LCOS 10.90

Addendum

03/2025

LANCOM
SYSTEMS

Contents

Copyright

While the information in this manual has been compiled with great care, it may not be deemed an assurance of product characteristics. LANCOM Systems shall be liable only to the degree specified in the terms of sale and delivery.

This document contains statements relating to future products and their attributes. LANCOM Systems reserves the right to change these without notice. No liability for technical errors and/or omissions.

LANCOM Systems GmbH

A Rohde & Schwarz Company

Adenauerstr. 20/B2

52146 Wuerselen

Germany

www.lancom-systems.com

1 Addendum to LCOS version 10.90

This document describes the changes and enhancements in LCOS version 10.90 since the previous version.

2 Configuration

2.1 Changing automatic uploads from USB

As of LCOS 10.90 the option to automatically load configuration and/or script files has been changed. The configuration option under **Management** > **Advanced**, like the CLI value **Setup** > **Autoload** > **USB** > **Config-and-script** (2.60.56.2), has been removed.

Configuration and/or script files are only automatically loaded into the device if the device is in its factory default settings. A configuration reset can be used to return the device to its factory settings at any time.

2.2 Enhancements to iperf

As of LCOS 10.90, the iperf command has been extended with options to measure the peer bandwidth and to allow automated execution, e.g., from the action table. With LCOS 10.90 RU2, the options `--ratediffperc` and `--expbandwidth` have been added.

These options address the following issue: During recurring measurements, the expected speed may not always be recorded for various reasons. Example: A customer measures a remote site that usually has 40 Down / 10 Up. On a Sunday, however, the rate suddenly drops to 2 Down / 1 Up (server is overloaded, customer backup is running unexpectedly, etc.). As a result, on Monday the customer unexpectedly experiences severe performance issues because the values for the remote site are set or adopted. Solution: If the measured downstream and upstream values fall below 20% of the previous values, the measurement results should be discarded, and the old values should remain in place. If the RxTx rate has not changed, this will be logged in the syslog.

Table 1: Overview of all CLI commands

Command	Description
`iperf [-s|-c <Host>] [options]`	Starts iPerf on the device to perform a bandwidth measurement with an iPerf2 counterpart. Possible options include: › **Client/Server** › `-q, --quiet`: Enables quiet mode where CLI output is suppressed, as the command can also be invoked via the action table. Additionally, in client mode, execution cannot be interrupted. › **Client-specific** › `-R, --reverse`: Reverses the measurement direction. › `-E, --peer <Interface>`: Establishes a connection using the interface specified by the peer name and sets rx/tx thresholds based on the result(s). If not executed in dual or tradeoff mode, the value of the unmeasured direction is set based on the last measurement if available. The result is recorded in the status table **Status** > **Iperf** > **Last-Results** > **Peer-Result** (1.96.1.3) under the values **Peer**, **Server-Bandwidth-kbps**, and **Client-Bandwidth-kbps**.

Command	Description
	> `--retry`: Number of retry attempts if a connection cannot be established. Maximum: 99. > `--ratediffperc #`: Maximum permitted rate deviation in percent in peer mode. Maximum: 99. > `--expbandwidth #/#{kKmM}`: Expected down/up stream bandwidth in peer mode. Values for unmeasured directions are ignored. Example: 10/10M

2.3 Automatic Detection of PMTU in the Ping Command

As of LCOS 10.90, there is a new command-line option for ping to determine the path MTU using the tracepath mode.

On the command line, use the new optional parameter `–m` with ping.

Parameter	Meaning
`-m`	Switches to the tracepath mode to determine the path MTU to the specified IP address.

2.4 Create a TCP-/HTTP Tunnel via CLI

As of LCOS 10.90, the TCP-/HTTP tunnel can also be created using a CLI command. Previously, this was only possible via WEBconfig.

You can set up a TCP-/HTTP tunnel via the CLI of your device.

1. For example, log in to the device via SSH, behind which the device to be accessed is reachable.
2. Navigate to this directory using `cd /setup/http`
3. Execute the command `do Start-TCP-HTTP-Tunnel -r <Routing Tag> -h <IP Address> -p <Local Port> [-a <Remote Address>]`.

   -r
   Routing tag.

   -h
   Host address to be accessed via the tunnel.

   -p
   Local port.

   -a
   Optional remote address.

The TCP-/HTTP tunnel has been created.

2.4.1 Additions to the Setup menu

Start-TCP-HTTP-Tunnel

With this action, you can create a TCP-/HTTP tunnel.

SNMP ID:

2.21.50

Console path:

Setup > **HTTP**

Possible arguments:

-r

Routing tag.

-h

Host address to be accessed via the tunnel.

-p

Local port.

-a

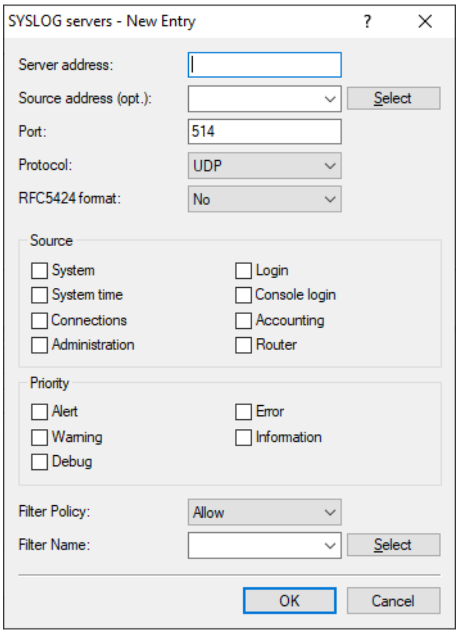
Optional remote address.

3 Diagnosis

3.1 Support for TLS in the syslog client

As of LCOS 10.90 the syslog client supports TLS-encrypted transmission in addition to the transport protocols UDP and TCP.

The corresponding setting can be found in LANconfig under **Logging/Monitoring** > **Protocols** > **SYSLOG** via **Protocol**.



Server address:
Source address (opt.):
Port: 514
Protocol: UDP
RFC5424 format: No

Source
☐ System ☐ Login
☐ System time ☐ Console login
☐ Connections ☐ Accounting
☐ Administration ☐ Router

Priority
☐ Alert ☐ Error
☐ Warning ☐ Information
☐ Debug

Filter Policy: Allow
Filter Name:

Protocol

Defines the protocol used. Possible values:

UDP

User Datagram Protocol

TCP

Transmission Control Protocol

TLS

The syslog client supports three scenarios in TLS mode:

1. The syslog client accepts all TLS server certificates from the syslog server. For this purpose, no trusted CA certificate is stored in the router.
2. The syslog client only accepts server certificates signed by a trusted CA. To do this, the CA certificate must be uploaded to the corresponding certificate slot on the router.
3. The syslog client authenticates itself with the syslog server using a TLS client certificate and the syslog server authenticates itself with its CA certificate. To do this, both the TLS client certificate for the router and the CA certificate must be uploaded to the corresponding certificate slot on the router, e.g. in a container as a PKCS#12 file.

Certificates for syslog can be loaded into the device either via WEBconfig or LANconfig.

- **LANconfig**:**Right-click on the device** > **Configuration Management** > **Upload Certificate or File**
  - **Syslog - container as PKCS#12 file** or
  - **Syslog - Root CA Certificate**
- **WEBconfig**: **Extras** > **File management** > **Upload Certificate or File** > **File Type**
  - **Syslog - container as PKCS#12 file** or
  - **Syslog - Root CA Certificate**

3.1.1 Additions to the Setup menu

Protocol

Specifies which transport protocol the syslog client should use for sending syslog messages to the server.

SNMP ID:

2.22.2.9

Console path:

Setup > **SYSLOG** > **Server**

Possible values:

TCP

Transmission Control Protocol

UDP

User Datagram Protocol

TLS

The syslog client supports three scenarios in TLS mode:

1. The syslog client accepts all TLS server certificates from the syslog server. For this purpose, no trusted CA certificate is stored in the router.
2. The syslog client only accepts server certificates signed by a trusted CA. To do this, the CA certificate must be uploaded to the corresponding certificate slot on the router.
3. The syslog client authenticates itself with the syslog server using a TLS client certificate and the syslog server authenticates itself with its CA certificate. To do this, both the TLS client certificate for the router and the CA certificate must be uploaded to the corresponding certificate slot on the router, e.g. in a container as a PKCS#12 file.

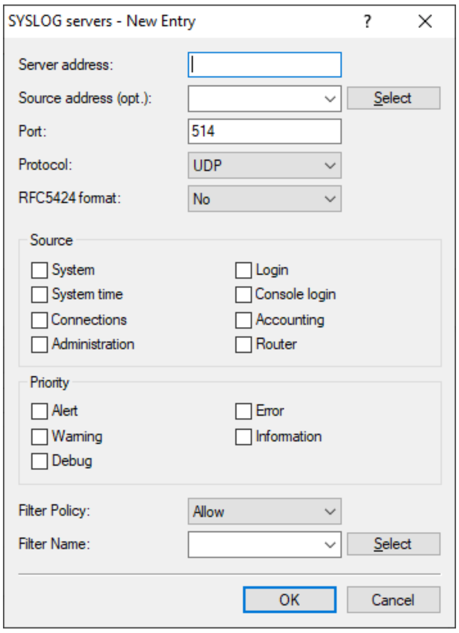
Default:

UDP

3.2 Syslog messages as per the RFC 5424 standard

As of LCOS 10.90 the syslog client also supports the formatting of syslog messages according to the RFC 5424 standard.

The corresponding setting can be found in LANconfig under **Logging/Monitoring** > **Protocols** > **SYSLOG** via **SYSLOG servers**.



SYSLOG servers - New Entry

Server address:

Source address (opt.):

Port: 514

Protocol: UDP

RFC5424 format: No

Source

□ System
□ System time
□ Connections
□ Administration
□ Login
□ Console login
□ Accounting
□ Router

Priority

□ Alert
□ Warning
□ Debug
□ Error
□ Information

Filter Policy: Allow

Filter Name:

RFC5424 format

Specifies whether the syslog client should send messages to the syslog server in RFC5424 format.

3.2.1 Additions to the Setup menu

RFC5424-Format

Specifies whether the syslog client should send messages to the syslog server in RFC5424 format.

SNMP ID:

2.22.2.12

Console path:

Setup > **SYSLOG** > **Server**

Possible values:

Yes
No

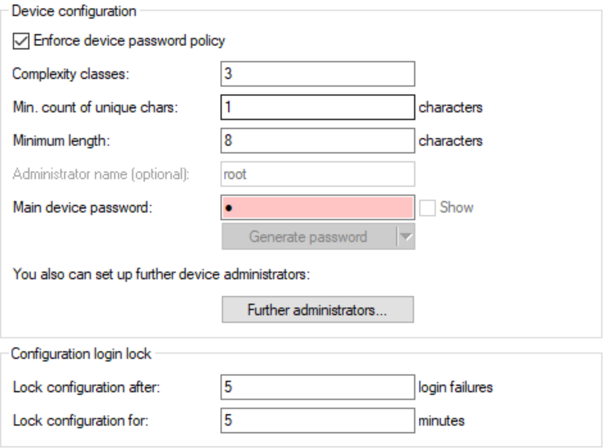
Default:

No

4 Security

4.1 Configurable Password Policy

Starting from LCOS 10.90, you can configure the policy for device passwords. To do so, navigate in LANconfig to **Management** > **Admin** > **Device configuration** > **Enforce device password policy** and adjust the settings.



Device configuration

☑ Enforce device password policy

Complexity classes: 3

Min. count of unique chars: 1 characters

Minimum length: 8 characters

Administrator name (optional): root

Main device password: • □ Show

You also can set up further device administrators:

Configuration login lock

Lock configuration after: 5 login failures

Lock configuration for: 5 minutes

Complexity classes

Configure the required number of different complexity classes for passwords. Complexity classes include lower and upper case letters, numbers, and special characters. With a setting of 2, the password must include characters from at least two of these complexity classes.

Minimum count of unique chars

Configure the required number of unique characters for passwords.

Minimum length

Configure the minimum number of characters for passwords.

4.1.1 Additions to the Setup menu

Password-Complexity

Use this menu to configure password-length and complexity requirements.

SNMP ID:

2.11.89.4

Console path:

Setup > **Config** > **Passwords**

Minimum-Length

Configure the minimum number of characters for passwords here.

SNMP ID:

2.11.89.4.1

Console path:

Setup > **Config** > **Passwords** > **Password-Complexity**

Possible values:

Max. 3 characters from `[0-9]`

Default:

8

Unique-Characters

Configure the required number of unique characters for passwords here.

SNMP ID:

2.11.89.4.2

Console path:

Setup > **Config** > **Passwords** > **Password-Complexity**

Possible values:

Max. 3 characters from `[0-9]`

Default:

3

Complexity-Classes

Configure the required number of complexity classes for passwords here. Complexity classes are lower and upper case letters, numbers, and special characters. If the setting is 2, the password would have to contain characters from at least two of these complexity classes.

SNMP ID:

2.11.89.4.3

Console path:

Setup > **Config** > **Passwords** > **Password-Complexity**

Possible values:

0 … 4

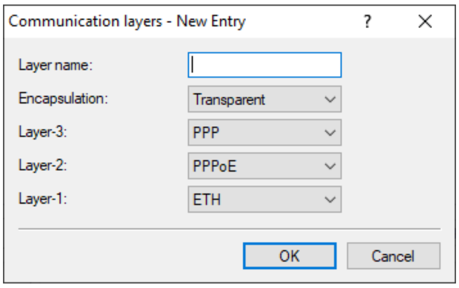
Default:

3

5 Routing and WAN connections

5.1 Configurable DHCP Client Broadcast Bit

From LCOS 10.90, the DHCP client broadcast bit can be set for the **Layer-3** parameter in LANconfig under **Communication** > **General** > **Communication layers**.



Communication layers - New Entry

Layer name:

Encapsulation: Transparent

Layer-3: PPP

Layer-2: PPPoE

Layer-1: ETH

Layer-3

The following new option is available for the network layer (or Layer-3):

DHCP (Broadcast Flag)

The connection is established using a DHCP client with the broadcast flag set in DHCP.

5.1.1 Additions to the Setup menu

Lay-3

The following options are available for the network layer:

SNMP ID:

2.2.4.3

Console path:

Setup > **WAN** > **Layer**

Possible values:

PPP

The connection is established according to the PPP protocol (in synchronous mode, i.e. bit oriented). The configuration data are taken from the PPP table.

DHCP

Assignment of network parameters by DHCP.

B-DHCP

The connection is established with DHCP client and broadcast flag set in DHCP.

TRANS

Transparent: No additional header is inserted.

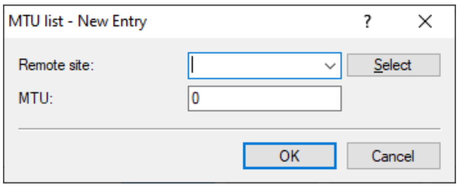
Default:

PPP

5.2 Extension of the MTU List

From LCOS 10.90, wildcards can be used in the MTU list.

LANconfig: **Communication** > **Protocols** > **MTU list**



MTU list - New Entry

Remote site:

MTU: 0

Remote Site

Enter the name of the peer here. This name must match an entry in the list of peers. You can also directly select a name from the list of peers.

You can use the wildcards “?” and “*” at any position in the peer name. “?” represents exactly one character. “*” represents any number of characters or none. The MTU list is sorted in descending order by the length of the peer name and, for names of the same length, in descending alphabetical order. This ensures that complete names always appear before names with wildcards.

5.2.1 Additions to the Setup menu

Peer

Enter the name of the peer here. This name must match an entry in the list of peers. You can also directly select a name from the list of peers.

You can use the wildcards “?” and “*” at any position in the peer name. “?” represents exactly one character. “*” represents any number of characters or none. The MTU list is sorted in descending order by the length of the peer name and, for names of the same length, in descending alphabetical order. This ensures that complete names always appear before names with wildcards.

SNMP ID:

2.2.26.1

Console path:

Setup > **WAN** > **MTU-List**

Possible values:

Selection from the list of defined peers

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

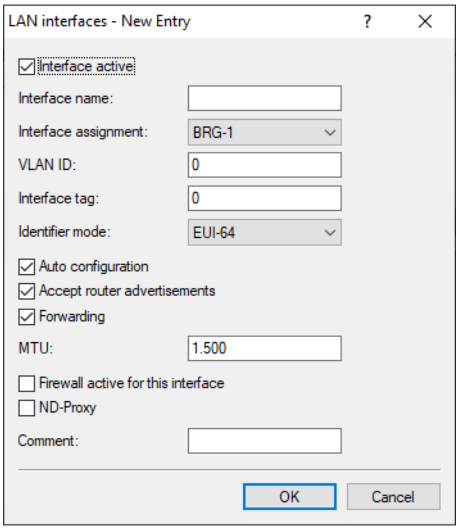
Default:

empty

6 IPv6

6.1 Stable-Private IPv6 Autoconfig Addresses

From LCOS 10.90, the new parameter **Identifier Mode** is available in LANconfig under both **IPv6** > **General** > **LAN interfaces** and **IPv6** > **General** > **WAN profiles**



LAN interfaces - New Entry

☑ Interface active

Interface name:

Interface assignment: BRG-1

VLAN ID: 0

Interface tag: 0

Identifier mode: EUI-64

☑ Auto configuration

☑ Accept router advertisements

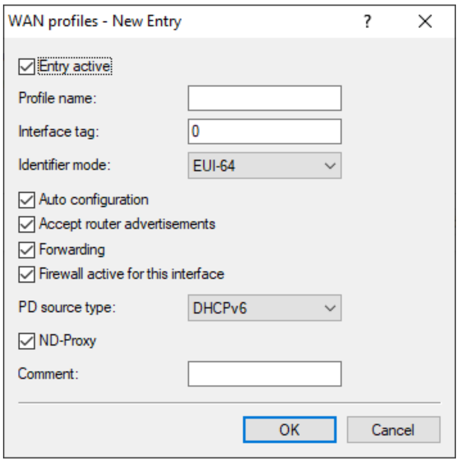
☑ Forwarding

MTU: 1.500

□ Firewall active for this interface

□ ND-Proxy

Comment:



WAN profiles - New Entry

☑ Entry active

Profile name:

Interface tag: 0

Identifier mode: EUI-64

☑ Auto configuration

☑ Accept router advertisements

☑ Forwarding

☑ Firewall active for this interface

PD source type: DHCPv6

☑ ND-Proxy

Comment:

Identifier mode

Defines how automatically generated IPv6 addresses are created on the respective interface of the device.

EUI-64

Automatically generated IPv6 addresses on the configured interface are generated according to the EUI-64 principle, i.e., the MAC address is used as the basis for the host portion of the IPv6 address.

Stable privacy

Automatically generated IPv6 addresses on the configured interface are formed according to RFC 7217. The generation no longer relies on the unique MAC address of the device or the interface but, for privacy reasons, uses a combination of random values and the received provider prefix. The generated interface identifier remains stable or identical as long as the received prefix is the same. If the prefix changes, the interface identifier and, therefore, the entire IPv6 address of the device also changes.

Additionally, under **IPv6** > **General** > **IPv6 addresses**, the parameter **Address type** includes the following new option:

- Stable privacy

  Automatically generated IPv6 addresses on the configured interface are formed according to RFC 7217. The generation no longer relies on the unique MAC address of the device or the interface but, for privacy reasons, uses a combination of random values and the received provider prefix. The generated interface identifier remains stable or identical as long as the received prefix is the same. If the prefix changes, the interface identifier and, therefore, the entire IPv6 address of the device also changes.

6.1.1 Additions to the Setup menu

Address type

Specify the type of IPv6 address.

SNMP ID:

2.70.4.1.3

Console path:

Setup > **IPv6** > **Network** > **Addresses**

Possible values:

Unicast

With the Unicast address type, you use the field *2.70.4.1.2 IPv6-Address-Prefixlength* to specify a full IPv6 address along with its interface identifier, e.g. “2001:db8::1234/64”.

Anycast

With the Anycast address type, you can also use the field *2.70.4.1.2 IPv6-Address-Prefixlength* to specify a full IPv6 address along with its interface identifier, e.g. “2001:db8::1234/64”. Internally, the device handles this address as an anycast address.

EUI-64

The IPv6 address is formed according to the IEEE standard “EUI-64”. The MAC address of the interface thus forms a uniquely identifiable part of the IPv6 address. The correct input format for an IPv6 address including the prefix length as per EUI-64 would be: “2001:db8:1::/64”.

EUI-64 ignores any value set as “interface identifier” in the corresponding IPv6 address and replaces it with an “interface identifier” as per EUI-64.

The prefix length for EUI-64 must be “/64”.

Delegated-Auto-Configuration

The IPv6 address is formed from the router advertisement prefix received on the selected interface (field *2.70.4.1.1 Interface name*) and the host identifier from the field *2.70.4.1.2 IPv6-Address-Prefixlength*.

The field *2.70.4.1.2 IPv6-Address-Prefixlength* can be filled out e.g. with the value" ::2/64" in combination with the prefix "2001:db8::/64" on the interface to form the address "2001:db8::2/64".

Delegated-DHCPv6

The IPv6 address is formed from the delegated DHCPv6 prefix received on the selected interface (field *2.70.4.1.1 Interface name*) and the host identifier from the field *2.70.4.1.2 IPv6-Address-Prefixlength*. The field *2.70.4.1.2 IPv6-Address-Prefixlength* can be filled out e.g. with the value "::2/64" in combination with the prefix "2001:db8::/56" on the interface to form the address "2001:db8::2/64". Similarly, an address can be formed from any subnet of the delegated prefix, e.g "0:0:0:0001::1" and the prefix "2001:db8::/56" go to form the address "2001:db8:0:0001::1/64".

Stable-Privacy

Automatically generated IPv6 addresses on the configured interface are formed according to RFC 7217. The generation no longer relies on the unique MAC address of the device or the interface but, for privacy reasons, uses a combination of random values and the received provider prefix. The generated interface identifier remains stable or identical as long as the received prefix is the same. If the prefix changes, the interface identifier and, therefore, the entire IPv6 address of the device also changes.

Default:

Unicast

Identifier-Mode

Defines how automatically generated IPv6 addresses are created on the respective interface of the device.

SNMP ID:

2.70.6.15

Console path:

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

Possible values:

EUI-64

Automatically generated IPv6 addresses on the configured interface are generated according to the EUI-64 principle, i.e., the MAC address is used as the basis for the host portion of the IPv6 address.

Stable-Privacy

Automatically generated IPv6 addresses on the configured interface are formed according to RFC 7217. The generation no longer relies on the unique MAC address of the device or the interface but, for privacy reasons, uses a combination of random values and the received provider prefix. The generated interface identifier remains stable or identical as long as the received prefix is the same. If the prefix changes, the interface identifier and, therefore, the entire IPv6 address of the device also changes.

Default:

EUI-64

Identifier-Mode

Defines how automatically generated IPv6 addresses are created on the respective interface of the device.

SNMP ID:

2.70.7.13

Console path:

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

Possible values:

EUI-64

Automatically generated IPv6 addresses on the configured interface are generated according to the EUI-64 principle, i.e., the MAC address is used as the basis for the host portion of the IPv6 address.

Stable-Privacy

Automatically generated IPv6 addresses on the configured interface are formed according to RFC 7217. The generation no longer relies on the unique MAC address of the device or the interface but, for privacy reasons, uses a combination of random values and the received provider prefix. The generated interface identifier remains stable or identical as long as the received prefix is the same. If the prefix changes, the interface identifier and, therefore, the entire IPv6 address of the device also changes.

Default:

EUI-64

7 Quality of Service

7.1 Quality-of-Service (QoS) with 8 queues

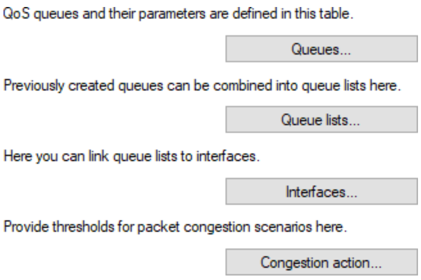
In the following explains the concept of how Quality of Service functions with eight queues. Routers should fundamentally be able to prioritize packets according to the DSCP value in the IP header. A total of eight **queues** are available for this purpose, which are strictly prioritized. This means that packets are sent starting with the **queue** with the highest priority and working through to the **queue** with the lowest priority. A packet is assigned to a **queue** based either on the DSCP value in the IP header or by a firewall rule. Of the eight available **queues** two are reserved, one for the **Urgent-Queue** (highest priority, for internal services such as VCM and protocol packets) and the other for the **Best-Effort-Queue** (lowest priority, for all non-priority packets). The remaining six **queues** are freely available to the user. The priority levels of the individual **queues** are set by placing them in a **Queue-List** in descending order of priority. The internal **Urgent-Queue** and **Best-Effort-Queue** are inserted at the front and end of this **Queue-List**. The completed **queue list** must then be assigned to a physical **WAN interface**. Following this, any packets sent to this **WAN interface** are prioritized according to the configuration of the **queues**.

For QoS to work, the bandwidths or rates of an interface must be known in order for QoS to correctly distribute the load, e.g. in the case where bandwidths are allocated as a percentage. The bandwidths are usually taken from the upstream and downstream data rates from the internal DSL modems or from the bandwidth transmitted in the PPP by the provider.

For WAN connections via external modems or pure Ethernet connections, the actual bandwidths for the corresponding interfaces must be specified in the table **Interfaces** > **WAN** > **Interface settings** under **Downstream rate** and **Upstream rate**.

> Please note that the LCOS automatically sorts certain packets into the urgent queue. These include important negotiation packets such as IKEv2, BGP, or keepalive packets.
>
> Forwarded TCP SYN and ACK packets are given preferential treatment and also sorted into the urgent queue. This behavior can be configured under **IP Router** > **General** > **Routing options** > **Pass on TCP SYN and ACK packets preferentially**.

These **queues** are configured in LANconfig under **Firewall/QoS** > **QoS**.



QoS queues and their parameters are defined in this table.

Previously created queues can be combined into queue lists here.

Here you can link queue lists to interfaces.

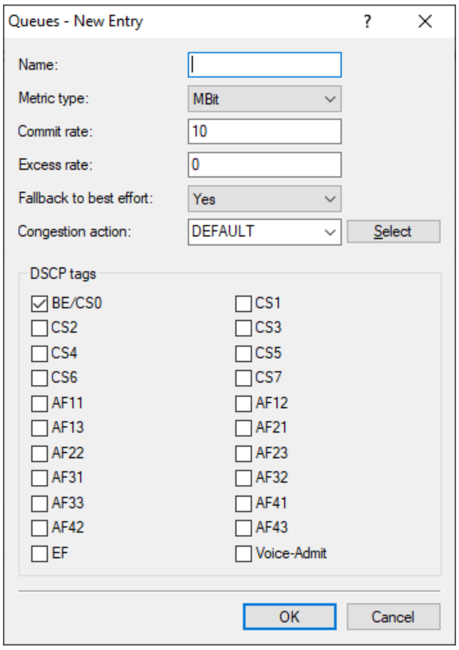
Provide thresholds for packet congestion scenarios here.

7.1.1 Queues

This table is used to configure **queue templates**. This does not mean that every entry in this table creates a queue. A **queue** is only created when it is used in a **Queue-List** and assigned to a **WAN interface**. This means a template created here can be the basis for any number of **queues** or none at all.

Example: If an entry named “Test” is created and this entry is then divided into two **Queue-List** objects, each of which is assigned to a different **WAN interface**, then the result will be two **queues** with name “Test”, which are completely independent of one another.

The configuration of the queues and their parameters in LANconfig is done under **Firewall/QoS** > **QoS** > **Queues**.



Queues - New Entry

Name:	
Metric type:	MBit
Commit rate:	10
Excess rate:	0
Fallback to best effort:	Yes
Congestion action:	DEFAULT

DSCP tags

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

Name

This is where the name of the **queue template** is entered. Other tables reference the template by using this name. The name must be unique within the table.

Metric type

Here the metric of the columns **Commit rate** and **Excess rate** is set.

Commit rate

Here you enter how much bandwidth is available to this **Queue**. The value is also commonly referred to as CIR (Committed Information Rate). The unit of the input is specified in the column **Metric Type**. The following value ranges apply:

- *Percent:* 1 < x < 100
- *Kbit:* 1 < x < 4294967295
- *Mbit:* 1 < x < 4294967295

Excess rate

Here you enter the bandwidth the **Queue** can use in addition to its **Commit-Rate**. The value is also commonly referred to as EIR (Excess Information Rate). To prevent higher-priority **queues** from taking the **commit rate** of lower-priority **queues**, the following concept was used:

The QoS operates in time slots, during which each **queue** can use its **commit rate**. At the end of the time slot, the unused **Commit-Rate** from all **queues** is carried over into the next time slot and used as a pool for the **Excess-Rate**. This pool then limits the bandwidth that can be used with the **Excess-Rate**. This fulfills two important aspects: Firstly, the **Excess-Rate** of a queue is not subtracted from another queue's current **Commit-Rate**, but from the unused rate of the previous time slot. Second, the pool for the **Excess-Rate** is reset at the beginning of each time slot and is not added up, which means the unused **Commit-Rate** of a time slot can only be used in the following time slot. This prevents an accumulation, which could cause **queues** with a configured excess rate to starve the lower-priority queues.

Example: Two **queues** are configured, concatenated into a **Queue-List**, and assigned to a **WAN interface**. **Queue A** has a **commit rate** of 10 Mbps and an **excess rate** of 4 Mbps. **Queue B** has a **commit rate** of 5 Mbps and an **excess rate** of 0. If now in time slot 1 **Queue A** uses 9 Mbps and **Queue B** uses 4 Mbps, then

2 Mbps are unused rate and added to the pool of the **excess rate** for time slot 2. In this time slot, **Queue A** can then use its 10 Mbps **commit rate** and an additional 2 Mbps from the pool as part of its **excess rate**. Important is that only as much **Excess-Rate** can be used as the pool provides.

The unit of the input is specified in the column **Metric Type**. The following value ranges apply:

- *Percent:* 0 < x < 100
- *Kbit:* 0 < x < 4294967295
- *Mbit:* 0 < x < 4294967295

Fallback to best effort

This control determines what happens to packets that cannot be sent as part of the commit rate or excess rate. If **Yes** the packets are sent via the best-effort queue, otherwise they are discarded.

Congestion action

An object from the *Congestion Action* on page 25 table is referenced here, which determines when packets are discarded because the send queues are filling up.

DSCP tags

The DSCP tags (Differentiated Services Code Point) to be assigned to this queue are entered here. Multiple values can be passed.

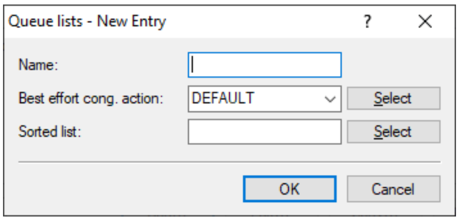
7.1.2 Queue lists

The configured **queue templates** are concatenated into a **queue list** here. This is done by a comma-separated list, with the order specifying the priority from high to low.

It is when creating a **queue list**, make sure that the **commit rates** of the **queues** do not overbook the bandwidth of the **WAN interface**. Otherwise, the low priority **queues** may be starved.

It is also important to ensure that **DSCP tags** are not assigned multiple times. If this happens, the nature of the implementation means that the tag is assigned to the lowest-priority **queue**.

Previously created queues can be found in LANconfig under **Firewall/QoS** > **QoS** > **Queue lists**.



Queue lists - New Entry

Name:

Best effort cong. action: DEFAULT

Sorted list:

Name

This name is used to reference the **Queue-List** from other tables. It must be unique within the table.

Best effort cong. action

This references a **Congestion action** in the Congestion action table to assign a **Congestion action** to the **Best-Effort-Queue**. By default, the DEFAULT entry is used.

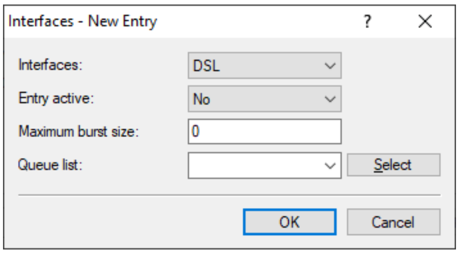
Sorted list

A comma-separated list of **queue templates** is entered here, with their priorities ranging from high to low. Up to six of your own custom **queue templates** be concatenated here, since two places are reserved for the internal **Urgent-Queue** and **Best-Effort-Queue**.

Example of a list: Gold, silver, bronze. The priority of the queues starts with gold, then silver and bronze.

7.1.3 Interfaces

In LANconfig under **Firewall/QoS** > **QoS** > **Interfaces** you link queue lists to interfaces.



Interfaces - New Entry

Interfaces: DSL

Entry active: No

Maximum burst size: 0

Queue list:

Interfaces

The name of the physical **WAN interface** is entered here. The input is limited to an input set of the **WAN interfaces available on the device**.

Entry active

The configured QoS on the **WAN interface** is switched on and off here.

Maximum burst size

The Maximum Burst Size (MBS) regulates the number of bytes that can be sent within a short period (burst). This parameter ensures that massively or continuously oversubscribed traffic does not completely exhaust the available buffer resources, e.g., on upstream provider routers. The default value of 0 means that the operating system manages the parameter internally. Typically, the internal value corresponds to the MTU of the WAN connection in use. The value should be set according to the provider's specifications for the subscribed connection.

Queue list

References an entry from the queue-list table.

7.1.4 Congestion Action

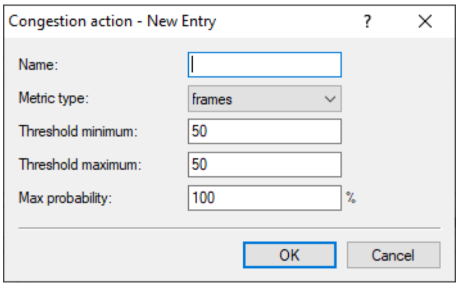
The Congestion action determines how a backed-up send queue is handled. Since this queue cannot grow indefinitely, packets must be discarded at some point. Two mechanisms are available here: Designated as **Taildrop**, **Random Early Detection (RED)**, or **Random Early Discard**. With taildrop, a limit is set beyond which all further incoming packets are discarded. In RED, two limits are determined. As of the first one, packets are discarded with a probability P. P increases the closer you get to the second limit. If the second limit is exceeded, all incoming packets are discarded, like taildrop.

The **Conjestion action** table is defined in such a way that **RED** and **Taildrop** can be configured passively. A **taildrop** can be recognized by the fact that the **threshold minimum** is equal to the **threshold maximum**. **Max-Probability** with a **Taildrop** has no purpose, but should be entered as 100 to specify that everything above the limit will be discarded.

You only specify the **Metric-Type** and **Limit-Minimum**, the other values are set so that a **Taildrop** is configured.

For a **RED**, the **Limit-Minimum** is not equal to **Limit-Maximum**. Starting from the **Limit-Minimum**, the probability of a packet being discarded is P = 0, with P linearly approaching **Max-Probability** the closer you get to the **Threshold-Max**.

In LANconfig, the limits for Congestion incidents are set under **Firewall/QoS** > **QoS** > **Congestion action**.



Congestion action - New Entry

Name:

Metric type: frames

Threshold minimum: 50

Threshold maximum: 50

Max probability: 100 %

Name

The name of the **Congestion-Action** entered here is used to reference the entry from other tables. The name must be unique within this table.

Metric type

This specifies which metric is used by the values in columns **Commit-Rate** and **Excess-Rate**.

Threshold minimum

Specifies the lower threshold for the **Congestion action**.

Threshold maximum

Specifies the upper threshold for the **Congestion action**. From here on, all packets are discarded.

Max. probability

Specifies the maximum drop probability for a configured **RED**. Is ignored if there is a **Taildrop** and should be set to 100 there.

7.1.5 Example 1: Configuring a QoS concept with four classes

In the following example, a customer needs a router that uses a QoS concept with four QoS classes on the connection. The classes are defined as VoIP, Gold, Silver and Best Effort.

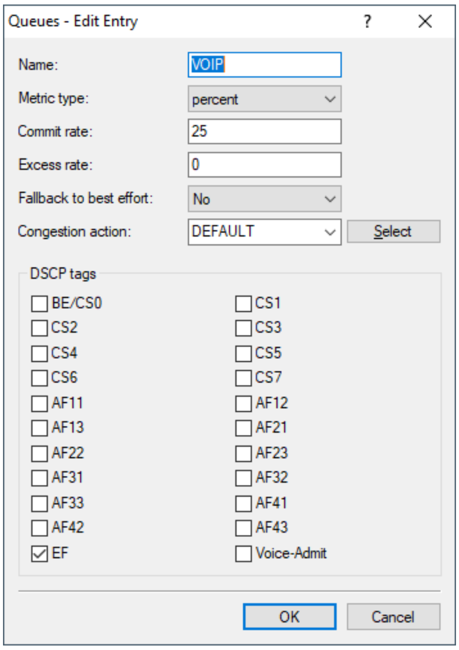
Each service class is allocated 25% of the bandwidth. The customer tags their packets using DSCP so that the packets can be assigned to the correct queue in the router.

If more data is transmitted in the defined service class than there is bandwidth available, this data is discarded. A reversion to the Best Effort service class is not permitted. The definition is as follows:

Class	DSCP
VOIP	EF
Gold	CS3
Silver	CS2
Best effort	0

1. Start LANconfig and open the configuration dialog for the device.
2. Go to the dialog **Firewall/QoS** > **QoS** > **Queues**.

3. Create the three templates for the service classes VOIP, GOLD and SILVER. The Best Effort class does not need to be configured manually as it is present by default.



Queues - Edit Entry

Name: VOIP

Metric type: percent

Commit rate: 25

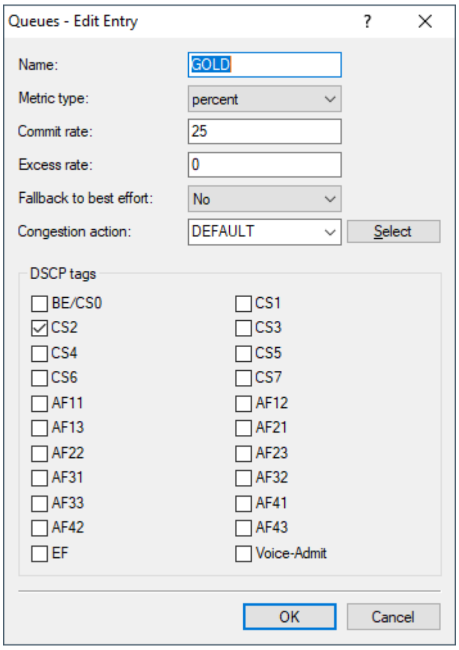
Excess rate: 0

Fallback to best effort: No

Congestion action: DEFAULT

DSCP tags

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



Queues - Edit Entry

Name: GOLD

Metric type: percent

Commit rate: 25

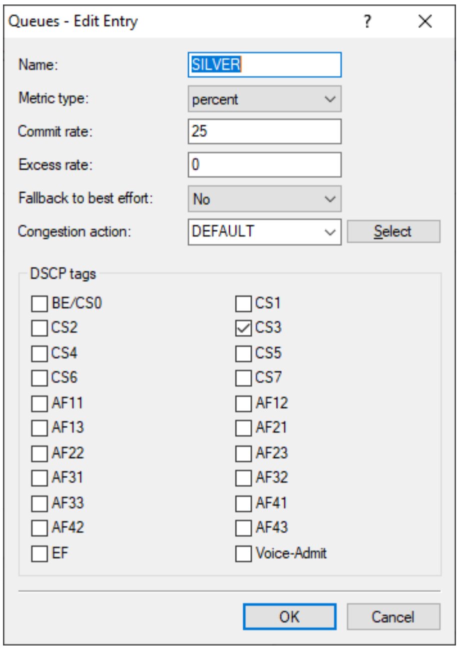
Excess rate: 0

Fallback to best effort: No

Congestion action: DEFAULT

DSCP tags

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



Queues - Edit Entry

Name: SILVER

Metric type: percent

Commit rate: 25

Excess rate: 0

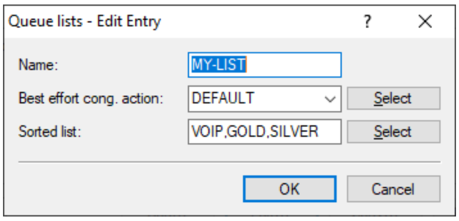
Fallback to best effort: No

Congestion action: DEFAULT

DSCP tags

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

4. Switch to the dialog **Firewall/QoS** > **QoS** > **Queue lists**.
5. Create a list that specifies a strict order for the classes you create. The first class in the list has the highest priority.



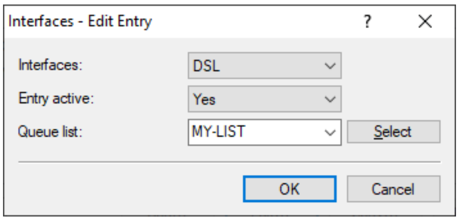
Queue lists - Edit Entry

Name: MY-LIST

Best effort cong. action: DEFAULT

Sorted list: VOIP,GOLD,SILVER

6. Finally, the configured list must be assigned to a WAN interface. In this example we take DSL. Switch to the dialog **Firewall/QoS** > **QoS** > **Interfaces**.



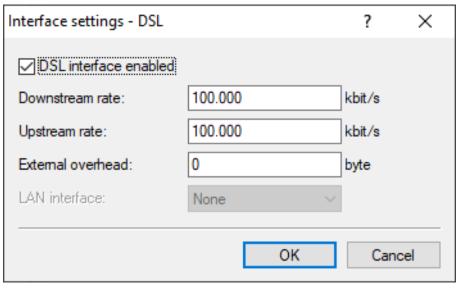
Interfaces - Edit Entry

Interfaces: DSL

Entry active: Yes

Queue list: MY-LIST

7. (Optional): Depending on the WAN interface used, the available data rate in the case of an Ethernet connection must still be configured. This is not necessary if an internal xDSL modem is used. In this case, the synchronized DSL data rate is used. Switch to the dialog **Interfaces** > **WAN** > **Interface settings**.



Interface settings - DSL

☑ DSL interface enabled

Downstream rate: 100.000 kbit/s

Upstream rate: 100.000 kbit/s

External overhead: 0 byte

LAN interface: None

The packet statistics and the distribution into the queues can be viewed on the CLI under `/status/WAN/QoS/Statistics` can be retrieved (abbreviated version here):

```
root@:/
> ls /status/WAN/QoS/Statistics

Interface  Priority   Queue-Name           Pre-Classified       DSCP-Classified      Total-Classified
===============================================================================================================
DSL-1      0          #urgent              0                    0                    0

DSL-1      1          VOIP                 0                    0                    0

DSL-1      2          GOLD                 0                    0                    0

DSL-1      3          SILVER               0                    0                    0

DSL-1      4          #best-effort         0                    0                    0
```

7.1.6 Example 2: Configuring a QoS concept on the VDSL connection with two QoS classes

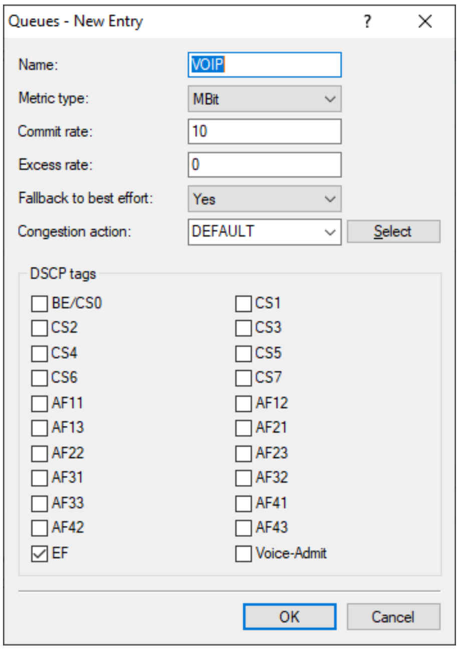
In the following example, a customer needs a router that uses a QoS concept with two QoS classes on the VDSL connection. The classes are defined as VoIP and Best Effort. The device used is a router with an internal xDSL modem.

The VoIP service class is assigned an absolute bandwidth of 10 Mbps. The customer tags their packets using DSCP so that the packets can be assigned to the correct queue in the router.

If more data is transmitted in the defined service class than there is bandwidth available, this data is assigned to the Best Effort class. The definition is as follows:

Class	DSCP
VOIP	EF

1. Start LANconfig and open the configuration dialog for the device.
2. Go to the dialog **Firewall/QoS** > **QoS** > **Queues**.
3. Create the template for the VOIP service class. The Best Effort class does not need to be configured manually as it is present by default.

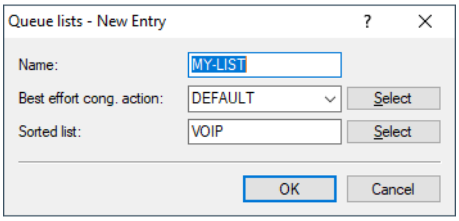


Name: VOIP
Metric type: MBit
Commit rate: 10
Excess rate: 0
Fallback to best effort: Yes
Congestion action: DEFAULT

DSCP tags
☐ BE/CS0 ☐ CS1
☐ CS2 ☐ CS3
☐ CS4 ☐ CS5
☐ CS6 ☐ CS7
☐ AF11 ☐ AF12
☐ AF13 ☐ AF21
☐ AF22 ☐ AF23
☐ AF31 ☐ AF32
☐ AF33 ☐ AF41
☐ AF42 ☐ AF43
☑ EF ☐ Voice-Admit

4. Switch to the dialog **Firewall/QoS** > **QoS** > **Queue lists**.

5. Create a list that specifies a strict order for the classes you create. The first class in the list has the highest priority.



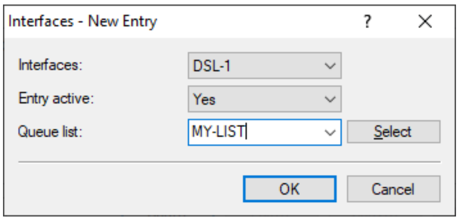
Queue lists - New Entry

Name: MY-LIST

Best effort cong. action: DEFAULT

Sorted list: VOIP

6. Finally, the configured list must be assigned to a WAN interface. In this example we use DSL-1. Switch to the dialog **Firewall/QoS** > **QoS** > **Interfaces**.



Interfaces - New Entry

Interfaces: DSL-1

Entry active: Yes

Queue list: MY-LIST

The packet statistics and the distribution into the queues can be viewed on the CLI under `/status/WAN/QoS/Statistics` can be retrieved (abbreviated version here):

```
root@:/
> ls /status/WAN/QoS/Statistics

Interface  Priority    Queue-Name            Pre-Classified       DSCP-Classified       Total-Classified
======================-------------------------------------------------------------------------------------
DSL-1      0           #urgent               0                    0                     0

DSL-1      1           VOIP                  0                    0                     0

DSL-1      2           #best-effort          0                    0                     0
```

7.1.7 Queue usage in the firewall

The firewall uses rules to assign packets to the queues configured in the QoS. This assignment is independent of the DSCP value in the IP header. The assignment is handled by actions that are assigned to a rule. If a rule matches an action and a session is opened in the firewall, the system checks whether the target or source interface of the session has been assigned to a queue and notes the assignment in the action. When data is flowing during the session and the action is executed, the respective packet is tagged with the assignment, is ignored by the DSCP classifier, and is counted as “Pre-Classified” in the QoS statistics for the respective queue.

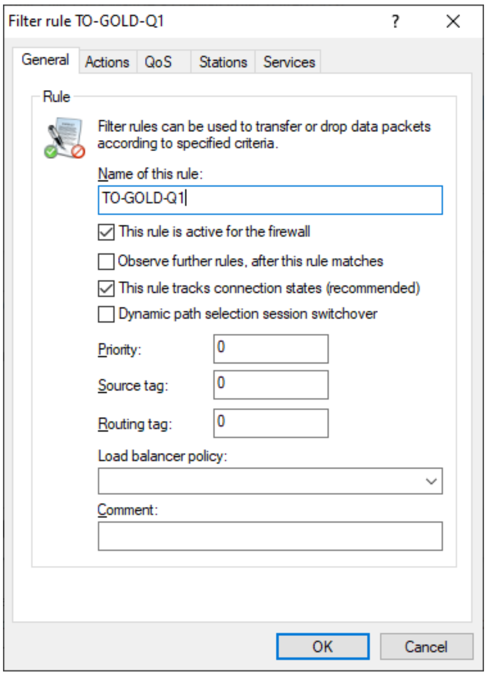
The queue assignment refers to queues that have been assigned to physical interfaces, but is inherited by interfaces stacked above them. For example, if the target interface of a session is a VPN interface, the queue assignment is passed on to the physical interface (WAN) and applied there.

Since the IPv4 and IPv6 firewalls differ in their configuration, they are listed separately below.

IPv4 firewall

Below is an example of the procedure for a queue assignment:

1. A queue assignment is implemented by a firewall rule, which is added under **Firewall/QoS** > **IPv4 Rules** > **Firewall rules (Filter/QoS)** > **Rules**. First, give a name to the rule on the **General** tab.



Filter rules can be used to transfer or drop data packets according to specified criteria.

Name of this rule: TO-GOLD-Q1

☑ This rule is active for the firewall

□ Observe further rules, after this rule matches

☑ This rule tracks connection states (recommended)

□ Dynamic path selection session switchover

Priority: 0

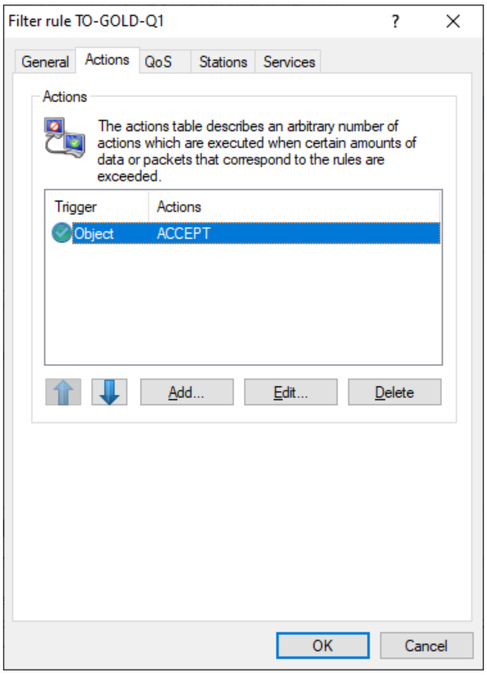
Source tag: 0

Routing tag: 0

Load balancer policy:

Comment:

2. On the **Actions** tab you then add an “ACCEPT” action and remove the default “REJECT” action.

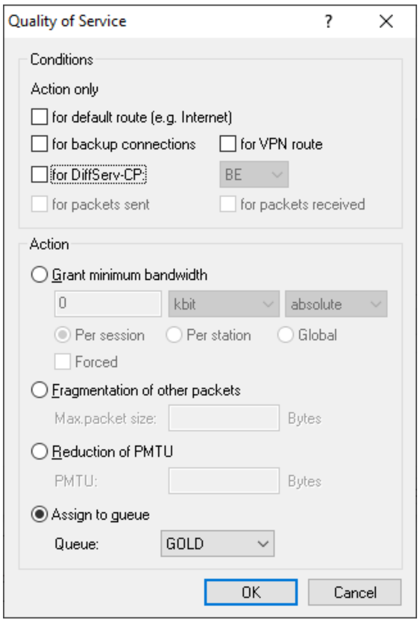


The actions table describes an arbitrary number of actions which are executed when certain amounts of data or packets that correspond to the rules are exceeded.

Trigger	Actions
Object	ACCEPT

3. Next, add a new QoS object on the tab **QoS**. On the tab **General** give it a name and then assign it to the desired queue on the tab **QoS**.

The action can be restricted with conditions, for example if the assignment should only apply in a certain direction or only for a certain DSCP value.



Quality of Service

Conditions

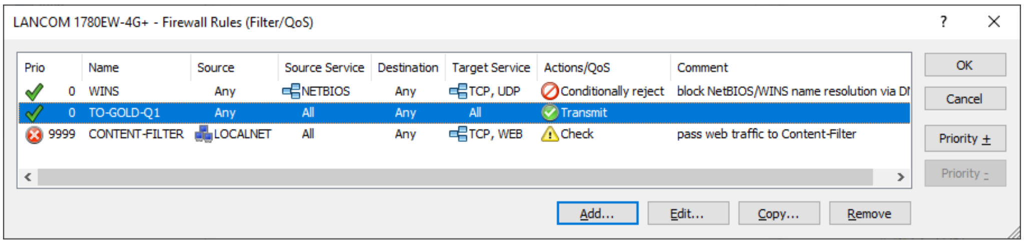
Action only

- ☐ for default route (e.g. Internet)
- ☐ for backup connections ☐ for VPN route
- ☐ for DiffServ-CP: BE
- ☐ for packets sent ☐ for packets received

Action

- ○ Grant minimum bandwidth: 0 kbit absolute
  - ● Per session ○ Per station ○ Global
  - ☐ Forced
- ○ Fragmentation of other packets
  - Max.packet size: Bytes
- ○ Reduction of PMTU
  - PMTU: Bytes
- ● Assign to queue
  - Queue: GOLD

4. The result is a rule that assigns the desired packets to a queue – in this example “GOLD”.



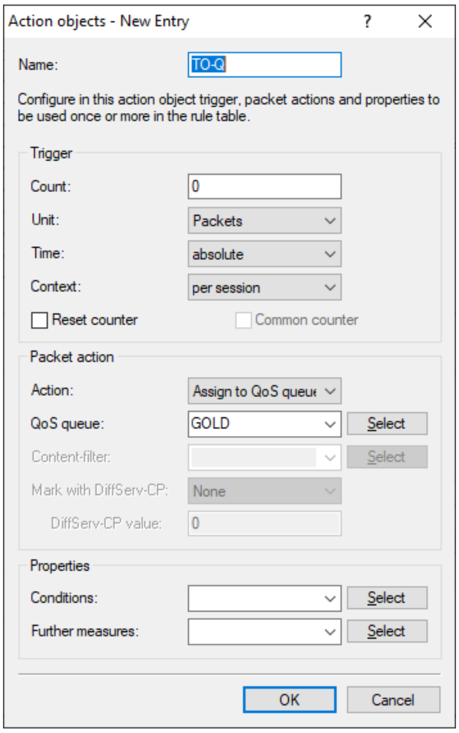
LANCOM 1780EW-4G+ - Firewall Rules (Filter/QoS)

	Prio	Name	Source	Source Service	Destination	Target Service	Actions/QoS	Comment
✓	0	WINS	Any	NETBIOS	Any	TCP, UDP	Conditionally reject	block NetBIOS/WINS name resolution via DI
✓	0	TO-GOLD-Q1	Any	All	Any	All	Transmit	
✗	9999	CONTENT-FILTER	LOCALNET	All	Any	TCP, WEB	Check	pass web traffic to Content-Filter

IPv6 firewall

Below is an example of the procedure for a queue assignment:

1. A queue is assigned via an action object assigned in an IPv6 forwarding rule. First, create an action object that assigns the desired queue. Do this under **Firewall/QoS** > **IPv6 Rules** > **Firewall Objects** > **Action objects**.



Action objects - New Entry

Name: TO-Q

Configure in this action object trigger, packet actions and properties to be used once or more in the rule table.

Trigger

Count: 0

Unit: Packets

Time: absolute

Context: per session

□ Reset counter □ Common counter

Packet action

Action: Assign to QoS queue

QoS queue: GOLD

Content-filter:

Mark with DiffServ-CP: None

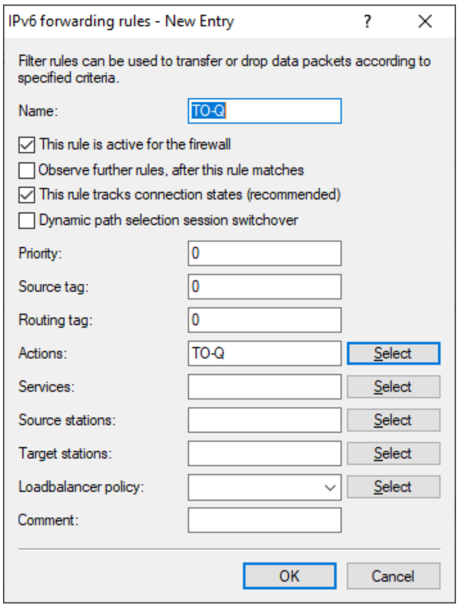
DiffServ-CP value: 0

Properties

Conditions:

Further measures:

2. Under **Firewall/QoS** > **IPv6 Rules** > **IPv6 forwarding rules** you then create a new rule that uses this action object.



IPv6 forwarding rules - New Entry

Filter rules can be used to transfer or drop data packets according to specified criteria.

Name: TO-Q

☑ This rule is active for the firewall

□ Observe further rules, after this rule matches

☑ This rule tracks connection states (recommended)

□ Dynamic path selection session switchover

Priority: 0

Source tag: 0

Routing tag: 0

Actions: TO-Q

Services:

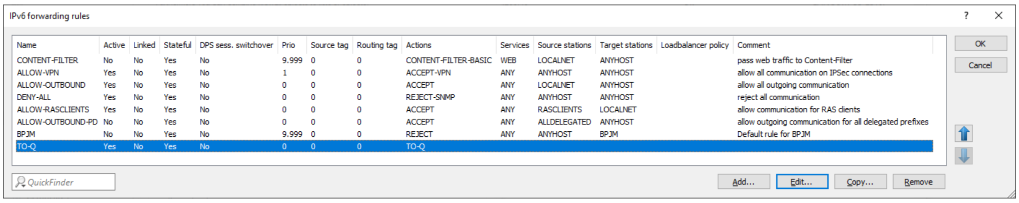
Source stations:

Target stations:

Loadbalancer policy:

Comment:

3. The result is a rule that assigns the desired packets to a queue – in this example “GOLD”.



IPv6 forwarding rules

Name	Active	Linked	Stateful	DPS sess. switchover	Prio	Source tag	Routing tag	Actions	Services	Source stations	Target stations	Loadbalancer policy	Comment
CONTENT-FILTER	No	No	Yes	No	9.999	0	0	CONTENT-FILTER-BASIC	WEB	LOCALNET	ANYHOST		pass web traffic to Content-Filter
ALLOW-VPN	Yes	No	Yes	No	1	0	0	ACCEPT-VPN	ANY	ANYHOST	ANYHOST		allow all communication on IPSec connections
ALLOW-OUTBOUND	Yes	No	Yes	No	0	0	0	ACCEPT	ANY	LOCALNET	ANYHOST		allow all outgoing communication
DENY-ALL	Yes	No	Yes	No	0	0	0	REJECT-SNMP	ANY	ANYHOST	ANYHOST		reject all communication
ALLOW-RASCLIENTS	Yes	No	Yes	No	0	0	0	ACCEPT	ANY	RASCLIENTS	LOCALNET		allow communication for RAS clients
ALLOW-OUTBOUND-PD	No	No	Yes	No	0	0	0	ACCEPT	ANY	ALLDELEGATED	ANYHOST		allow outgoing communication for all delegated prefixes
BPJM	No	No	Yes	No	9.999	0	0	REJECT	ANY	ANYHOST	BPJM		Default rule for BPJM
TO-Q	Yes	No	Yes	No	0	0	0	TO-Q					

7.1.8 Additions to the Setup menu

QoS

LCOS supports up to eight different queues (service classes) with corresponding priority levels for applications in the network, and include “VoIP”, “Gold”, “Silver” or “Best Effort”. Data packets are assigned to the appropriate Quality of Service (QoS) class using DSCP markings or firewall rules. The router then sorts the packets into the correct priority level and ensures that the corresponding services only use as much upload bandwidth as was previously configured for the class in percent or Mbps. This ensures that important services such as VoIP or video calls always receive sufficient bandwidth, even when the network is under heavy load.

In the following explains the concept of how Quality of Service functions with eight queues. Routers should fundamentally be able to prioritize packets according to the DSCP value in the IP header. A total of eight **queues** are available for this purpose, which are strictly prioritized. This means that packets are sent starting with the **queue** with the highest priority and working through to the **queue** with the lowest priority. A packet is assigned to a **queue** based either on the DSCP value in the IP header or by a firewall rule. Of the eight available **queues** two are reserved, one for the **Urgent-Queue** (highest priority, for internal services such as VCM and protocol packets) and the other for the **Best-Effort-Queue** (lowest priority, for all non-priority packets). The remaining six **queues** are freely available to the user. The priority levels of the individual **queues** are set by placing them in a **Queue-List** in descending order of priority. The internal **Urgent-Queue** and **Best-Effort-Queue** are inserted at the front and end of this **Queue-List**. The completed **queue list** must then be assigned to a physical **WAN interface**. Following this, any packets sent to this **WAN interface** are prioritized according to the configuration of the **queues**.

For QoS to work, the bandwidths or rates of an interface must be known in order for QoS to correctly distribute the load, e.g. in the case where bandwidths are allocated as a percentage. The bandwidths are usually taken from the upstream and downstream data rates from the internal DSL modems or from the bandwidth transmitted in the PPP by the provider.

SNMP ID:

2.2.71

Console path:

Setup > **WAN**

Congestion-Action

The Congestion Action determines how a backed-up send queue is handled. Since this queue cannot grow indefinitely, packets must be discarded at some point. Two mechanisms are available here: **Taildrop** and **Random Early Detection (RED)** , also known as **Random Early Discard**. With taildrop, a limit is set beyond which all further incoming packets are discarded. In RED, two limits are determined. As of the first one, packets are discarded with a probability P. P increases the closer you get to the second limit. If the second limit is exceeded, all incoming packets are discarded, like taildrop.

The table **Congestion-Action** is defined in such a way that it can be configured to contain **RED** and **Taildrop**. This decision ensures maximum flexibility, on the one hand, but also a high potential for errors leading to a non-functional configuration. Hence the following explanation of the framework conditions for both concepts. A **Taildrop** is recognized by the fact that **Threshold-Min** is equal to **Threshold-Max**. **Max-Probability** with a **Taildrop** has no purpose, but should be entered as 100 to indicate that everything above the limit will be discarded. For a user to configure a **Taildrop** as easily as possible, a shortened input can be used:

```
root@:/Setup/WAN/QoS
> add Congestion-Action/test bytes 2000
set ok:
Name                  Metric-Type   Threshold-Min    Threshold-Max    Max-Probability-Percentage
======================------------------------------------------------------------------------------
TEST                  Bytes         2000             2000             100
```

You only specify the **Metric-Type** and **Limit-Min**, the other values are set so that a **Taildrop** is configured.

For a **RED**, the **Threshold-Min** is not equal to **Threshold-Max**. The packet is discarded as of **Threshold-Min** starting with a probability P=0, where P linearly approaches **Max-Probability** the closer you get to **Threshold-Max**.

SNMP ID:

2.2.71.1

Console path:

Setup > **WAN** > **QoS**

Name

The name of the **Congestion-Action** entered here is used to reference the entry from other tables. The name must be unique within this table.

SNMP ID:

2.2.71.1.1

Console path:

Setup > **WAN** > **QoS** > **Congestion-Action**

Possible values:

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

Metric-Type

This specifies which metric is used by the values in columns *2.2.71.1.3 Threshold-Min* on page 35 and *2.2.71.1.4 Threshold-Max* on page 36

SNMP ID:

2.2.71.1.2

Console path:

Setup > **WAN** > **QoS** > **Congestion-Action**

Possible values:

Frames
Bytes
KBytes

Threshold-Min

Specifies the lower threshold for the **Congestion-Action**.

SNMP ID:

2.2.71.1.3

Console path:

Setup > **WAN** > **QoS** > **Congestion-Action**

Possible values:

Max. 10 characters from `[0-9]`

Threshold-Max

Specifies the upper threshold for the **Congestion-Action**. From here on, all packets are discarded.

SNMP ID:

2.2.71.1.4

Console path:

Setup > **WAN** > **QoS** > **Congestion-Action**

Possible values:

Max. 10 characters from `[0-9]`

Max-Probability-Percentage

Specifies the maximum drop probability for a configured **RED**. Is ignored if there is a **Taildrop** and should be set to 100 there.

SNMP ID:

2.2.71.1.5

Console path:

Setup > **WAN** > **QoS** > **Congestion-Action**

Possible values:

0 … 100

Queues

This table is used to configure **queue templates**. This does not mean that every entry in this table creates a queue. A **queue** is only created when it is used in a **Queue-List** and assigned to a **WAN interface**. This means a template created here can be the basis for any number of **queues** or none at all.

Example: If an entry named “Test” is created and this entry is then divided into two **Queue-List** objects, each of which is assigned to a different **WAN interface**, then the result will be two **queues** with name “Test”, which are completely independent of one another.

SNMP ID:

2.2.71.2

Console path:

Setup > **WAN** > **QoS**

Name

This is where the name of the **queue template** is entered. Other tables reference the template by using this name. The name must be unique within the table.

SNMP ID:

2.2.71.2.1

Console path:

Setup > **WAN** > **QoS** > **Queues**

Possible values:

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

Metric-Type

This is where the metric of the columns *2.2.71.2.3 Commit-Rate* on page 37 and *2.2.71.2.4 Excess-Rate* on page 38 is set.

SNMP ID:

2.2.71.2.2

Console path:

Setup > **WAN** > **QoS** > **Queues**

Possible values:

Percentage

The rate is given as a percentage. The basic value for the calculation is the bandwidth available on the WAN interface.

Kbit

The rate is nominally given in kilobits per second.

Mbit

The rate is nominally given in megabits per second.

Commit-Rate

Here you enter how much bandwidth is available to this **Queue**. The value is also commonly referred to as CIR (Committed Information Rate). The unit of the input is set in the column *2.2.71.2.2 Metric-Type* on page 37. The following value ranges apply:

- *Percent:* 1 < x < 100
- *Kbit:* 1 < x < 4294967295
- *Mbit:* 1 < x < 4294967295

SNMP ID:

2.2.71.2.3

Console path:

Setup > **WAN** > **QoS** > **Queues**

Possible values:

Max. 10 characters from `[0-9]`

Excess-Rate

Here you enter the bandwidth the **Queue** can use in addition to its **Commit-Rate**. The value is also commonly referred to as EIR (Excess Information Rate). To prevent higher-priority **queues** from taking the **commit rate** of lower-priority **queues**, the following concept was used:

The QoS operates in time slots, during which each **queue** can use its **commit rate**. At the end of the time slot, the unused **Commit-Rate** from all **queues** is carried over into the next time slot and used as a pool for the **Excess-Rate**. This pool then limits the bandwidth that can be used with the **Excess-Rate**. This fulfills two important aspects: Firstly, the **Excess-Rate** of a queue is not subtracted from another queue's current **Commit-Rate**, but from the unused rate of the previous time slot. Second, the pool for the **Excess-Rate** is reset at the beginning of each time slot and is not added up, which means the unused **Commit-Rate** of a time slot can only be used in the following time slot. This prevents an accumulation, which could cause **queues** with a configured excess rate to starve the lower-priority queues.

Example: Two **queues** are configured, concatenated into a **Queue-List**, and assigned to a **WAN interface**. **Queue A** has a **commit rate** of 10 Mbps and an **excess rate** of 4 Mbps. **Queue B** has a **commit rate** of 5 Mbps and an **excess rate** of 0. If now in time slot 1 **Queue A** uses 9 Mbps and **Queue B** uses 4 Mbps, then 2 Mbps are unused rate and added to the pool of the **excess rate** for time slot 2. In this time slot, **Queue A** can then use its 10 Mbps **commit rate** and an additional 2 Mbps from the pool as part of its **excess rate**. Important is that only as much **Excess-Rate** can be used as the pool provides.

The unit of the input is set in the column *2.2.71.2.2 Metric-Type* on page 37. The following value ranges apply:

- *Percent:* 0 < x < 100
- *Kbit:* 0 < x < 4294967295
- *Mbit:* 0 < x < 4294967295

SNMP ID:

2.2.71.2.4

Console path:

Setup > **WAN** > **QoS** > **Queues**

Possible values:

Max. 10 characters from `[0-9]`

Fallback-to-Best-Effort

This control determines what happens to packets that cannot be sent as part of the commit rate or excess rate.

SNMP ID:

2.2.71.2.5

Console path:

Setup > **WAN** > **QoS** > **Queues**

Possible values:

Yes

The packets are sent via the best-effort queue.

No

The packets are discarded.

Congestion-Action

This references an object from the table *2.2.71.1 Congestion-Action* on page 34, which determines when packets are discarded due to full send queues.

SNMP ID:

2.2.71.2.6

Console path:

Setup > **WAN** > **QoS** > **Queues**

DSCP-Tags

The DSCP tags (Differentiated Services Code Point) to be assigned to this queue are entered here. Multiple values can be passed using a comma-separated list.

SNMP ID:

2.2.71.2.7

Console path:

Setup > **WAN** > **QoS** > **Queues**

Possible values:

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

Queue-List

The configured **queue templates** are concatenated into a **queue list** here. This is done by a comma-separated list, with the order specifying the priority from high to low.

❗ It is when creating a **queue list**, make sure that the **commit rates** of the **queues** do not overbook the bandwidth of the **WAN interface**. Otherwise, the low priority **queues** may be starved.

❗ It is also important to ensure that **DSCP tags** are not assigned multiple times. If this happens, the nature of the implementation means that the tag is assigned to the lowest-priority **queue**.

SNMP ID:

2.2.71.3

Console path:

Setup > **WAN** > **QoS**

Name

This name is used to reference the **Queue-List** from other tables. It must be unique within the table.

SNMP ID:

2.2.71.3.1

Console path:

Setup > **WAN** > **QoS** > **Queue-List**

Possible values:

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

Best-Effort-Congestion-Action

This references a **Congestion-Action** in the Congestion-Action table to assign a **Congestion-Action** to the **Best-Effort-Queue**. By default, the DEFAULT entry is used.

SNMP ID:

2.2.71.3.2

Console path:

Setup > **WAN** > **QoS** > **Queue-List**

Possible values:

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

Ordered-List

A comma-separated list of **queue templates** is entered here, with their priorities ranging from high to low. Up to six of your own custom **queue templates** be concatenated here, since two places are reserved for the internal **Urgent-Queue** and **Best-Effort-Queue**.

Example of a list: Gold, silver, bronze. The priority of the queues starts with gold, then silver and bronze.

SNMP ID:

2.2.71.3.3

Console path:

Setup > **WAN** > **QoS** > **Queue-List**

Possible values:

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

Interfaces

Configured **queue lists** are assigned to **WAN interfaces** here.

SNMP ID:

2.2.71.4

Console path:

Setup > **WAN** > **QoS**

Interface

Enter the name of the physical **WAN interface** here. Entries are limited to the **WAN interfaces** available on the device.

SNMP ID:

2.2.71.4.1

Console path:

Setup > **WAN** > **QoS** > **Interfaces**

Enabled

This switches the configured QoS on the **WAN interface** on or off.

SNMP ID:

2.2.71.4.2

Console path:

Setup > **WAN** > **QoS** > **Interfaces**

Possible values:

Yes
No

Queue-List

This references an entry in the queue-list table.

SNMP ID:

2.2.71.4.3

Console path:

Setup > **WAN** > **QoS** > **Interfaces**

Possible values:

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

Maximum-Burst-Size

The Maximum Burst Size (MBS) regulates the number of bytes that can be sent within a short period (burst). This parameter ensures that massively or continuously oversubscribed traffic does not completely exhaust the available buffer resources, e.g., on upstream provider routers. The value should be set according to the provider's specifications for the subscribed connection.

SNMP ID:

2.2.71.4.4

Console path:

Setup > **WAN** > **QoS** > **Interfaces**

Possible values:

max. 5 characters `[0-9]`

Default:

0

Special values:

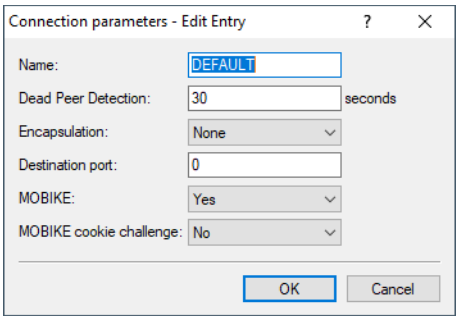
0

The default value 0 means that the operating system manages the parameter internally. Typically, the internal value corresponds to the MTU of the used WAN connection.

8 Virtual Private Networks – VPN

8.1 MOBIKE

From LCOS 10.90, the new parameters **MOBIKE** and **MOBIKE cookie challenge** are located in the table **VPN** > **IKEv2/IPsec** > **VPN connections** > **Connection parameters**.



Name: DEFAULT
Dead Peer Detection: 30 seconds
Encapsulation: None
Destination port: 0
MOBIKE: Yes
MOBIKE cookie challenge: No

MOBIKE

Defines whether MOBIKE as per *RFC 4555* should be supported.

MOBIKE according to RFC 4555 for IKEv2 optionally allows mobile clients to roam between different networks without disconnecting the VPN tunnel. For example, a VPN client can roam seamlessly from cellular to Wi-Fi, whereby an IKEv2 update message updates the external IP address on the VPN gateway. The advantage is that the VPN tunnel or the Security Associations (SAs) do not have to be terminated and setup again.

MOBIKE is only supported as a responder role, i.e. when VPN clients establish connections to the LANCOM VPN router. The establishment of VPN tunnels with the MOBIKE extension is not supported.

MOBIKE cookie challenge

Defines whether the device should send a cookie challenge to determine whether the VPN client can actually receive packets at the new address (“Return Routability Check”).

8.1.1 Additions to the Setup menu

MOBIKE

Defines whether MOBIKE as per *RFC 4555* should be supported.

MOBIKE according to RFC 4555 for IKEv2 optionally allows mobile clients to roam between different networks without disconnecting the VPN tunnel. For example, a VPN client can roam seamlessly from cellular to Wi-Fi, whereby an IKEv2 update message updates the external IP address on the VPN gateway. The advantage is that the VPN tunnel or the Security Associations (SAs) do not have to be terminated and setup again.

MOBIKE is only supported as a responder role, i.e. when VPN clients establish connections to the LANCOM VPN router. The establishment of VPN tunnels with the MOBIKE extension is not supported.

SNMP ID:

2.19.36.4.9

Console path:

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

Possible values:

Yes

MOBIKE is supported.

No

MOBIKE is not supported.

Default:

Yes

MOBIKE-Cookie-Challenge

Defines whether the device should send a cookie challenge to determine whether the VPN client can actually receive packets at the new address ("Return Routability Check").

SNMP ID:

2.19.36.4.10

Console path:

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

Possible values:

Yes

MOBIKE-Cookie-Challenge is sent.

No

MOBIKE-Cookie-Challenge is not sent.

Default:

No

8.2 IKEv2 post-quantum pre-shared keys (PPK)

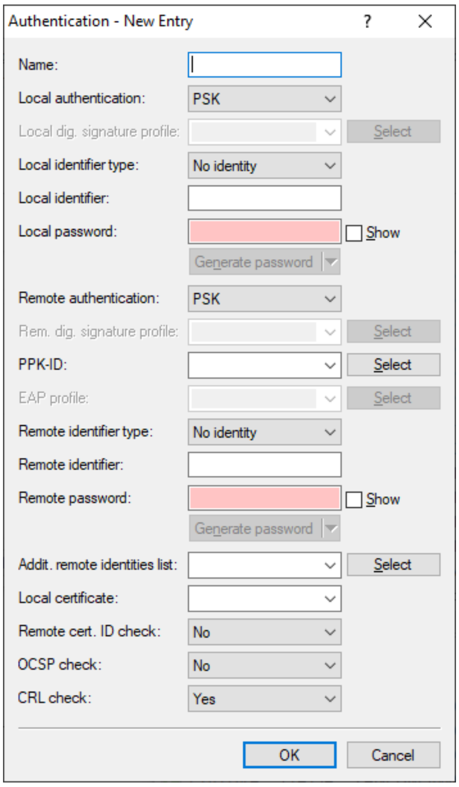
Quantum computers pose a potential challenge to current cryptographic algorithms, such as those used in IKEv2 VPN. Current algorithms are considered to be very robust, but the challenge is that an attacker can record encrypted data today and decrypt it using quantum computers in the future.

The *RFC 8784* "Mixing Preshared Keys in the Internet Key Exchange Protocol Version 2 (IKEv2) for Post-quantum Security" offers a way to resist quantum computers when passwords (PSKs) are used. The extension works by "mixing" the standard IKEv2 password key (PSK) with another key in the form of a Post-quantum Preshared Key (PPK) to increase resistance.

Existing IKEv2 PSK tunnels can easily be supplemented with PPKs. The PPK is independent of the existing PSK.

LCOS supports manual configuration of PPKs. Automatic procedures for changing PPKs are not supported.

Table VPN > IKEv2/IPSec > Authentication



Authentication - New Entry

Name:

Local authentication: PSK

Local dig. signature profile:

Local identifier type: No identity

Local identifier:

Local password: □ Show

Remote authentication: PSK

Rem. dig. signature profile:

PPK-ID:

EAP profile:

Remote identifier type: No identity

Remote identifier:

Remote password: □ Show

Addit. remote identities list:

Local certificate:

Remote cert. ID check: No

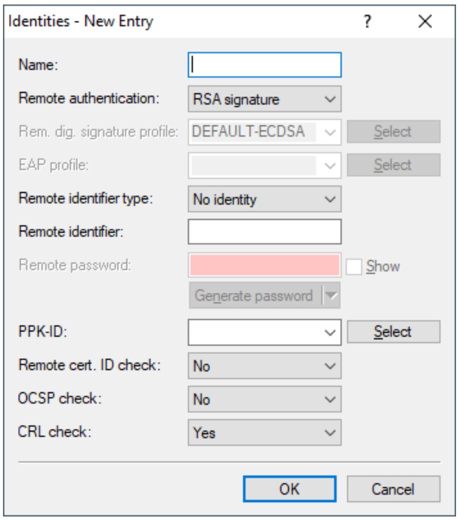
OCSP check: No

CRL check: Yes

PPK ID

Enter the name of the PPK-ID (Post-quantum Preshared Keys as per *RFC 8784*) from the table of PPKs.

Table VPN > IKEv2/IPSec > Extended settings > Authentication > Identities



Identities - New Entry

Name:

Remote authentication: RSA signature

Rem. dig. signature profile: DEFAULT-ECDSA

EAP profile:

Remote identifier type: No identity

Remote identifier:

Remote password: □ Show

PPK-ID:

Remote cert. ID check: No

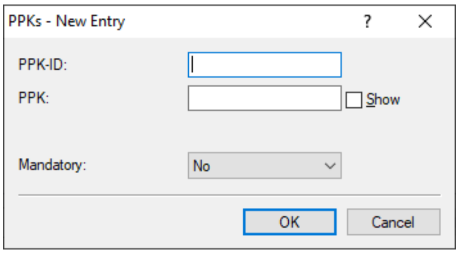
OCSP check: No

CRL check: Yes

PPK ID

Enter the name of the PPK-ID (Post-quantum Preshared Keys as per *RFC 8784*) from the table of PPKs.

Table VPN > IKEv2/IPSec > Extended settings > Authentication > PPKs



PPKs - New Entry

PPK-ID:

PPK: □ Show

Mandatory: No

PPK-ID

Set a unique name for this entry. The input format can be a string or hexadecimal number (identified by a leading 0x).

PPK

Enter the post-quantum preshared key here as a character string or hexadecimal number (identified by a leading 0x).

Required

If the use of PPKs is configured as required, the corresponding VPN connection will be rejected if the remote site does not support or has not configured a PPK. If the use of PPKs is configured as optional, both PPK and non-PPK connections are accepted.

RADIUS attributes

Corresponding RADIUS attributes are also supported:

ID	Name	Meaning
LANCOM 33	LCS-IKEv2-PPK	Specifies the post-quantum preshared key as a string or hexadecimal number (identified by a leading 0x).
LANCOM 34	LCS-IKEv2-PPK-MANDATORY	Specifies whether the use of the passed post-quantum preshared key (PPK) is required. If yes, the corresponding VPN connection will be rejected if the remote site does not support or has not configured a PPK. If the use of PPKs is configured as optional, both PPK and non-PPK connections are accepted.
LANCOM 33	LCS-IKEv2-PPK	Specifies the post-quantum preshared key as a string or hexadecimal number (identified by a leading 0x).
LANCOM 34	LCS-IKEv2-PPK-MANDATORY	Specifies whether the use of the passed post-quantum preshared key (PPK) is required. If yes, the corresponding VPN connection will be rejected if the remote site does not support or has not configured a PPK. If the use of PPKs is configured as optional, both PPK and non-PPK connections are accepted.

8.2.1 Additions to the Setup menu

PPK-ID

Points to a *PPK*.

SNMP ID:

2.19.36.3.1.18

Console path:

Setup > **VPN** > **IKEv2** > **Auth** > **Parameter**

Possible values:

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

Default:

empty

PPK-ID

Points to a *PPK*.

SNMP ID:

2.19.36.3.3.11

Console path:

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

Possible values:

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

Default:

empty

PPKs

Quantum computers pose a potential challenge to current cryptographic algorithms, such as those used in IKEv2 VPN. Current algorithms are considered to be very robust, but the challenge is that an attacker can record encrypted data today and decrypt it using quantum computers in the future.

The *RFC 8784* "Mixing Preshared Keys in the Internet Key Exchange Protocol Version 2 (IKEv2) for Post-quantum Security" offers a way to resist quantum computers when passwords (PSKs) are used. The extension works by "mixing" the standard IKEv2 password key (PSK) with another key in the form of a Post-quantum Preshared Key (PPK) to increase resistance.

Existing IKEv2 PSK tunnels can easily be supplemented with PPKs. The PPK is independent of the existing PSK.

LCOS supports manual configuration of PPKs. Automatic procedures for changing PPKs are not supported.

This table is used to configure the PPKs.

SNMP ID:

2.19.36.3.6

Console path:

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

PPK-ID

Set a unique name for this entry. The input format can be a string or hexadecimal number (identified by a leading 0x).

SNMP ID:

2.19.36.3.6.1

Console path:

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

Possible values:

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

Default:

empty

PPK

Enter the post-quantum preshared key here as a character string or hexadecimal number (identified by a leading 0x).

SNMP ID:

2.19.36.3.6.2

Console path:

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

Possible values:

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

Default:

empty

Required

If the use of PPKs is configured as required, the corresponding VPN connection will be rejected if the remote site does not support or has not configured a PPK. If the use of PPKs is configured as optional, both PPK and non-PPK connections are accepted.

SNMP ID:

2.19.36.3.6.3

Console path:

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

Possible values:

No
Yes

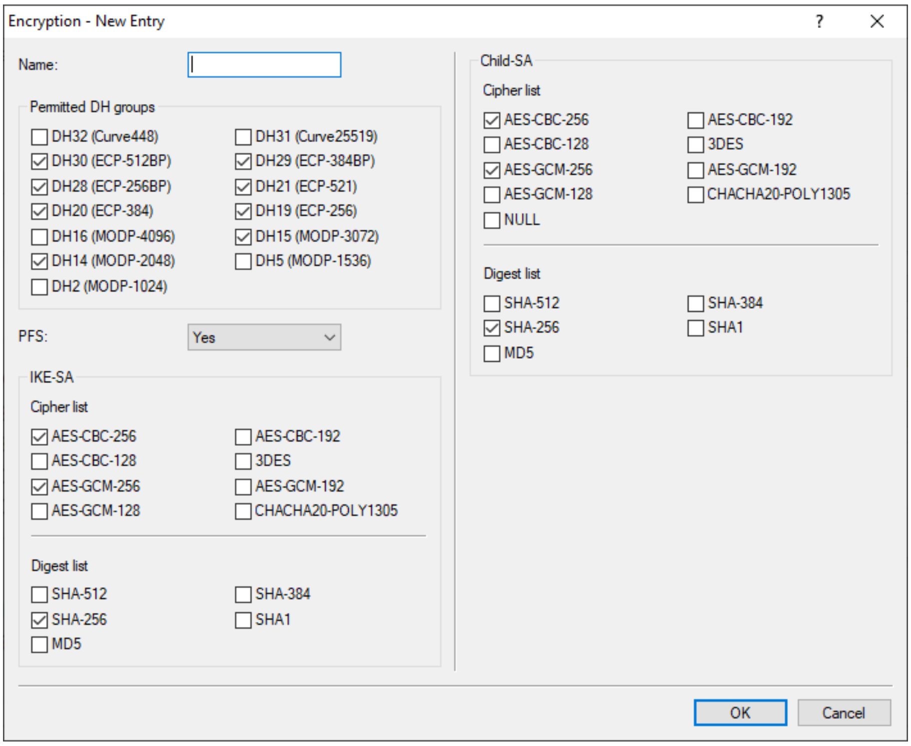
Default:

No

8.3 Null encryption in the IKEv2 child SA

As of LCOS 10.90 , zero encryption is supported in the IKEv2 child SA. Note that the data packets are no longer encrypted. This feature is only needed in special scenarios and is generally not recommended.

For this purpose, the cipher list in LANconfig has been expanded under **VPN** > **IKEv2 / IPSec** > **Encryption**.



Encryption - New Entry

Name:

Permitted DH groups

□ DH32 (Curve448)	□ DH31 (Curve25519)
☑ DH30 (ECP-512BP)	☑ DH29 (ECP-384BP)
☑ DH28 (ECP-256BP)	☑ DH21 (ECP-521)
☑ DH20 (ECP-384)	☑ DH19 (ECP-256)
□ DH16 (MODP-4096)	☑ DH15 (MODP-3072)
☑ DH14 (MODP-2048)	□ DH5 (MODP-1536)
□ DH2 (MODP-1024)	

PFS: Yes

IKE-SA

Cipher list

☑ AES-CBC-256	□ AES-CBC-192
□ AES-CBC-128	□ 3DES
☑ AES-GCM-256	□ AES-GCM-192
□ AES-GCM-128	□ CHACHA20-POLY1305

Digest list

□ SHA-512	□ SHA-384
☑ SHA-256	□ SHA1
□ MD5	

Child-SA

Cipher list

☑ AES-CBC-256	□ AES-CBC-192
□ AES-CBC-128	□ 3DES
☑ AES-GCM-256	□ AES-GCM-192
□ AES-GCM-128	□ CHACHA20-POLY1305
□ NULL	

Digest list

□ SHA-512	□ SHA-384
☑ SHA-256	□ SHA1
□ MD5	

Cipher list

- NULL

> The data packets are no longer encrypted. This feature is only needed in special scenarios and is generally not recommended.

8.3.1 Additions to the Setup menu

IKE-SA-Cipher-List

Specifies which encryption algorithms are enabled.

SNMP ID:

2.19.36.2.4

Console path:

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

Possible values:

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 data stream encryption in conjunction with the Poly1305 Authenticator, see *RFC 7634*, will be supported from LCOS version 10.40.

> ⓘ Please note that ChaCha20-Poly1305 is currently not accelerated by hardware and is therefore not recommended for VPN scenarios where high encryption performance is required.

NULL

> ⓘ The data packets are no longer encrypted here. This function is only required in special scenarios and is generally not recommended.

Default:

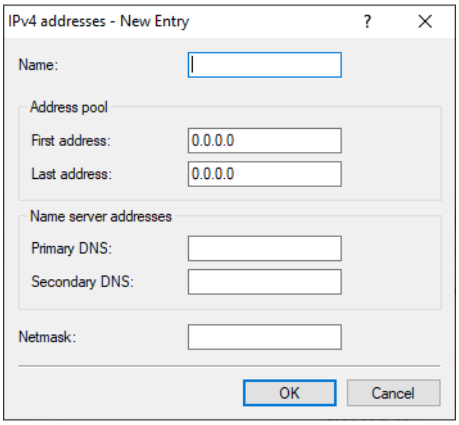
AES-CBC-256

AES-GCM-256

8.4 IKE-CFG sends subnet mask for the negotiated IP address

As of LCOS 10.90 the netmask (IPv4) or prefix length (IPv6) can be specified for the addresses assigned to the clients.

For this purpose, LANconfig now has the following parameters under **VPN** > **IKEv2 / IPSec** > **IPv4 addresses** or **VPN** > **IKEv2 / IPSec** > **IPv6 addresses**.



IPv4 addresses - New Entry

Name:

Address pool

First address: 0.0.0.0

Last address: 0.0.0.0

Name server addresses

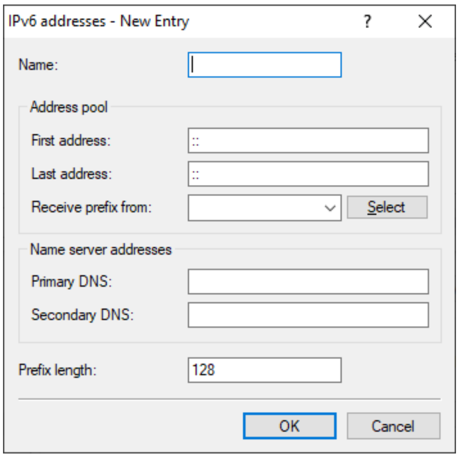
Primary DNS:

Secondary DNS:

Netmask:

Netmask

Optional netmask sent along with the negotiated IP address.



IPv6 addresses - New Entry

Name:

Address pool

First address: ::

Last address: ::

Receive prefix from:

Name server addresses

Primary DNS:

Secondary DNS:

Prefix length: 128

Prefix length

Optional prefix length sent for the negotiated IP address.

Corresponding RADIUS attributes are also supported:

ID	Name	Meaning
9	Framed IP netmask	Specifies the IP netmask to be configured for the client (in IKE-CFG mode “Server”). This attribute value causes a static route to be added for the framed IP address with the specified mask.
LANCOM 32	LCS-IPv6-Prefix-Length	Specifies the IPv6 prefix length to be configured for the client (in IKE-CFG mode “Server”).
9	Framed IP netmask	Specifies the IP netmask to be configured for the client (in IKE-CFG mode “Server”). This attribute value causes a static route to be added for the framed IP address with the specified mask.
LANCOM 32	LCS-IPv6-Prefix-Length	Specifies the IPv6 prefix length to be configured for the client (in IKE-CFG mode “Server”).

8.4.1 Additions to the Setup menu

Netmask

Optional netmask sent along with the negotiated IP address.

SNMP ID:

2.19.36.7.1.5

Console path:

Setup > **VPN** > **IKEv2** > **IKE-CFG** > **IPv4**

Possible values:

Max. 3 characters from `[0-9]`

Default:

empty

Prefix-Length

Optional prefix length sent for the negotiated IP address.

SNMP ID:

2.19.36.7.2.7

Console path:

Setup > **VPN** > **IKEv2** > **IKE-CFG** > **IPv6**

Possible values:

Max. 3 characters from `[0-9]`

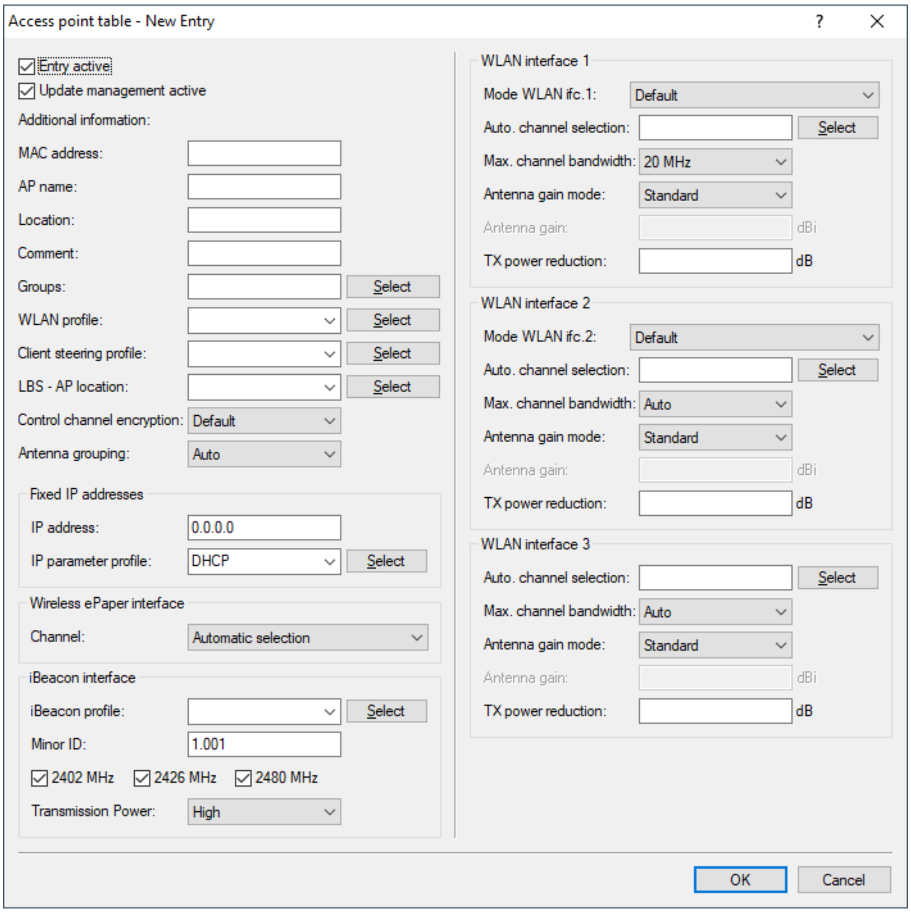
Default:

128

9 WLAN management

9.1 WLAN Management with Wi-Fi 7

As of LCOS 10.90, WLAN management supports Wi-Fi 7 access points such as the LANCOM LX-7300 and LANCOM LX-7500. These are now selectable in the **Firmware version management** under **WLAN Controller** > **AP Update** > **Firmware and script management**. Wi-Fi 7 (IEEE 802.11be) has also been added as a mode, along with 320 MHz as a possible maximum bandwidth for the third module.


Access point table - New Entry

☑ Entry active
☑ Update management active

Additional information:

MAC address:	
AP name:	
Location:	
Comment:	
Groups:	
WLAN profile:	
Client steering profile:	
LBS - AP location:	
Control channel encryption:	Default
Antenna grouping:	Auto

Fixed IP addresses

IP address:	0.0.0.0
IP parameter profile:	DHCP

Wireless ePaper interface

Channel:	Automatic selection

iBeacon interface

iBeacon profile:	
Minor ID:	1.001

☑ 2402 MHz ☑ 2426 MHz ☑ 2480 MHz

Transmission Power:	High

WLAN interface 1

Mode WLAN ifc.1:	Default
Auto. channel selection:	
Max. channel bandwidth:	20 MHz
Antenna gain mode:	Standard
Antenna gain:	dBi
TX power reduction:	dB

WLAN interface 2

Mode WLAN ifc.2:	Default
Auto. channel selection:	
Max. channel bandwidth:	Auto
Antenna gain mode:	Standard
Antenna gain:	dBi
TX power reduction:	dB

WLAN interface 3

Auto. channel selection:	
Max. channel bandwidth:	Auto
Antenna gain mode:	Standard
Antenna gain:	dBi
TX power reduction:	dB

Figure 1: WLAN Controller > AP Configuration > Access point table

9.1.1 Additions to the Setup menu

2.4GHz-Mode

Here you specify the radio standard(s) that the physical WLAN interface provides to the WLAN clients in the 2.4 GHz frequency band. Depending on the device type and selected frequency band, you have the option of operating an AP in just one particular mode or one of the compatibility modes.

Please observe that WLAN clients supporting only a slower standard may not be able to associate with the WLAN if the value for the mode is set too high. However, compatibility is always achieved at the expense of performance. It is therefore recommended to allow only those modes of operation that are absolutely necessary for the wireless LAN clients in use.

SNMP ID:

2.37.1.2.6

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Radioprofiles**

Possible values:

11bg mixed
802.11g/b (mixed)

11b-only
802.11b only (11Mbps)

11g-only
802.11g only (54Mbps)

108Mbps
802.11g++ (108Mbps mode / Turbo mode)

11bgn mixed
802.11g/b/n

11gn mixed
802.11g/n

Greenfield
802.11n only (greenfield mode)

11bgnax-mixed
802.11g/b/n/ax

11gnax-mixed
802.11g/n/ax

11bgnaxbe-mixed
802.11g/b/n/ax/be

11gnaxbe-mixed
802.11g/n/ax/be

Auto
Automatic. In the 2.4 GHz mode, automatic selection provides either **11bgn-mixed** or **11bg-mixed**.

Default:

Auto

5GHz-Mode

Here you specify the radio standard(s) that the physical WLAN interface provides to the WLAN clients in the 5 GHz frequency band. Depending on the device type and selected frequency band, you have the option of operating an AP in just one particular mode or one of the compatibility modes.

ⓘ Please observe that WLAN clients supporting only a slower standard may not be able to associate with the WLAN if the value for the mode is set too high. However, compatibility is always achieved at the expense of performance. It is therefore recommended to allow only those modes of operation that are absolutely necessary for the wireless LAN clients in use.

SNMP ID:

2.37.1.2.7

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Radioprofiles**

Possible values:

Normal
802.11g (54Mbps mode)

108Mbps
802.11g++ (108Mbps mode / Turbo mode)

11an mixed
802.11a/n (mixed)

Greenfield
802.11n only (greenfield mode)

11anac mixed
802.11a/n/ac (mixed)

11nac mixed
802.11n/ac (mixed)

11ac-only
802.11ac only

11anacax-mixed
802.11a/n/ac/ax (mixed)

11anacaxbe-mixed
802.11a/n/ac/ax/be (mixed)

Auto
Automatic. In the 5 GHz mode, automatic selection provides either **11anac-mixed**, **11an-mixed**, or **Normal**.

Default:

Auto

6GHz-Mode

Specify which radio standards the physical WLAN interface you configured supports against a WLAN client in the 6 GHz frequency band.

SNMP ID:

2.37.1.2.27

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Radioprofiles**

Possible values:

11axbe-mixed

802.11ax/be

Auto

Automatic. Within the 6 GHz mode, the automatic leads to 802.11ax.

Default:

Auto

Module-2-Max.-Channel-Bandwidth

Enter how and to what extent the AP specifies the channel bandwidth for the 2nd physical WLAN interface.

By default, the physical WLAN interface automatically determines the frequency range used to modulate the data onto the carrier signals. 802.11a/b/g use 48 carrier signals in one 20-MHz channel. The use of double the frequency range of 40 MHz means that 96 carrier signals can be used, resulting in a doubling of the data throughput.

802.11n can use 52 carrier signals in a 20-MHz channel for modulation, and even up to 108 carrier signals in a 40-MHz channel. The use of the 40 MHz option for 802.11n therefore means a performance gain of more than double.

SNMP ID:

2.37.1.4.25

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Accesspoints**

Possible values:

Auto

The AP automatically detects the maximum channel bandwidth.

20MHz

The AP uses channels bundled at 20 MHz.

40MHz

The AP uses channels bundled at 40MHz.

80MHz

The AP uses channels bundled at 80MHz.

80+80MHz

The AP uses two channels bundled at 80 MHz.

160MHz

The AP uses channels bundled at 160 MHz.

Default:

Auto

Module-1-Max.-Channel-Bandwidth

Enter how and to what extent the AP specifies the channel bandwidth for the 1st physical WLAN interface.

By default, the physical WLAN interface automatically determines the frequency range used to modulate the data onto the carrier signals. 802.11a/b/g use 48 carrier signals in one 20-MHz channel. The use of double the frequency range of 40 MHz means that 96 carrier signals can be used, resulting in a doubling of the data throughput.

802.11n can use 52 carrier signals in a 20-MHz channel for modulation, and even up to 108 carrier signals in a 40-MHz channel. The use of the 40 MHz option for 802.11n therefore means a performance gain of more than double.

SNMP ID:

2.37.1.4.26

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Accesspoints**

Possible values:

Automatic
The AP automatically detects the maximum channel bandwidth.

20MHz
The AP uses channels bundled at 20 MHz.

40MHz
The AP uses channels bundled at 40MHz.

80MHz
The AP uses channels bundled at 80MHz.

80+80MHz
The AP uses two channels bundled at 80 MHz.

160MHz
The AP uses channels bundled at 160 MHz.

Default:

Automatic

Module-3-Max.-Channel-Bandwidth

Enter how and to what extent the AP specifies the channel bandwidth for the 2nd physical WLAN interface.

SNMP ID:

2.37.1.4.40

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Accesspoints**

Possible values:

Auto
The AP automatically detects the maximum channel bandwidth.

20MHz
The AP uses channels bundled at 20 MHz.

40MHz
The AP uses channels bundled at 40 MHz.

80MHz
The AP uses channels bundled at 80 MHz.

80+80MHz
The AP uses two channels bundled at 80 MHz.

160MHz
The AP uses channels bundled at 160 MHz.

320MHz
The AP uses channels bundled at 320 MHz.

Default:

Auto

10 Public Spot

10.1 Public Spot Captive Portal API

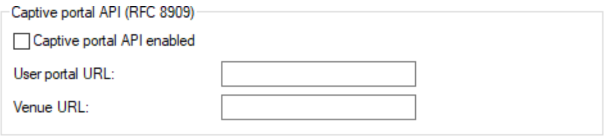
As of LCOS 10.90 the Public Spot supports the new Captive Portal API standard according to *RFC 8908*. The standard allows Wi-Fi clients in a hotspot to automatically find a captive portal or login page.

The client receives the URL of the portal page via DHCP and uses an API request to the hotspot to check whether a login is required or whether access is already permitted for the client. This significantly speeds up the user experience in a hotspot and, by defining a standard, now provides better manufacturer interoperability between hotspots and clients.

The following steps are required:

1. The use of TLS certificates in the Public Spot is mandatory. Without an HTTPS login, the client does not send a request to the portal.
2. The DHCP server must provide the Captive Portal DHCP option to the client.

The configuration in LANconfig is located under **Public-Spot** > **Server** > **Captive Portal API (RFC 8908)**.



Captive portal API (RFC 8909)

☐ Captive portal API enabled

User portal URL:

Venue URL:

Captive portal API enabled

Enables or disables the Captive Portal API function in the Public Spot.

User portal URL

(Optional) By default, the Captive Portal API supports TLS only. For this reason the device must have a trusted certificate and a DNS name. By default, the parameter can be left empty and it will be inserted automatically by the system. To do this, the device name must be configured in the Public Spot operating settings and agree with the TLS certificate. If an external hotspot server is used, a URL of this server can be entered here. Another requirement is that the clients in the hotspot must find the captive portal via DHCP option. For this purpose, the corresponding DHCP option according to *RFC 8910* must be configured for the hotspot network.

Venue URL

(Optional) URL (TLS) through which the operator can provide the user with additional information about the location of the hotspot, e.g. the website of the hotel with the hotspot.

Configure DHCPv4 option (according to RFC 8910)

In LANconfig, create a new table entry under **IPv4** > **DHCPv4** > **DHCP options**.

Option number

Number of the option that should be sent to the DHCP client. In this case 114.

Network name

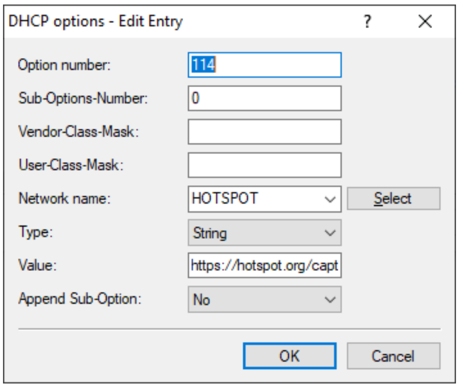
Name of the Public Spot network (see IPv4 networks)

Type

Entry type. In this case String.

Value

HTTPs URL of LANCOM router in the hotspot, e.g. “https://hotspot.org/captive-portal-api”. The DNS name, e.g. “hotspot.org”, is the device name of the router in the TLS certificate supplemented by the internal path of the Public Spot login page “captive-portal-api”. The hotspot client must be able to resolve the DNS name. Also, the device name must be configured in the Public Spot operating settings and agree with the TLS certificate.



DHCP options - Edit Entry

Option number:	114
Sub-Options-Number:	0
Vendor-Class-Mask:	
User-Class-Mask:	
Network name:	HOTSPOT
Type:	String
Value:	https://hotspot.org/capt
Append Sub-Option:	No

Configure DHCPv6 option (according to RFC8910)

In LANconfig, create a new table entry under **IPv6** > **DHCPv6** > **DHCPv6 server** > **Additional options**.

Interface name/Relay IP

Name of the Public Spot network (see IPv6 networks)

Option code

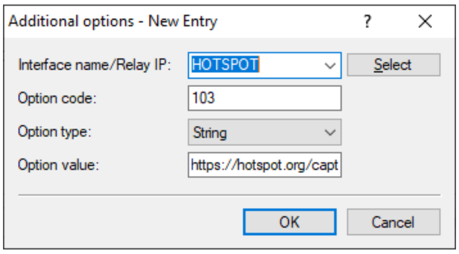
103

Option type

String

Option value

HTTPs URL of LANCOM router in the hotspot, e.g. “https://hotspot.org/captive-portal-api”. The DNS name, e.g. “hotspot.org”, is the device name of the router in the TLS certificate supplemented by the internal path of the Public Spot login page “captive-portal-api”. The hotspot client must be able to resolve the DNS name. Also, the device name must be configured in the Public Spot operating settings and agree with the TLS certificate.



Additional options - New Entry

Interface name/Relay IP:	HOTSPOT
Option code:	103
Option type:	String
Option value:	https://hotspot.org/capt

10.1.1 Additions to the Setup menu

Api-Server

The Public Spot supports the new Captive Portal API standard according to *RFC 8908*. The standard allows Wi-Fi clients in a hotspot to automatically find a captive portal or login page.

The client receives the URL of the portal page via DHCP and uses an API request to the hotspot to check whether a login is required or whether access is already permitted for the client. This significantly speeds up the user experience in a hotspot and, by defining a standard, now provides better manufacturer interoperability between hotspots and clients.

The following steps are required:

1. The use of TLS certificates in the Public Spot is mandatory. Without an HTTPS login, the client does not send a request to the portal.
2. The DHCP server must provide the Captive Portal DHCP option to the client.

SNMP ID:

2.24.63

Console path:

Setup > **Public-Spot-Module**

Operating

Enables or disables the Captive Portal API function in the Public Spot.

SNMP ID:

2.24.63.1

Console path:

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

Possible values:

No
Yes

Default:

No

User-Portal-URL

(Optional) By default, the Captive Portal API supports TLS only. For this reason the device must have a trusted certificate and a DNS name. By default, the parameter can be left empty and it will be inserted automatically by the system. To do this, the device name must be configured in the Public Spot operating settings and agree with the TLS certificate. If an external hotspot server is used, a URL of this server can be entered here. Another requirement is that the clients in the hotspot must find the captive portal via DHCP option. For this purpose, the corresponding DHCP option according to *RFC 8910* must be configured for the hotspot network.

SNMP ID:

2.24.63.2

Console path:

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

Possible values:

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

Default:

empty

Venue-Info-URL

(Optional) URL (TLS) through which the operator can provide the user with additional information about the location of the hotspot, e.g. the website of the hotel with the hotspot.

SNMP ID:

2.24.63.3

Console path:

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

Possible values:

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

Default:

empty

11 Backup solutions

11.1 VRRPv3

As of LCOS 10.90 the Virtual Router Redundancy Protocol Version 3 (VRRPv3) is supported.

The configuration by command line has been moved from **Setup** > **IP-Router** > **VRRP** to **Setup** > **VRRP**.

11.1.1 Interaction with the WAN backup module

The VRRP module is closely linked to the WAN backup module to enable interaction between the two functionalities. The interaction is in both directions: On the one hand, VRRP can request or prevent the establishment of WAN connections depending on the state of the virtual routers, and on the other hand, the connection state of a WAN connection (established/backup/disconnected) can influence the priority used by the virtual routers.

A virtual router in the VRRP interacts with a maximum of one WAN connection (and its backup connections), and only if the name of the WAN connection is entered in the column **Monitored interface** in the configuration table **Virtual routers**. If there is no entry for a virtual router, this router does not interact with the WAN backup module.

11.1.2 Control of WAN/WAN backup by VRRP

If virtual routers exist and are monitoring a WAN interface, but none of them is in the "Master" state, the VRRP requests a disconnect of the monitored WAN and prevents a reconnect. As soon as one of the routers changes to the Master state, the connection can be re-established and a connection attempt is started. Since WAN connections for IPv4 and IPv6 are established and terminated together, the IP version of the virtual routers is irrelevant. In general: If the VRRP control **VRRP activate** is not enabled, the VRRP has no influence on the WAN backup module.

Also note the switch **Setup** > **VRRP** > **WAN-Connection-Control** (2.141.7).

11.1.3 Configuration of VRRPv3

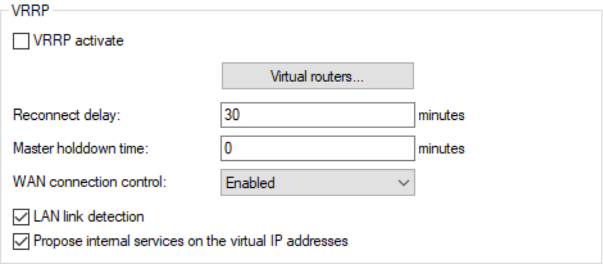
LCOS supports VRRPv2 and VRRPv3 (*RFC 5798* and also *RFC 9568*) for IPv4 and IPv6.

VRRP with IPv6 only works with static addresses or Network Prefix Translation (NPTv6) in the direction of the Internet provider.

VRRP operates independently for IPv4 and IPv6, even if configured together in a single line. This is even recommended to ensure that the advertisement interval and priorities are consistent.

The settings for VRRP can be found in LANconfig under **IP router** > **VRRP**.

Command line: **Setup** > **VRRP**



VRRP

□ VRRP activate

Reconnect delay: 30 minutes

Master holddown time: 0 minutes

WAN connection control: Enabled

☑ LAN link detection

☑ Propose internal services on the virtual IP addresses

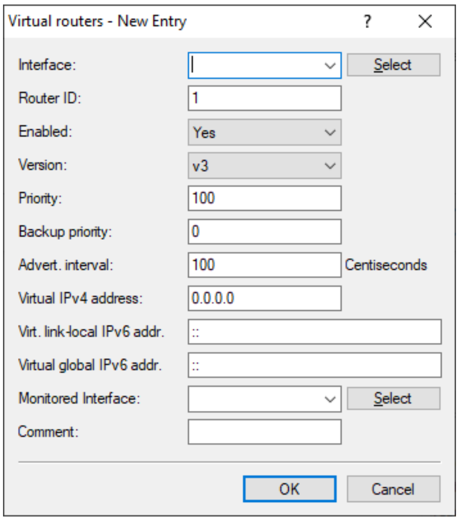
In order to configure failover (router redundancy) or load balancing with VRRP, the following parameters can be set:

VRRP activate

This switches the VRRP module on or off (default: Off).

Virtual routers

In the Virtual Routers table, the virtual routers can be defined for each interface.



Virtual routers - New Entry

Interface:		Select
Router ID:	1	
Enabled:	Yes	
Version:	v3	
Priority:	100	
Backup priority:	0	
Advert. interval:	100	Centiseconds
Virtual IPv4 address:	0.0.0.0	
Virt. link-local IPv6 addr.:	::	
Virtual global IPv6 addr.:	::	
Monitored Interface:		Select
Comment:		

Interface

Logical IPv4 or IPv6 interface or network on which VRRP should be enabled. In principle, only LAN interfaces are meaningful. Other interfaces can be selected but may lead to undefined behavior.

Router ID

Unique ID for the virtual router. Values between 1 and 255 are possible. The router ID is used to consolidate several physical routers into a single virtual router or a standby group. The router ID is sometimes called VRRP ID or VRID for short.

Enabled

Enables or disables VRRP for this configuration entry.

Version

Defines which VRRP version should be used. Supported are VRRPv2, VRRPv3, or VRRPv2 and VRRPv3. IPv6 is only supported with VRRPv3. IPv4 is supported in both VRRPv2 and VRRPv3.

The v2+v3 mode is intended as a transitional solution for the move from VRRPv2 to VRRPv3 operation under IPv4. It doubles the packet volume, since a virtual router configured in this way sends advertisements in both protocol versions.

A virtual router configured to use one protocol version will discard advertisements from other routers if they have the wrong protocol version, it will be output to the VRRP packet trace and add an entry to the event log table.

Priority

Specifies the priority with which the virtual router operates. This is transmitted in the advertisements and largely determines which device is the master for a VRRP network. The specified priority must be greater than 0. The value 255 has a special meaning:

- The value 255 is automatically set if the virtual router's address is the same as the address of the interface to which the router is bound. In all other cases, the priority is automatically lowered.

Backup priority

The backup priority of the virtual router refers to the interface for which a backup connection is configured, i.e. with routers with DSL and cellular support to the cellular interface. Values between 0 and the configured priority are permitted. The value 0 has a special meaning:

- 0 disables the virtual router in the backup event. Checks are conducted regularly in order to determine whether or not the standard connection can be reestablished. The inspection interval is defined in the reconnect delay.

When the backup connection cannot be established in backup mode, then the virtual router logs off completely and attempts to reestablish the standard or backup connection in intervals defined by the reconnect delay.

Advert. interval

The advertisement interval specifies the time until a virtual router is propagated again. The default value is 100 centiseconds (1 second).

Additionally, version v2 or v2+v3 require the interval to be an integer of 100, since for VRRPv2 the interval must be an integer number of seconds. If the version is subsequently changed, the advert interval is automatically adjusted to a valid value and should be checked.

ⓘ With a propagation time of 1 second, the routers in the VRRP group can change quickly when a device or interface fails. An interruption of this type will usually remain undetected due to the fact that the TCP connection is not interrupted. Other routing protocols require up to 5 minutes or longer in order to conduct the transfer to a backup router.

Virtual IPv4 address

Defines the virtual IPv4 address of the virtual router. The address must be identical on all routers in the VRRP network.

To avoid conflicts, virtual IP addresses should only be IP addresses that are not dynamically assigned to end devices that do not speak VRRP.

If the assigned virtual IPv4 corresponds to the physical address of the device on the LAN interface, the configured priorities and backup priorities are ignored and priority 255 is always used instead, in compliance with RFC.

ⓘ An unspecified IPv4 address (0.0.0.0) disables IPv4 for this configuration entry.

Virtual link-local IPv6 address

Defines the virtual link-local IPv6 address of the virtual router, for example fe80::1. The address must be identical on all routers in the VRRP network. This address is used as the sender address for sending router advertisements. The parameter is only supported in VRRPv3 mode.

ⓘ Assigning a virtual link-local address is mandatory to define a virtual router for IPv6.

If the assigned link-local virtual IPv6 corresponds to the physical address of the device on the LAN interface, the configured priorities and backup priorities are ignored and priority 255 is always used instead, in compliance with RFC.

ⓘ An unspecified IPv6 address (::) disables IPv6 for this configuration entry.

Virtual global IPv6 address

Defines the optional global IPv6 address of the virtual router, for example 2001:db8::1. The address must be identical on all routers in the VRRP network. The parameter is only supported in VRRPv3 mode.

This address is required for the VPN load balancer if it is to operate with IPv6.

Monitored interface

Name of the remote site that controls the virtual router behavior. The remote site can still also be assigned to other virtual routers.

Entering the remote site is optional. Linking the backup requirement to a remote site allows the use of the LANCOM-specific enhancement to VRRP not only to secure against device failure (VRRP standard) but also against interface failure or disruption at a remote site.

Comment

Enter a comment for this entry.

Reconnect delay

This specifies the number of minutes before a virtual router that has logged off attempts to reestablish its main connection. The router remains logged off during this connection attempt. It is only broadcasted with its main or backup priority after the connection has been established successfully. The default value is 30 minutes. Input is entered as <minutes>:<seconds>.

Master holddown time

If a time is configured here, the virtual router changes to the "Hold-Down" state as soon as the monitored WAN connection is terminated with an error and the backup delay expires (i.e. switches to backup state). In the "Hold-Down" state, the monitored WAN connection can no longer be established. Also, no further VRRP advertisements will be sent.

As soon as the "Master-Holddown-Time" expires, the virtual router transitions to the "Standby" state, in which the monitored WAN connection can be reestablished.

The "Master-Holddown-Time" is a string with a maximum of 6 characters, which may include the digits 0-9 and a colon. This allows the entry of times of up to 999 minutes 59 seconds (999:59).

If there is no colon (e.g. "30") then the specification is interpreted as minutes. In this case the maximum is "999".

If a colon is present, the colon must be followed by two characters that are interpreted as seconds. The maximum possible value here is "59".

Correct time specifications are, for example "5" (5 minutes), "5:30" (5 minutes, 30 seconds) or "0:30" (30 seconds).

A value of "0" or "0:00" disables the Master-Holddown.

WAN connection control

Defines whether VRRP should suppress the connection establishment of the monitored WAN counterpart in the standby role. Possible values:

Enabled

In the standby role, the connection establishment of the monitored WAN counterpart is not suppressed, and the WAN connection is established. Additionally, in this case, the routes to the monitored WAN are not switched when the virtual router goes into standby.

Packets sent to the physical MAC address of the router are not forwarded to the master in the standby state.

Disabled

In the standby role, the connection establishment of the monitored WAN counterpart is suppressed.

LAN link detection

Specifies whether the WAN connection should be established if no LAN connection is available.

The feature is relevant for a scenario where the router is still in operation without a LAN connection, but management of the router should be possible via the WAN connection. In this scenario, the LAN-link detection has to be deactivated.

Propose internal services on the virtual IPs

This item controls whether the virtual router is assigned as a DNS server in DHCPv4, DHCPv6 and Router Advertisement.

11.1.4 Additions to the Setup menu

VRRP

This menu contains the configuration of VRRP for your IP router.

The Virtual Router Redundancy Protocol enables multiple physical routers to appear as a single “virtual” router. Of the existing physical routers, one is always the "master". The master is the only router that establishes a data connection to the Internet, for example, and transfers data. Only when the master fails, for example as a result of a power outage or if its Internet connection is dropped, will the other routers become active. They will then negotiate with the VRRP protocol to determine which router should assume the role of master. The new master completely takes over the tasks that were carried out by the previous master.

ⓘ VRRP operates independently for IPv4 and IPv6, even if configured together in a single line. This is even recommended to ensure that the advertisement interval and priorities are consistent.

SNMP ID:

2.141

Console path:

Setup

Operating

Switch the VRRP module on and off.

SNMP ID:

2.141.1

Console path:

Setup > **VRRP**

Possible values:

Yes
No

Default:

No

Virtual-Routers

In the Virtual Routers table, the virtual routers can be defined for each interface.

SNMP ID:

2.141.2

Console path:

Setup > **VRRP**

Interface

Logical IPv4 or IPv6 interface or network on which VRRP should be enabled. Only LAN interfaces are supported.

SNMP ID:

2.141.2.1

Console path:

Setup > **VRRP** > **Virtual-Routers**

Possible values:

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

Default:

empty

Router-ID

Unique ID for the virtual router. The router ID is used to consolidate several physical routers into a single virtual router or a standby group. The router ID is sometimes called VRRP ID or VRID for short.

SNMP ID:

2.141.2.2

Console path:

Setup > **VRRP** > **Virtual-Routers**

Possible values:

1 … 255

Default:

1

Enabled

Enables or disables VRRP on the interface.

SNMP ID:

2.141.2.3

Console path:

Setup > **VRRP** > **Virtual-Routers**

Possible values:

Yes
No

Default:

Yes

Version

Defines which VRRP version should be used. Supported are VRRPv2, VRRPv3, or VRRPv2 and VRRPv3. IPv6 is only supported with VRRPv3. IPv4 is supported in both VRRPv2 and VRRPv3.

The v2+v3 mode is intended as a transitional solution for the move from VRRPv2 to VRRPv3 operation under IPv4. It doubles the packet volume, since a virtual router configured in this way sends advertisements in both protocol versions.

A virtual router configured to use one protocol version will discard advertisements from other routers if they have the wrong protocol version, it will be output to the VRRP packet trace and add an entry to the event log table.

SNMP ID:

2.141.2.4

Console path:

Setup > **VRRP** > **Virtual-Routers**

Possible values:

v2
v3
v2+v3

Default:

v3

Prio

Specifies the priority with which the virtual router operates. This is transmitted in the advertisements and largely determines which device is the master for a VRRP network. The specified priority must be greater than 0. The value 255 has a special meaning:

- The value 255 is automatically set if the virtual router's address is the same as the address of the interface to which the router is bound. In all other cases, the priority is automatically lowered.

SNMP ID:

2.141.2.5

Console path:

Setup > **VRRP** > **Virtual-Routers**

Possible values:

Max. 3 characters from `[0-9]`

Default:

100

Backup-Prio

The backup priority of the virtual router refers to the interface for which a backup connection is configured, i.e. with routers with DSL and cellular support to the cellular interface. Values between 0 and the configured priority are permitted. The value 0 has a special meaning:

- 0 disables the virtual router in the backup event. Checks are conducted regularly in order to determine whether or not the standard connection can be reestablished. The inspection interval is defined in the reconnect delay.

When the backup connection cannot be established in backup mode, then the virtual router logs off completely and attempts to reestablish the standard or backup connection in intervals defined by the reconnect delay.

SNMP ID:

2.141.2.6

Console path:

Setup > **VRRP** > **Virtual-Routers**

Possible values:

Max. 3 characters from `[0-9]`

Default:

0

Advert.-Interval

The advertisement interval specifies the time until a virtual router is propagated again. The default value is 100 centiseconds (1 second).

Additionally, version v2 or v2+v3 require the interval to be an integer of 100, since for VRRPv2 the interval must be an integer number of seconds. If the version is subsequently changed, the advert interval is automatically adjusted to a valid value and should be checked.

ⓘ With a propagation time of 1 second, the routers in the VRRP group can change quickly when a device or interface fails. An interruption of this type will usually remain undetected due to the fact that the TCP connection is not interrupted. Other routing protocols require up to 5 minutes or longer in order to conduct the transfer to a backup router.

SNMP ID:

2.141.2.7

Console path:

Setup > **VRRP** > **Virtual-Routers**

Possible values:

Max. 5 characters from `[0-9]`

Default:

100

Virtual-IPv4

Defines the virtual IPv4 address of the virtual router. The address must be identical on all routers in the VRRP network.

To avoid conflicts, virtual IP addresses should only be IP addresses that are not dynamically assigned to end devices that do not speak VRRP.

If the assigned virtual IPv4 corresponds to the physical address of the device on the LAN interface, the configured priorities and backup priorities are ignored and priority 255 is always used instead, in compliance with RFC.

ⓘ An unspecified IPv4 address (0.0.0.0) disables IPv4 for this configuration entry.

SNMP ID:

2.141.2.8

Console path:

Setup > **VRRP** > **Virtual-Routers**

Possible values:

Max. 15 characters from `[0-9].`

Link-Local-Virtual-IPv6

Defines the virtual link-local IPv6 address of the virtual router, for example fe80::1. The address must be identical on all routers in the VRRP network. This address is used as the sender address for sending router advertisements. The parameter is only supported in VRRPv3 mode.

ⓘ Assigning a virtual link-local address is mandatory to define a virtual router for IPv6.

If the assigned link-local virtual IPv6 corresponds to the physical address of the device on the LAN interface, the configured priorities and backup priorities are ignored and priority 255 is always used instead, in compliance with RFC.

ⓘ An unspecified IPv6 address (::) disables IPv6 for this configuration entry.

SNMP ID:

2.141.2.9

Console path:

Setup > **VRRP** > **Virtual-Routers**

Possible values:

Max. 39 characters from `[A-F][a-f][0-9]:.`

Global-Virtual-IPv6

Defines the optional global IPv6 address of the virtual router, for example 2001:db8::1. The address must be identical on all routers in the VRRP network. The parameter is only supported in VRRPv3 mode.

> ⓘ This address is required for the VPN load balancer if it is to operate with IPv6.

SNMP ID:

2.141.2.10

Console path:

Setup > **VRRP** > **Virtual-Routers**

Possible values:

Max. 39 characters from `[A-F][a-f][0-9]:.`

Monitored-WAN

Name of the remote site that controls the virtual router behavior. The remote site can still also be assigned to other virtual routers.

Entering the remote site is optional. Linking the backup requirement to a remote site allows the use of the LANCOM-specific enhancement to VRRP not only to secure against device failure (VRRP standard) but also against interface failure or disruption at a remote site.

SNMP ID:

2.141.2.11

Console path:

Setup > **VRRP** > **Virtual-Routers**

Possible values:

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

Default:

empty

Comment

Enter a comment for this entry.

SNMP ID:

2.141.2.12

Console path:

Setup > **VRRP** > **Virtual-Routers**

Possible values:

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

Default:

empty

Master-Holddown-Time

If a time is configured here, the virtual router changes to the “Hold-Down” state as soon as the monitored WAN connection is terminated with an error and the backup delay expires (i.e. switches to backup state). In the “Hold-Down” state, the monitored WAN connection can no longer be established. Also, no further VRRP advertisements will be sent.

As soon as the “Master-Holddown-Time” expires, the virtual router transitions to the “Standby” state, in which the monitored WAN connection can be reestablished.

The “Master-Holddown-Time” is a string with a maximum of 6 characters, which may include the digits 0-9 and a colon. This allows the entry of times of up to 999 minutes 59 seconds (999:59).

If there is no colon (e.g. “30”) then the specification is interpreted as minutes. In this case the maximum is “999”.

If a colon is present, the colon must be followed by two characters that are interpreted as seconds. The maximum possible value here is “59”.

Correct time specifications are, for example “5” (5 minutes), “5:30” (5 minutes, 30 seconds) or “0:30” (30 seconds).

A value of “0” or “0:00” disables the Master-Holddown.

SNMP ID:

2.141.3

Console path:

Setup > **VRRP**

Possible values:

Max. 6 characters from `[0-9]:`

Default:

0:00

Reconnect-Delay

The router will no longer be propagated if the backup connection could not be established. The reconnect delay specifies after how many minutes such a router should in this case attempt to establish its main or backup connection. While the attempt is being made, the router will not be propagated. Input is entered as <minutes>:<seconds>.

SNMP ID:

2.141.4

Console path:

Setup > **VRRP**

Possible values:

Max. 6 characters from `[0-9]:`

Default:

30:00

Assign-Internal-Services

This item controls whether the virtual router is assigned as a DNS server in DHCPv4, DHCPv6 and Router Advertisement.

SNMP ID:

2.141.5

Console path:

Setup > **VRRP**

Possible values:

Yes
No

Default:

Yes

Lan-Link-Detection

Specifies whether the WAN connection should be established if no LAN connection is available.

The feature is relevant for a scenario where the router is still in operation without a LAN connection, but management of the router should be possible via the WAN connection. In this scenario, the LAN-link detection has to be deactivated.

SNMP ID:

2.141.6

Console path:

Setup > **VRRP**

Possible values:

Yes
No

Default:

Yes

WAN-Connection-Control

Defines whether VRRP should suppress the connection establishment of the monitored WAN remote peer in standby mode.

SNMP ID:

2.141.7

Console path:

Setup > **VRRP**

Possible values:

Disabled

In standby mode, the connection establishment of the monitored WAN remote peer is not suppressed, and the WAN connection is established. Additionally, in this case, the routes to the monitored WAN are not switched when the virtual router switches to standby.

❗ Packets sent to the physical MAC address of the router are not forwarded to the master in standby mode.

Enabled

In standby mode, the connection establishment of the monitored WAN remote peer is suppressed.

Default:

Enabled

V2-Checksum-for-IPv4

Defines how the checksum of VRRPv3 packets for IPv4 should be calculated. For compatibility reasons with third-party network devices, the checksum for VRRPv3 IPv4 can be calculated as in VRRPv2.

SNMP ID:

2.141.8

Console path:

Setup > **VRRP**

Possible values:

Yes

Calculate the checksum for VRRPv3 IPv4 as in VRRPv2.

No

Do not calculate the checksum for VRRPv3 IPv4 as in VRRPv2.

Default:

No

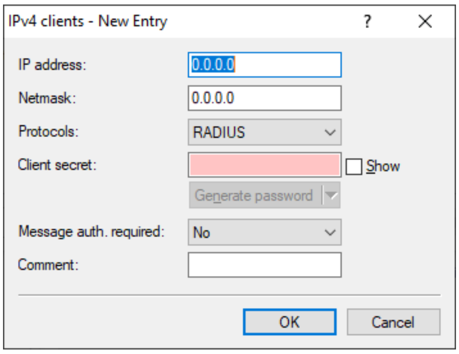
12 RADIUS

12.1 RADIUS message authenticator check

As of LCOS 10.90, the new parameter **Message-Authenticator Required** has been introduced in multiple locations.

In LANconfig, you can find these under

- **Communication** > **RADIUS**,
- **RADIUS** > **Server** > **RADIUS-/RADSEC clients** > **IPv4 clients**,
- **RADIUS** > **Server** > **RADIUS-/RADSEC clients** > **IPv6 clients**,
- **RADIUS** > **Server** > **Extended configuration** > **Forwarding** > **Forwarding server**,
- **Management** > **Authentication** > **RADIUS authentication** > **RADIUS servers** and
- **VPN** > **IKEv2/IPSec** > **Extended settings** > **RADIUS authentication** > **RADIUS server**.


IPv4 clients - New Entry

IP address: 0.0.0.0
Netmask: 0.0.0.0
Protocols: RADIUS
Client secret: □ Show
Message auth. required: No
Comment:

Figure 2: Example in LANconfig

Message Auth. required

Defines whether the presence of the message authenticator attribute in RADIUS messages is enforced on the client side. The client side is the side that receives the RADIUS accept/fail.

12.1.1 Additions to the Setup menu

Require-Msg-Authenticator

Defines whether the presence of the message authenticator attribute in RADIUS messages is enforced on the client side. The client side is the side that receives the RADIUS accept/fail.

SNMP ID:

2.2.22.28

Console path:

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

Possible values:

No
Access requests do not have to contain a message authenticator.

Yes
Access requests must always contain a message authenticator.

Default:

No

L2TP-Require-Msg-Authenticator

Defines whether the presence of the message authenticator attribute in RADIUS messages is enforced on the client side. The client side is the side that receives the RADIUS accept/fail.

SNMP ID:

2.2.22.29

Console path:

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

Possible values:

No
Access requests do not have to contain a message authenticator.

Yes
Access requests must always contain a message authenticator.

Default:

No

Require-Msg-Authenticator

Defines whether the presence of the message authenticator attribute in RADIUS messages is enforced on the client side. The client side is the side that receives the RADIUS accept/fail.

SNMP ID:

2.11.81.1.10

Console path:

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

Possible values:

No
Access requests do not have to contain a message authenticator.

Yes
Access requests must always contain a message authenticator.

Default:

No

Require-Msg-Authenticator

Defines whether the presence of the message authenticator attribute in RADIUS messages is enforced on the client side. The client side is the side that receives the RADIUS accept/fail.

SNMP ID:

2.12.29.21

Console path:

Setup > **WLAN** > **RADIUS-Access-Check**

Possible values:

No
Access requests do not have to contain a message authenticator.

Yes
Access requests must always contain a message authenticator.

Default:

No

Backup-Require-Msg-Authenticator

Defines whether the presence of the message authenticator attribute in RADIUS messages is enforced on the client side. The client side is the side that receives the RADIUS accept/fail.

SNMP ID:

2.12.29.22

Console path:

Setup > **WLAN** > **RADIUS-Access-Check**

Possible values:

No
Access requests do not have to contain a message authenticator.

Yes
Access requests must always contain a message authenticator.

Default:

No

Require-Msg-Authenticator

Defines whether the presence of the message authenticator attribute in RADIUS messages is enforced on the client side. The client side is the side that receives the RADIUS accept/fail.

SNMP ID:

2.19.36.9.1.1.11

Console path:

Setup > **VPN** > **IKEv2** > **RADIUS** > **Authorization** > **Server**

Possible values:

No
Access requests do not have to contain a message authenticator.

Yes
Access requests must always contain a message authenticator.

Default:

No

Require-Msg-Authenticator

Defines whether the presence of the message authenticator attribute in RADIUS messages is enforced on the client side. The client side is the side that receives the RADIUS accept/fail.

SNMP ID:

2.25.10.2.6

Console path:

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

Possible values:

No
Access requests do not have to contain a message authenticator.

Yes
Access requests must always contain a message authenticator.

Proxy-Only
If an access request contains a proxy state attribute, a message authenticator must be included.

Default:

No

Require-Msg-Authenticator

Defines whether the presence of the message authenticator attribute in RADIUS messages is enforced on the client side. The client side is the side that receives the RADIUS accept/fail.

SNMP ID:

2.25.10.3.18

Console path:

Setup > **RADIUS** > **Server** > **Forward-Servers**

Possible values:

No
Access requests do not have to contain a message authenticator.

Yes
Access requests must always contain a message authenticator.

Default:

No

Require-Msg-Authenticator

Defines whether the presence of the message authenticator attribute in RADIUS messages is enforced on the client side. The client side is the side that receives the RADIUS accept/fail.

SNMP ID:

2.25.10.16.6

Console path:

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

Possible values:

No

Access requests do not have to contain a message authenticator.

Yes

Access requests must always contain a message authenticator.

Proxy-Only

If an access request contains a proxy state attribute, a message authenticator must be included.

Default:

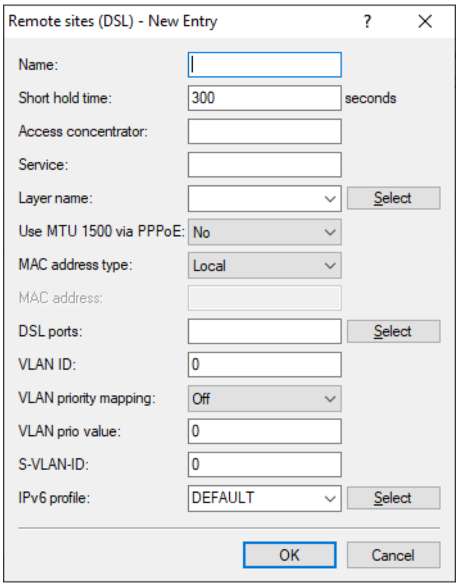
No

13 Other services

13.1 Support for MTU 1500 in PPPoE according to RFC 4638

As of LCOS 10.90, MTU 1500 in the PPPoE as per *RFC 4638* is supported.

Two new parameters have been introduced. The first can be found in DSL broadband remote site settings under **Communication** > **Remote Sites** > **Remote Sites (DSL)**.



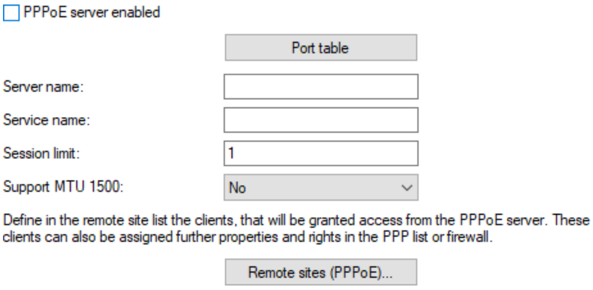
Remote sites (DSL) - New Entry

Name:	
Short hold time:	300 seconds
Access concentrator:	
Service:	
Layer name:	
Use MTU 1500 via PPPoE:	No
MAC address type:	Local
MAC address:	
DSL ports:	
VLAN ID:	0
VLAN priority mapping:	Off
VLAN prio value:	0
S-VLAN-ID:	0
IPv6 profile:	DEFAULT

Use MTU 1500 via PPPoE

Defines, if the devices should negotiate a PPPoE MTU of 1500 based on *RFC 4638*. The remote peer must support this extension as well.

The second new parameter is found in the PPPoE server settings. In LANconfig under **Communication** > **General**.



□ PPPoE server enabled

Server name:	
Service name:	
Session limit:	1
Support MTU 1500:	No

Define in the remote site list the clients, that will be granted access from the PPPoE server. These clients can also be assigned further properties and rights in the PPP list or firewall.

Support MTU 1500

Defines, if the devices should negotiate a PPPoE MTU of 1500 based on *RFC 4638*. The remote peer must support this extension as well.

13.1.1 Additions to the Setup menu

PPPoE-MTU-1500

Defines, if the devices should negotiate a PPPoE MTU of 1500 based on *RFC 4638*. The remote peer must support this extension as well.

SNMP ID:

2.2.19.22

Console path:

Setup > **WAN** > **DSL-Broadband-Peers**

Possible values:

Yes
No

Default:

No

MTU-1500

Defines, if the devices should negotiate a PPPoE MTU of 1500 based on *RFC 4638*. The remote peer must support this extension as well.

SNMP ID:

2.31.7

Console path:

Setup > **PPPoE-Server**

Possible values:

Yes
No

Default:

No

13.2 Operations, Administration, and Management (OAM)

Ethernet OAM according to IEEE 802.3ah is used by ISPs to monitor an Ethernet-based **last mile**, for example, in FTTH or VDSL2 access.

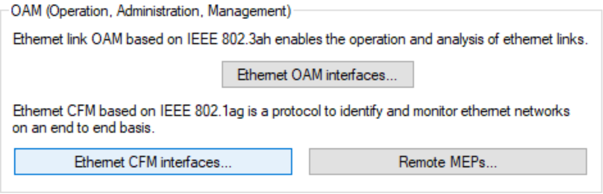
For this purpose, the active side, usually representing the ISP side, regularly transmits OAM packets (OAM Protocol Data Units – OAMPDUs). The passive side, usually representing the CPE side, responds to these OAMPDUs and replies. This verifies the reachability of the other side. This process is called **OAM Discovery**.

Previously, this feature was only available in the CLI. As of LCOS 10.90, two parameters have been added, and the feature has been exposed in LANconfig.

As of LCOS 10.90, Connectivity Fault Management (CFM) according to IEEE 802.1ag / ITU-T Y.1731 is also supported.

Connectivity Fault Management (CFM) according to IEEE 802.1ag / ITU-T Y.1731 is a collection of protocols and tools for so-called OAM on Layer 2. CFM is used for monitoring and fault analysis in LANs, bridges, or Ethernet-based WANs.

In LANconfig, you can configure OAM under **Miscellaneous Services** > **Services** > **OAM (Operation, Administration, Management)**.



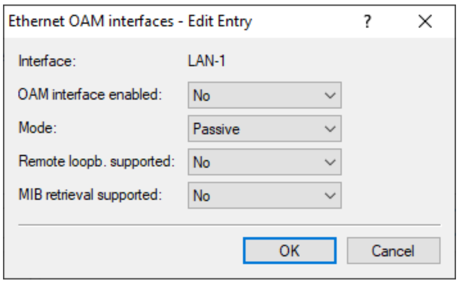
OAM (Operation, Administration, Management)

Ethernet link OAM based on IEEE 802.3ah enables the operation and analysis of ethernet links.

Ethernet CFM based on IEEE 802.1ag is a protocol to identify and monitor ethernet networks on an end to end basis.

13.2.1 Ethernet Link OAM (IEEE 802.3ah)

In LANconfig, configure Ethernet OAM according to IEEE 802.3ah under **Miscellaneous Services** > **Services** > **OAM (Operation, Administration, Management)** > **Ethernet OAM interfaces**.



Ethernet OAM interfaces - Edit Entry

Interface: LAN-1
OAM interface enabled: No
Mode: Passive
Remote loopb. supported: No
MIB retrieval supported: No

Interface

Name of the interface.

OAM interface enabled

Enables/disables OAM on the respective interface.

Mode

Defines the mode (Active/Passive) for the respective interface.

Active

The passive side (usually the CPE side) responds to the OAM packets (OAMPDUs) sent by the sender.

Passive (Default)

The active side (usually the internet provider) sends the OAM packets (OAMPDUs) to the receiver.

Remote loopback supported

Defines whether the device can be placed into loopback mode by the remote side. In loopback mode, the device disables forwarding and sends all received packets back on the interface. The packet is sent back exactly as it was received, with no mirroring of MAC or IP addresses.

MIB retrieval supported

Defines whether the device allows the remote side to retrieve specific status values or counters from the device via packets.

The following two commands are supported on the CLI:

Additions to the Setup menu

Remote-Loopback-Supported

Defines whether the device can be placed into loopback mode by the remote side. In loopback mode, the device disables forwarding and sends all received packets back on the interface. The packet is sent back exactly as it was received, without mirroring MAC or IP addresses.

SNMP ID:

2.105.1.4

Console path:

Setup > **OAM** > **Interfaces**

Possible values:

Yes

The device can be placed into loopback mode by the remote side.

No

The device cannot be placed into loopback mode by the remote side.

Default:

No

MIB-Retrieval-Supported

Defines whether the device allows the remote side to retrieve specific status values or counters from the device via packets.

SNMP ID:

2.105.1.5

Console path:

Setup > **OAM** > **Interfaces**

Possible values:

Yes

The device supports MIB retrieval.

No

The device does not support MIB retrieval.

Default:

No

Remote-Loopback

With this command, the device sends a Loopback Control OAMPDU to the counterpart, causing the counterpart to enter or exit the loopback mode accordingly. In loopback mode, the counterpart device sets the forwarding mode on this interface and returns all received packets. The packet is sent back exactly as it was received, without mirroring MAC or IP addresses.

SNMP ID:

2.105.4

Console path:

Setup > **OAM**

Possible arguments:

-i <interface>

Specifies the interface on which to start or stop the loopback mode. The device sends the message on this interface to place the remote side into loopback mode or to terminate it there.

Possible values from the OAM setup table, e.g., LAN-1, DSL-1, …

[-?]

Displays brief help for the parameters.

<start|stop>

Starts or stops loopback mode.

Variable-Read

This command allows the device to send a Variable Request OAMPDU to the remote side. The remote side responds with the value of the requested variable based on the local MIB. This method can be used to read packet counters on the remote side, for example. The remote side must support the feature of reading MIB variables via OAM.

Variables from IEEE 802.3.1 are supported, among others.

Example:

```
> do Variable-Read -i LAN-3 aFramesTransmittedOK

aFramesTransmittedOK = 8444
OK: Action Variable-Read done
```

SNMP ID:

2.105.6

Console path:

Setup > **OAM**

Possible arguments:

-i <interface>

Specifies the interface from which the variable is to be read.

[-?]

Displays brief help for the parameters.

<variable name> [more variable names]

One or more variable names separated by spaces.

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

Connectivity Fault Management (CFM) as per IEEE 802.1ag / ITU-T Y.1731 is a collection of protocols and tools for OAM on Layer 2. CFM is used for monitoring and fault analysis in LANs, bridges, or Ethernet-based WANs.

The protocols particularly enable providers or operators and administrators of Ethernet connections to proactively monitor these connections or analyze them in case of faults.

LCOS supports the following functions:

- **Continuity Check Messages (CCM):** Regular status messages are exchanged to monitor the availability of network elements.
- **Loopback:** Loopback messages can be sent and returned by the remote side (ethping / Layer 2). This function is analogous to the ICMP-based Ping on Layer 3. Both Ethernet unicast and multicast addresses are supported.
- **Linktrace:** Linktrace messages can be sent, which are returned by the remote side and responded to by network elements along the path (Layer 2). This function is analogous to the ICMP-based Traceroute on Layer 3.

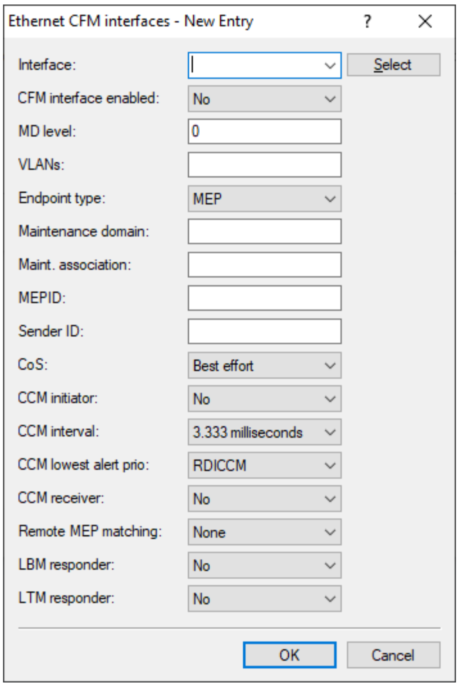
The CCM, Loopback, and Linktrace functions can be used independently, meaning Loopback and Linktrace can be utilized even without regular CCM messages.

Additionally, LCOS supports the following functions from ITU-T Y.1731:

- Reception and status display of ETH-AIS (Alarm Indication Signal)
- Reception and status display of ETH-LCK (Ethernet Locked Signal)
- Reception and processing of ETH-RDI (Remote Defect Indication)

Ethernet CFM Interfaces

In LANconfig, configure Ethernet OAM according to IEEE 802.3ah under **Miscellaneous Services** > **Services** > **OAM (Operation, Administration, Management)** > **Ethernet CFM Interfaces**.



Ethernet CFM interfaces - New Entry

Interface:	
CFM interface enabled:	No
MD level:	0
VLANs:	
Endpoint type:	MEP
Maintenance domain:	
Maint. association:	
MEPID:	
Sender ID:	
CoS:	Best effort
CCM initiator:	No
CCM interval:	3.333 milliseconds
CCM lowest alert prio:	RDICCM
CCM receiver:	No
Remote MEP matching:	None
LBM responder:	No
LTM responder:	No

Interface

Specifies the interface where CFM should be enabled. Possible values are LAN interfaces like LAN-1 or WAN interfaces like DSL-1.

CFM interface enabled

Enables or disables CFM on the configured interface.

MD level

Defines the Maintenance Domain Level for this interface.

VLANs

Defines the VLANs on the interface where CFM messages can be sent and received. If left empty, all VLANs are accepted. You can configure either a single VLAN or a comma-separated list of VLANs.

Endpoint type

Defines the CFM endpoint type. Possible values:

MEP (Maintenance Association End Point)

The Maintenance Association End Point represents the boundary of a domain and performs fault detection between the domain boundaries. The MEP creates and sends CFM packets.

MIP (Maintenance Intermediate Point)

The Maintenance Intermediate Point is located within the domain and performs path and fault detection within the domain boundaries. The MIP responds to CFM packets.

Maintenance domain

Specifies the name of the Maintenance Domain (MD).

Maintenance association

Specifies the name of the Maintenance Association (MA).

MEPID

Defines the Maintenance Endpoint ID of the device for this entry (1-8191). This must be unique on each device.

Sender ID

Specifies the optional Sender ID in CFM CCM messages.

CoS

Defines the Class of Service with which CFM CCM (Continuity Check Message) packets are marked. Possible values: Best-Effort (0), Background (1), Excellent-Effort (3), Controlled-Latency (4), Video (5), Voice (6), Network-Control (7).

CCM initiator

Specifies whether the device should send regular CCM (Continuity Check Message) packets.

CCM interval

Defines the interval at which CCM messages are sent by the device. CCM intervals must be consistent between communication partners.

CCM lowest alert prio

Defines the minimum severity level of detected issues required for the MEP to set the RDI (Remote Defect Indication) flag and propagate it in CCM packets. Levels, in ascending severity, include:

RDICCM

A CC frame with the RDI flag set was received from at least one other MEP.

MACstatus (Default)

At least one MEP reported an interface status other than 'up' (e.g., hardware issue), or all MEPs report a port status other than 'up' (e.g., network segment isolated).

RemoteCCM

No CCM frames are being received from at least one configured MEP.

ErrorCCM

Another MEP is using the same MEPID as the local device, or CCM frames are received from an unconfigured MEP (if Matching is not none), or a different CCM interval is being used by another MEP.

XconCCM

CC frames were received from another MEP with a lower MD level, or with a different domain or association.

CCM receiver

Specifies whether the device should process or receive CCM messages.

Remote MEP matching

Defines how the device handles remote MEP presence. Unconfigured remote MEPs can be dynamically learned or treated as an error if a configured remote MEP is not found.

None

Unconfigured MEPs are included in the status table and considered in RDICCM and MACstatus conditions.

Yes

Unconfigured MEPs are included in the status table but not considered in RDICCM and MACstatus conditions. They trigger ErrorCCM.

Strict

Unconfigured MEPs are not included in the status table and not considered in RDICCM and MACstatus conditions. They trigger ErrorCCM.

LBM responder

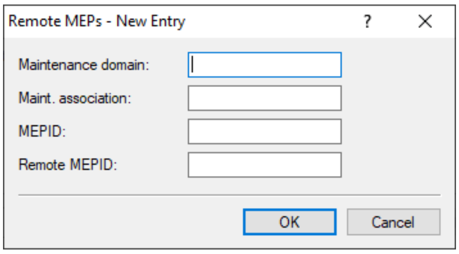
Defines whether the device should respond to CFM Loopback Messages (Ethernet Ping). This feature can be used independently of the CCM operating mode.

LTM responder

Defines whether the device should respond to CFM Linktrace Messages (Ethernet Traceroute). This feature can be used independently of the CCM operating mode.

Remote MEPs

In this table, you can optionally define remote MEPs that the device expects on the remote side. In LANconfig, configure these under **Miscellaneous Services** > **Services** > **OAM (Operation, Administration, Management)** > **Remote MEPs**.


Remote MEPs - New Entry

Maintenance domain:

Maint. association:

MEPID:

Remote MEPID:

Maintenance domain

Defines the name of the Maintenance Domain (MD).

Maintenance association

Defines the name of the Maintenance Association (MA).

MEPID

Defines the Maintenance Endpoint ID of the device for this entry (1-8191). This must be unique on each device.

Remote MEPID

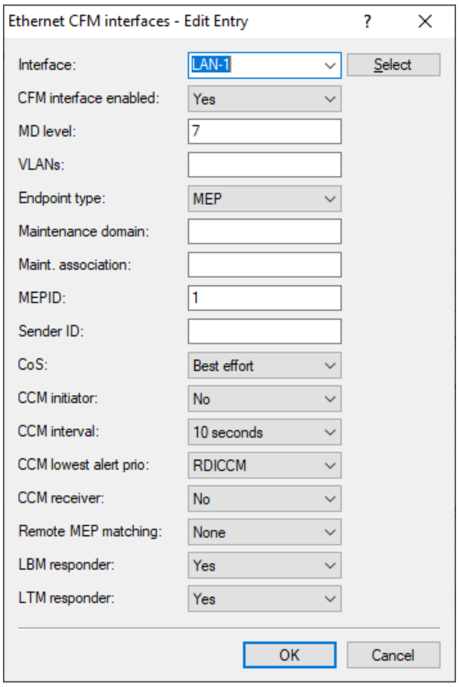
Defines the remote MEPID that is expected for this configuration (1-8191). This must be unique on each device.

Commands on the Console

Ethping

```
ethping -i <interface> [-?] [-c count] [-v vlan] [-s size] [-l mdlevel]
<target address>
```

Example: To use CFM Ethernet Ping, a minimal configuration in the Ethernet CFM Interfaces table is required. On the second device, a corresponding configuration is also necessary; however, the MEPID must differ or be unique. In this example, MD-Level 7 is used.



Interface:	LAN-1
CFM interface enabled:	Yes
MD level:	7
VLANs:	
Endpoint type:	MEP
Maintenance domain:	
Maint. association:	
MEPID:	1
Sender ID:	
CoS:	Best effort
CCM initiator:	No
CCM interval:	10 seconds
CCM lowest alert prio:	RDICCM
CCM receiver:	No
Remote MEP matching:	None
LBM responder:	Yes
LTM responder:	Yes

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

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

Instead of sending the CFM Ethernet Ping to an Ethernet unicast MAC address, the standardized multicast group can also be used. The structure of the multicast address is as follows: 01:80:C2:00:00:3x. Here, x is a value between 0 and 7 and corresponds to the domain level number for the MEP.

Additions to the Setup menu

CFM-Interfaces

This table defines the CFM parameters for the respective interface.

SNMP ID:

2.105.3

Console path:

Setup > OAM

Interface

Interface on which CFM should be activated. Possible values include LAN interfaces such as LAN-1 or WAN interfaces like DSL-1.

SNMP ID:

2.105.3.1

Console path:

Setup > **OAM** > **CFM-Interfaces**

Possible values:

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

Default:

empty

MD-Level

Defines the Maintenance Domain Level for this interface.

SNMP ID:

2.105.3.2

Console path:

Setup > **OAM** > **CFM-Interfaces**

Possible values:

0 … 7

Default:

0

VLANs

Defines the VLANs on the interface with which CFM messages can be received and sent. Either a single VLAN or a comma-separated list of VLANs can be configured.

SNMP ID:

2.105.3.3

Console path:

Setup > **OAM** > **CFM-Interfaces**

Possible values:

Max. 50 characters from `[0-9] ,-/`

Default:

empty

Special values:

empty

All VLANs are accepted.

Operating

Enables or disables CFM on the configured interface.

SNMP ID:

2.105.3.4

Console path:

Setup > **OAM** > **CFM-Interfaces**

Possible values:

No

CFM disabled.

Yes

CFM enabled.

Default:

No

Endpoint-Type

Defines the CFM endpoint type.

SNMP ID:

2.105.3.5

Console path:

Setup > **OAM** > **CFM-Interfaces**

Possible values:

MEP

The Maintenance Association End Point (MEP) represents the boundary of a domain and performs fault detection between the domain boundaries. The MEP creates and sends CFM packets.

MIP

The Maintenance Intermediate Point (MIP) is located within the domain and performs path and fault detection within the domain boundaries. The MIP responds to CFM packets.

Default:

MEP

Maintenance-Domain

Defines the name of the Maintenance Domain (MD).

SNMP ID:

2.105.3.6

Console path:

Setup > **OAM** > **CFM-Interfaces**

Possible values:

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

Default:

empty

Maintenance-Association

Defines the name of the Maintenance Association (MA).

SNMP ID:

2.105.3.7

Console path:

Setup > **OAM** > **CFM-Interfaces**

Possible values:

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

Default:

empty

MEPID

Defines the Maintenance Endpoint ID of the device for this entry. This must be unique on each device.

SNMP ID:

2.105.3.8

Console path:

Setup > **OAM** > **CFM-Interfaces**

Possible values:

1 … 8191

Sender-ID

Defines the optional sender ID in CFM-CCM messages.

SNMP ID:

2.105.3.9

Console path:

Setup > **OAM** > **CFM-Interfaces**

Possible values:

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

Default:

empty

CoS

Defines the Class-of-Service with which CFM-CCM (Continuity Check Message) packets are marked.

SNMP ID:

2.105.3.10

Console path:

Setup > **OAM** > **CFM-Interfaces**

Possible values:

Best-Effort
Background
Excellent-Effort
Controlled-Latency
Video
Voice
Network-Control

Default:

Best-Effort

LBM-Responder

Defines whether the device should respond to CFM loopback messages (Ethernet ping). The function can be used independently of the CCM operating mode.

SNMP ID:

2.105.3.11

Console path:

Setup > **OAM** > **CFM-Interfaces**

Possible values:

No
Yes

Default:

No

LTM-Responder

Defines whether the device should respond to CFM linktrace messages (Ethernet traceroute). The function can be used independently of the CCM operating mode.

SNMP ID:

2.105.3.21

Console path:

Setup > **OAM** > **CFM-Interfaces**

Possible values:

No
Yes

Default:

No

CCM-Initiator

Defines whether the device should send regular CCM messages (Continuity Check Message).

SNMP ID:

2.105.3.31

Console path:

Setup > **OAM** > **CFM-Interfaces**

Possible values:

No
Yes

Default:

No

CCM-Interval

Defines the interval at which CCM messages (Continuity Check Message) should be sent by the device. CCM intervals must be consistent between communication partners.

SNMP ID:

2.105.3.32

Console path:

Setup > **OAM** > **CFM-Interfaces**

Possible values:

3.333-msec
Interval of 3.333 milliseconds.

10-msec
Interval of 10 milliseconds.

100-msec
Interval of 100 milliseconds.

1-sec
Interval of one second.

10-sec
Interval of 10 seconds.

1-min
Interval of one minute.

10-min
Interval of 10 minutes.

Default:

3.333-msec

CCM-Lowest-Alarm-Prio

Defines the minimum severity level of detected faults required for the MEP to set the RDI (Remote Defect Indication) flag and propagate it in CCM packets. Levels, in ascending severity, are: RDICCM, MACstatus, RemoteCCM, ErrorCCM, XconCCM.

SNMP ID:

2.105.3.33

Console path:

Setup > **OAM** > **CFM-Interfaces**

Possible values:

RDICCM
A CCM frame with the RDI flag set was received from at least one other MEP.

MACstatus
At least one other MEP reported an interface status other than 'up' (e.g., hardware issue), or all other MEPs report a PortStatus other than 'up' (e.g., isolated network segment).

RemoteCCM
No CCM frames are received from at least one configured MEP.

ErrorCCM
Another MEP is using the same MEPID as the local device, or CCMs from an unconfigured MEP are received (if matching is not set to none), or another MEP is using a different CCM interval.

XconCCM
CCs were received from another MEP with a lower MD level or with a differing domain or association.

Default:

MACstatus

CCM-Receiver

Defines whether the device should process or receive CCM messages.

SNMP ID:

2.105.3.41

Console path:

Setup > **OAM** > **CFM-Interfaces**

Possible values:

No
Yes

Default:

No

Remote-MEP-Matching

Defines how the device should handle the presence of remote MEPs. Arbitrary remote MEPs can be dynamically learned, or it can be treated as an error if a configured remote MEP is not found.

SNMP ID:

2.105.3.42

Console path:

Setup > **OAM** > **CFM-Interfaces**

Possible values:

None
: Unconfigured MEPs are added to the status table and are included in the RDICCM and MACstatus conditions.

Yes
: Unconfigured MEPs are added to the status table but are not included in the RDICCM and MACstatus conditions. They trigger ErrorCCM.

Strict
: Unconfigured MEPs are not added to the status table, are not included in the RDICCM and MACstatus conditions, and they trigger ErrorCCM.

Default:

None

Remote-MEPs

In this table, remote MEPs can optionally be defined that the device expects on the remote side.

SNMP ID:

2.105.5

Console path:

Setup > **OAM**

Maintenance-Domain

Defines the name of the Maintenance Domain (MD).

SNMP ID:

2.105.5.1

Console path:

Setup > **OAM** > **Remote-MEPs**

Possible values:

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

Default:

empty

Maintenance-Association

Defines the name of the Maintenance Association (MA).

SNMP ID:

2.105.5.2

Console path:

Setup > **OAM** > **Remote-MEPs**

Possible values:

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

Default:

empty

MEPID

Defines the Maintenance Endpoint ID of the device for this entry. This must be unique on each device.

SNMP ID:

2.105.5.3

Console path:

Setup > **OAM** > **Remote-MEPs**

Possible values:

1 … 8191

Remote-MEPID

Defines the remote MEPID expected for this configuration. This must be unique on each device.

SNMP ID:

2.105.5.4

Console path:

Setup > **OAM** > **Remote-MEPs**

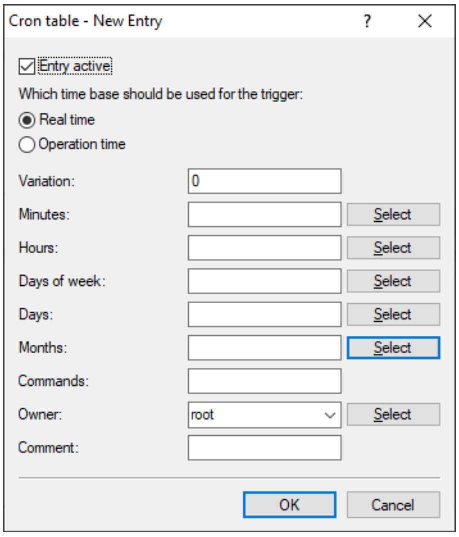
Possible values:

1 … 8191

13.3 Input options for the cron table refined

As of LCOS 10.90, the allowed inputs for certain parameters in the Cron table have been restricted to valid characters. This prevents erroneous entries.

In LANconfig, the Cron table can be found under **Date & Time** > **General** > **Cron Table**. In the CLI, it is located under **Setup** > **Config** > **Cron Table**.



☑ Entry active

Which time base should be used for the trigger:

● Real time

○ Operation time

Variation:	0
Minutes:	
Hours:	
Days of week:	
Days:	
Months:	
Commands:	
Owner:	root
Comment:	

13.3.1 Additions to the Setup menu

Minute

The value defines the time at which a command is to be executed. If no value is specified, it will not be included in the scheduling. A comma-separated list of values or a range can also be entered. A step size can be specified using /. If a range precedes the step size, it applies to the defined range. Minute values range from 0 to 59.

Examples:

- /10 – Every 10 minutes
- 0,10,20,30,40,50 – Every 10 minutes
- 0-30/5 – Every 5 minutes within the first half-hour
- 0-59 – Every minute
- 25-30 – At minutes 25 through 30
- 25,26,27,28,29,30 – At minutes 25 through 30
- 55-5 – At minutes 55 through 5
- 55,56,57,58,59,0,1,2,3,4,5 – At minutes 55 through 5

SNMP ID:

2.11.20.2

Console path:

Setup > **Config** > **Cron-Table**

Possible values:

Max. 50 characters from `[0-9] ,-/`

Default:

empty

Hour

The value defines the time at which a command is to be executed. If no value is specified, it will not be included in the scheduling. A comma-separated list of values or a range can also be entered. A step size can be specified using /. If a range precedes the step size, it applies to the defined range. Hour values range from 0 to 23.

Examples:

- /4 – Every 4 hours
- 0,4,8,12,16,20 – Every 4 hours
- 8-20/2 – Every 2 hours between 8 AM and 8 PM
- 0-23 – Every hour
- 13-16 – Between hours 13 and 16
- 13,14,15,16 – Between hours 13 and 16
- 22-1 – Between hours 22 and 1
- 22,23,0,1 – Between hours 22 and 1

SNMP ID:

2.11.20.3

Console path:

Setup > **Config** > **Cron-Table**

Possible values:

Max. 50 characters from `[0-9] ,-/`

Default:

empty

DayOfWeek

The value defines the time at which a command is to be executed. If no value is specified, it will not be included in the scheduling. A comma-separated list of values or a range can also be entered. A step size can be specified using /. If a range precedes the step size, it applies to the defined range. Day-of-week values range from 0 (Sunday) to 6 (Saturday). For syntax examples, see Minute or Hour.

SNMP ID:

2.11.20.4

Console path:

Setup > **Config** > **Cron-Table**

Possible values:

Max. 50 characters from `[0-9] ,-/`

Default:

empty

Day

The value defines the time at which a command is to be executed. If no value is specified, it will not be included in the scheduling. A comma-separated list of values or a range can also be entered. A step size can be specified using /. If a range precedes the step size, it applies to the defined range. Day values range from 1 to 31. For syntax examples, see Minute or Hour.

SNMP ID:

2.11.20.5

Console path:

Setup > **Config** > **Cron Table**

Possible values:

Max. 50 characters from `[0-9] ,-/`

Default:

empty

Month

The value defines the time at which a command is to be executed. If no value is specified, it will not be included in the scheduling. A comma-separated list of values or a range can also be entered. A step size can be specified using /. If a range precedes the step size, it applies to the defined range. Month values range from 1 (January) to 12 (December). For syntax examples, see Minute or Hour.

SNMP ID:

2.11.20.6

Console path:

Setup > **Config** > **Cron-Table**

Possible values:

Max. 50 characters from `[0-9] ,-/`

Default:

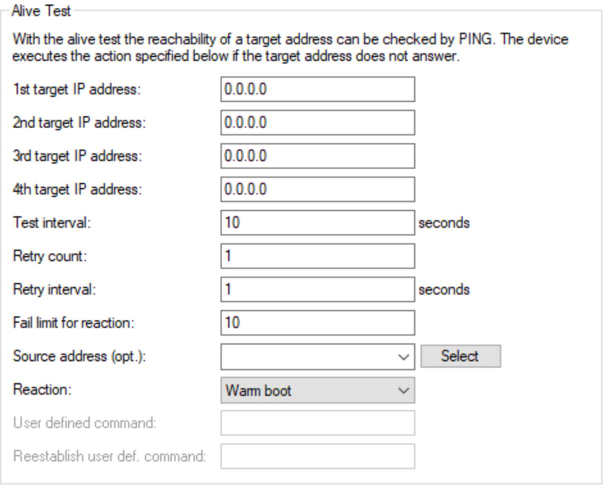
empty

13.4 Enhancements in Alive Test

As of LCOS 10.90, you can configure additional target addresses and a recovery action in the alive test.

The alive test allows you to check the reachability of IPv4 addresses using ping. If no response is received or if connectivity is restored after being unreachable, the device can perform a configurable action.

In LANconfig, configure the Alive Test under **IPv4** > **General** > **Alive Test**.



Alive Test

With the alive test the reachability of a target address can be checked by PING. The device executes the action specified below if the target address does not answer.

1st target IP address:	0.0.0.0	
2nd target IP address:	0.0.0.0	
3rd target IP address:	0.0.0.0	
4th target IP address:	0.0.0.0	
Test interval:	10	seconds
Retry count:	1	
Retry interval:	1	seconds
Fail limit for reaction:	10	
Source address (opt.):		Select
Reaction:	Warm boot	
User defined command:		
Reestablish user def. command:		

Target IP address 1-4

Up to four possible target IPv4 addresses to which the device sends a ping. Only one address needs to be reachable for the Alive Test to be considered successful.

Reestablish user-defined command

Any console-executable command can be specified as a recovery action. This is executed once when the device transitions from the error state of unreachable target addresses to a state where the configured target address is reachable again.

ⓘ This action is only executed if **Reaction** is set to **User-defined command**.

13.4.1 Additions to the Setup menu

Reestablish-Action

Any command that can be executed on the command line can be specified as a restore action. If the device is in an error state where it cannot reach the target address, this command is executed once when the target address can be reached again.

SNMP ID:

2.7.21.9

Console path:

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

Possible values:

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

Default:

empty

Target-Address-2

One of four possible target IPv4 addresses to which the device sends a ping. Only one address needs to be reachable for the alive test to be considered successful.

SNMP ID:

2.7.21.11

Console path:

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

Possible values:

Max. 15 characters from `[0-9].`

Target-Address-3

One of four possible target IPv4 addresses to which the device sends a ping. Only one address needs to be reachable for the alive test to be considered successful.

SNMP ID:

2.7.21.12

Console path:

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

Possible values:

Max. 15 characters from `[0-9].`

Target-Address-4

One of four possible target IPv4 addresses to which the device sends a ping. Only one address needs to be reachable for the alive test to be considered successful.

SNMP ID:

2.7.21.13

Console path:

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

Possible values:

Max. 15 characters from `[0-9].`

14 Enhancements in the menu system

14.1 Additions to the Setup menu

14.1.1 Max-Auth-Tries

Defines the number of consecutive attempts allowed for public key authentication. When the configured value is reached, the SSH server terminates the connection.

SNMP ID:

2.11.28.20

Console path:

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

Possible values:

max. 5 characters from `[0-9]`

Default:

6

Special values:

0

Function disabled.

14.1.2 Comment

Optionally enter a meaningful comment as a description.

SNMP ID:

2.23.30.10

Console path:

Setup > **Interfaces** > **Ethernet-ports**

Possible values:

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

14.1.3 SFP Ports

Here you can find settings for the SFP port interfaces of the device.

SNMP ID:

2.23.31

Console path:

Setup > **Interfaces**

Port

The name of the selected port.

SNMP ID:

2.23.31.1

Console path:

Setup > **Interfaces** > **SFP-Ports**

Autoneg-Bypass

If an optical peer is detected with Auto-Negotiation enabled, but the negotiation cannot be completed, attempt a connection without Auto-Negotiation as an alternative.

SNMP ID:

2.23.31.2

Console path:

Setup > **Interfaces** > **SFP-Ports**

Possible values:

Yes
No

14.1.4 Data-model

Use this entry to specify the CWMP data model.

SNMP ID:

2.44.18

Console path:

Setup > **CWMP**

Possible values:

TR-098
TR-181

Default:

TR-181

14.1.5 boot-system

With this action you manually restart the device. Parameters can be used to do this at a later time, or or even to delete a planned restart again.

This feature can be used for scenarios where critical changes are made to the configuration, where a misconfiguration could lead to the device being unreachable (e.g. WAN connection or management connection). The command can be used in conjunction with the test mode “flash no” in which configuration changes are not stored persistently in flash. Example:

1. On the CLI, “flash no” is executed.
2. Set a timed reboot in 30 minutes, e.g. do /other/boot-system 30m
3. Implementing critical configuration changes.
4. - If the changes were successful, the reboot timer can be stopped with “do /other/boot-system stop” and the system can be returned to “flash yes”.
   - If the changes make the device unreachable, the device will automatically reboot after 30 minutes with the old configuration that was active before “flash no” was set.

SNMP ID:

4.2

Console path:

Other

Possible arguments:

<num>s

Restart after a specified duration in seconds, example: do /other/boot-system 10s

<num>m

Restart after a specified time in minutes, example: do /other/boot-system 10m

<num>h

Restart after a specified duration in hours, example: do /other/boot-system 10h

stop

Stop timer, example: do /other/boot-system stop

14.1.6 Cold-Boot

This action is used to reboot the device. Parameters can be used to execute a cold-boot at a later time, or or even to delete a planned restart again.

This feature can be used for scenarios where critical changes are made to the configuration, where a misconfiguration could lead to the device being unreachable (e.g. WAN connection or management connection). The command can be used in conjunction with the test mode “flash no” in which configuration changes are not stored persistently in flash. Example:

1. On the CLI, “flash no” is executed.
2. Set a timed cold-boot in 30 minutes, e.g. do /other/cold-boot 30m
3. Implementing critical configuration changes.
4.
   - If the changes were successful, the reboot timer can be stopped with “do /other/cold-boot stop” and the system can be returned to “flash yes”.
   - If the changes make the device unreachable, the device will automatically reboot after 30 minutes with the old configuration that was active before “flash no” was set.

SNMP ID:

4.5

Console path:

Other

Possible arguments:

<num>s

Restart after a specified duration in seconds, example: do /other/cold-boot 10s

<num>m

Restart after a specified time in minutes, example: do /other/cold-boot 10m

<num>h

Restart after a specified duration in hours, example: do /other/cold-boot 10h

stop

Stop timer, example: do /other/cold-boot stop

15 Deprecated features

As of LCOS 10.90 the following features are deprecated:

- AsyncPPP (2.2.4.5)
- CLIP for RAS Dial-In (2.2.22.6, 2.2.22.7)
- Parameter Data-Rate in 2.23.7 removed (2.23.7.21)
- IKEv1/VPN algorithms cast128_cbc, blowfish_cbc and DES
- ISDN peer table without dial-up connections (2.2.2.4, 2.2.2.6, 2.2.3, 2.2.6, 2.2.7, 2.2.8, 2.2.9, 2.2.10, 2.2.11, 2.15, 2.3.3, 2.3.4, 2.3.5, 2.3.6, 2.3.15)
- ISDN location verification (2.11.31.2, 2.11.31.3, 2.11.31.4, 2.11.31.6, 2.11.31.7)
- ISDN time reference (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 for DHCP and 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)