LCOS 10.94

Addendum

10/2025



Contents

1 Addendum to LCOS version 10.94	٠
2 Configuration	6
2.1 Support for aliases on the CLI	
2.1.1 Additions to the Setup menu	
2.2 Support for history in the console	
2.2.1 Additions to the Setup menu	
3 Security	
3.1 Two-Factor Authentication (2FA) for Device Access	(
3.1.1 Additions to the Setup menu	
4 Routing and WAN connections	17
4.1 eSIM	
4.1.1 Configuration	18
4.1.2 CLI Configuration	20
4.2 Additional IPv6 variable for the action table	2 ²
4.3 Configuring APN credentials in the WWAN profile table	e22
4.3.1 Additions to the Setup menu	22
4.4 WWAN Bridge Mode	24
4.4.1 Additions to the Setup menu	24
5 Virtual Private Networks - VPN	28
5.1 WireGuard	28
5.1.1 Licensing	28
5.1.2 Configuration	28
5.1.3 Configuration with LANconfig	29
5.1.4 Trace Commands	
5.1.5 Show commands	
5.1.6 Additions to the Setup menu	
6 Voice over IP – VoIP	40
6.1 Configuration of Lines: SIP Lines	40
6.1.1 Additions to the Setup menu	
6.2 Prioritized Phone Numbers	
6.2.1 Additions to the Setup menu	
7 RADIUS	
7.1 RADIUS CoA for 802.1X Authenticator Ethernet Ports	43
8 Other services	45
8.1 New DHCPv4 Client Configuration	45
8.1.1 Additions to the Setup menu	46
9 Enhancements in the menu system	49
9.1 Additions to the Setup menu	49
9.1.1 Parameter-Format	49

Contents

10 Discontinued Features	53
9.1.4 Elliptic curves	51
9.1.3 IPv4-WAN-Access	50
9.1.2 Key-Exchange-Algorithms	49

Copyright

Copyright

© 2025 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, LANCOM Service LANcare, LANCOM Active Radio Control, and AirLancer are registered trademarks. All other names or descriptions used may be trademarks or registered trademarks of their owners. This document contains statements relating to future products and their attributes. LANCOM Systems reserves the right to change these without notice. No liability for technical errors and/or omissions.

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

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

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

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

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

LANCOM Systems GmbH

A Rohde & Schwarz Company

Adenauerstr. 20/B2

52146 Wuerselen

Germany

www.lancom-systems.com

1 Addendum to LCOS version 10.94

This document describes the changes and enhancements in LCOS version 10.94 since the previous version.

2 Configuration

2 Configuration

2.1 Support for aliases on the CLI

As of LCOS 10.94, command aliases can be configured on the CLI. With these command aliases, CLI commands can be shortened or predefined on the console.

2.1.1 Additions to the Setup menu

2.1.1.1 Command-Aliases

Here you can configure command aliases on the CLI. With these command aliases, CLI commands on the console can be shortened or predefined. For example, setting parameters or displaying a (status) table.

To do this, define pairs of a new alias and the corresponding command to be executed. Examples:

In the following example, the user-defined alias "show wwan" should display the status of the cellular modem from the status tree using the command "Is /status/modem-mobile".

An alias is created to make the command Ping send two packets to the IP address 8.8.8.8:

SNMP ID:

2.11.98

Console path:

Setup > Config

2.1.1.1.1 Command

Define the new alias here as the command of this alias entry.

SNMP ID:

2.11.98.1

Console path:

Setup > **Config** > **Command-Aliases**

Possible values:

Max. 32 characters from [a-z][0-9]

2.1.1.1.2 **Definition**

Define here the command to be executed for this alias entry.

SNMP ID:

2.11.98.2

Console path:

Setup > Config > Command-Aliases

Possible values:

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

2.2 Support for history in the console

As of LCOS 10.94, entered CLI commands are persistently saved by default and are therefore available after a reboot. The entered commands can be displayed with the "history" command and recalled with the "up arrow" and "down arrow" keys on the keyboard. Persistent storage can be disabled via configuration.

Command		escription
history [options]	f	risplays a list of the last executed commands. With the command ! #, commands rom the list can be called directly by their number (#): For example, ! 3 executes the third command in the list.
		he history is saved persistently across reboots. See also <i>2.11.99 Persistent-History</i> n page 8.
	:	-c: Clears the stored history.
	:	-w: Writes the current history to a file.
	:	-a: Appends the commands from this session's history to the end of a file.
	;	<count>: Outputs only the number of commands specified in <count> on the command line.</count></count>

2.2.1 Additions to the Setup menu

2.2.1.1 Persistent-History

When persistent CLI history is enabled, entered CLI commands are persistently saved by default and are therefore available after a reboot. The entered commands can be displayed with the "history" command and recalled using the "up arrow" and "down arrow" keys on the keyboard. Persistent storage can be disabled here.

You can define the number of entries in the history list in 2.11.100 History-File-Size-Limit on page 8.

```
SNMP ID:
```

2.11.99

Console path:

Setup > Config

Possible values:

No

Persistent CLI history is disabled.

Yes

Persistent CLI history is enabled.

Default:

Yes

2.2.1.2 History-File-Size-Limit

Defines the number of entries in the history list.

See also 2.11.99 Persistent-History on page 8.

SNMP ID:

2.11.100

Console path:

Setup > Config

Possible values:

Max. 4 characters from [0-9]

Default:

100

3 Security

3.1 Two-Factor Authentication (2FA) for Device Access

Access to management protocols (e.g., WEBconfig, SSH, Telnet) can be secured using two-factor authentication (2FA) in addition to the regular password. The feature can be configured separately for additional administrators or for the default root user.

In certain cases, management protocols must be allowed over unsecure channels, such as the Internet. To provide additional protection and safeguard the device against brute-force attacks, two-factor authentication can be enabled granularly for different access paths.

Common authenticator apps for mobile devices, such as smartphones, are supported.

Note that in the event of loss of the authenticator, a complete device reset may be required in the worst case. It is therefore recommended not to require 2FA for all configuration access methods — for example, not for serial console access or local LAN access — so that in the event of loss or misconfiguration, the device can still be accessed through normal means without 2FA.

It is especially recommended to enable 2FA protection for access via the WAN interface, including the use of encrypted protocols such as HTTPS or SSH.

Using 2FA requires the device to have the correct time. Therefore, the time reference should always be configured via the NTP client on the router in LANconfig under **Date & Time** > **Synchronization**.

The basic configuration process for two-factor authentication is as follows:

- 1. Create an entry in the "Admin-OTPs" table, specifying the administrator account name to which this entry applies.
- 2. Open WEBconfig under Extras > Admin-OTPs. From there, the generated QR code for the user can be displayed, saved, or scanned by an external authenticator app.
- **3.** When the management connection for the admin user is initiated, the user will be prompted to enter the one-time password (OTP) after entering their regular password.

Generating QR Codes for Connection with the Authenticator

The QR codes used to connect the authenticator with the device are generated in WEBconfig under **Extras** > **Admin-OTPs** or alternatively via the CLI command "show Admin-OTP-QR".

Show Commands

- > Admin-OTP Displays the administrator OTP profiles
- > Admin-OTP-CODES Displays the administrator OTP profiles (codes only)
- Admin-OTP-QR Displays the administrator OTP profiles (QR code only)
- > Admin-OTP-URI Displays the administrator OTP profiles (URI only)

3.1.1 Additions to the Setup menu

3.1.1.1 Admin-OTPs

Access to management protocols (e.g., WEBconfig, SSH, Telnet) can be secured using two-factor authentication (2FA) in addition to the regular password. The feature can be configured separately for additional administrators or for the default root user.

3 Security

In certain cases, management protocols must be allowed over unsecure channels, such as the Internet. To provide additional protection and safeguard the device against brute-force attacks, two-factor authentication can be enabled granularly for different access paths.

Common authenticator apps for mobile devices, such as smartphones, are supported.

Note that in the event of loss of the authenticator, a complete device reset may be required in the worst case. It is therefore recommended not to require 2FA for all configuration access methods — for example, not for serial console access or local LAN access — so that in the event of loss or misconfiguration, the device can still be accessed through normal means without 2FA.

It is especially recommended to enable 2FA protection for access via the WAN interface, including the use of encrypted protocols such as HTTPS or SSH.

Using 2FA requires the device to have the correct time. Therefore, the time reference should always be configured via the NTP client on the router in LANconfig under **Date & Time** > **Synchronization**.

The basic configuration process for two-factor authentication is as follows:

- 1. Create an entry in the "Admin-OTPs" table, specifying the administrator account name to which this entry applies.
- 2. Open WEBconfig under Extras > Admin-OTPs. From there, the generated QR code for the user can be displayed, saved, or scanned by an external authenticator app.
- **3.** When the management connection for the admin user is initiated, the user will be prompted to enter the one-time password (OTP) after entering their regular password.

This table defines the OTP administrators.

SNMP ID:

2.11.101

Console path:

Setup > Config

3.1.1.1.1 Administrator

Username of the administrator for whom two-factor authentication is to be enabled, e.g., "root".

SNMP ID:

2.11.101.1

Console path:

Setup > Config > Admin-OTPs

Possible values:

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

3.1.1.1.2 Hash-Algorithm

Defines the hash algorithm to be used.



Make sure that the authenticator app supports the highest possible hash algorithm.

SNMP ID:

2.11.101.2

Console path:

Setup > **Config** > **Admin-OTPs**

Possible values:

SHA1 SHA256 SHA512

3.1.1.1.3 Time-Step

Defines the interval in seconds after which a new OTP is generated.

SNMP ID:

2.11.101.3

Console path:

Setup > Config > Admin-OTPs

Possible values:

Max. 10 characters from [0-9]

3.1.1.1.4 Network-Delay

Defines the maximum number of time steps by which the client's clock may differ. The device checks the OTP that is older or newer by this value.

SNMP ID:

2.11.101.4

Console path:

Setup > **Config** > **Admin-OTPs**

Possible values:

Max. 3 characters from [0-9]

3.1.1.1.5 Secret

Defines the actual shared secret that must be shared with the authenticator app. The secret must be unique for each user. There are currently three input options in the table:

Base32 (Default)

Prefix "base32:" followed by the Base32-encoded secret. The prefix may also be omitted.

3 Security

Hexadecimal

Prefix "hex:" followed by an even number of hex digits.

Plain text passphrase

Prefix "ascii:" followed by the characters.



For Google Authenticator, the secret must be 16 characters long (80 bits, Base32 encoded), e.g. E3U5IDWEE3KFCJ7G.

SNMP ID:

2.11.101.5

Console path:

Setup > Config > Admin-OTPs

Possible values:

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

3.1.1.1.6 Issuer

Freely definable text used in the authenticator to distinguish between multiple keys or for general display purposes when the same username is used. The value must not contain a colon.

SNMP ID:

2.11.101.6

Console path:

Setup > Config > Admin-OTPs

Possible values:

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

3.1.1.1.7 Num-Digits

Length of the OTPs.



For Google Authenticator, the value should be set to 6.

SNMP ID:

2.11.101.7

Console path:

Setup > **Config** > **Admin-OTPs**

Possible values:

Max. 3 characters from [0-9]

3.1.1.1.8 Request-on-Outband

Defines whether two-factor authentication is required for this user when logging in via the serial interface, or whether the device should request it.

SNMP ID:

2.11.101.11

Console path:

Setup > Config > Admin-OTPs

Possible values:

No

Yes

3.1.1.1.9 Request-on-Telnet

Defines whether two-factor authentication is required for this user when logging in via Telnet, or whether the device should request it. It can be configured granularly to specify which access paths require two-factor authentication, e.g., only via a WAN connection.

SNMP ID:

2.11.101.12

Console path:

Setup > Config > Admin-OTPs

Possible values:

never

LAN

WAN

WLAN

VPN-over-LAN

VPN-over-WAN VPN-over-WLAN

always

3.1.1.1.10 Request-on-TFTP

Defines whether two-factor authentication is required for this user when logging in via TFTP, or whether the device should request it. It can be configured granularly to specify which access paths require two-factor authentication, e.g., only via a WAN connection.

3 Security

SNMP ID:

2.11.101.13

Console path:

Setup > Config > Admin-OTPs

Possible values:

never

LAN

WAN

WLAN

VPN-over-LAN

VPN-over-WAN

VPN-over-WLAN

always

3.1.1.1.11 Request-on-HTTP

Defines whether two-factor authentication is required for this user when logging in via HTTP, or whether the device should request it. It can be configured granularly to specify which access paths require two-factor authentication, e.g., only via a WAN connection.

SNMP ID:

2.11.101.14

Console path:

Setup > Config > Admin-OTPs

Possible values:

never

LAN

WAN

WLAN

VPN-over-LAN

VPN-over-WAN

VPN-over-WLAN

always

3.1.1.1.12 Request-on-HTTPS

Defines whether two-factor authentication is required for this user when logging in via HTTPS, or whether the device should request it. It can be configured granularly to specify which access paths require two-factor authentication, e.g., only via a WAN connection.

SNMP ID:

2.11.101.16

Console path:

Setup > Config > Admin-OTPs

Possible values:

never LAN

WAN

WLAN

VPN-over-LAN

VPN-over-WAN

VPN-over-WLAN

always

3.1.1.1.13 Request-on-Telnet-SSL

Defines whether two-factor authentication is required for this user when logging in via Telnet-SSL, or whether the device should request it. It can be configured granularly to specify which access paths require two-factor authentication, e.g., only via a WAN connection.

SNMP ID:

2.11.101.17

Console path:

Setup > **Config** > **Admin-OTPs**

Possible values:

never

LAN

WAN

WLAN

VPN-over-LAN

VPN-over-WAN

VPN-over-WLAN

always

3.1.1.1.14 Request-on-SSH

Defines whether two-factor authentication is required for this user when logging in via SSH, or whether the device should request it. It can be configured granularly to specify which access paths require two-factor authentication, e.g., only via a WAN connection.

SNMP ID:

2.11.101.18

Console path:

Setup > Config > Admin-OTPs

3 Security

Possible values:

never

LAN

WAN

WLAN

VPN-over-LAN

VPN-over-WAN

VPN-over-WLAN

always

4 Routing and WAN connections

4.1 eSIM

To gain access to mobile networks, mobile network operators (MNOs) issue so-called SIM cards (Subscriber Identity Module Cards) to their customers. Each MNO issues its own SIM cards per customer. SIM cards consist of a plastic carrier and a security chip with security keys that grant access to the mobile network. If a customer wanted to change operators, the old SIM card had to be replaced with a new SIM card from the new MNO in the device. SIM cards are usually sent by the MNO via postal mail, which the customer receives a few days after signing the contract.

An eSIM is, simply put, the digital version of the classic SIM card. It consists of a chip (e.g., in the M2FF form factor) that is permanently installed in the mobile phone or router, and a solution for managing mobile profiles, referred to as eUICC (embedded Universal Integrated Circuit Card). eUICC functionality can be provided in different form factors. In the following, the terms eSIM and eUICC are used synonymously for simplicity.

Basically, three different types or solution architectures of eSIMs exist:

- M2M eSIM: Machine-to-Machine (M2M) eSIMs are designed for machines and device types without a user interface
 or user interaction on the device. M2M eSIMs are centrally managed by a management portal or provisioning system
 and can be transferred to the end device over-the-air (OTA) via SMS. Typically, these are closed systems provided by
 solution vendors for customers with many end devices. M2M eSIMs are specified according to the SGP.02 standard.
- 2. Consumer eSIMs: Consumer eSIMs are issued by MNOs and are used in mobile phones, smartwatches, or routers. Typically, the MNO supplies a QR code or activation code that the customer can use to install the eSIM or profile on the device. Closed or proprietary provisioning systems also exist from certain smartphone manufacturers, enabling the MNO to notify the customer that the eSIM is ready for download. Unlike the M2M eSIM, the end customer must initiate the installation of the eSIM. End devices have software called the Local Profile Assistant (LPA), which establishes encrypted communication between the embedded eSIM/mobile chip and the MNO's system. Downloading the eSIM profile always requires an existing internet connection, e.g., through the phone's integrated WLAN. Consumer eSIMs are defined in the SGP.22 standard.
- 3. IoT eSIM: IoT eSIMs are designed for a large number of IoT devices and combine part of the LPA functionality on the device with a server for managing the eSIMs. IoT eSIMs are defined in the SGP.32 standard and are the newest of the solution architectures.

LANCOM routers include an eSIM chip in the M2FF form factor with eUICC functionality. This is a consumer eSIM according to the SGP.22 standard. This solution is compatible with common eSIMs issued by MNOs for mobile phones. The eSIM can be used with all mobile profiles for consumer eSIMs according to the SGP.22 standard and is not technically restricted. In principle, eSIMs must be supported by the MNO and must not be limited to specific devices or device types.

As of LCOS 10.94, LANCOM routers support, in addition to classic plastic SIM cards, an eSIM solution in cellular routers. Several prerequisites are required:

- 1. At least LCOS 10.94 firmware
- 2. Cellular router with integrated on-board eSIM chip
- 3. Possibly an update of the WWAN firmware to the minimum version supporting eSIM functionality

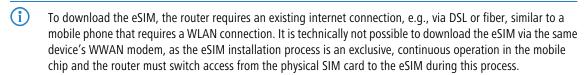
The general process of installing an eSIM on a LANCOM router is as follows:

- 1. Sign a mobile contract with an MNO.
- The MNO supplies a QR code or activation code (both contain the same information, just in different formats) for the eSIM.
- **3.** The activation code is entered via WEBconfig or the router's command line. The router then downloads the corresponding profile from the MNO's server via an existing internet connection (e.g., DSL or fiber) to the integrated

4 Routing and WAN connections

chip. The profile is stored permanently in the chip. The activation code contains both the server URL and a code for retrieving the eSIM.

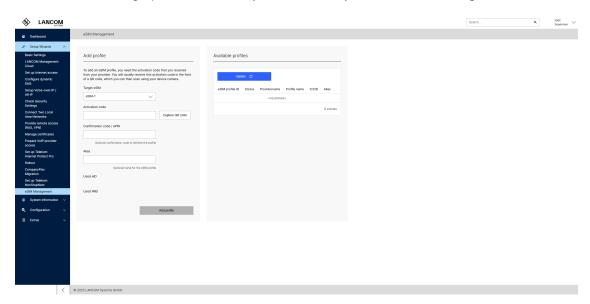
4. The successfully downloaded eSIM is configured in the router's WWAN profile table for use.



- **(i)** Further notes on usage:
 - > Up to eight eSIM profiles can be stored on the integrated eSIM
 - > eSIMs can be installed and managed via WEBconfig or CLI commands
 - > An optional GSMA test profile, if present on the eSIM, can be safely deleted and serves to simplify testing for MNOs, developers, or certification/test procedures
 - > The eSIM is implemented as a "virtual SIM slot" that can hold up to eight profiles
 - > Only the active eSIM profile is used when the eSIM is referenced as "eSIM-1" in the SIM slot configuration
 - > If the internal cellular modem is unavailable, the eSIM management cannot be accessed
 - > A device reset is not a secure method for deleting eSIM profiles, as it cannot be guaranteed that the modem has access to the eSIM at that moment
 - > To securely delete eSIMs, the profiles must be manually removed via eSIM management. If this is not possible, the corresponding eSIM profile can, as a last resort, be disabled by the MNO, as is already the case with physical SIM cards
 - > eSIMs can generally only be downloaded once and cannot be re-downloaded. eSIMs must explicitly be re-enabled by the MNO for download.
 - > Downloaded eSIMs are permanently tied to the embedded chip and cannot be transferred between different devices.

4.1.1 Configuration

In the device's WEBconfig, open the section **Add profile** under **Setup Wizards** > **eSIM Management**.



Target eSIM

Select the desired target eSIM, e.g., eSIM-1.

Activation code

Insert here the eSIM activation code provided by your mobile network operator (MNO), e.g., LPA:1\$prov.example.com\$ABCDEFGH12345.

This is the so-called LPA string ("Local Profile Assistant" string). It is a character string that contains the address of the SM-DP+ server (Server for Profile Management) and an activation code to manually install an eSIM profile on a device. It is identical to the content of the QR code. The string follows the format LPA:1\$SM-DP+address\$activation-code and is used by the LPA in the device to download and install the eSIM profile from the SM-DP+ server over an existing Internet connection.

The activation code can either be entered as text or scanned from a QR code if the device has a camera.

Confirmation code / ePIN

Optional confirmation code that is entered together with the activation code. Some MNOs refer to this as an ePIN. The code is provided by your mobile network operator along with the QR code/activation code.

Alias

The alias is an optional label for the eSIM profile. It allows easier identification of the profile in the profile table.

Used eID

Displays the eID (Embedded Identity Document). The eID is the globally unique identifier of the eSIM installed in the device. This information is for reference only.

Used IMEI

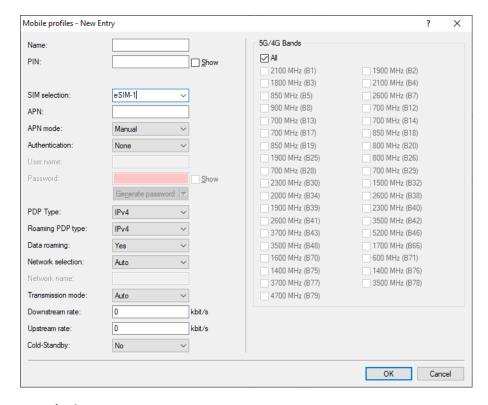
Displays the IMEI (International Mobile Equipment Identity). The IMEI is a 15-digit number assigned to your LANCOM cellular router that uniquely identifies it worldwide. This information is for reference only.

Section "Existing profiles"

This section displays the eSIM profiles stored on the local device. Only one eSIM profile can be active at a time. The active profile can be used in the configuration of the WWAN profiles in the SIM selection as "eSIM-1".

Assign WWAN profile in LANconfig

In LANconfig, open Interfaces > WAN > Mobile settings > Mobile profiles.



SIM selection

Defines the SIM slot or eSIM of the device to be used. Possible values (depending on the device):

- > SIM-1 (Default): first SIM slot in the device
- > SIM-2: second SIM slot in the device
- > eSIM-1: embedded eSIM in the device. The currently active profile configured in WEBconfig is used.
- > Iccid:<iccid of the SIM card or eSIM profile>: With this value, the SIM card or eSIM profile can be explicitly selected via the unique ICCID (Integrated Circuit Card Identifier). The ICCID of the installed eSIM profiles can be found in the eSIM management section of WEBconfig.

4.1.2 CLI Configuration

In addition to management via WEBconfig, eSIMs can also be managed via the command line. This allows eSIM profiles to be downloaded or deleted.

Under **Status** > **Modem-Mobile** > **eSIM** you will find the status table **eSIM Profiles**, which displays the currently installed eSIMs.

You will also find the actions Change-Alias, Delete-Profile, and Download-Profile here.

Change-Alias

This command allows you to change the alias or user-defined label of the eSIM.

Usage: do Change-Alias "<eSIM Profile ID>" "<New alias>"

Delete-Profile

This command allows you to delete an eSIM profile.

Usage: do Delete-Profile <eSIM Profile ID>

Download-Profile

This command allows you to download an eSIM profile.

Usage: do Download-Profile [Option]... "<eSIM activation code>"

- Options:
- > -a "<Alias>" Set alias for the profile after download
- > -c "<Confirmation code>" Provide confirmation code
- > -s "<Target SIM>" Set target SIM (Default: eSIM-1)

4.2 Additional IPv6 variable for the action table

As of LCOS 10.94, an additional variable for IPv6 can be used in the action table.

In LANconfig, you can find the action table under **Communication** > **General** > **Action table**.



Under **Action**, you can use this variable to extend the actions:

%w

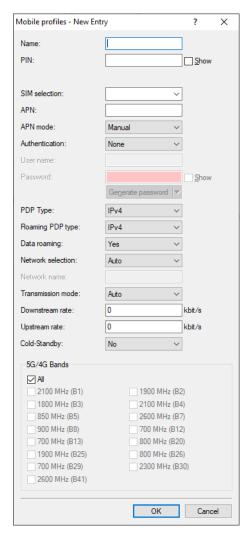
Variable for IPv6. With the variable %w, together with the network name, e.g., %{wINTRANET}, a static address with a fixed host identifier can be assigned to any station in the local network.

```
Example: %{wINTRANET}dd06:57b3:flee:201e together with the prefix 2003:c9:1703:5b51::/64 on the INTRANET network results in: 2003:c9:1703:5b51:dd06:57b3:flee:20ff
```

The prefix is formatted so that only the 64-bit host portion needs to be appended to form a complete 128-bit address. The prefix length "::64/" is truncated in the process.

4.3 Configuring APN credentials in the WWAN profile table

As of LCOS 10.94, you can define in the WWAN profile table under **Interfaces** > **WAN** > **Mobile profiles** whether authentication is required for logging in to the APN.



Authentication

Specify whether authentication is required for logging in to the APN. Possible values: None, PAP, CHAP.

User name

If authentication is required for logging in to the APN, enter the user name here.

Password

If authentication is required for logging in to the APN, enter the password here.

4.3.1 Additions to the Setup menu

4.3.1.1 Authentication

Specify whether authentication is required for logging in to the APN.

```
SNMP ID:
```

2.23.41.1.19

Console path:

Setup > Interfaces > Mobile > Profiles

Possible values:

None

PAP

CHAP

Default:

None

4.3.1.2 Username

If authentication is required for logging in to the APN, enter the user name here.

SNMP ID:

2.23.41.1.20

Console path:

```
Setup > Interfaces > Mobile > Profiles
```

Possible values:

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

Default:

empty

4.3.1.3 Password

If authentication is required for logging in to the APN, enter the password here.

SNMP ID:

2.23.41.1.21

Console path:

```
Setup > Interfaces > Mobile > Profiles
```

Possible values:

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

Default:

empty

4.4 WWAN Bridge Mode

The cellular modem integrated into the router can be used in two operating modes: Router mode and Bridge mode. In router mode, the router establishes the mobile connection itself and receives an IP address on its WWAN connection (e.g., IPv4 address and/or IPv6 address/prefix), allowing a downstream network to access the Internet via Network Address Translation (NAT). The IP address assigned by the provider is shared with multiple LAN clients in this case.

In bridge mode, the router acts as a simple network bridge and forwards all IP packets from the mobile network to exactly one downstream device. This device therefore receives the IP address assigned by the provider directly and must establish the WAN connection (via DHCP) to the provider and handle NAT and routing for the internal network.

Bridge mode is useful when the device is intended to operate purely as a modem, for example, to avoid double NAT in a router cascade. The WWAN bridge mode is conceptually comparable to the bridge mode of DSL modems.

The device providing bridge mode itself does not have an IP address on the WWAN interface and therefore cannot establish a direct connection to the mobile network, as data packets are transparently forwarded. If the device is to be managed via the LMC, for example, Internet access must be established through an alternative route.

Only the first client that connects to the device in bridge mode receives the IP address assigned by the mobile network. Packets from the cellular modem are passed on without VLAN tagging.

It is recommended to configure ICMP polling on the WAN connection of the downstream device, as it is not possible by design for the modem to notify the downstream device of a connection loss or address change. ICMP polling allows the downstream device to detect an interruption in the mobile connection.

Configuration of the WWAN bridge mode is generally performed in the following steps:

- **1.** The operating mode of the WWAN modem is set to "Bridge", and an appropriate WWAN profile for the cellular parameters must also be specified.
- 2. The "WWAN" interface is configured together with a LAN interface (e.g., LAN-2) in a common bridge group. The corresponding LAN interface is assigned to an ETH port.

4.4.1 Additions to the Setup menu

4.4.1.1 WWAN

Settings for WWAN.

SNMP ID:

2.46

Console path:

Setup

4.4.1.1.1 WAN-Bridge

The cellular modem integrated into the router can be used in two operating modes: Router mode and Bridge mode. In router mode, the router establishes the mobile connection itself and receives an IP address on its WWAN connection (e.g., IPv4 address and/or IPv6 address/prefix), allowing a downstream network to access the Internet via Network Address Translation (NAT). The IP address assigned by the provider is shared with multiple LAN clients in this case.

In bridge mode, the router acts as a simple network bridge and forwards all IP packets from the mobile network to exactly one downstream device. This device therefore receives the IP address assigned by the provider directly and must establish the WAN connection (via DHCP) to the provider and handle NAT and routing for the internal network.

Bridge mode is useful when the device is intended to operate purely as a modem, for example, to avoid double NAT in a router cascade. The WWAN bridge mode is conceptually comparable to the bridge mode of DSL modems.

The device providing bridge mode itself does not have an IP address on the WWAN interface and therefore cannot establish a direct connection to the mobile network, as data packets are transparently forwarded. If the device is to be managed via the LMC, for example, Internet access must be established through an alternative route.

Only the first client that connects to the device in bridge mode receives the IP address assigned by the mobile network. Packets from the cellular modem are passed on without VLAN tagging.

It is recommended to configure ICMP polling on the WAN connection of the downstream device, as it is not possible by design for the modem to notify the downstream device of a connection loss or address change. ICMP polling allows the downstream device to detect an interruption in the mobile connection.

Configuration of the WWAN bridge mode is generally performed in the following steps:

- **1.** The operating mode of the WWAN modem is set to "Bridge", and an appropriate WWAN profile for the cellular parameters must also be specified.
- 2. The "WWAN" interface is configured together with a LAN interface (e.g., LAN-2) in a common bridge group. The corresponding LAN interface is assigned to an ETH port.

SNMP ID:

2.46.2

Console path:

Setup > WWAN

Interface

Specifies the name of the internal cellular modem, e.g., WWAN, that should be used.

SNMP ID:

2.46.2.1

Console path:

Setup > WWAN > WAN-Bridge

Mode

Defines the operating mode of the internal cellular interface in the device.

SNMP ID:

2.46.2.2

Console path:

Setup > WWAN > WAN-Bridge

4 Routing and WAN connections

Possible values:

Router

In router mode, the router establishes the mobile connection itself and receives an IP address on its WWAN interface, allowing a downstream network to access the Internet via Network Address Translation (NAT).

Bridge

In bridge mode, the router acts as a simple network bridge and forwards all IP packets from the mobile network to exactly one downstream device. The detailed bridge configuration is performed in the LAN bridge.

Default:

Router

LAN-Peer-MAC

MAC address of the device or client in the LAN that should receive the IP address directly from the mobile network. If the MAC address is 0, the MAC address learned from received packets is used automatically.

SNMP ID:

2.46.2.3

Console path:

```
Setup > WWAN > WAN-Bridge
```

Possible values:

Max. 12 characters from [a-f][0-9]

Default:

00000000000

Bridge-MAC

MAC address to be used as the sender address. If the MAC address is 0, a "locally administered" address derived automatically from the device's MAC address is used.

SNMP ID:

2.46.2.4

Console path:

Setup > WWAN > WAN-Bridge

Possible values:

Max. 12 characters from [a-f][0-9]

Default:

00000000000

Profile

Defines the WWAN profile to be used.

SNMP ID:

2.46.2.5

Console path:

Setup > WWAN > WAN-Bridge

Possible values:

Max. 12 characters from $[A-Z][0-9]@{|} \sim ! \% \&'() +-, /:; <=>?[\]^_.$

5 Virtual Private Networks - VPN

5.1 WireGuard

WireGuard is a simple and lightweight VPN protocol. Unlike IKEv2/IPSec, WireGuard focuses on simplicity, speed, and ease of use. It is also a protocol with a very compact code base and functionality, making it ideal for use on IoT and embedded devices.

IKEv2 is an IETF-standardized protocol offering many extensions and high flexibility, but also significant complexity. While IKEv2, for example, supports crypto agility—meaning encryption algorithms can be exchanged or negotiated between endpoints—WireGuard uses a fixed key exchange (Curve25519) and a fixed encryption protocol (ChaCha20/Poly1305). In WireGuard, authentication is only possible via public/private keys, whereas IKEv2 allows flexible authentication methods such as PSK, certificates, or EAP. IKEv2 also supports many extensions, such as RADIUS or two-factor authentication, which are not available in WireGuard. Furthermore, WireGuard only supports transmission over UDP but includes built-in roaming functionality similar to MOBIKE in IKEv2.

IKEv2/IPSec continues to be the recommended standard protocol for branch connectivity and SD-WAN due to its wide range of configuration and deployment scenarios in LCOS. WireGuard on LANCOM router platforms does not provide hardware acceleration for ChaChaPoly1305, meaning encryption is handled in software. For scenarios requiring high VPN throughput, IKEv2/IPSec remains the preferred option.

Within LCOS, IKEv2/IPSec is based on many years of practical use in VPN site connectivity and numerous protocol and feature extensions for medium, large, and complex VPN or SD-WAN scenarios. WireGuard in LCOS is therefore an ideal addition for simpler use cases where only basic encrypted connections are needed. Another scenario for WireGuard use is when the VPN protocol is specified by a service provider or VPN vendor.

Conceptually, WireGuard is a "silent" protocol—no control or negotiation packets are exchanged until user data needs to be transmitted. In contrast, IKE tunnels can be configured to initiate immediately. For this reason, there is no hold time or related configuration for WireGuard in LCOS. WireGuard supports both IPv4 and IPv6, as transport protocols and for data transmission within the tunnel.

For IPv6, the inbound UDP ports used for the tunnel must be configured manually in the IPv6 firewall inbound table, since the ports in WireGuard are freely configurable.

WireGuard tunnels in LCOS can be defined as either "Unnumbered"—i.e., without a configured IP address—or with assigned IP addresses under **Communication** > **Protocols** > **IP parameters**.

5.1.1 Licensing

In LCOS, WireGuard counts as a VPN tunnel and is included in the device's VPN license count, sharing the same license pool with other VPN tunnels such as IKE/IPSec or PPTP-MPPE. A WireGuard license is consumed as soon as data is transmitted through the WireGuard tunnel. Any number of WireGuard tunnels can be configured.

Additional WireGuard licenses can be added through the VPN option upgrade.

Example:

If a device is licensed for 5 VPN tunnels and 3 IPSec tunnels are already active, two additional WireGuard tunnels can still be used.

5.1.2 Configuration

A WireGuard configuration in LCOS consists of at least two configuration elements, as well as additional optional elements:

- 1. An entry in the WireGuard tunnel configuration table.
- 2. An entry in the IPv4 and/or IPv6 routing table. This entry corresponds to the concept of "Allowed IP Addresses" in WireGuard on other platforms.
- **3.** (Optional) Configure local IP addresses for the WireGuard peer via the IP Parameters table in LANconfig under **Communication** > **Protocols** > **IP Parameters**.
- **4.** (Optional) Firewall configuration for granular control of network access rights.

5.1.3 Configuration with LANconfig

WireGuard is configured in LANconfig under **VPN** > **WireGuard**.

WireGuard operatingCookie challenge		
WireGuard connections Use this table to configure WireGuard	ard connections.	
	Connection list	

WireGuard operating

Enables or disables the WireGuard function on the device.

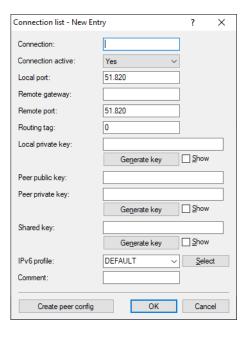
Cookie challenge

The cookie challenge is a protection mechanism against CPU exhaustion attacks during the handshake process. The computation of the Diffie-Hellman (DH) function during the WireGuard handshake is inherently CPU-intensive. An attacker could attempt to overload the router by sending a large number of handshake requests to crash it or severely impact its performance (CPU exhaustion attack). This mechanism forces the attacker to perform an additional network round trip and respond to the cookie for each handshake attempt. This significantly increases the cost of the attack, making it much less effective, while allowing the server to limit the number of DH computations it must perform, thus protecting its resources.

When the cookie challenge is enabled, the device always sends a cookie-reply message during the handshake.

Connection list

This section defines the WireGuard connections.



Connection

Name of the WireGuard connection or WireGuard peer.

Connection active

Enables or disables this connection.

Local port

Defines the local (UDP) port on which this connection should be accepted by the device. The configured local private key must be identical for all connections using the same port. Multiple configured connections using the same local port but different private keys are not supported and will prevent connections from being established or the internal configuration from being created.

For a WireGuard tunnel using IPv6 as a transport protocol, the incoming UDP ports for the tunnel must be manually configured or allowed in the IPv6 firewall's inbound table.

Remote gateway

IPv4, IPv6, or DNS address of the remote gateway or client. If the IP address of the remote side is unknown or dynamic, the field can be left blank. In this case, the connection must be initiated from the remote side. If an explicit IP address is configured, it must exactly match during connection establishment.

Allowed values: IPv4 address, IPv6 address, 0.0.0.0, ::, or empty. The values 0.0.0.0 and :: for IPv6 have the same effect as an empty entry.

Remote port

Port number on the remote gateway side. If the remote port for incoming connections is dynamic or unknown, it can be left empty or set to 0. If an explicit port is configured, it must exactly match during connection setup; otherwise, the connection will be rejected or discarded.

Allowed values: Port, 0, or empty entry.

Routing tag

Defines the routing tag through which the WireGuard connection is established.

Local private key

Local private key for the WireGuard connection in Base64 format. Hex-formatted keys are not supported. The device automatically derives its public key from the local private key.

The configured local private key must be identical for all connections using the same local port. Multiple configured connections using the same port but different private keys are not supported and will prevent connections from being established or the internal configuration from being created.

The local private key is confidential and is generally not shared with the remote side—unless an administrator generates key pairs for managed devices. In this case, the administrator knows all device key pairs.

Peer public key

Public key of the remote gateway in Base64 format. Hex-formatted entries are not supported.

Each communication partner in the WireGuard connection must generate its own unique public/private key pair and share its public key with the remote side.

Peer private key

The peer private key is optional and only configured when LANconfig is used to generate a configuration or QR code for the remote side. It is not required for LCOS functionality and is only stored so that the configuration for the remote side can be displayed or regenerated later.

Shared key

An optional additional key used alongside the public/private key pair for the connection. The key must be configured identically on both communication partners.

IPv6 profile

This entry defines the IPv6 WAN profile. An empty entry disables IPv6 for this interface.

IPv6 WAN profiles are configured under IPv6 > General > IPv6 interfaces > WAN profiles.

Comment

Enter a comment for this entry.

5.1.3.1 Configuration Profiles for Clients

Within the WireGuard configuration page, LANconfig can generate minimal configuration profiles for remote WireGuard clients in the WireGuard configuration format, either as plain text or as a QR code. This configuration can be imported into compatible WireGuard clients via copy & paste or scanned directly from a mobile app using the QR code.

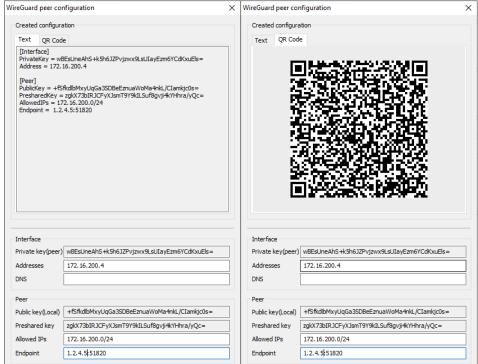
This function works similarly to a wizard, but with the advantage that the generated configuration can be recalled and displayed again at any time.

However, for this to work, the router or LANconfig must store the private key of the remote side — something that is typically undesirable when WireGuard peers belong to different administrative domains. Normally, each communication partner generates its own private/public key pair and shares only the public key with the remote side. The private key remains secret and is only known to the respective partner. This function is ideally suited for administrators who want to generate configurations for devices under their own control.

The parameters DNS and Pre-Shared Key are optional. All other parameters must be entered in order to generate a minimal configuration.

The parameters **Address**, **Allowed IPs**, and **Endpoint** are not stored by LANconfig and must be re-entered when the configuration is reopened.





Supported configuration parameters for the remote side:

Interface

Private key (peer)

Defines the client's private key.

Addresses

Local IP address of the WireGuard interface on the client side.

DNS

DNS server that the client should use for name resolution (optional).

Peer

From the perspective of the remote client, the LCOS device acts as the peer.

Public key (local)

Public key of the LCOS device.

Preshared key

Optional additional key used alongside the public/private key pair for the connection. The key must be configured identically on both communication partners.

Allowed IPs

IP addresses that the client should route into or allow through the WireGuard tunnel. The local networks of the router that the client should access must be specified here.

Endpoint

Public IP address including port in the format <IP address>:<Port> of the LCOS device to which the client should establish the connection.

QR Code

Using the displayed QR code, you can import the configuration into a WireGuard app. Open the WireGuard app and add a new peer via QR code. Additional parameters can then be modified or added if necessary.

5.1.4 Trace Commands

This parameter	triggers the following display during tracing:
WireGuard	Enables the basic WireGuard traces of negotiation packets as well as status and debug information.
WG-Packet	Displays the WireGuard payload packets.

5.1.5 Show commands

- > wg-connection Displays information about WireGuard connections
- > wg-detail Displays detailed information about WireGuard connections
- > wg-peer Displays information about configured WireGuard peers

5.1.6 Additions to the Setup menu

5.1.6.1 WireGuard

WireGuard is a simple and lightweight VPN protocol. Unlike IKEv2/IPSec, WireGuard focuses on simplicity, speed, and ease of use. It is also a protocol with a very compact code base and functionality, making it ideal for use on IoT and embedded devices.

A WireGuard configuration in LCOS consists of at least two configuration elements, as well as additional optional elements:

- 1. An entry in the WireGuard tunnel configuration table.
- **2.** An entry in the IPv4 and/or IPv6 routing table. This entry corresponds to the concept of "Allowed IP Addresses" in WireGuard on other platforms.
- **3.** (Optional) Configure local IP addresses for the WireGuard peer via the IP Parameters table in LANconfig under **Communication** > **Protocols** > **IP Parameters**.
- **4.** (Optional) Firewall configuration for granular control of network access rights.

SNMP ID:

2.19.70

Console path:

Setup > VPN

5.1.6.1.1 Operating

Enables or disables the WireGuard function on the device.

5 Virtual Private Networks - VPN

SNMP ID:

2.19.70.1

Console path:

Setup > VPN > WireGuard

Possible values:

No

Yes

Default:

No

5.1.6.1.2 Cookie-Challenge

The cookie challenge is a protection mechanism against CPU exhaustion attacks during the handshake process. The computation of the Diffie-Hellman (DH) function during the WireGuard handshake is inherently CPU-intensive. An attacker could attempt to overload the router by sending a large number of handshake requests to crash it or severely impact its performance (CPU exhaustion attack). This mechanism forces the attacker to perform an additional network round trip and respond to the cookie for each handshake attempt. This significantly increases the cost of the attack, making it much less effective, while allowing the server to limit the number of DH computations it must perform, thus protecting its resources.

When the cookie challenge is enabled, the device always sends a cookie-reply message during the handshake.

SNMP ID:

2.19.70.2

Console path:

Setup > VPN > WireGuard

Possible values:

No

Yes

Default:

No

5.1.6.1.3 Peers

This table defines the WireGuard connections.

SNMP ID:

2.19.70.3

Console path:

Setup > VPN > WireGuard

Peer

Name of the WireGuard connection or WireGuard peer.

SNMP ID:

2.19.70.3.1

Console path:

```
Setup > VPN > WireGuard > Peers
```

Possible values:

```
Max. 16 characters from [A-Z][0-9]@{|}^{-1} %&'()+-,/:;<=>?[\]^.
```

Default:

empty

Active

Enables or disables this connection.

SNMP ID:

2.19.70.3.2

Console path:

Setup > VPN > WireGuard > Peers

Possible values:

No

Yes

Default:

Yes

Local-Port

Defines the local (UDP) port on which this connection should be accepted by the device. The configured local private key must be identical for all connections using the same port. Multiple configured connections using the same local port but different private keys are not supported and will prevent connections from being established or the internal configuration from being created.

For a WireGuard tunnel using IPv6 as a transport protocol, the incoming UDP ports for the tunnel must be manually configured or allowed in the IPv6 firewall's inbound table.

5 Virtual Private Networks - VPN

SNMP ID:

2.19.70.3.3

Console path:

```
Setup > VPN > WireGuard > Peers
```

Possible values:

Max. 5 characters from [0-9]

Default:

51820

Remote-Gateway

IPv4, IPv6, or DNS address of the remote gateway or client. If the IP address of the remote side is unknown or dynamic, the field can be left blank. In this case, the connection must be initiated from the remote side. If an explicit IP address is configured, it must exactly match during connection establishment.

Allowed values: IPv4 address, IPv6 address, 0.0.0.0, ::, or empty. The values 0.0.0.0 and :: for IPv6 have the same effect as an empty entry.

SNMP ID:

2.19.70.3.4

Console path:

```
Setup > VPN > WireGuard > Peers
```

Possible values:

```
Max. 64 characters from [A-Z][a-z][0-9].-:%?
```

Default:

empty

Remote-Port

Port number on the remote gateway side. If the remote port for incoming connections is dynamic or unknown, it can be left empty or set to 0. If an explicit port is configured, it must exactly match during connection setup; otherwise, the connection will be rejected or discarded.

Allowed values: Port, 0, or empty entry.

SNMP ID:

2.19.70.3.5

Console path:

```
Setup > VPN > WireGuard > Peers
```

Possible values:

Max. 5 characters from [0-9]

Default:

51820

Rtg-Tag

Defines the routing tag through which the WireGuard connection is established.

SNMP ID:

2.19.70.3.6

Console path:

```
Setup > VPN > WireGuard > Peers
```

Possible values:

0 ... 65535

Default:

0

Local-Private-Key

Local private key for the WireGuard connection in Base64 format. Hex-formatted keys are not supported. The device automatically derives its public key from the local private key.

The configured local private key must be identical for all connections using the same local port. Multiple configured connections using the same port but different private keys are not supported and will prevent connections from being established or the internal configuration from being created.

The local private key is confidential and is generally not shared with the remote side—unless an administrator generates key pairs for managed devices. In this case, the administrator knows all device key pairs.

SNMP ID:

2.19.70.3.7

Console path:

```
Setup > VPN > WireGuard > Peers
```

Possible values:

```
Max. 44 characters from [A-Z][a-z][0-9]+/=
```

Default:

empty

Peer-Private-Key

The peer private key is optional and only configured when LANconfig is used to generate a configuration or QR code for the remote side. It is not required for LCOS functionality and is only stored so that the configuration for the remote side can be displayed or regenerated later.

5 Virtual Private Networks - VPN

```
SNMP ID:
```

2.19.70.3.9

Console path:

```
Setup > VPN > WireGuard > Peers
```

Possible values:

```
Max. 44 characters from [A-Z][a-z][0-9]+/=
```

Default:

empty

Peer-Public-Key

Public key of the remote gateway in Base64 format. Hex-formatted entries are not supported.

Each communication partner in the WireGuard connection must generate its own unique public/private key pair and share its public key with the remote side.

SNMP ID:

2.19.70.3.10

Console path:

```
Setup > VPN > WireGuard > Peers
```

Possible values:

```
Max. 44 characters from [A-Z][a-z][0-9]+/=
```

Default:

empty

Shared-Key

An optional additional key used alongside the public/private key pair for the connection. The key must be configured identically on both communication partners.

SNMP ID:

2.19.70.3.11

Console path:

```
Setup > VPN > WireGuard > Peers
```

Possible values:

```
Max. 44 characters from [A-Z][a-z][0-9]+/=
```

Default:

IPv6

This entry defines the IPv6 WAN profile. An empty entry disables IPv6 for this interface.

SNMP ID:

2.19.70.3.13

Console path:

```
Setup > VPN > WireGuard > Peers
```

Possible values:

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

Default:

empty

Comment

Enter a comment for this entry.

SNMP ID:

2.19.70.3.14

Console path:

```
Setup \ > VPN \ > WireGuard \ > Peers
```

Possible values:

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

Default:

6 Voice over IP - VoIP

6.1 Configuration of Lines: SIP Lines

As of LCOS 10.94, it is possible to enter a phone number in the **Account-Number** field of the SIP Lines table (**Voice-Call-Manager** > **Lines** > **SIP Lines**) that belongs to this SIP connection.

6.1.1 Additions to the Setup menu

6.1.1.1 Account-Number

Enter here a phone number that belongs to this SIP connection.

For SIP lines of the type "Flex", this source number is transmitted in the PPI for account verification.

If the FROM number is modified by call routing or if the SIP phone sends a number that does not match the connection, this will not cause the call to be rejected by the provider.

This allows CLIP no screening calls to be made directly via the VCM, provided the feature is supported by the SIP provider.

SNMP ID:

2.33.4.1.1.43

Console path:

 $\mbox{Setup} > \mbox{Voice-Call-Manager} > \mbox{Line} > \mbox{SIP-Provider} > \mbox{Line}$

Possible values:

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

Default:

empty

6.2 Prioritized Phone Numbers

As of LCOS 10.94, emergency phone numbers can be stored.

6.2.1 Additions to the Setup menu

6.2.1.1 Preferred-Numbers

Enter emergency phone numbers in this table. If a call to an emergency number cannot be established due to an error message from the SIP provider, an existing call that is using this line (line type Trunk/Flex) or the associated line group (line type Single Account/Provider) will be terminated. This ensures that a voice channel is available for the emergency call.

A line group is defined in the "Dynamic SIP Lines" table. SIP lines with the same "Dynamic-Line-Name" belong to the same group. Typically, these are multiple individual numbers that together provide a certain number of voice channels.

SNMP ID:

2.33.12.1

Console path:

Setup > Voice-Call-Manager > Call-Handling

6.2.1.1.1 Called-Number

Enter your phone number here.

SNMP ID:

2.33.12.1.1

Console path:

Setup > Voice-Call-Manager > Call-Handling > Preferred-Numbers

Possible values:

Max. 19 characters from $[A-Z][0-9]#@{|}~!$%&'()+-,/:;<=>?[]^_.$

Default:

empty

6.2.1.1.2 Type

Enter the phone number type here.

SNMP ID:

2.33.12.1.2

Console path:

Setup > Voice-Call-Manager > Call-Handling > Preferred-Numbers

Possible values:

Emergency

This is an emergency number.

Private

This number disables the overlap dialing wait time for this destination.

6.2.1.1.3 Comment

Enter a comment for the selected phone number here.

SNMP ID:

2.33.12.1.4

6 Voice over IP – VoIP

Console path:

Setup > Voice-Call-Manager > Call-Handling > Preferred-Numbers

Possible values:

Max. 63 characters from $[A-Z][a-z][0-9]\#@{|}^{-!}\%&'()*+-,/:;<=>?[]^_. `$

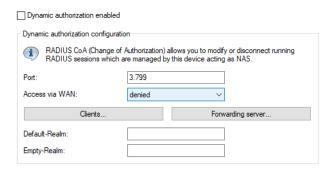
Default:

7 RADIUS

7.1 RADIUS CoA for 802.1X Authenticator Ethernet Ports

The 802.1X Authenticator for Ethernet ports supports RADIUS Change of Authorization (CoA) and Disconnect Messages (DM) for 802.1X, as well as for authentication based on MAC addresses.

The shared configuration for Dynamic Authorization is used. In LANconfig under **RADIUS** > **Dyn. Authorization** and on the CLI under **Setup** > **RADIUS** > **Dyn-Auth.**. This configuration is also used by Public Spot or IKEv2.



The following CoA functions are supported:

- > Disconnecting the session of a current user (Disconnect Message)
- > Changing the current user session by modifying the VLAN via a CoA message

Examples:

1. The currently active sessions can be displayed via the status menu:



2. The status for CoA can be displayed with the show command "show ethernet-dynauth":

```
> show ethernet-dynauth
MAC address e8:9c:25:5b:7b:86 on ETH-2: NAS-Identifier 'test-8021x-dm', User-Name 'test'
```

3. A user session can be disconnected using the CLI command "Radclient" under Setup > RADIUS > Dyn-Auth. in the LCOS, for example:

```
do Radclient 192.168.1.112 disconnect 12345678 "NAS-Identifier=test-8021x-dm;User-Name=test;"
```

Where:

- > "192.168.1.112" is the IP address of the NAS, i.e., the router
- > "disconnect" is the disconnect message to be sent
- > "12345678" is the configured Dyn-Auth/CoA password
- > "NAS-Identifier" is the name of the router or the unique identifier of the NAS
- > "User-Name" is the 802.1X username used by the client during authentication

7 RADIUS

All of these parameters are required.

4. The VLAN of an active session for a MAC-authenticated user can be changed as follows:

do Radclient 192.168.1.112 coa 12345678 "NAS-Identifier=test-8021x-dm;User-Name=e89c255b7b86;
Tunnel-Type:0=VLAN;Tunnel-Medium-Type:0=IEEE-802;Tunnel-Private-Group-Id:0=200;

Where:

- > "192.168.1.112" is the IP address of the NAS, i.e., the router
- > "coa" is the CoA message to be sent
- > "12345678" is the configured Dyn-Auth/CoA password
- > "NAS-Identifier" is the name of the router or the unique identifier of the NAS
- > "Tunnel-Type:0=VLAN;Tunnel-Medium-Type:0=IEEE-802;Tunnel-Private-Group-Id:0=200" are the required RADIUS attributes to move the client into VLAN 200

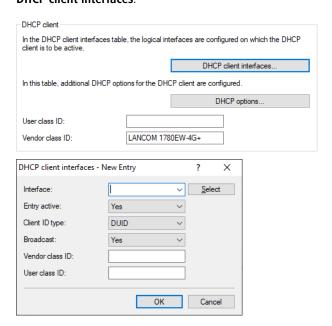
All of these parameters are required.

For analyzing CoA functionality, the traces "DYN-AUTH-Client" and "DYN-AUTH-Server" are available.

8 Other services

8.1 New DHCPv4 Client Configuration

As of LCOS 10.94, you can configure client interfaces of the DHCP client for IPv4 under IPv4 > DHCPv4 > DHCPv4 > DHCP client > DHCP client interfaces.



Interface

Name of the interface on which the client is active (LAN, physical WAN, or WWAN interface). Depending on the device, default entries for Zero Config exist after a system reset: "INTERNET-DHCPDEF", "INTERNET-DEFAULT".

Entry active

Switch to specify whether this entry is active.

Client ID type

Switch that specifies the type of client ID.

Broadcast

Switch that specifies the type of client ID.

Vendor class ID

String containing the vendor class identifier to be reported on this interface. If this value is empty, the (global) value under IPv4 > DHCPv4 > DHCP client > Vendor class ID will be used.

User class ID

String containing the user class identifier to be reported on this interface. If this value is empty, the (global) value under IPv4 > DHCPv4 > DHCP client > User class ID will be used.

8 Other services

Other changes

- > Under setup > dhcp > client (SNMP ID 2.10.40), the menu items LAN-Client-ID-Type (SNMP ID 31) and WAN-Client-ID-Type (SNMP ID 32) have been removed, as the values can now be set per client.
- Under setup > dhcp > network-list (SNMP ID 2.10.20), the option "Client" was removed from the Operating switch.
- > Under **setup** > **wan** > **layer** (SNMP ID 2.2.4), the values "DHCP" and "B-DHCP" were removed from the **Layer-3** column (SNMP ID 3).
- > A configuration converter performs the following actions:
 - > For all WAN connections using a layer with DHCP or B-DHCP, an entry is created in the **setup** > **dhcp** > **client** > **interfaces** table. This applies to DSL, xDSL, and WWAN connections.
 - For all LAN interfaces where the operating switch is set to "Client", an entry is created in the **setup** > **dhcp** > **client** > **interfaces** table. In addition, the corresponding entry is removed from **setup** > **dhcp** > **network-list**.

8.1.1 Additions to the Setup menu

8.1.1.1 Interfaces

Use this table to configure the IPv4 DHCP client interfaces.

SNMP ID:

2.10.40.1

Console path:

Setup > DHCP > Client

8.1.1.1.1 Interface

Name of the interface on which the client is active (LAN, physical WAN, or WWAN interface). Depending on the device, default entries for Zero Config exist after a system reset: "INTERNET-DHCPDEF", "INTERNET-DEFAULT", or "WWAN-DEFAULT".

SNMP ID:

2.10.40.1.1

Console path:

```
Setup > DHCP > Client > Interfaces
```

Possible values:

```
Max. 16 characters from [A-Z][0-9]@{|}^{-1} .
```

Default:

empty

8.1.1.1.2 Operating

Switch to specify whether this entry is active.

```
SNMP ID:
    2.10.40.1.2
Console path:
    Setup > DHCP > Client > Interfaces
Possible values:
    No
    Yes
Default:
    Yes
8.1.1.1.3 Client-ID-Type
Switch that specifies the type of client ID.
SNMP ID:
    2.10.40.1.3
Console path:
    Setup > DHCP > Client > Interfaces
Possible values:
    MAC
    DUID
Default:
    DUID
8.1.1.1.4 Broadcast
Switch that specifies whether the client sets the "Broadcast" flag. On a LAN interface, this value is always set to "Yes".
SNMP ID:
    2.10.40.1.4
```

Console path:

Setup > DHCP > Client > Interfaces

8 Other services

Possible values:

No

Yes

Default:

Yes

8.1.1.1.5 Vendor-Class-Identifer

String containing the vendor class identifier to be reported on this interface. If this value is empty, the (global) value under *2.10.40.3 Vendor class identifier* is used.

SNMP ID:

2.10.40.1.5

Console path:

```
Setup > DHCP > Client > Interfaces
```

Possible values:

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

Default:

empty

8.1.1.1.6 User-Class-Identifer

String containing the user class identifier to be reported on this interface. If this value is empty, the (global) value under 2.10.40.2 User-Class-Identifier is used.

SNMP ID:

2.10.40.1.6

Console path:

```
Setup > DHCP > Client > Interfaces
```

Possible values:

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

Default:

9 Enhancements in the menu system

9.1 Additions to the Setup menu

9.1.1 Parameter-Format

As of LCOS version 10.94, the new parameter lineid is supported.

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

- > {txrate} Upstream-Rate
- > {rxrate} Downstream-Rate
- > {lineid} Line ID of the connection. This is displayed for information purposes only or to identify the line.

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

SNMP ID:

2.2.62.2

Console path:

Setup > WAN > Provider-Specifics

Possible values:

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

Default:

empty

9.1.2 Key-Exchange-Algorithms

As of LCOS version 10.94, SSH supports mlkem768x25519-sha256 algorithm.

The MAC key exchange algorithms are used to negotiate the key algorithm. Select one or more of the available algorithms.

SNMP ID:

2.11.28.3

Console path:

Setup > Config > SSH

9 Enhancements in the menu system

Possible values:

diffie-hellman-group1-sha1
diffie-hellman-group14-sha1
diffie-hellman-group-exchange-sha1
diffie-hellman-group-exchange-sha256
ecdh-sha2
curve25519-sha256
curve448-sha512
sntrup761x25519-sha512
diffie-hellman-group14-sha256
diffie-hellman-group16-sha512
diffie-hellman-group17-sha512
diffie-hellman-group18-sha512
sntrup4591761x25519-sha512
mlkem768x25519-sha256

Hybrid post-quantum algorithm mlkem768x25519. In this case, the post-quantum algorithm ML-KEM (Module-Lattice-Based Key-Encapsulation Mechanism) is combined with the well-known classical method Curve25519.

Default:

diffie-hellman-group-exchange-sha256
ecdh-sha2
curve25519-sha256
curve448-sha512
sntrup761x25519-sha512
diffie-hellman-group14-sha256
diffie-hellman-group15-sha512
diffie-hellman-group16-sha512

mlkem768x25519-sha256

9.1.3 IPv4-WAN-Access

Defines whether access from WAN interfaces to the DNS server or DNS forwarder via IPv4 is generally allowed. Access to these services via IPv6 is controlled exclusively through the IPv6 inbound firewall.

Access can be controlled globally for the corresponding interface types using this switch. For more granular control than this level, corresponding IPv4 firewall rules can be configured.

Access to the DNS service must be allowed via VPN if VPN clients are to use the router as a DNS server or DNS forwarder, for example, to resolve locally configured station names.

Access to the DNS service via WAN must be allowed if clients are to connect to the router using PPPoE, L2TP, or PPTP. In this case, it is recommended to configure granular control for the local DNS service via firewall rules.

VPN interfaces include IPSec VPN (IKEv1/IKEv2) and WireGuard. WAN interfaces include all WAN counterparts such as Internet connections and RAS dial-ins to the LANCOM router acting as a PPPoE, PPTP, or L2TP server.

SNMP ID:

2.17.18

Console path:

Setup > DNS

Possible values:

Nο

Access to the DNS server and DNS forwarder via IPv4 from WAN and VPN interfaces is not allowed.

Yes

Access to the DNS server and DNS forwarder via IPv4 is generally allowed from all interfaces such as LAN, WAN, and VPN.

VPN

Access to the DNS server and DNS forwarder via IPv4 is allowed from LAN interfaces and via VPN (IPSec VPN and WireGuard). Access from WAN interfaces, such as Internet connections or RAS dial-ins to the LANCOM router acting as a PPPoE, PPTP, or L2TP server, is not allowed.

Default:

VPN

9.1.4 Elliptic curves

As of LCOS version 10.94, the hybrid post-quantum algorithm X25519MLKEM768 is supported for TLS. Here you specify which elliptic curves are to be used for encryption.

SNMP ID:

2.21.40.9

Console path:

Setup > HTTP > 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.

9 Enhancements in the menu system

x448

x448 is used for encryption.

X25519MLKEM768

X25519MLKEM768 is used for encryption. The X25519MLKEM768 algorithm combines the post-quantum algorithm ML-KEM (Module-Lattice-Based Key-Encapsulation Mechanism) with the well-known classical algorithm Curve25519. Post-quantum algorithm key agreement is only supported for TLS 1.3. For TLS 1.2, this new algorithm cannot be used, as it is not defined in the standard by the IETF.

Default:

secp256r1

secp384r1

secp521r1

x25519

x448

X25519MLKEM768

10 Discontinued Features

As of LCOS 10.94, the following features have been discontinued:

- > AutoWDS (2.37.1.15, 2.37.1.16, 2.59.4)
- > LANCOM Battery Pack (2.97)
- > The value "Exclusive" has been removed from **Setup** > **WAN** > **RADIUS** > **Active**. Existing configurations have been changed to "Yes", so RADIUS remains active.