

LCOS 10.80

Addendum

11/2023

Contents

- 1 Addendum to LCOS version 10.80.....5**
- 2 Diagnosis.....6**
 - 2.1 Trace to an attached USB drive.....6
 - 2.2 Output capture data to a USB drive.....7
 - 2.2.1 Additions to the Setup menu.....7
- 3 Security.....10**
 - 3.1 Length of the main device password.....10
 - 3.1.1 Additions to the Setup menu.....10
- 4 Routing and WAN connections.....12**
 - 4.1 DPS switchover now considers line priorities.....12
 - 4.1.1 Additions to the Setup menu.....13
 - 4.2 Priority bit for WAN connection.....14
 - 4.2.1 Additions to the Setup menu.....14
 - 4.3 Automatic APN.....15
 - 4.3.1 Additions to the Setup menu.....16
 - 4.4 Automatic WWAN connection establishment for unconfigured devices.....17
 - 4.5 Parameter LTE-Delayed-Attach removed.....17
 - 4.6 Cellular cold standby.....18
 - 4.6.1 Additions to the Setup menu.....18
- 5 IPv6.....20**
 - 5.1 Multiple DHCPv6 relay targets.....20
 - 5.1.1 Additions to the Setup menu.....21
 - 5.2 Further options for the DHCPv6 client.....25
 - 5.2.1 Additions to the Setup menu.....26
 - 5.3 DS-Lite tunnel with target interface.....28
 - 5.3.1 Additions to the Setup menu.....29
- 6 Firewall.....30**
 - 6.1 Manually executing actions from the action table.....30
 - 6.1.1 Additions to the Setup menu.....30
- 7 Virtual Private Networks – VPN.....31**
 - 7.1 LANCOM Trusted Access.....31
 - 7.1.1 Additions to the Setup menu.....32
- 8 WLAN management.....36**
 - 8.1 Kanal-Profile im WLC.....36
 - 8.1.1 Additions to the Setup menu.....37
 - 8.2 LACP configuration via WLC.....39
 - 8.2.1 Additions to the Setup menu.....40
- 9 Backup solutions.....42**
 - 9.1 Support for vRouter redundancy in Amazon AWS.....42

10 Other services.....	43
10.1 DHCPv4 client options.....	43
10.1.1 Additions to the Setup menu.....	43
10.2 Accounting.....	46
10.2.1 Operating principles.....	47
10.2.2 Switching accounting on or off on the fly.....	47
10.2.3 Data traffic counting.....	47
10.2.4 Other changes to accounting.....	48
10.2.5 Additions to the Setup menu.....	49
10.3 New Netflow parameter “Active-Flow-Timeout”.....	50
10.3.1 Additions to the Setup menu.....	50
10.4 PON password in hexadecimal format.....	50
10.4.1 Additions to the Setup menu.....	51
10.5 ACME-Client.....	51
10.5.1 ACME client configuration.....	53
10.5.2 Additions to the Setup menu.....	54
10.6 Execute actions on incoming SMS.....	65
10.6.1 Additions to the Setup menu.....	66
11 Enhancements in the menu system.....	70
11.1 Additions to the Setup menu.....	70
11.1.1 Configuration-Upload-Check.....	70
11.1.2 Syslog.....	70
11.1.3 LCOSCap-WAN-Access.....	71
11.1.4 RPCap-WAN-Access.....	71
11.1.5 Operating.....	72

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

Adenauerstr. 20/B2

52146 Würselen

Germany

www.lancom-systems.com

1 Addendum to LCOS version 10.80

This document describes the changes and enhancements in LCOS version 10.80 since the previous version.


2 Diagnosis

2.1 Trace to an attached USB drive

As of LCOS 10.80 it is possible to save traces to a connected USB drive, e.g. a USB stick in the background. An active console session is not required for this, as the recording is carried out in the background.

After recording, the file can be accessed by plugging the USB stick into a computer. Alternatively, the /usb/ directory on the device can be accessed remotely via SCP.

The USB drive must be FAT32 formatted. The device writes to the USB stick until it is full, after which the capture stops.

 It is not possible to write or load a file to the internal flash of the device.

An ICMP trace on the console is e.g. redirected to a USB drive as follows:

```
Trace # ICMP > /usb/file.lct
```

The ICMP trace is stopped as follows:

```
Trace # ICMP > /usb/file.lct or Trace - all > /usb/file.lct
```

The show command "show trace-file" shows active trace sessions on USB.

A `Trace - all` does not terminate the running sessions that are being recorded on USB, only the active traces of the active console session.

```
root@lc1900ef-aa:/
> tr # icmp >/usb/my
created trace session for '/usb/my.lct'
/usb/my.lct:
ICMP                ON

root@lc1900ef-aa:/
> show trace-file

/usb/my.lct:
  ICMP                ON

root@lc1900ef-aa:/
> tr # tcp >/usb/my
/usb/my.lct:
TCP                 ON

root@lc1900ef-aa:/
> show trace-file

/usb/my.lct:
  ICMP                ON
  TCP                 ON

root@lc1900ef-aa:/
> tr - all >/usb/my
/usb/my.lct:
remove trace session for '/usb/my.lct'
```

2.2 Output capture data to a USB drive

As of LCOS 10.80 Wireshark captures performed in the background by the router can be output to a connected USB drive, e.g. a USB stick. An active management session from the computer to the device is not required for this.

After recording, the file can be accessed by plugging the USB stick into a computer. Alternatively, the /usb/ directory on the device can be accessed remotely via SCP.

The USB drive must be FAT32 formatted. The device writes to the USB stick until it is full, after which the capture stops.



It is not possible to write or load a file to the internal flash of the device.

Enter the file name and all other necessary information using the command line in the table **Setup > Packet-Capture > Capture-to-File > Files**.

2.2.1 Additions to the Setup menu

Capture-to-File

This menu contains the settings for recording network data traffic to a USB drive in the PCAP format. This is used by Wireshark, for example.

SNMP ID:

2.63.20

Console path:

Setup > Packet-Capture

Files

In this table you configure the Wireshark traces on a connected USB drive.

SNMP ID:

2.63.20.1

Console path:

Setup > Packet-Capture > Capture-to-File

Name

Name of the entry.

SNMP ID:

2.63.20.1.1

Console path:

Setup > Packet-Capture > Capture-to-File > Files

Possible values:

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

Operating

Defines whether the configuration entry is active or inactive.

SNMP ID:

2.63.20.1.2

Console path:

Setup > Packet-Capture > Capture-to-File > Files

Possible values:

No
Yes

File-Name

Full path and name of Wireshark capture file, e.g. `/usb/capture.pcap`.

SNMP ID:

2.63.20.1.3

Console path:

Setup > Packet-Capture > Capture-to-File > Files

Possible values:

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

Interface

Name of the logical interface used for the Wireshark capture, e.g. DSL-1, LAN-1, etc.

SNMP ID:

2.63.20.1.4

Console path:

Setup > Packet-Capture > Capture-to-File > Files

Possible values:

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

MAC-Address

MAC address to which the capture should be restricted, formatted without separators like "-" or ":".

SNMP ID:

2.63.20.1.5

Console path:

Setup > Packet-Capture > Capture-to-File > Files

Possible values:

Max. 17 characters from `[0-9a-e]`

3 Security

3.1 Length of the main device password

As of LCOS 10.80 the maximum length of the main device password has been increased to 128 characters. This has also been adjusted for other administrators and SNMP users.

Special attention should be paid to the WLC with managed access points in case of password synchronization. If the longer password is used on the WLC, all of the managed access points must also operate LCOS 10.80. In this case, it is no longer possible to locally log in to access points with less than LCOS 10.80.

The above information only applies if the new option of using more than 16 characters in the password is used.

 Please note that a firmware downgrade to a version less than LCOS 10.80 with passwords longer than 16 characters is not supported.

3.1.1 Additions to the Setup menu

Authentication-Password

Enter the user password necessary for authentication here and repeat it in the box below.

SNMP ID:

2.9.32.6

Console path:

Setup > SNMP > Users

Possible values:

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

Default:

empty

Privacy-Password

Enter the user password required by the encryption here and repeat it in the box below.

SNMP ID:

2.9.32.9

Console path:

Setup > SNMP > Users

Possible values:

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

Default:

empty

Password

Password for this entry.

SNMP ID:

2.11.21.2

Console path:

Setup > Config > Admins

Possible values:

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

Default:

empty

4 Routing and WAN connections

4.1 DPS switchover now considers line priorities

As of LCOS 10.80, DPS switchover supports an option that allows line priorities to be taken into account for Dynamic Path Selection.

To configure this feature in LANconfig, go to **IP Router > Routing > SD-WAN Dynamic Path Selection > Switchover-Profiles**.

Regard LB prio

This parameter controls the behavior of the DPS session switchover.

i If the table is reset to the default, the row "AGGRESSIVE-SWITCHOVER" is set to "Yes" and "SOFT-SWITCHOVER" is set to "No".

Possible values:

Yes


Sessions also switch between interfaces with the same score, provided that the prioritization specified in table [Policy-Assignments](#) favors one of them. Appropriately, the output tables **Status > Firewall > Dynamic-Path-Selection > IPv4-Preferred-Lines-Log** and **Status > Firewall > Dynamic-Path-Selection > IPv6-Preferred-Lines-Log** will only show the highest-priority interface as "Preferred" in such a case. This is also the interface that all sessions switch over to, with a speed and in the corresponding number of intermediate steps according to the other parameters in the corresponding switchover profile.

i This setting is useful in the following scenario, an an example: LTE or 5G is used together with VDSL. In some locations, LTE/ 5G is significantly better than VDSL. For cost reasons, however, DSL should be used first instead of LTE/5G, since this should only be used as a booster. This works for example with the priorities of the load balancer. With the default behavior, however, the switchover does not switch back from the bad line to the better one.

i This is the default for new entries.

No

The behavior of the DPS session switchover is that it is only performed if another line is actually better (better score) than the line currently used by the session. Not taken into account is the prioritization that can be entered into the load balancer policy assignments. For this reason there are no switch-overs between interfaces with identical policy scores.

 This is the default for entries from before LCOS 10.80.

4.1.1 Additions to the Setup menu

Regard-LB-Prio

This parameter controls the behavior of the DPS session switchover.

 If the table is reset to the default, the row "AGGRESSIVE-SWITCHOVER" is set to "Yes" and "SOFT-SWITCHOVER" is set to "No".

SNMP ID:

2.110.4.32.4


Console path:

Setup > Firewall > Dynamic-Path-Selection > Switchover-Profiles

Possible values:

Yes


Sessions also switch between interfaces with the same score, provided that the prioritization specified in table [2.110.4.17 Policy-Assignments](#) favors one of them. In this case, the output tables **Status > Firewall > Dynamic-Path-Selection > IPv4-Preferred-Lines-Log** and **Status > Firewall > Dynamic-Path-Selection > IPv6-Preferred-Lines-Log** will only show the highest-priority interface as "Preferred". This is also the interface that all sessions switch over to, with a speed and with the number of intermediate steps as determined by the other parameters in the corresponding switchover profile.

 This setting is useful in the following scenario, an an example: LTE or 5G is used together with VDSL. In some locations, LTE/5G is significantly faster than VDSL. For cost reasons, however, DSL should be used first instead of LTE/5G, since this should only be used as a booster. This also works with the priorities of the load balancer, for example. With the default behavior, however, the switchover does not switch back from the bad line to the better one.

 This is the default for new entries.

No

The DPS session switchover is only performed if another line is actually better (higher score) than the line currently used by the session. Not taken into account is the prioritization that can be entered into the load balancer policy assignments. For this reason there are no switch-overs between interfaces with identical policy scores.

 This is the default for entries from before LCOS 10.80.

Default:

Yes

4.2 Priority bit for WAN connection

As of LCOS 10.80 the priority bit is supported for WAN connections.

To do this, the parameter **VLAN priority mapping** was expanded and the new parameter **VLAN prio value** was added. Both can be found in LANconfig under **Communication > Remote Sites > Remote sites (DSL)**.

VLAN priority mapping

This determines how the packets should be marked in the VLAN priority field.

Value

All packets sent to the WAN are marked with the priority tag configured under **VLAN- Prio-Value**. However, this only happens if a VLAN other than 0 is also configured. Otherwise it would be equivalent to being set to "Off".

VLAN prio value

This value is set as the VLAN priority value when **VLAN priority mapping** is set to "Value".

4.2.1 Additions to the Setup menu

Prio-Mapping

This entry controls how the priority mapping functions.

SNMP ID:

2.2.19.17

Console path:

Setup > WAN > DSL-Broadband-Peers

Possible values:**Off**

Prio-mapping is disabled.

1TR-112

The value "1TR112" maps the precedence (i.e., the top 3 bits) of the DSCP into the VLAN Prio field if the DSCP is not EF. If it is EF, the precedence of CS6 is mapped into the VLAN prio (110b).

DSCP

The "DSCP" value maps the precedence (i.e. the top 3 bits) of the DSCP into the VLAN Prio field.

Value

All packets sent to the WAN are marked with the priority tag configured under [2.2.19.20 Prio-Value](#) on page 15. However, this only happens if a VLAN other than 0 is also configured. Otherwise it would be equivalent to being set to "Off".

Default:

Off

Prio-Value

This value is set as the VLAN priority value when [2.2.19.17 Prio-Mapping](#) on page 14 is set to "Value".

SNMP ID:

2.2.19.20

Console path:

Setup > WAN > DSL-Broadband-Peers

Possible values:

0 ... 7

4.3 Automatic APN

As of LCOS 10.80 mobile routers support the option of using the APN from the internal carrier list of the operating system. It is no longer necessary to manually configure an APN for a WWAN connection. A manual configuration of the APN is only necessary for private APNs or private mobile networks. With the automatic selection of the APN, all common mobile phone providers are supported. For this purpose, the provider is queried from the SIM card (MCC/MNC) and searched for in the internal database.

The new parameter for this is the **APN mode** under **Interfaces > WAN > Mobile settings > Mobile profiles**.

APN mode

Defines in which mode the APN is to be used.

- > With Automatic, the APN is taken from the internal database of the provider settings of the operating system. For this purpose, the provider is queried from the SIM card (MCC/MNC) and searched for in the internal database. The "Automatic" mode only works with public provider APNs and not with private APNs. For private APNs, the mode must be set to "Manual" and the APN entered in the "APN" field.
- > For Manual, the APN from the APN field is used

4.3.1 Additions to the Setup menu

APN-Mode

Defines in which mode the APN is to be used.

SNMP ID:

2.23.41.1.14

Console path:

Setup > Interfaces > Mobile > Profiles

Possible values:

Auto

With Automatic, the APN is taken from the internal database of the provider settings of the operating system. For this purpose, the provider is queried from the SIM card (MCC/MNC) and searched for in the

internal database. The “Automatic” mode only works with public provider APNs and not with private APNs. For private APNs, the mode must be set to “Manual” and the APN entered in the field [2.23.41.1.3 APN](#).

Manual

For Manual, the APN from the field [2.23.41.1.3 APN](#) is used.

Default:

Auto

4.4 Automatic WWAN connection establishment for unconfigured devices

As of LCOS 10.80 it is possible for devices with WWAN to automatically connect to the Internet over the cellular connection, so allowing the LANCOM Management Cloud to perform a zero-touch rollout. For this, the LCOS features new default entries for setting up a WWAN remote site.

The following requirements must be met for this:

- The device must feature at least LCOS 10.80 or be updated, for example via USB stick, to the necessary LCOS version.
- The inserted SIM card must not have a PIN. This can be deactivated on a cellular phone beforehand.
- The provider's APN must be included in the internal carrier list of the LCOS. The scenario with private APNs is not supported.
- The provider must support IPv4. A zero-touch rollout scenario via IPv6-only APNs is currently not supported.

Clients located in the LAN behind the device cannot connect to the Internet in this state, since the device still has the automatic LAN IP address, which cannot be used with forwarding. To do this, the device needs a fixed IP address on the LAN interface. This happens automatically when the LMC assigns a network to the device. The device itself can reach any Internet address.

4.5 Parameter LTE-Delayed-Attach removed

As of LCOS 10.80, the **LTE-Delayed-Attach** parameter is omitted under **Setup > Interfaces > Mobile > Profiles**.

4.6 Cellular cold standby

As of LCOS 10.80 there is the new parameter **Cold-Standby** under **Interfaces > WAN > Mobile profiles**.

The screenshot shows a configuration window titled "Mobile profiles - New Entry". It contains the following fields and options:

- Name: [Text input field]
- PIN: [Text input field] with a "Show" checkbox.
- APN: [Text input field]
- APN mode: [Auto] (dropdown menu)
- PDP Type: [IPv4] (dropdown menu)
- Network selection: [Auto] (dropdown menu)
- Network name: [Text input field]
- Transmission mode: [Auto] (dropdown menu)
- Downstream rate: [0] kbit/s
- Upstream rate: [0] kbit/s
- Cold-Standby: [No] (dropdown menu)
- 5G/4G Bands section with a checked "All" checkbox and a grid of checkboxes for various frequency bands:
 - 2100 MHz (B1)
 - 1800 MHz (B3)
 - 850 MHz (B5)
 - 900 MHz (B8)
 - 700 MHz (B13)
 - 1900 MHz (B25)
 - 700 MHz (B29)
 - 2600 MHz (B41)
 - 1900 MHz (B2)
 - 2100 MHz (B4)
 - 2600 MHz (B7)
 - 700 MHz (B12)
 - 800 MHz (B20)
 - 800 MHz (B26)
 - 2300 MHz (B30)

At the bottom of the window are "OK" and "Cancel" buttons.

Cold-Standby

This parameter specifies whether the cellular modem should be logged into the cellular network in non-backup cases. If "Yes" the cellular modem is not logged into the cellular network in the non-backup case. In the case of a backup, it takes correspondingly longer for the module to establish a complete backup connection. This function is only supported if the backup table is used. This function has no effect or cannot be used when working with administrative distances, since in that case the WWAN modem has always established an active data connection. Default: No.

4.6.1 Additions to the Setup menu

Cold-Standby

Specifies whether the cellular modem should be logged into the cellular network in non-backup cases. If "Yes" the cellular modem is not logged into the cellular network in the non-backup case. In the case of a backup, it takes correspondingly longer for the module to fully establish a backup connection. This function is only supported if the backup table is used. This function has no effect or cannot be used when working with administrative distances, since in that case the WWAN modem has always established an active data connection.

SNMP ID:

2.23.41.1.15

Console path:

Setup > Interfaces > Mobile > Profiles

Possible values:

Yes

No

Default:

No

5 IPv6

5.1 Multiple DHCPv6 relay targets

As of LCOS 10.80 the DHCPv6 relay agent can be configured with several server destinations to which the relay agent sends the requests. The requests are always sent to all configured servers at the same time.

An optional IPv6 sender address can also be specified, which the relay agent uses for packets directed to the DHCPv6 server.

You can find the new settings under **IPv6 > DHCPv6 > Relay agent interfaces**.

Destination address

The IPv6 address of the (destination) DHCPv6 server which the relay agent is to forward DHCP requests to. The address can be either a unicast or link-local multicast address. When using a link-local multicast address, you must specify the destination interface where the DHCPv6 server is to be reached. All DHCPv6 servers and relay agents are available at the link-local multicast address "ff02::1:2".



Using the parameters **2nd Destination address** to **4th Destination address** you can define additional server destinations.




If multiple server destinations are configured, the requests are always sent to all configured servers at the same time.

Destination interface

The destination interface where the parent DHCPv6 server or the next relay agent is to be reached. This information is essential if a link-local multicast address is configured under the destination address, as link local-multicast addresses are only valid at that respective link.

 Using the parameters **2nd Destination interface** to **4th Destination interface** you can define additional server destinations.

 If multiple server destinations are configured, the requests are always sent to all configured servers at the same time.


Source address (optional)


Set an optional source address that the relay agent uses for packets directed to the DHCPv6 server.

5.1.1 Additions to the Setup menu

Dest-Address

Define the IPv6 address of the (destination) DHCPv6 server which the relay agent is to forward DHCP requests to. The address can be either a unicast or link-local multicast address. When using a link-local multicast address, you must specify the destination interface where the DHCPv6 server is to be reached. All DHCPv6 servers and relay agents are available at the link-local multicast address ff02::1:2.

 You can define additional server targets via [2.70.3.3.1.6 Dest-Address-2](#) on page 22, [2.70.3.3.1.8 Dest-Address-3](#) on page 23 and [2.70.3.3.1.10 Dest-Address-4](#) on page 24.

 In case of multiple configured server targets, the requests are always sent to all configured servers simultaneously.

SNMP ID:

2.70.3.3.1.4

Console path:

Setup > IPv6 > DHCPv6 > Relay-Agent > Interface-List

Possible values:


Max. 39 characters from `[A-Z] [a-z] [0-9]` :

Default:

ff02::1:2

Dest-Interface

Here you specify the destination interface where the parent DHCPv6 server or the next relay agent is to be reached. This information is essential if a link-local multicast address is configured under the destination address, as link local-multicast addresses are only valid at that respective link.

 You can define additional server targets via [2.70.3.3.1.7 Dest-Interface-2](#) on page 22, [2.70.3.3.1.9 Dest-Interface-3](#) on page 23 and [2.70.3.3.1.11 Dest-Interface-4](#) on page 24.

 In case of multiple configured server targets, the requests are always sent to all configured servers simultaneously.

SNMP ID:

2.70.3.3.1.5

Console path:

Setup > IPv6 > DHCPv6 > Relay-Agent > Interface-List

Possible values:


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

Default:

empty

Dest-Address-2

Define a second IPv6 address of a (destination) DHCPv6 server which the relay agent is to forward DHCP requests to. The address can be either a unicast or link-local multicast address. When using a link-local multicast address, you must specify the destination interface where the DHCPv6 server is to be reached. All DHCPv6 servers and relay agents are available at the link-local multicast address ff02::1:2.

 You can define additional server targets via [2.70.3.3.1.4 Dest-Address](#) on page 21, [2.70.3.3.1.8 Dest-Address-3](#) on page 23 and [2.70.3.3.1.10 Dest-Address-4](#) on page 24.

 In case of multiple configured server targets, the requests are always sent to all configured servers simultaneously.

SNMP ID:

2.70.3.3.1.6

Console path:

Setup > IPv6 > DHCPv6 > Relay-Agent > Interface-List

Possible values:


Max. 39 characters from `[A-Z][a-z][0-9]:`


Default:

empty

Dest-Interface-2

Here you specify a second destination interface where the parent DHCPv6 server or the next relay agent is to be reached. This information is essential if a link-local multicast address is configured under the destination address, as link local-multicast addresses are only valid at that respective link.

 You can define additional server targets via [2.70.3.3.1.5 Dest-Interface](#) on page 21, [2.70.3.3.1.9 Dest-Interface-3](#) on page 23 and [2.70.3.3.1.11 Dest-Interface-4](#) on page 24.

 In case of multiple configured server targets, the requests are always sent to all configured servers simultaneously.

SNMP ID:

2.70.3.3.1.7

Console path:

Setup > IPv6 > DHCPv6 > Relay-Agent > Interface-List

Possible values:


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

Default:

empty

Dest-Address-3

Define a third IPv6 address of a (destination) DHCPv6 server which the relay agent is to forward DHCP requests to. The address can be either a unicast or link-local multicast address. When using a link-local multicast address, you must specify the destination interface where the DHCPv6 server is to be reached. All DHCPv6 servers and relay agents are available at the link-local multicast address ff02::1:2.

 You can define additional server targets via [2.70.3.3.1.4 Dest-Address](#) on page 21, [2.70.3.3.1.6 Dest-Address-2](#) on page 22 and [2.70.3.3.1.10 Dest-Address-4](#) on page 24.

 In case of multiple configured server targets, the requests are always sent to all configured servers simultaneously.

SNMP ID:

2.70.3.3.1.8

Console path:

Setup > IPv6 > DHCPv6 > Relay-Agent > Interface-List

Possible values:


Max. 39 characters from `[A-Z][a-z][0-9]:`

Default:

empty

Dest-Interface-3

Here you specify a third destination interface where the parent DHCPv6 server or the next relay agent is to be reached. This information is essential if a link-local multicast address is configured under the destination address, as link local-multicast addresses are only valid at that respective link.

 You can define additional server targets via [2.70.3.3.1.5 Dest-Interface](#) on page 21, [2.70.3.3.1.7 Dest-Interface-2](#) on page 22 and [2.70.3.3.1.11 Dest-Interface-4](#) on page 24.

 In case of multiple configured server targets, the requests are always sent to all configured servers simultaneously.

SNMP ID:

2.70.3.3.1.9

Console path:

Setup > IPv6 > DHCPv6 > Relay-Agent > Interface-List

Possible values:


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

Default:

empty

Dest-Address-4

Define a fourth IPv6 address of a (destination) DHCPv6 server which the relay agent is to forward DHCP requests to. The address can be either a unicast or link-local multicast address. When using a link-local multicast address, you must specify the destination interface where the DHCPv6 server is to be reached. All DHCPv6 servers and relay agents are available at the link-local multicast address ff02::1:2.

 You can define additional server targets via [2.70.3.3.1.4 Dest-Address](#) on page 21, [2.70.3.3.1.6 Dest-Address-2](#) on page 22 and [2.70.3.3.1.8 Dest-Address-3](#) on page 23.

 In case of multiple configured server targets, the requests are always sent to all configured servers simultaneously.

SNMP ID:

2.70.3.3.1.10

Console path:

Setup > IPv6 > DHCPv6 > Relay-Agent > Interface-List

Possible values:


Max. 39 characters from `[A-Z][a-z][0-9]:`

Default:

empty

Dest-Interface-4

Here you specify a fourth destination interface where the parent DHCPv6 server or the next relay agent is to be reached. This information is essential if a link-local multicast address is configured under the destination address, as link local-multicast addresses are only valid at that respective link.

 You can define additional server targets via [2.70.3.3.1.5 Dest-Interface](#) on page 21, [2.70.3.3.1.7 Dest-Interface-2](#) on page 22 and [2.70.3.3.1.9 Dest-Interface-3](#) on page 23.

 In case of multiple configured server targets, the requests are always sent to all configured servers simultaneously.

SNMP ID:

2.70.3.3.1.11

Console path:

Setup > IPv6 > DHCPv6 > Relay-Agent > Interface-List

Possible values:

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

Default:

empty

Dest-Loopback

Specify here an optional sender address that the relay agent uses for packets towards the DHCPv6 server.

SNMP ID:

2.70.3.3.1.12

Console path:

Setup > IPv6 > DHCPv6 > Relay-Agent > Interface-List

Possible values:

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

Default:

empty

5.2 Further options for the DHCPv6 client

As of LCOS 10.80 certain options can be configured for the DHCPv6 client, which are then transmitted. This is required if the Internet provider expects certain data in DHCPv6 messages. The options are found in the DHCP Options table under **IPv6 > DHCPv6 > DHCPv6-Client > Additional options** and can be freely configured.

Interface name

Interface that the DHCPv6 client should use for this option, e.g. WAN remote site or IPv6 LAN network.

Option number

Specifies the assigned IANA number of the DHCPv6 option as defined in the RFC.

Option type

Specifies the type of the DHCPv6 option. Possible values: String, Integer8, Integer16, Integer32, IPv6-Addresses, Domain-List, Hexdump, or Dont-Send



The option type "Dont-Send" means that no option content is sent, only the option number in the option request if no option value is provided in the RFC.

Option value

Specifies the content of the DHCPv6 option

A comma and/or space-separated list can also be specified, except in the case of a string. For integer values the C-codes for numbers apply, i.e. 0x results in a hex value and if the number starts with 0, it is an octal value. With the Integer8 type, it is additionally possible to specify a single hex string (of even length) without a separator. Values from the default options can be overwritten. The following options cannot be overridden or configured: Elapsed-Time, Server-DUID, Reconfigure-Accept and Rapid-Commit.

Request option

Specifies whether the DHCPv6 request should request the option number. The behavior is defined via the respective RFC of the DHCPv6 option. Possible values: Yes, No

5.2.1 Additions to the Setup menu

Additional-Options

In this table certain options can be configured for the DHCPv6 client.

SNMP ID:

2.70.3.2.5

Console path:

Setup > IPv6 > DHCPv6 > Client

Interface-Name

Interface that the DHCPv6 client should use for this option, e.g. WAN remote site or IPv6 LAN network.

SNMP ID:

2.70.3.2.5.1

Console path:

Setup > IPv6 > DHCPv6 > Client > Additional-Options

Possible values:

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

Default:

empty

Option-Number

Specifies the assigned IANA number of the DHCP option as defined in the RFC.

SNMP ID:

2.70.3.2.5.2

Console path:

Setup > IPv6 > DHCPv6 > Client > Additional-Options

Possible values:

Max. 5 characters from [0-9]

Default:

empty

Option-Type

Specifies the type of the DHCPv6 option.

SNMP ID:

2.70.3.2.5.3

Console path:

Setup > IPv6 > DHCPv6 > Client > Additional-Options

Possible values:

Integer8
Integer16
Integer32
IPv6 addresses
Domain-List
String
Hexdump
Do-not-send

This option type means that no option content is sent, only the option number in the option request if no option value is provided in the RFC.

Option-Value

Specifies the content of the DHCPv6 option.

A comma and/or space-separated list can also be specified, except in the case of a string. For integer values the C-codes for numbers apply, i.e. 0x results in a hex value and if the number starts with 0, it is an octal value. With the Integer8 type, it is additionally possible to specify a single hex string (of even length) without a separator. Values from the default options can be overwritten. The following options cannot be overridden or configured: Elapsed-Time, Server-DUID, Reconfigure-Accept and Rapid-Commit.

SNMP ID:

2.70.3.2.5.4

Console path:

Setup > IPv6 > DHCPv6 > Client > Additional-Options

Possible values:

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

Default:

empty

Request-Option

Specifies whether the DHCPv6-Option-Request should request the option number. The behavior is defined via the respective RFC of the DHCPv6 option.

SNMP ID:

2.70.3.2.5.5

Console path:

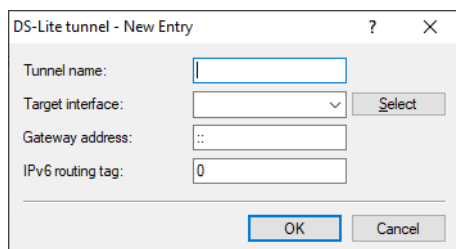
Setup > IPv6 > DHCPv6 > Client > Additional-Options

Possible values:

- Yes
- No

5.3 DS-Lite tunnel with target interface

As of LCOS 10.80, there is a new **Target interface** column for DS-Lite tunnels under LANconfig **IPv6 > Tunnel > DS-Lite tunnel**.



Target interface

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

5.3.1 Additions to the Setup menu

Target-Interface

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

SNMP ID:

2.2.40.5

Console path:

Setup > WAN > DS-Lite-Tunnel

Possible values:

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

6 Firewall

6.1 Manually executing actions from the action table

As of LCOS 10.80 actions can be manually triggered in the action table by simulating events. Certain connection events (e.g. establish, disconnect, volume budget event, etc.) can be triggered without the event actually occurring. This allows entries in the action table to be tested. The action of the action table to which the event applies is executed. All entries that match the event are always executed.


Under `/Setup/WAN` there is a new command-line action to do this: `Manual-Action-Start`.


6.1.1 Additions to the Setup menu

Manual-Action-Start

This action can be used to manually execute actions in the action table by simulating events. Certain connection events (e.g. establish, disconnect, volume budget event, etc.) can be triggered without the event actually occurring. This allows entries in the action table to be tested. The action of the action table to which the event applies is executed. All entries that match the event are always executed.

Example: `do Manual-Action-Start internet/establish`

 The result of the execution can be analyzed with the "connect" trace.

 If several instruction chains are stored for a connection (e.g. for different DynDNS hosts), they are always all executed. Whether it is necessary to specify an IPv6 address depends on the entry in the action table. When testing DynDNS entries or entries that use an IP address, the IP address must always be transferred with `-4` or `-6`.

SNMP ID:

2.2.64

Console path:

Setup > WAN

Possible arguments:

[-4 <IPv4-address>]

Optional specification of an IPv4 address

[-6 <IPv6-address>]

Optional specification of an IPv6 address

<Connection-Name>/<Condition>]

<Condition> is one of the following conditions: ESTABLISH, DISCONNECT, FAILURE, ESTABLISH-FAILURE, VOLUME-BUDGET-EXPIRED, VOLUME-BUDGET-RESET.

If no condition is specified, the default is to establish a connection, i.e. the ESTABLISH condition.

7 Virtual Private Networks – VPN

7.1 LANCOM Trusted Access

As of LCOS 10.80, LANCOM Trusted Access is supported, a solution for cloud-managed secure network access.

LANCOM Trusted Access is the trusted network access security solution for enterprise networks. It enables secure and scalable access to enterprise applications for employees in the office, at home, or on the road, protecting modern hybrid working from anywhere, anytime. The LANCOM Trusted Access solution adapts to increasing security requirements in your organization and enables both cloud-managed VPN client networking for access to entire networks and the move to a zero trust security architecture for comprehensive network security. Based on granular access rights, users are only granted access to applications that have been assigned to them (zero trust principle). Existing systems for managing users and user groups (Active Directory) can be fully integrated into the LANCOM Management Cloud (LMC). For smaller networks, the LMC alternatively offers internal user management. LANCOM Trusted Access 100% GDPR compliant and scales for small businesses as well as for very large networks with several thousand users.

show

Using the show command, you can display the groups and the peers assigned to them““.

Syntax:

```
show lta
Usage:
show lta <option> [<parameter>...]

Options:
groups [group1 ...]: if one or more groups are specified, show the given groups, otherwise show all groups
peers [peer1 ...] : if one or more peers are specified, show the given peers, otherwise show all peers
help,
? : this help
```

Example:

```
> l /Status/Firewall/LTA-Database/Groups/
Group-UUID                               IP-Address                               Peer
-----
550e8400-e29b-11d4-a716-446655440000    2001:db8::23                             PEER-1
550e8400-e29b-22d4-a726-446655440000    2001:db8::23                             PEER-1
550e8400-e29b-22d4-a726-446655440000    2001:db8::42                             PEER-2
550e8400-e29b-33d4-a736-446655440000    2001:db8::42                             PEER-2

> l /Status/VPN/LTA/Connections/
Peer           Certificate-ID           User-ID           User-Name
-----
PEER-1         11111111-1111-1111-1111-111111111111    22222222-2222-2222-2222-222222222222
TESTER-LTA-USER-NAME
33333333-3333-3333-3333-333333333333    TESTER-LTA-ENDPOINT-NAME
PEER-2         11111111-1111-1111-1111-111111111111    22222222-2222-2222-2222-222222222222
TESTER-LTA-USER-NAME

> show lta groups
550e8400-e29b-11d4-a716-446655440000
  PEER-1                               2001:db8::23

550e8400-e29b-22d4-a726-446655440000
  PEER-1                               2001:db8::23
  PEER-2                               2001:db8::42

550e8400-e29b-33d4-a736-446655440000
```

```

PEER-2                                2001:db8::42
> show lta peers
PEER-1                                2001:db8::23
550e8400-e29b-11d4-a716-446655440000
550e8400-e29b-22d4-a726-446655440000
PEER-2                                2001:db8::42
550e8400-e29b-22d4-a726-446655440000
550e8400-e29b-33d4-a736-446655440000
    
```

7.1.1 Additions to the Setup menu

Objects

Elements/objects that are to be used in the firewall rules table are defined in the objects table. Objects can be:

- > Individual computers (MAC or IP address, hostname)
- > Complete networks
- > Protocols
- > Services (ports or port ranges, e.g. HTTP, Mail&News, FTP,...)
- > Linking of group UUIDs from the LANCOM Trusted Access with station names

SNMP ID:


2.8.10.1

Console path:

Setup > IP-Router > Firewall

Name

Specify here a unique name for this object.

 Object names for the LANCOM Trusted Access always start with the abbreviation "LTA-" and are usually created and managed by the LANCOM Management Cloud. In a firewall rule, you can use this name to reference an LTA group object as a source.

SNMP ID:

2.8.10.1.1

Console path:

Setup > IP-Router > Firewall > Objects

Possible values:

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

Default:


empty


Description


Objects can be combined and hierarchically structured in any way. For example, objects for the TCP and UDP protocols can be defined first. Building upon this, objects can subsequently be created, for example, for FTP (= TCP + ports 20 and 21), HTTP (= TCP + port 80) and DNS (= TCP, UDP + port 53). These can in turn be combined into one object that contains all the definitions of the individual objects.

Stations and services can be defined in the objects table according to the following rules.

Table 1: Objects for firewall actions

Description	Object-ID	Examples and comments
Local network	%L	
Remote sites	%H	Name must be in DSL/ISDN/PPTP or VPN remote site list
Host name	%D	
MAC-Address	%E	00:A0:57:01:02:03
IP-Address	%A	%A10.0.0.1, 10.0.0.2; %A0 (all addresses)
Netmask	%M	%M255.255.255.0
Protocol (TCP/UDP/ICMP, etc.)	%P	%P6 (for TCP)
Service (port)	%S	%S20-25 (for ports 20 to 25)
LANCOM Trusted Access	%g	 The UUID for objects of the LANCOM Trusted Access must meet the following criteria: <ul style="list-style-type: none"> > They may only contain hexadecimal numbers ('0'...'9', 'a'...'f', 'A'...'F') and the minus sign ('-'). > The minus may only be at propositions 8, 13, 18 and 23 > The minus character must appear 4 times in total > The UUID must be at least 36 characters long Example: 550e8400-e29b-11d4-a716-446655440000

 Definitions of the same type can be created as comma-separated lists, such as host lists/address lists (%A10.0.0.1, 10.0.0.2) or with ranges separated by hyphens, such as port lists (%S20-25). Specifying "0" or an empty string denotes the Any object.

 For configuration from the CLI (Telnet or terminal application), the combined parameters (port, destination, source) must be enclosed with quotation marks (").

SNMP ID:

2.8.10.1.2

Console path:

Setup > IP-Router > Firewall > Objects

Possible values:

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

Default:

empty

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:

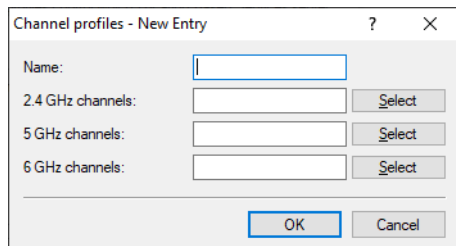
Local-network

8 WLAN management

8.1 Kanal-Profil im WLC

As of LCOS 10.80, the configuration of WLAN channels has been moved from the physical WLAN profile to the newly created channel profile. Within the channel profile, the WLAN channels can be defined per frequency band. In this way, even channels whose numbering is repeated in different frequency bands (e.g. at 2.4 GHz and 6 GHz) can be defined uniquely.

You create the configuration of the WLAN channels via **WLAN Controller > Profiles > Advanced Profiles > Channel Profiles**.



The screenshot shows a dialog box titled "Channel profiles - New Entry". It has a standard window header with a question mark and a close button. The main area contains four input fields: "Name:" followed by a text box; "2.4 GHz channels:" followed by a text box and a "Select" button; "5 GHz channels:" followed by a text box and a "Select" button; and "6 GHz channels:" followed by a text box and a "Select" button. At the bottom of the dialog are "OK" and "Cancel" buttons.

Name

Name of the profile.

2.4 GHz channels

Select the 2.4 GHz channels for this profile.

5 GHz channels

Select the 5 GHz channels for this profile.


6 GHz channels


Select the 6 GHz channels for this profile.

Then link the newly created channel profile within the physical WLAN profile under **WLAN controller > Profiles > Physical WLAN parameters**.

Channel profile

Select a channel profile. See [Channel Profile Table](#).

 The DEFAULT profile activates all allowed channels of the set country.

 When upgrading to LCOS 10.80, the previous channel settings are automatically migrated to a new channel profile.

8.1.1 Additions to the Setup menu

Channel-Profile

Select the name of a channel profile. See [2.37.1.30 Channel-Profiles](#) on page 37.

 The DEFAULT profile activates all allowed channels of the set country.

SNMP ID:


2.37.1.2.29

Console path:

Setup > WLAN-Management > AP-Configuration > Radioprofiles

Channel-Profiles

Use this table to create the configuration of the WLAN channels. Within the channel profile, the WLAN channels can be defined per frequency band. In this way, you can also uniquely define channels whose numbering is repeated in different frequency bands (e.g., at 2.4 GHz and 6 GHz). Then link newly created channel profiles within the physical WLAN profile.

 The DEFAULT profile activates all allowed channels.

SNMP-ID:

2.37.1.30

Pfad Konsole:**Setup > WLAN-Management > AP-Configuration****Name**Name of the profile. Specify it in [2.37.1.2.29 Channel-Profile](#) on page 37.**SNMP ID:**

2.37.1.30.1

Console path:**Setup > WLAN-Management > AP-Configuration > Channel-Profiles****2.4GHz-Channels**

Select the 2.4 GHz channels for this profile.

SNMP ID:

2.37.1.30.2

Console path:**Setup > WLAN-Management > AP-Configuration > Channel-Profiles****5GHz-Channels**

Select the 5 GHz channels for this profile.

SNMP ID:

2.37.1.30.3

Console path:**Setup > WLAN-Management > AP-Configuration > Channel-Profiles****6GHz-Channels**

Select the 6 GHz channels for this profile.

SNMP ID:

2.37.1.30.4

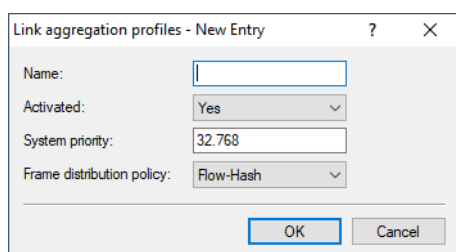
Console path:**Setup > WLAN-Management > AP-Configuration > Channel-Profiles**

8.2 LACP configuration via WLC

LACP according to IEEE 802.1AX allows several Ethernet connections to be bundled in a so-called LAG (Link Aggregation Group) in order to increase the achievable data throughput within the LAG. For this purpose, the outgoing packets on the sending side are distributed to the various individual links within the LAG on the basis of the configured frame distribution policy.

The LACP configuration of the managed access points can be specified and configured by the WLC from LCOS 10.80 RU1.

You create the configuration of the link aggregation profiles under **WLAN Controller > Profiles > Advanced Profiles > Link aggregation profiles**.

**Name**

The name of this LAG (Link Aggregation Group).

Activated

Enables or disables this LAG (Link Aggregation Group).

System priority

The system priority of this LAG (Link Aggregation Group).

Frame distribution policy

Frame distribution policy of this LAG (Link Aggregation Group). Possible options:

Flow-Hash

For outgoing packets, a flow hash is formed over the IP addresses and TCP/UDP ports contained and the packets are distributed to the individual links of the LAG on the basis of this. This achieves a distribution at session level, so that sessions of a single client can also be distributed to multiple links. This setting is recommended for most scenarios.

Source-Dest-MAC

Outgoing packets are distributed to the individual links of the LAG based on the contained pair of source MAC address and destination MAC address.

8.2.1 Additions to the Setup menu

Link-Aggregation-Profiles

LACP according to IEEE 802.1AX allows several Ethernet connections to be bundled in a so-called LAG (Link Aggregation Group) in order to increase the achievable data throughput within the LAG. For this purpose, the outgoing packets on the sending side are distributed to the various individual links within the LAG on the basis of the configured frame distribution policy.

SNMP ID:

2.37.1.29

Console path:**Setup > WLAN-Management > AP-Configuration****Name**

The name of this LAG (Link Aggregation Group).

SNMP ID:

2.37.1.29.1

Console path:**Setup > WLAN-Management > AP-Configuration > Link-Aggregation-Profiles****Possible values:**Max. 31 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/;<=>?[\]^_.`**Default:***empty***Operating**

Enables or disables this LAG (Link Aggregation Group).

SNMP ID:

2.37.1.29.2

Console path:**Setup > WLAN-Management > AP-Configuration > Link-Aggregation-Profiles****Possible values:****No**

Disabled

Yes

Enabled

Default:

No

System-Priority

The system priority of this LAG (Link Aggregation Group).

SNMP ID:

2.37.1.29.3

Console path:**Setup > WLAN-Management > AP-Configuration > Link-Aggregation-Profiles****Possible values:**

Max. 5 characters from [0-9]

Default:

32768

Frame-Distribution-Policy

Frame distribution policy of this LAG (Link Aggregation Group).

SNMP ID:

2.37.1.29.4

Console path:**Setup > WLAN-Management > AP-Configuration > Link-Aggregation-Profiles****Possible values:****Flow-Hash**

For outgoing packets, a flow hash is formed over the IP addresses and TCP/UDP ports contained and the packets are distributed to the individual links of the LAG on the basis of this. This achieves a distribution at session level, so that sessions of a single client can also be distributed to multiple links. This setting is recommended for most scenarios.

Source-Dest-MAC

Outgoing packets are distributed to the individual links of the LAG based on the contained pair of source MAC address and destination MAC address.

Default:

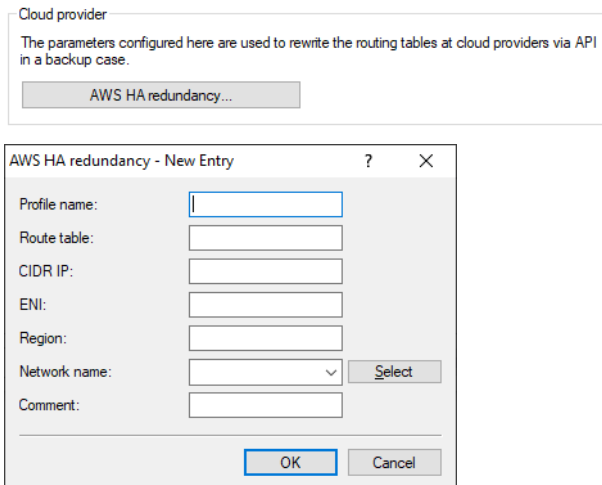
Flow-Hash

9 Backup solutions

9.1 Support for vRouter redundancy in Amazon AWS

As of LCOS 10.80, you can also set up vRouter redundancy support in Amazon AWS through LANconfig.

Configure vRouter redundancy for AWS in LANconfig under **Miscellaneous Services > Services > Cloud provider > AWS HA redundancy**.



Profile name

Unique name of the profile. This name is used by the route-change command to reference the profile.

Route table

Name of the routing table to change in AWS, e.g. "rtb-099605ce6cb4ac319". This value can be taken from the AWS management interface.

CIDR IP

Prefix in the routing table for which the next hop is to be changed, e.g. "0.0.0.0/0".

ENI

Name of the AWS network adapter (Elastic Network Interface) that the command is to set as the next hop, e.g. "eni-00c734d6da1fd8968". This value can be taken from the AWS management interface.

Region

Region where the AWS route table is located, e.g. "eu-central-1"

Network name

Name of the interface or remote site used by the vRouter to reach the AWS API, e.g. "INTERNET".

Comment

Enter a descriptive comment for this entry.

10 Other services

10.1 DHCPv4 client options

As of LCOS 10.80 certain options can be configured for the DHCPv4 client, which are then transmitted. This is required if the Internet provider expects certain data in DHCP messages. The options is found in the DHCP Options table under **IPv4 > DHCPv4 > DHCP client > DHCP options** and can be freely configured.

Interface

Interface that the DHCPv4 client should use for this option, e.g. WAN remote site or IPv4 LAN network.

Option number

Specifies the assigned IANA number of the DHCP option as defined in the RFC.

Option type

Specifies the type of the DHCP option. Possible values: String, Integer8, Integer16, Integer32, or IP address

Option value

Specifies the content of the DHCP option

A comma and/or space-separated list can also be specified, except in the case of a string. C-coding applies to integer values, i.e. for numbers 0x gives a hex value and, if the number starts with 0, it is an octal value. With the Integer8 type, it is additionally possible to specify a single hex string (of even length) without a separator. Values from the default options can be overwritten. The following options cannot be overridden or configured: padding (0), overload (52), message-type (53), server-id (54), request-list (55), message-size (57), and end (255).

Request list

Specifies whether the DHCP request should request the option number. The behavior is defined via the respective RFC of the DHCP option. Possible values: Yes, No

10.1.1 Additions to the Setup menu

Client

Here you will find all settings for the DHCP client for IPv4.

SNMP ID:

2.10.40

Console path:**Setup > DHCP****Additional options**

In this table certain options can be configured for the DHCPv4 client.

SNMP ID:

2.10.40.5

Console path:**Setup > DHCP > Client****Interface**

Interface that the DHCPv4 client should use for this option, e.g. WAN remote site or IPv4 LAN network.

SNMP ID:

2.10.40.5.1

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

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

Default:*empty***Option-Number**

Specifies the assigned IANA number of the DHCP option as defined in the RFC.

SNMP ID:

2.10.40.5.2

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

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

Default:*empty***Option-Type**

Specifies the type of the DHCP option.

SNMP ID:

2.10.40.5.3

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

String
Integer8
Integer16
Integer32
IP address

Option-Value

Specifies the content of the DHCP option

A comma and/or space-separated list can also be specified, except in the case of a string. C-coding applies to integer values, i.e. for numbers 0x gives a hex value and, if the number starts with 0, it is an octal value. With the Integer8 type, it is additionally possible to specify a single hex string (of even length) without a separator. Values from the default options can be overwritten. The following options cannot be overridden or configured: padding (0), overload (52), message-type (53), server-id (54), request-list (55), message-size (57), and end (255).

SNMP ID:

2.10.40.5.4

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

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

Default:*empty***Request-List**

Specifies whether the DHCP request should request the option number. The behavior is defined via the respective RFC of the DHCP option.

SNMP ID:

2.10.40.5.5

Console path:

Setup > DHCP > Client > Additional-Options

Possible values:

- No
- Yes

10.2 Accounting

As of LCOS 10.80, accounting has been expanded. Along with support for IPv6, a new function has been added to display the current data throughput of individual stations or logical interfaces on the network. This function is particularly suitable for analyzing which station on the network is currently causing which data traffic. For example, this allows stations that are using the Internet connection to be identified, or to see how much traffic is running via which interface at the current time.

For performance reasons, it is recommended to only activate this function while the analysis is running and to deactivate it again afterwards. For more extensive traffic monitoring, Netflow is recommended in conjunction with an external collector.

To use the analysis function, use the command line and set the "Operating" item under /setup/accounting to "Yes". Set the "Intermittent-Reporting-Interval" to a small value in seconds, e.g. 5 seconds.

To deactivate the function again after the analysis, set the "Active" switch to "No".

To display the current throughput per user, use the command "show accounting users"

```
show accounting users
```

Username	Interface	Rx-Total	Tx-Total	Rx-IPv4	Tx-IPv4	Rx-IPv6	Tx-IPv6
192.168.1.7	INTERNET	0 Bit/s	115 Bit/s	0 Bit/s	115 Bit/s	0 Bit/s	0 Bit/s
192.168.1.9	INTERNET	9.38 KBit/s	3.92 KBit/s	9.38 KBit/s	3.92 KBit/s	0 Bit/s	0 Bit/s

Next update of accounting bandwidth data in: 3s

As an alternative to the show command, the status table /Status/Accounting/User-Bandwidth-Usage can also be accessed.

The show command has a number of options that can be displayed by entering ?:

```
> show accounting ?
Displays short-term bandwidth usage statistics based on accounting.
NOTE: Accounting must be enabled and the Intermittent-Reporting-Interval must be set. All bandwidth data is updated according to that interval.
USAGE:
show accounting-bandwidth <COMMAND> [FLAGS]:

COMMANDS:
  interfaces:      Displays accounted bandwidth usage per interface
  users:           Displays accounted bandwidth usage per user per interface

FLAGS:
  -bps:           Displays all data as bps without decimals
  -kpbs:          Displays all data as kbps with 3 fixed decimal places
  -mbps:          Displays all data as mbps with 3 fixed decimal places
  -gbps:          Displays all data as gbps with 3 fixed decimal places
NOTE: You can only choose one of the unit display flags. If none is given, the correct output unit is automatically determined. All numbers are given with 3 significant digits.
  -compact:       Reduces output to bandwidth usage totals per traffic direction
  -totals-only:   (Only for command 'users') Does not show bandwidth usage per interface, but as a total value
```

Examples:

“show accounting interfaces” shows the load or current data throughput of the interfaces. This information can also be found in the /Status/Accounting/Interface-Bandwidth-Usage table

With the command “repeat 5 show accounting users” on the CLI you can have the command displayed automatically every 5 seconds.

10.2.1 Operating principles

Accounting users are identified by their user name. Potential accounting users are:

- > All stations on the LAN (user name is their IPv4 or IPv6 address, or if known to the router via DNS, the station's hostname)
- > All VPN peers (user name is the peer name)
- > All dialed-in RAS clients (user name is the RAS client ID; multiple dial-ins are mapped to the same ID)

The data traffic counted by accounting is any data traffic that takes place between a user and an IP address behind one of the following interface types (regardless of whether Rx or Tx traffic):

- > WAN
- > RAS
- > VPN

When connecting VPN to VPN, for example, the traffic is counted and booked separately for both VPN users.

The accounting records the data traffic with each remote site separately for each user. What this means is: Traffic, for example, from VPN to WAN1 and traffic from VPN to WAN2 are separate records.

From the user's point of view, the accounting records incoming and outgoing data as well as IPv4 and IPv6 traffic separately. This means that an IPv6 data packet from VPN1 to VPN2 is counted as IPv6-Tx for VPN1, and as IPv6-Rx for VPN2.

Also, the accounting records the number of data streams (sessions) that have occurred, but not separately according to Rx and Tx.

Bidirectional traffic is counted as 2 sessions because there are 2 streams. One incoming and one outgoing data stream from the user's point of view.

10.2.2 Switching accounting on or off on the fly

The check as to whether a data connection is reported by accounting takes place when the connection is established (first data packet). Data connections that already exist when accounting is switched on are not considered by accounting.

If accounting is switched off during operation, the data connections that are currently running are no longer included in the accounting data.

10.2.3 Data traffic counting

In the default setting, traffic is always reported to accounting when a data connection (in the form of a firewall session) ends, for example after a timeout within the firewall or when a TCP connection is closed. In the case of long-running connections, this can lead to a considerable delay before data traffic actually appears in the accounting status tables. To handle this problem, accounting has an “intermittent reporting” function, which enters partial recordings at fixed intervals in the accounting. How often this happens is configured via the intermittent reporting interval. By default this is set to 0; i.e. the feature is disabled. If a value between 1 and 30 is entered there, this setting defines the interval in seconds at which intermediate data-connection reports are received by accounting.

The intermediate reports increase the system load depending on the number of active data connections. The intermediate reports of the data connections are carried out independently of each other (i.e. not all at once) in order to avoid peak loads.

Intermittent reporting can be switched on at any time while accounting is running. The first intermittent report then contains the complete data traffic of the individual data flows measured up to the time when enabled.

10.2.4 Other changes to accounting

When configuring accounting, the parameter **Differentiation criterion** is deprecated.

Accounting

Accounting information can be used to determine which stations and users have established connections and transferred data.

Collect accounting information
Specify whether the device should regularly store an accounting snapshot.

Store accounting information in flash ROM

Deprecated menu items

The following menu items have been removed:

- > Sort-by (SNMP ID: 2.18.3)
- > Current-User (SNMP ID: 2.18.4)
 - > User-name (SNMP ID: 2.18.4.1)
 - > MAC-Address (SNMP ID: 2.18.4.2)
 - > Peer (SNMP ID: 2.18.4.3)
 - > Conn.-Type (SNMP ID: 2.18.4.4)
 - > Rx-KBytes (SNMP ID: 2.18.4.5)
 - > Tx-KBytes (SNMP ID: 2.18.4.6)
 - > Total-Time (SNMP ID: 2.18.4.8)
 - > Connections (SNMP ID: 2.18.4.9)
- > Accounting-List (SNMP ID: 2.18.5)
 - > User-name (SNMP ID: 2.18.5.1)
 - > MAC-Address (SNMP ID: 2.18.5.2)
 - > Peer (SNMP ID: 2.18.5.3)
 - > Conn.-Type (SNMP ID: 2.18.5.4)
 - > Rx-KBytes (SNMP ID: 2.18.5.5)
 - > Tx-KBytes (SNMP ID: 2.18.5.6)
 - > Total-Time (SNMP ID: 2.18.5.8)
 - > Connections (SNMP ID: 2.18.5.9)
- > Delete-Accounting-List (SNMP ID: 2.18.6)
- > Create-Snapshot (SNMP ID: 2.18.7)
- > Last-Snapshot (SNMP ID: 2.18.9)
 - > Username(SNMP ID: 2.18.9.1)
 - > MAC-Address (SNMP ID: 2.18.9.2)
 - > Peer (SNMP ID: 2.18.9.3)
 - > Conn.-Type (SNMP ID: 2.18.9.4)
 - > Rx-KBytes (SNMP ID: 2.18.9.5)
 - > Tx-KBytes (SNMP ID: 2.18.9.6)
 - > Total-Time (SNMP ID: 2.18.9.8)
 - > Connections (SNMP ID: 2.18.9.9)
- > Discriminator (SNMP ID: 2.18.10)

10.2.5 Additions to the Setup menu

Intermittent-Reporting-Interval

Defines the interval in seconds for the information in the show command "show accounting" or the corresponding status tables to be updated.

SNMP ID:

2.18.16

Console path:

Setup > Accounting

Possible values:

0 ... 30 Seconds

Special values:

0

Switched off

Status-Table-Entry-Limit

Specifies the maximum number of entries saved by the accounting.

SNMP ID:

2.18.17

Console path:

Setup > Accounting

Possible values:

0 ... 999,999 Entries

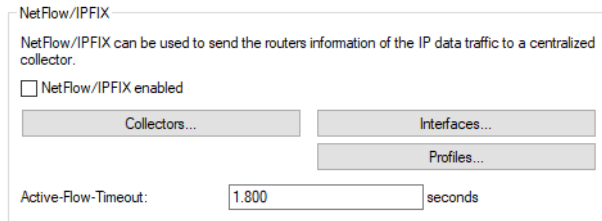
Special values:

0

Unlimited

10.3 New Netflow parameter “Active-Flow-Timeout”

As of LCOS 10.80 you can set the new parameter under **Logging/Monitoring > Protocols** in the section **NetFlow/IPFIX** with **Active-Flow-Timeout**.



Active-Flow-Timeout

Defines the interval in seconds after a running data stream is exported via Netflow. This makes it possible to run longer sessions, e.g. to export large downloads at runtime. Subsequent traffic is classified as a new data flow, and the logging of the data traffic by the collector starts again.

Possible values: 60–1800 seconds (0 turns the function off)

10.3.1 Additions to the Setup menu

Active-Flow-Timeout

Defines the interval in seconds after a running data stream is exported via Netflow. This makes it possible to run longer sessions, e.g. to export large downloads at runtime. Subsequent traffic is classified as a new data flow, and the logging of the data traffic by the collector starts again.

SNMP ID:

2.109.5

Console path:

Setup > NetFlow

Possible values:

60 ... 1800 Seconds

Special values:

0

Switched off

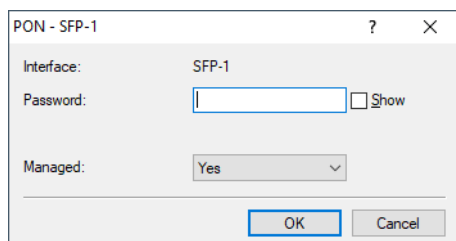
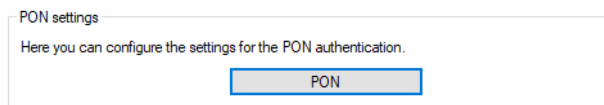
Default:

1800

10.4 PON password in hexadecimal format

As of LCOS 10.80 you can now enter the PON password as 20 hexadecimal characters in addition to the previous representation with 10 ASCII characters.

The setting for the PON password can be found as before in LANconfig under **Interfaces > WAN > PON** or in the console under **Setup > Interfaces > PON > Password**.



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 either 10 octets in ASCII representation or 20 characters in hexadecimal representation. The password is empty by default.

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

10.4.1 Additions to the Setup menu

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 either 10 octets in ASCII representation or 20 characters in hexadecimal representation. 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:

Either 10 ASCII or 20 hexadecimal characters from

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

Default:

empty

10.5 ACME-Client

As of LCOS 10.80 the Automatic Certificate Management Environment (ACME) client as per [RFC 8555](#) is supported for Let's Encrypt certificates. [Let's Encrypt](#) is a free and open certification authority that makes it possible to obtain free SSL/TLS certificates. The certificates can be used for WEBconfig and for the Public Spot.

The prerequisite for using Let's Encrypt is that the device has a publicly resolvable domain name, e.g. DynDNS. For the certificates to be used correctly, the device's WEBconfig must be accessed via its domain name and not the IP address. If WEBconfig is called via the IP address, the certificate check fails because Let's Encrypt certificates are issued for domain names and not IP addresses.


With Let's Encrypt, certificates are issued when a device can prove that it has control of the domain name. For this purpose, Let's Encrypt provides a so-called "challenge" that the device must satisfy. The ACME client in the device performs this process automatically. The ACME client also renews the certificate automatically before a specified certificate expiry period.


A domain name must first be entered into the configuration. The device then automatically submits a certificate request to Let's Encrypt and temporarily opens (for example) the port 443 or 80. Let's Encrypt then checks whether the device and the previously set challenge (e.g. token) can be reached under the specified domain name and port 443 or 80. If this is successful, the certificate is issued. The device renews the certificate automatically before it expires. For this process, the device briefly opens port 80 or 443 for this challenge and closes it again in the second step.

Use of Let's Encrypt is not possible or fails in the following scenarios:

- > The device does not have a public IP address
- > An upstream firewall blocks access to port 443 or 80 from the Internet

In principle, multiple domain names are also supported in the SAN field (Subject Alternative Name) of the certificate.

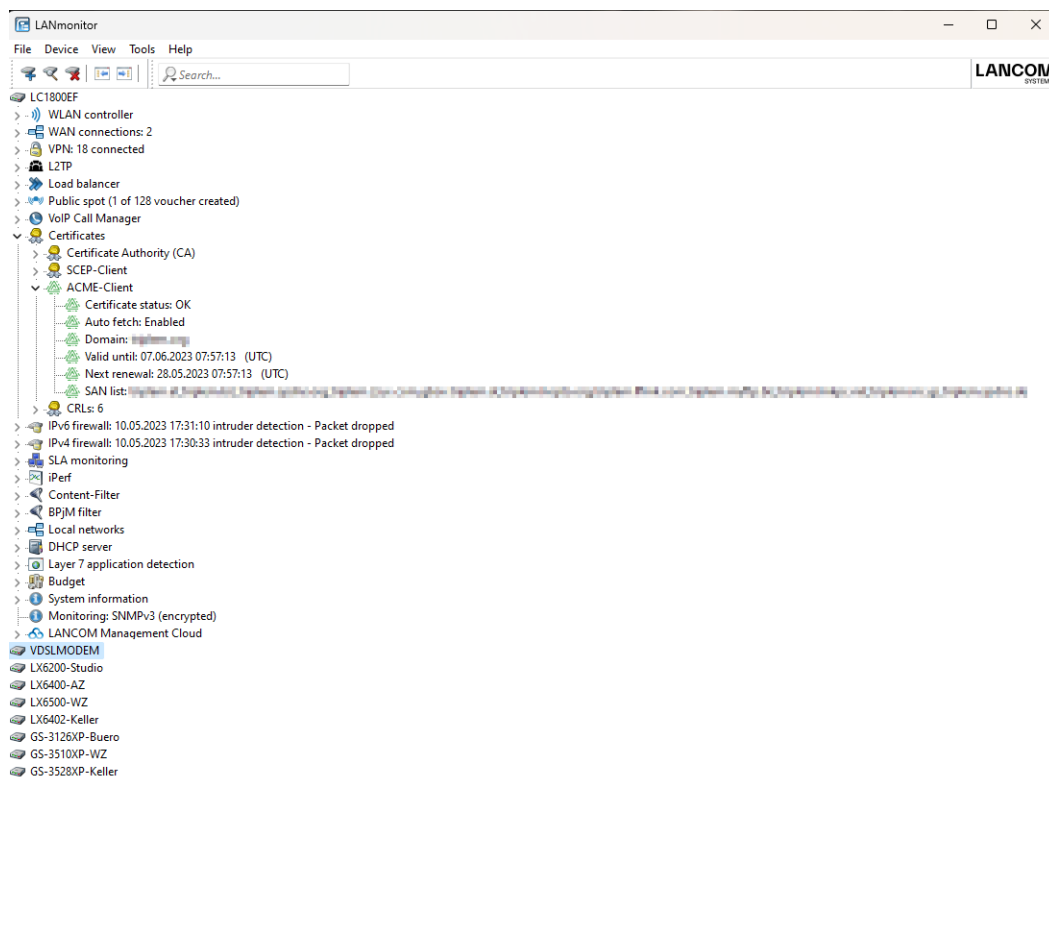
 By default, port 443 and the method `tls-alpn-01` is used for the ACME challenge. If the method `http-01` is to be used on port 80, the LANconfig configuration parameter **General > Admin > Access settings > HTTP access from a WAN interface** must be set to "Automatic".

 Please note that it is not possible to use the ACME client with the `tls-alpn-01` authorization challenge and simultaneous port forwarding with port 443. The same applies if the ACME client is to be used via the `http-01` method for port 80.

Manual adjustment of the ACME client to any port is not possible according to [RFC 8737](#) in the protocol.



You can see information about the ACME client in LANmonitor and start or stop a trace with the command line `trace # acme`.



10.5.1 ACME client configuration

In LANconfig, configure the Automatic Certificate Management Environment (ACME) client under **Certificates > ACME client**.

ACME client/Let's Encrypt client

With the ACME (Automatic Certificate Management Environment) client it is possible to automate receiving and renewing Let's Encrypt certificates.

ACME client enabled

Domain:

Contact (e-mail address):

Certificate type: RSA-2K

Authorization challenge: tls-alpn-01,http-01

Endpoint resolution: IPv6 or IPv4

SAN list:

Minimum validity: 30 days

Source address (optional):

ACME client enabled

Activates or deactivates the automatic fetching and renewal of the certificate.

Domain

DNS domain name for which the certificate is to be created, e.g. "test.example.com"

Contact (e-mail address)

Defines the contact information for the certificate request, e.g. the e-mail address "test@example.com".

Certificate type

Defines the certificate type including key length.

Possible values: RSA-2K, RSA-3K, RSA-4K, ECC-256, ECC-384

Authorization challenge

Specifies the method used to perform the Let's Encrypt authorization challenge. Possible values:

- > TLS-alpn-01: Authorization is performed over TLS and port 443
- > http-01: Authorization is performed over HTTP and port 80
- > http-01,tls-alpn-01: http-01 is preferred over tls-alpn-01
- > tls-alpn-01,http-01: tls-alpn-01 is preferred over http-01

Endpoint resolution

Defines the protocol to be used to resolve the endpoint. Possible values:

- > IPv4-only
- > IPv6-only
- > IPv6-or-IPv4

SAN-List

Defines which other domain names should be entered into the SAN field (Subject Alternative Name) of the certificate. This can be a comma-separated list of domain names (without spaces).

Minimum validity

Minimum number of days before expiry for the certificate to be renewed. Default: 30 days

Source address (optional)

References a named loopback address that is used as the sender. If the field is left empty, the router automatically selects an address.

10.5.2 Additions to the Setup menu

ACME-Client

This table contains the settings for the ACME client. The Automatic Certificate Management Environment (ACME) client as per [RFC 8555](#) is supported for Let's Encrypt certificates. *Let's Encrypt* is a free and open certification authority that makes it possible to obtain free SSL/TLS certificates. The certificates can be used for WEBconfig and for the Public Spot.

SNMP ID:

2.39.8

Console path:

Setup > Certificates

Endpoint

Endpoint or URL to which the certificate request is addressed.

SNMP ID:

2.39.8.1

Console path:

Setup > Certificates > ACME-Client

Possible values:

Max. 100 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+,-./:;<=>?[\]^_`~``

Default:

`https://acme-v02.api.letsencrypt.org/directory`

Domain

DNS domain name for which the certificate is to be created, e.g. "test.example.com"

SNMP ID:

2.39.8.2

Console path:

Setup > Certificates > ACME-Client

Possible values:

Max. 100 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+,-./:;<=>?[\]^_`~``

Default:

empty

SAN-List

Defines which other domain names should be entered into the SAN field (Subject Alternative Name) of the certificate. This can be a comma-separated list of domain names (without spaces).

SNMP ID:

2.39.8.3

Console path:

Setup > Certificates > ACME-Client

Possible values:

Max. 200 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+,-./:;<=>?[\]^_`~``

Default:

empty

Contact

Defines the contact information for the certificate request, e.g. the e-mail address "test@example.com".

SNMP ID:

2.39.8.4

Console path:

Setup > Certificates > ACME-Client

Possible values:

Max. 200 characters from `[A-Z][a-z][0-9]#@{ }~!$%&'()*+,-./:;<=>?[\]^_`~``

Default:

empty

Endpoint-Resolution

Defines the protocol to be used to resolve the endpoint.

SNMP ID:

2.39.8.5

Console path:

Setup > Certificates > ACME-Client

Possible values:

IPv4-Only

IPv6-Only

IPv6-Or-IPv4

Certificate-Type

Defines the certificate type including key length.

SNMP ID:

2.39.8.6

Console path:

Setup > Certificates > ACME-Client

Possible values:

RSA-2K
RSA-3K
RSA-4K
ECC-256
ECC-384

Default:

RSA-2K

Destination-PKCS12-File

Internal destination where the received certificate is saved.

SNMP ID:

2.39.8.7

Console path:

Setup > Certificates > ACME-Client

Possible values:

ssl_pkcs12_int
Certificate store for WEBconfig certificates.

Default:

ssl_pkcs12_int

Authorization-Challenges

Specifies the method used to perform the Let's Encrypt authorization challenge.

SNMP ID:

2.39.8.8

Console path:

Setup > Certificates > ACME-Client

Possible values:

http-01
Authorization is performed over HTTP and port 80.
tls-alpn-01
Authorization is performed over TLS and port 443.

http-01,tls-alpn-01

http-01 is preferred over tls-alpn-01.

tls-alpn-01,http-01

tls-alpn-01 is preferred over http-01.

Default:

tls-alpn-01,http-01

SSL

In this menu, you configure the settings for a SSL/TLS secured connection to the Let's Encrypt server.

SNMP ID:

2.39.8.10

Console path:

Setup > Certificates > ACME-Client

Versions

Here, select the encryption protocols for the TLS connection.

SNMP ID:

2.39.8.10.1

Console path:

Setup > Certificates > ACME-Client > SSL

Possible values:

SSLv3
TLSv1
TLSv1.1
TLSv1.2
TLSv1.3

Default:

TLSv1.2

TLSv1.3

Keyex-Algorithms

Here, select the encryption method for the SSL/TLS connection.

SNMP ID:

2.39.8.10.2

Console path:

Setup > Certificates > ACME-Client > SSL

Possible values:

RSA
DHE
ECDHE

Default:

RSA
DHE
ECDHE

Crypto-Algorithms

Here, select the crypto algorithms for the SSL/TLS connection.

SNMP ID:

2.39.8.10.3

Console path:

Setup > Certificates > ACME-Client > SSL

Possible values:

RC4-40
RC4-56
RC4-128
DES40
DES
3DES
AES-128
AES-256
AESGCM-128
AESGCM-256
Chacha20-Poly1305

Default:

3DES
AES-128
AES-256

AESGCM-128

AESGCM-256

Chacha20-Poly1305

Hash-Algorithms

Here, select the hash algorithms for the SSL/TLS connection.

SNMP ID:

2.39.8.10.4

Console path:

Setup > Certificates > ACME-Client > SSL

Possible values:

MD5
SHA1
SHA-2-256
SHA2-384

Default:

SHA-2-256

SHA2-384

Prefer-PFS

Specify whether PFS (perfect forward secrecy) is enabled for the SSL/TLS secured connection.

SNMP ID:

2.39.8.10.5

Console path:

Setup > Certificates > ACME-Client > SSL

Possible values:

Yes
No

Default:

Yes

Renegotiations

With this setting you control whether the client can trigger a renegotiation of SSL/TLS.

SNMP ID:

2.39.8.10.6

Console path:

Setup > Certificates > ACME-Client > SSL

Possible values:

Forbidden

The device disconnects from the remote station if this requests a renegotiation.

Allowed

The device permits renegotiations with the remote station.

Ignored

The device ignores the request to renegotiate sent by the remote station.

Default:

Ignored

Elliptic-Curves

Here you specify which elliptic curves are to be used for encryption.

SNMP ID:

2.39.8.10.7

Console path:

Setup > Certificates > ACME-Client > SSL

Possible values:

secp256r1

secp256r1 is used for encryption.

secp384r1

secp384r1 is used for encryption.

secp521r1

secp521r1 is used for encryption.

x25519

x25519 is used for encryption.

x448

x448 is used for encryption.

Default:

secp256r1

secp384r1

secp521r1

x25519

x448

Signature-Hash-Algorithms

Use this entry to specify which hash algorithm is used to encrypt the signature.

SNMP ID:

2.39.8.10.21

Console path:**Setup > Certificates > ACME-Client > SSL****Possible values:****MD5-RSA****SHA1-RSA****SHA224-RSA****SHA256-RSA****SHA384-RSA****SHA512-RSA****MD5-ECDSA****SHA1-ECDSA****SHA224-ECDSA****SHA256-ECDSA****SHA384-ECDSA****SHA512-ECDSA****Default:**

SHA256-RSA

SHA384-RSA

SHA512-RSA

SHA256-ECDSA

SHA384-ECDSA

SHA512-ECDSA

Min-DH-Length

This value refers to the Diffie-Hellman agreement used to derive the master secret for the SSL tunnel, more precisely to the length range of the keys used for this purpose. Sensible lengths are in the range 2048...8192.

SNMP ID:

2.39.8.10.22

Console path:

Setup > Certificates > ACME-Client > SSL

Possible values:

Max. 4 characters from `[0-9]`

Default:

2048

Max-DH-Length

This value refers to the Diffie-Hellman agreement used to derive the master secret for the SSL tunnel, more precisely to the length range of the keys used for this purpose. Sensible lengths are in the range 2048...8192.

SNMP ID:

2.39.8.10.23

Console path:

Setup > Certificates > ACME-Client > SSL

Possible values:

Max. 4 characters from `[0-9]`

Default:

8192

Endpoint-Loopback-Address

Enter the loopback address for the ACME router here.

SNMP ID:

2.39.8.11

Console path:

Setup > Certificates > ACME-Client

Possible values:

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

Default:*empty***Manually-Fetch-Certificate**

With this action you trigger a manual fetch of the certificate.

SNMP ID:

2.39.8.21

Console path:**Setup > Certificates > ACME-Client****Auto-Fetch-Certificate**

Settings for automatically fetching and renewing the certificate.

SNMP ID:

2.39.8.22

Console path:**Setup > Certificates > ACME-Client****Operating**

Activates or deactivates the automatic fetching and renewal of the certificate.

SNMP ID:

2.39.8.22.1

Console path:**Setup > Certificates > ACME-Client > Auto-Fetch-Certificate****Possible values:****Yes****No****Default:**

No

Minimum-Validity-Days

Minimum number of days before expiry for the certificate to be renewed.

SNMP ID:

2.39.8.22.2

Console path:**Setup > Certificates > ACME-Client > Auto-Fetch-Certificate****Possible values:**

Max. 5 characters from [0-9]

Default:

30

10.6 Execute actions on incoming SMS

As of LCOS 10.80 routers with a WWAN module can react to incoming SMS text messages with predefined actions. This allows you to respond to an incoming SMS (e.g. data budget used up) by sending your own SMS to the Internet provider, for example to book a new data budget.

In LANconfig you configure this under **Logging/Monitoring > SMS messages > SMS action table > Action table**.

Entry active

Activates or deactivates this table entry.

Sender

Sender address of the incoming SMS, which is the basis for the subsequent action. E.g. 7277 for Deutsche Telekom.

Check for

Content of the incoming SMS to be checked for. For example, `contains=' used up '` in the event of an exhausted data budget. The text that is checked for is case-sensitive!

Action

Defines the action to be executed after checking the specifications under **Sender** and **Check for**. For example, `exec:smssend -d 7277 -t "Speed"` to book a SpeedOn in the Deutsche Telekom network. With `exec` a command is executed on the command line, in this case the command `smssend`.

Lock time

Defines the lockout time in seconds, in which the action may not be executed again.

Syslog

Text field for defining the message to be written to the syslog when this action is executed.

Comment

Comment field.

10.6.1 Additions to the Setup menu

Action-Table

Use this table to react to incoming SMS text messages with predefined actions. This allows you to respond to an incoming SMS (e.g. data budget used up) by sending your own SMS to the Internet provider, for example to book a new data budget.

SNMP ID:

2.83.11

Console path:

Setup > SMS

Idx.

Index for this entry in the list.

SNMP ID:

2.83.11.1

Console path:

Setup > SMS > Action-Table

Possible values:

Max. 6 characters from `0123456789`

Default:

empty

Operating

Activates or deactivates this table entry.

SNMP ID:

2.83.11.2

Console path:**Setup > SMS > Action-Table****Possible values:****No**

Disables the table entry.

Yes

Enables the table entry.

Default:

Yes

Sender

Sender address of the incoming SMS text message, which is the basis for the subsequent action. For example, 7277 for Deutsche Telekom.

SNMP ID:

2.83.11.4

Console path:**Setup > SMS > Action-Table****Possible values:**Max. 16 characters from `[A-Z][a-z][0-9]#@[|}~!$%&'()+-/,/:;<=>?[\]^_`~``**Default:***empty***Check-For**

Content of the incoming SMS text message to be checked for. For example, `contains=' used up'` in the event of an exhausted data budget. The text checks are case-sensitive!

SNMP ID:

2.83.11.5

Console path:**Setup > SMS > Action-Table****Possible values:**Max. 50 characters from `[A-Z][a-z][0-9]#@[|}~!$%&'()+-/,/:;<=>?[\]^_`~``

Default:*empty***Action**

Defines the action to be executed after checking the specifications under [2.83.11.4 Sender](#) on page 67 and [2.83.11.5 Check-For](#) on page 67. For example, `exec:smssend -d 7277 -t "Speed"` to book a SpeedOn in the Deutsche Telekom network. With `exec` a command is executed on the command line, in this case the command `smssend`.

SNMP ID:

2.83.11.6

Console path:**Setup > SMS > Action-Table****Possible values:**Max. 250 characters from `[A-Z][a-z][0-9]#@{|}~!"$%&'()*+,-./:;<=>?[\]^_`~``**Default:***empty***Lock-Time**

Defines the lockout time in seconds, in which the action may not be executed again.

SNMP ID:

2.83.11.7

Console path:**Setup > SMS > Action-Table****Possible values:**Max. 9 characters from `0123456789`**Default:**

300

Syslog

Text field for defining the message to be written to the syslog when this action is executed.

SNMP ID:

2.83.11.8

Console path:

Setup > SMS > Action-Table

Possible values:

Max. 50 characters from `[A-Z][a-z][0-9]#{|}~!$%&'()+-./:;<=>?[\]^_``

Default:

empty

Comment

Comment field.

SNMP ID:

2.83.11.10

Console path:

Setup > SMS > Action-Table

Possible values:

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

Default:

empty

11 Enhancements in the menu system

11.1 Additions to the Setup menu

11.1.1 Configuration-Upload-Check

Defines whether the device should process unknown OIDs in uploaded configurations. This switch is mainly used for validations and compatibility checks. By default, unknown OIDs are ignored and the configuration is accepted.

SNMP ID:

2.11.97

Console path:

Setup > Config

Possible values:

tolerant

Unknown OIDs are accepted.

strict

Unknown OIDs produce an error so that the configuration upload fails.

Default:

tolerant

11.1.2 Syslog

This menu contains entries that may trigger syslog messages.

SNMP ID:

2.23.41.14

Console path:

Setup > Interfaces > Mobile

Syslog-Signal-Hysteresis

Defines at how much dB difference in signal level fluctuations (previous value to current value) a syslog message should be generated.

SNMP ID:

2.23.41.14.1

Console path:**Setup > Interfaces > Mobile > Syslog****Possible values:**

Max. 4 characters from [0-9]

Default:

5

11.1.3 LCOSCap-WAN-Access

With this setting you control access to LCOSCAP from the WAN.

SNMP ID:

2.63.5

Console path:**Setup > Packet-Capture****Possible values:****No**

No access allowed. This is the default for new devices or when the device is reset to factory settings.

Yes

Access granted. This is the default for devices that were updated from an older version to version LCOS 10.80.

VPN-Only

Access only allowed via VPN connections.

Default:

No

11.1.4 RPCap-WAN-Access

With this setting you control access to RPCAP from the WAN.

SNMP ID:

2.63.14

Console path:**Setup > Packet-Capture**

11 Enhancements in the menu system

Possible values:**No**

No access allowed. This is the default for new devices or when the device is reset to factory settings.

Yes

Access granted. This is the default for devices that were updated from an older version to version LCOS 10.80.

VPN-Only

Access only allowed via VPN connections.

Default:

No

11.1.5 Operating

Enables or disables sending and receiving of SMS text messages on the device.

SNMP ID:

2.83.10

Console path:

Setup > SMS

Possible values:**No**

Sending and receiving SMS is disabled.

Yes

Sending and receiving SMS is enabled.

Default:

Yes