LCOS 10.40

Addendum

05/2020

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.

The reproduction and distribution of the documentation and software supplied with this product and the use of its contents is subject to written authorization from LANCOM Systems. We reserve the right to make any alterations that arise as the result of technical development.

Windows® and Microsoft® are registered trademarks of Microsoft, Corp.

LANCOM, LANCOM Systems, LCOS, LANcommunity and Hyper Integration are registered trademarks. All other names or descriptions used may be trademarks or registered trademarks of their owners. 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.

This product contains separate open-source software components which are subject to their own licenses, in particular the General Public License (GPL). The license information for the device firmware (LCOS) is available on the device's WEBconfig interface under "Extras > License information". If the respective license demands, the source files for the corresponding software components will be made available on a download server upon request.

Products from LANCOM Systems include software developed by the "OpenSSL Project" for use in the "OpenSSL Toolkit" (*www.openssl.org*).

Products from LANCOM Systems include cryptographic software written by Eric Young (*eay@cryptsoft.com*).

Products from LANCOM Systems include software developed by the NetBSD Foundation, Inc. and its contributors.

Products from LANCOM Systems contain the LZMA SDK developed by Igor Pavlov.

LANCOM Systems GmbH
Adenauerstr. 20/B2
52146 Wuerselen
Germany
www.lancom-systems.com

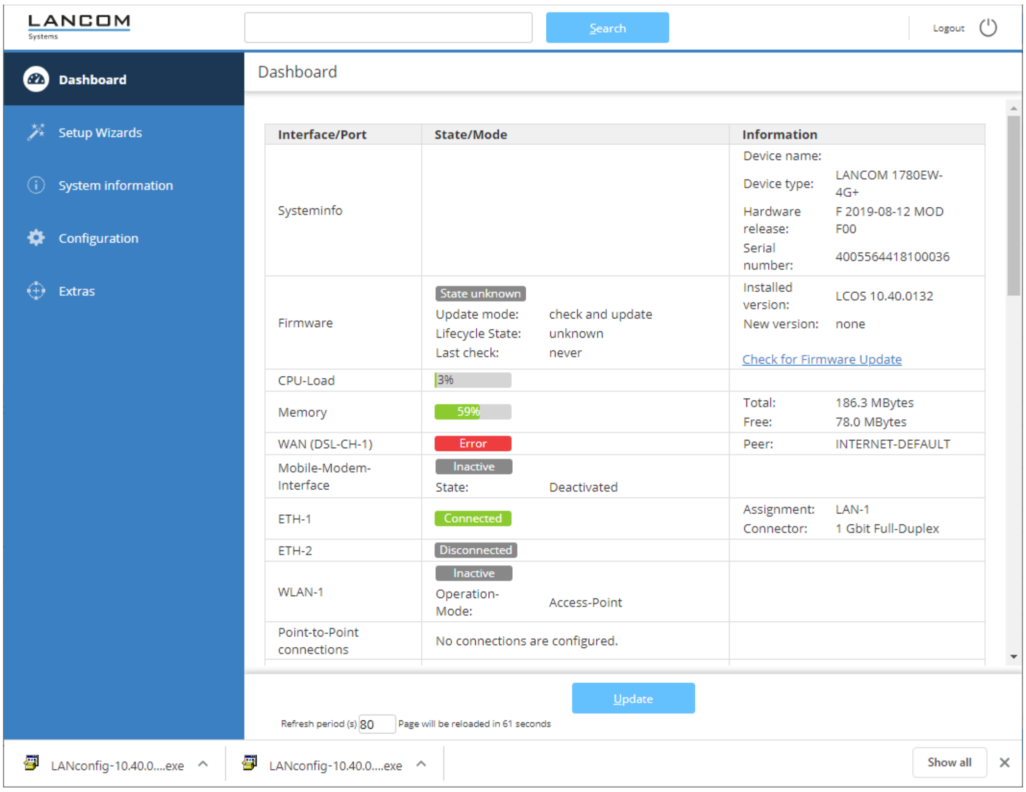
1 Addendum to LCOS version 10.40

This document describes the changes and enhancements in LCOS version 10.40 since the previous version.

2 Configuration

2.1 Modern Look & Feel: New WEBconfig

As of LCOS 10.40, you can now enjoy a completely new look & feel in LANCOM WEBconfig. Based on the modern and bright design of the LANCOM Management Cloud, the user interface has been completely revised. The attractive appearance and user guidance enhances usability.



Dashboard

Interface/Port	State/Mode	Information
Systeminfo		Device name: Device type: LANCOM 1780EW-4G+ Hardware release: F 2019-08-12 MOD F00 Serial number: 4005564418100036
Firmware	State unknown Update mode: check and update Lifecycle State: unknown Last check: never	Installed version: LCOS 10.40.0132 New version: none Check for Firmware Update
CPU-Load	3%	
Memory	59%	Total: 186.3 MBytes Free: 78.0 MBytes
WAN (DSL-CH-1)	Error	Peer: INTERNET-DEFAULT
Mobile-Modem-Interface	Inactive State: Deactivated	
ETH-1	Connected	Assignment: LAN-1 Connector: 1 Gbit Full-Duplex
ETH-2	Disconnected	
WLAN-1	Inactive Operation-Mode: Access-Point	
Point-to-Point connections	No connections are configured.	

Refresh period (s) 80 Page will be reloaded in 61 seconds

The **Dashboard** displays the information of your device. **System information**, **Configuration** and **Extras** are available as usual. You can now find the **LCOS menu tree** and **File management** under **Extras**.

2.2 TLS 1.3 client mode

As of LCOS 10.40 your device supports TLS 1.3 for accessing web servers. This is used to download updated firmware, for example. TLS 1.3 represents the latest advancement of the TLS standard and offers, for example, the exclusive use of state-of-the-art cipher suites and Perfect Forward Secrecy to provide improved security compared to previous versions.

An LCOS update automatically automatically supplements the configuration with TLS 1.3-support for the client mode. If necessary, remove older methods that LCOS should no longer use.

Support for TLS 1.3 in server mode has been available since LCOS 10.30.

2.2.1 Additions to the Setup menu

Versions

This entry specifies which versions of the protocol are allowed.

SNMP ID:

2.2.53.1

Console path:

Setup > **WAN** > **SSL-for-Action-Table**

Possible values:

SSLv3
TLSv1
TLSv1.1
TLSv1.2
TLSv1.3

Default:

TLSv1

TLSv1.1

TLSv1.2

TLSv1.3

Versions

This entry specifies which versions of the protocol are allowed.

SNMP ID:

2.11.29.2

Console path:

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

Possible values:

SSLv3
TLSv1
TLSv1.1
TLSv1.2
TLSv1.3

Default:

TLSv1.2

TLSv1.3

Versions

This entry specifies which versions of the protocol are allowed.

SNMP ID:

2.11.55.1

Console path:

Setup > **Config** > **SSL-for-Cron-Table**

Possible values:

SSLv3
TLSv1
TLSv1.1
TLSv1.2
TLSv1.3

Default:

TLSv1

TLSv1.1

TLSv1.2

TLSv1.3

Versions

This entry specifies the protocol versions allowed for the Rollout Agent.

SNMP ID:

2.11.92.15.1

Console path:

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

Possible values:

SSLv3
TLSv1
TLSv1.1
TLSv1.2
TLSv1.3

Default:

TLSv1

TLSv1.1

TLSv1.2

TLSv1.3

Versions

Here you select the encryption version(s) to be used.

SNMP ID:

2.21.20.11.1

Console path:

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

Possible values:

SSLv3
TLSv1
TLSv1.1
TLSv1.2
TLSv1.3

Default:

TLSv1

TLSv1.1

TLSv1.2

TLSv1.3

Versions

This entry specifies which versions of the protocol are allowed.

SNMP ID:

2.21.40.3

Console path:

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

Possible values:

SSLv3
TLSv1
TLSv1.1
TLSv1.2
TLSv1.3

Default:

TLSv1

TLSv1.1

TLSv1.2

TLSv1.3

Versions

This entry specifies which versions of the protocol are allowed.

SNMP ID:

2.24.41.2.19.1

Console path:

Setup > **Public-Spot-Module** > **Authentication-Modules** > **e-mail2SMS-Authentication** > **SSL**

Possible values:

SSLv3
TLSv1
TLSv1.1
TLSv1.2
TLSv1.3

Default:

TLSv1

TLSv1.1

TLSv1.2

TLSv1.3

Versions

This entry specifies which versions of the protocol are allowed.

SNMP ID:

2.24.41.5.4.1

Console path:

Setup > **Public-Spot-Module** > **Authentication-Modules** > **Radius-Server** > **SSL**

Possible values:

SSLv3
TLSv1
TLSv1.1
TLSv1.2
TLSv1.3

Default:

TLSv1

TLSv1.1

TLSv1.2

TLSv1.3

Versions

This entry specifies which versions of the protocol are allowed.

SNMP ID:

2.24.53.1

Console path:

Setup > **Public-Spot-Module** > **SSL-for-Page-Table**

Possible values:

SSLv3
TLSv1
TLSv1.1
TLSv1.2
TLSv1.3

Default:

TLSv1

TLSv1.1

TLSv1.2

TLSv1.3

Versions

This entry specifies which versions of the protocol are allowed.

SNMP ID:

2.27.14.1

Console path:

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

Possible values:

SSLv3
TLSv1
TLSv1.1
TLSv1.2
TLSv1.3

Default:

TLSv1

TLSv1.1

TLSv1.2

TLSv1.3

Versions

This entry specifies which versions of the protocol are allowed.

SNMP ID:

2.37.27.39.1

Console path:

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

Possible values:

SSLv3
TLSv1
TLSv1.1
TLSv1.2
TLSv1.3

Default:

TLSv1.2

TLSv1.3

Versions

This entry specifies which versions of the protocol are allowed.

SNMP ID:

2.44.26.1

Console path:

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

Possible values:

SSLv3
TLSv1
TLSv1.1
TLSv1.2
TLSv1.3

Default:

TLSv1

TLSv1.1

TLSv1.2

TLSv1.3

Versions

This entry specifies which versions of the protocol are allowed.

SNMP ID:

2.60.1.5.1

Console path:

Setup > **Autoload** > **Network** > **SSL**

Possible values:

SSLv3
TLSv1
TLSv1.1
TLSv1.2
TLSv1.3

Default:

TLSv1

TLSv1.1

TLSv1.2

TLSv1.3

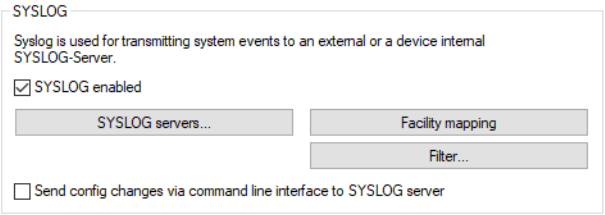
3 Diagnosis

3.1 Filter for syslog messages

As of LCOS 10.40 your device supports filters for syslog messages. If the syslog messages are transmitted to one or more servers by configuring settings for receiving certain messages, all configured messages are transmitted to the servers with the configured source and priority. However, it is sometimes desirable to filter out certain messages for the servers, to send only certain messages at all, or to change their source and priority if they should be weighted differently in the server log. The syslog filter allows the filtering of messages depending on the source, priority and/or message text.

3.1.1 Configuring SYSLOG

In LANconfig you configure SYSLOG under **Logging/Monitoring** > **Protocols** in the section **SYSLOG**.



SYSLOG

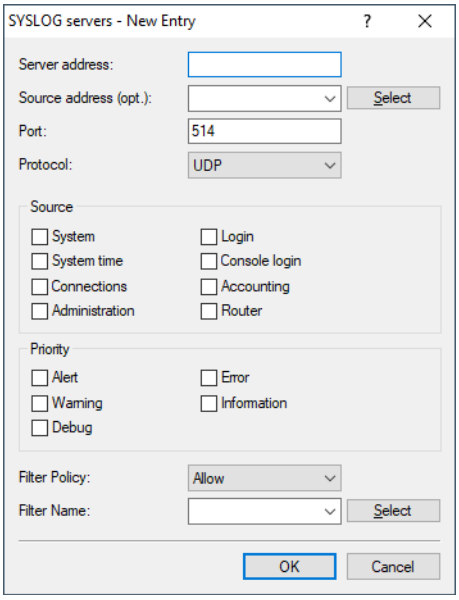
Syslog is used for transmitting system events to an external or a device internal SYSLOG-Server.

☑ SYSLOG enabled

□ Send config changes via command line interface to SYSLOG server

SYSLOG servers

In LANconfig, you configure the settings for the SYSLOG server under **Logging/Monitoring** > **Protocols** > **SYSLOG** and clicking **SYSLOG servers**.



SYSLOG servers - New Entry

Server address:

Source address (opt.):

Port: 514

Protocol: UDP

Source

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

Priority

□ Alert
□ Warning
□ Debug
□ Error
□ Information

Filter Policy: Allow

Filter Name:

Filter policy

If the syslog messages are transmitted to one or more servers by configuring settings for receiving certain messages, all configured messages are transmitted to the servers with the configured source and priority.

However, it is sometimes desirable to filter out certain messages for the servers, to send only certain messages at all, or to change their source and priority if they should be weighted differently in the server log. The syslog filter allows the filtering of messages depending on the source, priority and/or message text. Here you determine whether messages, which are identified by the filter set in the following field, are allowed or denied.

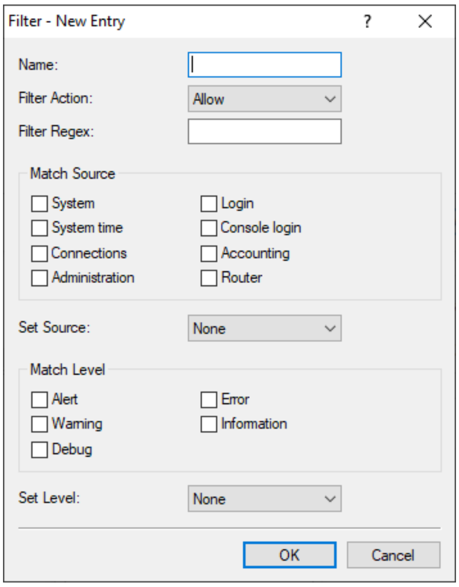
Filter name

Select one of the configured filters.

Filter

If the syslog messages are transmitted to one or more servers by configuring settings for receiving certain messages, all configured messages are transmitted to the servers with the configured source and priority. However, it is sometimes desirable to filter out certain messages for the servers, to send only certain messages at all, or to change their source and priority if they should be weighted differently in the server log. The syslog filter allows the filtering of messages depending on the source, priority and/or message text. Configure these filters here, which you can then use for entries on the SYSLOG server.

In LANconfig, you configure the filter settings for the SYSLOG server under **Logging/Monitoring** > **Protocols** > **SYSLOG** and clicking **Filter**.



Filter - New Entry

Name:

Filter Action: Allow

Filter Regex:

Match Source

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

Set Source: None

Match Level

□ Alert □ Error
□ Warning □ Information
□ Debug

Set Level: None

Name

Give the filter a descriptive name. Several rules can be created with the same filter name. These are then checked in the order in which they are created in the filter table when sending the messages. If there is no matching rule in this filter chain, the message is sent or discarded according to the server's default policy in the server table.

Filter action

Action when the rule applies; "Allow" enables messages to be sent to the server, "Deny" rejects the message.

Filter regex

Regular expression in Perl syntax (also see *Regular expressions in Perl*) to which the message text must apply. An empty string means that the message text is ignored, and therefore all message texts apply.

Match source

Source of the message to which this rule applies. The value "none" stands for any source.

Set source

New source of the message if the rule applies. The value “none” means that the source is not changed.

Match level

Priority of the message to which this rule applies. The value “none” stands for any priority.

Set level

New priority of the message if the rule applies. The value “none” means that the priority is not changed.

3.1.2 Additions to the Setup menu

Filter name

References a SYSLOG filter.

SNMP ID:

2.17.20.6

Console path:

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

Possible values:

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

Filter-Policy

If the syslog messages are transmitted to one or more servers by configuring settings for receiving certain messages, all configured messages are transmitted to the servers with the configured source and priority. However, it is sometimes desirable to filter out certain messages for the servers, to send only certain messages at all, or to change their source and priority if they should be weighted differently in the server log. The syslog filter allows the filtering of messages depending on the source, priority and/or message text. Here you determine whether messages, which are identified by the filter set in the field **Filter name**, are allowed or denied.

SNMP ID:

2.17.20.7

Console path:

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

Possible values:

Allow
Reject

Default:

Reject

Filter-Policy

If the syslog messages are transmitted to one or more servers by configuring settings for receiving certain messages, all configured messages are transmitted to the servers with the configured source and priority. However, it is sometimes desirable to filter out certain messages for the servers, to send only certain messages at all, or to change their source and priority if they should be weighted differently in the server log. The syslog filter allows the filtering of messages depending on the source, priority and/or message text. Here you determine whether messages, which are identified by the filter set in the field **Filter name**, are allowed or denied.

SNMP ID:

2.22.2.10

Console path:

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

Possible values:

Allow
Deny

Default:

Deny

Filter-Name

References a SYSLOG filter.

SNMP ID:

2.22.2.11

Console path:

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

Possible values:

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

Filter

This table is used to define the filter rules.

SNMP ID:

2.22.13

Console path:

Setup > **SYSLOG**

Idx.

Position of the entry in the table.

SNMP ID:

2.22.13.1

Console path:

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

Possible values:

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

Default:

empty

Filter-Name

The name of the filter rule; the server table references this name. Several rules can be created with the same filter name. When messages are sent, these rules are checked in the order of their position in the filter table. If there is no matching rule in this filter chain, the message is sent or discarded according to the server's default policy in the server table.

SNMP ID:

2.22.13.2

Console path:

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

Possible values:

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

Match-source

Source of the message to which this rule applies. The value "none" stands for any source.

SNMP ID:

2.22.13.3

Console path:

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

Possible values:

None
System
Login
System time
CLI login
Connections
Accounting
Administration
Router

Default:

None

Match-level

Priority of the message to which this rule applies. The value "none" stands for any priority.

SNMP ID:

2.22.13.4

Console path:

Setup > SYSLOG > Filter

Possible values:

None
Alert
Error
Warning
Info
Debug

Default:

None

Filter-Regex

Regular expression in Perl syntax to which the message text must apply. An empty string means that the message text is ignored, and therefore all message texts apply.

SNMP ID:

2.22.13.5

Console path:

Setup > SYSLOG > Filter

Possible values:

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

Set-source

New source of the message if the rule applies. The value “none” means that the source is not changed.

SNMP ID:

2.22.13.6

Console path:

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

Possible values:

None
System
Login
System time
CLI login
Connections
Accounting
Administration
Router

Default:

None

Set-level

New priority of the message if the rule applies. The value “None” means that the priority is not changed.

SNMP ID:

2.22.13.7

Console path:

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

Possible values:

None
Alert
Error
Warning
Info
Debug

Default:

None

Filter-Action

Action if the rule applies. Either allow or deny sending the message to the server.

SNMP ID:

2.22.13.8

Console path:

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

Possible values:

Allow
Deny

Default:

Deny

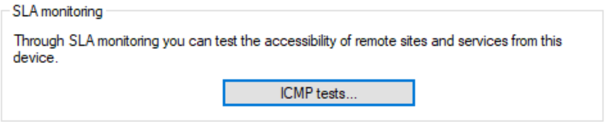
3.2 Support for DSCP tagging in the SLA monitor

From LCOS 10.40 your device supports DSCP tagging both in the ping on the command line and in the SLA monitor.

On the command line, use the new optional ping parameter `[-p <DSCP>]`.

Parameter	Meaning
`[-p <dscp>]`	Use a specific DSCP value for this ping. DSCP (Differentiated Services Code Point) is used for QoS (Quality of Service). Possible DSCP values: BE/CS0, CS1, CS2, CS3, CS4, CS5, CS6, CS7, AF11, AF12, AF13, AF21, AF22, AF23, AF31, AF32, AF33, AF41, AF42, AF43, EF

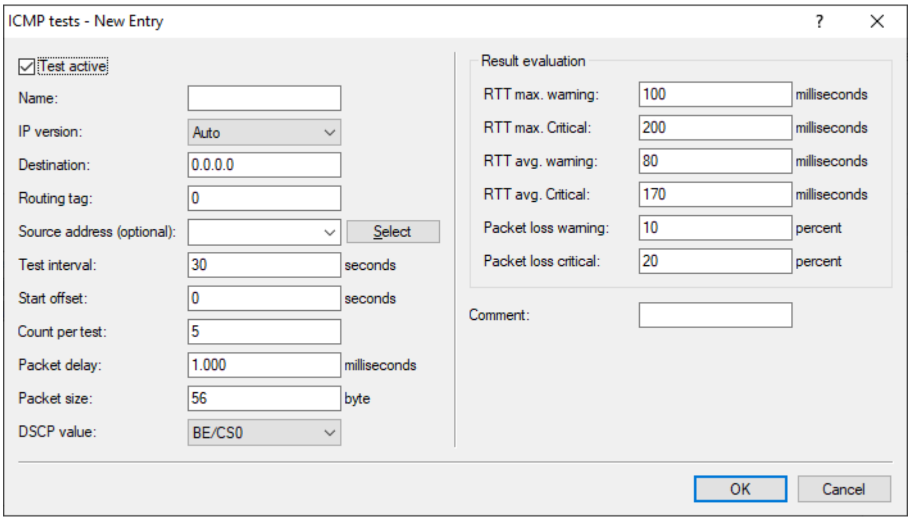
For configuration with LANconfig, the SLA monitor is located under **Logging/Monitoring** > **General** on the **SLA monitoring** pane.



SLA monitoring

Through SLA monitoring you can test the accessibility of remote sites and services from this device.

Click the button **ICMP tests**, add new queries and set guideline values for the connection tests.



ICMP tests - New Entry

☑ Test active

Name:

IP version: Auto

Destination: 0.0.0.0

Routing tag: 0

Source address (optional):

Test interval: 30 seconds

Start offset: 0 seconds

Count per test: 5

Packet delay: 1.000 milliseconds

Packet size: 56 byte

DSCP value: BE/CS0

Result evaluation

RTT max. warning: 100 milliseconds

RTT max. Critical: 200 milliseconds

RTT avg. warning: 80 milliseconds

RTT avg. Critical: 170 milliseconds

Packet loss warning: 10 percent

Packet loss critical: 20 percent

Comment:

DSCP value

Specifies the DSCP value of the ICMP message. DSCP (Differentiated Services Code Point) is used for QoS (Quality of Service). Possible values: BE/CS0, CS1, CS2, CS3, CS4, CS5, CS6, CS7, AF11, AF12, AF13, AF21, AF22, AF23, AF31, AF32, AF33, AF41, AF42, AF43, EF

3.2.1 Additions to the Setup menu

DSCP

Specifies the DSCP value of the ICMP message. DSCP (Differentiated Services Code Point) is used for QoS (Quality of Service).

SNMP ID:

2.45.1.22

Console path:

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

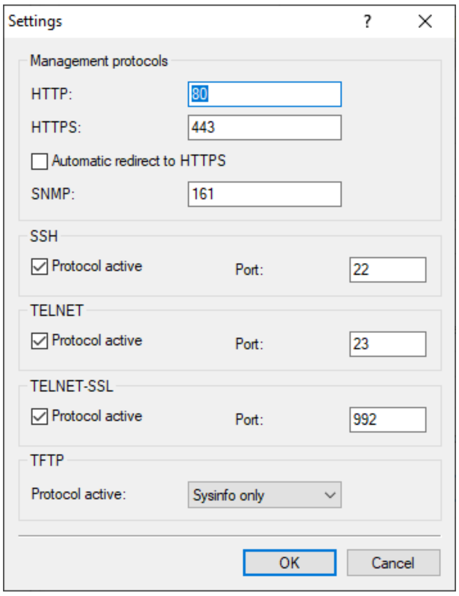
Possible values:

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

4 Security

4.1 TFTP for Sysinfo only

As of LCOS 10.40 your device supports the setting **Sysinfo only** for the management protocol TFTP. The setting is located under **Management** > **Admin** > **Management protocols**.



Management protocols

HTTP: 80

HTTPS: 443

□ Automatic redirect to HTTPS

SNMP: 161

SSH

☑ Protocol active Port: 22

TELNET

☑ Protocol active Port: 23

TELNET-SSL

☑ Protocol active Port: 992

TFTP

Protocol active: Sysinfo only

TFTP

Access is via TFTP The trivial file transfer protocol (TFTP) is a simpler variant of the file transfer protocol (FTP). In contrast to FTP, TFTP permits the reading or writing of files via UDP only. The setting **Sysinfo only** leaves the port open, but the device responds only to a Sysinfo request. As a result it is displayed in LANconfig and, in particular, it will be found when searching for devices. However, no configuration can be uploaded to the device. Since this protocol transmits unencrypted, sensitive data could be intercepted on the network.

4.1.1 Additions to the Setup menu

TFTP-Operating

The trivial file transfer protocol (TFTP) is a simpler variant of the file transfer protocol (FTP). In contrast to FTP, TFTP permits the reading or writing of files via UDP only.

This entry is used to enable or disable the TFTP.

SNMP ID:

2.11.36

Console path:

Setup > **Config**

Possible values:

No
Yes
Sysinfo-only

The port is kept open and the device responds to a sysinfo request. As a result it is displayed in LANconfig and, in particular, it will be found when searching for devices. However, no configuration can be uploaded to the device. Since this protocol transmits unencrypted, sensitive data could be intercepted on the network.

Default:

Sysinfo-only

4.2 Encrypted passwords

From LCOS 10.40 the main device password and the passwords of other administrators can be stored in encrypted form using the SHA-256 and SHA-512 hash methods.

For reasons of compatibility, the default setting in LCOS 10.40 is still to store the password so that it can be displayed in cleartext. You can turn this off with the option *2.11.89.1 Keep-Cleartext* on page 29.

ⓘ In future LCOS versions, storage as cleartext will be deactivated.

Protocols such as LL2M and LCOSCap have been adapted so that they can work with the encrypted passwords.

! If you switch off cleartext passwords on a WLAN controller and you have at the same time activated password synchronization, you can only manage access points that also have at least LCOS 10.40. Access points with an LCOS version earlier than 10.40 will then no longer be accepted by the WLAN controller.

! If you disable cleartext passwords, do not perform a firmware downgrade to a LCOS version less than 10.40 because older versions do not support this function.

! If you re-enable cleartext passwords, the main device password must be entered again via the change password dialog.

4.2.1 Additions to the Setup menu

Passwords

This item contains settings for the algorithm used to create the password hash.

SNMP ID:

2.11.89

Console path:

Setup > **Config**

Keep-Cleartext

As of LCOS 10.40 an algorithm is used to store the main device password and the administrator passwords in encrypted form as a hash value. Specify here whether the cleartext password is also retained.

SNMP ID:

2.11.89.1

Console path:

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

Possible values:

Yes

The main device password and the administrator passwords are internally also stored in cleartext. This means that the password can still be displayed in LANconfig, and that access points with an LCOS version earlier than 10.40 can still be managed by a WLC or the WLC option. The password is not visible from the CLI.

> ! If you wish to retain the option of downgrading the firmware to an LCOS version earlier than 10.40, this option must be set.

> ! If a firmware downgrade is made to an LCOS version prior to 10.40 that does not support encrypted passwords, the password will be deleted. Access to the router from the LAN or WLAN is then possible without a password! Access from the WAN is not possible without a password!

No

The main device password and the administrator passwords are internally stored in hashed form only.

Default:

Yes

Crypto-Algorithm

The algorithm used to encrypt the passwords.

SNMP ID:

2.11.89.2

Console path:

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

Possible values:

SHA-256
SHA-512

Default:

SHA-512

Rounds

This value determines how often the encryption algorithm is used. The more rounds are calculated, the higher the resistance to brute-force attacks. This does slow down the actual work with passwords. The 5000 rounds specified in the configuration offer a high level of security with a good working speed.

SNMP ID:

2.11.89.3

Console path:

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

Possible values:

1000 … 999999999

Default:

5000

Encrypted-Password

Encrypted password for this entry.

ⓘ This password is automatically encrypted by the algorithm specified in *2.11.89.2 Crypto-Algorithm* on page 29.

SNMP ID:

2.11.21.6

Console path:

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

Possible values:

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

Default:

empty

SNMP encrypted password

Encrypted SNMP password for this entry.

ⓘ This password is automatically encrypted by the algorithm specified in *2.11.89.2 Crypto-Algorithm* on page 29.

SNMP ID:

2.11.21.7

Console path:

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

Possible values:

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

Default:

empty

Crypto-Algorithms

This item is used to limit the range of encryption algorithms used for LL2M connections. This setting applies to the server and client mode. The Simple algorithm uses the cleartext password as the basis for key derivation, while the other two algorithms use an encrypted password as the basis, which is encrypted with either SHA-256 or SHA-512. Simple must remain enabled for communicating with LCOS versions before LCOS 10.40.

> ⓘ Note that the algorithm selection must be consistent with the selected password encryption algorithm: For example, if SHA-512 is used to encrypt admin passwords (see *2.11.89.2 Crypto-Algorithm* on page 29) and cleartext passwords are not stored (see *2.11.89.1 Keep-Cleartext* on page 29), SHA-512 must not be deactivated here, otherwise the device cannot be reached via LL2M.

SNMP ID:

2.11.50.3

Console path:

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

Possible values:

Simple
SHA-256
SHA-512

Default:

Simple

SHA-256

SHA-512

LCOSCap-Algorithms

This item is used to limit the range of encryption algorithms used for LCOSCap connections. The Simple algorithm uses the cleartext password as the basis for key derivation, while the other two algorithms use an encrypted password as the basis, which is encrypted with either SHA-256 or SHA-512. Simple must remain enabled for communicating with LCOS or LCOSCap versions before LCOS 10.40.

> ⓘ Note that the algorithm selection must be consistent with the selected password encryption algorithm: For example, if SHA-512 is used to encrypt admin passwords (see *2.11.89.2 Crypto-Algorithm* on page 29) and cleartext passwords are not stored (see *2.11.89.1 Keep-Cleartext* on page 29), SHA-512 must not be deactivated here, otherwise the device cannot be reached via LL2M.

SNMP ID:

2.63.4

Console path:

Setup > **Packet-Capture**

Possible values:

Simple
SHA-256
SHA-512

Default:

Simple

SHA-256

SHA-512

Keep-Cleartext

As of LCOS 10.40 an algorithm is used to store the password of SNMP users in encrypted form as a hash value. Specify here whether the cleartext password is also retained.

SNMP ID:

2.11.89.1

Console path:

Setup > **Config**

Possible values:

Yes

The passwords of SNMP users are internally also stored in cleartext.

> ⓘ If you wish to retain the option of downgrading the firmware to an LCOS version earlier than 10.40, this option must be set.

No

The passwords of SNMP users are internally stored in hashed form only.

Default:

Yes

Authentication-Key

Encrypted authentication password for this entry.

This password is automatically encrypted by the algorithm specified in *2.11.89.2 Crypto-Algorithm* on page 29.

SNMP ID:

2.9.32.14

Console path:

Setup > **SNMP** > **Users**

Possible values:

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

Default:

empty

Privacy-Key

Encrypted privacy password for this entry.

This password is automatically encrypted by the algorithm specified in *2.11.89.2 Crypto-Algorithm* on page 29.

SNMP ID:

2.9.32.15

Console path:

Setup > **SNMP** > **Users**

Possible values:

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

Default:

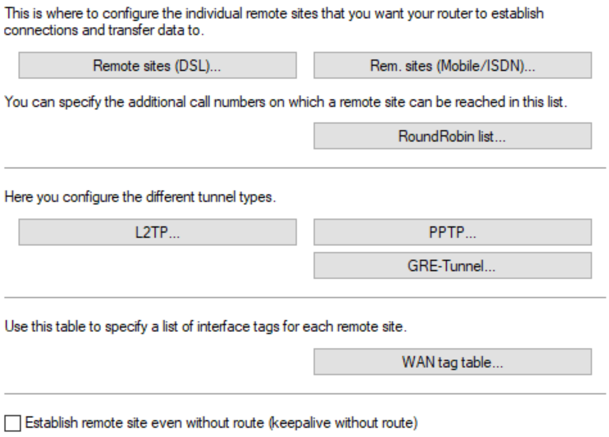
empty

5 Routing and WAN connections

5.1 Establish remote site even without a route

From LCOS 10.40 your device connects to remote sites even without an existing route.

The option is located under **Communication** > **Remote sites**.



This is where to configure the individual remote sites that you want your router to establish connections and transfer data to.

You can specify the additional call numbers on which a remote site can be reached in this list.

Here you configure the different tunnel types.

Use this table to specify a list of interface tags for each remote site.

□ Establish remote site even without route (keepalive without route)

Establish remote site even without route (keepalive without route)

Specifies whether a connection to a remote site, e.g. a VPN tunnel or an Internet connection, should be established even without a route. Connecting to the remote site without an explicit route in the routing table is necessary if the remote site transmits the routes, e.g. by DHCP (Classless Static Route Option) or a dynamic routing protocol.

5.1.1 Additions to the Setup menu

Keepalive-without-Route

Specifies whether a connection to a remote site, e.g. a VPN tunnel or an Internet connection, should be established even without a route. Connecting to the remote site without an explicit route in the routing table is necessary if the remote site transmits the routes, e.g. by DHCP (Classless Static Route Option) or a dynamic routing protocol.

SNMP ID:

2.2.15

Console path:

Setup > **WAN**

Possible values:

No

Connects to remote sites only when a route exists. This corresponds to the default behavior up until LCOS 10.40.

Yes

As of LCOS 10.40 this option allows connections to remote sites even without an existing route.

Default:

No

5.2 “Time-dependent default route” feature removed

As of LCOS 10.40 your device no longer supports the feature “Time-dependent default route”. This was created back in the times when the router was purely an ISDN router. The corresponding LANconfig options under **IP router** > **Routing** > **Time-dependent control** have been removed. This also applies to the command-line table Default-Time-List and the entry Usage-Default-Timetable under **Setup** > **IP-Router**.

5.3 Backup via the routing table

From LCOS 10.40 your device supports a configurable administrative distance for static routes, which provides a backup mechanism via the routing table.

5.3.1 Administrative distance

The administrative distance can be used to configure several identical routes or prefixes to different remote sites. The route with the lowest administrative distance is the preferred active route. This mechanism can be used, for example, to configure simple backup mechanisms.

The manipulation of the administrative distance for routes that are dynamic is handled by the respective dynamic routing protocol.

Example 1: Two VPN tunnels are to be configured with the route 192.168.2.0/24. The second VPN tunnel is to be configured as the “always-on” backup for the first VPN tunnel.

For the first tunnel, the prefix 192.168.2.0/24 is set up to the remote site VPN-1 with an administrative distance of 10. For the second tunnel, the prefix 192.168.2.0/24 is set up to the remote site VPN-2 with an administrative distance of 20. Both VPN tunnels will be established, but the route is only active for the first VPN tunnel as it has the better/lower administrative distance. If the first VPN tunnel disconnects, the operating system sets this route to the administrative distance of 255 (interface down), which automatically activates the route using the second tunnel.

Example 2: There is a static route for 192.168.1.0/24 to the remote peer VPN-Tunnel1. If the same prefix 192.168.1.0/24 is received via BGP, the static route has a better/lower administrative distance by default, so it has preference over the route via BGP.

If you now set the administrative distance of the static route to the value 210, then the route learned via BGP is preferred and active, since (e)BGP has an administrative distance of 20 or 200 (iBGP). The static route thus serves as a backup for the dynamic BGP route.

This feature does not replace the backup table, but it does offer a different kind of “backup”. When using the backup table, only one connection is active at a time. If the backup is required, the system attempts to activate the backup connection. While the backup connection is active, the system attempts to reestablish the primary connection and will switch back to it, if successful. The backup strategy based on the administrative distance assumes that connections to all remote sites are always established. This may be undesirable in certain scenarios, e.g. with backups via cellular networks, and the backup table would be the preferred choice.

ⓘ The backup table and backups over administrative distances are mutually exclusive ways of implementing backups.

The commands `show ipv4-static-routes` and `show ipv6-static-routes` displays all active and inactive static routes. The current administrative distances for route sources can be viewed from the CLI using the command `show admin-distance`.

The most important administrative distances are:

Table 1: Administrative distances

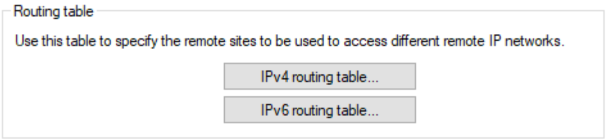
Type of route	Administrative distance
Static routes	5
VPN	15
eBGP	20
OSPF	110
RIP	120
iBGP	200
LISP	240
Interface Down	255

Static routes are defined as routes that a user manually configured in the IPv4 or IPv6 routing table.

VPN routes are defined as routes that are automatically entered into the routing table by the VPN, e.g. by IKEv2 routing.

5.3.2 Routing tables for IPv4/IPv6

Static routing entries are configured in the separate tables for IPv4 and IPv6. The tables are located in LANconfig under **IP router** > **Routing** > **Routing table**

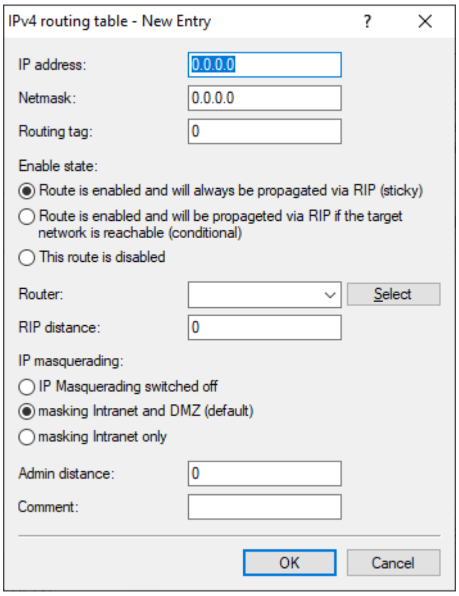


Routing table

Use this table to specify the remote sites to be used to access different remote IP networks.

IPv4

The routing table for the static routing of IPv4 packets is located under **IP router** > **Routing** > **Routing table** > **IPv4 routing table**.


IPv4 routing table - New Entry

IP address: 0.0.0.0

Netmask: 0.0.0.0

Routing tag: 0

Enable state:

● Route is enabled and will always be propagated via RIP (sticky)

○ Route is enabled and will be propageted via RIP if the target network is reachable (conditional)

○ This route is disabled

Router:

RIP distance: 0

IP masquerading:

○ IP Masquerading switched off

● masking Intranet and DMZ (default)

○ masking Intranet only

Admin distance: 0

Comment:

Router

Data packets that match the IP address and netmask are transmitted by the router to this remote site or IP address.

- As of LCOS 10.40 the syntax 'IP address@tag' can be used if the router or next-hop is to be resolved in a different routing context.

  This is the case, for example, if a static route has been created with a tag where this tag can only be assigned by a firewall rule.

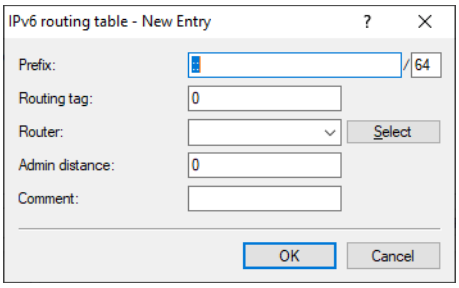
  Example: If the router 192.168.1.1 is to be resolved in routing context 1, the entry is '192.168.1.1@1'.

Administrative distance

Administrative distance for this route. The default is 0 (set automatically by the operating system). The administrative distance parameter can be used to configure several identical routes or prefixes to different remote sites. The route with the lowest administrative distance is the preferred active route. See *Administrative distance* on page 35.

IPv6

The routing table for the static routing of IPv6 packets is located under **IP router** > **Routing** > **Routing table** > **IPv6 routing table**.


IPv6 routing table - New Entry

Prefix: :: / 64

Routing tag: 0

Router:

Admin distance: 0

Comment:

Router

This is where you specify the destination or remote site for this route.

As of LCOS 10.40 the syntax 'IP address@tag' can be used if the router or next-hop is to be resolved in a different routing context.

This is the case, for example, if a static route has been created with a tag where this tag can only be assigned by a firewall rule.

Example: If the router 2001:db8::1 is to be resolved in routing context 1, the entry is '2001:db8::1@1'.

Admin distance

Here you set the administrative distance of this route. This parameter can be used to configure several identical routes or prefixes to different remote sites. The route with the lowest administrative distance is the preferred active route. The default is 0, i.e. the value is assigned automatically by the operating system. See *Administrative distance* on page 35.

5.3.3 Additions to the Setup menu

Admin-Distance

Administrative distance for this route. The default is 0 (set automatically by the operating system). The administrative distance parameter can be used to configure several identical routes or prefixes to different remote sites. The route with the lowest administrative distance is the preferred active route.

SNMP ID:

2.8.2.9

Console path:

Setup > **IP-Router** > **IP-Routing-Table**

Possible values:

0 … 255

Default:

0

Admin-Distance

Administrative distance of this route. This parameter can be used to configure several identical routes or prefixes to different remote sites. The route with the lowest administrative distance is the preferred active route. The default is 0, i.e. the value is assigned automatically by the operating system.

SNMP ID:

2.70.12.1.5

Console path:

Setup > **IPv6** > **Router** > **Routing-Table**

Possible values:

0 … 255

Default:

0

5.4 Load balancing

5.4.1 Dynamic load balancing

Load balancer from RADIUS configuration

As of LCOS 10.40 your device adds to its existing ability to configure a load balancer via the load balancer's configuration table in that it can now configure a load balancer based on RADIUS attributes for IKEv2 VPN tunnels.

In large-scale VPN scenarios, central configurations with all the necessary parameters of a VPN tunnel are not stored in the device itself; instead, this is outsourced to one or more central RADIUS servers. The aim of this is better scalability and administration. If these scenarios require several inbound IKEv2 VPN tunnels to be combined into a load balancer on the central-site VPN gateway, this can be implemented using additional RADIUS attributes.

The bundled peers of a dynamic load balancer are IKEv2 VPN clients that use RADIUS authorization. A VPN client becomes a part of a dynamic load-balancer cluster if the RADIUS response contains a corresponding RADIUS attribute (LCS-Load-Balancer). This attribute specifies the name of the load balancer cluster and also determines whether to activate client binding .

ⓘ If this type of VPN connection terminates, the client is removed from its load-balancer cluster. A new connection must be established by the client.

❗ A dynamic load-balancer cluster cannot have the same name as a statically configured cluster, so you cannot mix static and dynamic clients on the same load balancer.

For configuration via a RADIUS server, the syntax of the standard attributes “Framed-Route” and “Framed-IPv6-Route” have been extended to pass on dynamic routes that point to a load balancer. The attribute “LCS-Load-Balancer” ensures that routes used for IKEv2 routing automatically point to the load balancer instead of the dial-in interface.

This feature is also supported with IKEv2 routing. The route on the VPN gateway is then sent dynamically from the remote site instead of being received from the RADIUS server as a Framed-Route attribute. In this case, the RADIUS server only has to send the attribute “LCS-Load-Balancer”.

Table 2: RADIUS attributes

ID	Name	Meaning
22	Framed-Route	IPv4 routes that should be entered into the routing table on the VPN gateway in the direction of the client (next-hop client). Format (string): <Prefix> [ifc=<destination interface>] [rtg_tag=<routing tag>] [admin_distance=<distance>] **<Prefix>** IPv4 address + '/' + prefix length or netmask **ifc=<destination interface>** Name of the IP interface or a load balancer that the route should point to, or “#Ifc”. If no destination interface is specified or it is “#Ifc”, the route points to the VPN interface for the respective

ID	Name	Meaning
		dial-in client. The interface name can contain up to 16 characters. **rtg_tag=<routing tag>** Routing tag for the route. If this is not specified, the route is given the tag of the dial-in interface. **admin_distance=<distance>** Administrative distance of the route as a number from 0 to 255. If not specified, the route is given the default distance for VPN routes.
99	Framed-IPv6-Route	IPv6 routes that should be entered into the routing table on the VPN gateway in the direction of the client (next-hop client). Format (string): <Prefix> [ifc=<destination interface>] [rtg_tag=<routing tag>] [admin_distance=<distance>] **<Prefix>** IPv6 address + '/' + prefix length **ifc=<destination interface>** Name of the IP interface or a load balancer that the route should point to, or "#Ifc". If no destination interface is specified or it is "#Ifc", the route points to the VPN interface for the respective dial-in client. The interface name can contain up to 16 characters. **rtg_tag=<routing tag>** Routing tag for the route. If this is not specified, the route is given the tag of the dial-in interface. **admin_distance=<distance>** Administrative distance of the route as a number from 0 to 255. If not specified, the route is given the default distance for VPN routes.
LANCOM 28	LCS load balancer	Format (string): <Load balancer name> [client_binding={no|yes}] The <load balancer name> can be up to 16 characters long and specifies a load-balancing remote site on the LANCOM routers. (!) This remote site is used for dynamic IKEv2-VPN load balancing and therefore must not be already used for static load balancing under **IP router** > **Load balancing**. The option "client_binding" turns the client binding on or off. Unless otherwise specified, client binding is off.

ID	Name	Meaning
		❗ The first IKEv2-VPN client to connect specifies this setting. Any subsequent settings for the client binding in connection with this load-balancing remote site are ignored.

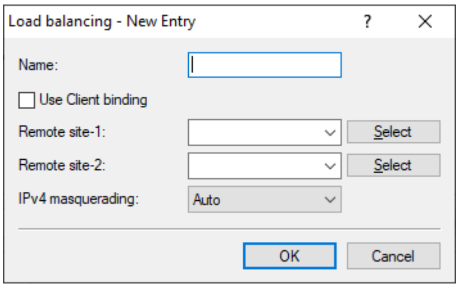
Example: RADIUS attributes for a simple load balancer made up of IKEv2 VPN tunnels to the central site

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

5.4.2 Accepting the masquerading setting of the load-balancer connection

From LCOS 10.40 your device supports the configuration of the masquerading setting of the load-balancer connection so that it is used for all of the different channels.

In LANconfig you find this setting under **IP router** > **Routing** > **Load balancing**.



Load balancing - New Entry

Name:

□ Use Client binding

Remote site-1:

Remote site-2:

IPv4 masquerading: Auto

IPv4 masquerading

This menu item contains the settings for IPv4 masquerading in the load balancer. Possible values:

Automatic

Adopts the masking option for each individual line from the routing table.

On

Activates NAT on all remote sites in the load balancer.

No

Deactivates NAT on all remote sites in the load balancer.

Only intranet

Activates NAT for networks of the type INTRANET. The DMZ will not be masked.

Additions to the Setup menu

IPv4-Masq.

This menu item contains the settings for IPv4 masquerading in the load balancer.

SNMP ID:

2.8.20.2.11

Console path:

Setup > **IP-Router** > **Load-Balancer** > **Bundle-Peers**

Possible values:

Auto
Adopts the masking option for each individual line from the routing table.

No
Deactivates NAT on all remote sites in the load balancer.

On
Activates NAT on all remote sites in the load balancer

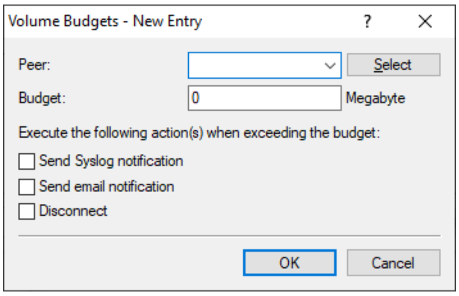
intranet
Enables NAT for INTRANET type networks. The DMZ is not masked.

Default:

Auto

5.5 Additional notification on volume budget

As of LCOS 10.40 your device uses Syslog and/or e-mail to notify you not only when 100% of the volume budget is reached, but also at 80% of the volume budget set under **Management** > **Budget** > **Budget monitoring** > **Volume budgets**.



Volume Budgets - New Entry

Peer: [ ] Select

Budget: 0 Megabyte

Execute the following action(s) when exceeding the budget:

□ Send Syslog notification

□ Send email notification

□ Disconnect

5.6 Show PPP bandwidth

As of LCOS 10.40 your device automatically extracts the actual down- and upstream rates from the PAP-ACK message during login. Some providers transmit the actual available layer-3 bandwidth after a successful PPP login (PPP PAP-ACK). This is relevant if the synchronized DSL bandwidth differs from the bandwidth agreed in the Internet tariff or if the actual bandwidth is unknown, such as with fiber-optic or Ethernet-based connections. In this case, the least value of the transmitted bandwidth and the DSL information is used as the QoS value. This information helps to operate of Quality of Service effectively.

A table is used that contains a parameter string with placeholders for the rates for each login ID of a provider. When logging in, the table is checked for the provider and the corresponding rates are used. If no provider string matches, all defined formats are checked in succession to see if there is a match. The first hit is taken and the up-/download rates are applied accordingly.

5.6.1 Additions to the Setup menu

Provider-Specifics

Some providers transmit the actual available layer-3 bandwidth after a successful PPP login (PPP PAP-ACK). This is relevant if the synchronized DSL bandwidth differs from the bandwidth agreed in the Internet tariff or if the actual bandwidth is unknown, such as with fiber-optic or Ethernet-based connections. In this case, the least value of the transmitted bandwidth and the DSL information is used as the QoS value. This information helps to operate of Quality of Service effectively.

This table contains login IDs with wildcards, for example to extract the actual up- and downstream speeds from the PAP ACK message sent during login.

If the table does not contain a matching login ID, then all of the parameter strings defined in the table are checked for a match. The first hit is taken and the up-/download rates are applied accordingly.

These values are displayed in the status menu under **Status** > **WAN** > **Connection-Bandwidth**. It shows the bandwidth synchronized by DSL, the bandwidth transmitted by the provider, as well as the resulting bandwidth used by the QoS.

SNMP ID:

2.2.62

Console path:

Setup > **WAN**

Provider

Provider login ID; may contain wildcards.

SNMP ID:

2.2.62.1

Console path:

Setup > **WAN** > **Provider-Specifics**

Possible values:

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

Default:

empty

Parameter-Format

Format of the parameter string contained in the PAP-ACK message for this provider. Possible placeholders are:

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

Example: The provider sends the string “SRU=39983#SRD=249973#” in their PAP-ACK message. The corresponding parameter string is then “SRU={txrate}#SRD={rxrate}#”.

SNMP ID:

2.2.62.2

Console path:

Setup > **WAN** > **Provider-Specifics**

Possible values:

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

Default:

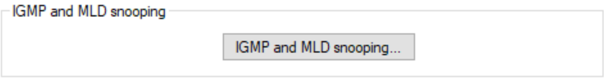
empty

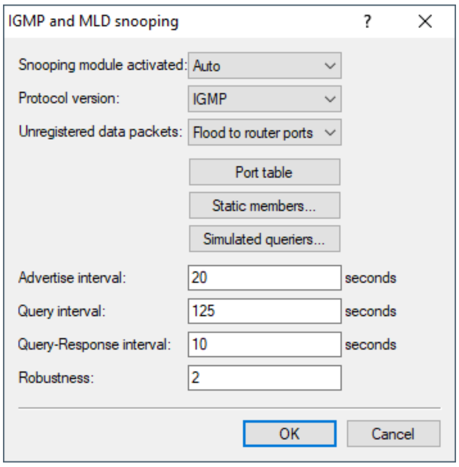
5.7 MLD snooping

As of LCOS 10.40 all devices with LAN bridge support MLD snooping (multicast listener discovery). For IPv6, this functions in a similar way to IGMP snooping for IPv4.

5.7.1 Configuration

In LANconfig, IGMP/MLD snooping are configured under **Interfaces** > **Snooping** > **IGMP and MLD snooping**





Snooping module activated: Auto
Protocol version: IGMP
Unregistered data packets: Flood to router ports
Advertise interval: 20 seconds
Query interval: 125 seconds
Query-Response interval: 10 seconds
Robustness: 2

Snooping module activated

Activates or deactivates IGMP/MLD snooping in the device and all of the defined querier instances. Without IGMP/MLD snooping the bridge functions like a simple switch and forwards all multicasts to all ports.

Possible values:

- On
- Off
- Automatic

Default:

- Automatic

In the setting **automatic** the bridge enables IGMP/MLD snooping only if there are queriers in the network.

If this function is deactivated, the bridge sends all IP multicast packets on all ports. With a change of the operating mode, the bridge completely resets the IGMP/MLD snooping function, i.e. it deletes all dynamically learned values (memberships, router-port properties).

Protocol version

Specify the supported protocols: IGMP, MLD, or both.

Unregistered data packets

This setting defines the handling of multicast data packets with a destination address outside of the reserved ranges “224.0.0.x” (IPv4) and “FF02::1” (IPv6), for which neither static memberships were defined nor were dynamic memberships learned.

Possible values:

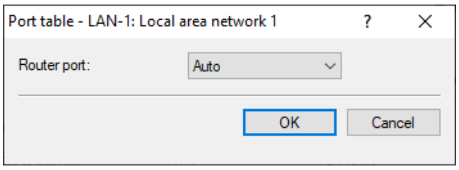
- Flood to router ports only: Sends these packets to all router ports.
- Flood to all ports: Sends these packets to all ports.
- Discard: Discards these packets.

Default:

- Router-Ports-only

Port table

This table is used to define the port-related settings for IGMP/MLD snooping.


Port table - LAN-1: Local area network 1

Router port: Auto

Port

The port for which the settings apply.

Possible values:

- Selects a port from the list of those available in the device.

Default:

- N/A

Router port

This option defines the port's behavior.

Possible values:

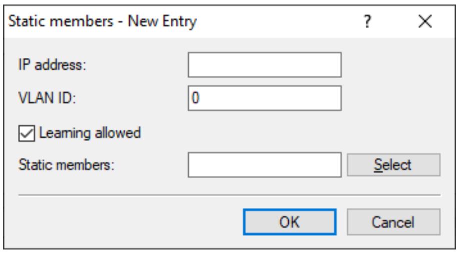
- Yes: This port will always work as a router port, irrespective of IGMP queries or router messages that the bridge receives on this port.
- No: This port will never work as a router port, irrespective of IGMP queries or router messages that the bridge receives on this port.
- Automatic: This port will work as a router port if IGMP queries or router messages are received. The port loses this status if the bridge receives no packets on this port for the duration of "Robustness*Query-Interval+(Query-Response-Interval/2)".

Default:

- Automatic

Static members

This table enables members to be defined manually, for example if they cannot or should not be learned automatically.



Static members - New Entry

IP address:

VLAN ID: 0

☑ Learning allowed

Static members:

IP address

The IP address of the manually defined multicast group.

Possible values:

- Valid IP multicast address.

VLAN ID

The VLAN ID used by the bridge to apply this static membership. For each IP multicast address you can make multiple entries with different VLAN IDs.

Possible values:

- 0 to 4096.

Default:

- 0

Special values:

- If “0” is selected as VLAN, the IGMP/MLD queries are sent without a VLAN tag. For this reason, this value only makes sense when VLAN is deactivated in general.

Learning allowed

This option activates the automatic learning of memberships in this multicast group. If automatic learning is deactivated, packets can only be sent via the ports which have been manually defined for the multicast group.

Static members

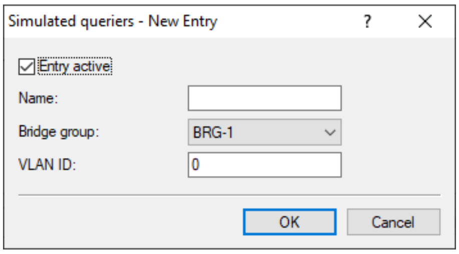
The bridge always delivers the packets with the corresponding IP multicast address to these ports, irrespective of any Join messages received.

Possible values:

- Comma-separated list of the desired ports, max. 215 alphanumerical characters.

Simulated queriers

This table contains all of the simulated queriers defined in the device. These units are employed if IGMP/MLD snooping functions are required but there is no multicast router in the network. The querier can be restricted to certain bridge groups or VLANs if you define multiple independent queriers which support the corresponding VLAN IDs.



Simulated queriers - New Entry

☑ Entry active

Name:

Bridge group: BRG-1

VLAN ID: 0

Entry active

Activates or deactivates the querier instance

Name

Name of the querier instance

Possible values:

- 8 alphanumerical characters.

Bridge group

Limits the querier instance to a certain bridge group.

Possible values:

- Select from the list of available bridge groups.
- None

Default:

- BRG-1

Special values:

- If the bridge group is set to “none”, the bridge outputs the IGMP/MLD queries to all bridge groups.

VLAN ID

Limits the querier instance to a certain VLAN.

Possible values:

- 0 to 4096

Default:

- 0

Special values:

- If “0” is selected as the VLAN ID, the bridge outputs IGMP/MLD queries without a VLAN tag. For this reason, this value only makes sense when VLAN is deactivated in general.

Advertise interval

The interval in seconds in which devices send packets advertising themselves as multicast routers. This information makes it quicker for other IGMP/MLD snooping devices to find which of their ports are to operate as router ports. When activating its ports, a switch (for example) can query for multicast routers, and the router can respond to this query with an advertisement of this type. Under some circumstances this method can be much quicker than the alternative IGMP/MLD queries.

Possible values:

- 4 to 180 seconds

Default:

- 20 seconds

Query interval

Interval in seconds in which a multicast-capable router (or a simulated querier) sends IGMP/MLD queries to the multicast address `224.0.0.1` (IPv4) "or FF02::1" (IPv6), so prompting the stations to transmit return messages about multicast group memberships. These regular queries influence the time in which memberships "age", expire, and are deleted.

- After the startup phase, the querier sends IGMP/MLD queries in this interval.
- A querier returns to the querier status after a time equal to "Robustness*Query-Interval+(Query-Response-Interval/2)".
- A port loses its router-port status after a time equal to "Robustness*Query-Interval+(Query-Response-Interval/2)".

Possible values:

- 10-figure number greater than 0.

Default:

- 125

❗ The query interval must be greater than the query response interval.

Query-Response-Interval

Interval in seconds influencing the timing between IGMP/MLD queries and router-port aging and/or memberships.

Interval in seconds in which a multicast-capable router (or a simulated querier) expects to receive responses to its IGMP/MLD queries. These regular queries influence the time in which memberships "age", expire, and are then deleted.

Possible values:

- 10-figure number greater than 0.

Default:

- 10

❗ The query response interval must be less than the query interval.

Robustness

This value defined the robustness of the IGMP/MLD protocol. This option tolerates packet losses of IGMP/MLD queries with respect to Join messages.

Possible values:

- 10-figure number greater than 0.

Default:

- 2

5.7.2 Additions to the Setup menu

IGMP-snooping

This menu contains the configuration options for IGMP/MLD snooping.

SNMP ID:

2.20.30

Console path:

Setup > **LAN-Bridge**

Operating

Activates or deactivates IGMP/MLD snooping in the device and all of the defined querier instances. Without IGMP/MLD snooping the bridge functions like a simple switch and forwards all multicasts to all ports.

> If this function is deactivated, the bridge sends all IP multicast packets on all ports. With a change of the operating mode, the device completely resets the IGMP/MLD snooping function, i.e. it deletes all dynamically learned values (memberships, router-port properties).

SNMP ID:

2.20.30.1

Console path:

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

Possible values:

No
Yes
Auto

Default:

Auto

Port-settings

This table defines the port-related settings for IGMP/MLD snooping.

SNMP ID:

2.20.30.2

Console path:

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

Router-port

This option defines the port's behavior.

SNMP ID:

2.20.30.2.2

Console path:

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

Possible values:

No

This port will never work as a router port, irrespective of IGMP/MLD queries or router messages received on this port.

Yes

This port will always work as a router port, irrespective of IGMP/MLD queries or router messages received on this port.

Auto

This port will work as a router port if IGMP/MLD queries or router messages are received. The port loses this status if no packets are received for the duration of “"Robustness*Query-Interval+(Query-Response-Interval/2)”.

Default:

Auto

Unregistered-Data-Packet-Handling

This setting defines the handling of multicast data packets with a destination address outside of the reserved ranges “224.0.0.x” and “FF02::1”, for which neither static memberships were defined nor were dynamic memberships learned.

SNMP ID:

2.20.30.3

Console path:

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

Possible values:

Router-Ports-only

Sends these packets to all router ports.

Flood

Sends these packets to all ports.

Discard

Discards these packets.

Default:

Router-Ports-only

Simulated-queriers

This table contains all of the simulated queriers defined in the device. These units are employed if IGMP/MLD snooping functions are required but there is no multicast router in the network. The querier can be limited to certain bridge groups or VLANs by defining multiple independent queriers to support the corresponding VLAN IDs.

SNMP ID:

2.20.30.4

Console path:

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

Bridge-group

Limits the querier instance to a certain bridge group.

SNMP ID:

2.20.30.4.3

Console path:

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

Possible values:

BRG-1
BRG-2
BRG-3
BRG-4
BRG-5
BRG-6
BRG-7
BRG-8
None

With this setting, the IGMP queries are issued on all bridge groups.

Default:

BRG-1

VLAN-ID

Limits the querier instance to a certain VLAN.

SNMP ID:

2.20.30.4.4

Console path:

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

Possible values:

0 … 4096

Default:

0

Special values:

0

If “0” is selected as VLAN, the IGMP/MLD queries are sent without a VLAN tag. For this reason, this value only makes sense when VLAN is deactivated in general.

Protocol

Limits the querier instance to a certain protocol.

SNMP ID:

2.20.30.4.6

Console path:

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

Possible values:

IGMP
MLD

Query-Interval

Interval in seconds in which a multicast-capable router (or a simulated querier) sends IGMP/MLD queries to the multicast address 224.0.0.1 or FF02::1, so prompting the stations to transmit return messages about multicast group memberships. These regular queries influence the time in which memberships “age”, expire, and are then deleted.

After the startup phase, the querier sends IGMP/MLD queries in this interval.

A querier returns to the querier status after a time equal to “Robustness*Query-Interval+(Query-Response-Interval/2)”.

A port loses its router-port status after a time equal to “Robustness*Query-Interval+(Query-Response-Interval/2)”.

ⓘ The query interval must be greater than the query response interval.

SNMP ID:

2.20.30.5

Console path:

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

Possible values:

Max. 10 characters from `[1-9]`

Default:

125

Query-Response-Interval

Interval in seconds influencing the timing between IGMP/MLD queries and router-port aging and/or memberships.

Interval in seconds in which a multicast-capable router (or a simulated querier) expects to receive responses to its IGMP/MLD queries. These regular queries influence the time in which memberships “age”, expire, and are then deleted.

The query response interval must be less than the query interval.

SNMP ID:

2.20.30.6

Console path:

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

Possible values:

Max. 10 characters from `[1-9]`

Default:

10

Robustness

This value defined the robustness of the IGMP/MLD protocol. This option tolerates packet losses of IGMP/MLD queries with respect to Join messages.

SNMP ID:

2.20.30.7

Console path:

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

Possible values:

Max. 10 characters from `[1-9]`

Default:

2

Static-Members

This table enables members to be defined manually, for example if they cannot or should not be learned automatically.

SNMP ID:

2.20.30.8

Console path:

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

Address

The IP address of the manually defined multicast group.

SNMP ID:

2.20.30.8.1

Console path:

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

Possible values:

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

VLAN-ID

The VLAN ID which is to support this static member. Each IP multicast address can have multiple entries with different VLAN IDs.

SNMP ID:

2.20.30.8.3

Console path:

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

Possible values:

0 … 4096

Default:

0

Special values:

0

If “0” is selected as VLAN, the IGMP/MLD queries are sent without a VLAN tag. For this reason, this value only makes sense when VLAN is deactivated in general.

Advertise-Interval

The interval in seconds in which devices send packets advertising themselves as multicast routers. This information makes it quicker for other IGMP/MLD snooping devices to find which of their ports are to operate as router ports. When activating its ports, a switch (for example) can query for multicast routers, and the router can respond to this query with an advertisement of this type. Under some circumstances this method can be much quicker than the alternative IGMP/MLD queries.

SNMP ID:

2.20.30.9

Console path:

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

Possible values:

4 … 180 Seconds

Default:

20

Protocols

Specify the supported protocols: IGMP, MLD, or both.

SNMP ID:

2.20.30.10

Console path:

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

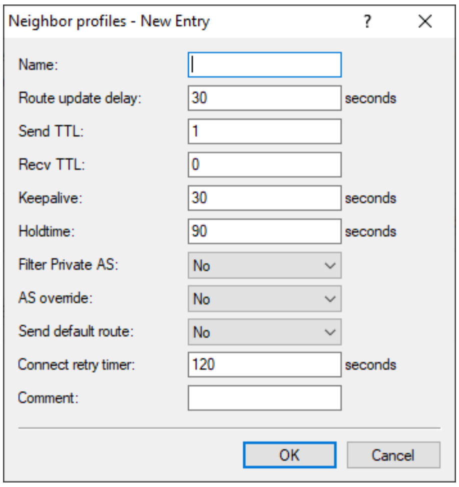
Possible values:

IGMP
MLD
IGMP and MLD

5.8 BGP: Switch for default route propagation

As of LCOS 10.40 your device has the option to handle default routes like normal routes when operating BGP.

In LANconfig you configure this option under **Routing protocols** > **BGP** > **Neighbor profiles**



Neighbor profiles - New Entry

Name:		
Route update delay:	30	seconds
Send TTL:	1	
Recv TTL:	0	
Keepalive:	30	seconds
Holdtime:	90	seconds
Filter Private AS:	No	
AS override:	No	
Send default route:	No	
Connect retry timer:	120	seconds
Comment:		

Send default route

This switch determines the behavior of the propagation of default routes. Possible values:

Yes

In BGP phase 3 (determining routes for redistribution), default routes are treated as normal routes.

No

Default routes are ignored if they are not sourced from the static BGP routes table (*IPv4 networks* or *IPv6 networks*).

5.8.1 Additions to the Setup menu

Send-Default-Route

This switch determines the behavior of the propagation of default routes.

SNMP ID:

2.93.1.3.11

Console path:

Setup > **Routing-Protocols** > **BGP** > **Neighbor-Profiles**

Possible values:

Yes

In BGP phase 3 (determining routes for redistribution), default routes are treated as normal routes.

No

Default routes are ignored if they are not sourced from the static BGP routes table (*2.93.1.6.1 IPv4* or *2.93.1.6.2 IPv6*).

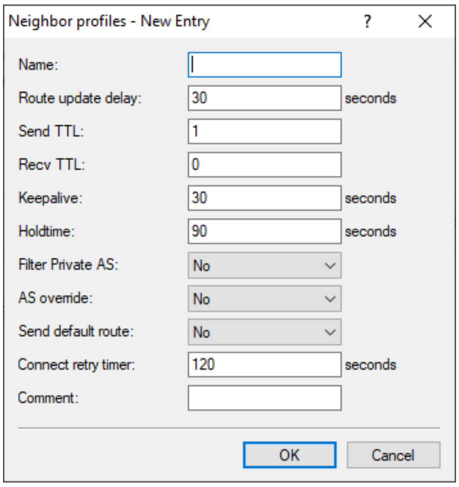
Default:

No

5.9 BGP: Adjustable connect retry timer

From LCOS 10.40 your device has the option to configure the Connect Retry Timer for BGP

In LANconfig you configure this option under **Routing protocols** > **BGP** > **Neighbor profiles**



Neighbor profiles - New Entry

Name:		
Route update delay:	30	seconds
Send TTL:	1	
Recv TTL:	0	
Keepalive:	30	seconds
Holdtime:	90	seconds
Filter Private AS:	No	
AS override:	No	
Send default route:	No	
Connect retry timer:	120	seconds
Comment:		

Connect retry timer

Specifies the time in seconds that the router waits until the next connection attempt following a failed BGP connection attempt. Generally speaking, this option is only necessary to speed things up when the remote site is in the “passive” connection mode. Default: 120 seconds

5.9.1 Additions to the Setup menu

Connect-Retry-Time

Specifies the time in seconds that the router waits until the next connection attempt following a failed BGP connection attempt. Generally speaking, this option is only necessary to speed things up when the remote site is in the “passive” connection mode.

SNMP ID:

2.93.1.3.12

Console path:

Setup > **Routing-Protocols** > **BGP** > **Neighbor-Profiles**

Possible values:

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

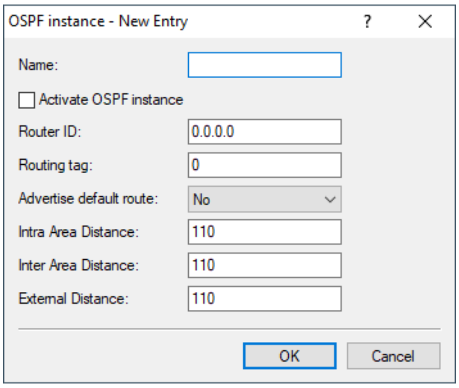
Default:

120

5.10 Administrative distance configurable with OSPF

As of LCOS 10.40 OSPF can now be configured with the administrative distances to be used when OSPF routes are entered into the routing table. The administrative distance can be specified according to the OSPF route type.

In order to configure the administrative distance for OSPF with LANconfig, navigate to the **Routing protocols** > **OSPF** > **OSPF instance** menu.



Name:

□ Activate OSPF instance

Router ID: 0.0.0.0

Routing tag: 0

Advertise default route: No

Intra Area Distance: 110

Inter Area Distance: 110

External Distance: 110

Intra Area Distance

Defines the administrative distance with which OSPF inserts incoming intra-area routes into the routing table.

Inter Area Distance

Defines the administrative distance with which OSPF inserts incoming inter-area routes into the routing table.

External distance

Defines the administrative distance with which OSPF inserts incoming external routes into the routing table.

5.10.1 Additions to the Setup menu

Intra-Area-Distance

Defines the administrative distance with which OSPF inserts incoming intra-area routes into the routing table.

SNMP ID:

2.93.3.1.7

Console path:

Setup > **Routing-Protocols** > **OSPF** > **OSPF-Instance**

Possible values:

0 … 255

Default:

110

Inter-Area-Distance

Defines the administrative distance with which OSPF inserts incoming inter-area routes into the routing table.

SNMP ID:

2.93.3.1.8

Console path:

Setup > **Routing-Protocols** > **OSPF** > **OSPF-Instance**

Possible values:

0 … 255

Default:

110

External-Distance

Defines the administrative distance with which OSPF inserts incoming external routes into the routing table.

SNMP ID:

2.93.3.1.9

Console path:

Setup > **Routing-Protocols** > **OSPF** > **OSPF-Instance**

Possible values:

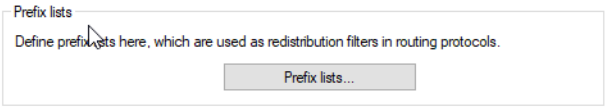
0 … 255

Default:

110

5.11 Filter list for redistribution in OSPF

Filter lists can be used to allow or reject certain prefixes during redistribution by the OSPF. This is done as with BGP, i.e. create the prefix filter list under **IP router** > **General** > **Prefix lists**.



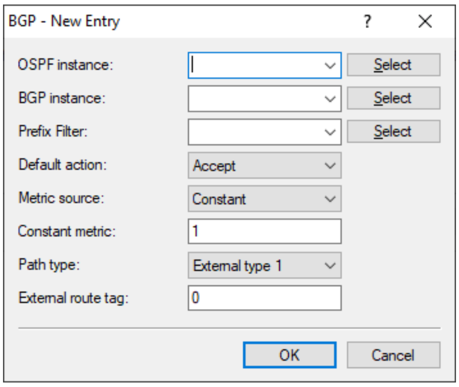
Prefix lists

Define prefix lists here, which are used as redistribution filters in routing protocols.

Using prefix lists with OSPF

These **prefix lists** can be referenced for the redistribution of static routes, BGP and OSPF protocol connected routes, and you can specify whether these prefix lists should be accepted or rejected.

Routing protocols > OSPF > BGP



BGP - New Entry

OSPF instance:		Select
BGP instance:		Select
Prefix Filter:		Select
Default action:	Accept	
Metric source:	Constant	
Constant metric:	1	
Path type:	External type 1	
External route tag:	0	

Prefix filter

Name of the prefix-filter list from *Prefix lists*.

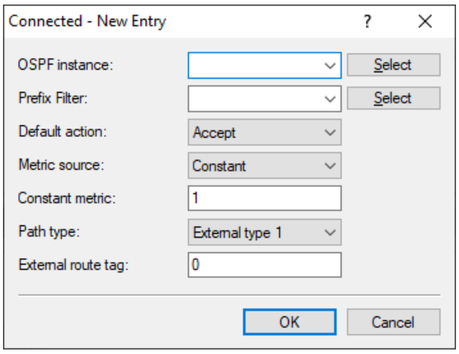
Default action

Defines the default handling of prefixes that are configured in the prefix list. Possible values:

Accept

Deny

Routing protocols > OSPF > Connected



Connected - New Entry

OSPF instance:		Select
Prefix Filter:		Select
Default action:	Accept	
Metric source:	Constant	
Constant metric:	1	
Path type:	External type 1	
External route tag:	0	

Prefix filter

Name of the prefix-filter list from *Prefix lists*.

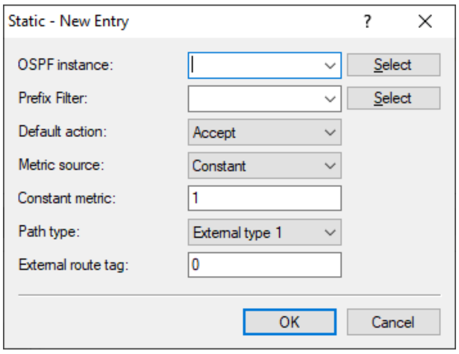
Default action

Defines the default handling of prefixes that are configured in the prefix list. Possible values:

Accept

Deny

Routing protocols > OSPF > Static



Static - New Entry

OSPF instance:	
Prefix Filter:	
Default action:	Accept
Metric source:	Constant
Constant metric:	1
Path type:	External type 1
External route tag:	0

Prefix filter

Name of the prefix-filter list from *Prefix lists*.

Default action

Defines the default handling of prefixes that are configured in the prefix list. Possible values:

Accept

Deny

5.11.1 Additions to the Setup menu

Filter-List

Name of the prefix filter list from **Setup** > **Routing-Protocols** > **Filter** > **Prefix-List**.

SNMP ID:

2.93.3.9.1.3

Console path:

Setup > **Routing-Protocols** > **OSPF** > **Route-Redistribution** > **BGP**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]-_`

Default:

empty

Default-Action

Defines the default handling of prefixes that are configured in the prefix list.

SNMP ID:

2.93.3.9.1.8

Console path:

Setup > **Routing-Protocols** > **OSPF** > **Route-Redistribution** > **BGP**

Possible values:

Accept
Deny

Default:

Accept

Filter-List

Name of the prefix filter list from **Setup** > **Routing-Protocols** > **Filter** > **Prefix-List**.

SNMP ID:

2.93.3.9.2.2

Console path:

Setup > **Routing-Protocols** > **OSPF** > **Route-Redistribution** > **Connected**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]-_`

Default:

empty

Default-Action

Defines the default handling of prefixes that are configured in the prefix list.

SNMP ID:

2.93.3.9.2.7

Console path:

Setup > **Routing-Protocols** > **OSPF** > **Route-Redistribution** > **Connected**

Possible values:

Accept
Deny

Default:

Accept

Filter-List

Name of the prefix filter list from **Setup** > **Routing-Protocols** > **Filter** > **Prefix-List**.

SNMP ID:

2.93.3.9.4.2

Console path:

Setup > **Routing-Protocols** > **OSPF** > **Route-Redistribution** > **Static**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]-_`

Default:

empty

Default-Action

Defines the default handling of prefixes that are configured in the prefix list.

SNMP ID:

2.93.3.9.4.7

Console path:

Setup > **Routing-Protocols** > **OSPF** > **Route-Redistribution** > **Static**

Possible values:

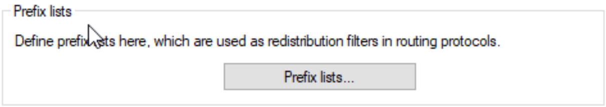
Accept
Deny

Default:

Accept

5.12 Filter list for redistribution in LISP

Filter lists can be used to allow certain prefixes during redistribution by the LISP. This is done as with BGP, i.e. create the prefix filter list under **IP router** > **General** > **Prefix lists**.



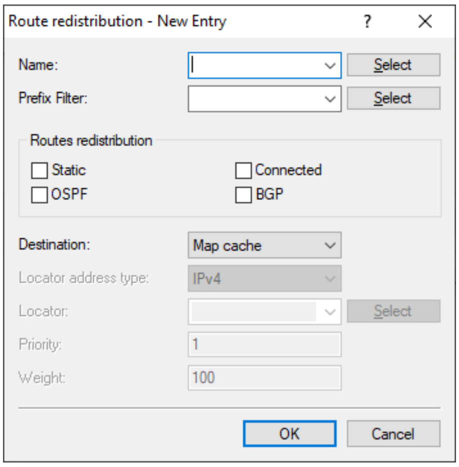
Prefix lists

Define prefix lists here, which are used as redistribution filters in routing protocols.

Using prefix lists with LISP

You can use these **Prefix lists** for redistributing static routes, BGP, OSPF and connected routes.

Routing protocols > LISP > Route redistribution



Route redistribution - New Entry

Name: | Select

Prefix Filter: Select

Routes redistribution

□ Static □ Connected

□ OSPF □ BGP

Destination: Map cache

Locator address type: IPv4

Locator: Select

Priority: 1

Weight: 100

Prefix filter

Name of the prefix-filter list from *Prefix lists*. Route redistribution is allowed for prefixes in this list.

5.12.1 Additions to the Setup menu

Filter-List

Name of the prefix filter list from **Setup** > **Routing-Protocols** > **Filter** > **Prefix-List**. Route redistribution is allowed for prefixes in this list.

SNMP ID:

2.93.4.10.8

Console path:

Setup > **Routing-Protocols** > **LISP** > **Redistribution**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]-_`

Default:

empty

6 Firewall

6.1 No MAC addresses as destinations in firewall rules

As of LCOS 10.40 MAC addresses are no longer supported as destinations in firewall rules. A station object created under **Firewall/QoS** > **IPv4 rules** > **Firewall objects** > **Station objects** cannot be used as a destination object in a firewall rule.

6.2 Configurable DNS cache time

From LCOS 10.40 you can configure the DNS cache time for using DNS objects in the firewall. The DNS minimum cache time specifies the minimum time in seconds that a DNS entry is stored if the TTL in the DNS packet is less than the configured value. A buffer of 10 seconds is added. The value used is the maximum of the DNS minimum cache time parameter and the TTL from the DNS packet plus 10 seconds.

6.2.1 Additions to the Setup menu

DNS minimum cache time

This option specifies the minimum time in seconds that a DNS entry is stored if the TTL in the DNS packet is less than the configured value. A buffer of 10 seconds is added. The value that is taken is the maximum of this parameter **DNS minimum cache time** and the TTL from the DNS packet plus 10 seconds.

SNMP ID:

2.110.3

Console path:

Setup > **Firewall**

Possible values:

Max. 11 characters from `[0-9]`

Default:

180

7 Multicast routing

In data communication, there are four basic categories of communication relationship: Unicast, broadcast, multicast and anycast. Unicast means 1:1 communication, i.e. one sender communicates with one receiver. With a broadcast, one sender sends data to all connected devices (1:n relationship, or “one to all”). This communication method is inefficient for certain services such as IPTV, since all clients would receive the data, including clients who don’t want it. This is why there is another method, multicast, for establishing sender / receiver relationships. Multicast is an efficient communication method for a sender to transmit data only to those devices that are interested in it (1:m relationship, or “one to many”). Receivers therefore have to announce their interest in receiving this data. With the communications relationship Anycast, a sender sends the data to any one receiver in a group. This chapter deals with multicast.

With multicast, there are two basic roles: Sender and receiver. A receiver is, for example, an IPTV receiver or a mobile device/PC. A sender is understood to mean the multicast source, e.g. an IPTV sender. If a client wishes to receive multicast data, e.g. an IPTV channel, it signals its interest by sending an IGMP (Internet Group Management Protocol) membership report or, with IPv6, an MLD (Multicast Listener Discovery) membership report. A multicast router will automatically generate a multicast routing entry for this group. In this instance data flow is “reversed”, i.e. from the source to the receiver. If the client is no longer interested in the multicast data, it sends a membership report to leave the group.

The IP address range for multicast is defined from 224.0.0.0 to 239.255.255.255 for IPv4, and for IPv6 with the prefix FF00::/8. The multicast address range is divided into different blocks, e.g. link local, source specific multicast (232.0.0.0 to 232.255.255.255) or organization-local scope (239.0.0.0 to 239.255.255.255).

Furthermore, there are two categories of multicast: Any Source Multicast (ASM) and Source Specific Multicast (SSM). For Any Source Multicast, represented as (*,G), the receiver only specifies the multicast group G and accepts it from any source *. Any Source Multicast is the older of the two methods. Source Specific Multicast is the modern variant where a receiver requests one or more sources S as well as the desired group. However, SSM requires IGMPv3 or MLDv2. If possible, SSM should be operated with IGMPv3 as this scales better. As a rule, IPTV architectures are based on SSM.

Multicast routes are not managed in the normal (unicast) routing table, but in a separate multicast routing table. Routing entries there are not usually configured statically, but are generated dynamically by multicast routing protocols such as PIM (Protocol Independent Multicast) or by a proxy, e.g. an IGMP proxy. Multicast basically requires a functional unicast routing table, as the reverse path forward check (RPF check) checks to see whether there is a route to the multicast source. As a rule, a multicast routing protocol such as PIM is always used with a unicast routing protocol, such as OSPF.

There are three approaches to a multicast routing scenario:

1. For a simple multicast routing scenario: Use of the IGMP/MLD proxy.
2. For a complex multicast routing scenario: PIM SSM.
3. Static group entries should only be configured if clients do not support IGMP/MLD.

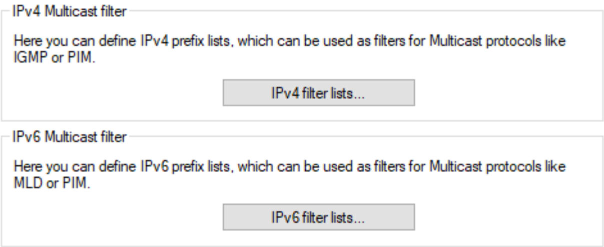
PIM Sparse Mode can also be used instead of PIM SSM, although both the role of the rendezvous point and that of the first-hop router must be performed by a third-party manufacturer directly in front of the multicast source.

7.1 General multicast show commands

- show IPv4-mfib / show IPv4-mfib (an alias is ipv4-mroute / ipv6-mroute): Displays the contents of the Multicast Forwarding Information Base/Routing Table.
- show iPv4-tib / show iPv6-tib: Displays the contents of the Tree Information Base. Contains information about the multicast group status and additional information from PIM.
- show igmp-groups: Displays information about multicast groups that the router itself has joined.

7.2 General settings

To configure the general Multicast settings, open LANconfig and go to **Multicast** > **General**.



IPv4 Multicast filter

Here you can define IPv4 prefix lists, which can be used as filters for Multicast protocols like IGMP or PIM.

IPv4 filter lists...

IPv6 Multicast filter

Here you can define IPv6 prefix lists, which can be used as filters for Multicast protocols like MLD or PIM.

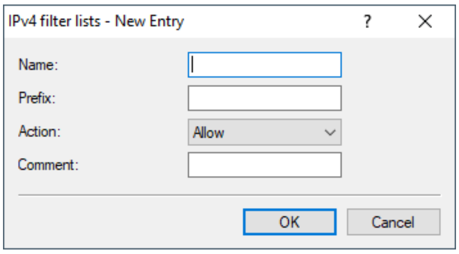
IPv6 filter lists...

7.2.1 IPv4 filter lists

In LANconfig you configure the IPv4 filter lists for Muilticast under **Muilticast** > **General** > **IPv4 Multicast filter** using **IPv4 filter lists**.

This table can be used to specify lists of desired or unwanted IPv4 multicast addresses and prefixes. Different individual filter rules can be combined into a rules list by using the same name. A rules list can be used to prohibit or allow certain prefixes.

The names of the filter lists can be referenced in various places and managed globally using this table.



IPv4 filter lists - New Entry

Name:	
Prefix:	
Action:	Allow
Comment:	

Name

Give this entry a name. A list is defined by several entries with the same name.

Prefix

Enter here the IPv4 address followed by the prefix length of the network (CIDR notation). This specifies how many most-significant bits (MSB) of the IP address are necessary for a match.

Action

Specify whether the prefixes in this filter entry should be allowed or denied.

Comment

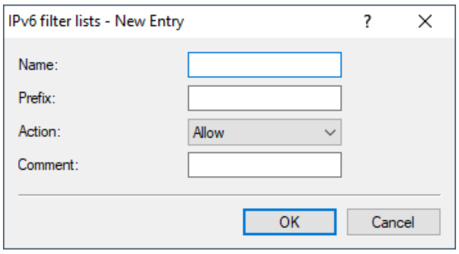
Comment on this entry.

7.2.2 IPv6 filter lists

In LANconfig you configure the IPv4 filter lists for Muilticast under **Multicast** > **General** > **IPv6 Multicast filter** using **IPv6 filter lists**.

This table can be used to specify lists of desired or unwanted IPv6 multicast addresses and prefixes. Different individual filter rules can be combined into a rules list by using the same name. A rules list can be used to prohibit or allow certain prefixes.

The names of the filter lists can be referenced in various places and managed globally using this table.



IPv6 filter lists - New Entry

Name:

Prefix:

Action: Allow

Comment:

Name

Give this entry a name. A list is defined by several entries with the same name.

Prefix

Enter the IPv6 multicast address and prefix here.

Action

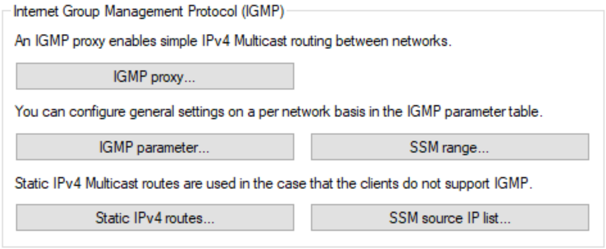
Specify whether the prefixes in this filter entry should be allowed or denied.

Comment

Comment on this entry.

7.3 IGMP (Internet Group Management Protocol)

IGMP is configured with LANconfig under **Multicast** > **IGMP / MLD** > **Internet Group Management Protocol (IGMP)**.



Internet Group Management Protocol (IGMP)

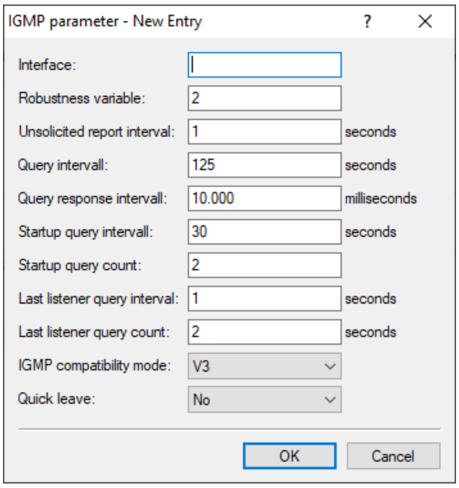
An IGMP proxy enables simple IPv4 Multicast routing between networks.

You can configure general settings on a per network basis in the IGMP parameter table.

Static IPv4 Multicast routes are used in the case that the clients do not support IGMP.

7.3.1 IGMP parameters

In LANconfig you configure the general IGMP parameters under **Multicast** > **IGMP/MLD** > **Internet Group Management Protocol (IGMP)** via **IGMP parameter**.



IGMP parameter - New Entry

Interface:		
Robustness variable:	2	
Unsolicited report interval:	1	seconds
Query intervall:	125	seconds
Query response intervall:	10.000	milliseconds
Startup query intervall:	30	seconds
Startup query count:	2	
Last listener query interval:	1	seconds
Last listener query count:	2	seconds
IGMP compatibility mode:	V3	
Quick leave:	No	

Interface

Name of the interface that the IGMP configuration applies to. The entry named DEFAULT applies to all interfaces without a specific entry. If there is no DEFAULT entry, the internal default values for a DEFAULT entry still apply. Possible values are DEFAULT, IPv4 networks, e.g. INTRANET or IPv4 (WAN) remotes. Also allowed are wildcard entries with * for RAS interfaces, e.g. “VPN*”.

Robustness variable

Number of IGMP message repeats. (1-10; Default: 2)

Unsolicited report interval

Specifies the time between repetitions of a host's initial report of membership in a group. (1-25 seconds; Default: 2)

Query interval

Interval between IGMP general queries. (2-99999 seconds; Default: 125)

Query response interval

Maximum response time. The maximum response time is inserted into periodic general queries. The value for the query response interval must be less than the value for query interval. (1-999999 milliseconds; Default: 10000)

Startup query interval

The interval between IGMP general queries sent after the querier starts up. (1-99998 seconds; Default: 30)

Startup query count

Number of IGMP general queries sent on startup, separated by the startup query interval. (1-10; Default: 2)

Last listener query interval

Specifies the value of the Maximum Response Time in Multicast Address-Specific Queries that are sent in response to Done messages. The parameter also specifies the time between multicast address-specific queries. (1-25 seconds; Default: 2)

Last listener query count

Number of multicast address-specific queries sent before the router assumes that there are no more local listeners. It also specifies the number of multicast address-specific queries sent before the router assumes there are no more listeners of a particular source. (1-10; Default: 2)

IGMP compatibility mode

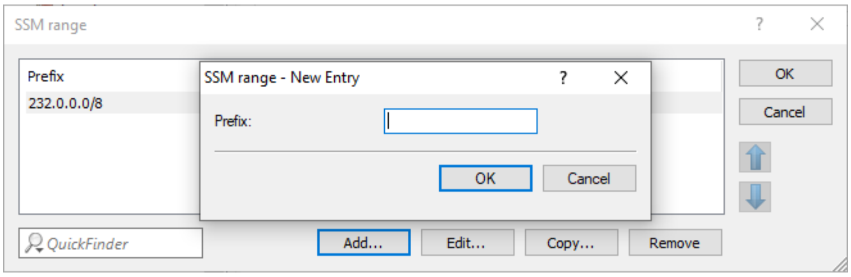
IGMP version used by the device when operating as a multicast router. Possible values: Off, V1, V2, V3. (default: V3)

Quick leave

Enables receivers to leave multicast groups quickly. This should only be used if there is only one receiver per group on the interface. Internally, the Last Listener Query Count parameter is set to 1 and the Last Listener Query Interval is set to 20 ms. Possible values: Yes, No (default: No)

7.3.2 SSM range

In LANconfig you configure the SSM range under **Multicast** > **IGMP / MLD** > **Internet Group Management Protocol (IGMP)** via **SSM range**.



SSM range

Prefix
232.0.0.0/8

SSM range - New Entry

Prefix:

Prefix

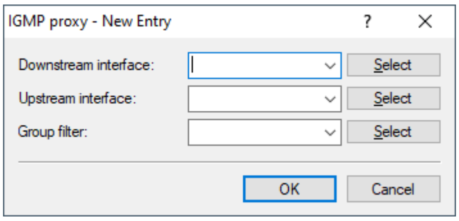
Specifies the IP address range in prefix notation used for SSM.

7.3.3 IGMP proxy

An IGMP proxy is typically used for Internet connections with multicast IPTV. Clients or IPTV set top boxes (STBs) on the local network send IGMP messages to receive a specific TV channel. To this end, they join certain multicast groups and later leave them again. The router and/or IGMP proxy receives the IGMP messages and forwards them to the provider network and filters the groups, if required. The IGMP proxy works for the local network with its clients.

An IGMP proxy can also be used in simple multicast routing scenarios, for example via VPN, without having to use PIM. The configuration of the IGMP proxy creates a static (tree) structure without alternative paths, redundancy or loop prevention. IGMP proxies can be "cascaded" by connecting multiple routers in series.

In LANconfig you configure the IGMP proxy under **Multicast** > **IGMP / MLD** > **Internet Group Management Protocol (IGMP)** via **IGMP proxy**.



IGMP proxy - New Entry

Downstream interface:

Upstream interface:

Group filter:

Downstream interface

Interface name used by IGMP clients to join groups and receive IGMP messages from the proxy. Possible values are IPv4 networks, e.g. INTRANET, IPv4 (WAN) remotes. Also allowed are wildcard entries with * for RAS interfaces, e.g. "VPN*".

For provider-based IPTV scenarios, the local network, e.g. INTRANET, must be configured here.

Upstream interface

Interface name used by the IGMP proxy to send messages on behalf of clients. The source of the multicast messages must be reached via this interface. Possible values are IPv4 networks, e.g. INTRANET and IPv4 (WAN) remotes.

For provider-based IPTV scenarios, the WAN remote site, e.g. INTERNET, must be configured here.

Group filter

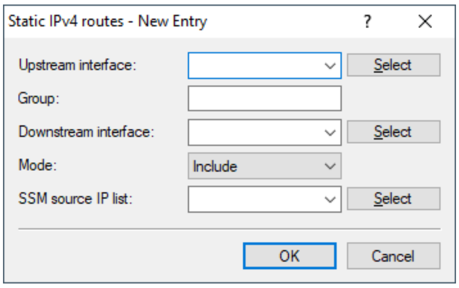
Name of the group filter that is to apply to this proxy. References the table IPv4 filter lists under **Multicast** > **General**. By default, the filter entry is blank or points to the filter list "ANY", which allows all multicast groups. The group filter can be used to restrict the multicast groups available for clients.

7.3.4 Static IPv4 multicast routing

Static multicast routing can be used where multicast clients do not support IGMP and in scenarios where multicast traffic has to keep flowing even if the clients do not request to join the corresponding group. When the entry is created, the router creates IGMP joins and group reports on the upstream interface.

Please note that static multicast routing can cause high traffic and load because the multicast data is forwarded at all times.

In LANconfig you configure the static IPv4 multicast routes under **Multicast** > **IGMP / MLD** > **Internet Group Management Protocol (IGMP)** via **Static IPv4 routes**.



Upstream interface

Interface name where the multicast packets reach the router. Possible values are IPv4 networks, e.g. INTRANET and IPv4 (WAN) remotes.

Group

The static forwarding of multicast data is to be configured for this multicast group, e.g. 239.0.0.1.

Downstream interface

Interface name where the multicast packets exit the router. Possible values are IPv4 networks, e.g. INTRANET and IPv4 (WAN) remotes.

Mode

If SSM is to be operated: This controls the way in which an IGMP membership report requests the source addresses of multicast sources. Possible values:

Include

An IGMP membership report is sent with the record type "Change to Include Mode". The entries from the SSM source IP list are sent as the desired source addresses. A combination of the setting "Include" and the SSM source IP list with an entry "ANY" will not produce meaningful results and is not accepted internally as a configuration. Otherwise all source IP addresses would be rejected.

Exclude

An IGMP membership report is sent with the record type "Change to Exclude Mode". If the source list contains the entry "ANY" or "0.0.0.0", i.e. all sources are allowed, then an IGMP membership report will be sent with a join group for "any sources". If the list contains an entry other than 0.0.0.0, an IGMP membership report "block sources" is sent with the corresponding IP address.

ⓘ If you want to use an SSM group with any source address, you have to link the mode "Exclude" and SSM source IP list "ANY".

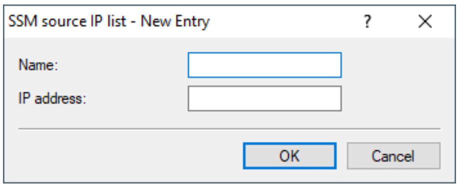
SSM source IP list

If SSM is to be operated, a list of desired sources can be specified here in addition to the multicast group. If all sources are to be allowed, the predefined list "ANY" can be used with the entry "0.0.0.0".

7.3.5 SSM source IP list

This table can be used to specify lists of desired or unwanted (unicast) source IP addresses. These can be referenced in various places and managed globally using this table. A list is defined by several entries with the same name.

In LANconfig you configure SSM source IP list under **Multicast** > **IGMP / MLD** > **Internet Group Management Protocol (IGMP)** via **SSM source IP list**.



Name

Enter a name for the entry. A list is defined by several entries with the same name.

IP address

Unicast source IPv4 address. Multicast addresses are not a valid entry at this point, since the source IP addresses of a multicast entry (S, G) are defined here.

7.3.6 Tutorial: Setting up an IGMP proxy

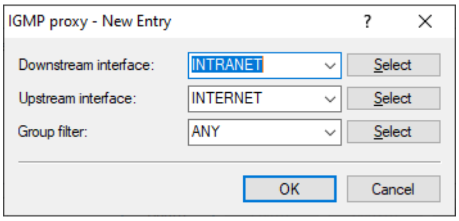
The following tutorial describes the steps required to set up an IGMP proxy for multicast routing.

In this example, multicast clients are located in the network "INTRANET" and the multicast sources are reached via the WAN remote site "INTERNET". The IGMP proxy forwards IGMP messages from INTRANET to the INTERNET on behalf of the clients. It is also possible to filter certain multicast groups.

1. Create a new table entry under **Multicast** > **IGMP/MLD** > **Internet Group Management Protocol (IGMP)** > **IGMP proxy**:

   - **Downstream interface**: Interface name used by IGMP clients to join groups and receive IGMP messages from the proxy. Enter the name of the client network, e.g., "INTRANET".
   - **Upstream interface**: Interface name used by the IGMP proxy to send messages on behalf of clients. The source of the multicast messages must be reached via this interface. Configure the name of the remote site for the Internet connection here, e.g. "INTERNET".
   - **Group filter**: Name of the group filter that is to apply to this proxy. References the table **IPv4 filter lists** under **Multicast** > **General**. The group filter can be used to restrict the multicast groups available to clients. Select "ANY" to allow all multicast groups.

ⓘ Further settings, for example in the firewall, are no longer necessary as of LCOS 10.40.



IGMP proxy - New Entry

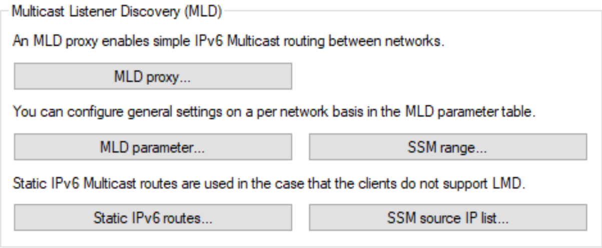
Downstream interface: INTRANET

Upstream interface: INTERNET

Group filter: ANY

7.4 MLD (Multicast Listener Discovery)

MLD is configured with LANconfig under **Multicast** > **IGMP / MLD** > **Multicast Listener Discovery (MLD)**.



Multicast Listener Discovery (MLD)

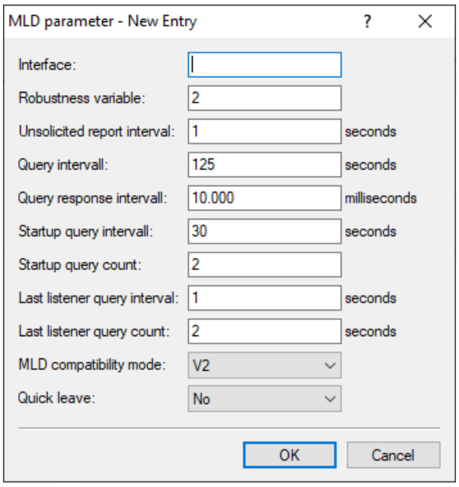
An MLD proxy enables simple IPv6 Multicast routing between networks.

You can configure general settings on a per network basis in the MLD parameter table.

Static IPv6 Multicast routes are used in the case that the clients do not support LMD.

7.4.1 MLD parameters

In LANconfig, you configure the general MLD parameters under **Multicast** > **IGMP / MLD** > **Multicast Listener Discovery (MLD)** via **MLD parameter**.



MLD parameter - New Entry

Interface:

Robustness variable: 2

Unsolicited report interval: 1 seconds

Query intervall: 125 seconds

Query response intervall: 10.000 milliseconds

Startup query intervall: 30 seconds

Startup query count: 2

Last listener query interval: 1 seconds

Last listener query count: 2 seconds

MLD compatibility mode: V2

Quick leave: No

Interface

Name of the interface that the MLD configuration applies to. The entry named DEFAULT applies to all interfaces without a specific entry. If there is no DEFAULT entry, the internal default values for a DEFAULT entry still apply. Possible values are DEFAULT, IPv6 networks, e.g. INTRANET, IPv6 (WAN) remotes or IPv6 RAS templates.

Robustness variable

Number of MLD message repeats. (1-10; Default: 2)

Unsolicited report interval

Specifies the time between repetitions of a host's initial report of membership in a group. (1-25 seconds; Default: 2)

Query interval

Interval between MLD general queries. (2-99999 seconds; Default: 125)

Query response interval

The maximum response time is inserted into periodic MLD general queries. The value for the query response interval must be less than the value for query interval. (1-999999 milliseconds; Default: 10000)

Startup query interval

The interval between MLD general queries sent after the querier starts up. (1-99998 seconds; Default: 30)

Startup query count

Number of MLD general messages on startup, separated by the startup query interval. (1-10; Default: 2)

Last listener query interval

Specifies the value of the Maximum Response Code (with IPv6) Multicast Address-Specific Queries that are sent to Done messages. The parameter also specifies the time between multicast address-specific queries. (1-25 seconds; Default: 2)

Last listener query count

Number of multicast address-specific queries sent before the router assumes that there are no more local listeners. It also specifies the number of multicast address-specific queries sent before the router assumes there are no more listeners of a particular source. (1-10; Default: 2)

MLD compatibility mode

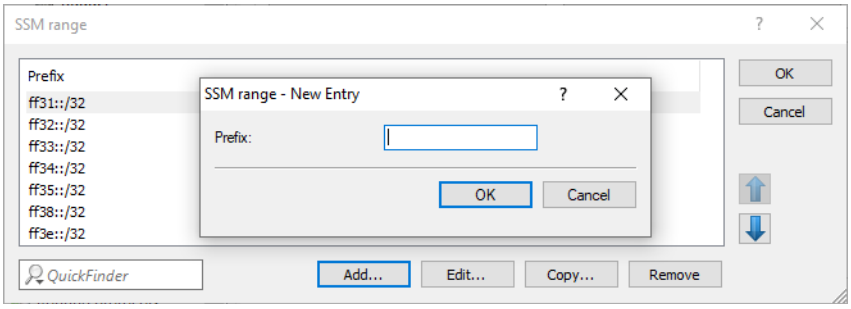
MLD version used by the device when operating as a multicast router. Possible values: Off, V1, V2 (default: V2)

Quick leave

Enables receivers to leave multicast groups quickly. This should only be used if there is only one receiver per group on the interface. Internally, the Last Listener Query Count parameter is set to 1 and the Last Listener Query Interval is set to 20 ms. Possible values: Yes, No (default: No)

7.4.2 SSM range

In LANconfig, you configure the SSM range under **Multicast** > **IGMP / MLD** > **Multicast Listener Discovery (MLD)** via **SSM range**.



SSM range

Prefix
ff31::/32
ff32::/32
ff33::/32
ff34::/32
ff35::/32
ff38::/32
ff3e::/32

SSM range - New Entry

Prefix:

Prefix

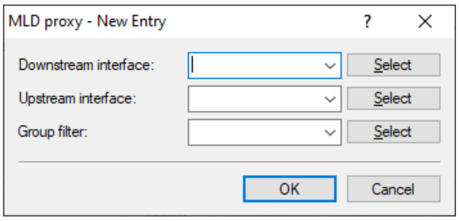
Specifies the IP address range in prefix notation used for SSM.

7.4.3 MLD proxy

An MLD proxy is typically used for multicast IPTV on IPv6 Internet connections. Clients or IPTV set top boxes (STBs) on the local network send MLD messages to receive a specific TV channel. To this end, they join certain multicast groups and later leave them again. The router and/or MLD proxy receives the MLD messages and forwards them to the provider network and filters the groups, if required. The MLD proxy works for the local network with its clients.

An MLD proxy can also be used in simple multicast routing scenarios, for example via VPN, without having to use PIM. The configuration of the MLD proxy creates a static (tree) structure without alternative paths, redundancy or loop prevention. MLD proxies can be "cascaded" by connecting multiple routers in series.

In LANconfig, you configure the MLD proxy under **Multicast** > **IGMP / MLD** > **Multicast Listener Discovery (MLD)** via **MLD proxy**.


MLD proxy - New Entry

Downstream interface:

Upstream interface:

Group filter:

Downstream interface

Interface name used by MLD clients to join groups and receive MLD messages from the proxy. Possible values are IPv6 networks, e.g. INTRANET, IPv6 (WAN) remotes or RAS templates.

For provider-based IPTV scenarios, the local network, e.g. INTRANET, must be configured here.

Upstream interface

Interface name used by the MLD proxy to send messages on behalf of clients. The source of the multicast messages must be reached via this interface. Possible values are IPv6 networks, e.g. INTRANET and IPv6 (WAN) remotes.

For provider-based IPTV scenarios, the WAN remote site, e.g. INTERNET, must be configured here.

Group filter

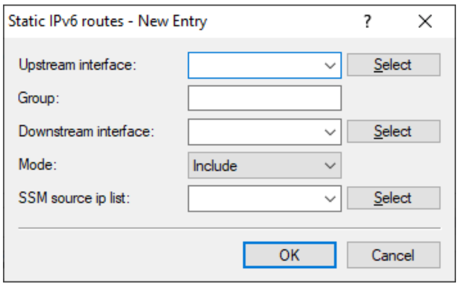
Name of the group filter that is to apply to this proxy. References the table IPv6 filter lists under **Multicast** > **General**. By default, the filter entry is blank or points to the filter list "ANY", which allows all multicast groups. The group filter can be used to restrict the multicast groups available for clients.

7.4.4 Static IPv6 multicast routing

Static multicast routing can be used where multicast clients do not support MLD and in scenarios where multicast traffic has to keep flowing even if the clients do not request to join the corresponding group. When the entry is created, the router creates MLD group reports on the upstream interface.

Please note that static multicast routing can cause high traffic and load because the multicast data is forwarded at all times.

In LANconfig you configure the static IPv6 multicast routes under **Multicast** > **IGMP / MLD** > **Multicast Listener Discovery (MLD)** via **Static IPv6 routes**.



Static IPv6 routes - New Entry

Upstream interface:		Select
Group:		
Downstream interface:		Select
Mode:	Include	
SSM source ip list:		Select

Upstream interface

Interface name where the multicast packets reach the router. Possible values are IPv6 networks, e.g. INTRANET and IPv6 (WAN) remotes.

Group

The static forwarding of multicast data is to be configured for this multicast group, e.g. “ff09::1”.

Downstream interface

Interface name where the multicast packets exit the router. Possible values are IPv6 networks, e.g. INTRANET and IPv6 (WAN) remotes.

Mode

If SSM is to be operated: This controls the way in which an MLD membership report requests the source addresses of multicast sources. Possible values:

Include

An MLD membership report is sent with the record type “Change to Include Mode”. The entries from the SSM source IP list are sent as the desired source addresses. A combination of the setting “Include” and the SSM source IP list with an entry “ANY” will not produce meaningful results and is not accepted internally as a configuration. Otherwise all source IP addresses would be rejected.

Exclude

An MLD membership report is sent with the record type “Change to Exclude Mode”. If the source list contains the entry “ANY” or “::”, i.e. all sources are allowed, then an MLD membership report will be sent with a join group for “any sources”. If the list contains an entry other than “::”, an MLD membership report “block sources” is sent with the corresponding IP address.

ⓘ If you want to use an SSM group with any source address, you have to link the mode “Exclude” and SSM source IP list “ANY”.

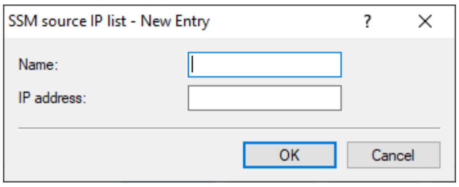
SSM source IP list

If SSM is to be operated, a list of desired sources can be specified here in addition to the multicast group. If all sources are to be allowed, the predefined list “ANY” can be used with the entry “::”.

7.4.5 SSM source IP list

This table can be used to specify lists of desired or unwanted (unicast) source IPv6 addresses. These can be referenced in various places and managed globally using this table. A list is defined by several entries with the same name.

In LANconfig you configure SSM source IP list under **Multicast** > **IGMP / MLD** > **Multicast Listener Discovery (MLD)** via **SSM source IP list**.



Name

Enter a name for the entry. A list is defined by several entries with the same name.

IP address

Unicast source IPv6 address. Multicast addresses are not a valid entry at this point, since the source IPv6 addresses of a multicast entry (S, G) are defined here.

7.5 PIM (Protocol Independent Multicast)

PIM (*RFC 7761*) enables the dynamic routing of multicast packets. Here, PIM uses routing information supplied by the unicast routing protocol operated in the router, although it does this independently of the routing protocols (e.g. RIP, OSPF or BGP).

For a PIM scenario based exclusively on LANCOM routers, only the PIM SSM (Source Specific Multicast) mode is fully supported. Operating the PIM Sparse Mode requires routers or components from third-party manufacturers. The advantage of PIM SSM is that its simpler architecture scales much better, making it ideally suited for modern multicast applications such as IPTV. PIM SSM requires IGMPv3 or MLDv2 (for IPv6) on the client side and does not need an additional rendezvous point (RP), since clients directly request not only the multicast source (S) but the desired multicast group (G) as well.

Basically, PIM SSM distinguishes between two router roles: First-hop router and last-hop router. A first-hop router is directly connected to multicast IGMP or MLD clients/receivers. A last-hop router is connected directly to the multicast source. There are also other routers located between the other two router roles. PIM must always be activated on all interfaces required to perform multicast routing. IGMP or MLD must be activated on client interfaces.

The following PIM functions are supported by the LCOS:

- PIM Sparse Mode (ASM) with external RP from a third-party manufacturer
- Static configuration of the RP in PIM Sparse Mode
- PIM SSM in the roles of last-hop router and first-hop router
- Supports IPv4 and IPv6 PIM
- SSM mapping, where PIM SSM joins are generated from IGMPv2 or MLD messages
- PIM native over IPSec VPN without GRE tunnel

The following PIM functions are not supported:

- The rendezvous point (RP) role
- Role as first-hop router for PIM Sparse, creating an automatic Register Unicast Tunnel to register a multicast source with the RP
- Dense mode, Bi-Dir mode
- Dynamic RP configuration, e.g. via Bootstrap Router (BSR) function

PIM show commands

The following show commands are available for PIM:

- PIM IPv4-Groups: Shows information about joined IPv4 multicast groups
- PIM IPv6-Groups: Shows information about joined IPv6 multicast groups
- PIM IPv4-Hello: Shows extended information about PIM neighbors and the PIM Hello-State on IPv4 interfaces
- PIM IPv6-Hello: Shows extended information about PIM neighbors and the PIM Hello-State on IPv6 interfaces
- PIM IPv4-Neighbors: Shows a short overview of PIM neighbors on IPv4 interfaces. Optionally, you can use the parameter `[-s] [--skip-own-info]` to omit the output of your own interface.
- PIM IPv6-Neighbors: Shows a short overview of PIM neighbors on IPv6 interfaces. Optionally, you can use the parameter `[-s] [--skip-own-info]` to omit the output of your own interface.

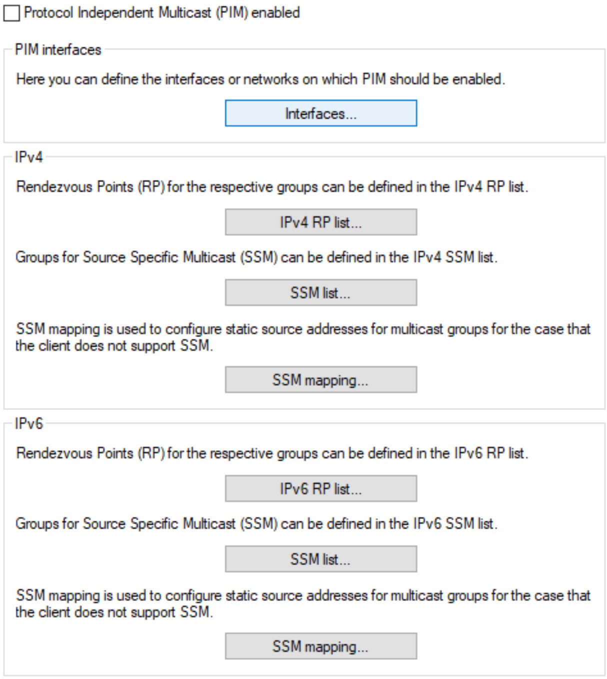
Example of the necessary configuration steps

The following configuration steps are necessary for a simple scenario with PIM SSM:

1. Activate PIM globally
2. An entry is required in the PIM interface table for every interface involved in multicast routing, including client interfaces and the source interface. You can use the default values.
3. To enable SSM, an entry must be made in the IPv4 or IPv6 SSM table. You can use the default values.

Configuration

In order to configure PIM with LANconfig, navigate to the **Multicast** > **PIM** menu.



☐ Protocol Independent Multicast (PIM) enabled

PIM interfaces

Here you can define the interfaces or networks on which PIM should be enabled.

IPv4

Rendezvous Points (RP) for the respective groups can be defined in the IPv4 RP list.

Groups for Source Specific Multicast (SSM) can be defined in the IPv4 SSM list.

SSM mapping is used to configure static source addresses for multicast groups for the case that the client does not support SSM.

IPv6

Rendezvous Points (RP) for the respective groups can be defined in the IPv6 RP list.

Groups for Source Specific Multicast (SSM) can be defined in the IPv6 SSM list.

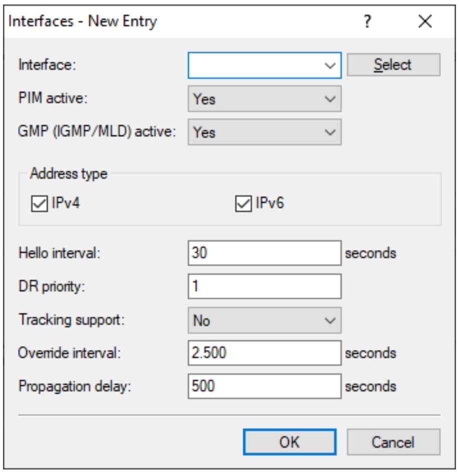
SSM mapping is used to configure static source addresses for multicast groups for the case that the client does not support SSM.

Protocol Independent Multicast (PIM) enabled

Enables or disables PIM on the device.

7.5.1 Interfaces

In LANconfig you configure the interfaces under **Multicast** > **PIM** > **PIM interfaces** using **Interfaces**. This table specifies the interfaces and logical networks where PIM is to be enabled. It also specifies the interfaces where clients can join multicast groups by means of IGMP or MLD. An entry is required in the PIM interface table for every interface involved in multicast routing, including client interfaces and the source interface.



Interfaces - New Entry

Interface:

PIM active: Yes

GMP (IGMP/MLD) active: Yes

Address type

☑ IPv4 ☑ IPv6

Hello interval: 30 seconds

DR priority: 1

Tracking support: No

Override interval: 2.500 seconds

Propagation delay: 500 seconds

Interface

Name of the logical interface on which PIM or a GMP (group management protocol such as IGMP or MLD) is to be activated. Possible values are IPv4 networks, e.g. INTRANET, WAN remote sites, wildcard entries with * for IPv4 RAS interfaces, for example “VPN*”. Other possible values are IPv6 interfaces and IPv6 RAS templates.

PIM active

Enables PIM as well as sending and receiving PIM messages on this logical interface. If this interface is only used by IGMP/MLD clients or multicast recipients, sending and receiving PIM messages can be explicitly disabled. In this case, only GMP (IGMP/MLD) has to be activated.

GMP (IGMP/MLD) active

Enables the IGMP or MLD router role on this logical interface. In this case, IGMP or MLD joins from clients are accepted. GMP can be disabled on interfaces where the network contains no clients but only PIM neighbor routers. IGMP/MLD joins will not be accepted in this case.

Address type

Here you specify the address family for which PIM or GMP should be enabled on this interface. If necessary, you can also activate both types of address at the same time. Possible values: IPv4, IPv6

Hello interval

Sets the time in seconds between the repetition of regular PIM Hello messages. The hold time is automatically 3.5 times the PIM Hello interval and cannot be configured separately.

Possible values: 0-255 seconds, default: 30. The value 0 disables the sending of Hello messages.

DR priority

Specifies the priority as designated router (DR) in the DR election process in PIM. A higher value means a higher priority in the DR election.

Possible values: 0 bis 2^{32}, default: 1.

Tracking support

Affects the “T bit” setting in the LAN Prune Delay option in outgoing Hello messages.

Possible values: Yes, No, default: No.

Override interval

Affects the setting of the override interval field in the LAN Prune Delay option in outgoing Hello messages. Specifies the maximum delay for transmitting Override Join messages for multicast networks that have Join-Suppression enabled.

Possible values: 0 bis 2^{32}, default: 0.

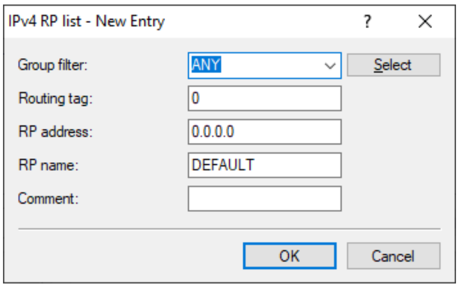
Propagation delay

Configures the setting of the Propagation Delay field in Hello messages sent for the LAN Prune Delay option. Specifies the delay for implementing a PIM prune message on the upstream routing device on a multicast network for which join suppression has been enabled.

Possible values: 250-2000 milliseconds, default: 500.

7.5.2 IPv4 RP list

In LANconfig you configure the IPv4 RP list under **Multicast** > **PIM** > **IPv4** using **IPv4 RP list**. In this table, the IPv4 rendezvous points (RPs) and their associated multicast groups are configured for PIM sparse mode.



IPv4 RP list - New Entry

Group filter: ANY

Routing tag: 0

RP address: 0.0.0.0

RP name: DEFAULT

Comment:

Group filter

Specifies the multicast groups for which the rendezvous points should be responsible. Addresses that match the group filter are managed by this rendezvous point. References a filter list from the table **Multicast** > **General** > **IPv4 filter lists**.

Routing tag

The routing tag used to reach this rendezvous point.

RP address

IPv4 address of the external rendezvous point. The device itself does not support the role of a rendezvous point.

RP name

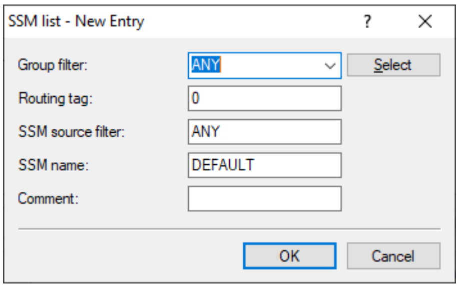
Name of the rendezvous point.

Comment

Optionally enter a meaningful comment as a description.

7.5.3 IPv4 SSM list

In LANconfig you configure the IPv4 SSM list under **Multicast** > **PIM** > **IPv4** using **SSM list**. This table configures the parameters for PIM SSM (Source Specific Multicast) mode.



SSM list - New Entry

Group filter: ANY
Routing tag: 0
SSM source filter: ANY
SSM name: DEFAULT
Comment:

Group filter

Specifies the multicast groups to which this SSM configuration applies. Addresses that match the group filter will be applied to this SSM configuration. References a filter list from the table **Multicast** > **General** > **IPv4 filter lists**.

Routing tag

Routing tag to which this configuration applies.

SSM source filter

Specifies the SSM source filter for this table entry. Multicast source addresses that match the SSM source filter will be applied to this SSM configuration. References a filter list from the table **Multicast** > **IGMP/MLD** > **Internet Group Management Protocol (IGMP)** > **SSM source IP list**.

SSM name

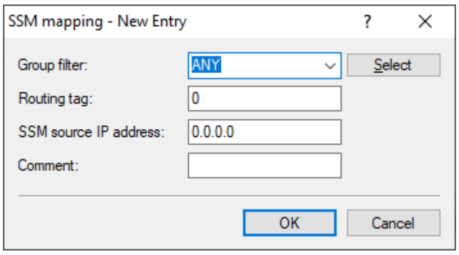
Name of this SSM configuration.

Comment

Optionally enter a meaningful comment as a description.

7.5.4 IPv4 SSM mapping

In LANconfig you configure the IPv4 SSM mapping under **Multicast** > **PIM** > **IPv4** using **SSM mapping**. In this table, IPv4 multicast source addresses (S) can be configured to be automatically inserted into PIM join messages if there are no source addresses (S) in received IGMP messages. As a result, the router automatically supplements (*,G) entries to be (S,G) entries.



SSM mapping - New Entry

Group filter: ANY
Routing tag: 0
SSM source IP address: 0.0.0.0
Comment:

Group filter

SSM mapping is performed for the multicast groups (G) specified here. References a filter list from the table **Multicast** > **General** > **IPv4 filter lists**.

Routing tag

Routing tag to which this configuration applies.

SSM source IP address

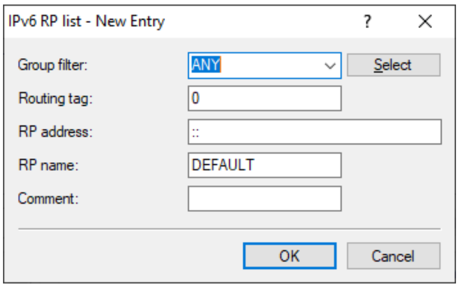
Specifies a source IPv4 address (S) that is automatically inserted into the (*,G) entries of PIM join messages to produce (S,G) entries.

Comment

Optionally enter a meaningful comment as a description.

7.5.5 IPv6 RP list

In LANconfig you configure the IPv6 RP list under **Multicast** > **PIM** > **IPv6** using **IPv6 RP list**. In this table, the rendezvous points (RPs) and their associated multicast groups are configured for PIM sparse mode.



IPv6 RP list - New Entry

Group filter:	ANY
Routing tag:	0
RP address:	::
RP name:	DEFAULT
Comment:	

Group filter

Specifies the multicast groups for which the rendezvous points should be responsible. Addresses that match the group filter are managed by this rendezvous point. References a filter list from the table **Multicast** > **General** > **IPv6 filter lists**.

Routing tag

The routing tag used to reach this rendezvous point.

RP address

IPv6 address of the external rendezvous point. The device itself does not support the role of a rendezvous point.

RP name

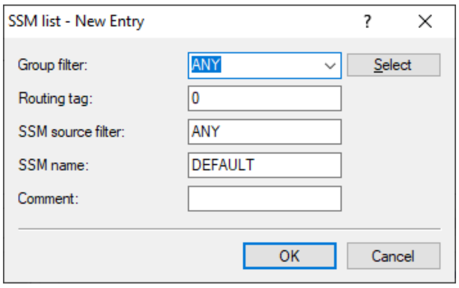
Name of the rendezvous point.

Comment

Optionally enter a meaningful comment as a description.

7.5.6 IPv6 SSM list

In LANconfig you configure the IPv6 SSM list under **Multicast** > **PIM** > **IPv6** using **SSM list**. This table configures the parameters for PIM IPv6 SSM (Source Specific Multicast) mode.



SSM list - New Entry

Group filter:	ANY
Routing tag:	0
SSM source filter:	ANY
SSM name:	DEFAULT
Comment:	

Group filter

Specifies the multicast groups to which this SSM configuration applies. Addresses that match the group filter will be applied to this SSM configuration. References a filter list from the table **Multicast** > **General** > **IPv6 filter lists**.

Routing tag

Routing tag to which this configuration applies.

SSM source filter

Specifies the SSM source filter for this table entry. Multicast source addresses that match the SSM source filter will be applied to this SSM configuration. References a filter list from the table **Multicast** > **IGMP/MLD** > **Internet Group Management Protocol (IGMP)** > **SSM source IP list**.

SSM name

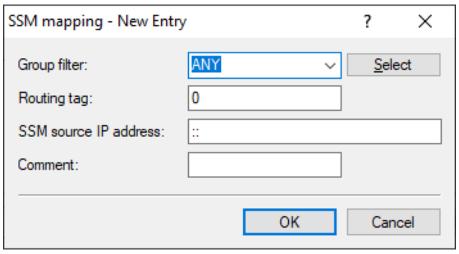
Name of this SSM configuration.

Comment

Optionally enter a meaningful comment as a description.

7.5.7 IPv6 SSM mapping

In LANconfig you configure the IPv6 SSM mapping under **Multicast** > **PIM** > **IPv6** using **SSM mapping**. In this table, IPv6 source addresses (S) can be configured to be automatically inserted into PIM join messages if there are no source addresses in received MLD messages. As a result, the router automatically supplements (*,G) entries to be (S,G) entries.


SSM mapping - New Entry

Group filter: ANY

Routing tag: 0

SSM source IP address: ::

Comment:

Group filter

SSM mapping is performed for the multicast groups (G) specified here. References a filter list from the table **Multicast** > **General** > **IPv6 filter lists**.

Routing tag

Routing tag to which this configuration applies.

SSM source IP address

Specifies a source IPv6 address (S) that is automatically inserted into the (*,G) entries of PIM join messages to produce (S,G) entries.

Comment

Optionally enter a meaningful comment as a description.

7.6 Additions to the Setup menu

7.6.1 Multicast

This item contains the settings for multicast protocols.

SNMP ID:

2.108

Console path:

Setup

IGMP

This item contains the settings for the Internet Group Management Protocol (IGMP).

SNMP ID:

2.108.1

Console path:

Setup > **Multicast**

IGMP-Proxy

An IGMP proxy is typically used for Internet connections with multicast IPTV. Clients or IPTV set top boxes (STBs) on the local network send IGMP messages to receive a specific TV channel. To this end, they join certain multicast groups and later leave them again. The router and/or IGMP proxy receives the IGMP messages and forwards them to the provider network and filters the groups, if required. The IGMP proxy works for the local network with its clients.

An IGMP proxy can also be used in simple multicast routing scenarios, for example via VPN, without having to use PIM. The configuration of the IGMP proxy creates a static (tree) structure without alternative paths, redundancy or loop prevention. IGMP proxies can be “cascaded” by connecting multiple routers in series.

SNMP ID:

2.108.1.1

Console path:

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

Downstream-Interface

Interface name used by IGMP clients to join groups and receive IGMP messages from the proxy. Possible values are IPv4 networks, e.g. INTRANET, IPv4 (WAN) remotes. Also allowed are wildcard entries with * for RAS interfaces, e.g. “VPN*”.

SNMP ID:

2.108.1.1.1

Console path:

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

Possible values:

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

Upstream-Interface

Interface name used by the IGMP proxy to send messages on behalf of clients. The source of the multicast messages must be reached via this interface. Possible values are IPv4 networks, e.g. INTRANET and IPv4 (WAN) remotes.

SNMP ID:

2.108.1.1.2

Console path:

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

Possible values:

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

Group-Filter

Name of the group filter that is to apply to this proxy. References the table *IPv4 filter table*. By default, the filter entry is blank or points to the filter list “ANY”, which allows all multicast groups. The group filter can be used to restrict the multicast groups available for clients.

SNMP ID:

2.108.1.1.3

Console path:

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

Possible values:

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

SSM-Ranges

Specifies the IP address range in prefix notation used for SSM.

SNMP ID:

2.108.1.3

Console path:

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

Prefix

These prefixes define the IPv4 address range used for SSM.

SNMP ID:

2.108.1.3.1

Console path:

Setup > **Multicast** > **IGMP** > **SSM-Ranges**

Possible values:

Max. 18 characters from `[0-9]./`

SSM-Source-IP-List

This table can be used to specify lists of desired or unwanted (unicast) source IP addresses. These can be referenced in various places and managed globally using this table. A list is defined by several entries with the same name.

SNMP ID:

2.108.1.4

Console path:

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

Name

Enter a name for the entry. A list is defined by several entries with the same name.

SNMP ID:

2.108.1.4.1

Console path:

Setup > **Multicast** > **IGMP** > **SSM-Source-IP-List**

Possible values:

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

IP-Address

Unicast source IP address. Multicast addresses are not a valid entry at this point, since the source IP addresses of a multicast entry (S, G) are defined here.

SNMP ID:

2.108.1.4.2

Console path:

Setup > **Multicast** > **IGMP** > **SSM-Source-IP-List**

Possible values:

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

Static-Routes

Static multicast routing can be used where multicast clients do not support IGMP and in scenarios where multicast traffic has to keep flowing even if the clients do not request to join the corresponding group. When the entry is created, the router creates IGMP joins and group reports on the upstream interface.

Please note that static multicast routing can cause high traffic and load because the multicast data is forwarded at all times.

SNMP ID:

2.108.1.5

Console path:

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

Upstream-Interface

Interface name where the multicast packets reach the router. Possible values are IPv4 networks, e.g. INTRANET and IPv4 (WAN) remotes.

SNMP ID:

2.108.1.5.1

Console path:

Setup > **Multicast** > **IGMP** > **Static-Routes**

Possible values:

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

Group

The static forwarding of multicast data is to be configured for this multicast group, e.g. 239.0.0.1.

SNMP ID:

2.108.1.5.2

Console path:

Setup > **Multicast** > **IGMP** > **Static-Routes**

Possible values:

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

Downstream-Interface

Interface name where the multicast packets exit the router. Possible values are IPv4 networks, e.g. INTRANET and IPv4 (WAN) remotes.

SNMP ID:

2.108.1.5.3

Console path:

Setup > **Multicast** > **IGMP** > **Static-Routes**

Possible values:

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

Mode

If SSM is to be operated: This controls the way in which an IGMP membership report requests the source addresses of multicast sources.

> ⓘ If you want to use an SSM group with any source address, you have to link the mode “Exclude” and SSM source IP list “ANY”.

SNMP ID:

2.108.1.5.4

Console path:

Setup > **Multicast** > **IGMP** > **Static-Routes**

Possible values:

Include

An IGMP membership report is sent with the record type “Change to Include Mode”. The entries from the SSM source IP list are sent as the desired source addresses. A combination of the setting “Include” and the SSM source IP list with an entry “ANY” will not produce meaningful results and is not accepted internally as a configuration. Otherwise all source IP addresses would be rejected.

Exclude

An IGMP membership report is sent with the record type “Change to Exclude Mode”. If the source list contains the entry “ANY” or “0.0.0.0”, i.e. all sources are allowed, then an IGMP membership report will be sent with a join group for “any sources”. If the list contains an entry other than 0.0.0.0, an IGMP membership report “block sources” is sent with the corresponding IP address.

SSM-Source-IP-List

If SSM is to be operated, a list of desired sources can be specified here in addition to the multicast group. If all sources are to be allowed, the predefined list “ANY” can be used with the entry “0.0.0.0”.

SNMP ID:

2.108.1.5.5

Console path:

Setup > **Multicast** > **IGMP** > **Static-Routes**

Possible values:

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

Parameter

The settings for the general IGMP parameters are located here.

SNMP ID:

2.108.1.6

Console path:

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

Interface

Name of the interface that the IGMP configuration applies to. The entry named DEFAULT applies to all interfaces without a specific entry. If there is no DEFAULT entry, the internal default values for a DEFAULT entry still apply. Possible values are DEFAULT, IPv4 networks, e.g. INTRANET or IPv4 (WAN) remotes. Also allowed are wildcard entries with * for RAS interfaces, e.g. “VPN*”.

SNMP ID:

2.108.1.6.1

Console path:

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

Possible values:

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

Robustness-Variable

Number of IGMP message repeats.

SNMP ID:

2.108.1.6.2

Console path:

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

Possible values:

1 … 10

Default:

2

Unsolicited-Report-Interval

Specifies the time in seconds between repetitions of a host's initial report of membership in a group.

SNMP ID:

2.108.1.6.3

Console path:

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

Possible values:

1 … 25

Default:

2

Query-Interval

Interval between IGMP general queries.

SNMP ID:

2.108.1.6.4

Console path:

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

Possible values:

2 … 99999

Default:

125

Query-Response-Interval

Maximum response time in milliseconds. The maximum response time is inserted into periodic general queries. The value for the query response interval must be less than the value for query interval.

SNMP ID:

2.108.1.6.5

Console path:

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

Possible values:

1 … 999999

Default:

10000

Startup-Query-Interval

The interval in seconds between IGMP general queries sent after the querier starts up.

SNMP ID:

2.108.1.6.6

Console path:

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

Possible values:

1 … 99998

Default:

30

Startup-Query-Count

Number of IGMP general queries sent on startup, separated by the startup query interval.

SNMP ID:

2.108.1.6.7

Console path:

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

Possible values:

1 … 10

Default:

2

Last-Listener-Query-Interval

Specifies the value in seconds of the Maximum Response Time in Multicast Address-Specific Queries that are sent in response to Done messages. The parameter also specifies the time between multicast address-specific queries.

SNMP ID:

2.108.1.6.8

Console path:

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

Possible values:

1 … 25

Default:

2

Last-Listener-Query-Count

Number of multicast address-specific queries sent before the router assumes that there are no more local listeners. It also specifies the number of multicast address-specific queries sent before the router assumes there are no more listeners of a particular source.

SNMP ID:

2.108.1.6.9

Console path:

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

Possible values:

1 … 10

Default:

2

IGMP-Compatibility-Mode

IGMP version used by the device when operating as a multicast router.

SNMP ID:

2.108.1.6.10

Console path:

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

Possible values:

Off
V1
V2
V3

Default:

V3

Quick-Leave

Enables receivers to leave multicast groups quickly. This should only be used if there is only one receiver per group on the interface. Internally, the Last Listener Query Count parameter is set to 1 and the Last Listener Query Interval is set to 20 ms.

SNMP ID:

2.108.1.6.11

Console path:

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

Possible values:

No
Yes

Default:

No

Check-Router-Alert

Defines whether received IGMP messages are checked for the Router Alert option. According to RFC, IGMP packets that do not contain the Router Alert option should be discarded. This is designed to ensure compatibility in case of faulty client implementations.

SNMP ID:

2.108.1.7

Console path:

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

Possible values:

No
Yes

Default:

Yes

Collect-Statistics

Defines whether IPv4 multicast statistics should be collected. Collecting these statistics may affect device performance.

SNMP ID:

2.108.1.8

Console path:

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

Possible values:

No
Yes

Default:

No

Static-Join

This table is used to define IPv4 multicast groups that the device can join through IGMP in order to test client interfaces. This allows the simulation of multicast clients joining certain IGMP groups. The corresponding client interface must be part of the IGMP proxy or PIM configuration. The device then processes and discards inbound multicast traffic. This feature is not suitable for permanent operation in productive scenarios.

SNMP ID:

2.108.1.9

Console path:

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

Interface

(Client) interface name used to simulate the multicast client.

SNMP ID:

2.108.1.9.1

Console path:

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

Possible values:

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

Group

IPv4 multicast group that the device joins statically.

SNMP ID:

2.108.1.9.2

Console path:

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

Possible values:

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

Comment

Optionally enter a meaningful comment as a description.

SNMP ID:

2.108.1.9.3

Console path:

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

Possible values:

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

MLD

This item contains the settings for the Multicast Listener Discovery (MLD).

SNMP ID:

2.108.2

Console path:

Setup > **Multicast**

MLD-Proxy

An MLD proxy is typically used for multicast IPTV on IPv6 Internet connections. Clients or IPTV set top boxes (STBs) on the local network send MLD messages to receive a specific TV channel. To this end, they join certain multicast groups and later leave them again. The router and/or MLD proxy receives the MLD messages and forwards them to the provider network and filters the groups, if required. The MLD proxy works for the local network with its clients.

An MLD proxy can also be used in simple multicast routing scenarios, for example via VPN, without having to use PIM. The configuration of the MLD proxy creates a static (tree) structure without alternative paths, redundancy or loop prevention. MLD proxies can be "cascaded" by connecting multiple routers in series.

SNMP ID:

2.108.2.1

Console path:

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

Downstream-Interface

Interface name used by MLD clients to join groups and receive MLD messages from the proxy. Possible values are IPv6 networks, e.g. INTRANET, IPv6 (WAN) remotes or RAS templates.

SNMP ID:

2.108.2.1.1

Console path:

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

Possible values:

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

Upstream-Interface

Interface name used by the MLD proxy to send messages on behalf of clients. The source of the multicast messages must be reached via this interface. Possible values are IPv6 networks, e.g. INTRANET and IPv6 (WAN) remotes.

SNMP ID:

2.108.2.1.2

Console path:

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

Possible values:

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

Group-Filter

Name of the group filter that is to apply to this proxy. References the table *IPv6 filter table*. By default, the filter entry is blank or points to the filter list "ANY", which allows all multicast groups. The group filter can be used to restrict the multicast groups available for clients.

SNMP ID:

2.108.2.1.3

Console path:

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

Possible values:

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

SSM-Ranges

Specifies the IP address range in prefix notation used for SSM.

SNMP ID:

2.108.2.3

Console path:

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

Prefix

These prefixes define the IP address range used for SSM.

SNMP ID:

2.108.2.3.1

Console path:

Setup > **Multicast** > **MLD** > **SSM-Ranges**

Possible values:

Max. 43 characters from `[A-F][a-f][0-9]:./`

SSM-Source-IP-List

This table can be used to specify lists of desired or unwanted (unicast) source IP addresses. These can be referenced in various places and managed globally using this table. A list is defined by several entries with the same name.

SNMP ID:

2.108.2.4

Console path:

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

Name

Enter a name for the entry. A list is defined by several entries with the same name.

SNMP ID:

2.108.2.4.1

Console path:

Setup > **Multicast** > **MLD** > **SSM-Source-IP-List**

Possible values:

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

IP-Address

Unicast source IP address. Multicast addresses are not a valid entry at this point, since the source IP addresses of a multicast entry (S, G) are defined here.

SNMP ID:

2.108.2.4.2

Console path:

Setup > **Multicast** > **MLD** > **SSM-Source-IP-List**

Possible values:

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

Static-Routes

Static multicast routing can be used where multicast clients do not support MLD and in scenarios where multicast traffic has to keep flowing even if the clients do not request to join the corresponding group. When the entry is created, the router creates MLD group reports on the upstream interface.

Please note that static multicast routing can cause high traffic and load because the multicast data is forwarded at all times.

SNMP ID:

2.108.2.5

Console path:

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

Upstream-Interface

Interface name where the multicast packets reach the router. Possible values are IPv6 networks, e.g. INTRANET and IPv6 (WAN) remotes.

SNMP ID:

2.108.2.5.1

Console path:

Setup > **Multicast** > **MLD** > **Static-Routes**

Possible values:

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

Group

The static forwarding of multicast data is to be configured for this multicast group, e.g. “ff09::1”.

SNMP ID:

2.108.2.5.2

Console path:

Setup > **Multicast** > **MLD** > **Static-Routes**

Possible values:

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

Downstream-Interface

Interface name where the multicast packets exit the router. Possible values are IPv6 networks, e.g. INTRANET and IPv6 (WAN) remotes.

SNMP ID:

2.108.2.5.3

Console path:

Setup > **Multicast** > **MLD** > **Static-Routes**

Possible values:

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

Mode

If SSM is to be operated: This controls the way in which an MLD membership report requests the source addresses of multicast sources.

If you want to use an SSM group with any source address, you have to link the mode "Exclude" and SSM source IP list "ANY".

SNMP ID:

2.108.2.5.4

Console path:

Setup > **Multicast** > **MLD** > **Static-Routes**

Possible values:

Include

An MLD membership report is sent with the record type "Change to Include Mode". The entries from the SSM source IP list are sent as the desired source addresses. A combination of the setting "Include" and the SSM source IP list with an entry "ANY" will not produce meaningful results and is not accepted internally as a configuration. Otherwise all source IP addresses would be rejected.

Exclude

An MLD membership report is sent with the record type "Change to Exclude Mode". If the source list contains the entry "ANY" or "0.0.0.0", i.e. all sources are allowed, then an MLD membership report will be sent with a join group for "any sources". If the list contains an entry other than 0.0.0.0, an MLD membership report "block sources" is sent with the corresponding IP address.

SSM-Source-IP-List

If SSM is to be operated, a list of desired sources can be specified here in addition to the multicast group. If all sources are to be allowed, the predefined list "ANY" can be used with the entry "0.0.0.0".

SNMP ID:

2.108.2.5.5

Console path:

Setup > **Multicast** > **MLD** > **Static-Routes**

Possible values:

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

Parameter

The settings for the general MLD parameters are located here.

SNMP ID:

2.108.2.6

Console path:

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

Interface

Name of the interface that the MLD configuration applies to. The entry named DEFAULT applies to all interfaces without a specific entry. If there is no DEFAULT entry, the internal default values for a DEFAULT entry still apply. Possible values are DEFAULT, IPv6 networks, e.g. INTRANET, IPv6 (WAN) remotes or IPv6 RAS templates.

SNMP ID:

2.108.2.6.1

Console path:

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

Possible values:

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

Robustness variable

Number of MLD message repeats.

SNMP ID:

2.108.2.6.2

Console path:

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

Possible values:

1 … 10

Default:

2

Unsolicited-Report-Interval

Specifies the time in seconds between repetitions of a host's initial report of membership in a group.

SNMP ID:

2.108.2.6.3

Console path:

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

Possible values:

1 … 25

Default:

2

Query-Interval

Interval in seconds between MLD general queries.

SNMP ID:

2.108.2.6.4

Console path:

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

Possible values:

2 … 99999

Default:

125

Query-Response-Interval

The maximum response time is inserted into periodic MLD general queries. The value for the query response interval must be less than the value for query interval.

SNMP ID:

2.108.2.6.5

Console path:

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

Possible values:

1 … 999999

Default:

10000

Startup-Query-Interval

The interval in seconds between MLD general queries sent after the MLD querier starts up.

SNMP ID:

2.108.2.6.6

Console path:

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

Possible values:

1 … 99998

Default:

30

Startup-Query-Count

Number of MLD general messages on startup, separated by the startup query interval.

SNMP ID:

2.108.2.6.7

Console path:

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

Possible values:

1 … 10

Default:

2

Last-Listener-Query-Interval

Specifies the value in seconds of the Maximum Response Code (with IPv6) in Multicast Address-Specific Queries that are sent in response to Done messages. The parameter also specifies the time between multicast address-specific queries.

SNMP ID:

2.108.2.6.8

Console path:

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

Possible values:

1 … 25

Default:

2

Last-Listener-Query-Count

Number of multicast address-specific queries sent before the router assumes that there are no more local listeners. It also specifies the number of multicast address-specific queries sent before the router assumes there are no more listeners of a particular source.

SNMP ID:

2.108.2.6.9

Console path:

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

Possible values:

1 … 10

Default:

2

MLD-Compatibility-Mode

MLD version used by the device when operating as a multicast router.

SNMP ID:

2.108.2.6.10

Console path:

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

Possible values:

Off
V1
V2

Default:

V2

Quick-Leave

Enables receivers to leave multicast groups quickly. This should only be used if there is only one receiver per group on the interface. Internally, the Last Listener Query Count parameter is set to 1 and the Last Listener Query Interval is set to 20 ms.

SNMP ID:

2.108.2.6.11

Console path:

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

Possible values:

No
Yes

Default:

No

Collect-Statistics

Defines whether IPv6 multicast statistics should be collected. Collecting these statistics may affect device performance.

SNMP ID:

2.108.2.8

Console path:

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

Possible values:

No
Yes

Default:

No

Static-Join

This table is used to IPv6 multicast groups that the device can join through MLD for in order to test client interfaces. This allows the simulation of multicast clients joining certain MLD groups. The corresponding client interface must be part of the IGMP proxy or PIM configuration. The device then processes and discards inbound multicast traffic. This feature is not suitable for permanent operation in productive scenarios.

SNMP ID:

2.108.2.9

Console path:

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

Interface

(Client) interface name used to simulate the multicast client.

SNMP ID:

2.108.2.9.1

Console path:

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

Possible values:

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

Group

IPv6 multicast group that the device joins statically.

SNMP ID:

2.108.2.9.2

Console path:

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

Possible values:

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

Comment

Optionally enter a meaningful comment as a description.

SNMP ID:

2.108.2.9.3

Console path:

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

Possible values:

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

Enable-Lancom-Group

Specifies whether the device should respond to the multicast address ff02::139. This multicast group is used by the LANtools to find LANCOM devices.

SNMP ID:

2.108.2.127

Console path:

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

Possible values:

No
Yes

Default:

Yes

PIM

This item contains the settings for PIM (Protocol Independent Multicast).

SNMP ID:

2.108.4

Console path:

Setup > **Multicast**

IPv4

This item contains the settings for PIM (Protocol Independent Multicast) with IPv4.

SNMP ID:

2.108.4.1

Console path:

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

RP-List

In this table, the rendezvous points (RPs) and their associated multicast groups are configured for PIM sparse mode.

SNMP ID:

2.108.4.1.1

Console path:

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

Group-Filter

Specifies the multicast groups for which the rendezvous points should be responsible. Addresses that match the group filter are managed by this rendezvous point. References a filter list from the *2.108.5 IPv4-Filter-Table* on page 121 table.

SNMP ID:

2.108.4.1.1.1

Console path:

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

Possible values:

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

Rtg-Tag

The routing tag used to reach this rendezvous point.

SNMP ID:

2.108.4.1.1.2

Console path:

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

Possible values:

0 … 65535

Default:

0

RP-Address

IPv4 address of the external rendezvous point. The device itself does not support the role of a rendezvous point.

SNMP ID:

2.108.4.1.1.3

Console path:

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

Possible values:

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

RP-Name

Name of the rendezvous point.

SNMP ID:

2.108.4.1.1.5

Console path:

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

Possible values:

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

Comment

Optionally enter a meaningful comment as a description.

SNMP ID:

2.108.4.1.1.6

Console path:

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

Possible values:

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

SSM-List

This table configures the parameters for PIM SSM (Source Specific Multicast) mode.

SNMP ID:

2.108.4.1.2

Console path:

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

Group-Filter

Specifies the multicast groups to which this SSM configuration applies. Addresses that match the group filter will be applied to this SSM configuration. References a filter list from the *2.108.5 IPv4-Filter-Table* on page 121 table.

SNMP ID:

2.108.4.1.2.1

Console path:

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

Possible values:

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

Rtg-Tag

Routing tag to which this configuration applies.

SNMP ID:

2.108.4.1.2.2

Console path:

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

Possible values:

0 … 65535

Default:

0

SSM-Source-Filter

Specifies the SSM source filter for this table entry. Multicast source addresses that match the SSM source filter will be applied to this SSM configuration. References a filter list from the *2.108.1.4 SSM-Source-IP-List* on page 86 table.

SNMP ID:

2.108.4.1.2.3

Console path:

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

Possible values:

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

SSM-Name

Name of this SSM configuration.

SNMP ID:

2.108.4.1.2.5

Console path:

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

Possible values:

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

Comment

Optionally enter a meaningful comment as a description.

SNMP ID:

2.108.4.1.2.6

Console path:

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

Possible values:

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

SSM-Mapping

In this table, IPv4 multicast source addresses (S) can be configured to be automatically inserted into PIM join messages if there are no source addresses (S) in received IGMP messages. As a result, the router automatically supplements (*,G) entries to be (S,G) entries.

SNMP ID:

2.108.4.1.3

Console path:

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

Group-Filter

SSM mapping is performed for the multicast groups (G) specified here. References a filter list from the *2.108.5 IPv4-Filter-Table* on page 121 table.

SNMP ID:

2.108.4.1.3.1

Console path:

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

Possible values:

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

Rtg-Tag

Routing tag to which this configuration applies.

SNMP ID:

2.108.4.1.3.2

Console path:

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

Possible values:

0 … 65535

Default:

0

SSM-Source-IP

Specifies a source IPv4 address (S) that is automatically inserted into the (*,G) entries of PIM join messages to produce (S,G) entries.

SNMP ID:

2.108.4.1.3.3

Console path:

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

Possible values:

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

Comment

Optionally enter a meaningful comment as a description.

SNMP ID:

2.108.4.1.3.4

Console path:

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

Possible values:

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

IPv6

This item contains the settings for PIM (Protocol Independent Multicast) with IPv6.

SNMP ID:

2.108.4.2

Console path:

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

RP-List

In this table, the rendezvous points (RPs) and their associated multicast groups are configured for PIM sparse mode.

SNMP ID:

2.108.4.2.1

Console path:

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

Group-Filter

Specifies the multicast groups for which the rendezvous points should be responsible. Addresses that match the group filter are managed by this rendezvous point. References a filter list from the *2.108.6 IPv6-Filter-Table* on page 123 table.

SNMP ID:

2.108.4.2.1.1

Console path:

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

Possible values:

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

Rtg-Tag

The routing tag used to reach this rendezvous point.

SNMP ID:

2.108.4.2.1.2

Console path:

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

Possible values:

0 … 65535

Default:

0

RP-Address

IPv6 address of the external rendezvous point. The device itself does not support the role of a rendezvous point.

SNMP ID:

2.108.4.2.1.3

Console path:

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

Possible values:

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

RP-Name

Name of the rendezvous point.

SNMP ID:

2.108.4.2.1.5

Console path:

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

Possible values:

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

Comment

Optionally enter a meaningful comment as a description.

SNMP ID:

2.108.4.2.1.6

Console path:

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

Possible values:

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

SSM-List

This table configures the parameters for PIM IPv6 SSM (Source Specific Multicast) mode.

SNMP ID:

2.108.4.2.2

Console path:

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

Group-Filter

Specifies the multicast groups to which this SSM configuration applies. Addresses that match the group filter will be applied to this SSM configuration. References a filter list from the *2.108.6 IPv6-Filter-Table* on page 123 table.

SNMP ID:

2.108.4.2.2.1

Console path:

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

Possible values:

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

Rtg-Tag

Routing tag to which this configuration applies.

SNMP ID:

2.108.4.2.2.2

Console path:

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

Possible values:

0 … 65535

Default:

0

SSM-Source-Filter

Specifies the SSM source filter for this table entry. Multicast source addresses that match the SSM source filter will be applied to this SSM configuration. References a filter list from the *2.108.1.4 SSM-Source-IP-List* on page 86 table.

SNMP ID:

2.108.4.2.2.3

Console path:

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

Possible values:

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

SSM-Name

Name of this SSM configuration.

SNMP ID:

2.108.4.2.2.5

Console path:

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

Possible values:

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

Comment

Optionally enter a meaningful comment as a description.

SNMP ID:

2.108.4.2.2.6

Console path:

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

Possible values:

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

SSM-Mapping

In this table, IPv6 source addresses (S) can be configured to be automatically inserted into PIM join messages if there are no source addresses in received MLD messages. As a result, the router automatically supplements (*,G) entries to be (S,G) entries.

SNMP ID:

2.108.4.2.3

Console path:

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

Group-Filter

SSM mapping is performed for the multicast groups (G) specified here. References a filter list from the *2.108.6 IPv6-Filter-Table* on page 123 table.

SNMP ID:

2.108.4.2.3.1

Console path:

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

Possible values:

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

Rtg-Tag

Routing tag to which this configuration applies.

SNMP ID:

2.108.4.2.3.2

Console path:

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

Possible values:

0 … 65535

Default:

0

SSM-Source-IP

Specifies a source IPv6 address (S) that is automatically inserted into the (*,G) entries of PIM join messages to produce (S,G) entries.

SNMP ID:

2.108.4.2.3.3

Console path:

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

Possible values:

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

Comment

Optionally enter a meaningful comment as a description.

SNMP ID:

2.108.4.2.3.4

Console path:

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

Possible values:

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

Interfaces

This table specifies the interfaces and logical networks where PIM is to be enabled. It also specifies the interfaces where clients can join multicast groups by means of IGMP or MLD.

SNMP ID:

2.108.4.3

Console path:

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

Interface

Name of the logical interface on which PIM or a GMP (group management protocol such as IGMP or MLD) is to be activated. Possible values are IPv4 networks, e.g. INTRANET, WAN remote sites, wildcard entries with * for IPv4 RAS interfaces, for example “VPN*”. Other possible values are IPv6 interfaces and IPv6 RAS templates.

SNMP ID:

2.108.4.3.1

Console path:

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

Possible values:

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

PIM-Active

Enables PIM as well as sending and receiving PIM messages on this logical interface. If this interface is only used by IGMP/MLD clients or multicast recipients, sending and receiving PIM messages can be explicitly disabled. In this case, only GMP (IGMP/MLD) has to be activated.

SNMP ID:

2.108.4.3.2

Console path:

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

Possible values:

No

PIM is disabled.

Yes

PIM is enabled.

GMP-Active

Enables the IGMP or MLD router role on this logical interface. In this case, IGMP or MLD joins from clients are accepted. GMP can be disabled on interfaces where the network contains no clients but only PIM neighbor routers. IGMP/MLD joins will not be accepted in this case.

SNMP ID:

2.108.4.3.3

Console path:

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

Possible values:

No

IGMP or MLD router role is disabled.

Yes

IGMP or MLD router role is enabled.

Address-Type

Here you specify the address family for which PIM or GMP should be enabled on this interface.

SNMP ID:

2.108.4.3.4

Console path:

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

Possible values:

IPv4

IPv6

Hello-Interval

Sets the time in seconds between the repetition of regular PIM Hello messages. The hold time is automatically 3.5 times the PIM Hello interval and cannot be configured separately.

SNMP ID:

2.108.4.3.5

Console path:

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

Possible values:

0 … 255

Default:

30

Special values:

0

The value 0 disables the sending of Hello messages.

DR-Priority

Specifies the priority as designated router (DR) in the DR election process in PIM. A higher value means a higher priority in the DR election.

SNMP ID:

2.108.4.3.6

Console path:

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

Possible values:

0 … 4294967296

Default:

1

Tracking-Support

Affects the “T bit” setting in the LAN Prune Delay option in outgoing Hello messages.

SNMP ID:

2.108.4.3.7

Console path:

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

Possible values:

Yes
Off

Default:

Off

Override-Interval

Affects the setting of the override interval field in the LAN Prune Delay option in outgoing Hello messages. Specifies the maximum delay for transmitting Override Join messages for multicast networks that have Join-Suppression enabled.

SNMP ID:

2.108.4.3.8

Console path:

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

Possible values:

0 … 4294967296

Default:

0

Propagation-Delay

Configures the setting of the Propagation Delay field in Hello messages sent for the LAN Prune Delay option. Specifies the delay in milliseconds for implementing a PIM prune message on the upstream routing device on a multicast network for which join suppression has been enabled.

SNMP ID:

2.108.4.3.9

Console path:

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

Possible values:

250 … 2000

Default:

500

Operating

Enables or disables PIM on the device.

SNMP ID:

2.108.4.6

Console path:

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

Possible values:

No

PIM is disabled.

Yes

PIM is enabled.

Default:

No

IPv4-Filter-Table

This table can be used to specify lists of desired or unwanted IPv4 multicast addresses and prefixes.

These can be referenced in various places and managed globally using this table. A list is defined by several entries with the same name.

SNMP ID:

2.108.5

Console path:

Setup > **Multicast**

Name

Give this entry a name. A list is defined by several entries with the same name.

SNMP ID:

2.108.5.1

Console path:

Setup > **Multicast** > **IPv4-Filter-Table**

Possible values:

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

Prefix

Enter here the IPv4 address followed by the prefix length of the network (CIDR notation). This specifies how many most-significant bits (MSB) of the IP address are necessary for a match.

SNMP ID:

2.108.5.2

Console path:

Setup > **Multicast** > **IPv4-Filter-Table**

Possible values:

Max. 18 characters from `[0-9]./`

Action

Specify whether the prefixes in this filter entry should be allowed or denied.

SNMP ID:

2.108.5.3

Console path:

Setup > **Multicast** > **IPv4-Filter-Table**

Possible values:

Allow
Deny

Comment

Optionally enter a meaningful comment as a description.

SNMP ID:

2.108.5.4

Console path:

Setup > **Multicast** > **IPv4-Filter-Table**

Possible values:

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

IPv6-Filter-Table

This table can be used to specify lists of desired or unwanted IPv6 multicast addresses and prefixes.

These can be referenced in various places and managed globally using this table. A list is defined by several entries with the same name.

SNMP ID:

2.108.6

Console path:

Setup > **Multicast**

Name

Give this entry a name. A list is defined by several entries with the same name.

SNMP ID:

2.108.6.1

Console path:

Setup > **Multicast** > **IPv6-Filter-Table**

Possible values:

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

Prefix

Enter the IPv6 multicast address and prefix here.

SNMP ID:

2.108.6.2

Console path:

Setup > **Multicast** > **IPv6-Filter-Table**

Possible values:

Max. 43 characters from `[A-F][a-f][0-9]:./`

Action

Specify whether the prefixes in this filter entry should be allowed or denied.

SNMP ID:

2.108.6.3

Console path:

Setup > **Multicast** > **IPv6-Filter-Table**

Possible values:

Allow
Deny

Comment

Optionally enter a meaningful comment as a description.

SNMP ID:

2.108.6.4

Console path:

Setup > **Multicast** > **IPv6-Filter-Table**

Possible values:

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

8 Virtual Private Networks – VPN

8.1 High Scalability VPN (HSVPN)

In SD-WAN scenarios where branches connect to one or more central sites, there are usually several logical networks that need to be securely separated from one another (e.g. for payment transactions, inventory management, or a hotspot) by means of VLAN and ARF. These local networks were previously connected to the central site either as "stacked" tunnels, i.e. PPTP or L2TP within a VPN tunnel, or as individual IPsec VPN tunnels. However, these architectures do not scale well with large numbers of branches and ARF networks. For example, in an architecture with one tunnel per ARF network, 1,000 branches and 8 ARF networks results in a total of 8,000 tunnels. Stacked tunnels have performance and MTU restrictions due to the protocol overhead.

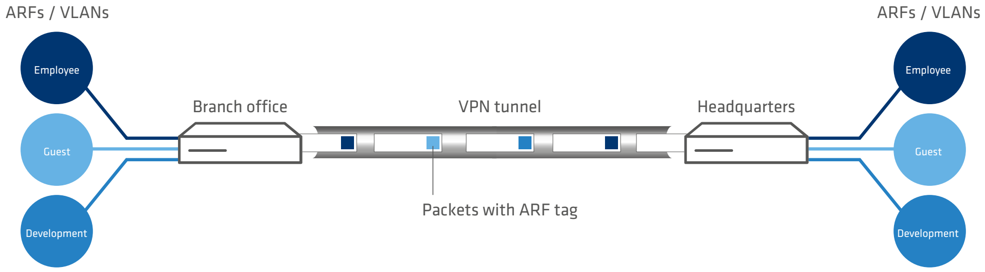


Figure 1: LANCOM HSVPN scenario for SD-WAN

The new architecture LANCOM HSVPN ("LANCOMHigh Scalability VPN") solves these challenges. With HSVPN, packets from ARF networks within an IPsec tunnel are marked with an ARF tag and transported in the VPN tunnel without overhead. This layer-3 based tagging method corresponds to the VLAN layer-2 approach and provides the same level of security. As fewer tunnels are required overall, tunnel establishment times are improved, especially in case of failover. Also, no major restrictions apply with regard to MTU.

The following configuration steps are necessary:

1. Creating the individual ARF networks
2. Creating an IKEv2 tunnel
3. The allowed ARF networks are configured as a tag list in the HSVPN configuration profile of the IKEv2 tunnel
4. For the desired ARF networks, corresponding routes must be created through the HSVPN tunnels.

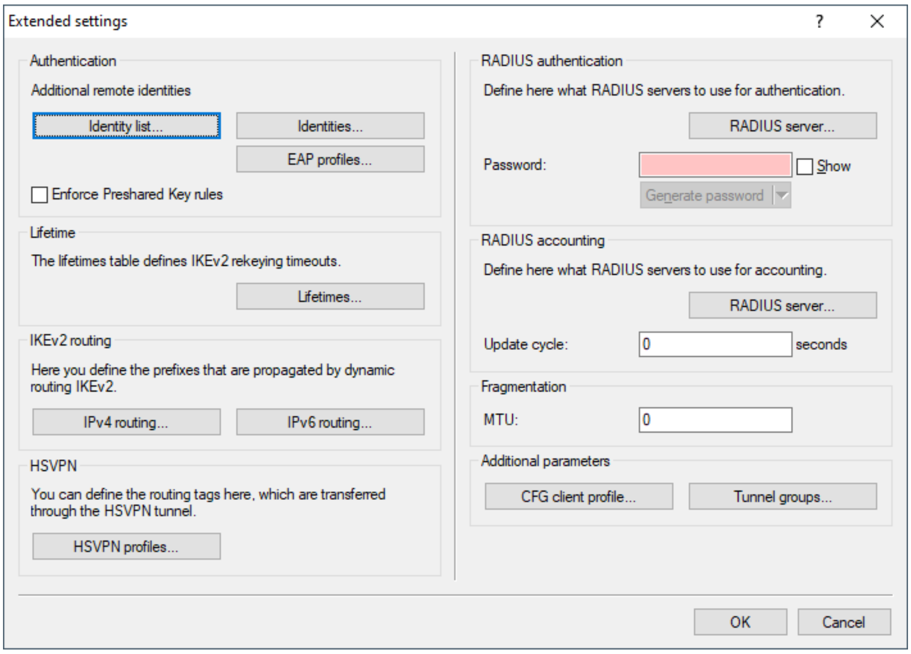
LANCOM HSVPN supports two modes:

- Classic site-to-site VPN
- CFG mode with IKEv2 routing, where routes and routing tags are transmitted

Current restrictions:

- Multicast routing is currently not supported over HSVPN. This requires a separate VPN tunnel for multicast.
- OSPF over HSVPN is not supported

In LANconfig, the HSVPN profiles are configured under **VPN** > **IKEv2/IPsec** > **Extended settings** > **HSVPN** with **HSVPN profiles**.


Extended settings

Authentication
Additional remote identities

Identity list... | Identities... | EAP profiles...

□ Enforce Preshared Key rules

Lifetime
The lifetimes table defines IKEv2 rekeying timeouts.

Lifetimes...

IKEv2 routing
Here you define the prefixes that are propagated by dynamic routing IKEv2.

IPv4 routing... | IPv6 routing...

HSVPN
You can define the routing tags here, which are transferred through the HSVPN tunnel.

HSVPN profiles...

RADIUS authentication
Define here what RADIUS servers to use for authentication.

RADIUS server...

Password: □ Show
Generate password

RADIUS accounting
Define here what RADIUS servers to use for accounting.

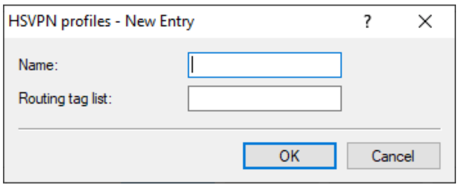
RADIUS server...

Update cycle: 0 seconds

Fragmentation
MTU: 0

Additional parameters
CFG client profile... | Tunnel groups...

OK | Cancel


HSVPN profiles - New Entry

Name:
Routing tag list:

OK | Cancel

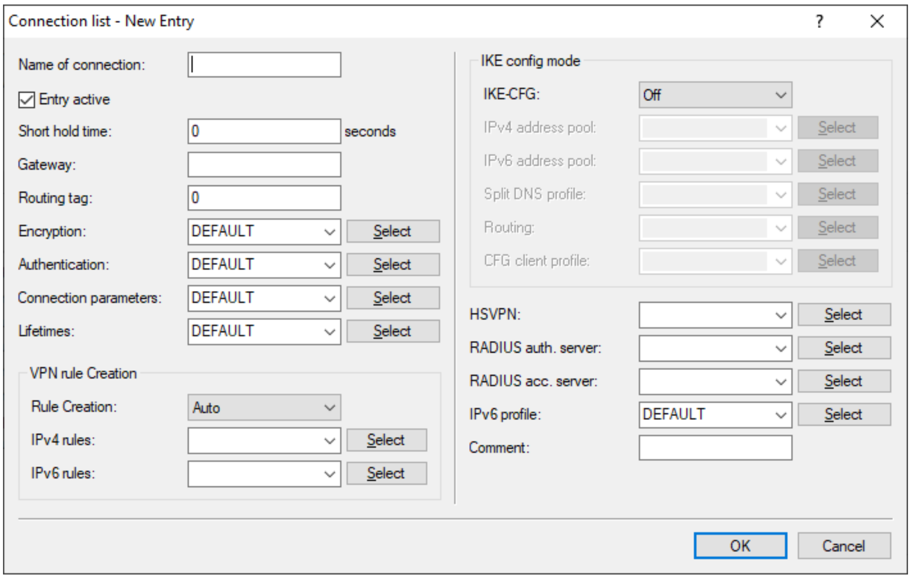
Name

Here you set a name for the HSVPN profile.

Routing tag list

Here you define the routing tags as a comma separated list (e.g. 1,2,3) that are to be transmitted via HSVPN. The Rtg-Tag list must be identical on both VPN partners in order for all of the desired ARF networks to be transported.

You can then select these profiles for the VPN connections under **VPN** > **IKEv2 / IPsec** > **Connection list**.



Connection list - New Entry

Name of connection:

☑ Entry active

Short hold time: 0 seconds

Gateway:

Routing tag: 0

Encryption: DEFAULT

Authentication: DEFAULT

Connection parameters: DEFAULT

Lifetimes: DEFAULT

VPN rule Creation

Rule Creation: Auto

IPv4 rules:

IPv6 rules:

IKE config mode

IKE-CFG: Off

IPv4 address pool:

IPv6 address pool:

Split DNS profile:

Routing:

CFG client profile:

HSVPN:

RADIUS auth. server:

RADIUS acc. server:

IPv6 profile: DEFAULT

Comment:

HSVPN

Here you set the name of the HSVPN profile from the table *HSVPN profiles*.

New RADIUS attributes for HSPVN

ID :	Name	Meaning
LANCOM 29	LCS-IKEv2-Routing-Tag-List	Format (string): #, e.g. `0,3,7` Contains the routing tags to be transmitted via HSVPN.
LANCOM 30	LCS-IKEv2-IPv4-Tagged-Route	Format (string): <Prefix> rtg_tag=<routing tag> **<Prefix>** HSVPN IPv4 route that the CFG mode server sends to the client as part of the IKEv2 routing. **rtg_tag=<routing tag>** The routing tag used here. For example, `192.168.1.0/24 rtg_tag = 1` A prefix with routing tag can occur several times in the attribute and is separated by a comma.
LANCOM 31	LCS-IKEv2-IPv6-Tagged-Route	Format (String), <Prefix> rtg_tag=<Routing-Tag> **<Prefix>** HSVPN IPv6 route that the CFG mode server sends to the client as part of the IKEv2 routing. **rtg_tag=<routing tag>** The routing tag used here.

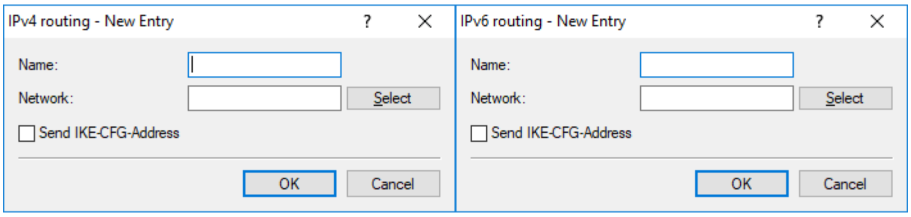
ID :	Name	Meaning
		For example, `2001:db8::/64 rtg_tag=1` A prefix with routing tag can occur several times in the attribute and is separated by a comma.

Example:

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

8.1.1 HSVPN and IKEv2 routing

The input syntax for HSVPN has been extended in the **VPN** > **IKEv2/IPSec** > **Extended settings** > **IPv4 routing** and **VPN** > **IKEv2/IPSec** > **Extended settings** > **IPv6 routing** tables. In addition to the network name or prefix, the corresponding routing tag can be specified here if HSVPN is to be used. For example 'INTRANET@1' or '192.168.1.0/24@1', where in this example 1 is the corresponding routing tag.



Console: **Setup** > **VPN** > **IKEv2** > **Routing** > **IPv4** resp. **Setup** > **VPN** > **IKEv2** > **Routing** > **IPv6**

8.1.2 Additions to the Setup menu

HSVPN

Here you set the name of the HSVPN profile from the table *HSVPN profiles*.

SNMP ID:

2.19.36.1.23

Console path:

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

Possible values:

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

HSVPN-Profiles

This table is used to configure the HSVPN profiles.

SNMP ID:

2.19.36.15

Console path:

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

Name

Here you set a name for the HSVPN profile.

SNMP ID:

2.19.36.15.1

Console path:

Setup > **VPN** > **IKEv2** > **HSVPN-Profiles**

Possible values:

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

Rtg-Tag-List

Here you define the routing tags as a comma separated list (e.g. 1,2,3) that are to be transmitted via HSVPN. The Rtg-Tag list must be identical on both VPN partners in order for all of the desired ARF networks to be transported.

SNMP ID:

2.19.36.15.2

Console path:

Setup > **VPN** > **IKEv2** > **HSVPN-Profiles**

Possible values:

Max. 100 characters from `[0-9] ,`

Networks

Contains the comma-separated list of IPv4 subnets.

Networks are entered in the following available formats:

- IP address
- IP address/netmask
- IP address/netmask@tag
- IP address/prefix length
- IP address/prefix length@tag
- IP interface name
- IP interface name@tag

The specification with routing tag is used for HSVPN.

SNMP ID:

2.19.36.6.1.2

Console path:

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

Possible values:

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

Networks

Contains the comma-separated list of IPv6 subnets.

Networks are entered in the following available formats:

- IPv6 address
- IPv6 address/prefix length
- IPv6 address/prefix length@tag
- IPv6 interface name
- IPv6 interface name@tag

The specification with routing tag is used for HSVPN.

SNMP ID:

2.19.36.6.2.2

Console path:

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

Possible values:

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

8.2 No further support for IP Compression and Authentication Header with IKEv1

As of LCOS 10.40 your device no longer supports the features IP Compression (IPCOMP) and Authentication Header (AH) in IKEv1. IPCOMP is a protocol for data compression in VPN tunnels and has been replaced by ESP. The Authentication Header (AH) was supposed to ensure the authenticity and integrity of the transmitted packets and authenticate the sender. However, since it cannot be used in combination with NAT, it is practically never used. This too has long since been replaced by ESP.

For this reason, the configuration under **VPN** > **IKE/IPSec** > **IPSec proposals** now no longer includes the options for selecting the **Mode**, the **AH proposals** and the **IPCOMP proposals**.

8.3 Grouping and prioritization of alternative gateways

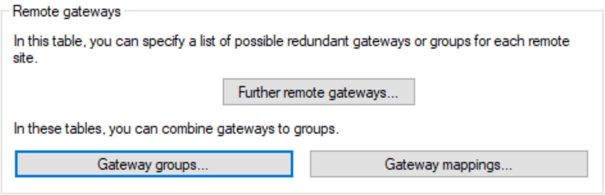
From LCOS 10.40 your device supports the grouping and prioritization of alternative VPN gateways. This enhances the existing ability to configure up to 32 additional gateways, which can be selected according to a configurable scheme (first, last used, random) as soon as the primary VPN gateway becomes unreachable.

Now gateways can optionally be collected into groups with equal priority. The highest priority is 0, the lowest 65535. The primary gateway is automatically placed in its own group with a priority of 0. If the primary gateway references a gateway group, this group is added to the level of priority 0, regardless of its configured priority. All gateways in the table of **Further remote gateways** that do not reference a group name are also added to the group of primary gateways. The selection strategy in the group of primary gateways is defined by the following rules:

- If there are further gateways, the selection strategy is set by the column **Begin with gateway** in the table of **Further remote gateways**.
- If there are no further gateways:
  - If there is only one primary gateway, then the selection strategy is "first".
  - If the primary gateway is a gateway group, the selection strategy of that group is used.

All defined groups are then added to the structure of levels in the order of the gateways from the **Further remote gateways** table with their priority as stored in the **Gateway groups** table. The strategy used to select from groups of the same priority is decided by the column **Begin with gateway** in the **Further remote gateways** table, and the selection strategy within a group is decided by the column **Begin with** in the **Gateway groups** table. The different levels are always used in ascending order of priority beginning with 0.

The configuration is performed under **VPN** > **General** > **Remote gateways**.



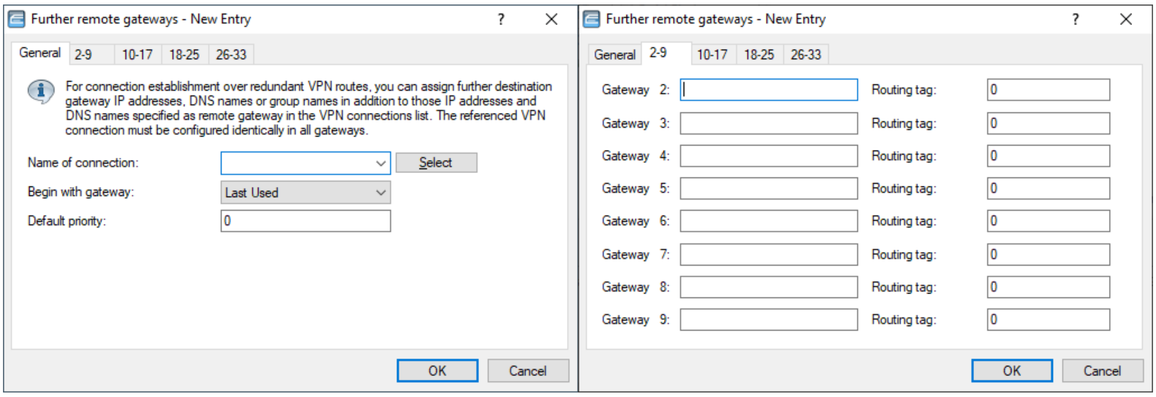
Remote gateways

In this table, you can specify a list of possible redundant gateways or groups for each remote site.

In these tables, you can combine gateways to groups.

8.3.1 Further remote gateways

The table **Further remote gateways** is used to specify redundant VPN routes by entering further destinations (as an IP address, DNS name or group name for the referenced connection) in addition to the IP address or DNS name specified as the remote gateway in the VPN connection list. All gateways have to be configured identically with respect to the referenced connection.



Further remote gateways - New Entry

For connection establishment over redundant VPN routes, you can assign further destination gateway IP addresses, DNS names or group names in addition to those IP addresses and DNS names specified as remote gateway in the VPN connections list. The referenced VPN connection must be configured identically in all gateways.

Name of connection:
Begin with gateway: Last Used
Default priority: 0

Further remote gateways - New Entry

Gateway 2:		Routing tag:	0
Gateway 3:		Routing tag:	0
Gateway 4:		Routing tag:	0
Gateway 5:		Routing tag:	0
Gateway 6:		Routing tag:	0
Gateway 7:		Routing tag:	0
Gateway 8:		Routing tag:	0
Gateway 9:		Routing tag:	0

Name of connection

From the list of defined VPN connections, select here the name of the VPN connection that the additional gateways defined here apply to.

Begin with gateway

Here you select the first gateway that is to be used for establishing the VPN connection. Possible values:

Last used

Selects the gateway that was most recently used to connect successfully.

First

Start with the first entry in the list.

Random

Selects a random entry from the list.

Default priority

This is the default priority for all gateways specified here. The highest priority is 0, the lowest 65535. All gateways are grouped together, with groups of equal priority placed next to each other on one level.

The primary gateway is automatically placed in its own group with a priority of 0. If the primary gateway references a gateway group, this group is added to the level of priority 0, regardless of its configured priority. If alternative gateways specified here do not reference a gateway group, these will also be added to the group of primary gateways.

Gateway 2-33

You can make three possible entries for each of the up to 32 alternative gateways:

1. The name of a gateway group
2. The DNS name of a gateway
3. The IP address of a gateway

When the table is processed, the first check is to see whether the entry matches with the name of a group specified in the **Gateway groups** table. In this case, all gateways that are mapped to this group in the **Gateway mappings** table are added to the gateway list.

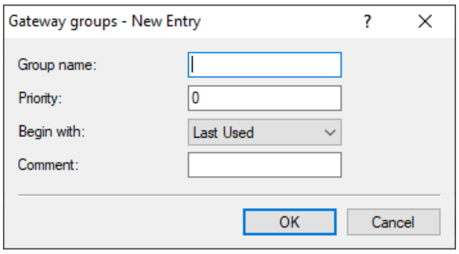
Routing tag

Enter the respective routing tag which is used to set the route to the associated remote gateway.

ⓘ If you do not specify a routing tag here (i.e. routing tag is 0), then the routing tag configured for this remote station in the VPN connection list is used for the associated gateway.

8.3.2 Gateway groups

The **Gateway groups** table is used to enter gateway groups that you can reference in *Further remote gateways*.


Gateway groups - New Entry

Group name:

Priority: 0

Begin with: Last Used

Comment:

Group name

Give this gateway group a unique name so that you can reference the group later.

Priority

The priority of this group. The highest priority is 0, the lowest 65535.

Begin with

Selection strategy within the group. Possible values:

Last used

Selects the gateway in the group which successfully connected most recently.

First

Start with the first entry in the list.

Random

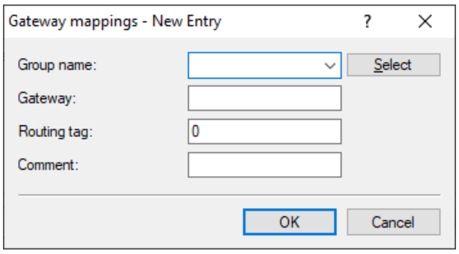
Selects a random entry from the list.

Comment

Optionally enter a meaningful comment as a description.

8.3.3 Gateway mappings

The **Gateway mappings** table is used to enter gateway groups that you can reference in *Further remote gateways*. **Gateway** and **Group name** together form the primary key of the table, i.e. the combination of the two must be unique within the table. This allows a single gateway to be mapped to multiple groups, if desired.



Gateway mappings - New Entry

Group name:

Gateway:

Routing tag: 0

Comment:

Group name

Name of the group that the gateway belongs to.

Gateway

DNS name or IP address of a gateway.

Routing tag

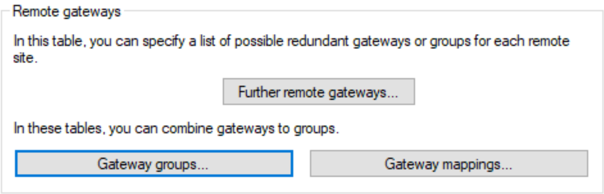
Routing tag of the gateway.

Comment

Optionally enter a meaningful comment as a description.

8.3.4 Example of an alternative gateway with prioritized groups

The customer “Telekom” uses the primary gateway 1.1.1.1 and the further gateway 1.1.1.2 without any particular group associations. Also, the further gateways, gateway groups and gateway mappings are specified under **VPN** > **General** > **Remote gateways** as follows:

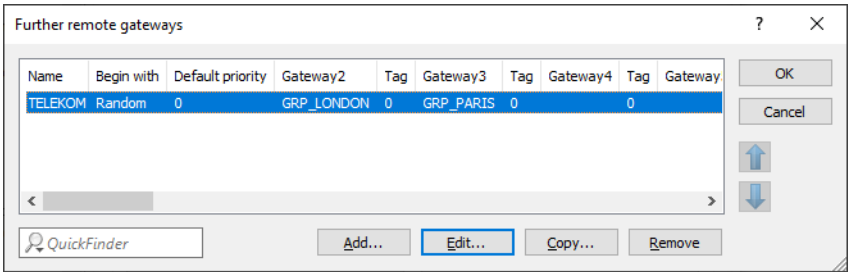


Remote gateways

In this table, you can specify a list of possible redundant gateways or groups for each remote site.

In these tables, you can combine gateways to groups.

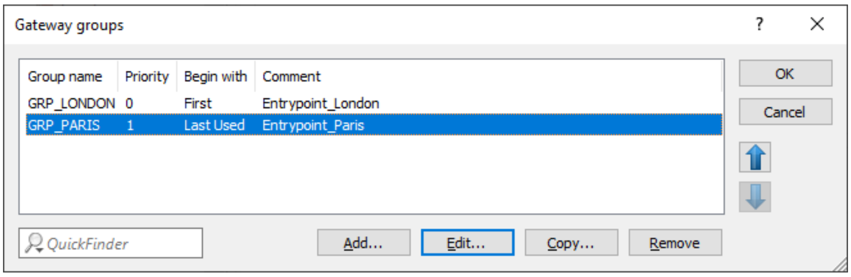
Figure 2: Remote gateways



Further remote gateways

Name	Begin with	Default priority	Gateway2	Tag	Gateway3	Tag	Gateway4	Tag	Gateway
TELEKOM	Random	0	GRP_LONDON	0	GRP_PARIS	0		0	

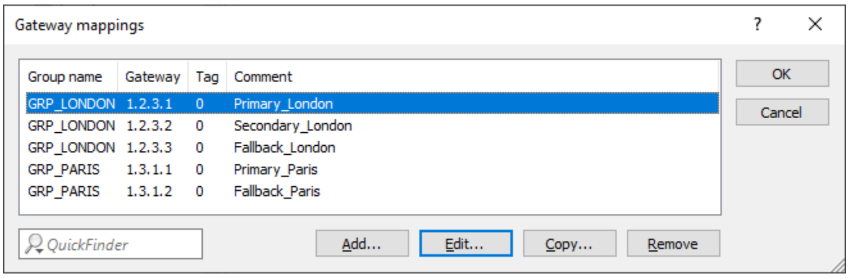
Figure 3: Further remote gateways



Gateway groups

Group name	Priority	Begin with	Comment
GRP_LONDON	0	First	Entrypoint_London
GRP_PARIS	1	Last Used	Entrypoint_Paris

Figure 4: Gateway groups



Gateway mappings

Group name	Gateway	Tag	Comment
GRP_LONDON	1.2.3.1	0	Primary_London
GRP_LONDON	1.2.3.2	0	Secondary_London
GRP_LONDON	1.2.3.3	0	Fallback_London
GRP_PARIS	1.3.1.1	0	Primary_Paris
GRP_PARIS	1.3.1.2	0	Fallback_Paris

Figure 5: Gateway mappings

This results in the following levels:

Priority	Group 1	Group 2
0	1.1.1.1, 1.1.1.2	GRP_LONDON
1	GRP_PARIS	

This addresses the gateways in the following order:

1. Priority 0: A group is selected at random because in the table **Further remote gateways**, the column **Begin with** is set to “Random”:
   - 1.1.1.1, 1.1.1.2 (primary gateway and additional gateway, which does not belong to any group)
   - 1.2.3.1, 1.2.3.2, 1.2.3.3 (GRP_LONDON) beginning with the first gateway in this group
2. Priority 1: A group is selected randomly because in the table **Further remote gateways**, the column **Begin with** is set to “Random”:
   - 1.3.1.1, 1.3.1.2 (GRP_PARIS) beginning with the last gateway in this group to be reached successfully.

8.3.5 Additions to the Setup menu

Default-Prio

This is the default priority for all gateways specified here. The highest priority is 0, the lowest 65535. All gateways are grouped together, with groups of equal priority placed next to each other on one level.

The primary gateway is automatically placed in its own group with a priority of 0. If the primary gateway references a gateway group, this group is added to the priority-0 layer, regardless of its configured priority. If alternative gateways specified here do not reference a gateway group, these will also be added to the group of primary gateways.

SNMP ID:

2.19.12.67

Console path:

Setup > **VPN** > **Additional-Gateways**

Possible values:

0 … 65535

Default:

0

Gateway-Groups

This table contains the settings for gateway groups, which you can reference in the list of additional gateways (see *2.19.12 Additional-Gateways*).

SNMP ID:

2.19.65

Console path:

Setup > **VPN**

Group-Name

Give this gateway group a unique name so that you can reference the group later.

SNMP ID:

2.19.65.1

Console path:

Setup > **VPN** > **Gateway-Groups**

Possible values:

Max. 24 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Priority

The priority of this group.

SNMP ID:

2.19.65.2

Console path:

Setup > **VPN** > **Gateway-Groups**

Possible values:

0 … 65535

Begin-With

Selection strategy within the group.

SNMP ID:

2.19.65.3

Console path:

Setup > **VPN** > **Gateway-Groups**

Possible values:

Last-Used
Selects the gateway in the group which successfully connected most recently.

First
Start with the first entry in the list.

Random
Selects a random entry from the list.

Comment

Optionally enter a meaningful comment as a description.

SNMP ID:

2.19.65.4

Console path:

Setup > **VPN** > **Gateway-Groups**

Possible values:

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

Gateway-Mappings

This table contains the settings for gateway mapping. Gateway mappings allow you to set up gateway groups (see also *2.19.65 Gateway-Groups* on page 135), which you can reference under *2.19.12 Additional-Gateways*. The gateway and group name together form the primary key of the table, i.e. the combination of the two must be unique in the table. This allows a single gateway to be mapped to multiple groups, if desired.

SNMP ID:

2.19.66

Console path:

Setup > **VPN**

Group-Name

Name of the group that the gateway belongs to.

SNMP ID:

2.19.66.1

Console path:

Setup > **VPN** > **Gateway-Mappings**

Possible values:

Max. 24 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Gateway

DNS name or IP address of a gateway.

SNMP ID:

2.19.66.2

Console path:

Setup > **VPN** > **Gateway-Mappings**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9].-:%`

Rtg-Tag

Routing tag of the gateway.

SNMP ID:

2.19.66.3

Console path:

Setup > **VPN** > **Gateway-Mappings**

Possible values:

0 … 65535

Default:

0

Comment

Optionally enter a meaningful comment as a description.

SNMP ID:

2.19.66.4

Console path:

Setup > **VPN** > **Gateway-Mappings**

Possible values:

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

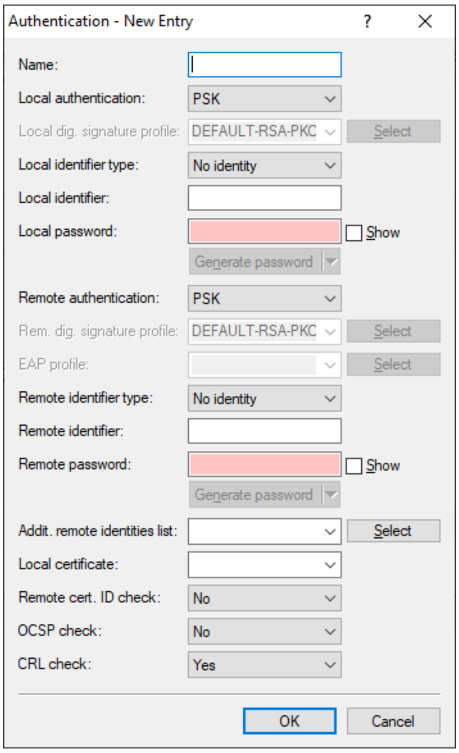
8.4 Extensible Authentication Protocol (EAP) supports IKEv2

As of LCOS version 10.40, IKEv2 clients can be authenticated using the Extensible Authentication Protocol (EAP). EAP is not a specific authentication mechanism, but rather a framework for various authentication methods such as TLS (authentication by certificate) or MSCHAP (authentication by username/password).

EAP authentication is handled by an external RADIUS server, such as the LANCOM RADIUS server, FreeRADIUS or Microsoft Network Policy Server (NPS). The VPN gateway merely acts as a mediator between the client and the RADIUS server. The VPN gateway must authenticate itself to the client using a certificate with a valid RSA signature. The RADIUS server must also have a valid certificate. The necessary certificates can be generated, for example, with the LANCOM SCEP CA in the router. After generation, the appropriate certificate containers are imported into the VPN gateway and into the RADIUS server.

To use the IKEv2 EAP authentication feature on LANCOM routers, you will need the VPN-25 Option or a router with 25 or more VPN tunnels. Check whether the router supports IKEv2 EAP in the LCOS Status menu under **Status** > **Software-Info** > **IKEv2-EAP-License**.

Under **VPN** > **IKEv2/IPSec** > **Authentication** you can select the **Remote authentication** used by EAP. You can optionally specify the EAP profile to be used.



Authentication - New Entry

Name:

Local authentication: PSK

Local dig. signature profile: DEFAULT-RSA-PKC Select

Local identifier type: No identity

Local identifier:

Local password: □ Show

Generate password

Remote authentication: PSK

Rem. dig. signature profile: DEFAULT-RSA-PKC Select

EAP profile: Select

Remote identifier type: No identity

Remote identifier:

Remote password: □ Show

Generate password

Addit. remote identities list: Select

Local certificate:

Remote cert. ID check: No

OCSP check: No

CRL check: Yes

OK Cancel

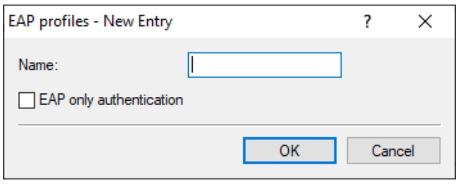
EAP profile

Specify an EAP profile if the method for the **Remote authentication** was set to EAP. The EAP profiles are specified under *EAP profiles*.

You can specify the EAP profiles under **VPN** > **IKEv2/IPSec** > **Extended settings** > **Authentication** > **EAP profiles**.

EAP profiles

This table is used to configure EAP profiles. You select this during **authentication** if you set the **remote authentication** method to EAP.



EAP profiles - New Entry

Name:

□ EAP only authentication

OK Cancel

Name

Give this EAP profile a name that can be used to reference it.

EAP-only authentication

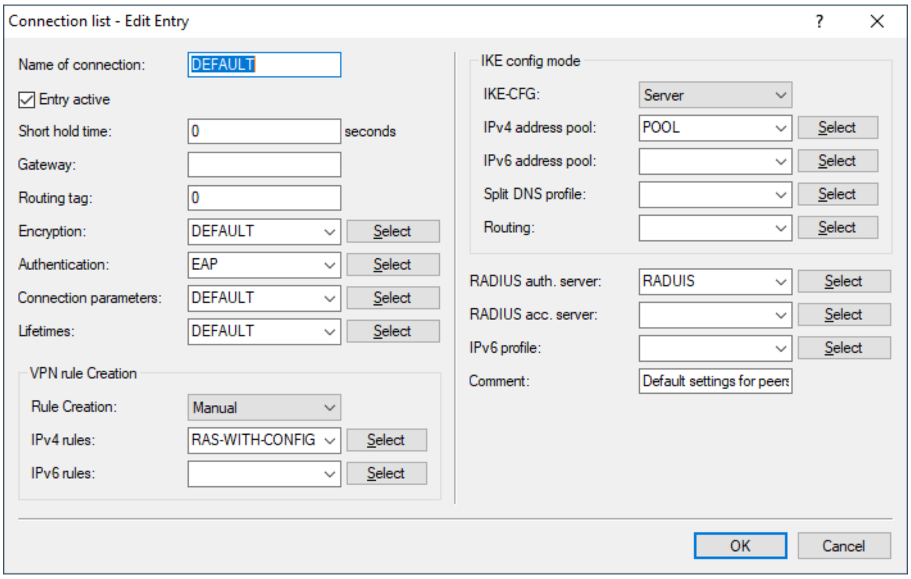
Optionally allows mutual authentication of remote sites within the EAP. Authentication outside the EAP is then not required. See also *RFC 5998*

8.4.1 Tutorial – EAP client at an EAP server

The following tutorial will configure an EAP client against an EAP server.

1. Create two certificates or certificate containers, for example with the LANCOM SCEP CA or OpenSSL.
2. Import a certificate into the VPN gateway and a certificate into the RADIUS server.

   Make sure the Subject Alternative Name (SAN) matches the valid DNS name of the VPN gateway and that the VPN client contacts the gateway under this DNS name.
3. Establish the trust relationship by importing the valid CA certificate into the IKEv2 EAP client.
4. Modify the DEFAULT entry of the IKEv2 remotes table under **VPN** > **IKEv2/IPSec** > **VPN connections** > **Connection list** as follows:



Connection list - Edit Entry

Name of connection: DEFAULT

☑ Entry active

Short hold time: 0 seconds

Gateway:

Routing tag: 0

Encryption: DEFAULT

Authentication: EAP

Connection parameters: DEFAULT

Lifetimes: DEFAULT

VPN rule Creation

Rule Creation: Manual

IPv4 rules: RAS-WITH-CONFIG

IPv6 rules:

IKE config mode

IKE-CFG: Server

IPv4 address pool: POOL

IPv6 address pool:

Split DNS profile:

Routing:

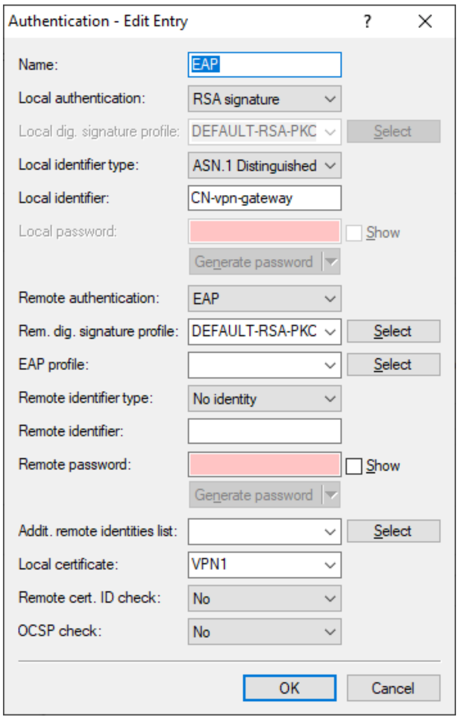
RADIUS auth. server: RADUIS

RADIUS acc. server:

IPv6 profile:

Comment: Default settings for peers

5. Insert a new row in the IKEv2 Authentication table under **VPN** > **IKEv2/IPSec** > **Authentication**. Local authentication of the VPN gateway uses a certificate (RSA signature), and remote authentication of the clients is done by EAP.



Authentication - Edit Entry

Name: EAP

Local authentication: RSA signature

Local dig. signature profile: DEFAULT-RSA-PKC

Local identifier type: ASN.1 Distinguished

Local identifier: CN-vpn-gateway

Local password: □ Show

Remote authentication: EAP

Rem. dig. signature profile: DEFAULT-RSA-PKC

EAP profile:

Remote identifier type: No identity

Remote identifier:

Remote password: □ Show

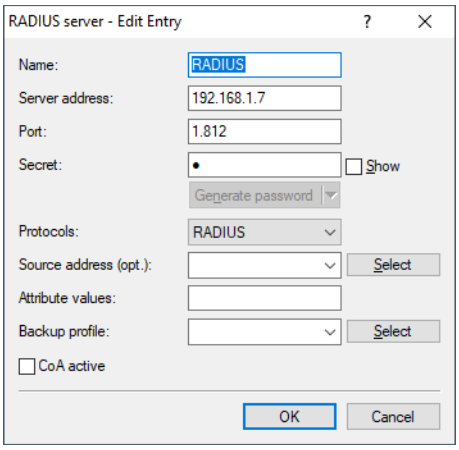
Addit. remote identities list:

Local certificate: VPN1

Remote cert. ID check: No

OCSP check: No

6. Configure the RADIUS server under **VPN** > **IKEv2/IPSec** > **Extended settings** > **RADIUS authentication** > **RADIUS server**.



RADIUS server - Edit Entry

Name: RADIUS

Server address: 192.168.1.7

Port: 1.812

Secret: • □ Show

Protocols: RADIUS

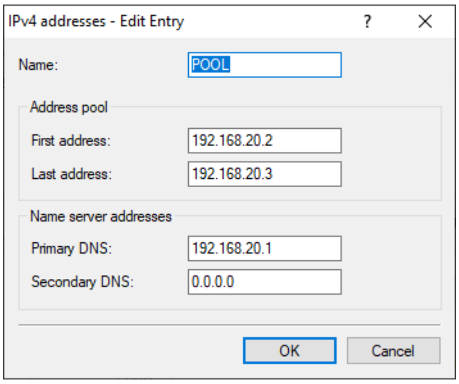
Source address (opt.):

Attribute values:

Backup profile:

□ CoA active

7. Configure an address pool under **VPN** > **IKEv2/IPSec** > **IPv4 addresses**.



IPv4 addresses - Edit Entry

Name: POOL

Address pool

First address: 192.168.20.2

Last address: 192.168.20.3

Name server addresses

Primary DNS: 192.168.20.1

Secondary DNS: 0.0.0.0

8.4.2 Additions to the Setup menu

Remote-Auth

Sets the authentication method for the remote identity.

SNMP ID:

2.19.36.3.1.6

Console path:

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

Possible values:

RSA-Signature

Authentication by RSA signature.

PSK

Authentication by pre-shared key (PSK).

Digital signature

Use of configurable authentication methods with digital certificates as per *RFC 7427*.

EAP

Authentication by the Extensible Authentication Protocol (EAP) *RFC 3748*.

ECDSA-256

Elliptic Curve Digital Signature Algorithm (ECDSA) according to *RFC 4754* with SHA-256 on the P-256 curve.

ECDSA-384

Elliptic Curve Digital Signature Algorithm (ECDSA) according to *RFC 4754* with SHA-384 on the P-384 curve.

ECDSA-521

Elliptic Curve Digital Signature Algorithm (ECDSA) according to *RFC 4754* with SHA-512 on the P-521 curve.

Default:

PSK

Remote-EAP-Profile

References an *EAP profile*.

SNMP ID:

2.19.36.3.1.16

Console path:

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

Possible values:

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

Default:

DEFAULT

EAP-Profiles

This table is used to configure the EAP profiles.

SNMP ID:

2.19.36.3.5

Console path:

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

Name

Give this EAP profile a name that can be used to reference it.

SNMP ID:

2.19.36.3.5.1

Console path:

Setup > **VPN** > **IKEv2** > **EAP-Profiles**

Possible values:

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

EAP-Only-Authentication

Optionally allows mutual authentication of remote sites within the EAP. Authentication outside the EAP is then not required. See also *RFC 5998*

SNMP ID:

2.19.36.3.5.4

Console path:

Setup > **VPN** > **IKEv2** > **EAP-Profiles**

Possible values:

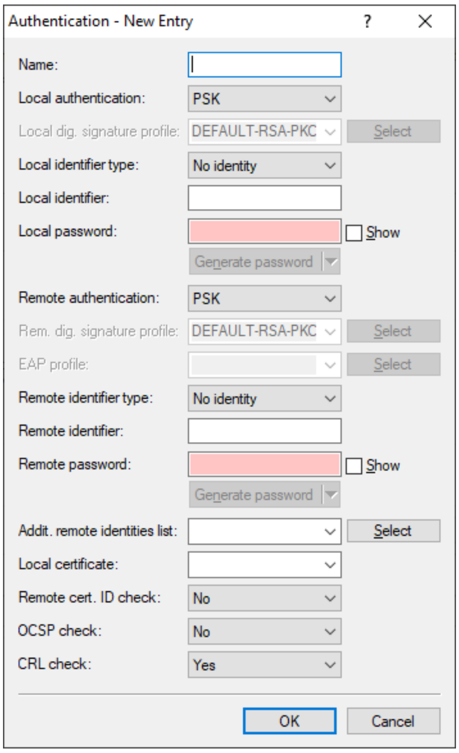
No
Yes

Optional authentication of the remote sites within the EAP.

8.5 Checking of certificate revocation lists can be switched off for IKEv2

From LCOS version 10.40 it is possible to disable checks on the validity of X.509 certificates by means of certificate revocation list (CRL).

Under **VPN** > **IKEv2/IPSec** > **Authentication** you can use the option **CRL check** to switch the checks off.



Authentication - New Entry

Name:		
Local authentication:	PSK	
Local dig. signature profile:	DEFAULT-RSA-PKC	Select
Local identifier type:	No identity	
Local identifier:		
Local password:		□ Show
	Generate password	
Remote authentication:	PSK	
Rem. dig. signature profile:	DEFAULT-RSA-PKC	Select
EAP profile:		Select
Remote identifier type:	No identity	
Remote identifier:		
Remote password:		□ Show
	Generate password	
Addit. remote identities list:		Select
Local certificate:		
Remote cert. ID check:	No	
OCSP check:	No	
CRL check:	Yes	

CRL check

This setting enables the checking of an X.509 certificate by certificate revocation list (CRL), which checks the validity of the remote station's certificate.

> ⓘ You should only switch this off if you are checking by other means, e.g. with OSCP.

8.5.1 Additions to the Setup menu

CRL-Check

This setting enables the checking of an X.509 certificate by certificate revocation list (CRL), which checks the validity of the remote station's certificate.

> ⓘ You should only switch this off if you are checking by other means, e.g. with OSCP.

SNMP ID:

2.19.36.3.1.17

Console path:

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

Possible values:

No
Yes

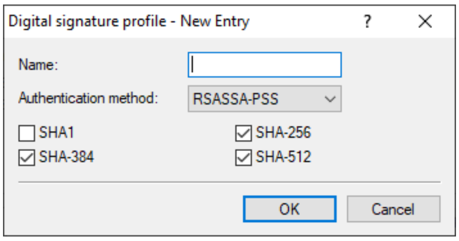
Default:

Yes

8.6 Digital signature profile

From LCOS version 10.40 your device supports the Elliptic Curve Digital Signature Algorithm (ECDSA), Edwards Curve 2551 (EdDSA25519) and Edwards Curve 448 (EdDSA448) authentication methods for the digital signature profiles.

Use this table to configure the parameters for the IKEv2 authentication.



Digital signature profile - New Entry

Name:

Authentication method: RSASSA-PSS

☐ SHA1 ☑ SHA-256
☑ SHA-384 ☑ SHA-512

Authentication method

Sets the authentication method for the digital signature. Possible values are:

- RSASSA-PSS: RSA with improved probabilistic signature schema as per version 2.1 of PKCS #1 (probabilistic signature scheme with appendix)
- RSASSA-PKCS1-v1_5: RSA according to the older version of the signature schema as per version 1.5 of PKCS #1 (probabilistic signature scheme with appendix)
- ECDSA: Elliptic Curve Digital Signature Algorithm (ECDSA)
- EdDSA25519: Edwards Curve 2551 (EdDSA25519) as per *RFC 8420*
- EdDSA448: Edwards Curve 448 (EdDSA448) as per *RFC 8420*

If RSASSA-PKCS1-v1_5 is selected, a check is made to see whether the remote site also supports the superior RSASSA-PSS method and switches to it if necessary. If RSASSA-PSS is selected, then a fallback to the older RSASSA-PKCS1-v1_5 is not provided.

You also specify the secure hash algorithms (SHA) to be used.

8.6.1 Additions to the Setup menu

Auth-Method

Sets the authentication method for the digital signature.

If RSASSA-PKCS1-v1_5 is selected, a check is made to see whether the remote site also supports the superior RSASSA-PSS method and switches to it if necessary. If RSASSA-PSS is selected, then a fallback to the older RSASSA-PKCS1-v1_5 is not provided.

SNMP ID:

2.19.36.3.4.2

Console path:

Setup > **VPN** > **IKEv2** > **Digital-Signature-Profiles**

Possible values:

RSASSA-PSS

RSASSA-PKCS1-v1_5

ECDSA

Elliptic Curve Digital Signature Algorithm

EdDSA25519

Authentication as per EdDSA25519 (Edwards Curve 2551) according to *RFC 8420*.

EdDSA448

Authentication as per EdDSA448 (Edwards Curve 448) according to *RFC 8420*.

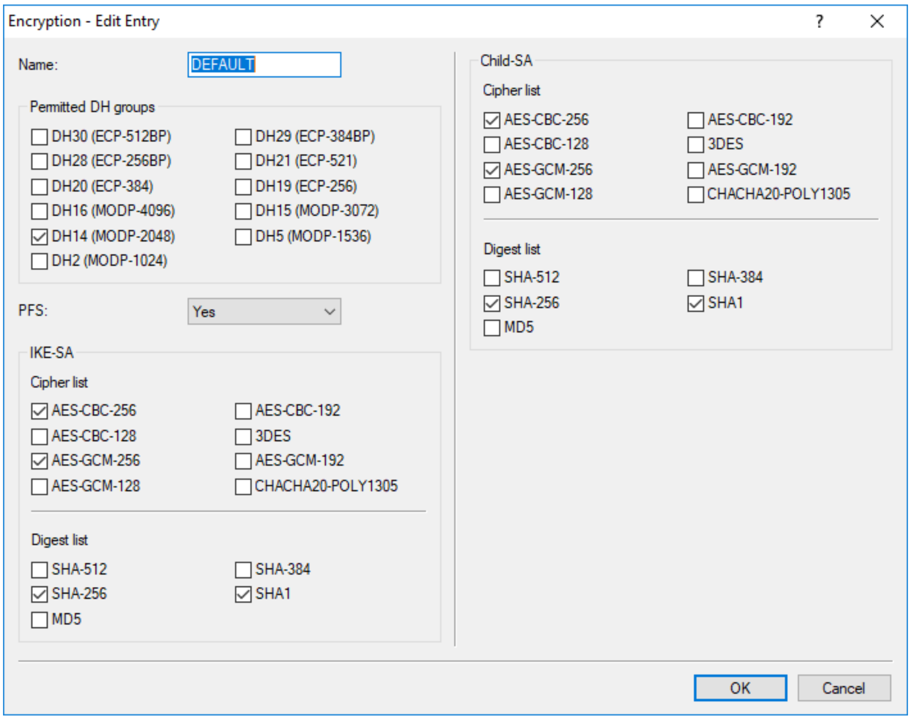
Default:

RSASSA-PSS

8.7 Additional DH groups and encryption algorithms for IKEv2

From LCOS version 10.40 the DH groups DH-31 (Curve25519) and DH-32 (Curve448) are supported. Further, the option Chacha20-Poly1305 supports the use of the ChaCha20 stream cipher along with with the Poly1305 authenticator, see *RFC 7634*.

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.



Encryption - Edit Entry

Name: DEFAULT

Permitted DH groups

□ 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

Digest list

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

8.7.1 Additions to the Setup menu

DH-Groups

Contains the selection of Diffie-Hellman groups.

SNMP ID:

2.19.36.2.2

Console path:

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

Possible values:

DH32
Curve448 (as of LCOS version 10.40)

DH31
Curve25519 (as of LCOS version 10.40)

DH30
(as of LCOS version 10.12)

DH29
(as of LCOS version 10.12)

DH28
(as of LCOS version 10.12)

DH21

(as of LCOS version 10.12)

DH20

(as of LCOS version 10.12)

DH19

(as of LCOS version 10.12)

DH16
DH15
DH14
DH5
DH2

Default:

DH14

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.

Default:

AES-CBC-256

AES-GCM-256

Child-SA-Cipher-List

Specifies which encryption algorithms are enabled in the Child-SA.

SNMP ID:

2.19.36.2.6

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.

Default:

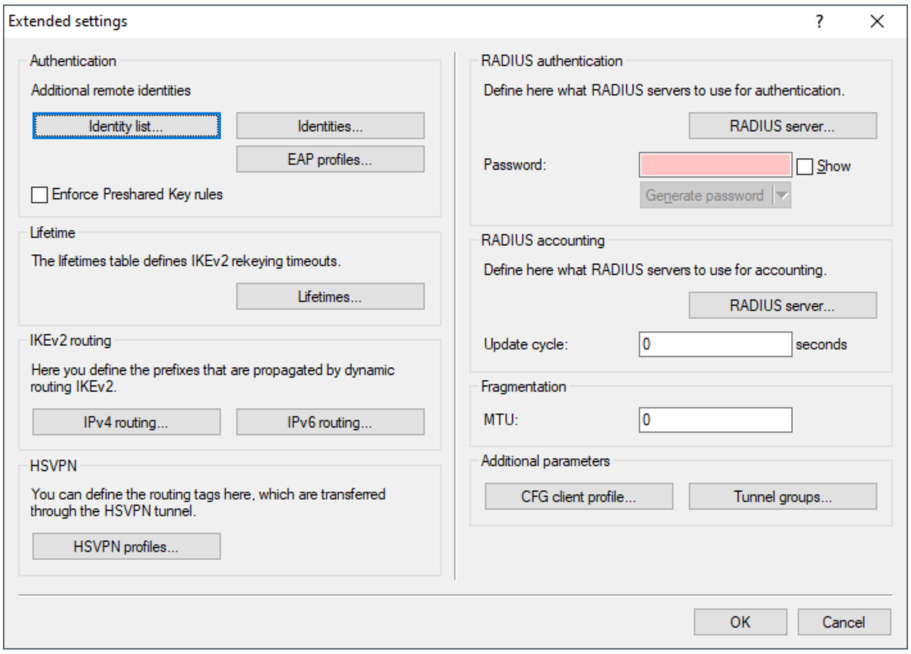
AES-CBC-256

AES-GCM-256

8.8 Address requests can be configured in IKEv2 CFG mode

As of LCOS version 10.40, your device supports the option to configure the address requests in IKEv2-CFG mode.

In LANconfig, the CFG profiles are configured under **VPN** > **IKEv2/IPSec** > **Extended settings** > **Additional parameters** using **CFG client profile**.



Extended settings

Authentication

Additional remote identities

□ Enforce Preshared Key rules

Lifetime

The lifetimes table defines IKEv2 rekeying timeouts.

IKEv2 routing

Here you define the prefixes that are propagated by dynamic routing IKEv2.

HSVPN

You can define the routing tags here, which are transferred through the HSVPN tunnel.

RADIUS authentication

Define here what RADIUS servers to use for authentication.

Password: □ Show

RADIUS accounting

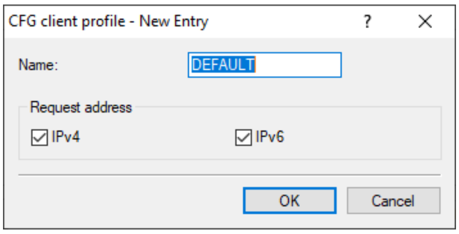
Define here what RADIUS servers to use for accounting.

Update cycle: 0 seconds

Fragmentation

MTU: 0

Additional parameters



CFG client profile - New Entry

Name: DEFAULT

Request address

☑ IPv4 ☑ IPv6

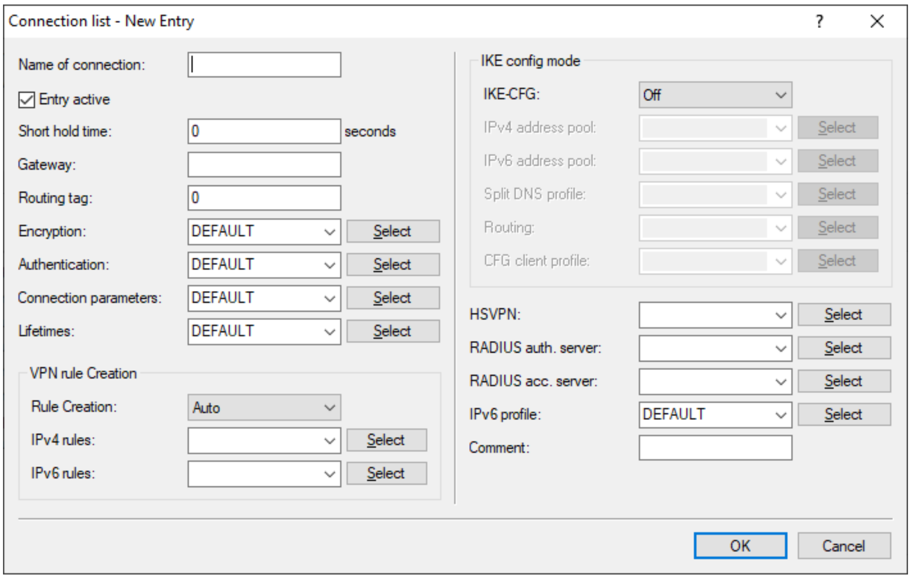
Name

Unique name for the CFG client profile.

Request address

Specify whether addresses for IPv4 and / or IPv6 should be requested for this profile.

You can then select these profiles for the VPN connections under **VPN** > **IKEv2 / IPSec** > **Connection list**.



Connection list - New Entry

Name of connection:

☑ Entry active

Short hold time: 0 seconds

Gateway:

Routing tag: 0

Encryption: DEFAULT

Authentication: DEFAULT

Connection parameters: DEFAULT

Lifetimes: DEFAULT

VPN rule Creation

Rule Creation: Auto

IPv4 rules:

IPv6 rules:

IKE config mode

IKE-CFG: Off

IPv4 address pool:

IPv6 address pool:

Split DNS profile:

Routing:

CFG client profile:

HSVPN:

RADIUS auth. server:

RADIUS acc. server:

IPv6 profile: DEFAULT

Comment:

CFG client profile

Select a CFG client profile that you created under *CFG client profile*. This profiles specifies whether the device in the role CFG-Mode client should request an address from the CFG-Mode server.

8.8.1 Additions to the Setup menu

CFG-Client-Profile

Here you define the name of the client profile from the *Client Profile* table. This determines whether the device in the role CFG mode client should request an address from the CFG mode server.

SNMP ID:

2.19.36.1.24

Console path:

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

Possible values:

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

Client-Profile

In this table you can specify whether the device in the role CFG-Mode client should request an address from the CFG-Mode server. This function is usually used in conjunction with IKEv2 routing.

SNMP ID:

2.19.36.7.4

Console path:

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

Name

Here you set a name for the Client profile.

SNMP ID:

2.19.36.7.4.1

Console path:

Setup > **VPN** > **IKEv2** > **IKE-CFG** > **Client-Profile**

Possible values:

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

Request-Address

Defines which address type should be requested in Config mode.

SNMP ID:

2.19.36.7.4.2

Console path:

Setup > **VPN** > **IKEv2** > **IKE-CFG** > **Client-Profile**

Possible values:

None
IPv4
IPv6

Default:

IPv4

IPv6

8.9 IKEv2 tunnel groups

Some VPN scenarios require that a given group of VPN tunnels of a device terminates on, or establishes to, a common VPN gateway. This is necessary, for example, where VPN tunnels are configured on a cluster of load balancers and VPN tunnels use the alternative gateway list and maybe even different paths or outbound Internet connections (DSL, LTE, Ethernet) to reach the destination.

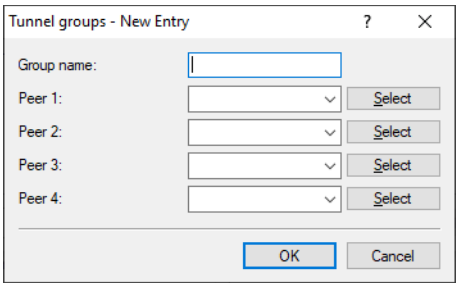
A VPN load balancer requires that the various VPN tunnels always terminate on a common VPN gateway.

IKEv2 tunnel groups is a feature that ensures that all VPN tunnels in a group always terminate on a common VPN gateway. The first VPN tunnel to be established in a group determines the common VPN gateway, and the VPN remote gateways for all of the other members of the tunnel group are transferred to this destination. Usually, this is the VPN tunnel that is established the fastest. The selection of a gateway is only performed again if all tunnel group members are unable to reach the gateway.

The function of the IKEv2 tunnel groups can basically be used independently of a load balancer.

Tunnel groups are not supported in conjunction with IKEv2 Redirect and the IKEv2 Redirect Load Balancer.

In LANconfig, navigate through the configuration to **VPN** > **IKEv2/IPSec** > **Extended settings** and, in the section **Additional parameters**, configure the **Tunnel groups**.



Group name

Unique name for the tunnel group.

Peer 1-4

The name of each remote site of the IKEv2 VPN tunnel terminating in the tunnel group.

8.9.1 Additions to the Setup menu

Tunnel-Groups

Some VPN scenarios require that a given group of VPN tunnels of a device terminates on, or establishes to, a common VPN gateway. This is necessary, for example, where VPN tunnels are configured on a cluster of load balancers and VPN tunnels use the alternative gateway list and maybe even different paths or outbound Internet connections (DSL, LTE, Ethernet) to reach the destination.

A VPN load balancer requires that the various VPN tunnels always terminate on a common VPN gateway.

IKEv2 tunnel groups is a feature that ensures that all VPN tunnels in a group always terminate on a common VPN gateway. The first VPN tunnel to be established in a group determines the common VPN gateway, and the VPN remote gateways for all of the other members of the tunnel group are transferred to this destination. Usually, this is the VPN tunnel that is established the fastest. The selection of a gateway is only performed again if all tunnel group members are unable to reach the gateway.

The function of the IKEv2 tunnel groups can basically be used independently of a load balancer.

Tunnel groups are not supported in conjunction with IKEv2 Redirect and the IKEv2 Redirect Load Balancer.

SNMP ID:

2.19.36.13

Console path:

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

Group-Name

Unique name for the tunnel group.

SNMP ID:

2.19.36.13.1

Console path:

Setup > **VPN** > **IKEv2** > **Tunnel-Groups**

Possible values:

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

Peer-1

The name of a remote site of the IKEv2 VPN tunnel that terminates in the tunnel group.

SNMP ID:

2.19.36.13.2

Console path:

Setup > **VPN** > **IKEv2** > **Tunnel-Groups**

Possible values:

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

Peer-2

The name of a remote site of the IKEv2 VPN tunnel that terminates in the tunnel group.

SNMP ID:

2.19.36.13.3

Console path:

Setup > **VPN** > **IKEv2** > **Tunnel-Groups**

Possible values:

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

Peer-3

The name of a remote site of the IKEv2 VPN tunnel that terminates in the tunnel group.

SNMP ID:

2.19.36.13.4

Console path:

Setup > **VPN** > **IKEv2** > **Tunnel-Groups**

Possible values:

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

Peer-4

The name of a remote site of the IKEv2 VPN tunnel that terminates in the tunnel group.

SNMP ID:

2.19.36.13.5

Console path:

Setup > **VPN** > **IKEv2** > **Tunnel-Groups**

Possible values:

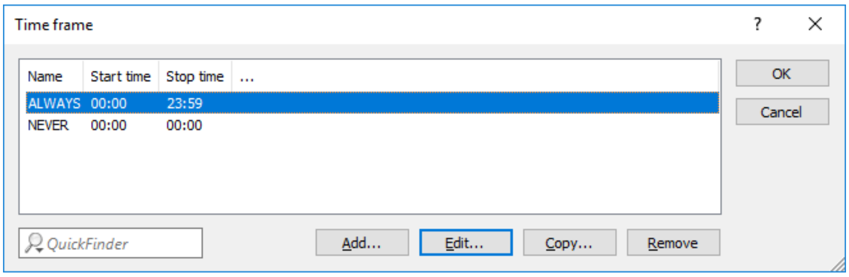
Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;< =>?[\]^_.`

9 Wireless LAN – WLAN

9.1 Time control for SSIDs

From LCOS 10.40 individual SSIDs can be switched on and off according to a schedule. This can be used, for example to activate a WLAN in a school only during class times. For example, a hotspot will only be activated during business hours or made available to students during school breaks.

The first step is to define the time frames in the appropriate table under **Date & Time** > **General** > **Time frame**.



Name	Start time	Stop time	...
ALWAYS	00:00	23:59	
NEVER	00:00	00:00	

Name

Enter the name of the time frame for referencing from the content-filter profile or by a WLAN SSID. Several entries with the same name result in a common profile.

Possible values:

- Name of a timeframe

Start

Here you set the start time (time of day) when the selected profile becomes valid.

Possible values:

- Format HH:MM (default: 00:00)

Stop

Here you set the stop time (time of day) when the selected profile ceases to be valid.

Possible values:

- Format HH:MM (default: 23:59)

A stop time of HH:MM usually runs until HH:MM:00. The stop time 00:00 is an exception, since this is interpreted as 23:59:59.

Weekdays

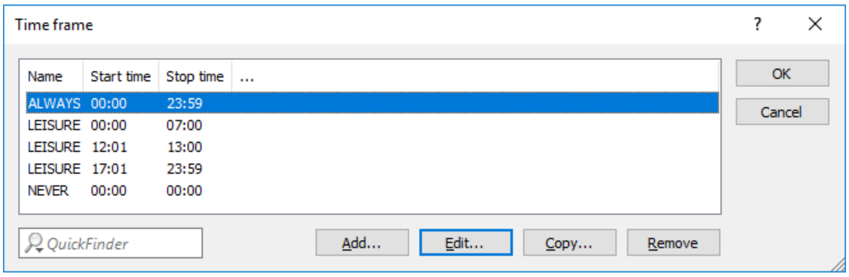
Here you select the weekday on which the timeframe is to be valid.

Possible values:

- Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday, Holiday

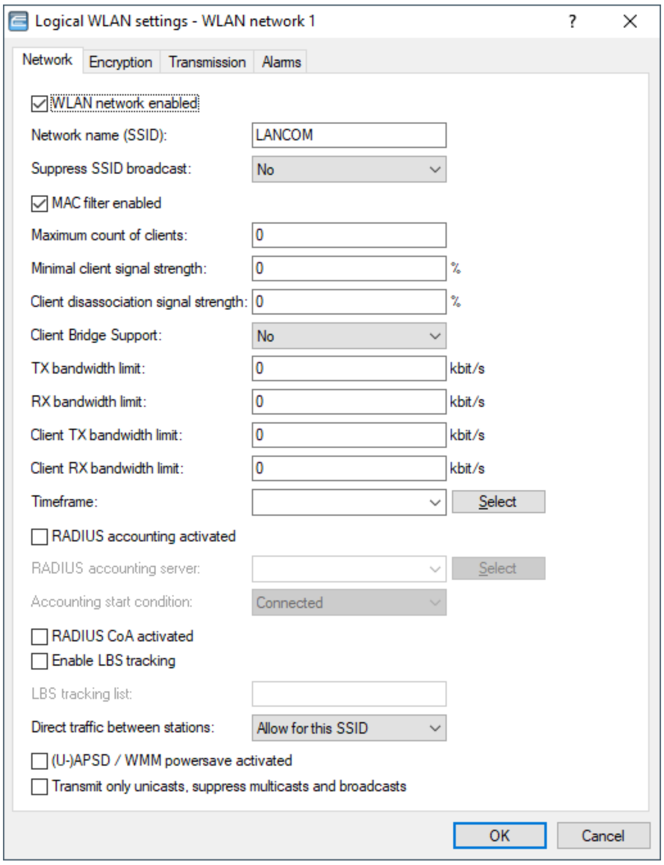
The holidays are set under **Date & Time** > **General** > **Public holidays**.

You can form a time schedule with the same name but with different times extending over several lines:


Time frame

Name	Start time	Stop time	...
ALWAYS	00:00	23:59	
LEISURE	00:00	07:00	
LEISURE	12:01	13:00	
LEISURE	17:01	23:59	
NEVER	00:00	00:00	

The second step is made under **Wireless LAN** > **General** > **Logical WLAN settings** > **Network** where you select the appropriate **Time frame**.


Logical WLAN settings - WLAN network 1

☑ WLAN network enabled

Network name (SSID):	LANCOM
Suppress SSID broadcast:	No

☑ MAC filter enabled

Maximum count of clients:	0
Minimal client signal strength:	0 %
Client disassociation signal strength:	0 %
Client Bridge Support:	No
TX bandwidth limit:	0 kbit/s
RX bandwidth limit:	0 kbit/s
Client TX bandwidth limit:	0 kbit/s
Client RX bandwidth limit:	0 kbit/s
Timeframe:	Select

□ RADIUS accounting activated

RADIUS accounting server:	Select
Accounting start condition:	Connected

□ RADIUS CoA activated
□ Enable LBS tracking

LBS tracking list:	
Direct traffic between stations:	Allow for this SSID

□ (U-)APSD / WMM powersave activated
□ Transmit only unicasts, suppress multicasts and broadcasts

Timeframe

Select one of the time frames defined in *Timeframe*. This can be used to restrict the broadcast of this SSID to the times defined there. This can be used, for example to activate a WLAN in a school only during class times.

9.1.1 Additions to the Setup menu

Stop

Here you set the end time (time of day) in the format HH:MM when the selected profile ceases to be valid.

A stop time from HH:MM normally goes to HH:MM:00, with the exception of stop time 00:00, which is interpreted as 23:59:59.

SNMP ID:

2.14.16.3

Console path:

Setup > **Time** > **Timeframe**

Possible values:

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

Default:

00:00

Timeframe

Select one of the time frames defined in *2.14.16 Timeframe*. This can be used to restrict the broadcast of this SSID to the times defined there. This can be used, for example to activate a WLAN in a school only during class times.

SNMP ID:

2.23.20.1.31

Console path:

Setup > **Interfaces** > **WLAN** > **Network**

Possible values:

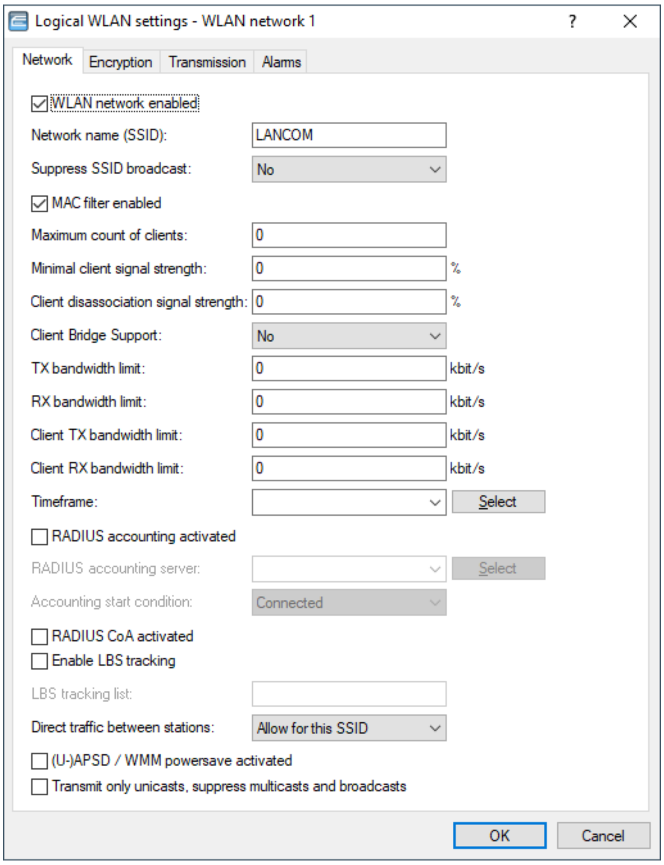
Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

9.2 Signal strength at which a client is disassociated

From LCOS 10.40 it is possible to disassociate a client if the signal strength drops too low.



☑ WLAN network enabled

Network name (SSID): LANCOM

Suppress SSID broadcast: No

☑ MAC filter enabled

Maximum count of clients: 0

Minimal client signal strength: 0 %

Client disassociation signal strength: 0 %

Client Bridge Support: No

TX bandwidth limit: 0 kbit/s

RX bandwidth limit: 0 kbit/s

Client TX bandwidth limit: 0 kbit/s

Client RX bandwidth limit: 0 kbit/s

Timeframe:

☐ RADIUS accounting activated

RADIUS accounting server:

Accounting start condition: Connected

☐ RADIUS CoA activated

☐ Enable LBS tracking

LBS tracking list:

Direct traffic between stations: Allow for this SSID

☐ (U-)APSD / WMM powersave activated

☐ Transmit only unicasts, suppress multicasts and broadcasts

Client disassociation signal strength

If values drop below this threshold, the client is disassociated. This prevents the client from sticking with a WLAN connection that is actually unusable because of the poor signal rather than switching to a better cell phone connection—behavior that is all too common for mobile phones and can be very annoying for the user.

This threshold only works if the value **Minimum client signal strength** is also set and the **Client disassociation signal strength** is less than this value.

9.2.1 Additions to the Setup menu

Min-Client-Disassoc-Strength

If values drop below this threshold, the client is disassociated. This prevents the client from sticking with a WLAN connection that is actually unusable because of the poor signal rather than switching to a better cell phone connection—behavior that is all too common for mobile phones and can be very annoying for the user.

This threshold only works if the value *2.23.20.1.16 Min-Client-Strength* is also set and the Min-Stations-Disassoc-Strength is less than this value.

SNMP ID:

2.23.20.1.32

Console path:

Setup > **Interfaces** > **WLAN** > **Network**

Possible values:

0 … 100

Default:

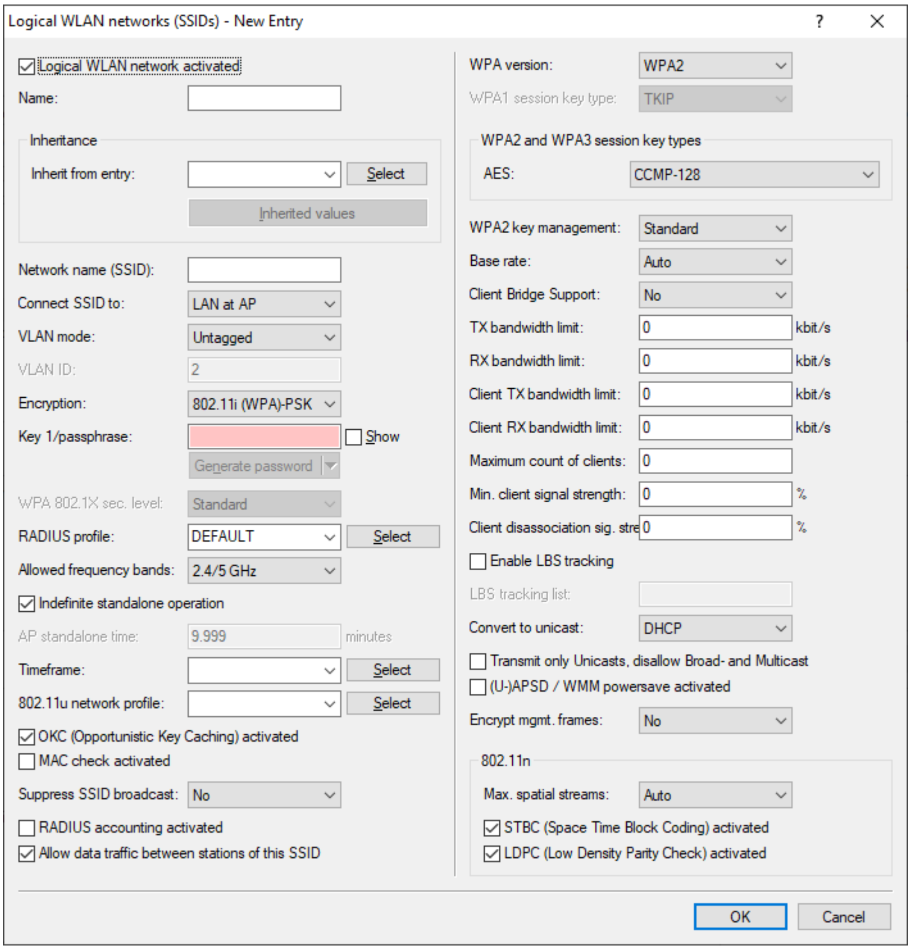
0

10 WLAN management

10.1 Client bandwidth limit

As of LCOS 10.40 you can limit the bandwidth for clients.

To do this, navigate in LANconfig to **WLAN controller** > **Profiles** > **Logical WLAN networks**.



Logical WLAN networks (SSIDs) - New Entry

☑ Logical WLAN network activated

Name:

Inheritance

Inherit from entry:

Network name (SSID):

Connect SSID to: LAN at AP

VLAN mode: Untagged

VLAN ID: 2

Encryption: 802.11i (WPA)-PSK

Key 1/passphrase: □ Show

WPA 802.1X sec. level: Standard

RADIUS profile: DEFAULT

Allowed frequency bands: 2.4/5 GHz

☑ Indefinite standalone operation

AP standalone time: 9.999 minutes

Timeframe:

802.11u network profile:

☑ OKC (Opportunistic Key Caching) activated

□ MAC check activated

Suppress SSID broadcast: No

□ RADIUS accounting activated

☑ Allow data traffic between stations of this SSID

WPA version: WPA2

WPA1 session key type: TKIP

WPA2 and WPA3 session key types

AES: CCMP-128

WPA2 key management: Standard

Base rate: Auto

Client Bridge Support: No

TX bandwidth limit: 0 kbit/s

RX bandwidth limit: 0 kbit/s

Client TX bandwidth limit: 0 kbit/s

Client RX bandwidth limit: 0 kbit/s

Maximum count of clients: 0

Min. client signal strength: 0 %

Client disassociation sig. stre 0 %

□ Enable LBS tracking

LBS tracking list:

Convert to unicast: DHCP

□ Transmit only Unicasts, disallow Broad- and Multicast

□ (U-)APSD / WMM powersave activated

Encrypt mgmt. frames: No

802.11n

Max. spatial streams: Auto

☑ STBC (Space Time Block Coding) activated

☑ LDPC (Low Density Parity Check) activated

Client TX bandwidth limit

Here, you set the transmit-direction bandwidth limit (in kbps) available to each wireless client on this SSID. A value of 0 disables the limit.

Client RX bandwidth limit

Here, you set the receive-direction bandwidth limit (in kbps) available to each wireless client on this SSID. A value of 0 disables the limit.

10.1.1 Additions to the Setup menu

Per-Client-Tx-Limit

Here, you set the transmit-direction bandwidth limit (in kbps) available to each wireless client on this SSID. A value of 0 disables the limit.

SNMP ID:

2.37.1.1.55

Console path:

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

Possible values:

Max. 10 characters from `0123456789`

Default:

0

Special values:

0

Disables the limit.

Per-Client-Rx-Limit

Here, you set the receive-direction bandwidth limit (in kbps) available to each wireless client on this SSID. A value of 0 disables the limit.

SNMP ID:

2.37.1.1.56

Console path:

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

Possible values:

Max. 10 characters from `0123456789`

Default:

0

Special values:

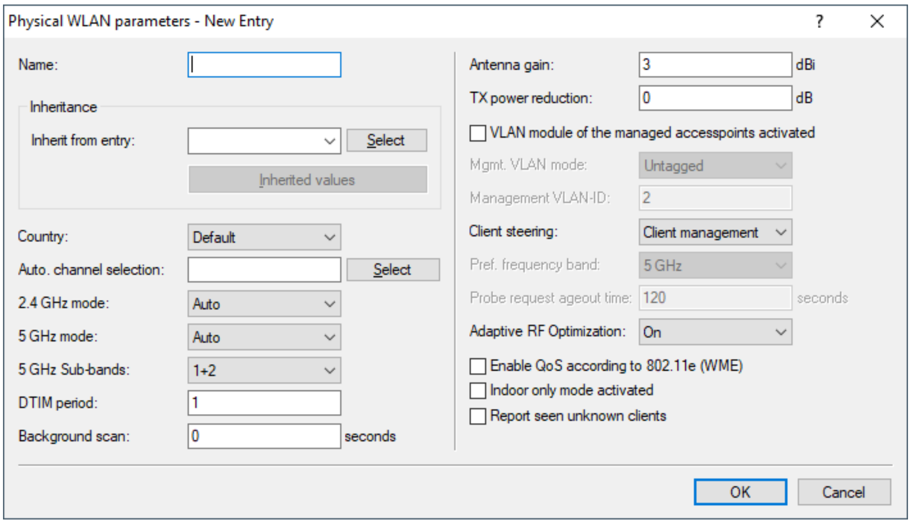
0

Disables the limit.

10.2 New default for “Report seen unknown clients”

As of LCOS 10.40 the presetting of the parameter **Report seen unknown clients** has been changed to “Off”.

This parameter in LANconfig is located under **WLAN controller** > **Profiles** > **Physical WLAN parameters**.



Physical WLAN parameters - New Entry

Name:

Inheritance

Inherit from entry: Select

Inherited values

Country: Default

Auto. channel selection: Select

2.4 GHz mode: Auto

5 GHz mode: Auto

5 GHz Sub-bands: 1+2

DTIM period: 1

Background scan: 0 seconds

Antenna gain: 3 dBi

TX power reduction: 0 dB

□ VLAN module of the managed accesspoints activated

Mgmt. VLAN mode: Untagged

Management VLAN-ID: 2

Client steering: Client management

Pref. frequency band: 5 GHz

Probe request ageout time: 120 seconds

Adaptive RF Optimization: On

□ Enable QoS according to 802.11e (WME)

□ Indoor only mode activated

□ Report seen unknown clients

OK Cancel

Report seen unknown clients

By default, the access point only reports associated clients to the WLC. If all other seen clients should be reported, i.e. unassociated clients as well, you can activate this switch. This will increase the traffic on the network. You should therefore activate this switch only temporarily or for test purposes.

If you have a large number of unknown clients (e.g., with a Public Spot or in areas with lots of traffic), you should not activate this switch, otherwise you will be flooded by inbound messages.

10.2.1 Additions to the Setup menu

Report-seen-clients

By default, the access point only reports associated clients to the WLC. If all other seen clients should be reported, i.e. unassociated clients as well, you can activate this switch. This will increase the traffic on the network. You should therefore activate this switch only temporarily or for test purposes.

If you have a large number of unknown clients (e.g., with a Public Spot or in areas with lots of traffic), you should not activate this switch, otherwise you will be flooded by inbound messages.

SNMP ID:

2.37.1.2.20

Console path:

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

Possible values:

No
Yes

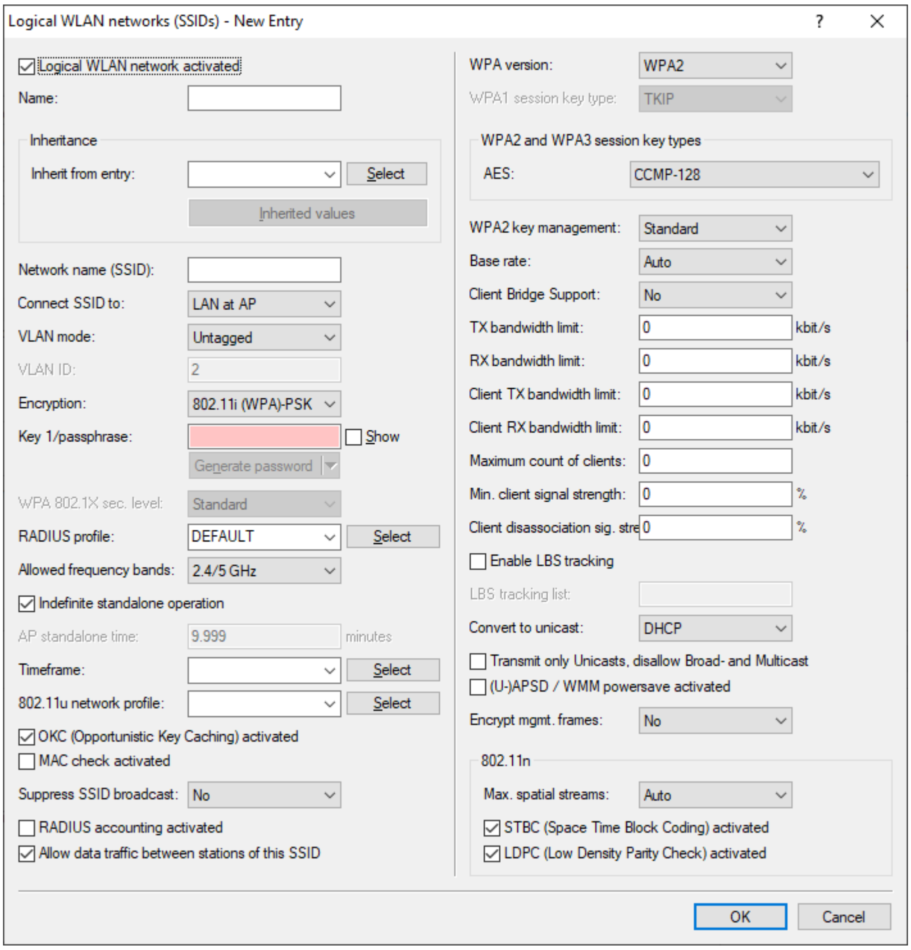
Default:

No

10.3 Time control for SSIDs

Similar to the feature described under *Time control for SSIDs* on page 156, this option is also available for WLAN controllers.

You enter the time frame under **WLAN controller** > **Profiles** > **Logical WLAN networks**.



Logical WLAN networks (SSIDs) - New Entry

☑ Logical WLAN network activated

Name:

Inheritance

Inherit from entry: Select

Inherited values

Network name (SSID):

Connect SSID to: LAN at AP

VLAN mode: Untagged

VLAN ID: 2

Encryption: 802.11i (WPA)-PSK

Key 1/passphrase: □ Show

Generate password

WPA 802.1X sec. level: Standard

RADIUS profile: DEFAULT Select

Allowed frequency bands: 2.4/5 GHz

☑ Indefinite standalone operation

AP standalone time: 9.999 minutes

Timeframe: Select

802.11u network profile: Select

☑ OKC (Opportunistic Key Caching) activated

□ MAC check activated

Suppress SSID broadcast: No

□ RADIUS accounting activated

☑ Allow data traffic between stations of this SSID

WPA version: WPA2

WPA1 session key type: TKIP

WPA2 and WPA3 session key types

AES: CCMP-128

WPA2 key management: Standard

Base rate: Auto

Client Bridge Support: No

TX bandwidth limit: 0 kbit/s

RX bandwidth limit: 0 kbit/s

Client TX bandwidth limit: 0 kbit/s

Client RX bandwidth limit: 0 kbit/s

Maximum count of clients: 0

Min. client signal strength: 0 %

Client disassociation sig. stre 0 %

□ Enable LBS tracking

LBS tracking list:

Convert to unicast: DHCP

□ Transmit only Unicasts, disallow Broad- and Multicast

□ (U-)APSD / WMM powersave activated

Encrypt mgmt. frames: No

802.11n

Max. spatial streams: Auto

☑ STBC (Space Time Block Coding) activated

☑ LDPC (Low Density Parity Check) activated

OK Cancel

Timeframe

Select one of the time frames defined in **WLAN controller** > **General** > **Time frame**. This can be used to restrict the broadcast of this SSID to the times defined there. This can be used, for example to activate a WLAN in a school only during class times. The time frame for the WLAN controller is configured in the same way as the settings in *Timeframe*.

10.3.1 Additions to the Setup menu

Timeframe

Select one of the time frames defined in *2.37.1.26 Timeframe* on page 165. This can be used to restrict the broadcast of this SSID to the times defined there. This can be used, for example to activate a WLAN in a school only during class times.

SNMP ID:

2.37.1.1.57

Console path:

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

Possible values:

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

Default:

empty

Timeframe

Time frames are used when a WLAN SSID should not be broadcast permanently. One profile may contain several lines with different timeframes. Different lines in a timeframe should complement one another, i.e. if you specify WORKTIME you will should probably specify a timeframe called FREETIME to cover the time outside of working hours.

SNMP ID:

2.37.1.26

Console path:

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

Name

Enter the name of the timeframe for referencing.

SNMP ID:

2.37.1.26.1

Console path:

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

Possible values:

Max. 31 characters from `` [A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ` ``

Default:

empty

Home

Here you set the start time (time of day) in the format HH:MM when the selected profile becomes valid.

SNMP ID:

2.37.1.26.2

Console path:

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

Possible values:

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

Default:

00:00

Stop

Here you set the end time (time of day) in the format HH:MM when the selected profile ceases to be valid.

A stop time from HH:MM normally goes to HH:MM:00, with the exception of stop time 00:00, which is interpreted as 23:59:59.

SNMP ID:

2.37.1.26.3

Console path:

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

Possible values:

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

Default:

00:00

Weekdays

Here you select the weekday on which the timeframe is to be valid.

SNMP ID:

2.37.1.26.4

Console path:

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

Possible values:

Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday, Holiday

Default:

Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday, Holiday

Holidays

This table contains the holidays that have been defined.

SNMP ID:

2.37.1.27

Console path:

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

Index

This describes the position of the entry in the table.

SNMP ID:

2.37.1.27.1

Console path:

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

Possible values:

0 … 9999

Default:

empty

Date

If you have created entries in the time control table that should apply on public holidays, enter the days here.

SNMP ID:

2.37.1.27.2

Console path:

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

Possible values:

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

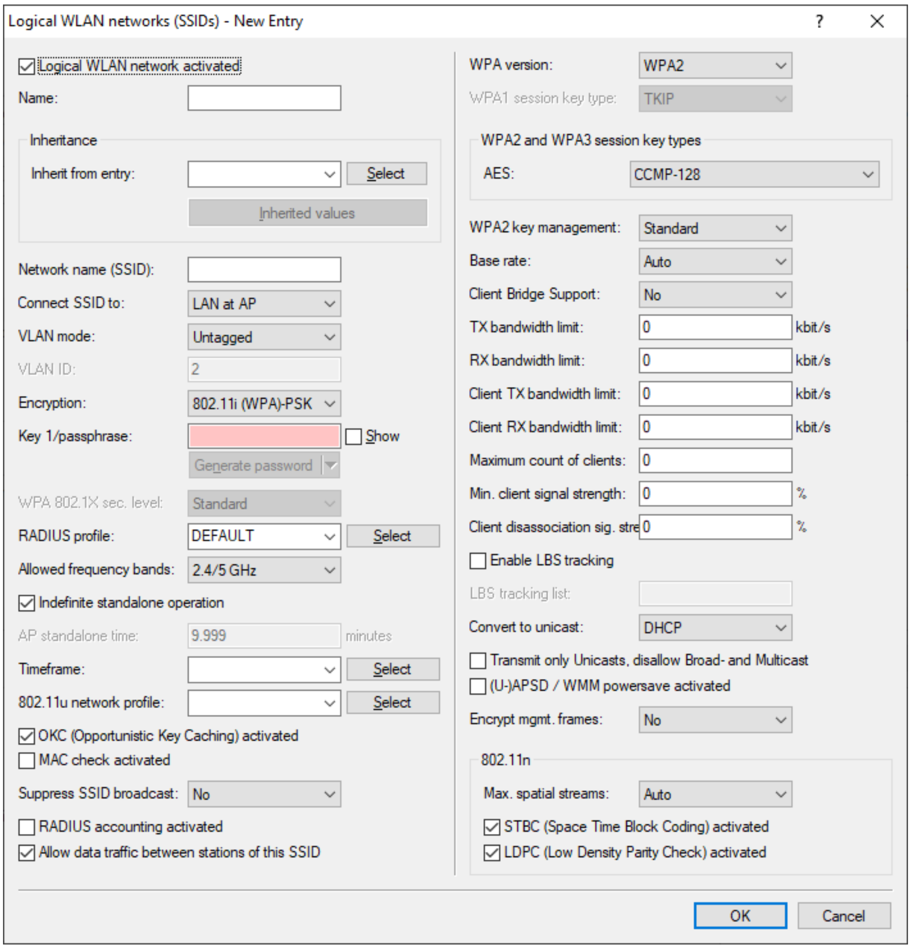
Default:

empty

10.4 Signal strength at which a client is disassociated

Similar to the feature described under *Signal strength at which a client is disassociated* on page 159, this option is also available for WLAN controllers.

You enter the threshold value for **Client disassociation signal strength** under **WLAN controller** > **Profiles** > **Logical WLAN networks**.



Logical WLAN networks (SSIDs) - New Entry

☑ Logical WLAN network activated

Name:

Inheritance

Inherit from entry: Select

Inherited values

Network name (SSID):

Connect SSID to: LAN at AP

VLAN mode: Untagged

VLAN ID: 2

Encryption: 802.11i (WPA)-PSK

Key 1/passphrase: □ Show

Generate password

WPA 802.1X sec. level: Standard

RADIUS profile: DEFAULT Select

Allowed frequency bands: 2.4/5 GHz

☑ Indefinite standalone operation

AP standalone time: 9.999 minutes

Timeframe: Select

802.11u network profile: Select

☑ OKC (Opportunistic Key Caching) activated

□ MAC check activated

Suppress SSID broadcast: No

□ RADIUS accounting activated

☑ Allow data traffic between stations of this SSID

WPA version: WPA2

WPA1 session key type: TKIP

WPA2 and WPA3 session key types

AES: CCMP-128

WPA2 key management: Standard

Base rate: Auto

Client Bridge Support: No

TX bandwidth limit: 0 kbit/s

RX bandwidth limit: 0 kbit/s

Client TX bandwidth limit: 0 kbit/s

Client RX bandwidth limit: 0 kbit/s

Maximum count of clients: 0

Min. client signal strength: 0 %

Client disassociation sig. stre 0 %

□ Enable LBS tracking

LBS tracking list:

Convert to unicast: DHCP

□ Transmit only Unicasts, disallow Broad- and Multicast

□ (U-)APSD / WMM powersave activated

Encrypt mgmt. frames: No

802.11n

Max. spatial streams: Auto

☑ STBC (Space Time Block Coding) activated

☑ LDPC (Low Density Parity Check) activated

OK Cancel

Client disassociation signal strength

If values drop below this threshold, the client is disassociated. This prevents the client from sticking with a WLAN connection that is actually unusable because of the poor signal rather than switching to a better cell phone connection—behavior that is all too common for mobile phones and can be very annoying for the user.

> This threshold only works if the value **Minimum client signal strength** is also set and the **Client disassociation signal strength** is less than this value.

10.4.1 Additions to the Setup menu

Min-Client-Disassoc-Strength

If values drop below this threshold, the client is disassociated. This prevents the client from sticking with a WLAN connection that is actually unusable because of the poor signal rather than switching to a better cell phone connection—behavior that is all too common for mobile phones and can be very annoying for the user.

> This threshold only works if the value *2.37.1.1.38 Min-Client-Strength* is also set and the Min-Stations-Disassoc-Strength is less than this value.

SNMP ID:

2.37.1.1.58

Console path:

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

Possible values:

0 … 100

Default:

0

11 Public Spot

11.1 Passpoint® Release 2

As of LCOS 10.40 you can use LANconfig to configure the extended Hotspot 2.0 feature Passpoint® Release 2 as specified by the Wi-Fi Alliance and supported by your WLAN device since LCOS 10.32 RU4. The RADIUS server in the LCOS has been equipped with the necessary features since 10.32 version RU4.

Passpoint® Release 2 simplifies the onboarding of devices into a network using the WPA2-Enterprise (802.1X) encryption method. A dedicated onboarding SSID allows a user with a device that supports Passpoint® Release 2 to install a profile and automatically switch to the encrypted network using the stored credentials. This helps to implement hotspots that provide encrypted wireless communication. An onboarding SSID can be used to give guests temporary access credentials.

Similarly, a mobile service provider can relieve the load on their cellular network by introducing Wi-Fi offloading and allowing mobile devices with a SIM card to automatically log into their WLAN network. Customers' devices find the WLAN network from the mobile service provider and automatically login to the operator's WLAN network using the user data stored on the SIM card.

Passpoint® Release 2 adds the following features to Hotspot 2.0:

- Online Sign-Up (OSU) – with Passpoint® Release 2, companies and network operators can use "Online Sign-Up" servers (OSU servers) to deliver profiles to their users. Using an open OSU SSID, users can identify various OSU servers by their icons and thus select the one that suits them best. The OSU server can optionally ask the user for credentials before providing a profile that best suits the user's device. In addition to the open OSU-SSID, an encrypted SSID can be used to exchange user data by means of "anonymous EAP-TLS". This requires the use of a RADIUS server that supports "anonymous EAP-TLS".

  ⓘ An OSU server is not included with LCOS. However, solutions are available from LANCOM partners.

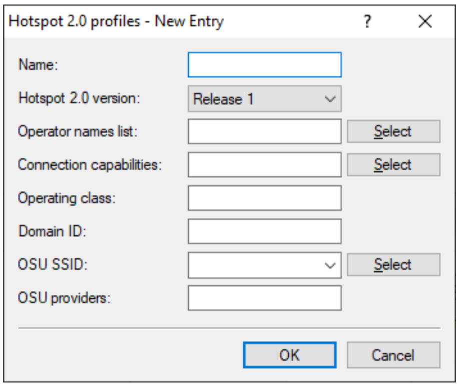
- OSU icons – icons corresponding to the supported OSU servers can be uploaded to the LCOS as files using the WEBconfig feature **File management**. We recommend PNG as the file format.
- Notification – the network can notify the user about an imminent logout from the RADIUS server. This may be the case if the user credentials have expired or if the specified connection duration has been reached.
- QoS Map – the "QoS Map Set" function enables an access point to instruct its clients to use a specific QoS map. This defines the values for the contention window (media access via EDCA) of the various access categories (voice, video, best effort and background data packets) and the corresponding DSCP parameters. At the same time, the access points also use the values stored in the QoS map.

  ⓘ Currently available are the two QoS maps required by the Wi-Fi-Alliance and the default QoS map of the LCOS.

11.1.1 Configuring Hotspot 2.0

Hotspot 2.0 profiles

Using this table you manage the profile lists for the Hotspot 2.0. **Hotspot 2.0 profiles** offer you the ability to group certain ANQP elements (from the Hotspot 2.0 specification) and to assign them to mutually independent logical WLAN interfaces in the table **Interfaces**. These include, for example, the operator-friendly name, the connection capabilities, operating class and WAN metrics. Some of the elements are located in other profile lists.



Hotspot 2.0 profiles - New Entry

Name:

Hotspot 2.0 version: Release 1

Operator names list:

Connection capabilities:

Operating class:

Domain ID:

OSU SSID:

OSU providers:

Hotspot 2.0 version

Set the Hotspot-2.0 release supported by this profile.

A client must support this release in order to connect.

Domain ID

The domain ID indicates which ANQP server is used. All access points and SSIDs with the same number/domain ID (16- value) use the same ANQP server.

A client sending an ANQP request to access points / SSIDs with the same domain ID would always receive the same response. To get different responses, the client would have to look for different domain IDs.

OSU SSID

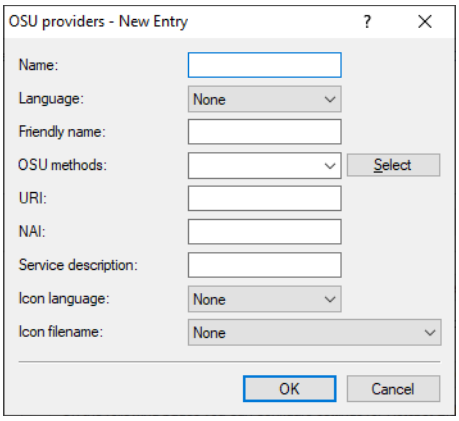
Name of the SSID that provides access to the OSU server.

OSU providers

List of OSU provider names in *OSU providers* on page 171 that are supported in the profile.

OSU providers

In this table, you configure the OSU providers for online sign-up with Passpoint® Release 2.



OSU providers - New Entry

Name:

Language: None

Friendly name:

OSU methods:

URI:

NAI:

Service description:

Icon language: None

Icon filename: None

Name

Give this OSU provider a name so that you can reference it later. By using the same name repeatedly, this provider can be used for several languages.

Language

Set the language supported by this OSU provider.

Friendly name

Give this OSU provider a descriptive name.

OSU methods

Set the OSU methods used by this OSU provider. Options are “OMA-DM” or “SOAP-XML-SPP”.

Available methods with the online sign-up server with Passpoint® Release 2:

- OMA – Open Mobile Alliance
- DM – Device Management
- SOAP – Simple Object Access Protocol
- XML – eXtended Markup Language
- SPP – Subscription Provisioning Protocol

URI

Enter a URI where a client can reach the OSU server.

NAI

Enter the Network Access Identifier (NAI) for this OSU provider.

Service description

Enter a descriptive text for this service here.

Icon language

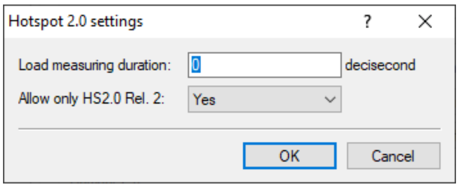
This item sets the language for the selected icon.

Icon-Filename

Select an icon for this OSU provider. Icons can be uploaded as files with WEBconfig by using the ***File management*** feature. We recommend PNG as the file format.

Hotspot 2.0 settings

This table is used to configure particular settings for Hotspot 2.0.



Hotspot 2.0 settings

Load measuring duration: 0 decisecond

Allow only HS2.0 Rel. 2: Yes

Load measuring duration

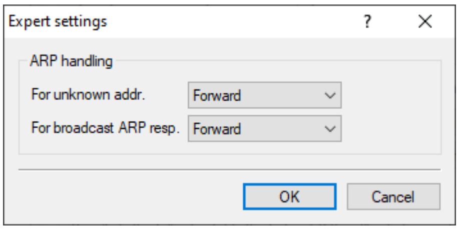
Measurement cycle for WAN downlink/uplink speeds in tenths of a second.

Allow only Hotspot 2.0 Release 2

A requirement of HotSpot 2.0 Release 2 is that it only allows Release 2 clients. This can be turned off with this switch.

Expert settings

This table is used to configure the expert settings for Hotspot 2.0. The settings in this menu are for suppressing ARP (IPv4) or Neighbor Solicitation (IPv6) between the clients within the SSID. An alternative solution would be to suppressing broadcast/multicasts via **Transmit only unicasts, suppress multicasts and broadcasts** in the logical WLAN network settings.



Expert settings

ARP handling

For unknown addr. Forward

For broadcast ARP resp. Forward

For unknown addresses

In case of an unknown address, the packet is either forwarded or discarded.

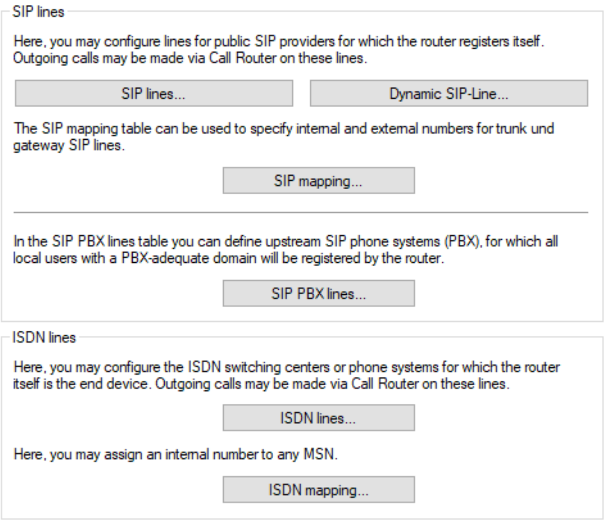
For broadcast ARP responses

In case of a broadcast, the packet is either forwarded or discarded.

12 Voice over IP – VoIP

12.1 Dynamic SIP lines

From LCOS 10.40 it is possible to set up dynamic SIP lines. The configuration is found under **Voice call manager** > **Lines** by clicking the button **Dynamic SIP line**.



SIP lines

Here, you may configure lines for public SIP providers for which the router registers itself. Outgoing calls may be made via Call Router on these lines.

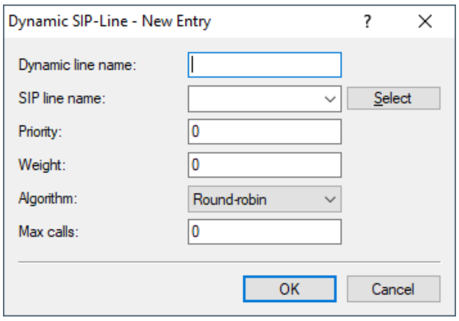
The SIP mapping table can be used to specify internal and external numbers for trunk und gateway SIP lines.

In the SIP PBX lines table you can define upstream SIP phone systems (PBX), for which all local users with a PBX-adequate domain will be registered by the router.

ISDN lines

Here, you may configure the ISDN switching centers or phone systems for which the router itself is the end device. Outgoing calls may be made via Call Router on these lines.

Here, you may assign an internal number to any MSN.



Dynamic SIP-Line - New Entry

Dynamic line name:	
SIP line name:	
Priority:	0
Weight:	0
Algorithm:	Round-robin
Max calls:	0

Dynamic line name

Enter the name for the dynamic line here. If the dynamic line consists of several physical lines, you can also use this dynamic line name for other table entries. This dynamic line name can later be used in the call routing table as the destination line.

SIP line name

Here you select one of the already configured physical SIP connections.

Priority

Here you specify the priority of the physical line for consideration when outgoing calls are distributed.

Weight

Here you specify the weighting of the physical line for consideration when outgoing calls are distributed.

Algorithm

The algorithm must be configured identically for all entries that belong to a dynamic line. The following algorithms can be used:

Weight

This algorithm controls the percentage of calls being distributed between different physical lines.

Round-Robin

With this algorithm, outgoing calls are distributed sequentially to the physical lines.

Priority

The physical line with the highest priority is fully utilized first, before the physical line with the next-lowest priority is used.

Max. calls

Here you enter how many simultaneous voice channels can be used on the physical SIP line. For no restriction on the number of voice channels, enter 0 here.

12.1.1 Additions to the Setup menu

Dynamic-Line

Configure the dynamic SIP lines here.

SNMP ID:

2.33.4.1.3

Console path:

Setup > **Voice-Call-Manager** > **Line** > **SIP-Provider**

Dynamic-Line-Name

Enter the name for the dynamic line here. If the dynamic line consists of several physical lines, you can also use this dynamic line name for other table entries. This dynamic line name can later be used in the call routing table as the destination line.

SNMP ID:

2.33.4.1.3.1

Console path:

Setup > **Voice-Call-Manager** > **Lines** > **SIP-Provider** > **Dynamic-Line**

Possible values:

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

SIP-Line-Name

Here you specify one of the already configured physical SIP connections.

SNMP ID:

2.33.4.1.3.2

Console path:

Setup > **Voice-Call-Manager** > **Lines** > **SIP-Provider** > **Dynamic-Line**

Possible values:

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

Priority

Here you specify the priority of the physical line for consideration when outgoing calls are distributed.

SNMP ID:

2.33.4.1.3.3

Console path:

Setup > **Voice-Call-Manager** > **Lines** > **SIP-Provider** > **Dynamic-Line**

Possible values:

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

Weight

Here you specify the weighting of the physical line for consideration when outgoing calls are distributed.

SNMP ID:

2.33.4.1.3.4

Console path:

Setup > **Voice-Call-Manager** > **Lines** > **SIP-Provider** > **Dynamic-Line**

Possible values:

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

Algorithm

The algorithm must be configured identically for all entries that belong to a dynamic line.

SNMP ID:

2.33.4.1.3.5

Console path:

Setup > **Voice-Call-Manager** > **Lines** > **SIP-Provider** > **Dynamic-Line**

Possible values:

Weight
This algorithm controls the percentage of calls being distributed between different physical lines.

Round-Robin
With this algorithm, outgoing calls are distributed sequentially to the physical lines.

Priority
The physical line with the highest priority is fully utilized first, before the physical line with the next-lowest priority is used.

Max-Calls

Here you enter how many simultaneous voice channels can be used on the physical SIP line. For no restriction on the number of voice channels, enter 0 here.

SNMP ID:

2.33.4.1.3.6

Console path:

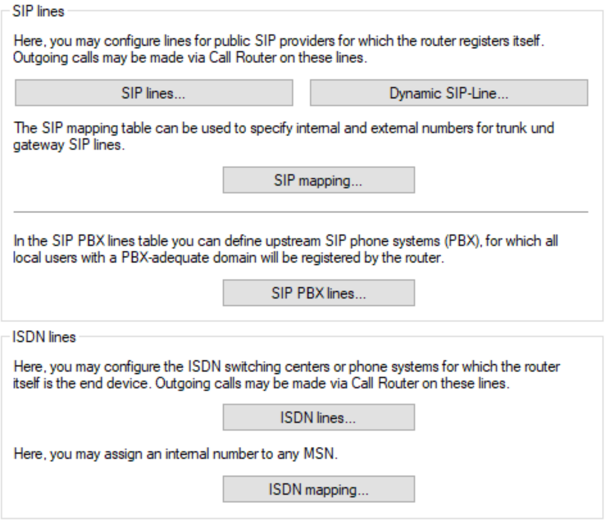
Setup > **Voice-Call-Manager** > **Lines** > **SIP-Provider** > **Dynamic-Line**

Possible values:

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

12.2 Flex mode

From LCOS 10.40 the new Flex mode for SIP lines is supported. The configuration is found under **Voice call manager** > **Lines** by clicking the button **SIP lines**.



SIP lines

Here, you may configure lines for public SIP providers for which the router registers itself. Outgoing calls may be made via Call Router on these lines.

SIP lines... | Dynamic SIP-Line...

The SIP mapping table can be used to specify internal and external numbers for trunk und gateway SIP lines.

SIP mapping...

In the SIP PBX lines table you can define upstream SIP phone systems (PBX), for which all local users with a PBX-adequate domain will be registered by the router.

SIP PBX lines...

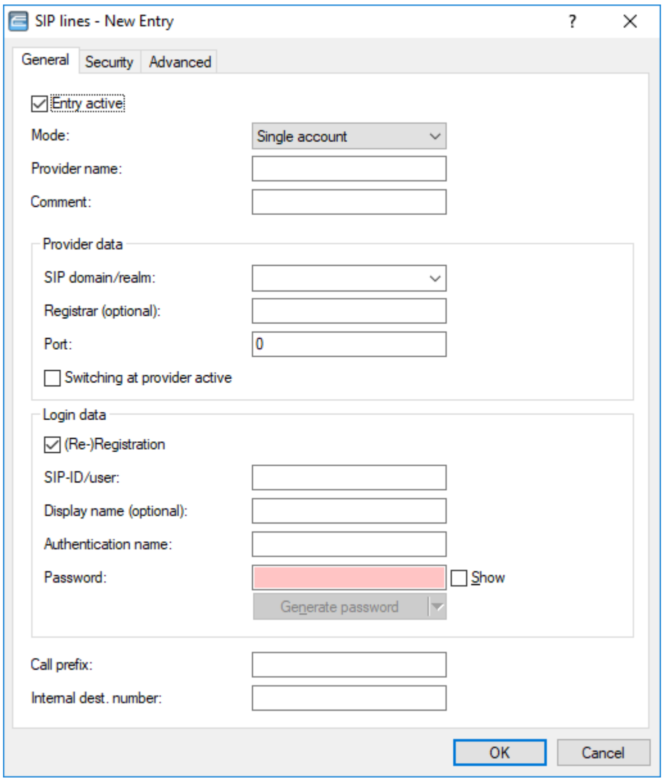
ISDN lines

Here, you may configure the ISDN switching centers or phone systems for which the router itself is the end device. Outgoing calls may be made via Call Router on these lines.

ISDN lines...

Here, you may assign an internal number to any MSN.

ISDN mapping...



SIP lines - New Entry

General | Security | Advanced

☑ Entry active

Mode: Single account

Provider name:

Comment:

Provider data

SIP domain/realm:

Registrar (optional):

Port: 0

□ Switching at provider active

Login data

☑ (Re-)Registration

SIP-ID/user:

Display name (optional):

Authentication name:

Password: □ Show

Generate password

Call prefix:

Internal dest. number:

OK | Cancel

Mode

Flex

- To the outside the line behaves like a commercially available SIP account with a single public number.

- The number is registered at the service provider and registration is refreshed on a regular basis.
- For outgoing calls, the calling-line number (sender) is not modified.
- For incoming calls the dialed number (destination) is not modified.
- The maximum number of connections at any one time is limited only by the available bandwidth.

12.2.1 Additions to the Setup menu

Mode

This selection specifies the operating mode of the SIP line.

> ⓘ The "Service provider" can be a server in the Internet, an IP PBX, or a voice gateway. Please observe the notices about "SIP mapping".

SNMP ID:

2.33.4.1.1.17

Console path:

Setup > **Voice-Call-Manager** > **Lines** > **SIP-Provider** > **Line**

Possible values:

Provider

Externally, the line behaves like a typical SIP account with a single public number. The number is registered with the service provider, the registration is refreshed at regular intervals (if (re-)registration has been activated for this SIP provider line). For outgoing calls, the calling-line number is replaced (masked) by the registered number. Incoming calls are sent to the configured internal destination number. Only one connection can exist at a time.

Trunk

Externally, the line acts like an extended SIP account with a main external telephone number and multiple extension numbers. The SIP ID is registered as the main switchboard number with the service provider and the registration is refreshed at regular intervals (if (re-)registration has been activated for this SIP provider line). For outgoing calls, the switchboard number acts as a prefix placed in front of each calling number (sender; SIP: “From:”). For incoming calls, the prefix is removed from the destination number (SIP: “To:”). The remaining digits are used as the internal extension number. In case of error (prefix not found, destination equals prefix) the call is forwarded to the internal destination number as configured. The maximum number of connections at any one time is limited only by the available bandwidth.

Gateway

Externally the line behaves like a typical SIP account with a single public number, the SIP ID. The number (SIP ID) is registered with the service provider and the registration is refreshed at regular intervals (if (re-)registration has been activated for this SIP provider line). For outgoing calls, the calling-line number (sender) is replaced (masked) by the registered number (SIP ID in SIP: “From:”) and sent in a separate field (SIP: “Contact:”). For incoming calls the dialed number (destination) is not modified. The maximum number of connections at any one time is limited only by the available bandwidth.

Link

Externally, the line behaves like a typical SIP account with a single public number (SIP ID). The number is registered with the service provider, the registration is refreshed at regular intervals (if (re-)registration has been activated for this SIP provider line). For outgoing calls, the calling-line number (sender; SIP:

"From:") is not modified. For incoming calls, the dialed number (destination; SIP: "To:") is not modified. The maximum number of connections at any one time is limited only by the available bandwidth.

Flex

- To the outside the line behaves like a commercially available SIP account with a single public number.
- The number is registered at the service provider and registration is refreshed on a regular basis.
- For outgoing calls, the calling-line number (sender) is not modified.
- For incoming calls the dialed number (destination) is not modified.
- The maximum number of connections at any one time is limited only by the available bandwidth.

Default:

Provider

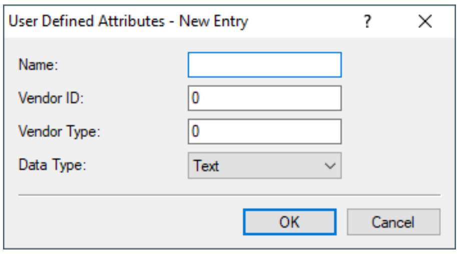
13 RADIUS

13.1 User-defined attributes

As of LCOS 10.40 your device supports user-defined RADIUS attributes.

RADIUS attributes are managed in what is known as a dictionary. LCOS supports many different attributes by default; however, there is a huge variety of manufacturer-specific attributes, which the administrator can enter into the LCOS configuration here. These attributes can then be used in the LCOS at any point where attributes can be added to a RADIUS request or response, e.g. in the RADIUS user management.

The user-defined attributes are configured via **RADIUS** > **Server** > **Extended configuration** > **User-defined attributes**



User Defined Attributes - New Entry

Name:

Vendor ID: 0

Vendor Type: 0

Data Type: Text

Name

The name used to reference the attribute in other places in LCOS.

Vendor ID

The specific vendor ID of the attribute.

Vendor type

The specific type ID of the attribute.

Data type

The data type of the attribute.

13.1.1 Additions to the Setup menu

User-Defined-Attributes

This directory is for user-defined attributes.

RADIUS attributes are managed in what is known as a dictionary. LCOS supports many different attributes by default; however, there is a huge variety of manufacturer-specific attributes, which the administrator can enter into the LCOS configuration here. These attributes can then be used in the LCOS at any point where attributes can be added to a RADIUS request or response, e.g. in the RADIUS user management.

SNMP ID:

2.25.22

Console path:

Setup > **RADIUS**

Attributes

Here you create the user-defined attributes for use with RADIUS servers.

SNMP ID:

2.25.22.1

Console path:

Setup > **RADIUS** > **User-Defined-Attributes**

Name

The name used to reference the attribute in other places in LCOS.

SNMP ID:

2.25.22.1.1

Console path:

Setup > **RADIUS** > **User-Defined-Attributes** > **Attributes**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]-_`

Vendor-ID

The specific vendor ID of the attribute.

SNMP ID:

2.25.22.1.2

Console path:

Setup > **RADIUS** > **User-Defined-Attributes** > **Attributes**

Possible values:

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

Vendor-Type

The specific type ID of the attribute.

SNMP ID:

2.25.22.1.3

Console path:

Setup > **RADIUS** > **User-Defined-Attributes** > **Attributes**

Possible values:

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

Data-Type

The specific type ID of the attribute.

SNMP ID:

2.25.22.1.4

Console path:

Setup > **RADIUS** > **User-Defined-Attributes** > **Attributes**

Possible values:

Text
Integer
IPv4-Address
IPv6-Address
Date

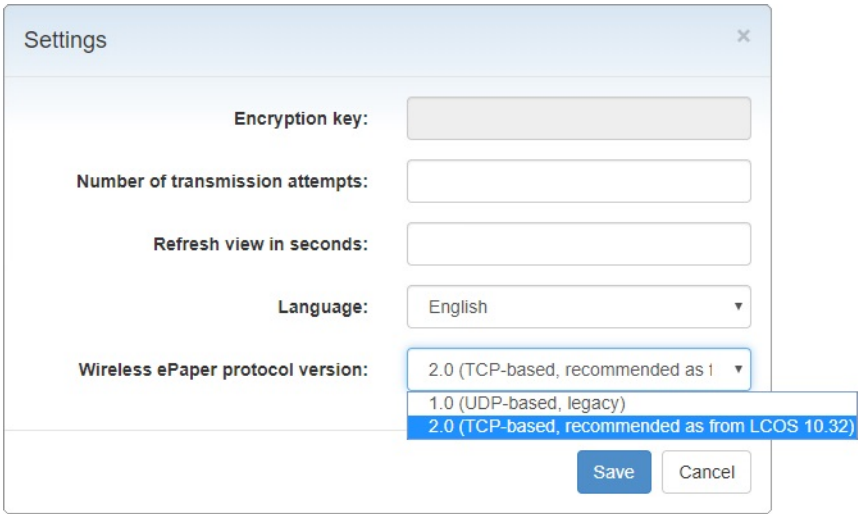
14 IoT – the Internet of Things

14.1 Wireless ePaper

Centralized management of your Wireless ePaper infrastructure

From LCOS 10.40 the LANCOM access points with Wireless ePaper support optionally use an extension of the TCP protocol that allows the establishment of TLS-encrypted connections (from Wireless ePaper access points, or routers with a USB interface and a Wireless ePaper USB stick) to the Wireless ePaper Server. To use this extension, both the Wireless ePaper Server and the Wireless ePaper device (access point or router with Wireless ePaper USB) have to be configured accordingly.

In the upper-right corner of the Wireless ePaper management, click on the gear-wheel icon to access the **general settings** for the Wireless ePaper Server. You can activate the new protocol here.



Settings

Encryption key:

Number of transmission attempts:

Refresh view in seconds:

Language: English

Wireless ePaper protocol version: 2.0 (TCP-based, recommended as f

1.0 (UDP-based, legacy)

2.0 (TCP-based, recommended as from LCOS 10.32)

In LANmonitor, the display of the device under **IoT** > **Wireless ePaper** > **Protocol version** displays the protocol that is in use:

- None – there is no connection to a controller/server
- ThinAP1.0/UDP – protocol version 1.0 (UDP-based, legacy)
- ThinAP2.0/TCP – protocol version 2.0 (TCP-based, from LCOS 10.32)
- ThinAP2.0/TLS – extension of protocol version 2.0 (TCP-based and encrypted, from LCOS 10.40)

Activating a TCP-based protocol on the Wireless ePaper Server

The Wireless ePaper Server supports “protocol version 2.0” as of version 1.91 and the TLS encryption based on it as of version 1.101. If you already use a supported Wireless ePaper Server and yet only “protocol version 1.0” or, from version 1.101 only “protocol version 2.0” is displayed here, the protocol was probably not yet enabled in the settings for the Wireless ePaper server. In this case you first have to activate the protocol version.

Follow these steps to activate “protocol version 2.0 (ThinAP2.0/TCP)”:

1. Check the following prerequisites:
   - LANCOM Wireless ePaper Server version 1.91 or higher is installed
   - cURL is installed

2. Open the command line on your operating system and enter the following command:

   ```
   curl -X PUT http://<server-ip>:8001/service/configuration/lancomUseTcpThinMode?value=true
   ```

3. Restart the Wireless ePaper Server.
4. Then enter the following command to verify that the feature was successfully enabled:

   ```
   curl -X GET http://<server-ip>:8001/service/configuration/lancomUseTcpThinMode
   ```

If activation was successful the output is as follows:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Configuration key="lancomUseTcpThinMode" type="BOOLEAN" defaultValue="false" value="true"/>
```

Follow these steps to activate “protocol version 2.0 (ThinAP2.0/TLS)”:

1. Check the following prerequisites:
   - LANCOM Wireless ePaper Server version 1,101 or higher is installed
   - cURL is installed
   - “Protocol version 2.0 (ThinAP2.0/TCP)” is activated
2. Open the command line on your operating system and enter the following command:

   [illegible]

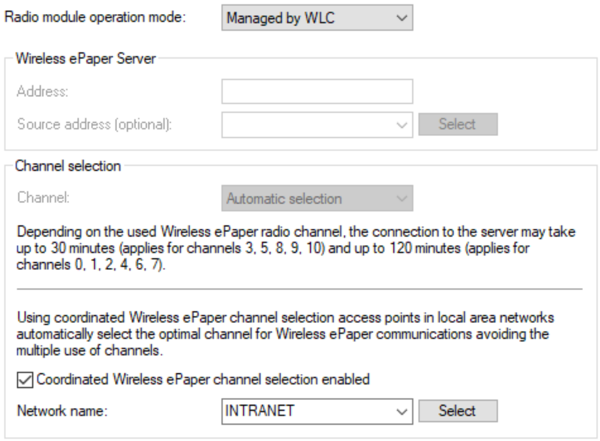
3. Restart the Wireless ePaper Server.
4. Then, as with the TCP protocol check, enter all three parameters with “GET” as the command to check whether the activation was successful. The output must be “`value="true"`”

To deactivate the function on the command line, enter the commands with the parameter “`value=false`” instead of the parameter “`value=true`”. The command would look like this:

```
curl -X PUT http://<server-ip>:8001/service/configuration/lancomUseTcpThinMode?value=false
```

14.1.1 Settings for Wireless ePaper

Activate the Wireless ePaper radio module in LANconfig under **IoT** > **Wireless ePaper**,



Radio module operation mode: Managed by WLC

Wireless ePaper Server

Address:

Source address (optional): Select

Channel selection

Channel: Automatic selection

Depending on the used Wireless ePaper radio channel, the connection to the server may take up to 30 minutes (applies for channels 3, 5, 8, 9, 10) and up to 120 minutes (applies for channels 0, 1, 2, 4, 6, 7).

Using coordinated Wireless ePaper channel selection access points in local area networks automatically select the optimal channel for Wireless ePaper communications avoiding the multiple use of channels.

☑ Coordinated Wireless ePaper channel selection enabled

Network name: INTRANET Select

Wireless ePaper Server

From LCOS 10.40 the LANCOM access points with Wireless ePaper support optionally use an extension of the TCP protocol that allows the establishment of TLS-encrypted connections (from Wireless ePaper access points, or routers with a USB interface and a Wireless ePaper USB stick) to the Wireless ePaper Server. The ThinAP2.0/TLS protocol must be set up on the Wireless ePaper Server and the IP address of the Wireless ePaper Server must be specified here.

Address

IP address of the Wireless ePaper Server.

Source address

Enter loopback address here.

14.2 Additions to the Setup menu

14.2.1 Outbound-Server

IP address of the Wireless ePaper Server.

SNMP ID:

2.111.88.5

Console path:

Setup > **IoT** > **Wireless-ePaper**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9].-:%`

14.2.2 SSL

This menu contains the parameters for the TLS authentication.

SNMP ID:

2.111.88.6

Console path:

Setup > **IoT** > **Wireless-ePaper**

Versions

This entry specifies which versions of the protocol are allowed.

SNMP ID:

2.111.88.6.1

Console path:

Setup > **IoT** > **Wireless-ePaper** > **SSL**

Possible values:

SSLv3
TLSv1
TLSv1.1
TLSv1.2

Default:

TLSv1.2

Keyex-Algorithms

This entry specifies which key-exchange methods are available.

SNMP ID:

2.111.88.6.2

Console path:

Setup > **IoT** > **Wireless-ePaper** > **SSL**

Possible values:

RSA
DHE
ECDHE

Default:

RSA

DHE

ECDHE

Crypto-Algorithms

This bitmask specifies which cryptographic algorithms are allowed.

SNMP ID:

2.111.88.6.3

Console path:

Setup > **IoT** > **Wireless-ePaper** > **SSL**

Possible values:

RC4-40
RC4-56
RC4-128
DES40
DES
3DES
AES-128
AES-256
AESGCM-128
AESGCM-256
Chacha20-Poly1305

ChaCha20 data stream encryption in conjunction with the Poly1305 Authenticator, see *RFC 7634*.

Default:

3DES

AES-128

AES-256

AESGCM-128

AESGCM-256

Chacha20-Poly1305

Hash-Algorithms

This entry specifies which hash algorithms are allowed and implies which HMAC algorithms are used to protect of the message integrity.

SNMP ID:

2.111.88.6.4

Console path:

Setup > **IoT** > **Wireless-ePaper** > **SSL**

Possible values:

MD5
SHA1
SHA2-256
SHA2-384

Default:

MD5

SHA1

SHA2-256

SHA2-384

Prefer-PFS

When setting the cipher suite, the device usually takes over the same setting as the requesting client. Certain client applications by default require a connection without perfect forward secrecy (PFS), even though both the device and the client are PFS-capable.

This option means that your device always prefers to connect with PFS, regardless of the default setting of the client.

SNMP ID:

2.111.88.6.5

Console path:

Setup > **IoT** > **Wireless-ePaper** > **SSL**

Possible values:

No
Yes

Default:

Yes

Renegotiations

With this setting you control whether the client can trigger a renegotiation of SSL/TLS.

SNMP ID:

2.111.88.6.6

Console path:

Setup > **IoT** > **Wireless-ePaper** > **SSL**

Possible values:

Forbidden

The device disconnects from the remote station if this requests a renegotiation.

Allowed

The device permits renegotiations with the remote station.

Ignored

The device ignores the request to renegotiate sent by the remote station.

Default:

Ignored

Elliptic-Curves

Here you specify which elliptic curves are to be used for encryption.

SNMP ID:

2.111.88.6.7

Console path:

Setup > **IoT** > **Wireless-ePaper** > **SSL**

Possible values:

secp256r1

secp256r1 is used for encryption.

secp384r1

secp384r1 is used for encryption.

secp521r1

secp521r1 is used for encryption.

ecdh_x25519

ecdh_x25519 is used for encryption.

Default:

secp256r1

secp384r1

secp521r1

ecdh_x25519

Signature-Hash-Algorithms

Use this entry to specify which hash algorithm is used to encrypt the signature.

SNMP ID:

2.111.88.6.21

Console path:

Setup > **IoT** > **Wireless-ePaper** > **SSL**

Possible values:

MD5-RSA
SHA1-RSA
SHA224-RSA
SHA256-RSA
SHA384-RSA
SHA512-RSA
SHA256-ECDSA
SHA384-ECDSA
SHA512-ECDSA

Default:

SHA256-RSA

SHA384-RSA

SHA512-RSA

SHA256-ECDSA

SHA384-ECDSA

SHA512-ECDSA

14.2.3 Loopback-Address

Enter loopback address here.

SNMP ID:

2.111.88.7

Console path:

Setup > **IoT** > **Wireless-ePaper**

Possible values:

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

Default:

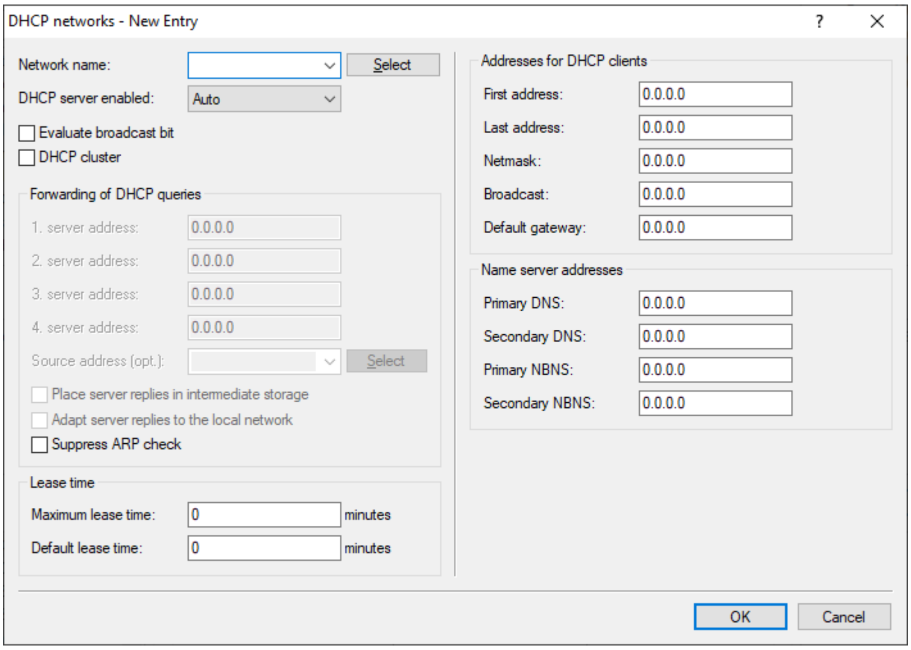
empty

15 Other services

15.1 DHCP server – suppress ARP request

From LCOS 10.40 the option to suppress the ARP request before assigning an IP address, available on the CLI since LCOS 10.32 RU4, is now also available in LANconfig.

The corresponding parameter is located under **IPv4** > **DHCPv4** > **DHCP networks**.



DHCP networks - New Entry

Network name: [ ] Select

DHCP server enabled: Auto

□ Evaluate broadcast bit

□ DHCP cluster

Forwarding of DHCP queries

1. server address: 0.0.0.0

2. server address: 0.0.0.0

3. server address: 0.0.0.0

4. server address: 0.0.0.0

Source address (opt.): [ ] Select

□ Place server replies in intermediate storage

□ Adapt server replies to the local network

□ Suppress ARP check

Lease time

Maximum lease time: 0 minutes

Default lease time: 0 minutes

Addresses for DHCP clients

First address: 0.0.0.0

Last address: 0.0.0.0

Netmask: 0.0.0.0

Broadcast: 0.0.0.0

Default gateway: 0.0.0.0

Name server addresses

Primary DNS: 0.0.0.0

Secondary DNS: 0.0.0.0

Primary NBNS: 0.0.0.0

Secondary NBNS: 0.0.0.0

Suppress ARP check

Before the DHCP server assigns an IP address, an ARP request is usually used to check whether the address has been assigned already. If there is no response to the ARP request within 3 seconds, the assignment goes ahead. This query is especially useful when computers are booting in normal networks that use fixed IP addresses. In a Public Spot network where, for example, a smartphone has to recognize that there is no Internet connection in order to display the login popup, this ARP request leads to an unnecessary delay. For scenarios such as this, this check can be disabled here.

15.2 DHCP-client option Classless Static Route

The DHCPv4 option Classless Static Route allows a DHCP server to pass a list of static routes to a DHCP client, which then enters those routes into its routing table. The routes in this list are “Classless”, i.e. a subnet mask or prefix length is transmitted for each route. According to RFC 3442, the option number 121 is used for this purpose.

On receiving this list, the DHCP client does not install a default route to the specified router, but only the list of the static routes in its routing table.

This feature is used, for example, by ISPs in scenarios where multiple virtual connections are separated by VLAN according to the individual service, e.g. with one VLAN each for Internet, VoIP and IPTV. In this case, the default route is used for the Internet connection (e.g. via PPPoE or DHCP), while the routes for IPTV are directed via a different VLAN as communicated by DHCP Classless Static Route Option.

By default, the LANCOM DHCPv4 client requests both the router option and the "Classless Static Routes" option. If the DHCP server sends a "Classless Static Routes" option, the client ignores any router option and only installs the list of routes. This behavior conforms with RFC 3442.

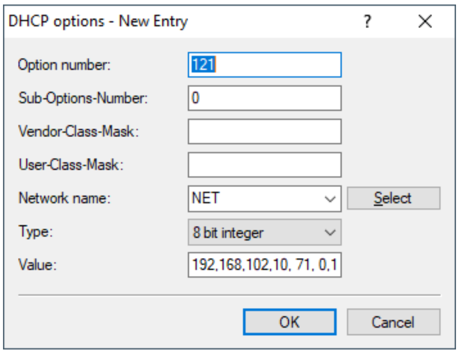
For a provider scenario with IPTV, you create a new DSL remote site with hold time 9999, layer DHCPOE and the corresponding VLAN according to provider specifications. Activate the switch **Establish remote site even without route (keepalive without route)** under **Communication** > **Remote Sites**. No entries are required in the routing table as the DHCP client provides the necessary routes by means of the "Classless Static Route" option.

The LANCOM DHCP server can also use a user-defined option to assign the "Classless Static Route" option to DHCP clients.

Example: Transmit "Classless Static Route" option in the DHCP server

To transmit the route 192.168.102.0/24 via 10.71.0.1 as a Classless Static Route Option (121) in the DHCP server, place the following entry in the table **IPv4** > **DHCPv4** > **DHCP options**:

- **Option number** – 121
- **Network name** – name of the network to which the option should be transmitted to clients.
- **Type** – 8-bit integer
- **Value** – 24,192,168,102,10, 71, 0,1



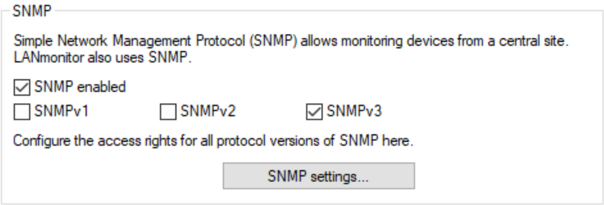
DHCP options - New Entry

Option number:	121
Sub-Options-Number:	0
Vendor-Class-Mask:	
User-Class-Mask:	
Network name:	NET
Type:	8 bit integer
Value:	192,168,102,10, 71, 0,1

15.3 Simple Network Management Protocol (SNMP)

15.3.1 Configuring SNMP

In LANconfig you configure SNMP under **Logging/Monitoring** > **Protocols** in the section **SNMP**.



SNMP

Simple Network Management Protocol (SNMP) allows monitoring devices from a central site. LANmonitor also uses SNMP.

☑ SNMP enabled

□ SNMPv1 □ SNMPv2 ☑ SNMPv3

Configure the access rights for all protocol versions of SNMP here.

SNMP enabled

Enable SNMP for the SNMP protocol versions specified below, which the device should support for SNMP requests and SNMP traps.

SNMPv1

Enables SNMPv1.

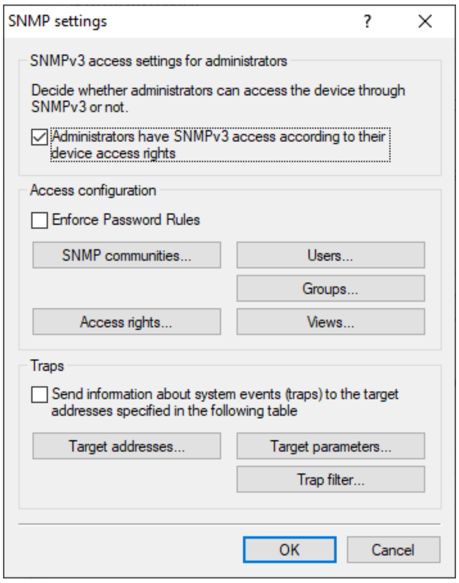
SNMPv2

Enables SNMPv2c.

SNMPv3

Enables SNMPv3.

Click on **SNMP settings** to open the configuration settings.



SNMPv3 access settings for administrators

Decide whether administrators can access the device through SNMPv3 or not.

☑ Administrators have SNMPv3 access according to their device access rights

Access configuration

□ Enforce Password Rules

Traps

□ Send information about system events (traps) to the target addresses specified in the following table

SNMP settings

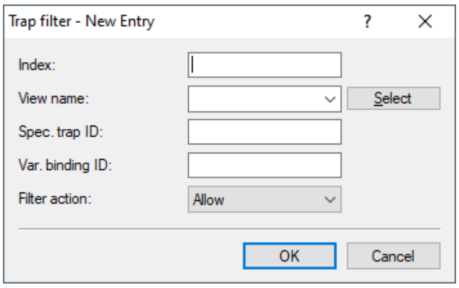
Traps

If you enable the option **Send information about system events (traps) to the target addresses specified in the following table**, the recipients configured under **Target addresses** and **Target parameters** will receive the corresponding information. The system events that trigger a message can be restricted by trap filters.

Trap filter

Certain SNMP traps or even large numbers of SNMP traps can be unwanted on the receiving servers. For this reason, as of LCOS 10.40 you can add an SNMP filter list that allows you to selectively pass or withhold SNMP traps based on their manufacturer-specific OIDs or the OIDs contained in the variable bindings.

Traps for the user “root” cannot be filtered. Filtering requires the use of a separate SNMP user.



Index:
View name:
Spec. trap ID:
Var. binding ID:
Filter action: Allow

Index

The position of this entry in the filter list. The list is checked from the smallest to the largest value until the first

hit.

View name

The **View name** is the name of a **view** that this filter rule applies to. If **Access to subtree** for the relevant view is set to “added”, the corresponding traps can be prevented by the **filter action** “deny” in a related filter rule. However, if **Access to subtree** of the relevant view is set to “removed”, the **filter action** “Allow” still sends the messages as an exception. Since the **views** can contain multiple entries of the same name with different access settings, it must be possible to set the **filter action** irrespective of the value of the corresponding setting for **Access to subtree**.

Spec. trap ID

Specifies a certain trap ID that can contain wildcards and ranges. An empty entry applies to all specific trap IDs of the device. See the examples in the following table.

OID	Description
	Applies to every OID.
1.2.3	Applies to all OIDs that start with “1.2.3”.
1.*.3	Applies to all OIDs that start with “1”, then contain any value, and then continue with “3”.
1.2-3.4	Applies to all OIDs that start with “1”, continue with a number ranging from “2 to 3”, and then a “4”.
1.2.3-4,7-8	Applies to all OIDs that start with “1.2” and continue with a number ranging from “3 to 4” or “7 to 8”.

Wildcards and ranges can occur anywhere in an OID, and an OID may also contain multiple wildcards or ranges. However, each position may only contain either a wildcard or a range.

A LANCOM device maps the generic trap OIDs of the SNMP protocol to certain vendor-specific OIDs:

Name	Generic OID	OID at LANCOM
coldStart	0	1.3.6.1.6.3.1.1.5.1
warmStart	1	1.3.6.1.6.3.1.1.5.2
linkDown	2	1.3.6.1.6.3.1.1.5.3
linkUp	3	1.3.6.1.6.3.1.1.5.4

Name	Generic OID	OID at LANCOM
authenticationFailure	4	1.3.6.1.6.3.1.1.5.5
egpNeighborLoss	5	1.3.6.1.6.3.1.1.5.6

Var. Binding ID

Specifies an OID that must be in the trap's variable bindings, which in turn may contain wildcards and ranges. Also see **Spec. trap ID**, An empty entry applies to all variable bindings of the device.

Filter action

In case of a match with the set IDs, you can either "Allow" the trap to so send it, or "Deny" it so that it is discarded.

Additions to the Setup menu

Filter

Certain SNMP traps or even large numbers of SNMP traps can be unwanted on the receiving servers. For this reason, you can add an SNMP filter list that allows you to selectively pass or withhold SNMP traps based on their manufacturer-specific OIDs or the OIDs contained in the variable bindings.

Traps for the user "root" cannot be filtered. Filtering requires the use of a separate SNMP user.

SNMP ID:

2.9.42

Console path:

Setup > **SNMP**

Index

The position of this entry in the filter list. The list is checked from the smallest to the largest value until the first hit.

SNMP ID:

2.9.42.1

Console path:

Setup > **SNMP** > **Filter**

Possible values:

Max. 4 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.``

View-Name

Enter the name of a view under **Setup** > **SNMP** > **Filters** > **View-Name** that this filter rule should apply to. If access in the value **Setup** > **SNMP** > **Filters** > **Type** is set to "Included" for this view, the corresponding traps can be prevented with the **filter action** "Prohibit" by means of a corresponding filter rule. However, if the corresponding access is set to

"Excluded", the filter action "Allow" will continue to send the messages as an exception. Since the views can contain multiple entries of the same name with different access settings, it must be possible to set the filter action irrespective of the value set for **Setup** > **SNMP** > **Filters** > **Type**.

SNMP ID:

2.9.42.2

Console path:

Setup > **SNMP** > **Filter**

Possible values:

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

Spec.-TrapID

Specifies a certain trap ID that can contain wildcards and ranges. An empty entry applies to all specific trap IDs of the device. See the examples in the following table.

OID	Description
	Applies to every OID.
1.2.3	Applies to all OIDs that start with "1.2.3".
1.*.3	Applies to all OIDs that start with "1", then contain any value, and then continue with "3".
1.2-3.4	Applies to all OIDs that start with "1", continue with a number ranging from "2 to 3", and then a "4".
1.2.3-4,7-8	Applies to all OIDs that start with "1.2" and continue with a number ranging from "3 to 4" or "7 to 8".

Wildcards and ranges can occur anywhere in an OID, and an OID may also contain multiple wildcards or ranges. However, each position may only contain either a wildcard or a range.

A LANCOM device maps the generic trap OIDs of the SNMP protocol to certain vendor-specific OIDs:

Name	Generic OID	OID at LANCOM
coldStart	0	1.3.6.1.6.3.1.1.5.1
warmStart	1	1.3.6.1.6.3.1.1.5.2
linkDown	2	1.3.6.1.6.3.1.1.5.3
linkUp	3	1.3.6.1.6.3.1.1.5.4
authenticationFailure	4	1.3.6.1.6.3.1.1.5.5
egpNeighborLoss	5	1.3.6.1.6.3.1.1.5.6

SNMP ID:

2.9.42.3

Console path:

Setup > **SNMP** > **Filter**

Possible values:

Max. 128 characters from `[0-9],-*.`

Var.BindingID

Specifies an OID that must be in the trap's variable bindings, which in turn may contain wildcards and ranges. An empty entry applies to all variable bindings of the device. See the examples in the following table.

OID	Description
	Applies to every OID.
1.2.3	Applies to all OIDs that start with "1.2.3".
1.*.3	Applies to all OIDs that start with "1", then contain any value, and then continue with "3".
1.2-3.4	Applies to all OIDs that start with "1", continue with a number ranging from "2 to 3", and then a "4".
1.2.3-4,7-8	Applies to all OIDs that start with "1.2" and continue with a number ranging from "3 to 4" or "7 to 8".

! Wildcards and ranges can occur anywhere in an OID, and an OID may also contain multiple wildcards or ranges. However, each position may only contain either a wildcard or a range.

SNMP ID:

2.9.42.4

Console path:

Setup > **SNMP** > **Filter**

Possible values:

Max. 128 characters from `[0-9],-*.`

Filter-Action

In case of a match with the set OID, you can either "Allow" the trap to send it, or "Deny" it so that it is discarded.

SNMP ID:

2.9.42.5

Console path:

Setup > **SNMP** > **Filter**

Possible values:

Allow
Deny

15.4 Netflow / IPFIX

NetFlow is a feature that allows network devices such as routers or switches to export information about their inbound and outbound IP traffic. The so-called IP flows are transmitted by UDP. An IP flow contains information about the source IP address, destination IP address, ports, timestamp and packet counters, among others. This information is received, stored and processed on a NetFlow collector. NetFlow can be used either permanently or temporarily for network analysis.

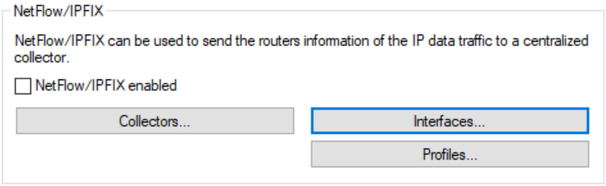
LANCOM supports the standards NetFlow 9 (*RFC 3954*) as well as IPFIX (*RFC 7011*), which is an extension of NetFlow Version 9, via the transport protocol UDP.

Notes on use:

- You need an external NetFlow collector that supports NetFlow 9 or IPFIX.
- The firewall must be activated.
- The only flow information collected with IPv4 is that being passed from one logical interface to another logical interface. Packets generated by or addressed to the router itself are not captured. For IPv6, this restriction does not apply.
- Only unicast IP flow information is collected, multicast (e.g. IPTV) is not supported.
- Depending on the scenario, using NetFlow/IPFIX increases CPU load and reduces the overall performance of the router.

15.4.1 Configuring NetFlow / IPFIX

In LANconfig you configure NetFlow/IPFIX under **Logging/Monitoring** > **Protocols** in the section **NetFlow/IPFIX**.



NetFlow/IPFIX

NetFlow/IPFIX can be used to send the routers information of the IP data traffic to a centralized collector.

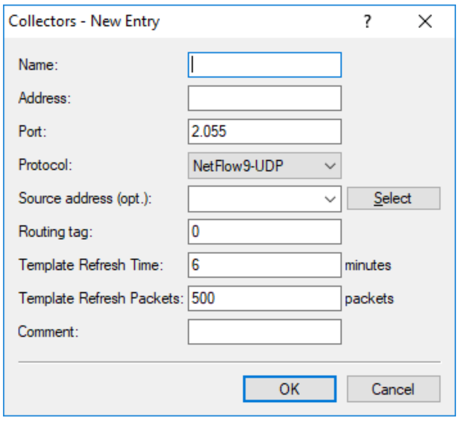
☐ NetFlow/IPFIX enabled

NetFlow/IPFIX enabled

Enable NetFlow/IPFIX on the device.

Collectors

You can configure the collectors for NetFlow/IPFIX under **Logging/Monitoring** > **Protocols** > **NetFlow/IPFIX** > **Collectors**.



Collectors - New Entry

Name:		
Address:		
Port:	2.055	
Protocol:	NetFlow9-UDP	
Source address (opt.):		Select
Routing tag:	0	
Template Refresh Time:	6	minutes
Template Refresh Packets:	500	packets
Comment:		

Name

Unique name of the NetFlow collector. This name is referenced in other tables.

Address

IPv4, IPv6 address or host name of the collector.

Port

NetFlow collector port. Usually port 2055 for NetFlow 9 and 4739 for IPFIX.

Protocol

Protocol version used by the NetFlow collector. Possible values are NetFlow 9 over UDP or IPFIX over UDP.

Source address

Optionally, specify a source address.

Routing tag

Specify a routing tag if a particular route is to be used to the collector.

Template refresh time

Specifies the time in minutes after which a NetFlow template record is refreshed. The value 0 deactivates the periodic refresh of template records.

ⓘ A NetFlow template packet is refreshed either after the specified time in minutes or after the corresponding number of Flow packets, whichever comes first.

Template refresh packets

Specifies the number of packets after which a NetFlow template record is refreshed. The value 0 deactivates the refresh of template records based on a packet counter.

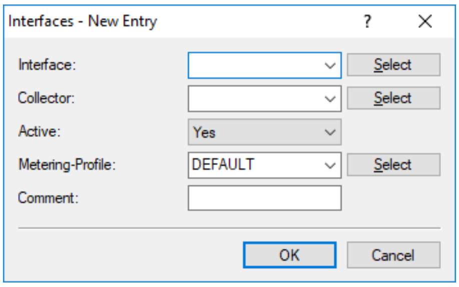
ⓘ A NetFlow template packet is refreshed either after the specified time in minutes or after the corresponding number of Flow packets, whichever comes first.

Comment

Optionally enter a meaningful comment as a description.

Interfaces

You can configure the interfaces for NetFlow/IPFIX under **Logging/Monitoring** > **Protocols** > **NetFlow/IPFIX** > **Interfaces**.



Interfaces - New Entry

Interface:

Collector:

Active: Yes

Metering-Profile: DEFAULT

Comment:

Interface

Logical interface on which NetFlow/IPFIX is to be activated. Possible values: IPv4, IPv6 LAN interfaces, remote sites, IPv6 RAS template. IPv4 remote sites can use a wildcard, e.g. Company*

Collector

This references an entry in the list of collectors.

Active

Enables/disables NetFlow/IPFIX for this entry for the interface and the collector.

Metering profile

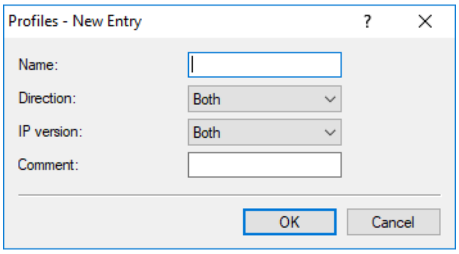
This references an entry in the Profiles list.

Comment

Optionally enter a meaningful comment as a description.

Profiles

You can configure the profiles for NetFlow/IPFIX under **Logging/Monitoring** > **Protocols** > **NetFlow/IPFIX** > **Profiles**.



Profiles - New Entry

Name:

Direction: Both

IP version: Both

Comment:

Name

Unique name of the metering profile. This name is referenced in other tables.

Direction

IP flow direction to be monitored by NetFlow/IPFIX. Possible values from the perspective of NetFlow/IPFIX: Ingress, Egress, Both

IP version

IP protocol version(s) to be monitored by NetFlow/IPFIX, possible values: IPv4, IPv6, Both

Comment

Optionally enter a meaningful comment as a description.

15.4.2 Additions to the Setup menu

NetFlow

NetFlow is a feature that allows network devices such as routers or switches to export information about their inbound and outbound IP traffic. The so-called IP flows are transmitted by UDP. An IP flow contains information about the source IP address, destination IP address, ports, timestamp and packet counters, among others. This information is received, stored and processed on a NetFlow collector. NetFlow can be used either permanently or temporarily for network analysis.

LANCOM supports the standards NetFlow 9 (*RFC 3954*) as well as IPFIX (*RFC 7011*), which is an extension of NetFlow Version 9, via the transport protocol UDP.

Notes on use:

- You need an external NetFlow collector that supports NetFlow 9 or IPFIX.
- The firewall must be activated.
- The only flow information collected with IPv4 is that being passed from one logical interface to another logical interface. Packets generated by or addressed to the router itself are not captured. For IPv6, this restriction does not apply.
- Only unicast IP flow information is collected, multicast (e.g. IPTV) is not supported.
- Depending on the scenario, using NetFlow/IPFIX increases CPU load and reduces the overall performance of the router.

SNMP ID:

2.109

Console path:

Setup

Collectors

Configure the collectors for NetFlow/IPFIX here.

SNMP ID:

2.109.1

Console path:

Setup > **NetFlow**

Name

Unique name of the NetFlow collector. This name is referenced in other tables.

SNMP ID:

2.109.1.1

Console path:

Setup > **NetFlow** > **Collectors**

Possible values:

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

Address

IPv4, IPv6 address or host name of the collector.

SNMP ID:

2.109.1.2

Console path:

Setup > **NetFlow** > **Collectors**

Possible values:

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

Port

NetFlow collector port. Usually port 2055 for NetFlow 9 and 4739 for IPFIX.

SNMP ID:

2.109.1.3

Console path:

Setup > **NetFlow** > **Collectors**

Possible values:

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

Protocol

Protocol version used by the NetFlow collector.

SNMP ID:

2.109.1.4

Console path:

Setup > **NetFlow** > **Collectors**

Possible values:

IPFIX-UDP
NetFlow9-UDP

Loopback-Addr.

Optionally, specify a source address.

SNMP ID:

2.109.1.5

Console path:

Setup > **NetFlow** > **Collectors**

Possible values:

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

Rtg-Tag

Specify a routing tag if a particular route is to be used to the collector.

SNMP ID:

2.109.1.6

Console path:

Setup > **NetFlow** > **Collectors**

Possible values:

0 … 65535

Default:

0

Template-Refresh-Time

Specifies the time in minutes after which a NetFlow template record is refreshed. The value 0 deactivates the periodic refresh of template records.

A NetFlow template packet is refreshed either after the specified time in minutes or after the corresponding number of Flow packets, whichever comes first.

SNMP ID:

2.109.1.7

Console path:

Setup > **NetFlow** > **Collectors**

Possible values:

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

Template-Refresh-Packets

Specifies the number of packets after which a NetFlow template record is refreshed. The value 0 deactivates the refresh of template records based on a packet counter.

ⓘ A NetFlow template packet is refreshed either after the specified time in minutes or after the corresponding number of Flow packets, whichever comes first.

SNMP ID:

2.109.1.8

Console path:

Setup > **NetFlow** > **Collectors**

Possible values:

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

Comment

Optionally enter a meaningful comment as a description.

SNMP ID:

2.109.1.99

Console path:

Setup > **NetFlow** > **Collectors**

Possible values:

Max. 50 characters from ``[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ` ``

Interfaces

Configure the interfaces for NetFlow/IPFIX here.

SNMP ID:

2.109.2

Console path:

Setup > **NetFlow**

Ifc

Logical interface on which NetFlow/IPFIX is to be activated. Possible values: IPv4, IPv6 LAN interfaces, remote sites, IPv6 RAS template. IPv4 remote sites can use a wildcard, e.g. Company*

SNMP ID:

2.109.2.1

Console path:

Setup > **NetFlow** > **Interfaces**

Possible values:

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

Collector

This references an entry in the list of collectors.

SNMP ID:

2.109.2.2

Console path:

Setup > **NetFlow** > **Interfaces**

Possible values:

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

Active

Enables/disables NetFlow/IPFIX for this entry for the interface and the collector.

SNMP ID:

2.109.2.3

Console path:

Setup > **NetFlow** > **Interfaces**

Possible values:

Yes

NetFlow/IPFIX is enabled for this interface.

No

NetFlow/IPFIX is disabled for this interface.

Metering-Profile

This references an entry in the list of metering profiles.

SNMP ID:

2.109.2.4

Console path:

Setup > **NetFlow** > **Interfaces**

Possible values:

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

Comment

Optionally enter a meaningful comment as a description.

SNMP ID:

2.109.2.99

Console path:

Setup > **NetFlow** > **Interfaces**

Possible values:

Max. 50 characters from `` [A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ` ``

Operating

Enable NetFlow/IPFIX on the device.

SNMP ID:

2.109.3

Console path:

Setup > **NetFlow**

Possible values:

Yes

NetFlow/IPFIX is enabled.

No

NetFlow/IPFIX is disabled.

Metering-Profiles

Configure the profiles for NetFlow/IPFIX here.

SNMP ID:

2.109.4

Console path:

Setup > **NetFlow**

Name

Unique name of the metering profile. This name is referenced in other tables.

SNMP ID:

2.109.4.1

Console path:

Setup > **NetFlow** > **Metering-Profiles**

Possible values:

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

Direction

IP flow direction to be monitored by NetFlow/IPFIX.

SNMP ID:

2.109.4.2

Console path:

Setup > **NetFlow** > **Metering-Profiles**

Possible values:

Ingress

Inbound IP data streams from the perspective of NetFlow/IPFIX.

Egress

Outbound IP streams from the perspective of NetFlow/IPFIX.

All

Inbound and outbound IP data streams.

IP-Version

IP protocol version(s) to be monitored by NetFlow/IPFIX.

SNMP ID:

2.109.4.3

Console path:

Setup > **NetFlow** > **Metering-Profiles**

Possible values:

IPv4
IPv6
All

Comment

Optionally enter a meaningful comment as a description.

SNMP ID:

2.109.4.99

Console path:

Setup > **NetFlow** > **Metering-Profiles**

Possible values:

Max. 50 characters from `` [A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ` ``