

LCOS 10.50

Addendum

05/2024



LANCOM
SYSTEMS

Contents

- 1 Addendum to LCOS version 10.50.....5**
- 2 Configuration.....6**
 - 2.1 New CLI command ikectl.....6
 - 2.2 Using load balancer selectors for ping.....7
 - 2.3 Configuration option for IPv4/IPv6 resolution with DNS resolutions.....7
- 3 Routing and WAN connections.....8**
 - 3.1 Dynamic Path Selection.....8
 - 3.1.1 Additions to the table ICMP measurement profiles.....8
 - 3.1.2 New table HTTP measurement profiles.....9
 - 3.1.3 Additions to the Policy assignments table.....10
 - 3.1.4 New table Switchover-Profiles.....10
 - 3.1.5 Additions to the Setup menu.....11
 - 3.2 Bidirectional Forwarding Detection (BFD).....20
 - 3.2.1 Profiles.....21
 - 3.2.2 Key-Chains.....22
 - 3.2.3 Show commands via CLI.....22
 - 3.2.4 Additions to the Setup menu.....23
 - 3.3 Restricting protocol filters to source or destination addresses.....28
 - 3.3.1 Additions to the Setup menu.....29
 - 3.4 Network name for IPv6 variables of the action table.....29
 - 3.4.1 Additions to the Setup menu.....30
- 4 IPv6.....32**
 - 4.1 NPTv6.....32
 - 4.1.1 Examples.....33
 - 4.1.2 Show commands via CLI.....33
 - 4.1.3 Additions to the Setup menu.....33
 - 4.2 MAC addresses as station objects.....35
 - 4.2.1 Additions to the Setup menu.....36
 - 4.3 Delegated prefix as station objects.....37
 - 4.3.1 Additions to the Setup menu.....38
 - 4.4 464XLAT.....40
 - 4.4.1 Additions to the Setup menu.....41
- 5 Firewall.....44**
 - 5.1 Central table for DNS-based applications (layer-7 app).....44
 - 5.1.1 Additions to the Setup menu.....45
 - 5.2 H.323 ALG no longer supported in the firewall.....47
- 6 Wireless LAN – WLAN.....48**
 - 6.1 Fast Roaming over-the-DS.....48
 - 6.1.1 Additions to the Setup menu.....49

6.2 WPA3 Transition Mode Termination.....	49
6.2.1 Additions to the Setup menu.....	50
6.3 WLAN data trace in LANconfig at new location.....	51
7 Public Spot.....	52
7.1 Public Spot authentication with name, password and MAC address: Configurable MAC address format.....	52
7.1.1 Additions to the Setup menu.....	52
8 Backup solutions.....	53
8.1 ICMPv6 polling.....	53
8.1.1 Additions to the Setup menu.....	54
9 RADIUS.....	59
9.1 Dynamic Peer Discovery.....	59
9.1.1 Additions to the Setup menu.....	60
10 Other services.....	65
10.1 Appending several DHCP Option 43 sub-options in the DHCP server.....	65
10.1.1 Additions to the Setup menu.....	65
10.2 Function for switching to alternative DSL modem firmware.....	66
10.2.1 Additions to the Setup menu.....	66
10.3 DNS settings moved to own area.....	68
10.4 DNS filter for DNS data tunnels.....	68
10.4.1 Additions to the Setup menu.....	69
10.5 GPON support.....	71
10.5.1 Additions to the Setup menu.....	72
10.6 802.1X authenticator for Ethernet ports.....	74
10.6.1 Additions to the Setup menu.....	74
11 Enhancements in the menu system.....	76
11.1 Require-Msg-Authenticator.....	76
11.2 L2TP-Require-Msg-Authenticator.....	76
11.3 Require-Msg-Authenticator.....	77
11.4 Require-Msg-Authenticator.....	77
11.5 Backup-Require-Msg-Authenticator.....	78
11.6 Require-Msg-Authenticator.....	78
11.7 Require-Msg-Authenticator.....	79
11.8 Require-Msg-Authenticator.....	79
11.9 Require-Msg-Authenticator.....	80

Copyright

© 2023 LANCOM Systems GmbH, Würselen (Germany). All rights reserved.

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 (ey@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

A Rohde & Schwarz Company

Adenauerstr. 20/B2

52146 Würselen

Germany

www.lancom-systems.com


1 Addendum to LCOS version 10.50

This document describes the changes and enhancements in LCOS version 10.50 since the previous version.

2 Configuration

2.1 New CLI command ikectl

As of LCOS 10.50 the command ikectl is a feature.


Command	Description
<pre>ikectl [-[r d D] <peer-name-list>] [-[e r d] <ipsec-name-list>] [-[r d] [<ike-cookies-list> <esp-spi-list>]] [-R <peer-name-list> <redirect-target>]</pre>	<p>This command widens the range of analysis options, for example by executing targeted actions to isolate the problem in the event of an error. This function allows you to quickly and automatically modify and test a VPN, among other things.</p> <ul style="list-style-type: none"> > -e <ipsec-name-list>: Creates a Phase 2-SA/CHILD_SA when entered with the VPN rule name > -r <peer-name-list>: Performs a rekeying of the Phase 1-SA/IKE_SA when entered with the name of the VPN remote peer > -r <ike-cookies-list>: Performs rekeying when entered with the IKE cookie > -r <ipsec-name-list>: Performs a rekeying of the Phase 2-SA/Child_SA when entered with the name of the VPN rule > -r <esp-spi-list>: Performs a rekeying of the Phase 2-SA/Child_SA when entered with the incoming or outgoing ESP-SPI > -d <peer-name-list>: Deletes a Phase 1-SA/IKE_SA when entered with the name of the VPN remote peer > -d <ike-cookies-list>: Deletes a Phase 1-SA / IKE_SA when entered with IKEv1 cookies / IKEv2 SPIs > -d <ipsec-name-list>: Deletes a Phase 2-SA/CHILD_SA when entered with the VPN rule name > -d <esp-spi-list>: Deletes a Phase 2-SA/Child_SA when entered with the incoming or outgoing ESP-SPI > -D <peer-name-list>: Starts the liveness check (Dead Peer Detection – DPD) when entered with the name of the VPN remote peer > -R <peer-name-list> <redirect-target>: Redirects IKEv2 remote sites to a new destination using the IKEv2 redirect. If the list of remote sites is empty, all remote sites are redirected. This command can be used for maintenance purposes to move VPN remote sites from the current VPN gateway to another gateway securely. > <peer-name-list>: List of remote peer names separated by spaces and consisting of max. 16 characters > <ipsec-name-list>: Space-separated list of VPN rule names, as displayed in “show vpn” as ipsec-0-PEER-pr0-l0-r0. <p> To find a certain CHILD_SA/Phase 2-SA for a road warrior, it is important to also specify the remote station name as follows: "peer-name ipsec-name".</p> <ul style="list-style-type: none"> > <ike-cookies-list>: Consists of a list of 16 hexadecimal values separated by spaces, e.g 0x000102030405060708090A0B0C0D0E0F

Command	Description
	<ul style="list-style-type: none"> > <esp-spi-list>: Consists of a list of 4 hexadecimal values separated by spaces, e.g. 0x00010203 > <redirect-target>: Target to which the remote site(s) are to be redirected. The target can be an IPv4 address, IPv6 address or a DNS name <p>Example: <code>ikectl -r peer ipsec-name-peer-2 -D peer3 -d peer 4 0 x 1 2 3 4 5 6 7 8 -e "RoadWarrior IPSEC-0-DEFAULT-PRO-L0-R0"</code></p>

2.2 Using load balancer selectors for ping

From LCOS 10.50 there is a new command-line option for ping to use load balancer selectors.

On the command line, use the new optional ping parameter `-l <Load-Balancer-Policy>`.

Parameter	Meaning
<code>-l <Load-Balancer-Policy></code>	<p>If the ping target is reached via a load balancer, the policy makes a load-balancer decision when the pings are sent. Possible values are traffic, bandwidth, round robin and all defined Dynamic Path Selection policies. If an invalid policy is specified, no pings are sent</p> <hr/> <p> It is not possible to use this CLI option in combination with the specification of a scope or an interface binding in the destination.</p>

2.3 Configuration option for IPv4/IPv6 resolution with DNS resolutions

From LCOS 10.50 parameters used to configure DNS host names can be transmitted with a switch that specifies how to prioritize IPv4 or IPv6 when a connection is established.

Specific use cases are, for example, the use of DNS names in VPN connections or SIP registrars, where you need to control whether the connection is established via IPv4 or IPv6.

Example 1: If the host name `vpn.example.org` is resolved to an IPv4 and an IPv6 address, a host usually prefers IPv6 over IPv4. However, if IPv4 is to be used, this can be controlled by appending `?4` to the host name, i.e. in this case: `vpn.example.org?4`.

Example 2: If IPv4 is to be preferred for a CLI ping of an IPv4/IPv6 DNS host name, the following syntax can be used: `ping www.example.org?4`.

The following suffixes are allowed:

- > `?4`: Resolve only over IPv4
- > `?6`: Resolve only over IPv6
- > `?46`: Prefer IPv4 over IPv6, i.e. if IPv4 cannot be resolved, IPv6 is used.
- > `?64`: Prefer IPv6 over IPv4, i.e. if IPv6 cannot be resolved, IPv4 is used.

3 Routing and WAN connections

3.1 Dynamic Path Selection

As of LCOS 10.50 the following new functions are supported by Dynamic Path Selection:

- > Session switchover: An active session can be moved to a better line during runtime (for unmasked connections only, e.g. VPN/overlay tunnel)
- > Along with ICMP, HTTP(S) is also supported as a measurement method
- > ICMP measurement intervals now support intervals with a time resolution in milliseconds
- > IPv6

3.1.1 Additions to the table ICMP measurement profiles

To configure the ICMP measurement profiles, navigate to the view **IP Router > Routing > SD-WAN Dynamic Path Selection > ICMP measurement profiles**.

IPv6 destination 1-4

Up to 4 measurement targets as valid IPv6 unicast addresses or DNS host names. With :: entered, the measurement target is determined dynamically by the VPN. If the field is left empty, no measurements are made for this family of addresses.

Unit

Specifies whether the ICMP measurements for the value should be in seconds or milliseconds. Possible values: Seconds (default), milliseconds.

3.1.2 New table HTTP measurement profiles

HTTP measurement profiles specify a parameter set used by measurements that are based on HTTP(S) connections. Interface metrics are derived from measurements that quantify the connection quality. These metrics are: Mean time to establish an HTTP(S) connection (latency), jitter, and connection-error rate (packet loss).

To configure the HTTP measurement profiles, navigate to the view **IP Router > Routing > SD-WAN Dynamic Path Selection > HTTP measurement profiles**.

Measurement profile

The name of the profile. This name is used to reference the profile in DPS policies.

DSCP value

Sets the DSCP value in the IP header of measurement packets. DSCP (Differentiated Services Code Point) is used for QoS (Quality of Service).

Source address (optional)

References a named loopback address that is used as the sender in the measurement packets. If the field is left empty, the router automatically selects an address that matches the sending interface.

IPv4 destination 1-4

Up to 4 measurement targets as valid IPv4 unicast addresses or DNS host names. With 0.0.0.0 entered, the measurement target is determined dynamically by the VPN. If the field is left empty, no measurements are made for this family of addresses.

IPv6 destination 1-4

Up to 4 measurement targets as valid IPv6 unicast addresses or DNS host names. With :: entered, the measurement target is determined dynamically by the VPN. If the field is left empty, no measurements are made for this family of addresses.

Payload size

Specifies the size of the data payload that follows the ICMP header (payload size) of the pings being sent.

Interval

The interval in seconds between 2 measurements. The maximum round trip time is also specified. Packets not answered within a measurement interval are counted as packet loss.

Sliding window

Maximum number of measurement values that are used to determine the interface metrics. If a measurement value is received after the number specified here has been reached, the oldest measurement is discarded.

3.1.3 Additions to the Policy assignments table

To configure the policy assignments, navigate to the view **IP Router > Routing > SD-WAN Dynamic Path Selection > Policy assignments**.

Switchover-Profile

Specify the name of the Switchover profile used for this policy. See also [New table Switchover-Profiles](#) on page 10.

3.1.4 New table Switchover-Profiles

By default, Dynamic Path Selection only distributes new sessions to a better line. If you want ongoing sessions to be shifted to a better line, you have to enable session switchover. A session switchover only makes sense for unmasked connections, such as VPN or SD-WAN overlays. With masked connections, the public WAN address would change during the session, so it would be rejected by servers offering SIP sessions or online banking. Two configuration steps are necessary to enable session switchover:

1. The firewall rules for Dynamic Path Selection must be enabled for session switchover.
To do this, the switch **Dynamic path selection session failover** has to be set for IPv4 under **Firewall/QoS > IPv4 Rules > Rules > General** and/or for IPv6 under **Firewall/QoS > IPv6 Rules > IPv6 forwarding rules**.
2. A switchover profile must be linked to the corresponding policy in the Policy assignments table

The switchover profile can be used to control how quickly the set of sessions is moved to the new line or interface on the same load balancer.

To prevent sessions from being concentrated on a single interface, sessions are usually moved step-by-step in groups within the configured timeframe. Before each step, a check sees whether the switchover is still necessary, because in the meantime the policy scores and thus the ranking of the interfaces may have changed. If it is no longer necessary, switchover is canceled and the sessions remain on their current interface. If it remains necessary, the sessions for the group being moved in the next step are determined at random.

If the number of steps = 1 or the overall time = 0, all sessions are moved immediately.

To configure the HTTP measurement profiles, navigate to the view **IP Router > Routing > SD-WAN Dynamic Path Selection > Switchover-Profiles**.

Switchover-Profile

The name of the switchover profile. This name is used to reference the profile.

Steps

Number of steps or groups in which the set of sessions is moved to the new line.

Timeframe

Timeframe in seconds within which the set of sessions is shifted to the new line.

3.1.5 Additions to the Setup menu

IPv6-Destination-1

The first of up to 4 measurement targets as valid IPv6 unicast addresses or DNS host names. With :: entered, the measurement target is determined dynamically by the VPN. If the field is left empty, no measurements are made for this family of addresses.

SNMP ID:

2.110.4.1.5

Console path:

Setup > Firewall > Dynamic-Path-Selection > ICMP-Measurement-Profiles

Possible values:

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

IPv6-Destination-2

The second of up to 4 measurement targets as valid IPv6 unicast addresses or DNS host names. With :: entered, the measurement target is determined dynamically by the VPN. If the field is left empty, no measurements are made for this family of addresses.

SNMP ID:

2.110.4.1.12

Console path:

Setup > Firewall > Dynamic-Path-Selection > ICMP-Measurement-Profiles

Possible values:

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

IPv6-Destination-3

The third of up to 4 measurement targets as valid IPv6 unicast addresses or DNS host names. With :: entered, the measurement target is determined dynamically by the VPN. If the field is left empty, no measurements are made for this family of addresses.

SNMP ID:

2.110.4.1.13

Console path:**Setup > Firewall > Dynamic-Path-Selection > ICMP-Measurement-Profiles****Possible values:**Max. 64 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()+-./:;<=>?[\]^_``**IPv6-Destination-4**

The fourth of up to 4 measurement targets as valid IPv6 unicast addresses or DNS host names. With :: entered, the measurement target is determined dynamically by the VPN. If the field is left empty, no measurements are made for this family of addresses.

SNMP ID:

2.110.4.1.14

Console path:**Setup > Firewall > Dynamic-Path-Selection > ICMP-Measurement-Profiles****Possible values:**Max. 64 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()+-./:;<=>?[\]^_``**Unit**

Specifies whether the ICMP measurements for the value should be in seconds or milliseconds.

SNMP ID:

2.110.4.1.15

Console path:**Setup > Firewall > Dynamic-Path-Selection > ICMP-Measurement-Profiles****Possible values:****Seconds**
Milliseconds**Default:**

Seconds

HTTP-Measurement-Profiles

HTTP measurement profiles specify a parameter set used by measurements that are based on HTTP(S) connections. Interface metrics are derived from measurements that quantify the connection quality. These metrics are: Mean time to establish an HTTP(S) connection (latency), jitter, and connection-error rate (packet loss).

SNMP ID:

2.110.4.2

Console path:**Setup > Firewall > Dynamic-Path-Selection**

Measurement-Profile

The name of the profile. This name is used to reference the profile in DPS policies.

SNMP ID:

2.110.4.2.1

Console path:**Setup > Firewall > Dynamic-Path-Selection > HTTP-Measurement-Profiles****Possible values:**Max. 32 characters from `[A-Z][0-9]@{|}~!$%&'()+,/:;<=>?[\]^_.`**DSCP value**

Sets the DSCP value in the IP header of measurement packets. DSCP (Differentiated Services Code Point) is used for QoS (Quality of Service).

SNMP ID:

2.110.4.2.2

Console path:**Setup > Firewall > Dynamic-Path-Selection > HTTP-Measurement-Profiles**

Possible values:

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

Loopback-Addr.

Optionally references a named loopback address used as the sender in the measurement packets. If the field is left empty, the router automatically selects an address that matches the sending interface.

SNMP ID:

2.110.4.2.3

Console path:

Setup > Firewall > Dynamic-Path-Selection > HTTP-Measurement-Profiles

Possible values:

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

IPv4-Destination-1

The first of up to 4 measurement targets as a valid IPv4 unicast address or DNS host name. With "0.0.0.0" entered, the measurement target is determined dynamically by the VPN. If the field is left empty, no measurements are made for this family of addresses.

SNMP ID:

2.110.4.2.4

Console path:

Setup > Firewall > Dynamic-Path-Selection > HTTP-Measurement-Profiles

Possible values:

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

IPv6-Destination-1

The first of up to 4 measurement targets as valid IPv6 unicast addresses or DNS host names. With `::` entered, the measurement target is determined dynamically by the VPN. If the field is left empty, no measurements are made for this family of addresses.

SNMP ID:

2.110.4.2.5

Console path:

Setup > Firewall > Dynamic-Path-Selection > HTTP-Measurement-Profiles

Possible values:

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

Interval

The interval in seconds between 2 measurements. The maximum round trip time is also specified. Packets not answered within a measurement interval are counted as packet loss.

SNMP ID:

2.110.4.2.6

Console path:

Setup > Firewall > Dynamic-Path-Selection > HTTP-Measurement-Profiles

Possible values:

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

Sliding-Window

Maximum number of measurement values that are used to determine the interface metrics. If a measurement value is received after the number specified here has been reached, the oldest measurement is discarded.

SNMP ID:

2.110.4.2.7

Console path:

Setup > Firewall > Dynamic-Path-Selection > HTTP-Measurement-Profiles

Possible values:

Max. 5 characters from [0-9]

IPv4-Destination-2

The second of up to 4 measurement targets as a valid IPv4 unicast address or DNS host name. With "0.0.0.0" entered, the measurement target is determined dynamically by the VPN. If the field is left empty, no measurements are made for this family of addresses.

SNMP ID:

2.110.4.2.8

Console path:**Setup > Firewall > Dynamic-Path-Selection > HTTP-Measurement-Profiles****Possible values:**

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

IPv4-Destination-3

The third of up to 4 measurement targets as a valid IPv4 unicast address or DNS host name. With "0.0.0.0" entered, the measurement target is determined dynamically by the VPN. If the field is left empty, no measurements are made for this family of addresses.

SNMP ID:

2.110.4.2.9

Console path:**Setup > Firewall > Dynamic-Path-Selection > HTTP-Measurement-Profiles****Possible values:**

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

IPv4-Destination-4

The fourth of up to 4 measurement targets as a valid IPv4 unicast address or DNS host name. With "0.0.0.0" entered, the measurement target is determined dynamically by the VPN. If the field is left empty, no measurements are made for this family of addresses.

SNMP ID:

2.110.4.2.10

Console path:**Setup > Firewall > Dynamic-Path-Selection > HTTP-Measurement-Profiles**

Possible values:

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

IPv6-Destination-2

The second of up to 4 measurement targets as valid IPv6 unicast addresses or DNS host names. With `::` entered, the measurement target is determined dynamically by the VPN. If the field is left empty, no measurements are made for this family of addresses.

SNMP ID:

2.110.4.2.11

Console path:

Setup > Firewall > Dynamic-Path-Selection > HTTP-Measurement-Profiles

Possible values:

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

IPv6-Destination-3

The third of up to 4 measurement targets as valid IPv6 unicast addresses or DNS host names. With `::` entered, the measurement target is determined dynamically by the VPN. If the field is left empty, no measurements are made for this family of addresses.

SNMP ID:

2.110.4.2.12

Console path:

Setup > Firewall > Dynamic-Path-Selection > HTTP-Measurement-Profiles

Possible values:

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

IPv6-Destination-4

The fourth of up to 4 measurement targets as valid IPv6 unicast addresses or DNS host names. With `::` entered, the measurement target is determined dynamically by the VPN. If the field is left empty, no measurements are made for this family of addresses.

SNMP ID:

2.110.4.2.13

Console path:

Setup > Firewall > Dynamic-Path-Selection > HTTP-Measurement-Profiles

Possible values:

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

Switchover-Profile

The name of a switchover profile to be used for this policy. Also see [2.110.4.32.1 Switchover-Profile](#) on page 18.

SNMP ID:

2.110.4.17.7

Console path:

Setup > Firewall > Dynamic-Path-Selection > Policy-Assignments

Possible values:

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

Switchover-Profiles

By default, Dynamic Path Selection only distributes new sessions to a better line. If you want ongoing sessions to be shifted to a better line, you have to enable session switchover. A session switchover only makes sense for unmasked connections, such as VPN or SD-WAN overlays. With masked connections, the public WAN address would change during the session, so it would be rejected by servers offering SIP sessions or online banking. Two configuration steps are necessary to enable session switchover:

1. The firewall rules for Dynamic Path Selection must have session switchover enabled
2. A switchover profile must be linked to the corresponding policy in the Policy assignments table

The switchover profile can be used to control how quickly the set of sessions is moved to the new line or interface on the same load balancer.

To prevent sessions from being concentrated on a single interface, sessions are usually moved step-by-step in groups within the configured timeframe. Before each step, a check sees whether the switchover is still necessary, because in the meantime the policy scores and thus the ranking of the interfaces may have changed. If it is no longer necessary, switchover is canceled and the sessions remain on their current interface. If it remains necessary, the sessions for the group being moved in the next step are determined at random.

If the number of steps = 1 or the overall time = 0, all of the sessions are moved immediately.

SNMP ID:

2.110.4.32

Console path:

Setup > Firewall > Dynamic-Path-Selection

Switchover-Profile

The name of the switchover profile. This name is used to reference the profile.

SNMP ID:

2.110.4.32.1

Console path:**Setup > Firewall > Dynamic-Path-Selection > Switchover-Profiles****Possible values:**Max. 32 characters from `[A-Z][0-9]@{|}~!$%&'()+,-./:;<=>?[\]^_.`**Steps**

Number of steps or groups in which the set of sessions is moved to the new line.

SNMP ID:

2.110.4.32.2

Console path:**Setup > Firewall > Dynamic-Path-Selection > Switchover-Profiles****Possible values:**Max. 2 characters from `[0-9]`**Timeframe(s)**

Timeframe in seconds within which the set of sessions is shifted to the new line.

SNMP ID:

2.110.4.32.3

Console path:**Setup > Firewall > Dynamic-Path-Selection > Switchover-Profiles****Possible values:**Max. 4 characters from `[0-9]`**LB-Switchover**

Specifies whether the sessions under these rules should be moved to a better line as identified by Dynamic Path Selection. This is only possible for unmasked connections, e.g. VPN connections.

SNMP ID:

2.8.10.2.17

Console path:**Setup > IP-Router > Firewall > Rules**

Possible values:


No
Yes

Default:

No

Flags

These options determine how the firewall handles the rule.

 You can select several options at the same time.

SNMP ID:

2.70.5.2.2

Console path:

Setup > IPv6 > Firewall > Forwarding-Rules

Possible values:**Disabled**

The rule is deactivated. The firewall skips this rule.

Linked

After processing the rule, the firewall looks for additional rules which come in question.

Stateless

This rule does not take the statuses of the TCP sessions into account.

LB-Switchover


Specifies whether the sessions under these rules should be moved to a better line as identified by Dynamic Path Selection. This is only possible for unmasked connections, e.g. VPN connections.

3.2 Bidirectional Forwarding Detection (BFD)

From LCOS 10.50 the Bidirectional Forwarding Detection protocol is supported.

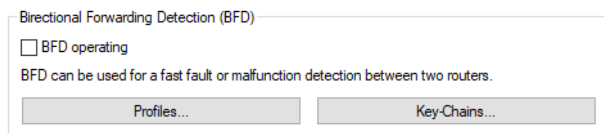
Bidirectional Forwarding Detection according to [RFC 5880](#) is a simple Hello protocol to detect the loss of a connection between two routers. Hello packets are sent by both routers at a set interval. If these Hello packets are not received within a certain interval, the connection is assumed to be broken. In combination with BGP, BFD allows broken connections to be detected more quickly, since the BFD timers can be significantly shorter than the BGP timers.

Adjusting the timer interval allows lost connections to be detected faster or slower. The lower the timer interval, the faster connection losses are detected.

-  > BFD supports IPv4 and IPv6.
> There is no echo mode.

- BFD is a protocol that requires significant system resources, CPU time and bandwidth. BFD is processed exclusively in software. Hardware processing is not supported for BFD.
- Setting the Hello to a very short interval may result in BFD flapping or the detection of false positives. If false positives occur, you should increase the Hello interval.
- We do not recommend setting the Hello interval at less than 250ms.

In LANconfig you configure BFD under **Routing protocols > General > Bidirectional Forwarding Detection (BFD)**.

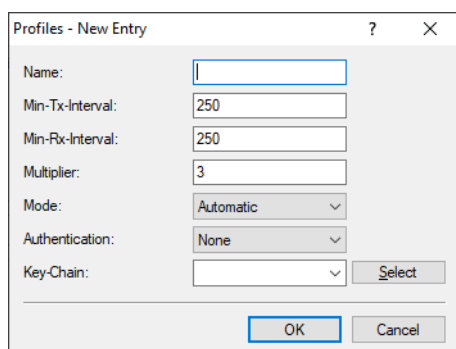


BFD operating

Activates or deactivates BFD globally

3.2.1 Profiles

To configure the BFD profiles switch to the view **IP Router > General > Bidirectional Forwarding Detection (BFD) > Profiles**.



Name

Enter a descriptive name for this BFD profile. If BFD is used in combination with BGP, this name is linked to the corresponding BGP neighbor.

Min-Tx-Interval

Minimum interval in milliseconds between sent BFD control messages. (Value range 1-9999 milliseconds, default 250)

Min-Rx-Interval

Minimum interval in milliseconds between received BFD control messages. (Value range 1-9999 milliseconds, default 250)

Multiplier

Number of packets not received for an interface to be declared as down. The multiplier and the interval together produce the time until a connection is declared as down. (Value range 1-255, default 3)

Mode

Specifies whether the BFD neighbor is single-hop or multi-hop connected. In single-hop mode, the UDP destination port 3784 and time-to-live of 1 are used in the IP header. Multi-hop mode uses UDP port 4784. In Automatic, single-hop mode is used if the route to the neighbor is of the type Connected LAN or WAN,

otherwise multi-hop is used. By default, eBGP sessions are single-hop. iBGP sessions can be multi-hop. Possible values:

- > Automatic
- > Single-Hop
- > Multi-Hop

Default: Automatic

Authentication

Specifies the type of authentication used for the BFD messages. Possible values:

- > None
- > Password
- > MD5
- > MD5-Meticulous
- > SHA1
- > SHA1-Meticulous

Default: None

Key-Chain

Name of the key chain from the table [Key-Chains](#). Defines the key used for the BFD messages. For the parameter **Authentication**, a value must be configured that is other than "None".

3.2.2 Key-Chains

To configure the key chains, switch to the view **IP Router > General > Bidirectional Forwarding Detection (BFD) > Key-Chains**.

The screenshot shows a dialog box titled "Key-Chains - New Entry". It has three input fields: "Name:" (empty), "Number:" (0), and "Key:" (empty). To the right of the "Key:" field is a checkbox labeled "Show". At the bottom of the dialog are two buttons: "OK" and "Cancel".

Name

Enter a descriptive name for this key chain. This name is used in the [BFD profiles](#) to reference this key chain.

Number

Key chain number.

Key

Key or password for this key chain.

3.2.3 Show commands via CLI

The available show commands are listed in the following:

- > **show BFD-v4-details**
Displays details about the IPv4 BFD connections.
- > **show BFD-v6-details**

Displays details about the IPv6 BFD connections.

> **show BFD-v4-status**

Displays the status of the IPv4 BFD connections.

> **show BFD-v6-status**

Displays the status of the IPv6 BFD connections.

3.2.4 Additions to the Setup menu

BFD-Profile

Contains the name of a BFD profile from **Setup > Routing-Protocols > BFD > Profiles**. In combination with BGP, BFD allows broken connections to be detected more quickly, since the BFD timers can be significantly shorter than the BGP timers.

SNMP ID:

2.93.1.2.17

Console path:

Setup > Routing-Protocols > BGP > Neighbors

Possible values:

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

BFD

In this directory you configure the Bidirectional Forwarding Detection (BFD) protocol. BFD according to [RFC 5880](#) is a simple Hello protocol to detect the loss of a connection between two routers. Hello packets are sent by both routers at a set interval. If these Hello packets are not received within a certain interval, the connection is assumed to be broken. In combination with BGP, BFD allows broken connections to be detected more quickly, since the BFD timers can be significantly shorter than the BGP timers.

Adjusting the timer interval allows lost connections to be detected faster or slower. The lower the timer interval, the faster connection losses are detected.



- > BFD supports IPv4 and IPv6.
- > There is no echo mode.
- > BFD is a protocol that requires significant system resources, CPU time and bandwidth. BFD is processed exclusively in software. Hardware processing is not supported for BFD.
- > Setting the Hello to a very short interval may result in BFD flapping or the detection of false positives. If false positives occur, you should increase the Hello interval.
- > We do not recommend setting the Hello interval at less than 250ms.

SNMP ID:

2.93.6

Console path:

Setup > Routing-Protocols

Key-Chains

This item is used to configure the key chains for BFD.

SNMP ID:

2.93.6.1

Console path:

Setup > Routing-Protocols > BFD

Name

Enter a descriptive name for this key chain. This name is used in the BFD profiles to reference this key chain.

SNMP ID:

2.93.6.1.1

Console path:

Setup > Routing-Protocols > BFD > Key-Chains

Possible values:

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

Number

Key chain number.

SNMP ID:

2.93.6.1.2

Console path:

Setup > Routing-Protocols > BFD > Key-Chains

Possible values:

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

Key

Key or password for this key chain.

SNMP ID:

2.93.6.1.3

Console path:

Setup > Routing-Protocols > BFD > Key-Chains

Possible values:

Max. 80 characters from `[A-Z][a-z][0-9]#@[|}~!$%&'()*+,-./:;<=>?[\]^_`~`

Profiles

Configure the BFD profiles here.

SNMP ID:

2.93.6.2

Console path:

Setup > Routing-Protocols > BFD

Name

Enter a descriptive name for this BFD profile. If BFD is used in combination with BGP, this name is linked to the corresponding BGP neighbor.

SNMP ID:

2.93.6.2.1

Console path:

Setup > Routing-Protocols > BFD > Profiles

Possible values:

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

Min-Tx-Interval

Minimum interval in milliseconds between sent BFD control messages.

SNMP ID:

2.93.6.2.2

Console path:

Setup > Routing-Protocols > BFD > Profiles

Possible values:

1 ... 9999

Default:

250

Min-Rx-Interval

Minimum interval in milliseconds between received BFD control messages.

SNMP ID:

2.93.6.2.3

Console path:

Setup > Routing-Protocols > BFD > Profiles

Possible values:

1 ... 9999

Default:

250

Multiplier

Number of packets not received for an interface to be declared as down. The multiplier and the interval together produce the time until a connection is declared as down.

SNMP ID:

2.93.6.2.4

Console path:

Setup > Routing-Protocols > BFD > Profiles

Possible values:

1 ... 255

Default:

3

Authentication

Specifies the type of authentication used for the BFD messages.

SNMP ID:

2.93.6.2.6

Console path:

Setup > Routing-Protocols > BFD > Profiles

Possible values:

None
Password
MD5
MD5-Meticulous
SHA1
SHA1-Meticulous

Default:

None

Key-Chain

Name of the key chain from the table [2.93.6.1 Key-Chains](#) on page 24. Defines the key used for the BFD messages. For the parameter [2.93.6.2.6 Authentication](#) on page 26, a value must be configured that is other than "None".

SNMP ID:

2.93.6.2.7

Console path:

Setup > Routing-Protocols > BFD > Profiles

Possible values:

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

Mode

Specifies whether the BFD neighbor is single-hop or multi-hop connected. In single-hop mode, the UDP destination port 3784 and time-to-live of 1 are used in the IP header. Multi-hop mode uses UDP port 4784. In Automatic, single-hop mode is used if the route to the neighbor is of the type Connected LAN or WAN, otherwise multi-hop is used. By default, eBGP sessions are single-hop. iBGP sessions can be multi-hop.

SNMP ID:

2.93.6.2.8

Console path:

Setup > Routing-Protocols > BFD > Profiles

Possible values:

Automatic
Single-Hop
Multi-Hop

Default:

Automatic

Operating

Activates or deactivates BFD globally

SNMP ID:

2.93.6.3

Console path:

Setup > Routing-Protocols > BFD

Possible values:

- No
- Yes

Default:

No

3.3 Restricting protocol filters to source or destination addresses

The (W)LAN protocol filter under **Interfaces > LAN > LAN bridge > Protocols** allow a rule to be linked to an IP network. A check is made to see whether either the source or destination address of a packet matches the configured IP network. Until now both the source and the destination address were checked. From LCOS 10.50 you can decide whether the source or destination address are checked. By default, the previous behavior is active.

The screenshot shows a configuration window titled "Protocols - New Entry". It has several sections:

- Name:** A text input field.
- Packet conditions:**
 - Protocol: Text input field.
 - Subtype: Text input field with value "0".
 - First port: Text input field with value "0".
 - Last port: Text input field with value "0".
- Route conditions:**
 - Remote MAC address: Text input field.
 - DHCP assigned IP: A dropdown menu with "Irrelevant" selected.
 - Network IP: Text input field with value "0.0.0.0".
 - Netmask: Text input field with value "0.0.0.0".
 - Match: A dropdown menu with "Source and destination" selected.
 - Interface list: Text input field with a "Select" button next to it.
- Action:**
 - Drop packets: Selected with a radio button.
 - Pass packets: Unselected with a radio button.
 - Redirect packets to the following IP address: Unselected with a radio button.
 - Redirect IP address: Text input field with value "0.0.0.0".

At the bottom, there are "OK" and "Cancel" buttons.

Match

By default, the source and the destination address are both checked. Here you can specify whether only the source or only the destination address is checked instead.

3.3.1 Additions to the Setup menu**IP-Match**

By default, the source and the destination address are both checked. Here you can specify whether only the source or only the destination address is checked instead.

SNMP ID:

2.20.10.14

Console path:

Setup > LAN-Bridge > Protocol-Table

Possible values:**Either**

Both the source and the destination address are checked.

Source

Only the source address is checked.

Destination

Only the destination address is checked.

Default:

Either

3.4 Network name for IPv6 variables of the action table

As of LCOS 10.50 RU5, new variables have been added for the syntax in the action table. The IPv6 variables %x and %y can now also pass the LAN network name used for this variable. The %x and %y variables only transfer the values of the network with the fixed name INTRANET.

- > `%{xNetworkname}` – e.g. `%{xTESTNET}` for the current IPv6 LAN prefix of the network TESTNET as a string in the format “fd00:0:0:1::/64”.



The variable %x transfers only the values of the network with the fixed name INTRANET. This can also be used to pass the LAN network name used for this variable.

- > `%{yNetworkname}` – e.g. `%{yTESTNET}` for the current IPv6 LAN address of the device in the TESTNET network as a string in the format “fd00::1:2a0:57ff:fa1b:9d7b”.



The variable %y transfers only the values of the network with the fixed name INTRANET. This can also be used to pass the LAN network name used for this variable.

3.4.1 Additions to the Setup menu

Action

0 switches off the monitoring of the time budget. Only one action can be triggered per entry. The result of the actions can be evaluated in the 'Check for' field.

Prefixes:

- > **exec**: – This prefix initiates any command as it would be entered at the Telnet console. For example, the action "exec:do /o/m/d" terminates all current connections.
- > **dnscheck**: – This prefix initiates an IPv4 DSN name resolution. For example, the action `dnscheck:myserver.dyndns.org` requests the IPv4 address of the indicated server.
- > **dnscheck6**: – This prefix initiates an IPv6 DSN name resolution. For example, the action `dnscheck6:myserver.dyndns.org` requests the IPv6 address of the indicated server.
- > **http**: – This prefix initiates an HTTP-get request. A DynDNS update at `dyndns.org` is initiated with the following action: `http://username:password@members.dyndns.org/nic/update?system=dyndns&hostname=%h&myip=%a` (the significance of the placeholders %h and %a are described in the following.)
- > **https**: – Like 'http:', except that the connection is encrypted.
- > **gnudip**: – This prefix initiates a request to the corresponding DynDNS server via the GnuDIP protocol. For example, you can use the following action to use the GnuDIP protocol to execute a DynDNS update at a DynDNS provider:


```
gnudip://gnudipsrv?method=tcp&user=myserver&domn=mydomain.org&pass=password&reqc=0&addr=%a
```

The meaning of the place holder %a is described below.


- > **repeat**: – This prefix together with a time in seconds repeats all actions with the condition "Establish" as soon as the connection has been established. For example, the action 'repeat 300' causes all of the establish actions to be repeated every 5 minutes.
- > **mailto**: – This prefix causes an e-mail to be sent. For example, you can use the following action to send an e-mail to the system administrator when a connection is terminated: `mailto:admin@mycompany.com?subject=VPN connection broken at %t?body=VPN connection to branch office 1 was broken.`

Optional variables for the actions:

- > **%a** – WAN IPv4 address of the WAN connection relating to the action.
- > **%x** – The current IPv6 LAN prefix as a string in the format "fd00:0:0:1::/64".
- > **%{xNetworkname}** – e.g. **%{xTESTNET}** for the current IPv6 LAN prefix of the network TESTNET as a string in the format "fd00:0:0:1::/64".

 The variable %x transfers only the values of the network with the fixed name INTRANET. This can also be used to pass the LAN network name used for this variable.

- > **%y** – The current IPv6 LAN address of the device as a string in the format "fd00::1:2a0:57ff:fa1b:9d7b".
- > **%{yNetworkname}** – e.g. **%{yTESTNET}** for the current IPv6 LAN address of the device in the TESTNET network as a string in the format "fd00::1:2a0:57ff:fa1b:9d7b".

 The variable %y transfers only the values of the network with the fixed name INTRANET. This can also be used to pass the LAN network name used for this variable.

- > **%z** – WAN IPv6 address of the WAN connection relating to the action.
- > **%H** – Host name of the WAN connection relating to the action.
- > **%h** – Like %H, except the hostname is in small letters.
- > **%c** – Connection name of the WAN connection relating to the action.

- > %n – Device name
- > %s – Device serial number
- > %m – Device MAC address (as in Sysinfo)
- > %t – Time and date in the format YYYY-MM-DD hh:mm:ss
- > %e – Description of the error that was reported when connection establishment failed.

SNMP ID:

2.2.25.6

Console path:**Setup > WAN > Action-Table****Possible values:**

Max. 250 characters

Default:*empty*


4 IPv6

4.1 NPTv6

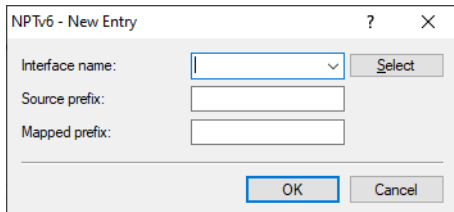
NPTv6 (Network Prefix Translation) according to [RFC 6296](#) allows the translation of one IPv6 prefix to another IPv6 prefix. The translation is 1:1, in that an address from prefix A is mapped to an address from prefix B. Only the prefix part is mapped, the host part is retained. This method thus works "stateless". NPTv6 cannot be used to mask an entire network behind a single address, as with IPv4.

Application scenarios for NPTv6 are, for example, VPNs or networks with dynamic prefixes that should be reachable whatever the public address. If the provider assigns a dynamic prefix, the prefix usually changes every time a connection is established. This is not desirable if certain resources require fixed IP addresses. With NPTv6, addresses from the (private) ULA range `fd00::/8` are then assigned to the clients in the network and an NPTv6 rule maps these addresses to the provider prefix.

Another use case is a load balancer scenario with several Internet providers, with each provider assigning its own prefix. With NPTv6, addresses from the ULA range `fd00::/8` are assigned to the clients in the network and a number of NPTv6 rules map these addresses to the provider prefixes.

 The IPv6 firewall must be enabled for NPTv6.

The configuration in LANconfig is done under **Firewall/QoS > IPv6 Rules > NPTv6**.



Interface name

Name of the network or the peer on which NPTv6 is to be performed. If a prefix is to be mapped for a dynamic provider prefix, the name of the Internet connection or peer has to be configured here, e.g. INTERNET.

Source prefix

Source network prefix, e.g. an explicit prefix `fd00::/64`.

Mapped prefix

Prefix that the source prefix is mapped to. Here you can configure either an explicit prefix such as `2001:db8::/32`, or the placeholder `::` with the appropriate prefix length in the case that the provider assigns a dynamic prefix.

4.1.1 Examples

Example 1

The provider (remote site INTERNET) assigns a dynamic prefix of length /56. The intranet is configured with the prefix fd00::/64. The source prefix fd00::/56 should be mapped 1:1 to the entire provider prefix (::/56).

The screenshot shows a dialog box titled "NPTv6 - New Entry". It has three input fields: "Interface name" with a dropdown menu showing "INTERNET" and a "Select" button; "Source prefix" with a text box containing "fd00::/56"; and "Mapped prefix" with a text box containing "::/56". At the bottom, there are "OK" and "Cancel" buttons.

Example 2

The provider (remote site INTERNET) assigns a dynamic prefix of length /56. The intranet is configured with the prefix fd00::/64. The source prefix fd00::/64 should be mapped to the special subnet "FF" from the dynamic provider prefix. For the mapped prefix, the placeholder :: is configured with the subnet ID FF, i.e. 0:0:0:00FF::/64.

The screenshot shows a dialog box titled "NPTv6 - New Entry". It has three input fields: "Interface name" with a dropdown menu showing "INTERNET" and a "Select" button; "Source prefix" with a text box containing "fd00::/64"; and "Mapped prefix" with a text box containing "0:0:0:00FF::/64". At the bottom, there are "OK" and "Cancel" buttons.

Example 3

For a VPN scenario, the internal source prefix fd00::/64 should be mapped to the prefix 2001:db8::/64.

The screenshot shows a dialog box titled "NPTv6 - New Entry". It has three input fields: "Interface name" with a dropdown menu showing "VPN" and a "Select" button; "Source prefix" with a text box containing "fd00::/64"; and "Mapped prefix" with a text box containing "2001:db8::/64". At the bottom, there are "OK" and "Cancel" buttons.

4.1.2 Show commands via CLI

The available show commands are listed in the following:

> show ipv6-npt

Shows the NPTv6 mapping rule.


4.1.3 Additions to the Setup menu

NPTV6

NPTv6 (Network Prefix Translation) according to [RFC 6296](#) allows the translation of one IPv6 prefix to another IPv6 prefix. The translation is 1:1, in that an address from prefix A is mapped to an address from prefix B. Only the prefix part is translated, the host part is retained. This method thus works "stateless". NPTv6 cannot be used to mask an entire network behind a single address, as with IPv4.

Application scenarios for NPTv6 are, for example, VPNs or networks with dynamic prefixes that should be reachable whatever the public address. If the provider assigns a dynamic prefix, the prefix usually changes every time a connection is established. This is not desirable if certain resources require fixed IP addresses. With NPTv6, addresses from the (private) ULA range `fd00::/8` are then assigned to the clients in the network and an NPTv6 rule maps these addresses to the provider prefix.

Another use case is a load balancer scenario with several Internet providers, with each provider assigning its own prefix. With NPTv6, addresses from the ULA range `fd00::/8` are assigned to the clients in the network and a number of NPTv6 rules map these addresses to the provider prefixes.

 The IPv6 firewall must be enabled for NPTv6.

SNMP ID:

2.70.5.30

Console path:**Setup > IPv6 > Firewall****Interface name**

Name of the network or the peer on which NPTv6 is to be performed. If a prefix is to be mapped for a dynamic provider prefix, the name of the Internet connection or peer has to be configured here, e.g. INTERNET.

SNMP ID:

2.70.5.30.1

Console path:**Setup > IPv6 > Firewall > NPTV6****Possible values:**Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-./:;<=>?[\]^_.`**source-prefix**

Source network prefix, e.g. an explicit prefix `fd00::/64`.

SNMP ID:

2.70.5.30.2

Console path:**Setup > IPv6 > Firewall > NPTV6****Possible values:**Max. 43 characters from `[A-F][a-f][0-9]:./`

mapped-prefix

Prefix that the source prefix is mapped to. Here you can configure either an explicit prefix such as 2001:db8::/32, or the placeholder :: with the appropriate prefix length in the case that the provider assigns a dynamic prefix.

SNMP ID:

2.70.5.30.3

Console path:


Setup > IPv6 > Firewall > NPTV6

Possible values:

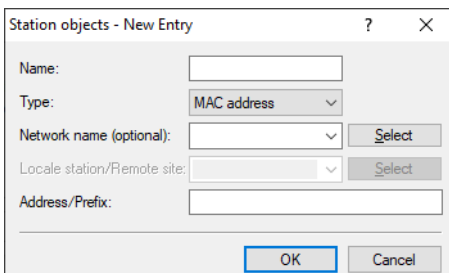
Max. 43 characters from `[A-F] [a-f] [0-9] : . /`

4.2 MAC addresses as station objects

From LCOS 10.50 MAC addresses can be used as station objects in the IPv6 firewall. This allows rules to be created for resources on the internal network that are identified by their MAC address. In dual-stack networks, this helps with the correlation to IPv4 station objects that are also handled by an IPv4 rule based on their MAC address.

 In rules, MAC addresses can be a source but not a target.

LANconfig: **Firewall/QoS > IPv6 Rules > Station objects**


Type

Determines the station type. The selection made here determines which of the following table columns (**Network name**, **Local station/Remote site name** and **Address/Prefix**) have to be filled out. New value:

MAC address

This allows rules to be created for resources on the internal network that are identified by their MAC address. In dual-stack networks, this helps with the correlation to IPv4 station objects that are also handled by an IPv4 rule based on their MAC address.

- > The **Name** column is optional and can contain the name of a network where the station object is located.
- > The column **Address/Prefix** contains the MAC address used to identify the object.

4.2.1 Additions to the Setup menu

Type

Determines the station type. Your selection determines which of the following table columns ([Local-network](#), [Remote-peer/local-host](#) and [Address/Prefix](#)) must be filled out.

SNMP ID:

2.70.5.9.2

Console path:

Setup > IPv6 > Firewall > Stations

Possible values:

Local-network

Name of a local network, e.g. INTRANET.

- > Only the column [Local-network](#) has to be filled out.
- > If it contains an interface name, then the station consists of all networks on this interface.
- > If you specify a network group, then the station consists of all prefixes under [Addresses](#) with this group.

Remote-peer

Name of a WAN remote site, e.g. INTERNET.

- > Only the column [Remote-peer/local-host](#) has to be filled out.
- > It can contain a WAN interface or a RAS template. With a WAN interface it resolves to all prefixes/networks to which a route exists via this WAN interface, and with a RAS template it resolves to all prefixes/networks to which a route exists via a RAS interface from this template.

Prefix

IPv6 prefix

- > Only the column [Address/Prefix](#) has to be filled out.
- > It contains an IPv6 prefix, e.g. "2001:db8::/32".

Identifier

- > The columns [Local-network](#) and [Address/Prefix](#) both have to be filled out
- > [Local-network](#) contains a WAN interface or a RAS template.
- > [Address/Prefix](#) contains an IPv6 identifier. These are the last 64 bits of the IPv6 address of an IPv6 host, e.g. "::2a0:57ff:fe1b:3a6a". The value must contain two leading colons.
- > This identifier forms an address when combined with the networks of the interface under [Local-network](#) or with the RAS interface from the specified template.
- > Furthermore, a link-local address with this identifier is formed for each of these interfaces.

IP-Address

- > Only the column [Address/Prefix](#) has to be filled out.
- > It contains an IPv6 address, e.g. "2001:db8::/1".

Named-host

Name of a local IPv6 host or local station.

- > The column [Remote-peer/local-host](#) must be filled out and contains a hostname.
- > The column [Local-network](#) is optional and can include a LAN interface.
- > The host name is resolved to a host address using the DHCPv6 server or the DNS server in the device.

- › If an interface has been specified, the address is only taken if it can be reached via this interface.

MAC-Address

This allows rules to be created for resources on the internal network that are identified by their MAC address. In dual-stack networks, this helps with the correlation to IPv4 station objects that are also handled by an IPv4 rule based on their MAC address.

- › The column *Local-network* is optional and can contain the name of a network where the station object is located.
- › The column *Address/Prefix* contains the MAC address used to identify the object.



In rules, MAC addresses can be a source but not a target.

Delegated-prefix

Especially where the provider prefix is dynamic, this allows a rule to be defined for downstream routers or resources.

- › The *Local-network* column is optional and can contain the name of a network where the station object is located. This can be used as a restriction on the local network.
- › The column *Remote-peer/local-host* is required and should contain the remote peer from which the delegated prefix is obtained or derived.
- › The column *Address/Prefix* contains a prefix or address that is linked (OR operator) with the prefix obtained from the provider. If the object should refer to the entire prefix, you can either configure `::/0` or the entry can be left blank.

Example: The provider delegates the prefix `2001:db8:1234::/48` to the remote peer INTERNET.

- › To use the subnet `abcd`, the *Address/Prefix* has to be configured as the value `0:0:0:abcd::/48`.
- › If the address to be used is `2001:db8:0:23::dead:beef/128`, then the *Address/Prefix* can be configured as `0:0:0:23::dead:beef/128`.
- › If the entire prefix is to be used, then the *Address/Prefix* can be configured as `::/0` or the entry can be left blank.

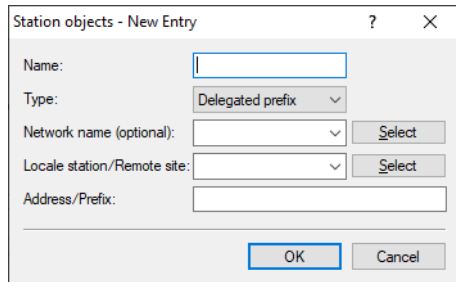
Default:

Local-network

4.3 Delegated prefix as station objects

From LCOS 10.50 the prefix delegated by the provider can be used as a station object in the IPv6 firewall. Especially where the provider prefix is dynamic, this allows a rule to be defined for downstream routers or resources.

LANconfig: **Firewall/QoS > IPv6 Rules > Station objects**



Delegated prefix

Especially where the provider prefix is dynamic, this allows a rule to be defined for downstream routers or resources.

- > The **Name** column is optional and can contain the name of a network where the station object is located. This can be used as a restriction on the local network.
- > The column **Local station/Remote site** is required and should contain the remote peer from which the delegated prefix is obtained or derived.
- > The column **Address/Prefix** contains a prefix or address that is linked (OR operator) with the prefix obtained from the provider. If the object should refer to the entire prefix, you can either configure `::/0` or the entry can be left blank.

Example: The provider delegates the prefix `2001:db8:1234::/48` to the remote peer INTERNET.

- > To use the subnet `abcd`, the **Address/Prefix** has to be configured as the value `0:0:0:abcd::/48`.
- > If the address to be used is `2001:db8:0:23::dead:beef/128`, then the **Address/Prefix** can be configured as `0:0:0:23::dead:beef/128`.
- > If the entire prefix is to be used, then the **Address/Prefix** can be configured as `::/0` or the entry can be left blank.

4.3.1 Additions to the Setup menu

Type

Determines the station type. Your selection determines which of the following table columns ([Local-network](#), [Remote-peer/local-host](#) and [Address/Prefix](#)) must be filled out.

SNMP ID:

2.70.5.9.2

Console path:

Setup > IPv6 > Firewall > Stations

Possible values:

Local-network

Name of a local network, e.g. INTRANET.

- > Only the column [Local-network](#) has to be filled out.
- > If it contains an interface name, then the station consists of all networks on this interface.
- > If you specify a network group, then the station consists of all prefixes under [Addresses](#) with this group.

Remote-peer

Name of a WAN remote site, e.g. INTERNET.

- Only the column *Remote-peer/local-host* has to be filled out.
- It can contain a WAN interface or a RAS template. With a WAN interface it resolves to all prefixes/networks to which a route exists via this WAN interface, and with a RAS template it resolves to all prefixes/networks to which a route exists via a RAS interface from this template.

Prefix

IPv6 prefix

- Only the column *Address/Prefix* has to be filled out.
- It contains an IPv6 prefix, e.g. "2001:db8::/32".

Identifier

- The columns *Local-network* and *Address/Prefix* both have to be filled out
- *Local-network* contains a WAN interface or a RAS template.
- *Address/Prefix* contains an IPv6 identifier. These are the last 64 bits of the IPv6 address of an IPv6 host, e.g. "::2a0:57ff:fe1b:3a6a". The value must contain two leading colons.
- This identifier forms an address when combined with the networks of the interface under *Local-network* or with the RAS interface from the specified template.
- Furthermore, a link-local address with this identifier is formed for each of these interfaces.

IP-Address

- Only the column *Address/Prefix* has to be filled out.
- It contains an IPv6 address, e.g. "2001:db8::/1".

Named-host

Name of a local IPv6 host or local station.

- The column *Remote-peer/local-host* must be filled out and contains a hostname.
- The column *Local-network* is optional and can include a LAN interface.
- The host name is resolved to a host address using the DHCPv6 server or the DNS server in the device.
- If an interface has been specified, the address is only taken if it can be reached via this interface.

MAC-Address

This allows rules to be created for resources on the internal network that are identified by their MAC address. In dual-stack networks, this helps with the correlation to IPv4 station objects that are also handled by an IPv4 rule based on their MAC address.

- The column *Local-network* is optional and can contain the name of a network where the station object is located.
- The column *Address/Prefix* contains the MAC address used to identify the object.



In rules, MAC addresses can be a source but not a target.

Delegated-prefix

Especially where the provider prefix is dynamic, this allows a rule to be defined for downstream routers or resources.

- The *Local-network* column is optional and can contain the name of a network where the station object is located. This can be used as a restriction on the local network.
- The column *Remote-peer/local-host* is required and should contain the remote peer from which the delegated prefix is obtained or derived.

- The column *Address/Prefix* contains a prefix or address that is linked (OR operator) with the prefix obtained from the provider. If the object should refer to the entire prefix, you can either configure `::/0` or the entry can be left blank.

Example: The provider delegates the prefix `2001:db8:1234::/48` to the remote peer INTERNET.

- To use the subnet `abcd`, the *Address/Prefix* has to be configured as the value `0:0:0:abcd::/48`.
- If the address to be used is `2001:db8:0:23::dead:beef/128`, then the *Address/Prefix* can be configured as `0:0:0:23::dead:beef/128`.
- If the entire prefix is to be used, then the *Address/Prefix* can be configured as `::/0` or the entry can be left blank.

Default:

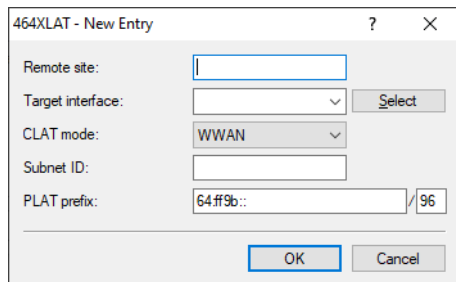
Local-network

4.4 464XLAT

From LCOS 10.50 the CLAT (Customer-Side Translator) function is supported by 464XLAT.

464XLAT according to [RFC 6877](#) is a procedure that translates from IPv4 to IPv6 and back to IPv4. The method is often used by mobile network providers to enable IPv4 access in an IPv6-only APN based on NAT64. Two sides are involved in 464XLAT: The client side or client translator (CLAT - customer-side translator) and the provider translator (PLAT - provider-side translator) or NAT64 gateway of the provider. The LCOS supports the CLAT side to enable a network behind a router to access IPv4 networks. In contrast to DS-Lite, which establishes a 4in6 tunnel to the AFTR gateway, 464XLAT uses a translation of the IPv4 packet to IPv6. On the PLAT side, the packet is translated back into IPv4. The name 464 results from the two-way translation. Generally, the NAT64 prefix `64:ff9b::/96` is used for the translation on the provider side. To use 464XLAT, it is first necessary to configure an IPv6 connection. A 464XLAT peer is then added. The IPv4 default route then points to this peer.

The configuration takes place in LANconfig under **IPv6 > Tunnel > 464XLAT**.



Peer

Set a unique name for this peer. Max. 16 characters as capital letters.

Destination interface

Name of the underlying WAN interface or the underlying peer, e.g. INTERNET. Max. 16 characters as capital letters.

CLAT mode

Defines with which method the CLAT prefix should be generated.

DHCPv6-PD

If the Internet provider uses DHCPv6 prefix delegation, e.g. for DSL or cable connections, the CLAT mode DHCPv6-PD must be used. The subnet ID can be used to control which subnet of the delegated prefix should be used for the CLAT prefix. The subnet ID can be configured as 0, 1 or FF, for example.

WWAN (Default)

If the Internet connection is a cellular connection (WWAN), the CLAT mode WWAN must be used. The CLAT prefix is formed from the /64 WAN prefix. The subnet ID must be 0 or empty. NAT must be enabled in the IPv4 routing table for the WAN connection.

Static

If the Internet provider uses a static prefix, the static /64 prefix for the CLAT prefix can be used in the Subnet ID field, e.g. 2001:db8:: (without the /64 specification). This mode can also be used if 464XLAT is to be used on a VPN connection or tunnel interface. In this case, the VPN interface must have a static IPv6 address configured.

Subnet ID

Subnet ID that is combined with the provider's delegated DHCPv6 prefix. The IPv4 source address is embedded in the resulting prefix when the packet is sent over the WAN. In the case of a WWAN connection (/64 prefix), the parameter can be configured either with the value 0 or left empty (default). If the value static is used for CLAT mode, the static /64 prefix can be configured as the CLAT prefix in the Subnet ID field, e.g. 2001:db8:: (without the /64 specification).

Example for subnet IDs: 0, 1, 12, 1f3b or 2001:db8::

PLAT prefix

IPv6 prefix used on the provider side for translation. If the value is left empty, a DNS prefix discovery according to [RFC 7050](#) is performed to automatically determine the PLAT prefix. Default: 64:ff9b::/96

4.4.1 Additions to the Setup menu

464XLAT

464XLAT according to [RFC 6877](#) is a procedure that translates from IPv4 to IPv6 and back to IPv4. The method is often used by mobile network providers to enable IPv4 access in an IPv6-only APN based on NAT64. Two sides are involved in 464XLAT: The client side or client translator (CLAT - customer-side translator) and the provider translator (PLAT - provider-side translator) or NAT64 gateway of the provider. The LCOS supports the CLAT side to enable a network behind a router to access IPv4 networks. In contrast to DS-Lite, which establishes a 4in6 tunnel to the AFTR gateway, 464XLAT uses a translation of the IPv4 packet to IPv6. On the PLAT side, the packet is translated back into IPv4. The name 464 results from the two-way translation. Generally, the NAT64 prefix 64:ff9b::/96 is used for the translation on the provider side. To use 464XLAT, it is first necessary to configure an IPv6 connection. A 464XLAT peer is then added. The IPv4 default route then points to this peer.

SNMP ID:

2.2.63

Console path:

Setup > WAN

Peer

Set a unique name for this peer.

SNMP ID:

2.2.63.1

Console path:

Setup > WAN > 464XLAT

Possible values:

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

Target-Interface

Name of the underlying WAN interface or the underlying peer, e.g. INTERNET.

SNMP ID:

2.2.63.2

Console path:

Setup > WAN > 464XLAT

Possible values:

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

Subnet-ID

Subnet ID that is combined with the provider's delegated DHCPv6 prefix. The IPv4 source address is embedded in the resulting prefix when the packet is sent over the WAN. In the case of a WWAN connection (/64 prefix), the parameter can be configured either with the value 0 or left empty (default). If the value static is used for CLAT mode, the static /64 prefix can be configured as the CLAT prefix in the Subnet ID field, e.g. 2001:db8:: (without the /64 specification).

Example for subnet IDs: 0, 1, 12, 1f3b or 2001:db8::

SNMP ID:

2.2.63.3

Console path:

Setup > WAN > 464XLAT

Possible values:

Max. 19 characters from `[A-F][a-f][0-9]:./`

Default:

empty

PLAT-Prefix

IPv6 prefix used on the provider side for translation. If the value is left empty, a DNS prefix discovery according to [RFC 7050](#) is performed to automatically determine the PLAT prefix.

SNMP ID:

2.2.63.4

Console path:

Setup > WAN > 464XLAT

Possible values:

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

Default:

64:ff9b::/96

CLAT-Mode

Defines with which method the CLAT prefix should be generated.

SNMP ID:

2.2.63.6

Console path:

Setup > WAN > 464XLAT

Possible values:**DHCPv6-PD**

If the Internet provider uses DHCPv6 prefix delegation, e.g. for DSL or cable connections, the CLAT mode DHCPv6-PD must be used. The subnet ID can be used to control which subnet of the delegated prefix should be used for the CLAT prefix. The subnet ID can be configured as 0, 1 or FF, for example.

WWAN

If the Internet connection is a cellular connection (WWAN), the CLAT mode WWAN must be used. The CLAT prefix is formed from the /64 WAN prefix. The subnet ID must be 0 or empty. NAT must be enabled in the IPv4 routing table for the WAN connection.

Static

If the Internet provider uses a static prefix, the static /64 prefix for the CLAT prefix can be used in the Subnet ID field, e.g. 2001:db8:: (without the /64 specification). This mode can also be used if 464XLAT is to be used on a VPN connection or tunnel interface. In this case, the VPN interface must have a static IPv6 address configured.

Default:

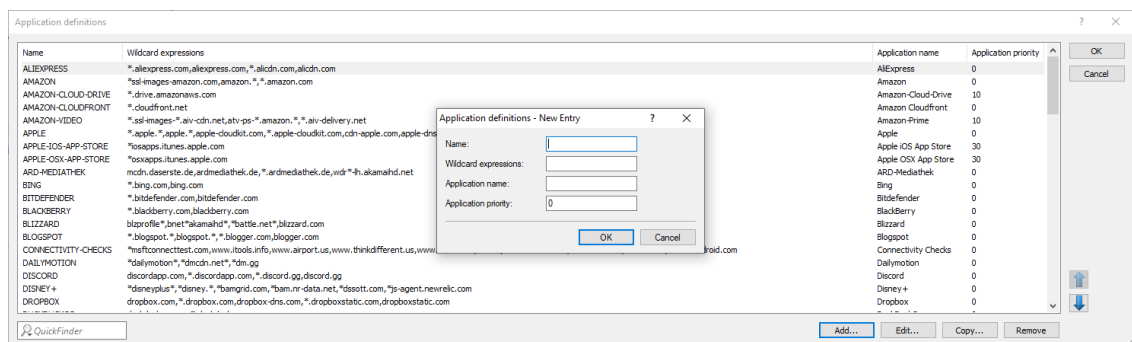
WWAN

5 Firewall

5.1 Central table for DNS-based applications (layer-7 app)

Until now the application definitions for layer-7 detection and layer-7 application control were in separate configuration tables. These have been merged as of LCOS 10.50 to improve usability. This also makes it easy for the definitions already stored for layer-7 detection to be used for layer-7 application control.

The previous tables **Configuration > Firewall/QoS > General > Layer-7 application detection** (CLI: **Setup > Layer-7-App-Detection > HTTP-HTTPS-tracking**) and **Configuration > Firewall/QoS > General > DNS destinations** (CLI: **Setup > Firewall > DNS-Destinations**) have been merged into the new table **Configuration > Firewall/QoS > General > Application definitions** (CLI: **Setup > App-Definitions**).



Name

The name for the destination. The name is used to reference this object.

There can be multiple entries for a name by appending the name of the destination with the # character and adding a number with up to three digits (e.g. "LANCOM", "LANCOM#1", "LANCOM#2" etc.).



To use this entry in the firewall, it has to be referenced under **Configuration > Firewall/QoS > General > DNS destination lists**.

Wildcard expressions

Contains a comma-separated or space-separated list of wildcard expressions. The expressions can contain any number of ? (any character) and * (several arbitrary characters), e.g. "*.lancom.*". The input is limited to 252 characters. If you need more DNS wildcard expressions for a service, then you can group multiple DNS destinations into one referenced object in the **DNS destinations list**.

Unicode characters for internationalized domain names can be entered as follows:

- > UTF-8: Here, one to four bytes must be entered individually as 'x' followed by two hexadecimal digits.
- > UTF-16: Here, one or two double bytes must be entered as 'u' followed by four hexadecimal digits.
- > UTF-32: Here, the value must be entered as 'U' followed by eight hexadecimal digits.

For the layer-7 application detection, use this table to specify which HTTP/HTTPS services are tracked. You should additionally specify parts of the application's host name.

Application name

Name for the tracking of HTTP/HTTPS connections for layer-7 application detection (e.g. youtube). Specifying this name activates the layer-7 application detection.

Application priority

By specifying the priority you set the order in which services are evaluated if certain host-name parts appear in multiple entries (e.g. *google).

5.1.1 Additions to the Setup menu

App-Definitions

Settings for the application definitions for layer-7 detection and layer-7 application control.

SNMP ID:

2.112

Console path:

Setup

Destinations

Table with the destinations for the application definitions for layer-7 detection and layer-7 application control. As soon as the new table contains an entry set for the column [2.112.1.3 Application-Name](#) on page 46, the entry is used by layer-7 detection. To be used in the firewall, the name of the entry must explicitly be entered under [2.110.2 DNS-Destination-List](#).

SNMP ID:

2.112.1

Console path:

Setup > App-Definitions

Name

The name for the destination. The name is used to reference this object.

There can be multiple entries for a name by appending the name of the destination with the # character and adding a number with up to three digits (e.g. "LANCOM", "LANCOM#1", "LANCOM#2" etc.).

SNMP ID:

2.112.1.1

Console path:

Setup > App-Definitions > Destinations

Possible values:

Max. 32 characters (without #) from [A-Z] [0-9] @ { | } ~ ! \$ % & ' () + - , / : ; < = > ? [\] ^ _ .

Max. 36 characters (with #) from [A-Z] [0-9] # @ { | } ~ ! \$ % & ' () + - , / : ; < = > ? [\] ^ _ .

Default:

empty

Wildcard-Expressions

Contains a comma-separated or space-separated list of wildcard expressions. The expressions can contain any number of ? (any character) and * (several arbitrary characters), e.g. "*.lancom.*". The input is limited to 252 characters. If you need more DNS wildcard expressions for a service, then you can group multiple DNS destinations into one referenced object in the **DNS destinations list**.

Unicode characters for internationalized domain names can be entered as follows:

- > UTF-8: Here, one to four bytes must be entered individually as 'x' followed by two hexadecimal digits.
- > UTF-16: Here, one or two double bytes must be entered as 'u' followed by four hexadecimal digits.
- > UTF-32: Here, the value must be entered as 'U' followed by eight hexadecimal digits.

For the layer-7 application detection, use this table to specify which HTTP/HTTPS services are tracked. You should additionally specify parts of the application's host name.

SNMP ID:

2.112.1.2

Console path:

Setup > App-Definitions > Destinations

Possible values:

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

Default:

empty

Application-Name

Name for the tracking of HTTP/HTTPS connections for layer-7 application detection (e.g. youtube).

SNMP ID:

2.112.1.3

Console path:

Setup > App-Definitions > Destinations

Possible values:

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

Default:*empty***Application-Prio**

Set the priority of HTTP/HTTPS tracking by the layer-7 application detection.

SNMP ID:

2.112.1.4

Console path:**Setup > App-Definitions > Destinations****Possible values:**

Max. 5 characters from [0-9]

Default:

0

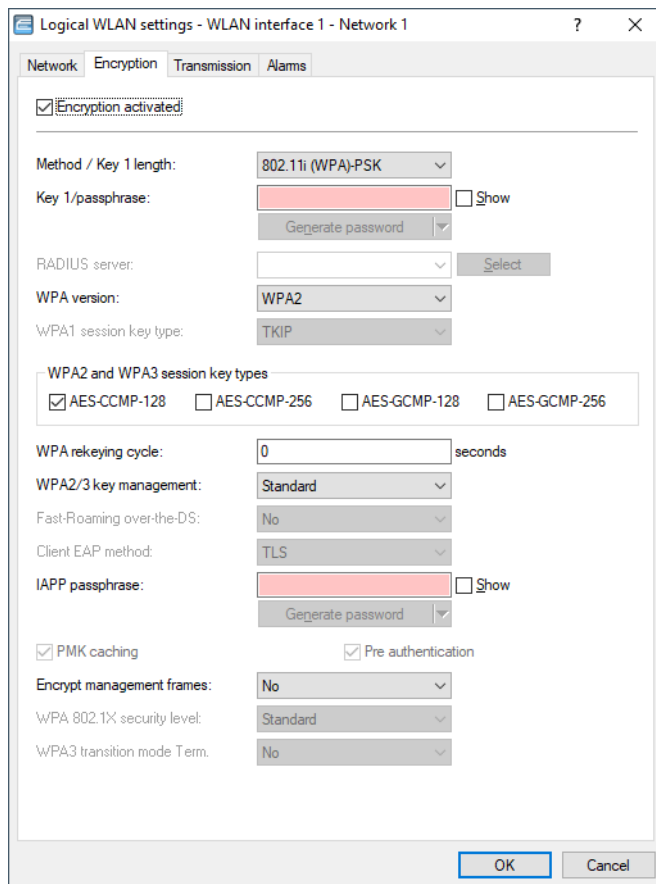
5.2 H.323 ALG no longer supported in the firewall

From LCOS 10.50 the handling of H.323 sessions is no longer supported in the firewall. This functionality is also known as H.323 Application Layer Gateway (ALG). On the command line, the path **Setup > IP-Router > Firewall > Applications > H.323** has been removed.

6 Wireless LAN – WLAN

6.1 Fast Roaming over-the-DS

From LCOS 10.50 a setting enables WLAN clients to be informed that an access point supports Fast Roaming over-the-DS. In LANconfig you configure the option under **Wireless LAN > General > Logical WLAN settings > Encryption**.



Fast-Roaming over-the-DS

With Fast Roaming over-the-DS (Distribution System) you can activate an option of the IEEE 801.11r standard, which takes advantage of the LAN connection between the access points. The roaming request is sent to the access point that the client is connected to. The AP forwards the request to the new access point and the swap is performed. This means significantly faster roaming speeds than possible with the usual “over-the-air fast transition”, which is a big benefit to real-time applications such as VoIP.

6.1.1 Additions to the Setup menu

Fast-Roaming-Over-the-DS

With Fast Roaming over-the-DS (Distribution System) you can activate an option of the IEEE 801.11r standard, which takes advantage of the LAN connection between the access points. The roaming request is sent to the access point that the client is connected to. The AP forwards the request to the new access point and the swap is performed. This means significantly faster roaming speeds than possible with the usual "over-the-air fast transition", which is a big benefit to real-time applications such as VoIP.

SNMP ID:

2.23.20.3.30

Console path:**Setup > Interfaces > WLAN > Encryption****Possible values:**

Yes

No

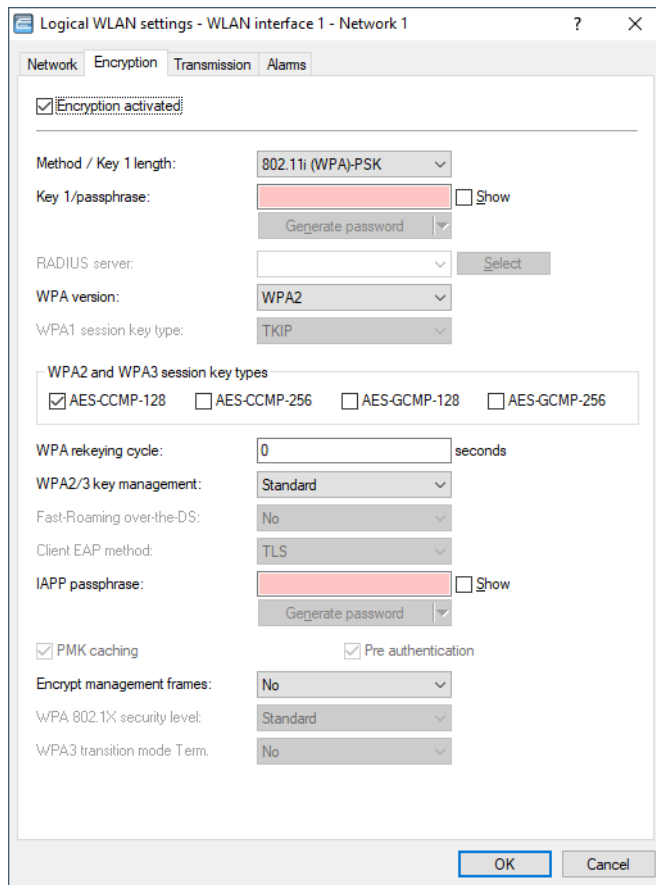
Default:

No

6.2 WPA3 Transition Mode Termination

As of LCOS 10.50, setting a switch can explicitly signal WLAN clients via an additional info element that the WPA3-PSK (SAE) encryption method is supported in mixed WPA2/3 mode. If the client in turn supports the "transition mode termination" feature, it will always use WPA3-PSK (SAE) for logging in at this SSID. This prevents a downgrade to WPA2-PSK, which is otherwise also allowed in mixed WPA2/3 mode.

In LANconfig, configure the option under **Wireless LAN > General > Logical WLAN settings > Encryption**.



WPA3 Transition Mode Term.

This setting uses an additional info element to explicitly signal WLAN clients that the WPA3-PSK (SAE) encryption method is supported in the mixed WPA2/3 mode. If the client supports the “Transition Mode Termination” feature, it will always use WPA3-PSK (SAE) to authenticate with this SSID. This prevents a downgrade to WPA2-PSK, which is otherwise also allowed in mixed WPA2/3 mode.

6.2.1 Additions to the Setup menu

Transition-Termination

Setting the switch explicitly signals WLAN clients via an additional info element that the WPA3-PSK (SAE) encryption method is supported in mixed WPA2/3 mode. If the client in turn supports the “transition mode termination” feature, it will always use WPA3-PSK (SAE) for logging in at this SSID. This prevents a downgrade to WPA2-PSK, which is otherwise also allowed in mixed WPA2/3 mode.

SNMP ID:

2.23.20.3.31

Console path:

Setup > Interfaces > WLAN > Encryption

Possible values:

Yes
No

Default:

No

6.3 WLAN data trace in LANconfig at new location

As of LCOS 10.50 you will no longer find the WLAN data trace under **Wireless LAN > Trace**, but now under **Wireless LAN > General > Extended Settings > Trace**.

7 Public Spot

7.1 Public Spot authentication with name, password and MAC address: Configurable MAC address format

With the login method "Authenticate with name, password and MAC address", the MAC address of the Public Spot client can be checked by an external RADIUS server. The format used to transmit the MAC address to the RADIUS server is set under LCOS 10.50. In the LCOS menu tree, this is done under the menu item **Setup > Public-Spot-Module > MAC-Address-Username-Format**.

7.1.1 Additions to the Setup menu

MAC-Address-Username-Format

With the login method "Authenticate with name, password and MAC address", the MAC address of the Public Spot client can be checked by an external RADIUS server. The format used to transmit the MAC address to the RADIUS server can be set here.

The individual bytes of the MAC address are represented here as the variables %a to %f. In the default setting specified here (%a%b%c-%d%e%f), the bytes of the MAC address are output one after the other with "-" as the separator. In addition to these variables, any of the characters supported by LCOS can be added.

SNMP ID:

2.24.62

Console path:

Setup > Public-Spot-Module

Possible values:

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

Default:

%a%b%c-%d%e%f

8 Backup solutions

From LCOS 10.50, ICMPv6 polling is available as an additional method for detecting failed network connections.

8.1 ICMPv6 polling

As with LCP monitoring or ICMP polling for IPv4, ICMPv6 polling regularly sends requests to a remote peer. Ping commands are transmitted and the answers to them are monitored. Unlike LCP monitoring, the target site for ICMPv6 pings can be freely defined. Pinging a router in a remote network thus provides monitoring for the entire connection and not just the section to the Internet provider.

A ping interval is defined for the remote site in the IPv6 polling table. Further, for the event that replies are missed, the number of retries before the transmission of a new LCP request is defined. Should the transmitter not receive any reply to the retries, the target for the ping requests is classified as unavailable.

Up to four different IPv6 addresses can be entered for each remote site that will be checked in the remote network in parallel. Only if all of the IPv6 addresses are unavailable is the connection considered to have failed.

The settings for ICMPv6 polling in LANconfig can be found in the configuration section **Communication > Protocols > IPv6 polling table**.

Remote site

Here you select the name of a remote site from the list of remote sites.

IPv6 address 1- 4

Enter here up to 4 IPv6 addresses, which are pinged one after the other in order to check the connection for this peer. The connection is considered to be intact even if just one of the specified IPv6 addresses can be reached.

Be sure to choose IPv6 addresses that can be reached reliably to avoid unnecessary backup connections being initiated.

If you set all four IPv6 addresses as ":", the DNS server that is pinged is the one assigned via DHCPv6 or router advertisement.


Ping interval

Enter the ping interval in seconds here.

 If you enter 0 both here and for retries, a default interval of 20 seconds and 5 repetitions is used.

Retries

Enter the number of tries each second if no response is received to a ping. If the repeated pings also go unanswered, the connection is terminated.

 If you enter 0 both here and ping interval, a default interval of 20 seconds and 5 repetitions is used.

Source address (optional)

This is where you can configure an optional sender address to be used instead of the one that would normally be selected automatically for this target address.

8.1.1 Additions to the Setup menu

Polling-Table

In this table, specify the settings for the ICMPv6 polling. As with LCP monitoring or ICMP polling for IPv4, ICMPv6 polling regularly sends requests to a remote peer. Ping commands are transmitted and the answers to them are monitored. Unlike LCP monitoring, the target site for ICMPv6 pings can be freely defined. Pinging a router in a remote network thus provides monitoring for the entire connection and not just the section to the Internet provider.

A ping interval is defined for the remote site in this table. Further, for the event that replies are missed, the number of retries before the transmission of a new LCP request is defined. Should the transmitter not receive any reply to the retries, the target for the ping requests is classified as unavailable.

Up to four different IPv6 addresses can be entered for each remote site that will be checked in the remote network in parallel. Only if all of the IPv6 addresses are unavailable is the connection considered to have failed.

SNMP ID:

2.70.15

Console path:

Setup > IPv6

Peer

Here you enter the name of a peer from the list of remote sites.

SNMP ID:

2.70.15.1

Console path:

Setup > IPv6 > Polling-Table

Possible values:

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

Default:

empty

IPv6-Address-1

Enter here the first of up to 4 IPv6 addresses, which are pinged one after the other in order to check the connection for this peer. The connection is considered to be intact even if just one of the specified IPv6 addresses can be reached.

Be sure to choose IPv6 addresses that can be reached reliably to avoid unnecessary backup connections being initiated.

If you set all four IPv6 addresses as "::", the DNS server that is pinged is the one assigned via DHCPv6 or router advertisement.

SNMP ID:

2.70.15.2

Console path:

Setup > IPv6 > Polling-Table

Possible values:

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

Default:

empty

IPv6-Address-2

Enter here the second of up to 4 IPv6 addresses, which are pinged one after the other in order to check the connection for this peer. The connection is considered to be intact even if just one of the specified IPv6 addresses can be reached.

Be sure to choose IPv6 addresses that can be reached reliably to avoid unnecessary backup connections being initiated.

If you set all four IPv6 addresses as "::", the DNS server that is pinged is the one assigned via DHCPv6 or router advertisement.

SNMP ID:

2.70.15.3

Console path:

Setup > IPv6 > Polling-Table

Possible values:

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

Default:

empty

IPv6-Address-3

Enter here the third of up to 4 IPv6 addresses, which are pinged one after the other in order to check the connection for this peer. The connection is considered to be intact even if just one of the specified IPv6 addresses can be reached.

Be sure to choose IPv6 addresses that can be reached reliably to avoid unnecessary backup connections being initiated.

If you set all four IPv6 addresses as "::", the DNS server that is pinged is the one assigned via DHCPv6 or router advertisement.

SNMP ID:

2.70.15.4

Console path:**Setup > IPv6 > Polling-Table****Possible values:**Max. 39 characters from `[A-F] [a-f] [0-9] : .`**Default:***empty***IPv6-Address-4**

Enter here the fourth of up to 4 IPv6 addresses, which are pinged one after the other in order to check the connection for this peer. The connection is considered to be intact even if just one of the specified IPv6 addresses can be reached.

Be sure to choose IPv6 addresses that can be reached reliably to avoid unnecessary backup connections being initiated.

If you set all four IPv6 addresses as ":", the DNS server that is pinged is the one assigned via DHCPv6 or router advertisement.

SNMP ID:

2.70.15.5

Console path:**Setup > IPv6 > Polling-Table****Possible values:**Max. 39 characters from `[A-F] [a-f] [0-9] : .`**Default:***empty***Time**

Enter the ping interval in seconds here.



If you enter 0 both here and at [2.70.15.7 Try](#) on page 57, a default interval of 20 seconds and 5 repetitions is used.

SNMP ID:

2.70.15.6

Console path:**Setup > IPv6 > Polling-Table****Possible values:**Max. 5 characters from `[0-9]`

Default:*empty***Try**

Enter the number of tries each second if no response is received to a ping. If the repeated pings also go unanswered, the connection is terminated.



If you enter 0 both here and at [2.70.15.6 Time](#) on page 56, a default interval of 20 seconds and 5 repetitions is used.

SNMP ID:

2.70.15.7

Console path:**Setup > IPv6 > Polling-Table****Possible values:**

Max. 3 characters from [0-9]

Default:*empty***Loopback-Addr.**

This is where you can configure an optional sender address to be used instead of the one that would normally be selected automatically for this target address.

SNMP ID:

2.70.15.8

Console path:**Setup > IPv6 > Polling-Table****Possible values:**

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

Default:*empty***Type**

This setting influences the behavior of the polling.

SNMP ID:

2.70.15.9

Console path:

Setup > IPv6 > Polling-Table

Possible values:

Auto

The device only polls actively if it receives no data. ICMP packets received are not considered to be data and are still ignored.

Forced

The device polls in the given interval.

Default:

Auto

9 RADIUS

9.1 Dynamic Peer Discovery

Support for [RFC 7585](#) "Dynamic Peer Discovery for RADIUS/TLS and RADIUS/DTLS Based on the Network Access Identifier (NAI)". Instead of statically forwarding RADIUS requests to one or more RADIUS servers, Dynamic Peer Discovery dynamically finds the correct RADIUS server based on the realm/NAI. If a request arrives, the correct server is found via DNS NAPTR/SRV record.

Dynamic Peer Discovery

Configure the RADIUS Dynamic Peer Discovery here, to dynamically resolve the servers belonging to the RADIUS-Realms.

DPD operating

DNS timeout: seconds


Minimal eff. TTL: seconds

Backoff time: seconds

Attribute values:

Routing tag:

Source address (opt.):

 Dynamic Peer Discovery is only used for RADIUS requests/forwards of the RADIUS server.

LANconfig: **RADIUS > Dyn. Peer Discovery**

Console: **Setup > RADIUS > Dynamic-Peer-Discovery**

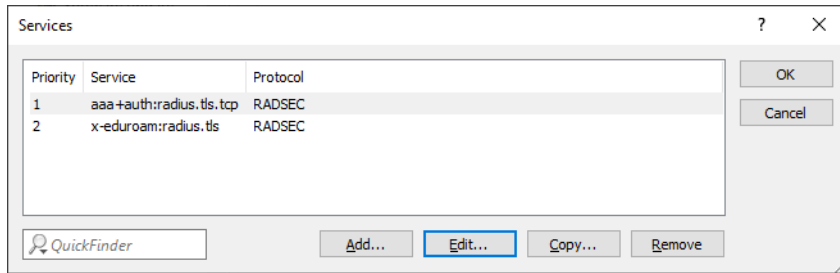
DPD operating

Switch Dynamic Peer Discovery on or off. As soon as Dynamic Peer Discovery is enabled, the RADIUS server branches to dynamic resolution if a specific realm is not defined in its forwarding table. dynamic resolution if a particular realm/NAI is not defined in its forwarding table. Local definitions for realms always have priority.

Services

Table with the services. The service is what is delivered in the NAPTR response in the service. All NAPTR entries are extracted and are extracted and further resolved, which have as service the one with the highest priority from this table. If the default setting, for example, NAPTR records for both service types are supplied, those for "x-eduroam:radius.tls" are ignored. The table is automatically sorted by the LCOS so that higher prioritized services are placed higher up. The protocol that must be used to such a server (RADIUS or RADSEC) is explicitly specified. In case the NAPTR request does not return any usable records, this table still has the meaning, which prefix is put in front of the NAI for the fallback SRV request. The highest priority entry is taken from the table for which a prefix is defined in an internally fixed table. Currently the services radius.tls,

radius.tls.tcp, radsec.tcp and radius.udp are defined, which respond to a prefix of `_radius.tls._tcp.`, `_radsec.tcp.` or `_radius._udp.` respectively.



Priority

Priority of this service.

Service

The services themselves. The defaults are “aaa+auth:radius.tls.tcp” and “x-eduroam:radius.tls”.

Protocol

The protocol (RADIUS or RADSEC) used for this service.

DNS timeout

The amount of time in seconds within which all DNS requests for an NAI must be handled. This also includes the two-step variant via NAPTR and subsequent SRV queries. Default: 3 seconds

Minimal eff. TTL

TTL values reported by the DNS server that are shorter than this time are raised to this value. Default: 60 seconds

Backoff time

If a resolution ends in an error (DNS response with error, timeout...), this is the time in seconds for which no new resolution attempts should be made for this realm. Default: 600 seconds

Attribute values

RADIUS attributes to be added or changed when forwarding to servers discovered by Dynamic Peer Discovery.

Routing tag

The routing tag that Dynamic Peer Discovery should use for its DNS queries. Default: 0

Source address (opt.)

The loopback address to use when forwarding to RADIUS servers determined by Dynamic Peer Discovery.

9.1.1 Additions to the Setup menu

Dynamic-Peer-Discovery

Support for [RFC 7585](#) “Dynamic Peer Discovery for RADIUS/TLS and RADIUS/DTLS Based on the Network Access Identifier (NAI)”. Instead of statically forwarding RADIUS requests to one or more RADIUS servers, Dynamic Peer Discovery dynamically finds the correct RADIUS server based on the realm/NAI. If a request arrives, the correct server is found via DNS NAPTR/SRV record.

SNMP ID:

2.25.23

Console path:**Setup > RADIUS****Operating**

Switch Dynamic Peer Discovery on or off. As soon as Dynamic Peer Discovery is enabled, the RADIUS server branches to dynamic resolution if a specific realm is not defined in its forwarding table. dynamic resolution if a particular realm/NAI is not defined in its forwarding table. Local definitions for realms always have priority.

SNMP ID:

2.25.23.1

Console path:**Setup > RADIUS > Dynamic-Peer-Discovery****Possible values:****No**
Yes**Default:**

No

Routing-Tag

The routing tag that Dynamic Peer Discovery should use for its DNS queries.

SNMP ID:

2.25.23.2

Console path:**Setup > RADIUS > Dynamic-Peer-Discovery****Possible values:**

Max. 5 characters from [0-9]

Default:

0

Loopback-Address

The loopback address to use when forwarding to RADIUS servers determined by Dynamic Peer Discovery.

SNMP ID:

2.25.23.3

Console path:**Setup > RADIUS > Dynamic-Peer-Discovery****Possible values:**Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-./:;<=>?[\]^_.`**Default:***empty***Attribute-Values**

RADIUS attributes to be added or changed when forwarding to servers discovered by Dynamic Peer Discovery.

SNMP ID:

2.25.23.4

Console path:**Setup > RADIUS > Dynamic-Peer-Discovery****Possible values:**Max. 251 characters from `[A-Z][a-z][0-9]#@{|}~!"$%&'()*+,-./:;<=>?[\]^_.``**Default:***empty***Services**

TTable with the services. The service is what is delivered in the NAPTR response in the service. All NAPTR entries are extracted and are extracted and further resolved, which have as service the one with the highest priority from this table. If the default setting, for example, NAPTR records for both service types are supplied, those for "x-eduroam:radius.tls" are ignored. The table is automatically sorted by the LCOS so that higher prioritized services are placed higher up. The protocol that must be used to such a server (RADIUS or RADSEC) is explicitly specified. In case the NAPTR request does not return any usable records, this table still has the meaning, which prefix is put in front of the NAI for the fallback SRV request. The highest priority entry is taken from the table for which a prefix is defined in an internally fixed table. Currently the services radius.tls, radius.tls.tcp, radsec.tcp and radius.udp are defined, which respond to a prefix of _radiustls._tcp., _radsec.tcp. or _radius._udp. respectively.

SNMP ID:

2.25.23.5

Console path:**Setup > RADIUS > Dynamic-Peer-Discovery**

Priority

Priority of this service.

SNMP ID:

2.25.23.5.1

Console path:

Setup > RADIUS > Dynamic-Peer-Discovery > Services

Possible values:

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

Service

The services themselves. The defaults are "aaa+auth:radius.tls.tcp" and "x-eduroam:radius.tls".

SNMP ID:

2.25.23.5.2

Console path:

Setup > RADIUS > Dynamic-Peer-Discovery > Services

Possible values:

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

Protocol

The protocol used for this service.

SNMP-ID:

2.25.23.5.3

Pfad Konsole:

Setup > RADIUS > Dynamic-Peer-Discovery > Services

Mögliche Werte:

**RADIUS
RADSEC**

DNS-Timeout

The amount of time in seconds within which all DNS requests for an NAI must be handled. This also includes the two-step variant via NAPTR and subsequent SRV queries.

SNMP ID:

2.25.23.6

Console path:**Setup > RADIUS > Dynamic-Peer-Discovery****Possible values:**

Max. 10 characters from [0-9]

Default:

3

Min.-Eff.-TTL

TTL values reported by the DNS server that are shorter than this time are raised to this value.

SNMP ID:

2.25.23.7

Console path:**Setup > RADIUS > Dynamic-Peer-Discovery****Possible values:**

Max. 10 characters from [0-9]

Default:

60

Backoff-Time

If a resolution ends in an error (DNS response with error, timeout...), this is the time in seconds for which no new resolution attempts should be made for this realm.

SNMP ID:

2.25.23.8

Console path:**Setup > RADIUS > Dynamic-Peer-Discovery****Possible values:**

Max. 10 characters from [0-9]

Default:

600

10 Other services


10.1 Appending several DHCP Option 43 sub-options in the DHCP server

With regard to the options configured under **IPv4 > DHCPv4 > DHCP options**, each of these was previously sent by the LCOS DHCP server to requesting DHCP clients as a separate DHCP option 43. From LCOS 10.50 it is now possible to append several sub-options to the DHCP option 43.

Append Sub-Option

For each sub-option of option 43, a separate option is created and transmitted. This switch allows several sub-options of DHCP option 43 to be appended. To do this, set this to **Yes**. Appending occurs when:

- > **Option-Number** equals 43
- > **Sub-Option-Number** is not equal to zero
- > Above that in the table an option 43 with a sub-option number not equal to zero


 Note that each option can have a maximum of 255 characters.

10.1.1 Additions to the Setup menu

Append-Sub-Option

For each sub-option of option 43, a separate option is created and transmitted. This switch allows several sub-options of DHCP option 43 to be appended. To do this, set this to "Yes". Appending occurs when:

- > **Option-Number** equals 43
- > **Sub-Option-Number** is not equal to zero
- > Above that in the table an option 43 with a sub-option number not equal to zero

 Note that each option can have a maximum of 255 characters.

SNMP ID:

2.10.26.8

Console path:**Setup > DHCP > Additional-Options****Possible values:****Yes**

If possible, append the sub-options of DHCP option 43.

No

Submit this sub-option of DHCP option 43 as a separate option.

10.2 Function for switching to alternative DSL modem firmware

This table contains the settings for the modem firmware. As there is no "best" DSL firmware for every situation, as of LCOS 10.50 you can switch to another modem firmware available in the LCOS, if necessary.

For this purpose, the settings in LANconfig moved to **Interfaces > WAN > Further XDSL settings**. Other generic settings for xDSL were also moved here so that they can now be set individually for each xDSL interface.

LANconfig: **Interfaces > WAN > Further XDSL settings**

Command prompt: **Setup > xDSL > General**

Vendor ID

The code specified by the German Federal Network Agency for LANCOM devices does not work in all countries. In these cases, for example in Switzerland, the alternative identifier must be selected.

Use Tx rate limit for QoS

This switch changes the use of the sync data rate as the QoS data rate. If activated (default), the sync data rate is used as the QoS data rate. Otherwise the sync data rate is not used and the interface behaves like a DSL interface with regard to the QoS data rate.

Modem firmware

This switch allows you to swap between two versions of the modem firmware stored in the LCOS.



This column is only available for devices with a LCOS that contains an alternative modem firmware.

10.2.1 Additions to the Setup menu

General

This table contains the settings for the modem firmware. As there is no "best" DSL firmware for every situation, you can switch to another modem firmware available in the LCOS, if necessary.

SNMP ID:

2.42.5

Console path:**Setup > xDSL****Interface**

Fixed value for this interface: 1 for XDSL-1, 2 for XDSL-2, etc.

SNMP ID:

2.42.5.1

Console path:**Setup > xDSL > General****Vendor-ID**

The code specified by the German Federal Network Agency for LANCOM devices does not work in all countries. In these cases, for example in Switzerland, the alternative identifier must be selected.

SNMP ID:

2.42.5.2

Console path:**Setup > xDSL > General****Possible values:****Default-ID**
Alternate-ID**Default:**

Default-ID

Sync-limits-Tx-Rate

This setting makes it possible to deactivate the limitation of the transmission data rate to the sync data rate. This is used for quality assurance tests, for example to determine the data rate at which the modem puts a limit on throughput.

SNMP ID:

2.42.5.3

Console path:**Setup > xDSL > General**

Possible values:**On**

The sync data rate is used as the QoS data rate.

Off


The sync data rate is not used and the interface behaves like a DSL interface with regard to the QoS data rate.

Default:

On

Modem-Firmware

This switch allows you to swap between two versions of the modem firmware stored in the LCOS.

 This column is only available for devices with a LCOS that contains an alternative modem firmware.

SNMP ID:

2.42.5.4

Console path:

Setup > xDSL > General

Possible values:**Default**

This chooses the version preferred by LANCOM.

Alternate

This setting selects a version that improves the behavior at some connections.

Default:

Default

10.3 DNS settings moved to own area

As of LCOS 10.50, you can find the DNS settings no longer under **IPv4 > DNS** or **IPv4 > DNS filter/aliases**, but in a separate section under **DNS > General** and **DNS > Filters/Aliases**.

10.4 DNS filter for DNS data tunnels

Methods and tools exist that use DNS packets to smuggle in data and avoid checks, for example by the firewall. This data tunnel can then be used to transport any data via the DNS protocol. Although this method conforms to the protocol's

standards, the establishment of these tunnels should be prevented under certain circumstances. The data tunnels are detected according to certain characteristics or properties of the DNS packets.

As of LCOS 10.50 you can set up this DNS filter for DNS data tunnels.

LANconfig: **DNS > Filter/Aliases > DNS tunnel filter**

Command prompt: **Setup > DNS > Tunnel-Filter**

Activated

The tunnel filter can be switched on and off with this switch.

Minimum TTL

Minimum TTL after which resource records are accepted. If a record (with the exception of A and AAAA) has a smaller TTL, the entire packet is discarded.

Area: 0-99; Default: 5

Address limit

Maximum number of A and AAAA records with a TTL smaller than the minimum TTL that are still accepted before the complete packet is discarded.

Area: 0-99; Default: 3

10.4.1 Additions to the Setup menu

Tunnel-Filter

Methods and tools exist that use DNS packets to smuggle in data and avoid checks, for example by the firewall. This data tunnel can then be used to transport any data via the DNS protocol.

Although this method conforms to the protocol's standards, the establishment of these tunnels should be prevented under certain circumstances. The data tunnels are detected according to certain characteristics or properties of the DNS packets.

SNMP ID:

2.17.21

Console path:

Setup > DNS

Operating

The tunnel filter can be switched on and off with this switch.

SNMP ID:

2.17.21.1

Console path:**Setup > DNS > Tunnel-Filter****Possible values:****No**

Tunnel filter is disabled.

Yes

Tunnel filter is enabled.

Default:

Yes

Minimum-TTL

Minimum TTL after which resource records are accepted. If a record (with the exception of A and AAAA) has a smaller TTL, the entire packet is discarded.

SNMP ID:

2.17.21.2

Console path:**Setup > DNS > Tunnel-Filter****Possible values:**

0 ... 99

Default:

5

Address-Limit

Maximum number of A and AAAA records with a TTL smaller than the minimum TTL that are still accepted before the complete packet is discarded.

SNMP ID:

2.17.21.3

Console path:**Setup > DNS > Tunnel-Filter****Possible values:**

0 ... 99

Default:

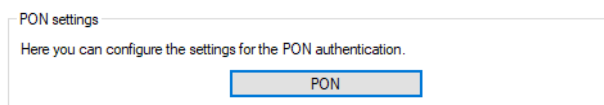
3

10.5 GPON support

GPON (Gigabit Passive Optical Network) is an optical transmission standard for fiber optic connections (FTTH). LANCOM offers GPON SFP modules for this purpose, which are available in LANCOM routers with SFP interface. The list of compatible devices can be found in the respective GPON SFP data sheet.

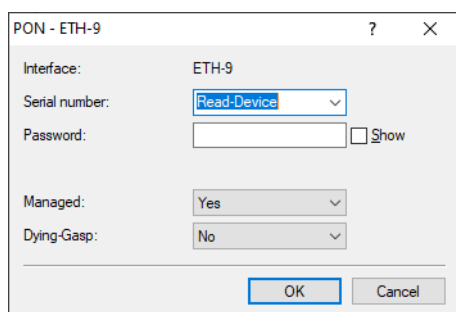
With a GPON module, the LANCOM router can be operated directly on the fiber optic connection of the provider without a separate modem. Please contact your provider if operation without modem and with SFP module is supported. Usually GPON modems are authenticated by serial number and/or GPON password, so operation without provider support is not possible.

As a rule, nothing has to be configured in the device for GPON operation.



LANconfig: **Interfaces > WAN > PON**

Console: **Setup > Interfaces > PON**



Interface

Select here the SFP interface in which the PON module is plugged, e.g. SFP-1.


Serial number


Each module already has a unique serial number from the manufacturer in the format manufacturer ID+number, e.g. GPON12345678. The serial number consists of 8 octets. The octets 1 to 4 contain the vendor ID, the octets 5 to 8 a manufacturer specific serial number. The representation is normally mixed ASCII/Hex. The vendor ID is represented in ASCII, the manufacturer-specific serial number in Hex. The length is 12 characters. The serial number is read from or written to the module.

Communicate this serial number to your Internet provider to register the module.

Change this serial number only if you want to replace an existing device that is already registered with your provider's OLT and you do not want a new registration with the provider.

A provider can authenticate a GPON modem uniquely by serial number, serial number and password, or by password only.

 In case of a module exchange, please reset the configuration to Default, otherwise the old serial number and password will also be adopted for the new module. Therefore proceed as follows: remove the old module, reset the configuration line, then insert the new module.

 Default is the special value **Read-Device**. If this is set, the configuration is read from the module and transferred to the LCOS configuration.

Password

Enter the PON password here if your provider performs password authentication. Other terms for PON password are "ONT installation identifier" or "PLOAM password". The password consists of 10 octets in ASCII representation. The length is 10 characters. The password is empty by default.

You can get the PON password for your connection from your Internet provider.

Managed

Configure here if the modem should be managed by the operating system. In this case the system writes the configured serial number and the PON password (recommended).

Dying-Gasp

Configure here if the PON modem should activate Dying Gasp. Dying Gasp is a signal that the modem sends to the provider to signal the loss of power.

10.5.1 Additions to the Setup menu

PON

This menu contains the settings for the PON (Passive Optical Network) interfaces.

GPON (Gigabit Passive Optical Network) is an optical transmission standard for fiber optic connections (FTTH). LANCOM offers GPON SFP modules for this purpose, which are available in LANCOM routers with SFP interface. The list of compatible devices can be found in the respective GPON SFP data sheet.

With a GPON module, the LANCOM router can be operated directly on the fiber optic connection of the provider without a separate modem. Please contact your provider if operation without modem and with SFP module is supported. Usually GPON modems are authenticated by serial number and/or GPON password, so operation without provider support is not possible.

SNMP ID:

2.23.23

Console path:

Setup > Interfaces

Interface

The PON interfaces available on the device. Select here the SFP interface in which the PON module is plugged, e.g. SFP-1.

SNMP ID:

2.23.23.1

Console path:

Setup > Interfaces > PON


Serial-number


Each module already has a unique serial number from the manufacturer in the format manufacturer ID+number, e.g. GPON12345678. The serial number consists of 8 octets. The octets 1 to 4 contain the vendor ID, the octets 5 to 8 a manufacturer specific serial number. The representation is normally mixed ASCII/Hex. The vendor ID is represented in ASCII, the manufacturer-specific serial number in Hex. The length is 12 characters. The serial number is read from or written to the module.

Communicate this serial number to your Internet provider to register the module.

Change this serial number only if you want to replace an existing device that is already registered with your provider's OLT and you do not want a new registration with the provider.

A provider can authenticate a GPON modem uniquely by serial number, serial number and password, or by password only.

 In case of a module exchange, please reset the configuration to Default, otherwise the old serial number and password will also be adopted for the new module. Therefore proceed as follows: remove the old module, reset the configuration line, then insert the new module.

 Default is the special value **Read-Device**. If this is set, the configuration is read from the module and transferred to the LCOS configuration.

SNMP ID:

2.23.23.2

Console path:

Setup > Interfaces > PON

Possible values:

Max. 12 characters from `[A-Z][a-z][0-9]#@[|]~!$%&'()*+,-./:;<=>?[\]^_``

Special values:

Read-Device

Reads the configuration from the module and transfers it to the LCOS configuration.

Password

Enter the PON password here if your provider performs password authentication. Other terms for PON password are "ONT installation identifier" or "PLOAM password". The password consists of 10 octets in ASCII representation. The length is 10 characters. The password is empty by default.

You can get the PON password for your connection from your Internet provider.

SNMP ID:

2.23.23.3

Console path:

Setup > Interfaces > PON

Possible values:

Max. 10 characters from `[A-Z][a-z][0-9]#@[|]~!$%&'()*+,-./:;<=>?[\]^_``

Managed

Configure here if the modem should be managed by the operating system. In this case the system writes the configured serial number and the PON password (recommended).

SNMP ID:

2.23.23.4

Console path:**Setup > Interfaces > PON****Possible values:****No**
Yes**Dying-Gasp**

Configure here if the PON modem should activate Dying Gasp. Dying Gasp is a signal that the modem sends to the provider to signal the loss of power.

SNMP ID:

2.23.23.5

Console path:**Setup > Interfaces > PON****Possible values:****No**
Yes

10.6 802.1X authenticator for Ethernet ports

Using the 802.1X authenticator, devices connected to the Ethernet ports of a LANCOM device can be authenticated using 802.1X. This increases security against unauthorized access to the network via Ethernet cables and ports.

As of LCOS 10.50 RU4, it is possible to specify a separate RADIUS server only for the MAC authentication bypass. This allows separate RADIUS servers to be used for 802.1X and the MAC authentication bypass. This is done via the entry **Setup > LAN > IEEE802.1X > Authenticator-Ifc-Setup > Bypass-RADIUS-Server** on the command line.

10.6.1 Additions to the Setup menu

Bypass-RADIUS-Server

The RADIUS server specified here is used only for the MAC authentication bypass. This allows separate RADIUS servers to be used for 802.1X and the MAC authentication bypass. To do this, reference one of the entries under [2.30.3 RADIUS server](#) or create a new entry there if necessary. You can adjust the format of the transmitted MAC address under [2.4.10.4 Username-Attribute-Format](#).

SNMP ID:

2.4.10.3.6

Console path:**Setup > LAN > IEEE802.1X > Authenticator-lfc-Setup****Possible values:****Name from Setup > IEEE802.1X > RADIUS-Server**Max. 16 characters from `# [A-Z] [a-z] [0-9] @ { | } ~ ! $ % & ' () + - , / : ; < = > ? [\] ^ _ . ``

11 Enhancements in the menu system

11.1 Require-Msg-Authenticator

New switch as of LCOS 10.50 SU14. Defines whether the presence of the message authenticator attribute in RADIUS messages is enforced on the client side. The client side is the side that receives the RADIUS accept/fail.

SNMP ID:

2.2.22.28

Console path:

Setup > WAN > RADIUS

Possible values:

No

Access requests do not have to contain a message authenticator.

Yes

Access requests must always contain a message authenticator.

Default:

No

11.2 L2TP-Require-Msg-Authenticator

New switch as of LCOS 10.50 SU14. Defines whether the presence of the message authenticator attribute in RADIUS messages is enforced on the client side. The client side is the side that receives the RADIUS accept/fail.

SNMP ID:

2.2.22.29

Console path:

Setup > WAN > RADIUS

Possible values:

No

Access requests do not have to contain a message authenticator.

Yes

Access requests must always contain a message authenticator.

Default:

No

11.3 Require-Msg-Authenticator

New switch as of LCOS 10.50 SU14. Defines whether the presence of the message authenticator attribute in RADIUS messages is enforced on the client side. The client side is the side that receives the RADIUS accept/fail.

SNMP ID:

2.11.81.1.10

Console path:**Setup > Config > RADIUS > Server****Possible values:****No**

Access requests do not have to contain a message authenticator.

Yes

Access requests must always contain a message authenticator.

Default:

No

11.4 Require-Msg-Authenticator

New switch as of LCOS 10.50 SU14. Defines whether the presence of the message authenticator attribute in RADIUS messages is enforced on the client side. The client side is the side that receives the RADIUS accept/fail.

SNMP ID:

2.12.29.21

Console path:**Setup > WLAN > RADIUS-Access-Check****Possible values:****No**

Access requests do not have to contain a message authenticator.

Yes

Access requests must always contain a message authenticator.

Default:

No

11.5 Backup-Require-Msg-Authenticator

New switch as of LCOS 10.50 SU14. Defines whether the presence of the message authenticator attribute in RADIUS messages is enforced on the client side. The client side is the side that receives the RADIUS accept/fail.

SNMP ID:

2.12.29.22

Console path:

Setup > WLAN > RADIUS-Access-Check

Possible values:**No**

Access requests do not have to contain a message authenticator.

Yes

Access requests must always contain a message authenticator.

Default:

No

11.6 Require-Msg-Authenticator

New switch as of LCOS 10.50 SU14. Defines whether the presence of the message authenticator attribute in RADIUS messages is enforced on the client side. The client side is the side that receives the RADIUS accept/fail.

SNMP ID:

2.19.36.9.1.1.11

Console path:

Setup > VPN > IKEv2 > RADIUS > Authorization > Server

Possible values:**No**

Access requests do not have to contain a message authenticator.

Yes

Access requests must always contain a message authenticator.

Default:

No

11.7 Require-Msg-Authenticator

New switch as of LCOS 10.50 SU14. Defines whether the presence of the message authenticator attribute in RADIUS messages is enforced on the client side. The client side is the side that receives the RADIUS accept/fail.

SNMP ID:

2.25.10.2.6

Console path:

Setup > RADIUS > Server > Clients

Possible values:**No**

Access requests do not have to contain a message authenticator.

Yes

Access requests must always contain a message authenticator.

Proxy-Only

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

Default:

No

11.8 Require-Msg-Authenticator

New switch as of LCOS 10.50 SU14. Defines whether the presence of the message authenticator attribute in RADIUS messages is enforced on the client side. The client side is the side that receives the RADIUS accept/fail.

SNMP ID:

2.25.10.3.18

Console path:

Setup > RADIUS > Server > Forward-Servers

Possible values:**No**

Access requests do not have to contain a message authenticator.

Yes

Access requests must always contain a message authenticator.

Default:

No

11.9 Require-Msg-Authenticator

New switch as of LCOS 10.50 SU14. Defines whether the presence of the message authenticator attribute in RADIUS messages is enforced on the client side. The client side is the side that receives the RADIUS accept/fail.

SNMP ID:

2.25.10.16.6

Console path:

Setup > RADIUS > Server > IPv6-Clients

Possible values:**No**

Access requests do not have to contain a message authenticator.

Yes

Access requests must always contain a message authenticator.

Proxy-Only

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

Default:

No