrag

Name: SILBER

Metrik-Typ: prozent

Commit-Rate: 25

Excess-Rate: 0

Rückfall auf Best Effort: Nein

Paketstau-Aktion: DEFAULT Wählen

DSCP-Tags

<input type="checkbox"/> BE/CS0	<input type="checkbox"/> CS1
<input type="checkbox"/> CS2	<input checked="" 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

OK Abbrechen

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.

Queue-Listen - Neuer Eintrag

Name: MEINE-LISTE

Best Effort Cong. Action: DEFAULT Wählen

Sortierte Liste: VOIP,GOLD,SILBER Wählen

OK Abbrechen

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**.

Schnittstellen - Neuer Eintrag

Schnittstellen: DSL

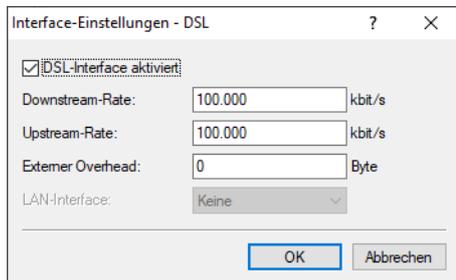
Eintrag aktiv: Ja

Queue-Liste: MEINE-LISTE Wählen

OK Abbrechen

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

5.1.6 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

5.1.7 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.

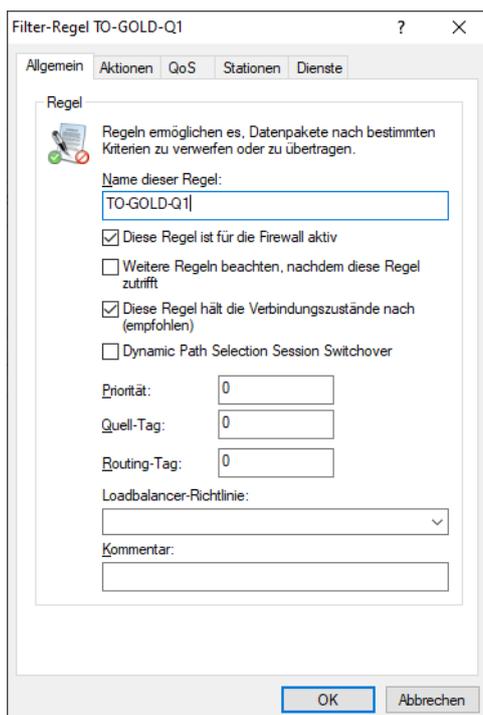
Die Queue-Zuweisung bezieht sich auf Queues, die physikalischen Interfaces zugewiesen wurden, wird aber auf darüber gestapelte Interfaces vererbt, d. h. wenn z. B. das Ziel-Interface einer Session ein VPN-Interface ist, dann propagiert sich die Queue-Zuweisung bis zum physikalischen Interface (WAN) durch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

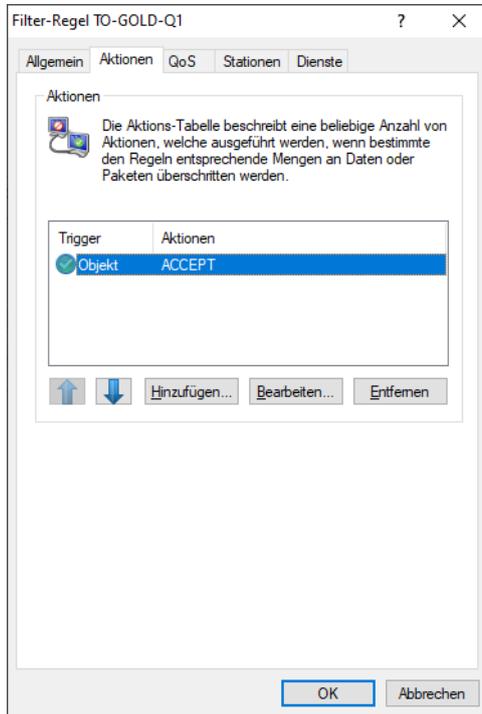
Im Folgenden ein Beispiel für die Vorgehensweise für eine Queuezuweisung:

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.



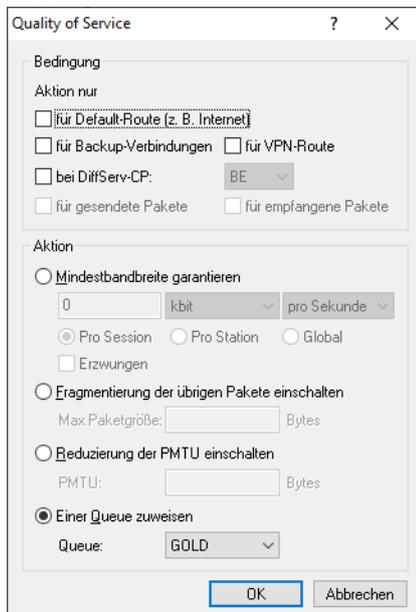
5 Quality-of-Service

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

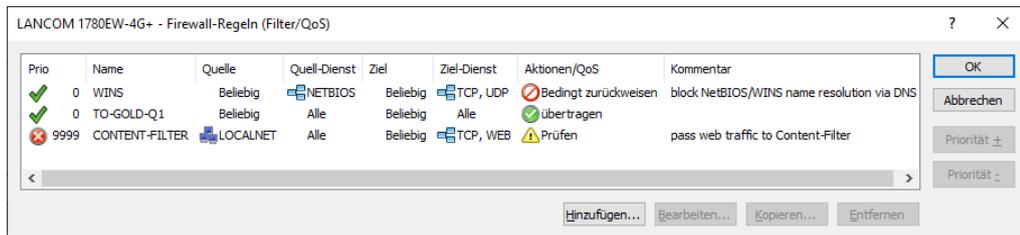


3. Als nächstes fügen Sie auf dem Reiter **QoS** ein neues QoS-Objekt an. Geben Sie diesem auf dem Reiter **Allgemein** einen Namen und weisen Sie dann auf dem Reiter **QoS** diesem die gewünschte Queue zu.

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.



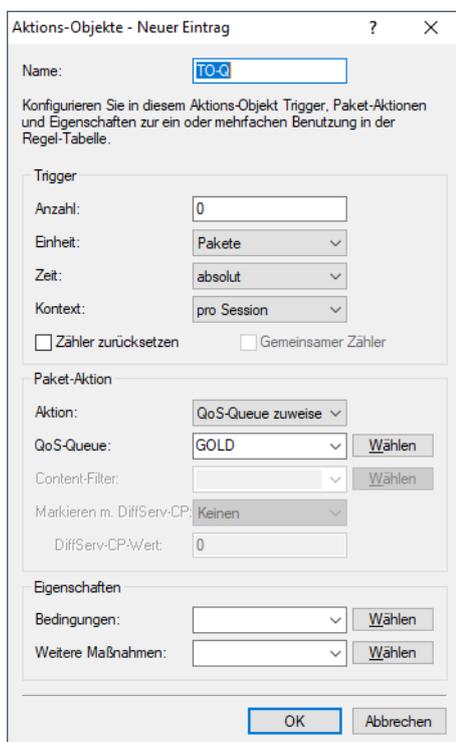
- Als Ergebnis erhalten Sie eine Regel, welche die gewünschten Pakete einer Queue – in diesem Beispiel „GOLD“ – zuweist.



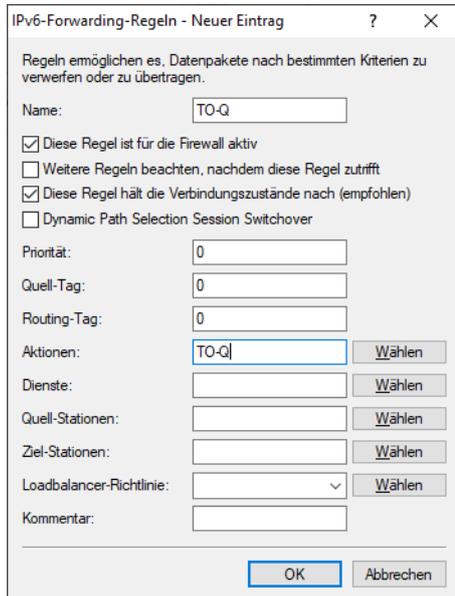
IPv6-Firewall

Im Folgenden ein Beispiel für die Vorgehensweise für eine Queuezuweisung:

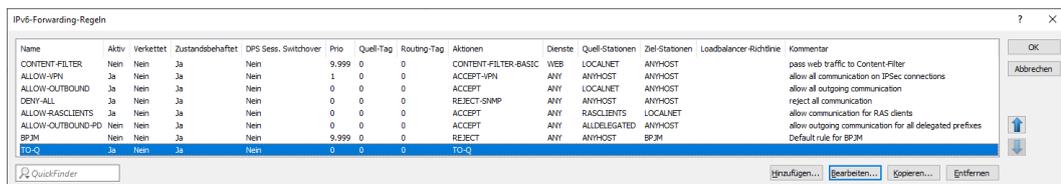
- Eine Queuezuweisung erfolgt über ein in einer IPv6-Forwarding-Regel zugewiesenes Aktions-Objekt. Legen Sie als erstes ein Aktions-Objekt unter **Firewall/QoS > IPv6-Regeln > Firewall-Objekte > Aktions-Objekte** an, in dem Sie die gewünschte Queue zuweisen.



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



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



5.1.8 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 Sendequue 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 26 und [2.2.71.1.4 Grenzwert-Max](#) auf Seite 26 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 28 und [2.2.71.2.4 Excess-Rate](#) auf Seite 29 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 28 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 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 [2.2.71.2.2 Metrik-Typ](#) auf Seite 28 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 > WAN > QoS > 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 > WAN > QoS > 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 25 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:

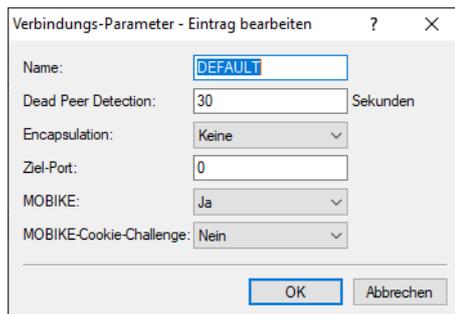
2.2.71.4.3

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

6 Virtual Private Networks – VPN

6.1 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**.



Parameter	Wert
Name	DEFAULT
Dead Peer Detection	30 Sekunden
Encapsulation	Keine
Ziel-Port	0
MOBIKE	Ja
MOBIKE-Cookie-Challenge	Nein

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“).

6.1.1 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

6.2 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

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.

6.2.1 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

6.3 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.

6.3.1 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

6.4 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.

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“).

6.4.1 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

7 Public Spot

7.1 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

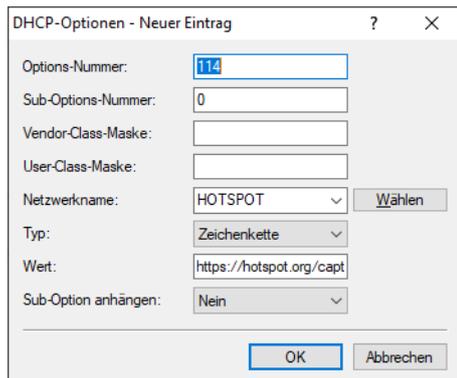
Name des Public Spot-Netzwerks (siehe IPv4-Netzwerke)

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.



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

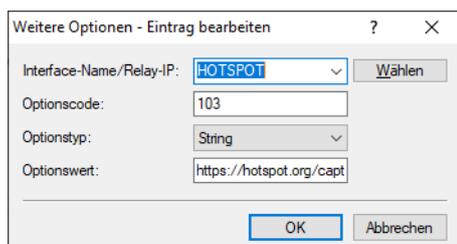
103

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.



7.1.1 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 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.

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]@{|}~!$%&'()+-,/ : ; <=>? [\] ^ _ . ``**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]@{|}~!$%&'()+-,/ : ; <=>? [\] ^ _ . ``**Default-Wert:***leer*

8 Backup-Lösungen

8.1 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.

8.1.1 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.

8.1.2 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.

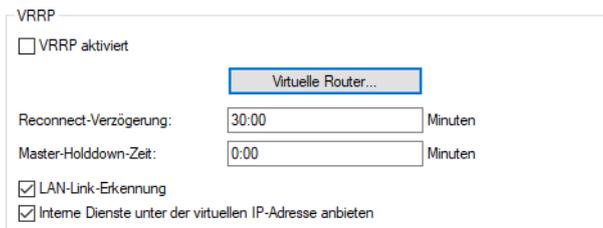
8.1.3 Konfiguration von VRRPv3

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

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

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

Kommandozeile: **Setup > VRRP**



VRRP

VRRP aktiviert

Reconnect-Verzögerung: Minuten

Master-Holddown-Zeit: Minuten

LAN-Link-Erkennung

Interne Dienste unter der virtuellen IP-Adresse anbieten

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. Es werden grundsätzlich nur LAN-Interfaces unterstützt.

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 auf dem Interface.

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-Verbind ist.

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 wiederum Werte zwischen 0 und 255 zulässig. Auch hier haben die Werte 0 und 255 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.
- 255 wird nur akzeptiert, 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

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 Advertising-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.

Virtuelle IPv4-Adresse

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.

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.

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.

Virtuelle Globale IPv6-Adresse

Definiert die 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.

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.

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.

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 als DNS-Server zugewiesen wird.

8.1.4 Ergänzungen im Setup-Menü

VRRP

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

SNMP-ID:

2.141

Pfad Konsole:

Setup

Aktiv

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.

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.

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 wiederum Werte zwischen 0 und 255 zulässig. Auch hier haben die Werte 0 und 255 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.
- > 255 wird nur akzeptiert, 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

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 Advertising-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.

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.

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.

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 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.

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.

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 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

9 RADIUS

9.1 Ergänzungen im Setup-Menü

9.1.1 Msg-Authenticator-erforderlich

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

SNMP-ID:

2.2.22.28

Pfad Konsole:

Setup > WAN > RADIUS

Mögliche Werte:

nein

Access-Requests müssen keinen Message-Authenticator enthalten.

ja

Access-Requests müssen immer einen Message-Authenticator enthalten.

Default-Wert:

nein

9.1.2 L2TP-Msg-Authenticator-erforderlich

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

SNMP-ID:

2.2.22.29

Pfad Konsole:

Setup > WAN > RADIUS

Mögliche Werte:

nein

Access-Requests müssen keinen Message-Authenticator enthalten.

ja

Access-Requests müssen immer einen Message-Authenticator enthalten.

Default-Wert:

nein

9.1.3 Msg-Authenticator-erforderlich

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

SNMP-ID:

2.11.81.1.10

Pfad Konsole:**Setup > Config > RADIUS > Server****Mögliche Werte:****nein**

Access-Requests müssen keinen Message-Authenticator enthalten.

ja

Access-Requests müssen immer einen Message-Authenticator enthalten.

Default-Wert:

nein

9.1.4 Msg-Authenticator-erforderlich

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

SNMP-ID:

2.12.29.21

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

Access-Requests müssen keinen Message-Authenticator enthalten.

ja

Access-Requests müssen immer einen Message-Authenticator enthalten.

Default-Wert:

nein

9.1.5 Backup-Msg-Authenticator-erforderlich

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

SNMP-ID:

2.12.29.22

Pfad Konsole:

Setup > WLAN > RADIUS-Zugriffspruefung

Mögliche Werte:

nein

Access-Requests müssen keinen Message-Authenticator enthalten.

ja

Access-Requests müssen immer einen Message-Authenticator enthalten.

Default-Wert:

nein

9.1.6 Msg-Authenticator-erforderlich

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

SNMP-ID:

2.19.36.9.1.1.11

Pfad Konsole:

Setup > VPN > IKEv2 > RADIUS > Autorisierung > Server

Mögliche Werte:

nein

Access-Requests müssen keinen Message-Authenticator enthalten.

ja

Access-Requests müssen immer einen Message-Authenticator enthalten.

Default-Wert:

nein

9.1.7 Msg-Authenticator-erforderlich

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

SNMP-ID:

2.25.10.2.6

Pfad Konsole:**Setup > RADIUS > Server > Clients****Mögliche Werte:****nein**

Access-Requests müssen keinen Message-Authenticator enthalten.

ja

Access-Requests müssen immer einen Message-Authenticator enthalten.

Nur-Proxy

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

Default-Wert:

nein

9.1.8 Msg-Authenticator-erforderlich

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

SNMP-ID:

2.25.10.3.18

Pfad Konsole:**Setup > RADIUS > Server > Weiterleit-Server****Mögliche Werte:****nein**

Access-Requests müssen keinen Message-Authenticator enthalten.

ja

Access-Requests müssen immer einen Message-Authenticator enthalten.

Default-Wert:

nein

9.1.9 Msg-Authenticator-erforderlich

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

SNMP-ID:

2.25.10.16.6

Pfad Konsole:

Setup > RADIUS > Server > IPv6-Clients

Mögliche Werte:**nein**

Access-Requests müssen keinen Message-Authenticator enthalten.

ja

Access-Requests müssen immer einen Message-Authenticator enthalten.

Nur-Proxy

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

Default-Wert:

nein

10 Weitere Dienste

10.1 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.

10.1.1 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

11 Ergänzungen im Menüsystem

11.1 Ergänzungen im Setup-Menü

11.1.1 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]#@{|}~!$%&'()*+,-./:;<=>?[\]^_`~`

11.1.2 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

11.1.3 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`

11.1.4 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

12 Entfallene Features

Ab LCOS 10.90 sind die folgenden Features entfallen:

- > IKEv1/VPN-Algorithmen cast128_cbc, blowfish_cbc und DES
- > 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)